1. Tortury algebrą liniową

Zadanie 1

Trudność: łatwe Punktów: 3

Sprzężenie Hermitowskie macierzy $A = (a_{i,j})$ to macierz $A^\dagger = (\overline{a_{j,i}})$, gdzie $\overline{a+bi} = a - bi$ (sprzężenie liczby zespolonej).

Pokaż, że $(AB)^\dagger = B^\dagger A^\dagger$.

Zadanie 2

Trudność: łatwe Punktów: 2

Pokaż, że jeśli $\forall x \in \mathbb{C}^N \ \langle x| M |x\rangle = \langle x|x\rangle$, to M musi być macierzą identycznościową.

Zadanie 3

Trudność: średnie Punktów: 2

Pokaż, że jeśli macierz A zamienia legalne stany kwantowe na legalne stany kwantowe, to $A^{-1} = A^\dagger$ (czyli A jest *macierzą unitarną*).

Zadanie 4

Trudność: średnie Punktów: 1

Operacja CNOT zamienia stan $|a, b\rangle$ na $|a, a \oplus b\rangle$. Jak wygląda macierz operacji $\sqrt{\text{CNOT}}$, która, zastosowana dwukrotnie, jest równoważna CNOT?

2. Pomiar

Powiedzieliśmy sobie, że jeśli nasz stan kwantowy w przestrzeni zdefiniowanej przez stany bazowe $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ (stany te mogą odpowiadać ciągom bitów—gdzie każdy bit to polaryzacja pojedynczego fotonu, wtedy $N = 2^n$, gdzie n to liczba fotonów) jest równy $|\phi\rangle = \sum_{i=0}^{N} \alpha_i |i\rangle$ to stan i zmierzymy z prawdopodobieństwem $|\alpha_i|^2$. A co się stanie ze stanem, gdy zmierzymy tylko jeden qubit (foton)? Na przykład mamy dwa fotony. Pomiar pierwszego daje

$$\begin{cases} |0\rangle, & \text{z prawdopodobieństwem } |\alpha_{00}|^2 + |\alpha_{01}|^2 \\ |1\rangle, & \text{z prawdopodobieństwem } |\alpha_{10}|^2 + |\alpha_{11}|^2 \end{cases}$$

Co się dzieje wtedy z pozostałym stanem kwantowym? To jest niestety bardziej skomplikowane i całego formalizmu, który opisuje takie sytuacje nauczymy się dopiero pod koniec semestru (m.in. dlatego, że wymaga to zdefiniowania, będziemy chcieli zawsze mierzyć wszystko na końcu algorytmu), ale można myśleć, że dzieje się to samo, co z prawdopodobieństwem warunkowym, czyli jeśli z pomiaru wyjdzie $|0\rangle$, to nasz stan zmienia się w

$$|0\rangle \otimes \frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Fizycy nazywają to *redukcją* albo *zapadnięciem się* funkcji falowej.

Zadanie 5

Trudność: łatwe Punktów: 1

Stan GHZ to $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Pokaż, że nie jest on iloczynem tensorowym stanów pojedynczych fotonów (czyli jest splątany).

Zadanie 6

Trudność: łatwe Punktów: 1

Pokaż, że po zmierzeniu jednego z trzech qubitów, stan staje się niesplątany. Niezależnie od wyniku tego pomiaru.

3. Paradoks Hardy'ego

Alicja i Bob wyprodukowali następujący stan 2 qubitów:

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |11\rangle}{\sqrt{3}}.$$

Alicja dostaje pierwszy qubit, Bob bierze drugi. Następnie każde z nich mierzy swój qubit w bazie $\{|+\rangle, |-\rangle\}$.

Zadanie 7

Trudność: łatwe Punktów: 3

Dowiedź następujących stwierdzeń:

(a) $|\psi\rangle = \frac{\sqrt{2}}{\sqrt{3}}|0+\rangle + \frac{1}{\sqrt{3}}|11\rangle$.

(b) $|\psi\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{\sqrt{2}}{\sqrt{3}}|+1\rangle$.

(c) Gdyby oboje zmierzyli swoje fotony w bazie standardowej, to nigdy nie uzyskają stanu $|10\rangle$.

(d) Alicja i Bob wspólnie zmierzą stan $|--\rangle$ z prawdopodobieństwem $\frac{1}{12}$.

Zadanie 8

Trudność: średnie Punktów: 2

Pan Lucien przestawia następujące rozumowanie:

1. Z punktu (a) poprzedniego zadania można wyciągnąć wniosek, że prawdopodobieństwo, że Bob zmierzy $|+\rangle$ pod warunkiem, że foton Alicji jest spolaryzowany poziomo wynosi 1.
2. Z punktu (b) poprzedniego zadania można wyciągnąć wniosek, że prawdopodobieństwo, że Alicja zmierzy $|+\rangle$ pod warunkiem, że foton Boba jest spolaryzowany pionowo wynosi 1.
3. Z punktu (c) poprzedniego zadania można wyciągnąć wniosek, że foton Boba jest spolaryzowany pionowo lub foton Alicji jest spolaryzowany poziomo.
4. Zatem, skoro przynajmniej jeden z warunków wymienionych w punktach 1-2 zachodzi, to jest niemożliwym, by Alicja i Bob zmierzyli stan $|--\rangle$, co stoi w sprzeczności z punktem (d) poprzedniego zadania.

Czy pan Lucien ma rację?

4. Kryptografia

Zadanie 9

Trudność: łatwe Punktów: 1

W protokole **BB84**, Ewa przejęła qubit $|x\rangle$ i dokonała na nim pomiaru w jakiejś bazie, a następnie przesłała tak spolaryzowany foton Bobowi. Jakie jest prawdopodobieństwo, że Alicja i Bob zorientują się?

Zadanie 10

Trudność: łatwe Punktów: 2

Proponujemy następujący atak na protokół **BB84**: Ewa przechwytuje foton po drodze między Alicją i Bobem. Zastosowuje na nim bramkę CNOT: $(\alpha|0\rangle + \beta|1\rangle)|0\rangle \mapsto \alpha|00\rangle + \beta|11\rangle$. Jeden qubit z tego splątanego stanu wysyła do Boba, a więc dostaje on stan $\alpha|0\rangle + \beta|1\rangle$ — taki jaki wysłała do niego Alicja. Drugi foton Ewa zmierzy w odpowiedniej bazie, gdy Bob i Alicja ją ujawnią.

Czemu ten atak nie działa?

Zadanie 11 [**No-cloning theorem**]

Trudność: średnie Punktów: 3

Pokaż, że nie istnieje operacja unitarna U zmieniająca stan $|x\rangle|0\rangle$ na $|x\rangle|x\rangle$.

Wskazówka: Operacje unitarne zachowują iloczyn skalarny.

Zadanie 12

Trudność: łatwe Punktów: 1

Pokaż, że twierdzenie to jest prawdziwe nawet jeśli $|x\rangle$ może być równy tylko $|0\rangle$, $|1\rangle$, $|+\rangle$ lub $|-\rangle$.

Zadanie 13

Trudność: łatwe Punktów: 3

W praktyce do wysyłania fotonów w protokołach uzgodnienia klucza używa się laserów, które w pojedynczym strzale czasem wyemitują 0 fotonów, czasem 1, a czasem więcej. Nasz laser z prawdopodobieństwem p_2 wysyła przynajmniej 2 fotony zamiast jednego, a z prawdopodobieństwem $p_3 < p_2$ wysyła aż 3 (lub więcej). Jaką część klucza może odkryć Ewa, jeśli jest w stanie przejąć nadmiarowe kopie spolaryzowanych fotonów?

Zadanie 14

Trudność: średnie Punktów: 3

Jakie będą p_2 i p_3 jeśli liczba fotonów w strzale pochodzi z rozkładu Poissona o średniej równej 0,2?