Informacja Kwantowa 1/2

Seria przygotowawcza do egzaminu, 2014

Zadanie 1 Wyobraźmy sobie że wiadomość którą chcą przesłać jest zbudowana z czterech rodzajów znaków ♣, ♢, ♡, ♠. przy czym znak ♣ występuje średnio z częstością 1/2, znak ♢ z częstością 1/4, znak ♡ z częstością 1/8 i znak ♠ z częstością 1/8. Jeśli spróbują sprytnie skompresować swoją wiadomość przed szyfrowaniem to jak długą w przybliżeniu wiadomosc mogą wysłać stosując szyfrowanie *one-time pad* przy użyciu N bitowego klucza (zakładamy, że N jest duże). Przez długość wiadomości rozumiemy liczbę znaków ♣, ♢, ♡, ♠ w wiadomości.

Zadanie 2 Poniżej podanych jest kilka par stanów. Uszereguj pary od pary zawierającej stany najłatwiej rozróżnialne do pary zawierającej stany najtrudniej rozróżnialne (jesli rozróżnialność jest taka sama dla jakiś par zaznacz to). Stan $|\alpha\rangle$ oznacza stan fotonu o polaryzacji liniowej pod kątem α do poziomu.

a) $|30°\rangle$, $|60°\rangle$

b) $|30°\rangle$, $|120°\rangle$

c) $|30°\rangle^{\otimes 2}$, $|120°\rangle^{\otimes 2}$

d) $|30°\rangle^{\otimes 2}$, $|60°\rangle^{\otimes 2}$

Zadanie 3 Alicja wysyła Bobowi qubit przygotowany z w jednym z czterech stanów:

$$|\tau_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\tau_2\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}, |\tau_3\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ e^{2\pi i/3}\sqrt{2} \end{pmatrix}, |\tau_4\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ e^{-2\pi i/3}\sqrt{2} \end{pmatrix}.$$

Bob mierzy qubit przy użyciu miary opisanej czterema operatorami $\hat{M}_i = \frac{1}{2} |\upsilon_i\rangle \langle\upsilon_i|, i = 1, 2, 3, 4$, gdzie

$$|\upsilon_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |\tau_2\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} \sqrt{2} \\ -1 \end{pmatrix}, |\tau_3\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} e^{-2\pi i/3}\sqrt{2} \\ -1 \end{pmatrix}, |\tau_4\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} e^{2\pi i/3}\sqrt{2} \\ -1 \end{pmatrix}.$$

a) Znaleźć prawdopodobieństwa warunkowe $p(i|j) = \langle\tau_j| \hat{M}_i |\tau_j\rangle$ otrzymania wyniku i jeśli Alicja wysłała stan $|\tau_j\rangle$.

b) Obliczyć informację wzajemną $I(A : B)$ gdy stany $|\tau_j\rangle$ są wysyłane przez Alicję z jednakowymi prawdopodobieństwami wynoszącymi $\frac{1}{4}$.

c) Oblicz wielkość Holevo odpowiadającą tej komunikacji, skomentuj wynik.

Zadanie 4 W jednej z serii domowych rozważyliśmy operację klonowania stanów z równika sfery Blocha. Transformacja miała postać:

$$U |0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \frac{1}{\sqrt{2}} |0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} + \frac{1}{\sqrt{2}} |\Psi_+\rangle_{AE} \otimes |1\rangle_{E'} \quad (1)$$

$$U |1\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \frac{1}{\sqrt{2}} |1\rangle_A \otimes |1\rangle_E \otimes |1\rangle_{E'} + \frac{1}{\sqrt{2}} |\Psi_+\rangle_{AE} \otimes |0\rangle_{E'} \quad (2)$$

gdzie $|\Psi_+\rangle = (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)/\sqrt{2}$, a podukłady pisane są w kolejności: stan A (klon 1), E (klon 2), E' (maszyna klonująca). Transformację można było wykorzystac jako atak na protokół BB84 i w ten sposób uzykać ograniczenie na maksymalną wartość QBER przy którym możliwa jest destylacja klucza. Rozważ nieco inną transformację klonującą U sparametryzowaną przez $\gamma \in [0, 1]$:

$$U |0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \sqrt{\gamma} |0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} + \sqrt{1-\gamma} |\Psi_+\rangle_{AE} \otimes |1\rangle_{E'} \quad (3)$$

$$U |1\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \sqrt{\gamma} |1\rangle_A \otimes |1\rangle_E \otimes |1\rangle_{E'} + \sqrt{1-\gamma} |\Psi_+\rangle_{AE} \otimes |0\rangle_{E'} \quad (4)$$

a) Jeśli wziąć parametr tak jak na ćwiczeniach, czyli $\gamma = 1/2$ wtedy transformacja nie wyróżniała żadnego ze stanów leżących na równiku sfery Blocha. A czy taka transformacja działała by w analogiczny sposób na stany z biegunów sfery Blocha? Ma to znaczenie jeśli chcielibyśmy zastosować nasz atak do protokołu 6-ścio stanowego a nie tylko do BB84. Postaraj się znaleźć taką wartość parametru γ dla którego powyższa operacja nie wyróżniałaby żadnej z trzech baz używanej w protokole 6-ścio stanowym — co oznacza że prawdopodobieństwo błędu w wyniku pomiaru klonu 1 oraz klonu 2 byłoby takie samo niezależnie od tego który stan został wysłany przez A.

b) Zastosuj tę optymalną operację klonującą aby przeanalizować bezpieczeństwo 6-ścio stanowego protokołu kryptografii kwantowej. Powyżej jakiego QBER, A i B nie mogą się czuć bezpieczni? Na ile ten wynik jest silniejszy od wyników jakie uzyskiwaliśmy używając bardziej prymitywnych ataków typu zmierz-odeślij?

c) Wiemy, że stan mieszany qubitu możemy przestawić za pomocą wektora $\vec{s}$ w kuli Blocha

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{s} \cdot \vec{\sigma})$$

(jeśli $|\vec{s}| = 1$, czyli jesteśmy na sferze Blocha to mamy stany czyste, a im bardziej do środka tym bardziej mamy stany mieszane). Jeśli by patrzeć na dowolny czysty stan wejściowy $|\psi\rangle_A$ a następnie na któryś z klonów tego stanu, który oczywiście będzie stanem mieszanym, to jak to by wyglądało w języku wektora Blocha. — podaj geometryczny opis co się dzieje z wektorem Blocha w wyniku klonowania qubitu, które znalazłe(a)ś w podpunkcie a).

Zadanie 5 Rozważ transformację unitarną działająca na dwóch qubitach, zdefiniowaną w następujący sposób:

$$U |0\rangle_1 \otimes |0\rangle_2 = |0\rangle_1 \otimes |0\rangle_2 \quad (5)$$

$$U |1\rangle_1 \otimes |0\rangle_2 = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2) \quad (6)$$

a) Zadziałaj macierzą U na stan wejściowy postaci $|\psi\rangle_1 \otimes |0\rangle_2$, gdzie $|\psi\rangle$ jest dowolnym stanem qubitu i napisz wyjściową zredukowaną macierz gęstości qubitu 1.

b) Podaj interpretację graficzną tego co się dzieje ze stanami qubitu 1, korzystając z obrazu kuli Blocha

c) Zapisz za pomocą operatorów Krausa efektywne odwzorowanie któremu poddawany jest qubit 1 w tej sytuacji.

d) Jak może zauważyłeś powyższa definicja operacji U nie jest kompletna (choć wystarczająca do rozwiązania wcześniejszych punktów). Do pełnej definicji U należałoby dodatkowo podać jak U działa na stany $|0\rangle \otimes |1\rangle$ oraz $|1\rangle \otimes |1\rangle$. Zaproponuj jakiekolwiek uzupełnienie definicji tak by U rzeczywiście była operacją unitarną.

Zadanie 6 Mając stan dwóch podukładów ρ_{AB}, kryterium splątania PPT mówi, że jeśli macierz $\rho_{AB}^{T_B}$ (częściowa transpozycja względem układu B), nie jest dodatnio określona to stan jest splątany. Na ćwiczeniach rozważaliśmy stan dwóch qubitów:

$$\rho = p \left|\Psi^-\right\rangle \left\langle\Psi^-\right| + \frac{(1-p)}{4} \mathbb{1} \tag{7}$$

gdzie $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ i pokazaliśmy, że dla $p > 1/3$ kryterium PPT mówi, że stan jest splątany. Na podstawie kryterium PPT nie ma natomiast pewności, że dla $p \leq 1/3$ stan jest separowalny. [1]

Żeby to pokazać można po prostu dla $p \leq 1/3$ spróbować jawnie napisać rozkład stanu ρ_{AB} na stany produktowe i wtedy mamy już kompletne rozwiązanie. Postaraj się znaleźć taki rozkład.

Wskazówka. Najpierw udowodnij, że trzy stany postaci

$$\rho_i = \frac{1}{4} \left(\mathbb{1} \otimes \mathbb{1} - \sigma_i \otimes \sigma_i\right), \tag{8}$$

gdzie σ_i są trzema macierzami Pauliego, są separowalne pisząc ich jawny rozkład na mieszankę stanów produktowych. Potem zmierz się z przypadkiem $p = 1/3$ a następnie z $p < 1/3$.

Zadanie 7 Łamanie nierówności Bella można traktować jako kryterium splątania. Wiemy, że kryterium PPT w pełni pozwala nam opisać zakres wartości parametru p dla którego stan postaci:

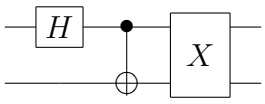
$$\rho = p \left|\Psi^-\right\rangle \left\langle\Psi^-\right| + \frac{(1-p)}{4} \mathbb{1} \tag{9}$$

jest splątany a dla jakich p jest separowalny.

Na zajęciach pokazane było, że stan $|\Psi^-\rangle$ maksymalnie łamie nierówność Bella dając wynik $|C| = 2\sqrt{2}$. Zbadaj dla jakich p stan ρ będzie łamał nierówność Bella. Czy nierówności Bella są równie dobrym kryterium splątania co PPT?

Zadanie 8 Rozważ zbiór zawierający wszystkie stany czyste leżące na sferze Blocha na równoleżniku a szerokości geograficznej θ. Jaki jest asymptotycznie maksymalny możliwy współczynnik kompresji stanu produktowego n qubitów, gdzie stan pojedynczego qubitu jest niezależnie losowany przypadkowo z powyższego zbioru.

Zadanie 9 Rozważ obwód kwantowy postaci:



[1] Dla dwóch qubitów okazuje się, że kryterium PPT daje taką pewność, ale my tego nie udowodniliśmy, więc udajemy, że o tym nie wiemy.

gdzie X jest bramką dwuqubitową dokonującą operacji:

$$\begin{aligned} |0\rangle \otimes |0\rangle &\rightarrow \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right) \\ |1\rangle \otimes |1\rangle &\rightarrow \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle\right) \end{aligned}$$

a pozostałe wektory bazowe pozostawia bez zmian.

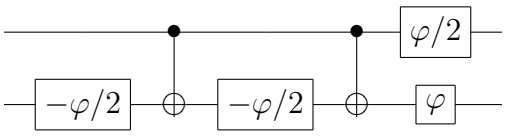
a) Napisz macierz odpowiadającą powyższemu obwodowi kwantowemu

b) Jaki stan uzyskamy na wyjściu obwodu jeśli wpuścimy do niego stan $|0\rangle \otimes |0\rangle$

c) Napisz macierz odpowiadającą operacji odwrotnej

d) Narysuj obwód kwantowy operacji odwrotnej

Zadanie 10 Rozważ następujący układ bramek kwantowych:



(10)

gdzie $\boxed{\varphi} = \begin{bmatrix} 1 & 0 \\ 0 & \exp(\mathrm{i}\varphi) \end{bmatrix}$ jest jednoqubitową bramką fazową.

a) Zapisz macierz tej transformacji (nazwijmy ją G) i zinterpretuj ją w jak najprostszy sposób

b) Załóżmy, że mamy do dyspozycji stan wejściowy $|0\rangle \otimes |0\rangle$, dowolne bramki jednoqubitowe oraz bramkę G. Zaprojektuj układ produkujący stan Bella $|\Psi_-\rangle = (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)/\sqrt{2}$.

c) Podaj implementacje optyczną powyższego schematu wytwarzania stanu Bella na qubitach polaryzacyjnych, traktując bramkę G jako czarną skrzynkę a opisując jedynie implementacje bramek jednoqubitowych. Czy bramkę G łatwo byłoby zrealizować w implementacji optycznej?