Komunikacja i Kryptografia Kwantowa

Seria 7

Odpowiedzi

Zadanie 1 (25 pkt) Na wykładzie wyprowadziliśmy minimalny średnie poziom błędu jaki się popełnia próbując rozróżnić dwa stany nieortogonalne $|\psi_1\rangle$, $|\psi_2\rangle$. Przez proste uogólnienie wyprowadziliśmy również minimalny średni poziom błędu przy rozróżnianiu gdy otrzymujemy n kopii jednego z tych dwóch stanów:

$$\langle E\rangle = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^{2n}}\right). \tag{1}$$

Rozważ teraz „lokalną” strategię rozróżniania polegającą na wykonywaniu na każdej z kopii pomiaru który byłby optymalny w sytuacji gdybyśmy otrzymywali tylko po jednym egzemplarzu stanu. Zastanów się jakieś byś zastosował(a) wnioskowanie, aby na podstawie uzyskanych wyników stwierdzić czy otrzymaliśmy stan $|\psi_1\rangle^{\otimes n}$ czy $|\psi_2\rangle^{\otimes n}$. Podaj wyrażenie na poziom błędów i porównaj go z (1). Dla obu strategii (optymalnej i „lokalnej”), narysuj wykres poziomu błędu od n dla przypadku $|\psi_1\rangle = |0\rangle$, $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

Odpowiedź Przyjmujemy strategię, że zgadujemy stan który nam częściej wypadł. Jeśli $e = 1/2(1 - \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2})$ jest prawdopodobieństwem błędu w pojedynczym pomiarze to dla n nieparzystego, prawdopodobieństwo błędu:

$$e_n = \sum_{k=0}^{\lfloor n/2\rfloor} \binom{n}{k} (1-e)^k e^{n-k}$$

. Dla parzystego trzeba dodatkowo zgadywać gdy wyjdzie po równo wyników.

Zadanie 2 (25 pkt) Z prawdopodobieństwem 1/2 otrzymujesz jeden z dwóch stanów nieortogonalnych $|\psi_1\rangle$, $|\psi_2\rangle$. Zajdź optymalną strategię rozróżniania tych stanów, która polega na tym, że albo wskazujesz stan bezbłędnie albo powstrzymujesz się od zgadywania w ogóle. Optymalność oznacza w tym przypadku minimalizację prawdopodobieństwa, że powstrzymujesz się od zgadywania. Ile wynosi to minimalne prawdopodobieństwo? Gdyby zamiast powstrzymywać się od zgadywania, zagadywałbyś w sposób zupełnie przypadkowy jeden ze stanów, jaki byłby średni poziom błędu dla tej strategii. Porównaj go ze średnim poziomem błędu dla optymalnej strategii rozróżniania wyprowadzonej na wykładzie.

Odpowiedź Potrzebujemy trzech operatorów pomiarowych M_1 (zgadujemy $|\psi_1\rangle$), M_2 (zgadujemy $|\psi_1\rangle$), $M_?$ (powstrzymujemy się od zgadywania). $M_1 = \alpha|\psi_2^\perp\rangle\langle\psi_2^\perp|$, $M_2 = \alpha|\psi_1^\perp\rangle\langle\psi_2^\perp|$ $M_? = \mathbb{1} - M_1 - M_2$. Optymalne $\alpha = 1/(1 + |\langle\psi_1|\psi_2\rangle|)$.

Zadanie 3 (25 pkt) Rozważ dowolny stan czysty qubitu $|\psi\rangle = \cos\theta/2|0\rangle + \sin\theta/2e^{i\varphi}|1\rangle$. Czy istnieje operacja kwantowa $\mathcal{E}$, która przekształcałaby dowolny stan ψ na stan do niego ortogonalny tzn:

$$\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi^\perp\rangle\langle\psi^\perp|, \tag{2}$$

gdzie $|\psi^\perp\rangle = \sin\theta/2|0\rangle - \cos\theta/2e^{i\varphi}|1\rangle$. Jeśli uważasz, że istnieje podaj ją; jeśli nie udowodnij, że rzeczywiście nie istnieje. Taka operację nazywa się w żargonie kwantowej informacji *universal NOT*.

Odpowiedź Załóżmy, że takie odwzorowanie istnieje. Niech K_i będą operatorami Krausa. Wtedy $\sum_i K_i|\psi\rangle\langle\psi|K_i^\dagger = |\psi^\perp\rangle\langle\psi^\perp|$. Obłóżmy obie strony przez $\langle\psi|$ i $|\psi\rangle$. Otrzymamy: $\sum_i |\langle\psi|K_i|\psi\rangle|^2 = 0$. Ponieważ $|\psi\rangle$ może być dowolny, a suma składa się z wyrazów nieujemnych, oznacza to, że $K_i = 0$, sprzeczność. Odwzorowanie universal NOT nie istnieje.

Zadanie 4 (25 pkt) Rozważ operację kwantową, którą można traktować jako przybliżone klonowanie qubitu. Operacja działa z przestrzeni trzech qubitów w przestrzeń trzech qubitów, przy czym stan klonowany zapisany jest w qubicie 1, qubit 2 na początku jest w stanie $|0\rangle$ (pusta kartka) a po klonowaniu chcielibyśmy aby znajdowała się w nim kopia klonowanego stanu, qubit 3 jest qubitem pomocniczym, który można traktować jako maszynę klonującą na początku przygotowaną w stanie $|0\rangle$. Ponieważ interesuje nas jedynie sytuacja, gdy qubity 2 i 3 są na początku w stanie $|0\rangle$, dlatego dla pełnego opisu wystarczy podać działanie tej operacji na stany $|0\rangle\otimes|0\rangle\otimes|0\rangle$ oraz $|1\rangle\otimes|0\rangle\otimes|0\rangle$:

$$\begin{aligned} U|0\rangle\otimes|0\rangle\otimes|0\rangle &= \sqrt{\tfrac{2}{3}}|0\rangle\otimes|0\rangle\otimes|0\rangle + \sqrt{\tfrac{1}{6}}(|0\rangle\otimes|1\rangle+|1\rangle\otimes|0\rangle)\otimes|1\rangle \\ U|1\rangle\otimes|0\rangle\otimes|0\rangle &= \sqrt{\tfrac{2}{3}}|1\rangle\otimes|1\rangle\otimes|1\rangle + \sqrt{\tfrac{1}{6}}(|0\rangle\otimes|1\rangle+|1\rangle\otimes|0\rangle)\otimes|0\rangle, \end{aligned} \tag{3}$$

a) Zapisz wynik działania operacji jeśli na wejściu qubit 1 jest dowolnym stanem czystym $|\psi\rangle = \cos\theta/2|0\rangle + \sin\theta/2\exp^{i\varphi}|1\rangle$.

b) Oblicz zredukowaną macierz gęstości ρ_1 wyjściowego qubitu 1, oraz zredukowaną macierz gęstości ρ_2 wyjściowego qubitu 2. Jak wyglądają wektory Blocha odpowiadające tym stanom, w porównaniu z wektorem Blocha stanu wejściowego $|\psi\rangle$.

c) Oblicz wierność klonowania, tzn. wielkość $F_1 = \langle\psi|\rho_1|\psi\rangle$, oraz $F_2 = \langle\psi|\rho_2|\psi\rangle$, która mówi jak bliskie stanowi wejściowemu są uzyskane w wyniku działania operacji klony ρ_1 oraz ρ_2. $F = 1$ oznacza idealne klonowanie. Czy wierność zależy od stanu wejściowego $|\psi\rangle$?

d) Oblicz łączny stan ρ_{12} dwóch klonów po zadziałaniu operacji. Czy pomiędzy klonami występując korelacje czy też można klony traktować jako niezależne od siebie.

Odpowiedź

a)

$$U|\psi\rangle\otimes|00\rangle = \cos\theta/2\left(\sqrt{\frac{2}{3}}|000\rangle + \sqrt{\frac{1}{6}}(|01\rangle+|10\rangle)\otimes|1\rangle\right) + \sin\theta/2 e^{i\varphi}\left(\sqrt{\frac{2}{3}}|111\rangle + \sqrt{\frac{1}{6}}(|01\rangle+|10\rangle)\otimes|0\rangle\right)$$

b) $\rho_1 = \rho_2 = \frac{1}{6}\mathbb{1} + \frac{2}{3}|\psi\rangle\langle\psi|$

c) $F = \frac{5}{6}$

d) $\rho_{12} \neq \rho_1\otimes\rho_2$, czyli są korelacje