Algorytmy Kwantowe

Lista 3

1. Entropia i teleportacja

Zadanie 1 [**1 ebit + 1 qubit $\geqslant$ 2 bity**]

Trudność: średnie Punktów: 4

Alicja i Bobek przygotowują sobie parę EPR (czyli $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$), a następnie każde z nich bierze po jednym qubicie i rozstają się. Alicja formułuje 2-bitową wiadomość $\overline{b_1 b_2}$, którą chce przekazać Bobowi. Dokonuje następujących operacji na swoim qubicie:

- Jeśli $b_1 = 1$, przepuszcza swój qubit przez bramkę NOT.
- Jeśli $b_2 = 1$, przepuszcza swój qubit przez bramkę $\mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Wysyła swój qubit Bobowi. Jakiego przekształcenia unitarnego ma on dokonać na obu qubitach, by za pomocą pomiaru wydedukować wiadomość od Alicji?

Wskazówka: Rozpisz sobie możliwe stany kwantowe. Napisz macierz przekształcającą do nich stany bazowe i ją odwróć.

Zadanie 2

Trudność: średnie Punktów: 3

Zaprojektuj obwód kwantowy realizujący tę operację.

2. Paradoks Hardy'ego

Alicja i Bob wyprodukowali następujący stan 2 qubitów:

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

Alicja dostaje pierwszy qubit, Bob bierze drugi. Następnie każde z nich rzuca monetą. Jeśli wypadnie Orzeł, to po prostu mierzą swój qubit. Jeśli wypadnie reszka, przepuszczają swój qubit przez bramkę Hadamarda i mierzą.

Zadanie 3

Trudność: łatwe Punktów: 3

Dowiedź następujących stwierdzeń:

(a) Jeśli Alicja wyrzuci O i Bob wyrzuci O, to jest *możliwe*, że zmierzą stan $|11\rangle$.

(b) Jeśli Alicja wyrzuci O, zaś Bob wyrzuci R, to jest *niemożliwe*, żeby zmierzyli stan $|10\rangle$.

(c) Jeśli Alicja wyrzuci R, zaś Bob wyrzuci O, to jest *niemożliwe*, żeby zmierzyli stan $|01\rangle$.

(d) Jeśli Alicja wyrzuci R i Bob wyrzuci R, to jest *niemożliwe*, żeby zmierzyli stan $|11\rangle$.

Zadanie 4

Trudność: średnie Punktów: 2

Pan Hardy przestawia następujące rozumowanie:

1. Z punktu (a) poprzedniego zadania można wyciągnąć wniosek, że jeśli Alicja wyrzuci orła i dokona bezpośredniego pomiaru swojego qubitu stanu $|\psi\rangle$, to *może* zmierzyć $|1\rangle$.
2. Skoro Alicja po wyrzuceniu orła może zmierzyć $|1\rangle$, to z punktu (b) można wyciągnąć wniosek, że Bob *nie może* zmierzyć $|0\rangle$ jeśli wyrzuci reszkę (czyli dokona Hadamard-plus-pomiaru).
3. Podobnie można wywnioskować, że jeśli Alicja wyrzuci reszkę i przepuści swój bit przez bramkę Hadamarda, to nie może zmierzyć $|0\rangle$.
4. Zatem jeśli oboje przepuszczą swoje qubity przez bramki Hadamarda, to *muszą* zmierzyć $|11\rangle$ — wszak żadne z nich nie może zmierzyć $|0\rangle$, co stoi w sprzeczności z punktem (d) poprzedniego zadania.

Czy pan Hardy ma rację?

Uwaga: To zadanie trzeba rozwiązać *porządnie*.

3. Kryptografia

W protokołach *kwantowego uzgodnienia klucza* mamy troje graczy — Alicję, Boba i Ewę. Alicja i Bob chcą umówić się na wspólny losowy ciąg bitów i utrzymać go w tajemnicy przed Ewą. O jednym takim protokole rozmawialiśmy z Piotrem Wieczorkiem podczas dni otwartych[1]. 20 lat po nim powstał inny, podobny algorytm — **SARG04**. Działa on następująco:

1. Alicja losuje dwa ciągi po n bitów. $(a_i)_{i=1,\ldots,n}$ to wartości, $(b_i)_{i=1,\ldots,n}$ to bazy. $b_i = 0$ wskazuje na bazę $\{|0\rangle, |1\rangle\}$; $b_i = 1$ na bazę $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$.
2. Alicja wysyła do Boba fotony, i-ty qubit to a_i w bazie wskazanej przez b_i.
3. Bob losuje swój ciąg n losowych bitów — b'. Mierzy każdy otrzymany qubit w bazie wskazanej przez b'. Nie wie oczywiście, czy $b_i = b'_i$.
4. Alicja ujawnia dla każdego qubitu x_i dwie wartości — jedna jest prawdziwa, a druga losowa pochodząca z drugiej bazy (może zatem wysłać jedną z czterech wiadomości).
5. Jeśli Bob jest w stanie wydedukować na podstawie swojego pomiaru oraz wiadomości Alicji oryginalną wartość bitu a_i, to bit ten staje się częścią uzgodnionego klucza.
6. Na koniec Alicja i Bob porównują (na publicznym kanale) wartości losowo wybranej 1/2 z uzgodnionych bitów. Jeśli wykryją niezgodność, uznają, że Ewa ich musiała podsłuchiwać i zawieszają komunikację.

Zadanie 5

Trudność: łatwe Punktów: 1

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 6

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

[1] https://youtu.be/njgUPW1WYUM?t=3964; Protokół jest bardzo prosty i warto obejrzeć wykład lub przeczytać jego opis na Wikipedii

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 (to jest różnica między **BB84** i **SARG04**).

Czemu ten atak nie działa?

Zadanie 7 [No-cloning theorem]

Trudność: średnie Punktów: 3

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

Wskazówka: Operacje unitarne zachowują iloczyn skalarny.

Zadanie 8

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 9

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 10

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?

3.1 Kopiowanie kwantowych pieniędzy

Mając w ręku autentyczny kwantowy banknot (według schematu Wiesnera) chcemy wyprodukować dwie kopie, które obie przejdą weryfikację przez bank. Qubity w banknocie są niezależne (niesplątane) więc fałszować będziemy qubit-po-qubicie. Załóżmy zatem, że nasz banknot ma jeden qubit.

Zadanie 11

Trudność: łatwe Punktów: 2

Wskaż nie korzystającą ze splątania procedurę, która wyprodukuje 2 banknoty, które bank zaakceptuje z prawdopodobieństwem 5/8.

Zadanie 12

Trudność: łatwe Punktów: 2

Bardziej skomplikowana procedura będzie wyglądała tam. Przygotowujemy stan $|\phi\rangle = |00\rangle \otimes |x\rangle$, gdzie $|x\rangle$ pochodzi z banknotu. Przepuszczamy go przez operację o następującej specyfikacji:

$$|000\rangle \mapsto \frac{\sqrt{3}}{2}|000\rangle + \frac{|110\rangle + |101\rangle + |011\rangle}{\sqrt{12}}$$

$$|001\rangle \mapsto \frac{\sqrt{3}}{2}|111\rangle + \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{12}}$$

Następnie mierzymy pierwszy qubit, a na banknotach umieszczamy pozostałe dwa.

Z jakim prawdopodobieństwem oba banknoty przejdą weryfikację przez bank?

Zadanie 13

Trudność: trudne Punktów: 5

Powiedzmy, że bank chce uniknąć ataku interaktywnego, o którym mówiliśmy na wykładzie. W związku z tym zwraca właścicielowi tylko banknoty, które przejdą weryfikację.

Zadanie polega na zaprojektowaniu ataku, który wysyła banknot do weryfikacji bardzo dużo razy, ale prawdopodobieństwo, że bank kiedykolwiek stwierdzi fałsz jest bardzo małe.

Wskazówka: Powiedzmy, że bank wybucha (jak bomba), gdy zmierzy qubit w odpowiedniej bazie i pomiar da wynik inny niż oczekiwano.