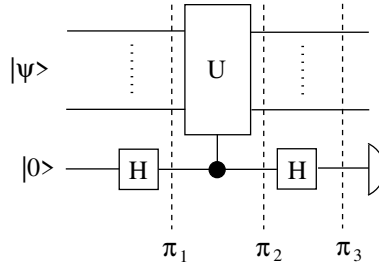


## 7 Problem estymacji fazy oraz kwantowa transformacja Fouriera

### 7.1 Sformułowanie zagadnienia i wstępna analiza

*Pytanie 7.1.* Dany obwód kwantowy reprezentujący operator unitarny  $U$  oraz dany stan  $|\psi\rangle$ , o którym wiemy że jest wektorem własnym  $U$ . Wyznaczyć odpowiednią wartość własną.

Z unitarności  $U$  wynika, że wartość własna  $\lambda$  odpowiadająca wektorowi  $|\psi\rangle$  jest liczbą zespoloną o module 1, tzn.  $\lambda = \exp(2\pi i\theta)$  gdzie  $\theta \in [0, 1)$ . Poszukujemy  $m$  pierwszych cyfr znaczących  $\theta$  zapisanego w postaci ułamka binarnego  $\theta \simeq \frac{y}{2^m}$ , gdzie  $y \in \{0, 1, 2, \dots, 2^m - 1\} \subset \mathbb{N}_0$  jest reprezentowane w postaci ciągu binarnego długości  $m$ .



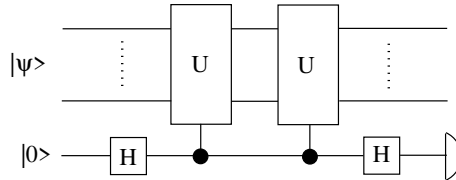
Założmy, że dysponujemy kontrolowaną wersją bramki  $U$  i na próbę przeanalizujemy kolejne etapy ewolucji stanu początkowego  $|\psi\rangle \otimes |0\rangle$  przy przechodzeniu przez kolejne części obwodu przedstawionego na rysunku powyżej

$$\begin{aligned} |\psi\rangle \otimes |0\rangle &\xrightarrow{H} |\pi_1\rangle = \frac{1}{\sqrt{2}} (|\psi\rangle \otimes |0\rangle + |\psi\rangle \otimes |1\rangle) \xrightarrow{C-U} |\pi_2\rangle = \frac{1}{\sqrt{2}} (|\psi\rangle \otimes |0\rangle + \exp(2\pi i\theta) |\psi\rangle \otimes |1\rangle) \xrightarrow{H} \\ |\pi_3\rangle &= |\psi\rangle \otimes \left( \frac{1 + \exp(2\pi i\theta)}{2} |0\rangle + \frac{1 - \exp(2\pi i\theta)}{2} |1\rangle \right). \end{aligned} \quad (7.1)$$

Prawdopodobieństwa pomiaru 0 oraz 1 wynoszą więc odpowiednio

$$P(0) = \left| \frac{1 + \exp(2\pi i\theta)}{2} \right|^2 = \cos^2(\pi\theta), \quad P(1) = \left| \frac{1 - \exp(2\pi i\theta)}{2} \right|^2 = \sin^2(\pi\theta). \quad (7.2)$$

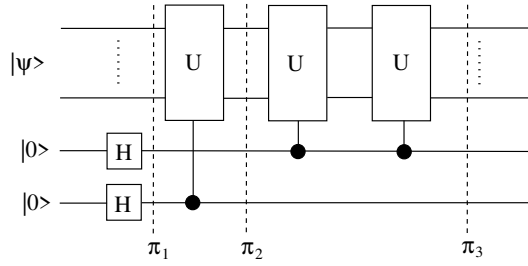
W szczególności, jeśli  $\theta = 0$  lub  $\theta = \frac{1}{2}$  (czyli  $y = 0$  lub  $y = 1$  dla  $m = 1$ ) to otrzymujemy dobrą odpowiedź. Jeśli  $\theta = \frac{1}{4}$  to  $P(0) = P(1) = \frac{1}{2}$ , więc przedstawiony powyżej obwód nie może być użyty do otrzymania odpowiedzi i musi być zmodyfikowany. Zauważmy, że wtedy  $2\theta = \frac{1}{2}$ , co wobec równości  $\lambda^2 = \exp(4\pi i\theta)$  sugeruje dwukrotne użycie bramki  $C - U$ . Ze względu na okresowość funkcji  $\exp$  ograniczy to zakres argumentu  $\theta$  do odcinka  $[0, \frac{1}{2})$



Zauważmy, że jeśli wiemy iż zachodzi dokładnie jedna z dwóch możliwości:  $\theta = 0$  lub  $\theta = \frac{1}{4}$ , to możemy te wartości zidentyfikować jeśli zmierzmy 0 lub 1, odpowiednio.

### 7.2 Dwukubitowa estymacja fazy

Połączmy oba obwody i przeprowadźmy analizę kolejnych etapów ewolucji stanu



$$\begin{aligned}
 |\psi\rangle \otimes |00\rangle &\xrightarrow{H^{\otimes 2}} |\pi_1\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_1=0}^1 \sum_{a_2=0}^1 |a_2 a_1\rangle \xrightarrow{C_2 \rightarrow U} |\pi_2\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_1=0}^1 \sum_{a_2=0}^1 \exp(2\pi i a_1 \theta) |a_2 a_1\rangle \xrightarrow{C_1 \rightarrow U^2} \\
 |\pi_3\rangle &= |\psi\rangle \otimes \frac{1}{2} \sum_{a_1=0}^1 \sum_{a_2=0}^1 \exp(2\pi i (a_1 + 2a_2)\theta) |a_2 a_1\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{x=0}^3 \exp(2\pi i x \theta) |x\rangle,
 \end{aligned} \tag{7.3}$$

gdzie  $x = 2a_2 + a_1$ . Załóżmy, że wiemy iż zachodzi jeden z następujących przypadków:  $\theta = \frac{y}{4}$ , gdzie  $y \in \{0, 1, 2, 3\}$ . Dla każdego z nich możemy zdefiniować odpowiedni stan

$$|\phi_y\rangle = \frac{1}{2} \sum_{x=0}^3 \exp(2\pi i x y) |x\rangle. \tag{7.4}$$

Zapisując te wektory w sposób jawny, mamy

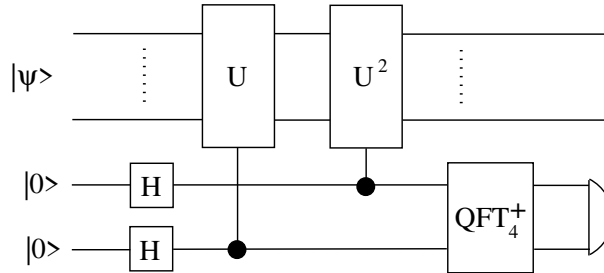
$$\begin{aligned}
 |\phi_0\rangle &= \frac{1}{2} (|0\rangle + |1\rangle + |2\rangle + |3\rangle), & |\phi_1\rangle &= \frac{1}{2} (|0\rangle + i|1\rangle - |2\rangle - i|3\rangle) \\
 |\phi_2\rangle &= \frac{1}{2} (|0\rangle - |1\rangle + |2\rangle - |3\rangle), & |\phi_3\rangle &= \frac{1}{2} (|0\rangle - i|1\rangle - |2\rangle + i|3\rangle).
 \end{aligned}$$

Zauważmy, że tworzą one bazę ortonormalną w  $\mathbb{C}^4$ , więc istnieje transformacja unitarna przeprowadzająca je w bazę obliczeniową  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ , czyli w obecnym zapisie  $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ . Macierz unitarna

$$M = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \tag{7.5}$$

które kolumnami są wektory  $|\phi_y\rangle$ ,  $y = 0, 1, 2, 3$ , działa jako  $M|y\rangle = |\phi_y\rangle$ . Jej odwrotność, czyli  $M^\dagger$ , przeprowadza bazę  $\{|\phi_y\rangle\}_{y=0}^3$  w standardową bazę obliczeniową  $M^\dagger|\phi_y\rangle = |y\rangle$ .

Macierz  $M$  jest znaną w matematyce macierzą dyskretnej transformacji Fouriera w  $\mathbb{C}^4$ . W kontekście obliczeń kwantowych oznacza się ją  $\text{QFT}_4$  (kwantowa transformacja Fouriera). Dwukubitowa estymacja fazy ma więc obwód kwantowy w postaci



Daje ono rozwiązanie dokładne dla  $\theta = \frac{y}{4}$ , gdzie  $y \in \{0, 1, 2, 3\}$ . Jeśli  $\theta$  przybiera inne wartości, to odpowiedź daje jej aproksymację, np. w przypadku  $y = \frac{3}{8}$  otrzymujemy wartości 1 lub 2 z prawdopodobieństwami bliskimi  $\frac{1}{2}$ .

### 7.3 Dyskretna transformacja Fouriera

Dyskretna transformacja Fouriera jest odwzorowaniem unitarnym  $F_N: \mathbb{C}^N \rightarrow \mathbb{C}^N$  szeroko używanym w analizie danych i transmisji sygnałów. Niech

$$\omega_N = \exp(2\pi i/N) = \cos\left(\frac{2\pi}{N}\right) + i \sin\left(\frac{2\pi}{N}\right), \quad (7.6)$$

będzie pierwotnym pierwiastkiem stopnia  $N$  z jedności, wtedy oznaczając wektory standardowej bazy ortonormalnej w  $\mathbb{C}^N$  kolejno jako  $|0\rangle, |1\rangle, \dots, |N-1\rangle$ , definiujemy  $F_N$  wzorem

$$F_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{xy} |y\rangle, \quad x = 0, 1, \dots, N-1. \quad (7.7)$$

**Przykład 7.1.** W przypadku  $N = 4$  mamy  $\omega_4 = i$  oraz kolejno

$$\begin{aligned} F_4|0\rangle &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = |\phi_0\rangle, & F_4|1\rangle &= \frac{1}{2}(|0\rangle + i|1\rangle - |2\rangle - i|3\rangle) = |\phi_1\rangle, \\ F_4|2\rangle &= \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle) = |\phi_2\rangle, & F_4|3\rangle &= \frac{1}{2}(|0\rangle - i|1\rangle - |2\rangle + i|3\rangle) = |\phi_3\rangle. \end{aligned}$$

Możemy więc zapisać macierz odwzorowania w postaci

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N & \omega_N^2 & \dots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \dots & \omega_N^{2(N-1)} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \dots & \omega_N^{(N-1)(N-1)} \end{pmatrix}. \quad (7.8)$$

Jeśli  $N = 2$  to otrzymujemy transformatę Hadamarda, a w przypadku  $N = 4$  macierz  $M$  rozważaną powyżej.

Warunek unitarności macierzy  $F_N$  sprowadza się do znanego wzoru

$$1 + \omega_N + \omega_N^2 + \dots + \omega_N^{N-1} = 0. \quad (7.9)$$

Macierz  $F_N^{-1} = F_N^\dagger$  otrzymujemy zamieniając  $\omega_N$  na jej sprzężenie zespolone, które w tym przypadku jest równe jej odwrotności  $\bar{\omega}_N = \omega_N^{-1}$ . Otrzymujemy więc wzór na transformację odwrotną postaci

$$F_N^\dagger|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} |y\rangle, \quad x = 0, 1, \dots, N-1. \quad (7.10)$$

### 7.4 Kwantowa transformacja Fouriera

W przypadku  $N = 2^m$  dyskretna transformacja Fouriera (DFT) może być efektywniej przedstawiona jako tzw. szybka transformacja Fouriera (FFT), a także zaimplementowana jako obwód kwantowy, co jeszcze bardziej przyspiesza obliczenia. Jeśli reprezentujemy

$$x = [x_m, x_{m-1}, \dots, x_2, x_1] = x_m 2^{m-1} + x_{m-1} 2^{m-2} + \dots + x_2 2 + x_1 \quad (7.11)$$

w notacji binarnej, to odpowiednia transformacja (używamy oznaczenia QFT) jest postaci

$$\begin{aligned} \text{QFT}(|x_m\rangle \otimes \dots \otimes |x_2\rangle \otimes |x_1\rangle) &= \frac{1}{\sqrt{2^m}} \bigotimes_{k=1}^m (|0\rangle + \omega_N^{2^{m-k}[x_k, \dots, x_1]} |1\rangle) = \\ &= \frac{1}{\sqrt{2^m}} (|0\rangle + \omega_N^{2^{m-1}[x_1]} |1\rangle) \otimes (|0\rangle + \omega_N^{2^{m-2}[x_2, x_1]} |1\rangle) \otimes \dots \otimes (|0\rangle + \omega_N^{[x_m, \dots, x_1]} |1\rangle), \end{aligned} \quad (7.12)$$

gdzie wykorzystujemy fakt, że  $\omega_N^N = 1$ .

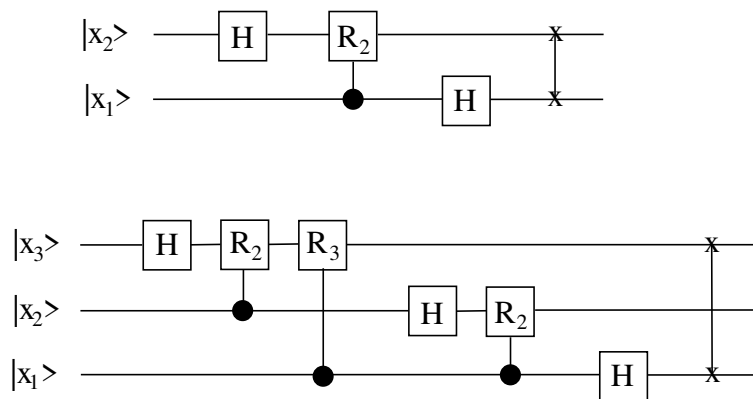
Chcąc budować obwód nie możemy wykorzystywać wcześniej zmienionych kubitów. Zauważmy, że w przedstawionym powyżej wzorze modyfikujemy zawartość pierwszego kubit, w którym przechowywaliśmy  $x_m$ , którego będziemy potrzebować później. Zamieńmy więc kolejność kubitów otrzymując w pierwszym etapie transformację, w której nie wykorzystujemy zmienionych kubitów

$$|x_m, \dots, x_2, x_1\rangle \mapsto \frac{1}{\sqrt{2^m}}(|0\rangle + \omega_N^{[x_m, \dots, x_1]}|1\rangle) \otimes \dots \otimes (|0\rangle + \omega_N^{2^{m-2}[x_2, x_1]}|1\rangle) \otimes (|0\rangle + \omega_N^{2^{m-1}[x_1]}|1\rangle),$$

co zrekompensujemy później bramkami SWAP. Ostatecznie, obwody reprezentujące QFT w przypadkach  $m = 2, 3$ , gdzie  $R_k$  oznacza bramkę

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{pmatrix}, \quad (7.13)$$

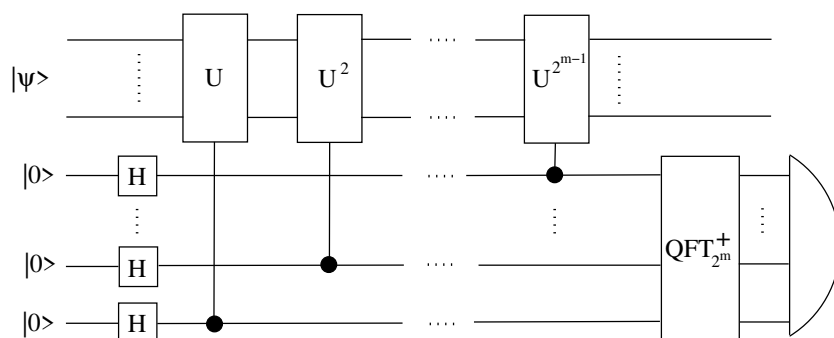
przedstawione są poniżej (w przypadku  $m = 1$  mamy transformację Hadamarda)



Transformację dla większych  $m$  otrzymujemy analogicznie dokładając bramkę  $H$  oraz bramki  $R_2, \dots, R_m$  kontrolowane kolejnymi kubitami, pamiętając o odpowiednich bramkach SWAP na koniec. Obwód transformacji odwrotnej otrzymujemy zapisując bramki w odwrotnej kolejności i zamieniając  $R_k$  na  $R_k^{-1}$ .

## 7.5 Analiza kwantowej estymacji fazy

Wróćmy do zagadnienia estymacji fazy w przypadku  $m$ -kubitowym. Przeprowadźmy analizę wykorzystywanego obwodu



$$\begin{aligned}
|\psi\rangle \otimes |0^{\otimes m}\rangle &\xrightarrow{H^{\otimes m}} |\psi\rangle \otimes \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} |b\rangle \xrightarrow{C_m \rightarrow U} |\psi\rangle \otimes \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \exp(2\pi i b_1 \theta) |b\rangle \xrightarrow{C_{m-1} \rightarrow U^2} \\
&|\psi\rangle \otimes \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \exp(2\pi i (2b_2 + b_1) \theta) |b\rangle \xrightarrow{C_{m-2} \rightarrow U^4} \dots \xrightarrow{C_1 \rightarrow U^{2^{m-1}}}
\end{aligned} \tag{7.14}$$

$$|\psi\rangle \otimes \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \exp(2\pi i (2^{m-1}b_m + \dots + 2b_2 + b_1) \theta) |b\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \exp(2\pi i b \theta) |b\rangle.$$

Zauważmy, że ciąg bramek  $C_m - U, C_{m-1} - U^2, \dots, C_1 - U^{2^{m-1}}$  można zapisać w postaci

$$U_C = \sum_{k=0}^{2^m-1} |k\rangle \langle k| \otimes U^k. \tag{7.15}$$

*Uwaga.* Jeśli  $\theta = \frac{y}{2^m}$ ,  $y \in \{0, 1, \dots, 2^m - 1\}$  jest ułamkiem binarnym długości  $m$ , to otrzymujemy stan

$$|\psi\rangle \otimes \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \omega_{2^m}^{by} |b\rangle, \tag{7.16}$$

którego prawa część (ostatnie  $m$  kubitów) jest dyskretną transformatą Fouriera wektora  $|y\rangle = |y_m, \dots, y_1\rangle$  reprezentującego liczbę  $y = 2^{m-1}y_m + \dots + 2y_2 + y_1$ . Stosując odwrotną dyskretną transformację Fouriera otrzymamy więc szukaną wartość  $y$  z prawdopodobieństwem 1.

Przeprowadźmy dokładną analizę. Jeśli zastosujemy odwrotną dyskretną transformację Fouriera do stanu

$$\frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \exp(2\pi i b \theta) |b\rangle, \tag{7.17}$$

to otrzymamy stan

$$\frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} \exp(2\pi i b \theta) \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \exp(-2\pi i k b / 2^m) |k\rangle = \sum_{k=0}^{2^m-1} C_k |k\rangle, \tag{7.18}$$

gdzie

$$C_k = \frac{1}{2^m} \sum_{b=0}^{2^m-1} \exp(-2\pi i b (k - 2^m \theta) / 2^m). \tag{7.19}$$

Oznaczmy

$$2^m \theta = a + 2^m \delta, \quad 0 \leq |2^m \delta| \leq \frac{1}{2}, \tag{7.20}$$

gdzie  $a$  jest liczbą całkowitą najbliższą  $2^m \theta$ , wtedy

$$C_k = \frac{1}{2^m} \sum_{b=0}^{2^m-1} \exp(-2\pi i b (k - a) / 2^m) \exp(2\pi i b \delta). \tag{7.21}$$

Jeśli  $\delta = 0$ , to otrzymujemy dokładną wartość  $a$  z prawdopodobieństwem równym 1, co wynika ze wzoru

$$\sum_{b=0}^{2^m-1} \exp(-2\pi i b k / 2^m) = \begin{cases} 2^m & \text{dla } k = 0, \\ 0 & \text{dla } k \neq 0. \end{cases} \tag{7.22}$$

Jeśli  $\delta \neq 0$  to prawdopodobieństwo zmierzenia  $a$  wynosi

$$P(a) = |C_a|^2 = \frac{1}{2^{2m}} \left| \sum_{b=0}^{2^m-1} \exp(2\pi i b \delta) \right|^2 = \frac{1}{2^{2m}} \left| \frac{1 - \exp(2\pi i \delta 2^m)}{1 - \exp(2\pi i \delta)} \right|^2 = \frac{1}{2^{2m}} \left| \frac{\sin(\pi \delta 2^m)}{\sin(\pi \delta)} \right|^2. \tag{7.23}$$

Biorąc pod uwagę oszacowanie słuszne dla  $x \in [0, \frac{\pi}{2}]$

$$\frac{2}{\pi}x \leq \sin x \leq x, \quad (7.24)$$

to dla rozważanych  $|\delta| \leq \frac{1}{2^{m+1}}$  mamy

$$P(a) \geq \frac{1}{2^{2m}} \left| \frac{\delta 2^{m+1}}{\pi \delta} \right|^2 = \frac{4}{\pi^2}. \quad (7.25)$$