Z zeszłego tygodnia

Zadanie 1 [Forrelation]

Trudność: łatwe Punktów: 3

Dla funkcji $f, g : \{0,1\}^n \to \{-1,1\}$ zdefiniujemy miarę *forrelacji* (korelacji z Fourierem) jako

$$\Psi_{f,g} = \frac{1}{\sqrt{2^n}^3} \sum_{x,y\in[2^n]} f(x)(-1)^{x\cdot y} g(y),$$

gdzie $x \cdot y$ to normalny iloczyn skalarny.

Dostajemy funkcje f i g, o których obiecano nam, że wpadają w jeden z przypadków:

(1) $\Psi_{f,g} \geqslant \frac{3}{5}$, albo

(2) $|\Psi_{f,g}| \leqslant \frac{1}{15}$.

Zaprojektuj obwód kwantowy, który korzysta z $O_f^{\pm}$ oraz $O_g^{\pm}$ po $\mathcal{O}(1)$ razy i pozwala odróżnić te przypadki ze stałym[1] prawdopodobieństwem błędu.

Zadanie 2

Trudność: trudne Punktów: 4

Rozwiązujemy to samo zadanie, co przed chwilą, ale tym razem dysponujemy obwodem CONTROLLED$-O_{f,g}^{\pm}$, który przyjmuje $n+1$ bitów i aplikuje na n bitach funkcję f lub g w zależności od wartości bitu kontrolnego. Obwód ten możemy wykorzystać tylko jednokrotnie.

Skonstruuj algorytm, który odpowie TAK z prawdopodobieństwem $\frac{1+\Psi_{f,g}}{2}$, a NIE z pozostałym.

Zadanie 3

Trudność: łatwe Punktów: 1

Zmodyfikuj powyższy algorytm tak, by zarówno w przypadku (1) jak i (2) zwracał poprawną odpowiedź z prawdopodobieństwem 60% (nie zwiększając liczby odpytań obwodu CONTROLLED$-O_{f,g}^{\pm}$).

Luki z wykładu

W najbliższych kilku zadaniach będziemy chcieli zbudować obwód kwantowy realizujący zaprezentowaną na wykładzie Dyskretną Transformatę Fouriera. Czyli chcemy, by nasz obwód realizował operację

$$|x\rangle \overset{F_N}{\mapsto} \frac{1}{\sqrt{N}} \sum_{\gamma\in\mathbb{Z}_N} \overline{\chi_\gamma}(x)\,|\gamma\rangle\,,$$

gdzie $\overline{\chi_\gamma}(x) = \omega^{-\gamma\cdot x}$ (ω to zespolony pierwiastek z 1 o najmniejszym dodatnim argumencie).

Zadanie 4

Trudność: łatwe Punktów: 1

Jak wygląda macierz F_2? A F_4? Jak wygląda macierz F_8?

Zadanie 5

Trudność: łatwe Punktów: 1

Jak wygląda macierz odwrotna do F_N?

Zadanie 6

Trudność: łatwe Punktów: 2

W macierzy F_4 zamieńmy drugą i trzecią kolumnę. Uzyskaną tak macierz F_4' wyraź za pomocą macierzy Hadamarda oraz $B = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$. Niech F_N' będzie F_N, w którym przesunęliśmy nieparzyste kolumny na lewo, a parzyste na prawo. Wyraź F_{2N}' za pomocą F_N i B_N, gdzie

$$B_N = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{N-1} \end{bmatrix}.$$

[1] Tzn. o stałą lepszym od $\frac{1}{2}$.

Zadanie 7 [FFT]

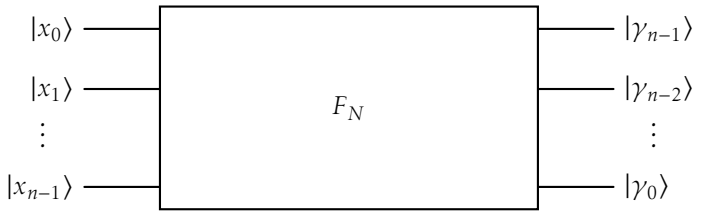
Trudność: średnie Punktów: 3

Jak wykorzystać powyższą zależność do skonstruowania klasycznego algorytmu do aplikowania macierzy F_N?

Zadanie 8

Trudność: średnie Punktów: 5

Przystępujemy teraz do budowy obwodu realizującego Transformatę Fouriera. Wygodniej będzie odwrócić wyjście obwodu tak,



by najmniej znaczący bit wejścia przechodził na najbardziej znaczący bit wyjścia.

$F_{N/2}$ jest teraz obwodem, który operuje na liczbach długości $n-1$ ($N = 2^n$). Jak wykorzystać naszą zależność rekurencyjną do zbudowania tego obwodu. Można korzystać z bramek Hadamarda, CCNOT, oraz bramek obracających stan o dowolną fazę (liczbę zespoloną o module 1).

Wskazówka: Przyda nam się operacja CONTROLLED–B, reprezentowana macierzą

$$\begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix}.$$

Musimy uzupełnić jeszcze algorytm rozwiązujęcy problem Simona nad $\mathbb{Z}_N$. Dostajemy funkcję $f : \mathbb{Z}_N \to \mathbb{Z}_M$, o której wiemy, że jest „różnowartościowa, okresowa", tzn. istnieje jakieś $s|N$, że na pierwszych s argumentach f daje różne wartości, ale dla każdego $x \in \mathbb{Z}_N$ zachodzi $f(x+s) = f(x)$.

Do obwodu O_f wkładamy stan $\left(\sum_{x\in\mathbb{Z}_N} \frac{1}{\sqrt{N}} |x\rangle\right) \otimes |0\rangle$. Uzyskujemy $|\phi\rangle = \sum_{x\in\mathbb{Z}_N} \frac{1}{\sqrt{N}} |x\rangle |f(x)\rangle$. Po zmierzeniu wyniku funkcji f uzyskujemy jakąś wartość $c \in \mathbb{Z}_M$, a stan $|\psi\rangle$ kolapsuje do $|\varphi\rangle = \sum_{x:f(x)=c} \frac{\sqrt{s}}{\sqrt{N}} |x\rangle = \sum_{i=0}^{N/s} \frac{\sqrt{s}}{\sqrt{N}} |t + s\cdot i\rangle$, dla jakiegoś t.

Zadanie 9

Trudność: łatwe Punktów: 2

Okazuje się, że

$$\widehat{\varphi}_a = \langle \varphi | \chi_a \rangle = \mathbb{E}_{x\sim\mathbb{Z}_N} \left[\overline{f(x)}\chi_a(x)\right] = \begin{cases} z_a & \text{jeśli } a \text{ jest wielokrotnością } \frac{N}{s}, \\ 0 & \text{wpp.} \end{cases}$$

Ile wynosi z_a (i jak zależy od c — wylosowanego wyniku funkcji)?

Zadanie 10

Trudność: średnie Punktów: 2

Z poprzedniego zadania wynika, że po przepuszczeniu $|\varphi\rangle$ przez kwantową transformatę Fouriera dostajemy z jednakowym prawdopodobieństwem jedną z wielokrotności $\frac{N}{s}$.

Niech $m = \frac{N}{s}$. Użyjemy obwodu dwa razy i uzyskamy dwie liczby am i bm. Jeśli $\gcd(a, b) = 1$, to łatwo wyłuskamy s.

Czy prawdopodobieństwo, że $\gcd(a, b) = 1$ dla (jednostajnie) losowych $a, b \in \mathbb{Z}_s$ jest mniejsze, czy większe niż $\frac{1}{2}$?

Wskazówka: $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.