10. Kwantowa przyszłość obliczeń

Andrzej Chmielowiec

10.1 Wstęp

Pomysł stworzenia komputera kwantowego przedstawił w 1982 roku laureat Nagrody Nobla, znany fizyk Richard Feynman. W swoich rozważaniach badał on problem symulacji zachowania R cząstek. Okazuje się, że złożoność modeli klasycznych rośnie wielomianowo względem liczby cząstek R. Natomiast złożoność modeli kwantowych rośnie już wykładniczo. Ten ogromny przeskok złożoności powoduje, że symulacje kwantowe są w zasadzie nie realizowalne dla większej liczby cząstek w klasycznym modelu obliczeń – czyli takim, który zakłada, że bity w każdej chwili czasu mają ściśle określoną wartość. Ideę zaproponowaną przez Feynmana rozwinął David Deutsch, który zdefiniował podwaliny obliczeń kwantowych i wprowadził model tak zwanej *kwantowej maszyny Turinga*.

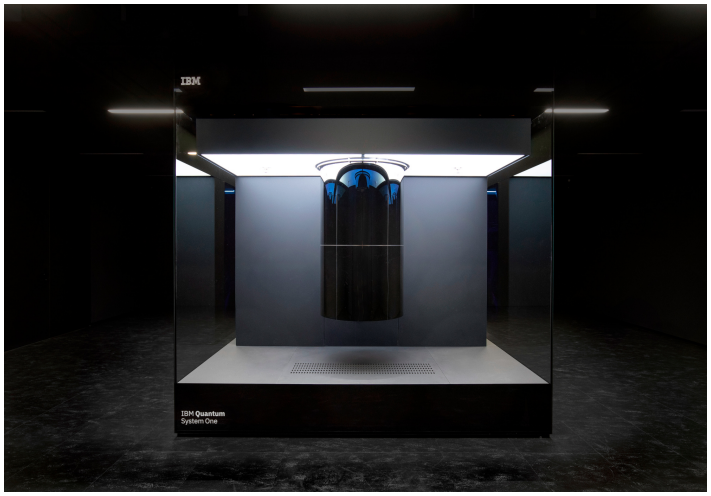
Propozycje Feynmana i Deutscha nie spotkały się ze zbyt wielkim zainteresowaniem naukowców. Zwrot w podejściu do obliczeń kwantowych nastąpił w roku 1994, kiedy Peter Shor opublikował kwantowy algorytm faktoryzacji. Odkrycie to skutecznie łamało zarówno algorytm RSA, jak i protokół Diffiego-Hellmana. Problemem był jedynie brak komputera kwantowego. W związku z tym od połowy lat 90-tych XX wieku trwają intensywne prace nad stworzeniem takiej maszyny. Te, które funkcjonują w laboratoriach potrafią przetwarzać kilkadzie-

Norway grants

Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).

Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

siąt bitów kwantowych. To jednak wciąż zbyt mało, aby skutecznie faktoryzować liczby użyte w konstrukcji szyfrów. Rok 2019 był w pewnym sensie przełomowy pod tym względem. Wtedy bowiem firma IBM wprowadziła na rynek pierwszy komputer kwantowy, który był dostępny na zasadach rynkowych. Komputer ma rozmiary niewielkiego pokoju, a jego koszt sięga 20 milionów dolarów. W celu zapewnienia stabilności stanów kwantowych komputer utrzymuje swoje podzespoły obliczeniowe w ekstremalnie niskiej temperaturze. Jest ona bardzo bliska temperatury zera absolutnego, co sprawia, że komputer musi mieć tak pokaźne rozmiary.



Rysunek 10.1: Pierwszy komputer kwantowy sprzedawany seryjnie przez firmę IBM [źródło: Wikipedia]

Aktualnie na świecie prowadzonych jest bardzo wiele pilotażowych projektów, w ramach których badana jest możliwość wykorzystania różnych efektów kwantowych do budowy komputera. Dużo wysiłków wkładana się między innymi w prace mające zweryfikować możliwość prowadzenia obliczeń w wyższych temperaturach.

10.2 Teoretyczne podstawy informatyki kwantowej

Podstawą przetwarzania informacji w komputerze kwantowym są tak zwane qbity. Ich zasadniczą cechą jest to, że poza stanami 0 i 1 potrafią również przechowywać stany pośrednie. To znaczy stany, w których qbit jest trochę zerem, a trochę jedynką. Poniżej definicja bitu kwantowego.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

Definicja 10.1 — Bit kwantowy (qbit). Bitem kwantowym nazywamy system kwantowy posiadający dwa poziomy (stopnie swobody). Z matematycznego punktu widzenia często utożsamia się go z dwuwymiarową przestrzenią Hilberta H_2, która posiada dwuelementową bazę $B = \{|0\rangle, |1\rangle\}$. Elementy bazy zapisujemy w formie wektorowej jako

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Stan bitu kwantowego reprezentowany jest przez wektor

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle,$$

dla którego amplitudy α_i spełniają warunek $\alpha_0^2 + \alpha_1^2 = 1$.

Pojawiająca się w definicji dwuwymiarowa przestrzeń Hilberta jest pojęciem dość ogólnym, niemniej jednak można przyjąć, że jest to dwuwymiarowa przestrzeń zespolona. Takie ograniczenie będzie w zupełności wystarczające na potrzeby naszych dalszych rozważań.

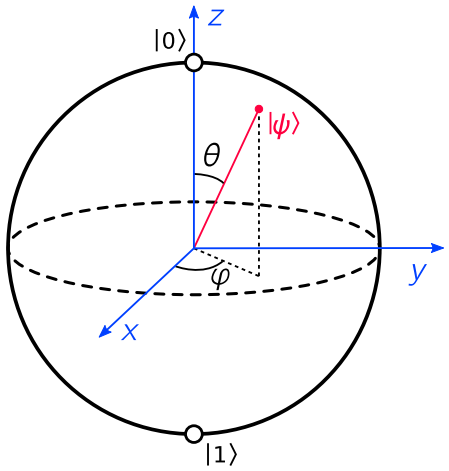
Widzimy zatem, że podstawowa jednostka informacji kwantowej – qbit, ma wartość nie do końca określoną. Mechanika kwantowa pokazuje nam jednak, że w momencie pomiaru stan kwantowy zawsze zostaje zdeterminowany do wartości $|0\rangle$ lub $|1\rangle$. Wynikiem pomiaru bitu kwantowego jest 0 z prawdopodobieństwem α_0^2 i 1 z prawdopodobieństwem α_1^2. Jeżeli zatem posiadamy 100 qbitów postaci $\alpha_0 |0\rangle + \alpha_1 |1\rangle$, to około $100 \cdot \alpha_0^2$ pomiarów da wartość 0, a $100 \cdot \alpha_1^2$ pomiarów da wartość 1.

■ **Przykład 10.1** Rozważmy zbiór 100 identycznych qbitów, których stan jest postaci $|\psi\rangle = 0.8 |0\rangle + 0.6 |1\rangle$. Jeżeli sprawdzimy wartości wszystkich qbitów z tego zbioru, to zaobserwujemy mniej więcej $100 \cdot (0.8)^4 = 64$ zera i $100 \cdot (0.6)^2 = 36$ jedynek. ■

Do reprezentowania stanu bitów kwantowych wykorzystywana jest najczęściej sfera Blocha pokazana na Rysunku 10.2. Ten sferyczny układ współrzędnych pozwala na przedstawienie dowolnego stanu kwantowego $|\psi\rangle$ w następującej postaci:

$$\begin{aligned} |\psi\rangle &= \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle \\ &= \cos\left(\frac{\theta}{2}\right) |0\rangle + (\cos\varphi + i \sin\varphi) \sin\left(\frac{\theta}{2}\right) |1\rangle. \end{aligned}$$

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.



Rysunek 10.2: Stan bitu kwantowego $|\psi\rangle$ reprezentowany za pomocą sfery Blocha

Definicja 10.2 — Bramka jednokrotna. Przekształcenie pojedynczego qbitu jest nazywane bramką jednokrotną, jeżeli jest ono zadane przez pewne przekształcenie unitarne $U : H_2 \to H_2$.

Przekształcenie liniowe $|0\rangle \mapsto \alpha\,|0\rangle + \beta\,|1\rangle$, $|1\rangle \mapsto \gamma\,|0\rangle + \delta\,|1\rangle$ nazywamy unitarnym, jeżeli współczynniki spełniają warunek:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

co zapisujemy również jako $UU^* = I$. Przy czym liczby $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ i $\bar{\delta}$ oznaczają sprzężenia liczb α, β, γ i δ. Poniżej przedstawione zostały podstawowe przykłady jednobitowych bramek kwantowych.

■ **Przykład 10.2 — Bramka NOT (Pauli X).** Negacja qbitu zdefiniowana jest za pomocą następującego przekształcenia

$$X = M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Bramka ta odpowiada obrotowi o π wokół osi X i neguje qbity przekazywane jako argumenty:

$$X\,|0\rangle = |1\rangle\,,$$
$$X\,|1\rangle = |0\rangle\,.$$

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

Możliwe są też obroty wokół osi Y i Z:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

■

■ **Przykład 10.3 — Bramka SQRT-NOT.** Okazuje się, że bramkę NOT można zrealizować za pomocą złożenia dwóch identycznych przekształceń unitarnych

$$\sqrt{X} = \sqrt{M_{\neg}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}.$$

Bramka ta przekształca qbity w następujący sposób:

$$\sqrt{X}\,|0\rangle = \frac{1+i}{2}\,|0\rangle + \frac{1-i}{2}\,|1\rangle\,,$$
$$\sqrt{X}\,|1\rangle = \frac{1-i}{2}\,|0\rangle + \frac{1+i}{2}\,|1\rangle\,.$$

■

■ **Przykład 10.4 — Bramka Hadamarda (H).** Bramka Hadamarda jest jedną z ważniejszych operacji na bitach kwantowych

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

Bramka ta neguje qbity przekazywane jako argumenty:

$$H\,|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,,$$
$$H\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\,.$$

Ważną własnością bramki H jest to, że jej dwukrotne złożenie daje identyczność:

$$H^2\,|0\rangle = |0\rangle\,, \quad H^2\,|1\rangle = |1\rangle\,.$$

■

Na samych przykładach bramek jednokrotnych widać już jak bardzo skomplikowany jest system obliczeń kwantowych. W przypadku bitów klasycznych istnieje tylko jedna nietrywialna bramka jednokrotna i jest nią bramka NOT. Dla bitów kwantowych mamy nieskończenie wiele

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

bramek jednokrotnych. Niemniej jednak w komputerze kwantowym może być zaimplementowana jedynie ich skończona liczba. Dlatego też w praktyce wykorzystuje się głównie te, które zostały przedstawione w powyższych przykładach.

Operacje na pojedynczych qbitach nie pozwalają jednak realizować skomplikowanych obliczeń. Aby było to możliwe konieczne jest wykorzystanie bramek, które posiadają przynajmniej dwa wejścia. Zanim do tego przejdziemy zobaczmy w jaki sposób od strony teoretycznej opisywane są układy dwóch bitów kwantowych. Zaczniemy od definicji dwubitowego rejestru kwantowego.

Definicja 10.3 — Dwubitowy rejestr kwantowy. System dwóch bitów kwantowych tworzy przestrzeń $H_4 = H_2 \otimes H_2$, gdzie $\otimes$ jest iloczynem tensorowym. Jeżeli $V_1 = \mathrm{Lin}(\mathbf{x_1}, \mathbf{x_2}) = \{\alpha_1 \mathbf{x_1} + \alpha_2 \mathbf{x_2}\}$ i $V_2 = \mathrm{Lin}(\mathbf{y_1}, \mathbf{y_2}) = \{\beta_1 \mathbf{y_1} + \beta_2 \mathbf{y_1}\}$, to

$$V_1 \otimes V_2 = \mathrm{Lin}(\mathbf{x_1} \otimes \mathbf{y_1}, \mathbf{x_1} \otimes \mathbf{y_2}, \mathbf{x_2} \otimes \mathbf{y_1}, \mathbf{x_2} \otimes \mathbf{y_2}),$$

gdzie $\mathbf{x_i} \otimes \mathbf{y_j}$ są wektorami bazy iloczynu tensorowego V_1 i V_2 oznaczanymi przez $\mathbf{x_i y_j}$. Ponadto dla dowolnych wektorów $\mathbf{v_1} = \alpha_1 \mathbf{x_1} + \alpha_2 \mathbf{x_2}$, $\mathbf{v_2} = \beta_1 \mathbf{y_1} + \beta_2 \mathbf{y_2}$ mamy

$$\mathbf{v_1} \otimes \mathbf{v_2} = \sum_{i,j} \alpha_i \beta_j \mathbf{x_i y_j}.$$

Być może od strony formalnej wygląda to nieco skomplikowanie, ale tak naprawdę iloczyn tensorowy możemy traktować jak iloczyn przestrzeni, w którym każdy wektor z jednej przestrzeni mnożony jest przez każdy wektor z drugiej przestrzeni. Zobaczmy, jak w praktyce wygląda iloczyn tensorowy qbitów.

Definicja 10.4 — Iloczyn tensorowy qbitów.

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Okazuje się, że nie wszystkie stany kwantowe mogą być iloczynem tensorowym dwóch innych stanów kwantowych. Dochodzimy tym sposobem do definicji splątania.

Definicja 10.5 — Stany rozkładalne i splątane. Jeżeli stan kwantowy $z \in H_4$ złożony z dwóch bitów kwantowych możemy zapisać jako iloczyn tensorowy stanów pojedynczych qbitów, to taki stan z nazywamy *rozkładalnym*. Jeżeli operacja taka jest niemożliwa, to taki stan nazywamy *splątanym*.

Poniżej przykłady stanu rozkładalnego i stanu splątanego.

■ **Przykład 10.5 — Stanu rozkładalny.** Aby wykazać, że stan jest rozkładalny wystarczy pokazać iloczyn tensorowy, który go generuje

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] \otimes \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right].$$

■

■ **Przykład 10.6 — Stan splątany.** W przypadku stanów splątanych rozumowanie jest trochę bardziej skomplikowane. Należy bowiem wykazać, że nie istnieje iloczyn tensorowy, który dany stan generuje. W tym celu przyjmujemy założenie przeciwne i próbujemy zapisać stan

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

kwantowy jako iloczyn tensorowy

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \\ (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) = \\ \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle .$$

Z powyższej zależności wynika następujący układ czterech równań: $\alpha_0\beta_0 = \frac{1}{\sqrt{2}}$, $\alpha_1\beta_1 = \frac{1}{\sqrt{2}}$, $\alpha_0\beta_1 = 0$ i $\alpha_1\beta_0 = 0$. Jest to ewidentnie układ równań sprzecznych, gdyż iloczyn pierwszych dwóch równań daje zależność $\alpha_0\alpha_1\beta_0\beta_1 = \frac{1}{2}$, a iloczyn trzeciego i czwartego daje $\alpha_0\alpha_1\beta_0\beta_1 = 0$. ■

Splątane qbity są bardzo ciekawym zjawiskiem fizycznym. Okazuje się bowiem, że jeśli dwa qbity są w stanie splątanym $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, to obserwacja jednego z nich może dać wartość 0, bądź 1 z prawdopodobieństwem $\frac{1}{2}$. Nie jest jednak możliwe obserwowanie różnych wartości na tych qbitach (albo pomiar obu daje wartość 00, albo 11). Doświadczenia pokazały, że jest to prawdą także w przypadku qbitów odległych od siebie nawet o więcej niż 10 km. Hipoteza jest taka, że ta prawidłowość jest niezależna od odległości pomiędzy bitami kwantowymi.

Po tym, jak zdefiniowaliśmy dwubitowy rejestr kwantowy i omówiliśmy podstawowe pojęcia z nim związane możemy przejść do opisu bramek dwukrotnych.

Definicja 10.6 — Bramka dwukrotna. Jednoczesne przekształcenie dwóch qbitów jest nazywane bramką dwukrotną, jeżeli jest ono zadane przez pewne przekształcenie unitarne $U : H_4 \to H_4$, gdzie $H_4 = H_2 \otimes H_2$. Do zdefiniowania operacji na bramce dwukrotnej wykorzystujemy następującą reprezentację qbitów:

$$|00\rangle = (1,0,0,0)^T,$$
$$|01\rangle = (0,1,0,0)^T,$$
$$|10\rangle = (0,0,1,0)^T,$$
$$|11\rangle = (0,0,0,1)^T.$$

Poniżej przedstawiamy dwa przykłady bramek dwukrotnych.

■ **Przykład 10.7 — Bramka CNOT (cX).** Warunkowa negacja qbitu zde-

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

finiowana jest za pomocą następującego przekształcenia

$$cX = M_{\text{cnot}} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Bramka ta neguje drugi qbit w zależności od wartości pierwszego:

$$\begin{aligned} cX\,|00\rangle &= |00\rangle\,, \\ cX\,|01\rangle &= |01\rangle\,, \\ cX\,|10\rangle &= |11\rangle\,, \\ cX\,|11\rangle &= |10\rangle\,. \end{aligned}$$

Analogicznie można zdefiniować bramki cY i cZ:

$$\begin{aligned} cY &= \begin{pmatrix} I & 0 \\ 0 & Y \end{pmatrix}, \\ cZ &= \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix}. \end{aligned}$$

■

■ **Przykład 10.8 — Dwukrotna bramka Hadamarda (H).** Iloczyn tensorowy dwóch jednokrotnych bramek Hadamarda daje nam bramkę dwukrotną

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Jej działanie na dwu qbitowym argumencie wygląda następująco

$$\begin{aligned} H\,|q_0 q_1\rangle = \frac{1}{2}(&|00\rangle + (-1)^{q_1}\,|01\rangle + \\ &(-1)^{q_0}\,|10\rangle + (-1)^{q_0+q_1}\,|11\rangle). \end{aligned}$$

■

Jeżeli bramka dwukrotna jest iloczynem tensorowym dwóch bramek jednokrotnych, to wynik jej działania tworzy rozkładalny stan bitów (bramka Hadamarda). Jeżeli natomiast bramka dwukrotna nie może być reprezentowana jako iloczyn tensorowy bramek jednokrotnych, to jej działanie tworzy splątany stan bitów (bramka cX).

Bardzo ważną własnością bitów kwantowych jest brak możliwości ich kopiowania. Ta cecha stanowi podstawę kwantowego algorytmu uzgadniania kluczy kryptograficznych.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

Twierdzenie 10.1 — Brak możliwości klonowania qbitów. Nie istnieje przekształcenie unitarne U takie, że dla dowolnego qbitu mamy:

$$U(|qa_1\rangle) = |qq\rangle\,.$$

Innymi słowy – nie ma możliwości skopiowania qbitu.

Niezależnie od braku możliwości kopiowania dowolnych stanów kwantowych należy podkreślić, że bez problemu możemy tworzyć kopie elementów bazy. Możemy zatem kopiować qbity $|0\rangle$ i $|1\rangle$.

10.3 Protokół kwantowej teleportacji

Obliczenia kwantowe kryją w sobie wiele nieoczywistych i nieintuicyjnych własności. Jedną z nich jest splątanie, które pozwala zrealizować protokół tak zwanej kwantowej teleportacji.

Załóżmy, że Alicja chce przesłać Bobowi qbit w stanie

$$a\,|0\rangle + b\,|1\rangle.$$

Dodatkowo będziemy zakładali, że obie strony dysponują po jednym qbicie ze stanu splątanego

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

przy czym Alicja posiada qbit lewy, a Bob posiada qbit prawy. W użyciu są zatem 3 qbity, których stan dany jest wzorem:

$$s_0 = \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle).$$

Alicja stosuje bramkę cX na swoich bitach doprowadzając układ do stanu s_1

$$s_1 = \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle).$$

Następnie Alicja stosuje bramkę H na pierwszym bicie (najbardziej

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.

lewym) doprowadzając układ qbitów do stanu s_2

$$\begin{aligned} s_2 = &\frac{a}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|00\rangle + \frac{a}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|11\rangle + \\ &\frac{b}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|10\rangle + \frac{b}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|01\rangle \\ = &\frac{1}{2}|00\rangle(a\,|0\rangle + b\,|1\rangle) + \frac{1}{2}|01\rangle(a\,|1\rangle + b\,|0\rangle) + \\ &\frac{1}{2}|10\rangle(a\,|0\rangle - b\,|1\rangle) + \frac{1}{2}|11\rangle(a\,|1\rangle - b\,|0\rangle). \end{aligned}$$

Alicja sprawdza wartość bitów i wysyła wynik do Boba. Bob odbiera bity przesłane przez Alicję i stwierdza w jakim stanie jest jego qbit. Następnie dobiera taką sekwencję bramek, która pozwala na odtworzenie stanu kwantowego $a\,|0\rangle + b\,|1\rangle$.

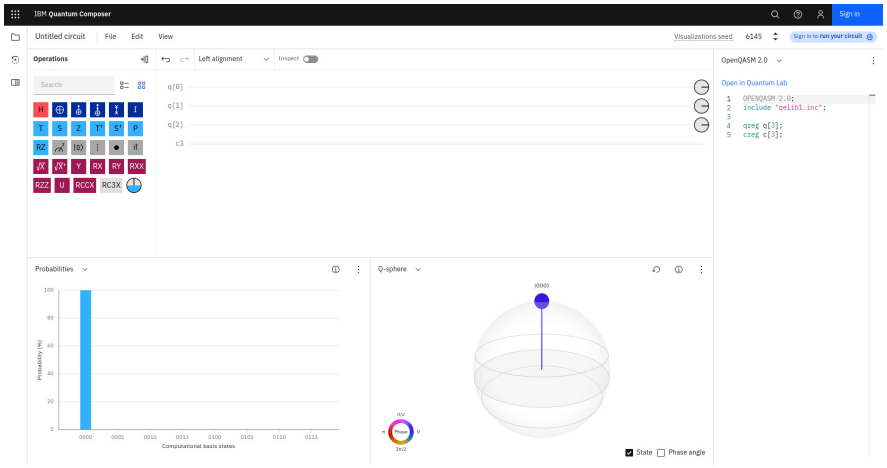
$$\begin{aligned} &00 \to s = a\,|0\rangle + b\,|1\rangle \to Is = a\,|0\rangle + b\,|1\rangle\,, \\ &01 \to s = a\,|1\rangle + b\,|0\rangle \to Xs = a\,|0\rangle + b\,|1\rangle\,, \\ &10 \to s = a\,|0\rangle - b\,|1\rangle \to Zs = a\,|0\rangle + b\,|1\rangle\,, \\ &11 \to s = a\,|1\rangle - b\,|0\rangle \to ZXs = a\,|0\rangle + b\,|1\rangle\,. \end{aligned}$$

10.4 Programowanie komputerów kwantowych

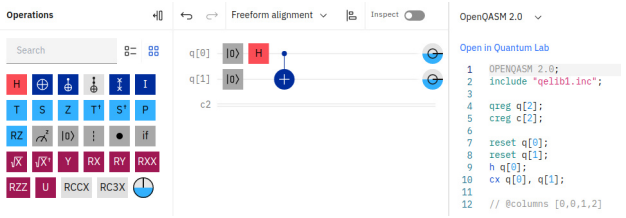
Mogłoby się wydawać, że skoro komputery kwantowe są tak drogimi urządzeniami, to tylko szczęśliwcy mogą mieć do nich dostęp. Od strony fizycznej faktycznie tak jest, ale zdalnie może to zrobić każdy. Firma IBM udostępnia bowiem część swoich komputerów kwantowych do obliczeń dla całej społeczności międzynarodowej. Za pomocą specjalnej aplikacji webowej można napisać program i mieć możliwość przeprowadzenia symulacji jego działania lub rzeczywistej realizacji na komputerze kwantowym. W tym drugim przypadku zadanie ustawiane jest w kolejce oczekujących, którzy chcą skorzystać z zasobów kwantowych firmy. Na Rysunku 10.3 przedstawiono zrzut ekranu z aplikacji webowej służącej do przygotowywania programów przeznaczonych dla komputerów kwantowych. Interfejs dostępny jest na stronach internetowych `https://quantum-computing.ibm.com/`. Zachęcamy czytelników do skorzystania z niego i napisania nawet najprostszego programu na komputer kwantowy.

Na Rysunku 10.4 przedstawiono fragment ekranu aplikacji, który ilustruje przykładowy program dla komputera kwantowego. Program wykorzystuje dwa qbity, a jego działanie polega na ich inicjacji stanem $|0\rangle$, wykorzystaniu bramki Hadamarda (H) i splątaniu za pomocą

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.



Rysunek 10.3: Ekran aplikacji webowej służącej do implementacji programów dla komputerów kwantowych

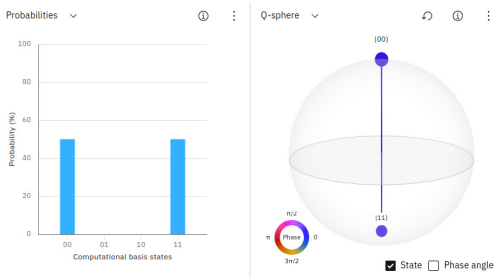


Rysunek 10.4: Fragment ekranu aplikacji webowej ilustrujący przykładowy program na komputer kwantowy

bramki CNOT (cX). Po lewej stronie panelu edycyjnego znajdują się instrukcje, które mogą zostać zrealizowane przez komputer kwantowy. Przenoszone są one do centralnej części edytora na zasadzie *przeciągnij i upuść*. Z kolei prawa część panelu przedstawia kod źródłowy programu w języku asembler dla komputerów kwantowych.

Na Rysunku 10.5 przedstawiono z kolei wynik działania stworzonego programu. Histogram umieszczony po lewej stronie ilustruje z jakim prawdopodobieństwem program da w wyniku swojego działania poszczególne ciągi bitów. Natomiast umieszczona po prawej stronie sfera Blocha pokazuje wyjściowy stan kwantowy z programu (przed wykonaniem pomiarów poszczególnych qbitów).

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.



Rysunek 10.5: Prawdopodobieństwa otrzymania konkretnych wyników obliczeń wraz z ilustracją wyjściowego stanu kwantowego na sferze Blocha

10.5 Podsumowanie

Systematycznie postępujące prace rozwojowe w dziedzinie konstrukcji komputerów kwantowych sprawiają, że prawdopodobnie już niebawem wejdą one do powszechnego użycia. Ich głównym zastosowaniem będą prawdopodobnie zagadnienia optymalizacyjne. Dlatego też warto interesować się tematyką komputerów i obliczeń kwantowych. Programowanie takich maszyn może stać się w przyszłości bardzo intratnym zajęciem. Pojęcia przedstawione w niniejszym rozdziale stanowią jedynie pobieżny wstęp do obliczeń kwantowych. Niemniej jednak pokazują, że tematyka ta jest niezwykle bogata i skomplikowana. Czytelników zainteresowanych przedstawionymi tutaj tematami zachęcamy do zgłębiania tajników obliczeń kwantowych. Bardzo przydatne pod tym względem są różnego rodzaju podręczniki i materiały udostępniane w internecie.

Norway grants
Projekt pt.: „MODELOWE ROZWIĄZANIA NA TRUDNE WYZWANIA – Plan Rozwoju Lokalnego i Instytucjonalnego Stalowej Woli" współfinansowany jest ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz Budżetu Państwa (15%).
Wspólnie działamy na rzecz Europy zielonej, konkurencyjnej i sprzyjającej integracji społecznej.