Algorytmy Kwantowe

Lista 6

1. Kwantowa Transformata Fouriera

1.1 Konstrukcja

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 1

Trudność: łatwe Punktów: 1

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

Zadanie 2

Trudność: łatwe Punktów: 2

Jak wygląda macierz odwrotna do F_N?

Zadanie 3

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

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

Zadanie 4 [FFT]

Trudność: średnie Punktów: 3

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

Zadanie 5

Trudność: średnie Punktów: 2

Jak wykorzystać powyższy algorytm do mnożenia dużych liczb? Jaką złożoność można uzyskać?

Zadanie 6

Trudność: trudne Punktów: 5

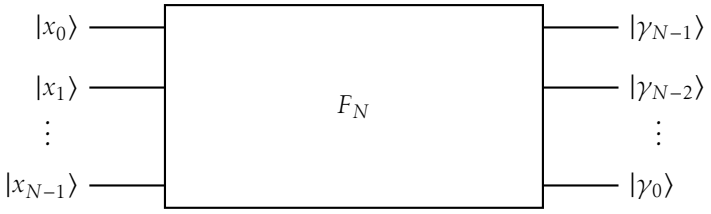
Jakiego algorytmu użyto do mnożenia dużych liczb w twoim ulubionym języku programowania? Zaimplementuj w tym języku mnożenie z użyciem FFT i porównaj wydajność tych metod.

Uwaga: Będą dodatkowe punkty za oryginalny język programowania.

Zadanie 7

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

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

1.2 Zastosowania

W najbliższych dwóch zadaniach dostajemy obwód realizujący przekształcenie unitarne $U = \mathbb{C}^{2^n \times 2^n}$. Dostajemy też wektor własny tego przekształcenia $|\psi\rangle$, czyli wiemy, że istnieje liczba zespolona λ, że $U|\psi\rangle = \lambda|\psi\rangle$. Z unitarności U wiemy, że λ ma moduł 1, czyli jest równa $e^{2\pi i\phi}$ dla jakiegoś $\phi \in [0;1)$.

Załóżmy też dla uproszczenia, że ϕ da się zapisać za pomocą m bitów po przecinku: $\phi = 0{,}\phi_1 \dots \phi_m$.

Zadanie 8

Trudność: średnie Punktów: 3

Powiedzmy, że poza obwodem U mamy obwody realizujące $U^k = \overbrace{U \cdots U}^{k \text{ razy}}$ dla dowolnej liczby k. Jak użyć ich do wyłuskania bitów liczby ϕ?

Twój obwód może być olbrzymi.

Zadanie 9

Trudność: średnie Punktów: 3

Jak zmniejszyć rozmiar obwodu używając tylko wyroczni U^{2^j} dla $j = 0, \dots, n-1$?

Okazuje się, że ten algorytm działa również (z dużym prawdopodobieństwem) dla ϕ, których nie da się zapisać na m bitach. Wtedy po prostu zaokrągla ϕ do najbliższej liczby m-bitowej. Dokładniej, prawdziwe jest:

Twierdzenie. *Dla każdego $\varepsilon > 0$ algorytm z użyciem $\mathcal{O}(1/\varepsilon)$ zapytań do U wydobędzie wartość $\bar{\phi}$ taką, że $|\phi - \bar{\phi}| < \varepsilon$ z prawdopodobieństwem 2/3 (2/3 można zmienić na dowolną inną stałą $p < 1$).*

Zadanie 10 [Zliczanie]

Trudność: średnie Punktów: 3

Dostajemy wyrocznię f^{flip} dla funkcji $f : \{0,1\}^n \to \{0,1\}$. Niech $A = \{x \mid f(x) = 1\}$. Załóżmy, że $r = |A|$ jest małe w porównaniu z N (na przykład między $c_1 N$ i $c_2 N$ dla jakichś małych stałych c_1, c_2).

Skonstruuj algorytm klasyczny, który oszacuje r, to znaczy znajdzie $\bar{r}$ takie, że $|r - \bar{r}| < \mathcal{O}(\delta\sqrt{r})$. Ile razy trzeba odpytać wyrocznię?

Zadanie 11

Trudność: trudne Punktów: 5

Skonstruuj algorytm kwantowy, który oszacuje r z taką dokładnością jak poprzednio. Ile razy trzeba odpytać wyrocznię?