1. Z poprzedniej listy

Zadanie 1

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 2

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?

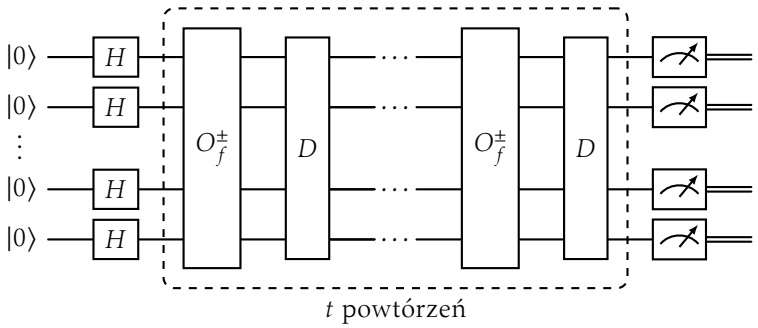
2. Algorytm Grovera

Zadanie 3

Trudność: łatwe Punktów: 2

Niech $A = \{x \mid f(x) = 1\}$ zaś $B = \{x \mid f(x) = 0\}$, gdzie f jest funkcją $\{0,1\}^n \to \{0,1\}$. Dysponujemy obwodem kwantowym $O_f^{\pm}$, jak na wykładzie. Niech $k = |A|$.

Przypomnijmy sobie algorytm Grovera z t powtórzeniami. Niech $|\psi^{(t)}\rangle$ będzie stanem po t powtórzeniach operacji $D \circ O_f^{\pm}$.



Udowodnij, że

$$|\psi^{(t)}\rangle = \alpha_t \frac{1}{\sqrt{k}} \sum_{x \in A} |x\rangle + \beta_t \frac{1}{\sqrt{2^n - k}} \sum_{x \in B} |x\rangle,$$

gdzie $\alpha_t, \beta_t \in \mathbb{R}$ oraz $\alpha_t^2 + \beta_t^2 = 1$. Ile wynosi α_0?.

Zadanie 4

Trudność: łatwe Punktów: 1

Potraktujmy (β_t, α_t) jako współrzędne punktu na okręgu. Niech θ_t będzie argumentem tego punktu (czyli $\alpha_t = \cos\theta_t$, $\beta_t = \sin\theta_t$). Pokaż, że przejście $(\beta_t, \alpha_t) \mapsto (\beta_{t+1}, \alpha_{t+1})$ jest obrotem o kąt $2\theta_0$.

Zadanie 5

Trudność: łatwe Punktów: 2

Załóżmy, że znamy k. Chcielibyśmy zatem wybrać $t = \frac{1}{2}\left(\frac{\pi}{2\theta_0} - 1\right)$. Prawdopodobnie nie będzie to jednak liczba całkowita. Pokaż, że gdy wybierzemy jako t zaokrąglenie tej liczby do najbliższej liczby całkowitej, to algorytm Grovera zwróci element zbioru A z prawdopodobieństwem przynajmniej $\frac{1}{2}$.

Zadanie 6

Trudność: łatwe Punktów: 2

Załóżmy znowu, że znamy k. Jak znaleźć jakiś element zbioru A z dużym prawdopodobieństwem odpytując wyrocznię $O_f^{\pm}$ tylko $\mathcal{O}(\sqrt{2^n/k})$ razy?

Zadanie 7

Trudność: średnie Punktów: 3

Tym razem nie znamy k. Skonstruuj algorytm, który wypluje jakiś element zbioru A odpytując $O_f^{\pm}$ tylko $\mathcal{O}(\sqrt{2^n/k})$ razy.

Uwaga: Tu raczej nie wykpimy się oszustwem typu *podwajanie*. Trzeba rozumować tak, jak w poprzednich zadaniach.

2.1 Zastosowania

Zadanie 8

Trudność: trudne Punktów: 5

Dostęp do grafu nieskierowanego G mamy przez wyrocznię O_G (obwód kwantowy), która dla wejścia $|i\rangle|j\rangle|b\rangle$ zwróci $|i\rangle|j\rangle|b \oplus \mathbb{1}[(i,j) \in E(G)]\rangle$. Opracuj algorytm, który poprawnie stwierdzi (z dużym prawdopodobieństwem), czy graf jest spójny, odwołując się do wyroczni $\mathcal{O}(n^{3/2})$ razy.

Uwaga: Nie rysuj obwodu kwantowego. Opisz algorytm używając standardowego języka algorytmicznego uruchamiając algorytm Grovera jako procedurę.

Zadanie 9

Trudność: średnie Punktów: 2

Pokaż, że algorytm klasyczny z dostępem do takiej wyroczni, jak w poprzednim zadaniu potrzebuje $\Omega(n^2)$ wywołań, by stwierdzić, czy graf jest spójny, czy nie (nawet ze stałym prawdopodobieństwem).

3. Transformata Fouriera

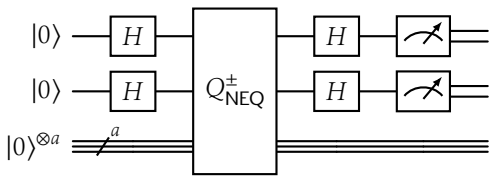
Zadanie 10 [Wykrywanie XOR-a]

Trudność: łatwe Punktów: 3

Funkcja $\mathsf{NEQ} : \{0,1\}^2 \to \{0,1\}$ zwraca jedynkę, gdy bity na jej wejściu są różne. Będziemy używać obwodu $Q^{\pm}_{\mathsf{NEQ}}$, który mapuje stan

$$|x_1\rangle|x_2\rangle|00\ldots0\rangle \mapsto (-1)^{\mathsf{NEQ}(x_1,x_2)}|x_1\rangle|x_2\rangle|00\ldots0\rangle.$$

Rozważmy obwód, jak na rysunku. Jaki jest rozkład prawdopodobieństwa poszczególnych wyników pomiarów?



Zadanie 11 [O konieczności sprzątania]

Trudność: łatwe Punktów: 2

Co by się zmieniło w poprzednim zadaniu, gdyby nasz obwód $O^{\pm}_{\mathsf{NEQ}}$ wypluwał na pomocniczych kablach śmieci zależne od x_1 i x_2?

Czasem — dla wygody — będziemy rozważać funkcję $f : \{-1,1\}^n \to \{-1,1\}$ zamiast $F : \{0,1\}^n \to \{0,1\}$. Jak przekonaliśmy się poniekąd w Zadaniu 10, różnica ta jest kosmetyczna. Umiemy tłumaczyć jedne funkcje na drugie. 0 przechodzi na 1, 1 na -1.

Zadanie 12 [Baza oznakowa]

Trudność: średnie Punktów: 1

Dla dowolnego wektora $y \in \{-1,1\}^n$, funkcja nazywająca się *Delta Kroneckera* (zwana też *indicator function*) jest zdefiniowana następująco

$$\delta_y(x) = \begin{cases} 1 & \text{gdy } x = y, \\ 0 & \text{gdy } x \neq y. \end{cases}$$

Pokaż, że każdą funkcję $f : \{-1,1\}^n \to \{-1,1\}$ można przedstawić jako kombinację liniową takich funkcji

$$f(x) = \sum_{y \in \{-1,1\}^n} \alpha_y \delta_y(x).$$

Zadanie 13

Trudność: średnie Punktów: 3

Wieloliniowym jednomianem nazywamy funkcję $\chi_S(x) = \prod_{i \in S} x_i$ dla jakiegoś zbioru $S \subseteq [n]$. Wielomian to kombinacja liniowa takich jednomianów. Pokaż, że każda funkcja boolowska $f : \{-1,1\}^n \to \{-1,1\}$ jest w rzeczywistości wielomianem!

Wskazówka: Kombinacja liniowa kombinacji liniowych jest kombinacją liniową.

Zadanie 14

Trudność: trudne Punktów: 5

Wręczono nam obwód kwantowy $Q_F^{\pm}$ o n wejściach i wyjściach (oraz osobno oznaczonych ancilla, żeby nie było wątpliwości, które wejścia są właściwymi argumentami funkcji F). Obiecano nam, że funkcja $F : \{0,1\}^n \to \{0,1\}$ gdy dostanie wektor x, patrzy tylko na współrzędne ze zbioru $S \subseteq [n]$ i zwraca XOR-a wartości x na tych współrzędnych. Nie znamy tylko zbioru S. Jak odkryć go używając obwodu $Q_F^{\pm}$ tylko raz?

Zadanie 15

Trudność: trudne Punktów: 5

Ile razy trzeba odpytać obwód Q_F, dla F jak z poprzedniego zadania, w klasycznym modelu obliczeń?