



# Wstęp do informatyki i kryptografii kwantowej

dr inż. Witold Jacak

mgr inż. Wojciech Donderowicz

mgr inż. Janusz Jacak

pod redakcją

prof. dra hab. inż. Lucjana Jacaka

E-skrypt opracowany w ramach projektu pt. „Wzrost liczby absolwentów w Politechnice Wrocławskiej na kierunkach o kluczowym znaczeniu dla gospodarki opartej na wiedzy” nr UDA-POKL.04.01.02-00-065/09-01



**KAPITAŁ LUDZKI**  
NARODOWA STRATEGIA SPÓJNOŚCI



Politechnika Wroclawska

UNIA EUROPEJSKA  
EUROPEJSKI  
FUNDUSZ SPOLECZNY



Recenzent: dr hab. inż. Andrzej Radosz, prof. PWr

Redaktor serii: dr hab. inż. Włodzimierz Salejda, prof. PWr

© Copyright by Politechnika Wroclawska  
OFICyna WYDAWNICZA POLITECHNIKI WROCLAWSKIEJ  
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław

ISBN 978-83-7493-604-0



## Spis treści

1.	Wprowadzenie .....	4
1.1.	Informacja klasyczna .....	4
1.2.	Informacja kwantowa .....	5
1.3.	Pomiar i dekoherencja .....	6
1.4.	Komputer kwantowy – perspektywy i ograniczenia.....	11
2.	Zasady kwantowego opisu.....	16
3.	Pomiar w mechanice kwantowej .....	18
3.1.	Pomiar w sensie von Neumanna – superwybór Żurka.....	20
4.	Macierz gęstości .....	23
5.	Reprezentacja Schmidta i liczba Schmidta, stany splątane .....	27
6.	Geometryczne własności macierzy gęstości .....	29
7.	Zbiór wypukły macierzy gęstości qubitu (sfera Blocha).....	31
8.	Protokoły kwantowe .....	35
8.1.	Super gęste kodowanie .....	35
8.2.	Teleportacja kwantowa.....	36
9.	Ewolucja w czasie macierzy gęstości .....	39
10.	Sterowanie qubitem – oscylacje Rabiego .....	42
11.	Twierdzenia No-cloning, No-broadcasting oraz No-deleting .....	46
11.1.	Twierdzenie No-cloning.....	46
11.2.	Twierdzenie No-broadcasting – konsekwencje.....	49
11.3.	Twierdzenie No-deleting – konsekwencje .....	49
12.	Bramki jedno-qubitowe .....	54
12.1.	Macierze Pauliego .....	54
12.2.	Bramka Pauliego $X$ .....	55
12.3.	Bramka Pauliego $Y$ .....	56
12.4.	Bramka Pauliego $Z$ .....	56
12.5.	Bramka Hadamarda.....	57
12.6.	Bramka fazy .....	58
12.7.	Bramka $\frac{\pi}{8}$ .....	59
12.8.	Bramka $e^{i\phi}$ (przesunięcie fazy o $\phi$ ).....	60
12.9.	Rotacje na sferze Blocha .....	61
12.10.	Twierdzenie o przedstawieniu dowolnej operacji jedno-qubitowej za pomocą operatorów obrotu .....	67
13.	Bramki wielo-qubitowe .....	71
13.1.	Bramka kontrolowanej negacji (CNOT) .....	71
13.2.	Układ kopiujący .....	75
13.3.	Bramka kontrolowanej operacji $U$ .....	76
13.4.	Działanie bramki $CNOT$ na macierz gęstości układu dwóch qubitów .....	79
13.5.	Bramka $SWAP$ .....	85
13.6.	Bramka $CNOT$ w reprezentacji dowolnej kontrolowanej bramki $U$ .....	86
13.7.	Bramka Toffoli.....	88
13.8.	Bramka Fredkina.....	90
13.9.	Dowolna kontrolowana operacja $U$ .....	91
13.10.	Operacje wielo-qubitowe – bramki uniwersalne .....	94
14.	Układ bramek kwantowych realizujący splątane stany (stany Bella) .....	100
15.	Układ bramek kwantowych realizujący teleportację kwantowych stanów .....	101
16.	Równoległość kwantowa .....	102
17.	Kwantowa transformata Fouriera.....	105
18.	Algorytm Grovera – poszukiwanie igły w stogu siana ( <i>finding needle in a haystack</i> ) .....	113
19.	Algorytm Shora – łamanie szyfru RSA .....	117
20.	Literatura.....	124



## 1. Wprowadzenie

### 1.1. Informacja klasyczna

Informacja klasyczna wyrażająca się poprzez makroskopowe wyniki konkretnych fizykalnych pomiarów, zrozumiała jest dla świadomości człowieka (wyraża się poprzez liczby rzeczywiste). Pomiary te są ściśle klasyczne, tzn. realizowane przez przyrządy makroskopowe dobrze opisywane przez klasyczną mechanikę, czy elektrodynamikę. Przetwarzanie każdej informacji, w tym informacji klasycznej, ma fizyczny charakter, gdyż potrzebne są tu fizyczne nośniki informacji i dla informatyki klasycznej wybiera się takie nośniki, które w najlepszy możliwy sposób imitują klasyczne zachowanie materii (mimo że w istocie cała materia jest kwantowa). Z dobrym przybliżeniem, pozwalającym na ewentualną korektę błędów w sensie klasycznym<sup>1</sup>, wiele układów elektrycznych, czy mechanicznych jest zatem użytecznych i używanych w klasycznej informatyce jako nośniki informacji (łącznie ze współczesnymi komputerami). Im większa jest jednak skala miniaturyzacji, tym bardziej klasyczne elementy układów informatycznych zbliżają się do granicy kwantowej, gdzie wymykają się klasycznemu opisowi. Dopóki rozmiary elementów (pamięci i procesorów) pozostają w skali  $\mu\text{m}$  (obecne techniki foto-litografii obejmują obszar dolnej granicy rozdzielczości dla światła widzialnego  $\sim 0.35 \mu\text{m}$ , a nawet bliskiego nadfioletu  $\sim 0.2 \mu\text{m}$ ), to opis klasyczny jest zadowalającym przybliżeniem, jednak już w obszarze nm w strukturach półprzewodnikowych, kwantowe efekty stają się dominujące (w półprzewodnikach efektywna masa elektronów może być dużo mniejsza niż swobodnego elektronu i w związku z tym kwantowe efekty są wyraźniejsze).

Przetwarzanie informacji, nawet klasycznej, pociąga za sobą jednak i głębsze odniesienia fizykalne. Wymazywanie informacji jest procesem *dysypatywnym* w sensie fizycznym<sup>2</sup>. Przeprowadzenie takiej operacji wymaga zmniejszenia objętości fazowej i przez to redukcji entropii – jest to zatem proces nieodwracalny (i niesamorzutny, konieczne jest wykonanie pracy, aby taki proces przeprowadzić). Dobrym przykładem jest tu porównanie rejestru bitów do układu pudełek, w których cząstka (każda w swoim) może zajmować jedną z dwóch możliwych części pudełka. *Resetowanie*, czyli wymazywanie informacji z rejestru, jest równoważne przesunięciu wszystkich cząstek w pudełkach na jedną stronę – żeby to wykonać trzeba przesunąć ścianki we wszystkich pudełkach do połowy, a to wymaga pracy przeciw ciśnieniu znajdującej się tam cząstki (mogła się znajdować w dowolnej części). Ta praca oznacza napływ energii do układu informatycznego, co odpowiada jego nagrzewaniu się. Zmiana entropii w przypadku wymazywania pojedynczego bitu wynosi  $k \ln 2$  (jest to obniżenie entropii odpowiadające dwukrotnemu zmniejszeniu objętości fazowej) i przy stałej temperaturze prowadzi to do *dysypacji* energii do otoczenia w ilości  $kT \ln 2$  na bit (równocześnie równej pracy wykonanej przy resetowaniu bitu, by utrzymać tę samą

<sup>1</sup> klasyczna korekta błędów polega na zwielokrotnieniu układu i zapisaniu we wszystkich kopiach tej samej informacji i częstym weryfikowaniu (przez porównanie) stanu całego zapisu – błędy pojawiają się mniejszościowo i w związku z tym mogą być zidentyfikowane i poprawiane za każdą kolejną weryfikacją (przy dostatecznym stopniu *redundancji*, czyli zwielokrotnienia i krótkim odstępem między weryfikacjami)

<sup>2</sup> na taki aspekt informacji zwrócono uwagę dostrzegając informacyjny charakter entropii wprowadzonej przez drugą zasadę termodynamiki i jej związek z procesami odwracalnymi i nieodwracalnymi



temperaturę – zgodnie z pierwszą zasadą termodynamiki). Te ograniczenia energetyczne nie są widoczne jeszcze przy obecnie stosowanych układach, gdyż na skutek niedoskonałości i makroskopowości *dyssypacje* energii przy klasycznych operacjach są zwykle o wiele rzędów większe, niż te związane z samym procesem wymazywania informacji.

By uniknąć jednak strat dyssypacyjnych w sensie redukcji objętości przestrzeni fazowej przy np. wymazywaniu informacji klasycznej, można by realizować operacje w sposób odwracalny czyli *niedyssypacyjny*. Przykład: typową operację NAND, która dwa bity (a,b) przerzuca na jeden  $\neg(a \wedge b)$  (nieodwracalna operacja) można by zastąpić *bramką Toffoli*, czyli odwracalną wersją NAND: (a,b,c) przerzuca na  $(a, b, c \oplus (a \wedge b))$  (w tym przypadku dla c=1 trzeci bit ma tę samą wartość logiczną jak w operacji NAND, ale 3 bity przechodzą na 3 bity, co pozwala na odwracalność).

$$\neg(a \wedge b) \Leftrightarrow \begin{bmatrix} 11 \\ 10 \\ 01 \\ 00 \end{bmatrix} \Rightarrow \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \text{ ale także } (a, b, (c = 1) \oplus (a \wedge b)) \Leftrightarrow \begin{bmatrix} 111 \\ 101 \\ 011 \\ 001 \end{bmatrix} \Rightarrow \begin{bmatrix} 110 \\ 101 \\ 011 \\ 001 \end{bmatrix}$$

*Równoważność logiczna nieodwracalnej bramki NAND i bramki Toffoli*

Realizacja odwracalnych operacji klasycznej informatyki prowadzi jednak, jak widać na powyższym przykładzie, do zwielokrotnienia układów i bramek logicznych, które zawierałyby wciąż rosnącą dodatkową informację. Nie jest jasne, czy realistyczny jest pomysł Ch. Benneta, by mimo tej złożoności wykonać procedury do końca, wynik zapisać i procedury (odwracalne) odwrócić. Czy będzie to w istocie zupełnie nie potrzebujący energii proces obróbki informacji, czy jednak nie, wobec konieczności dysponowania ogromnymi nadmiarowymi obszarami informatycznymi. Jest to nie do końca rozpoznany jeszcze problem/paradoks. Istotną uwagą może być tu fakt, że układy fizyczne są jednak w swej mikroskopowej warstwie nieklasyczne, ale kwantowe, i rozdrabnianie i zwielokrotnianie układów prowadzi w nieunikniony sposób do miniaturyzacji, gdzie z przyczyn podstawowych nie można dalej stosować klasycznych pojęć informatycznych.

## 1.2. Informacja kwantowa

Informacja kwantowa to stan obiektu w sensie kwantowym, np. stan cząstki opisany przez jej kwantową funkcję falową. Jest ona nieobserwowalna dla klasycznych obiektów (w szczególności, dla człowieka – obserwatora), chociaż w kwantowy sposób przetwarzana jest i przekazywana pomiędzy innymi układami kwantowymi. W ten sposób informacja kwantowa jest przez samą przyrodę przetwarzana, ale w sposób nieczytelny dla deterministycznego, klasycznego obserwatora. Można dokonywać pomiarów nad układem kwantowym i w ten sposób dowiadywać się w klasycznych (makroskopowych) terminach o jej zawartości; jednak jest to możliwe tylko w małym stopniu w stosunku do całej kwantowej informatycznej zawartości funkcji falowej. Na przeszkodzie stoją tu bowiem stoją zasady nieoznaczoności – pomiary jednej wielkości zwykle tak zaburzają stan kwantowy, że pomiary innej wielkości są już niemożliwe (i to nie z przyczyn związanych z precyzją przyrządu pomiarowego, ale



wobec kwantowych praw natury). Dla wielocząstkowego układu funkcja falowa jest bardzo pojemnym tworem z wielowymiarowej przestrzeni Hilberta (o wymiarze narastającym eksponencjalnie z liczbą cząstek). Możliwa do odczytania przez klasycznego obserwatora klasyczna informacja (w wyniki pomiarów kwantowego nośnika informacji) rośnie tylko liniowo z liczbą cząstek (tak jak dla klasycznej informatyki). Przewaga informatyki kwantowej polegać może zatem raczej na naturalnie silnie równoległym (zupełnie niedostępnym klasycznie) przetwarzaniu ogromnej kwantowej informacji, z której później można odczytać tylko niewielką klasyczną część (liniową z liczbą cząstek), ale różną w zależności od sposobu odczytu, przy wykorzystaniu zmiany reprezentacji kwantowej (np. wykorzystując transformatę Fouriera). Ten ostatni aspekt przypomina w pewnym sensie optyczne metody przetwarzania informacji (nic to dziwnego, gdyż fale świetlne są w pewnym stopniu analogiczne do funkcji falowych, a już na pewno w odniesieniu do transformacji Fouriera dobrze znanej w optyce). Dla światła, odtworzenie zapisanej fourierowsko informacji, nawet w małym kawałku tzw. *hologramu*, pozwala na podobny efekt jak wykorzystanie całego *hologramu* – to wskazuje na podobnie duże, jak w przypadku kwantowym, możliwości wynikające z interferencji (a także zmiany reprezentacji poprzez transformację Fouriera). Różnica jednak w stosunku do kwantowej informacji polega na niebywale wielkiej pojemności przestrzeni Hilberta w przypadku tej ostatniej, czego nie ma w przypadku optycznych nośników informacji. Należy się zatem zgodzić, że w przypadku wykorzystania kwantowego sposobu przetwarzania informacji, mamy do czynienia z zupełnie nową jakością, w stosunku do klasycznych i także optycznych rozwiązań. Tak jak i w innych przypadkach, kwantowy element informatyczny, czy nawet komputer kwantowy, byłby maszyną analogową, tyle że działającą w obszarze mikroświata rządzonego innymi niż klasyczne prawami fizyki.

### 1.3. Pomiar i dekoherencja

Kwantowa ewolucja zamkniętego układu opisanego hamiltonianem jest równie deterministyczna, jak ewolucja klasyczna opisywana przez równanie Newtona. Chociaż kwantowy układ nie ma trajektorii w przestrzeni fazowej, posiada ją w przestrzeni Hilberta. Nieodwracalną utratę informacji powoduje jednak pomiar. Zaburza deterministyczną ewolucję kwantowego układu i niszczy efekty interferencyjne. Według von Neumanna, pomiar prowadzi do utraty informacji zawartej w funkcji falowej poprzez jej rzutowanie na kierunek jednej z funkcji własnych operatora wielkości mierzonej  $A$ . Jeśli stan układu przed pomiarem jest  $|\psi\rangle = \sum a_i |\phi_i\rangle$ , to w wyniku pomiaru, z prawdopodobieństwem  $|a_i|^2$  otrzymujemy rezultat  $\lambda_i$  ( $i$ -ta wartość własna), a funkcja falowa  $|\psi\rangle$  zmienia się w  $|\phi_i\rangle$ . Gdyby natychmiast ponownie wykonać pomiar tej samej wielkości, znowu otrzymalibyśmy wynik  $\lambda_i$ , i to z całkowitą pewnością (dla widma dyskretnego, oraz pomiaru idealnego [1]). Ciągła obserwacja unieruchamia zatem kwantową ewolucję – mówi się w tym przypadku o kwantowym efekcie Zenona.

W czasie pomiaru informacja o mierzonym układzie zostaje zapisana w układzie pomiarowym, i to w makroskopowo odróżnialny sposób (powstaje tu przypadkowa 'ścieżka' od mikroskopowej prostoty do makroskopowej złożoności). Pomiar dokonuje się w wyniku oddziaływania przyrządu i układu mierzonego. Oddziałujące układy nie są z reguły opisane



swoimi funkcjami falowymi (nie są w stanach czystych), ale można je opisać przy pomocy macierzy gęstości. Dla stanu czystego, np.  $|\Psi\rangle$ , macierz gęstości ma postać operatora  $\hat{\rho} = |\Psi\rangle\langle\Psi|$ . Dla podukładu macierz gęstości jest wynikiem wycalkowania macierzy gęstości całego układu po zmiennych drugiego podukładu, tj.  $\hat{\rho}_1 = \text{Tr}_2 \hat{\rho}$ . Otrzymany w ten sposób operator macierzy gęstości podukładu nie ma w ogólności postaci  $|\varphi\rangle\langle\varphi|$ , co oznacza, że podukład nie jest w stanie czystym. Jest on w tzw. stanie mieszanym, zadanym liniową kombinacją macierzy gęstości stanów czystych podukładu, tj.  $\hat{\rho}_1 = \sum_a p_a |\psi_a\rangle\langle\psi_a|$ ,  $p_a \in R$ ,  $0 < p_a < 1$ ,  $\sum_a p_a = 1$ . Jest to niekoherentna superpozycja (zmieszanie stanów) – dotyczy ona macierzy gęstości, a nie funkcji falowych, w przeciwieństwie do koherentnej superpozycji funkcji falowych, w wyniku której ze stanów czystych otrzymuje się też stan czysty:  $|\psi\rangle = \sum_a q_a |\psi_a\rangle$ ,  $q_a \in C$ ,  $\sum_a |q_a|^2 = 1$ .

Powyższe uwagi zilustrować można prostym przykładem. Załóżmy, że mierzony układ ma tylko dwa dostępne stany  $|\psi_1\rangle$  i  $|\psi_2\rangle$ , będące stanami własnymi mierzonej wielkości  $A$ . Układ odizolowany od przyrządu opisany jest koherentną superpozycją,  $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$ ,  $\alpha = x$  i  $\beta = \sqrt{1-x^2}e^{i\varphi}$ ,  $x, \varphi \in R$ . Takiemu stanowi odpowiada macierz gęstości:

$$\hat{\rho}_1 = |\psi\rangle\langle\psi| = \begin{bmatrix} x^2 & x\sqrt{1-x^2}e^{-i\varphi} \\ x\sqrt{1-x^2}e^{i\varphi} & 1-x^2 \end{bmatrix} \Rightarrow \text{pomiar} \Rightarrow \begin{bmatrix} x^2 & 0 \\ 0 & 1-x^2 \end{bmatrix}.$$

W wyniku pomiaru znikają niediagonalne elementy zawierające różnicę faz między współczynnikami  $\alpha$  i  $\beta$  (przyczynę interferencji). Po pomiarze, macierz gęstości jest niekoherentną superpozycją dwóch macierzy gęstości  $|\psi_1\rangle\langle\psi_1|$  i  $|\psi_2\rangle\langle\psi_2|$ , ze współczynnikami  $x^2$  i  $1-x^2$ . W jaki sposób znikają niediagonalne elementy? Załóżmy, że przyrząd pomiarowy przed pomiarem jest w stanie  $|\Phi_0\rangle$ . Jeśli układ byłby w stanie  $|\psi_1\rangle$ , to wynik pomiaru byłby  $\lambda_1$  i informacja taka zapisałaby się w makroskopowym układzie pomiarowym, który w wyniku pomiaru znalazłby się w stanie  $|\Phi_1\rangle$ . Podobnie dla stanu  $|\psi_2\rangle$  wynik byłby  $\lambda_2$ , a stan przyrządu  $|\Phi_2\rangle$ . Cały układ: przyrząd i mierzony układ, niezależnie, czy przy włączonym, czy wyłączonym oddziaływaniu, jest w stanie czystym. Jeśli przed pomiarem jest to stan  $(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) \otimes |\Phi_0\rangle$ , to po pomiarze, stan:  $|\Omega\rangle = \alpha|\psi_1\rangle \otimes |\Phi_1\rangle + \beta|\psi_2\rangle \otimes |\Phi_2\rangle$ . Ani układ, ani przyrząd nie są już wtedy w stanach czystych – razem tworzą tzw. stan splątany, a macierz gęstości dla mierzonego układu ma postać:



$$\hat{\rho}_1 = Tr_2 |\Omega\rangle\langle\Omega| = \begin{bmatrix} |\alpha|^2 Tr_2 |\Phi_1\rangle\langle\Phi_1| & \alpha\beta^* Tr_2 |\Phi_1\rangle\langle\Phi_2| \\ \beta\alpha^* Tr_2 |\Phi_2\rangle\langle\Phi_1| & |\beta|^2 Tr_2 |\Phi_2\rangle\langle\Phi_2| \end{bmatrix}.$$

$Tr_2 |\Phi_1\rangle\langle\Phi_2|$  jest całką wielokrotną (o krotności rzędu liczby Avogadro) z iloczynu dwóch funkcji różniących się w makroskopowy sposób, a więc zależnością funkcyjną od ogromnej liczby zmiennych – daje to w rezultacie zero, nawet gdyby pojedyncze całki dawały wkłady tylko nieznacznie mniejsze od 1. Taki mechanizm znikania elementów niediagonalnych w macierzy gęstości prowadzi do ilustracji pomiaru von Neumanna (tzw. superwybór [2]). Dokładniejsza analiza zachowania się niediagonalnych elementów macierzy gęstości pozwala na określenie dynamiki ich wygaszania w czasie trwania pomiaru. W ogólności jest to bardzo szybki zanik eksponencjalny, z czasem defazowania (tj. znikania informacji o różnicy faz współczynników  $\alpha$  i  $\beta$ ) zależnym od szczegółów oddziaływania, od układu pomiarowego i od odległości  $\lambda_1$  i  $\lambda_2$  [4].

Każde oddziaływanie dwóch układów można by interpretować jako pomiar jednego układu przez drugi (pomiar von Neumanna zachodzi jednak tylko wtedy, gdy układ pomiarowy jest makroskopowy). Ewolucja macierzy gęstości jednego z układów pod wpływem oddziaływania drugiego jest nazywana ogólnie dekoherencją. W wyniku oddziaływania układów (np. pomiarów) dochodzi do splątania kwantowego. Czysty stan całego układu nazywa się stanem splątanym, jeśli nie jest prostym iloczynem tensorowym stanów czystych obu układów (jest on wtedy liniową kombinacją takich iloczynów). Splątanie układów jest naturalnym wynikiem ich oddziaływania i nie może być uzyskane lokalnie poprzez manipulowanie tylko w jednym z układów. Splątanie leży u podstaw pomiaru i dekoherencji – najpowszechniejszych zjawisk w mikroświecie. Dla dostatecznie małych układów (obu mikroskopowych, np. pojedynczych cząstek) można analizować i nawet kontrolować w czasie ewolucję splątania i wzajemnej dekoherencji. Stwarza to nowe możliwości przetwarzania informacji w kwantowy sposób, niedostępny dla informatyki klasycznej. Można planować deterministyczną kwantową ewolucję układów złożonych z małych oddziałujących podukładów, w analogii do klasycznych algorytmów. Konieczne jest jednak by zdążyć przetworzyć kwantową informację w niewielkim układzie, wykorzystując w kontrolowany sposób splątanie się jego podukładów, dopóki nie dopłącze się otoczenie i nie dokona dekoherencji (pomiaru) w niekontrolowany sposób.

Ze względu na nielokalny charakter mechaniki kwantowej przejawiający się w kwantowym splątaniu, przetwarzanie informacji kwantowej i jej przekazywanie jest zupełnie nieklasycznym zjawiskiem. Pojemność informacyjna nawet niewielkich układów kwantowych jest ogromna, również niespotykana w klasycznej informatyce – wymiar przestrzeni Hilberta dla np. 100 dwupoziomowych układów (qubitów) wynosi  $2^{100}$  (wymiar iloczynu tensorowego 100 dwuwymiarowych przestrzeni). Przetwarzanie informacji, jaką można zakodować w stanie kwantowym 100 dwupoziomowych układów, przekracza zatem możliwości jakichkolwiek klasycznych komputerów – chodzi o przetwarzanie macierzy  $2^{100} \times 2^{100}$  (układ kwantowy przetwarza je sam). Opanowanie technik sterowania procesami kwantowymi otworzyłoby niezwykle możliwości. Informację zrozumiałą dla człowieka (czyli klasyczną) należałoby wczytać w sterowany układ kwantowy, pozwolić jej błyskawicznie i nielokalnie ewoluować zgodnie z zaprojektowanym algorytmem





kwantowym, a następnie wynik odczytać w klasycznej postaci. Z odczytaniem byłyby trudności, zgodnie z zasadami nieoznaczoności, nie cała kwantowa informacja jest dostępna. Odpowiednio manipulując jednak koherentną superpozycją (czyli wykorzystując interferencyjne efekty) można uzyskać pożądaną część kwantowej informacji w klasycznej postaci. Równoległe i równoczesne przetwarzanie całej kwantowej informacji w wielocząstkowym układzie kwantowym eksponencjalnie dystansuje informatykę klasyczną (pewne spowolnienia wynikają z ograniczeń odczytu). Podanie szybkich kwantowych algorytmów (Tabela 1., [3,4]) dla rozwiązania kłopotliwych zagadnień klasycznej informatyki może zapowiadać zatem rewolucję informatyczną i technologiczną.

**Tabela 1. Algorytmy kwantowe**

1. Algorytm Deutscha i Jozsy, 1992	„Oracle setting“, rozróżnienie funkcji zbalansowanej od stałej	przysp. eksponencjalne
2. Algorytm Simona, 1997	Rozróżnienie funkcji 1-1 od funkcji 2-1	przysp. eksponencjalne
3. Algorytm Shora dla faktoryzacji, 1994	Znajdowanie liczb pierwszych	przysp. eksponencjalne
4. Transformata Fouriera a'la Kitaev, 1995	Szybka kwantowa transformata Fouriera	
5. Algorytm Grovera, 1995	„Finding needle in a haystack“, przeszukiwanie bazy danych	przysp. kwadratowe
6. Algorytm Shora kwantowej korekty błędów 1996	Kwantowa korekta błędów	

Należy podkreślić, że wyidealizowane algorytmy kwantowe są bardzo trudne do praktycznej realizacji. Nieunikniona dekoherencja wywołana przez otoczenie nawet najlepiej izolowanego układu prowadzi do kumulacji błędów i nieodwracalnej utraty informacji. Dopiero zastosowanie kwantowej korekty błędów [3,4,5] na każdym etapie kwantowego algorytmu mogłoby umożliwić praktyczną bezbłędną realizację procedur kwantowych. Dobrze już rozpoznane protokoły korekty błędów o charakterze kombinatorycznym, prowadzą jednak do silnego zwielokrotnienia układu, a co za tym idzie, do gwałtownego (eksponencjalnego) wzrostu dekoherencji wraz z liczbą qubitów. Stąd stosunek czasu dekoherencji do czasu kwantowych elementarnych operacji logicznych musi być dostatecznie duży (co najmniej  $10^6$ ), by można było skutecznie zastosować procedury korekty. To nie jedyne trudności na drodze praktycznego wykorzystania informacji kwantowej. Równie silne ograniczenia wynikają z podstawowych własności stanów kwantowych, w szczególności tzw. qubitów, odróżniających je od klasycznych bitów. Twierdzenia: *no-cloning* [6], *no-broadcasting* [7] i *no-deleting* [8], mówiące o niemożności kopiowania nieznanymi stanów kwantowych (kopiowanie umożliwiłoby równoczesne pomiary, przecząc zasadzie nieoznaczoności), rozpowszechniania, jak i wymazywania nieznanymi stanów, znacznie komplikują niektóre procedury, jak np. proste resetowanie kwantowego rejestru, niezbędne dla powtarzalności kwantowego komputera.



Informatyka kwantowa ma niezwykle i zadziwiająco możliwości – wynikają one jednak, podobnie jak splątanie, z elementarnych własności algebraicznych iloczynu tensorowego. Można to zademonstrować na przykładzie kwantowego kodowania i kwantowej teleportacji (Tabela 2. i 3., [3-5]). W przypadku kodowania kwantowego wykorzystuje się nielokalny charakter stanów splątanych. Dokonując operacji lokalnych tylko na jednym qubicie, z jednego stanu splątanego uzyskać można trzy pozostałe splątane stany tzw. bazy Bella w 4-wymiarowej przestrzeni Hilberta dwóch qubitów (w przypadku klasycznym kodowanie pary bitów wymaga działań na obu bitach).

Podobnie w przypadku teleportacji kwantowej, wykorzystanie własności iloczynu tensorowego pozwala na interpretację prostych relacji algebraicznych, jako przekazania zawartości qubitu 1 na inny, nawet odległy qubit 3 (Tabela 3.). Mimo, że kwantowy transport informacji jest natychmiastowy, w czasie teleportacji nie naruszona jest relatywistyczna zasada ograniczenia przekazu informacji przez prędkość światła. Qubit 3 ma wprawdzie natychmiastowo pełną informację o qubicie 1, ale w zbyt dużej ilości. Żeby odbiorca przy qubicie 3 wiedział, która jest właściwa, musi otrzymać dodatkową informację klasyczną, przekazaną wolniej niż prędkość światła w próżni. Fakt ten zwraca też uwagę na niezrozumiany jeszcze do końca aspekt wzajemnej relacji informacji klasycznej i kwantowej – układ kwantowy bez tej informacji, to co innego (nie ujawniona teleportacja), niż układ kwantowy zaopatrzony w taką informację (teleportacja dokonana).

**Tabela 2. Protokół gęstego kodowania kwantowego**

Stan pary qubitów – wektor z 4 wymiarowej przestrzeni Hilberta  $H_1 \otimes H_2$ , tj.

$$a|0\rangle \otimes |0\rangle + b|0\rangle \otimes |1\rangle + c|1\rangle \otimes |0\rangle + d|1\rangle \otimes |1\rangle,$$

ale w przestrzeni  $H_1 \otimes H_2$  można wybrać bazę inaczej, np. złożoną z maksymalnie splątanych ortogonalnych stanów (tzw. stanów Bella):

$$|\psi^1\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2), \quad |\psi^2\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2),$$

$$|\psi^3\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 \otimes |0\rangle_2 + |1\rangle_1 \otimes |1\rangle_2), \quad |\psi^4\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 \otimes |0\rangle_2 - |1\rangle_1 \otimes |1\rangle_2).$$

Dokonując wyłącznie lokalnych operacji na qubicie 2 można uzyskać wszystkie stany Bella wychodząc z jednego, np.:

1) operacja tożsamościowa,  $|0\rangle_2 \rightarrow |0\rangle_2$  i  $|1\rangle_2 \rightarrow |1\rangle_2$  daje

$$|\psi^1\rangle_{12} \Rightarrow |\psi^1\rangle_{12}$$

2) zamiana stanów,  $|0\rangle_2 \rightarrow |1\rangle_2$  i  $|1\rangle_2 \rightarrow |0\rangle_2$  daje

$$|\psi^1\rangle_{12} \Rightarrow |\psi^3\rangle_{12}$$

3) zróżnicowanie fazowe o  $\pi$ ,  $|0\rangle_2 \rightarrow -|0\rangle_2$  i  $|1\rangle_2 \rightarrow |1\rangle_2$  daje

$$|\psi^1\rangle_{12} \Rightarrow |\psi^2\rangle_{12}$$

4) zamiana stanów i zróżnicowanie fazowe,  $|0\rangle_2 \rightarrow -|1\rangle_2$  i  $|1\rangle_2 \rightarrow |0\rangle_2$  daje

$$|\psi^1\rangle_{12} \Rightarrow |\psi^4\rangle_{12}$$

Podobne kodowanie pary klasycznych bitów wymagałoby działania na obu bitach, zatem



kwantowe rejestry mają zwielokrotnioną pojemność.

Kwantowa teleportacja może być wykorzystana także do wykonywania operacji logicznych w odmienny sposób, niż przy pomocy fizycznie implementowanych bramek [9]. Uogólnienia protokołu teleportacji pozwalają bowiem transportować również unitarne operatory, tzn. wykonywać ewolucje kwantowe na odległość (zmieniając stan qubitu 1, zmienimy także stan qubitu 3 po teleportacji). Operacje logiczne reprezentowane są przez unitarne operatory ewolucji. Można by więc teleportacyjnie wykonywać operacje logiczne kwantowych algorytmów. Zamodelowanie w ten sposób uniwersalnej dwu-qubitowej operacji CNOT (Tablica 4.) wymagałoby wprowadzenia posługiwania się nie tylko stanami Bella, ale też splątanymi stanami trzech qubitów – tzw. stanami Greenbergera-Zorna-Zeilingera [5,9]. Lokalne wykonywanie pomiarów, w tym przypadku rzutowania na ortogonalne splątane stany, prowadzące do teleportacji, mogłyby być jednak wolne od dekoherencji fizycznie implementowanych bramek. Wydaje się prawdopodobne przeprowadzenie takiego scenariusza realizacji kwantowych algorytmów w ramach optyki liniowej, gdzie opanowano dokładne operacje jedno-qubitowe, i bardzo zaawansowane są techniki precyzyjnego splątywania dwóch i trzech qubitów.

#### 1.4. Komputer kwantowy – perspektywy i ograniczenia

Dowolną deterministyczną ewolucję kwantową można przedstawić jako sekwencję operacji jedno-qubitowych i uniwersalnej operacji dwu-qubitowej (np. CNOT) [3,4]. Pozwala to na algorytmizację procesów kwantowych i leży u podstaw koncepcji komputera kwantowego [4,5,10]. Jeśli by dysponować idealnymi qubitami i móc je dowolnie sprzęgać ze sobą oddziaływaniami w kontrolowany sposób, to nawet niewielka ich liczba (w porównaniu z liczbą tranzystorów w klasycznych procesorach), tj. 100 – 1000 qubitów pozwoliłaby na realizację nieosiągalnych klasycznie zadań w bardzo krótkim czasie [3-5,10]. Działają już 3-5-qubitowe komputery kwantowe (Tabela 5., [5,10]) na spulątkowanych jonach i spinach jądrowych molekuł, jednak ich możliwości są jeszcze niewielkie.

**Tabela 3. Protokół teleportacji kwantowej**

Chcemy przeteleportować stan qubitu 1,  $|\varphi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$ , na inny qubit 3.  
W tym celu splątujemy qubit 3 z pomocniczym qubitem 2, np.  
 $|\psi^2\rangle_{23} = \frac{1}{\sqrt{2}} (|0\rangle_2 \otimes |1\rangle_3 - |1\rangle_2 \otimes |0\rangle_3)$ ,  
wtedy układ trzech qubitów jest w stanie  $|\phi\rangle_{123} = |\varphi\rangle_1 \otimes |\psi^2\rangle_{23}$ ; można go przedstawić w innej bazie:  
$$2|\phi\rangle_{123} = |\psi^2\rangle_{12} \otimes (-\alpha|0\rangle_3 - \beta|1\rangle_3) + |\psi^1\rangle_{12} \otimes (-\alpha|0\rangle_3 + \beta|1\rangle_3) \\ + |\psi^4\rangle_{12} \otimes (\alpha|1\rangle_3 + \beta|0\rangle_3) + |\psi^3\rangle_{12} \otimes (\alpha|1\rangle_3 - \beta|0\rangle_3)$$
  
Wykorzystano tu bazę przestrzeni  $H_1 \otimes H_2 \otimes H_3$  rozpiętą przez wektory Bella w  $H_1 \otimes H_2$  (Tabela 2.).



Współczynniki  $\alpha$ ,  $\beta$ , które chcemy teleportować, od razu już znajdują się przy qubicie 3 (nawet bardzo odległym, ale splątany z 1) w 4-ch różnych kombinacjach. Wystarczy teraz w podprzestrzeni  $H_1 \otimes H_2$  wybrać jeden z ortogonalnych stanów  $|\psi^i\rangle_{12}$  (przez pomiar – rzutowanie), wtedy cały układ znajdzie się np. w stanie  $|\psi^4\rangle_{12} \otimes (\alpha|1\rangle_3 + \beta|0\rangle_3)$ , jeśli dla przykładu wybrać  $i = 4$ . Należy teraz poinformować (klasycznie) odbiorcę przy qubicie 3, które  $i$  uzyskaliśmy w wyniku pomiaru, żeby wiedział jak lokalnie na qubicie 3 uzyskać stan  $|\varphi\rangle_3 = \alpha|0\rangle_3 + \beta|1\rangle_3$ . Równocześnie qubit 1 przestaje być w stanie czystym  $|\varphi\rangle_1$ , bo qubit ten zostaje splątany z qubitami 2, podczas gdy qubit 3 odpłataje się i po lokalnej manipulacji uzyskuje wyjściową zawartość qubit 1. Stan qubit 1 jest więc teleportowany na qubit 3 bez naruszenia twierdzenia *no-cloning*, ani zasad relatywistycznych (klasyczna informacja o  $i$  została przekazana wolniej niż światło).

W przypadku obu istniejących konstrukcji 3(5)-qubitowych (na spletkowanych jonach i w technikach NMR) nie wydaje się możliwe skalowanie i przekroczenie bariery kilku-qubitowych układów (działania na jonach są zbyt wolne, ilość oddziałujących spinów jądrowych w molekułach jest mała i ograniczona, w obu konstrukcjach są kłopoty z resetowaniem [5]). Główny problem skalowania polega na tym, że wraz z liczbą qubitów niekontrolowana dekoherencja rośnie eksponencjalnie. Kwantowe schematy korekty błędów [3-5] wykorzystują niezmienniczość określonych podprzestrzeni zwielokrotnionych układów wobec skorelowanej dekoherencji. Taka dekoherencja rośnie wprawdzie szybciej z liczbą qubitów  $N$  (tj. jak  $e^{N^2}$ , podczas gdy nieskorelowana dekoherencja rośnie jak  $e^N$ ), ale umożliwia określenie nieczułych na dekoherencję podprzestrzeni (uogólnienia stanu typu *singlet*), w których można bezpiecznie przechowywać informację. Inne koncepcje ochrony przed dekoherencją, to czasowe wyteleportowanie informacji do bardziej odpornych części układu, lub znalezienie fizycznego mechanizmu korekty, jak np. w przypadku koncepcji topologicznego komputera na anyonach [11].

Konstrukcja komputera kwantowego w realistycznym układzie fizycznym wymaga spełnienia szeregu warunków (nazywanych *kryteriami DiVincenzo* [19]):

- 1) odpowiednio zdefiniowany qubit – dwa stany kwantowe oddzielone od pozostałych stanów układu (względnie duże odległości energetyczne, wzbronione przejścia), tak by informacja w niego wpisana nie ulegała wpływowi,
- 2) określenie możliwości wpisywania informacji w qubit – tj. możliwości uzyskania dowolnej superpozycji dwóch stanów qubit 1 przy pomocy zewnętrznego, makroskopowo regulowanego pola (np. oscylacje Rabiego w realistycznym obszarze pól),
- 3) możliwość skalowania qubit 1 do wielo-qubitowego urządzenia,
- 4) zaprojektowanie i implementowanie podstawowej operacji dwu-qubitowej, o którą oprócz by można wykonanie dowolnej kwantowej operacji logicznej (taką bramką może być CNOT lub inna [5,10], w każdym przypadku konieczne jest opanowanie techniki włączania i wyłączania oddziaływania qubitów w precyzyjny sposób, w bardzo krótkich odstępach czasu, tj. sterowanie splątaniem dwóch qubitów),
- 5) zapewnienie stosunku rzędów czasu potrzebnego na wykonanie elementarnych operacji logicznych i czasu dekoherencji na poziomie nie mniejszym niż 6,



- 6) zapewnienie możliwości oddziaływania dużej liczby qubitów, albo bezpośrednio (co trudne), albo poprzez qubit pośredniczący (np. foton), w celu skalowania komputera i implementacji korekty błędów,
- 7) zapewnienie możliwości odczytu informacji na wyjściu,
- 8) zapewnienie możliwości resetowania całego układu .

Niektóre zastosowania kwantowej informatyki, jak kodowanie i transmisja, nie wymagają spełnienia wszystkich wyżej wymienionych warunków i wydają się bardziej realistyczne, o czym świadczy znaczny postęp w tym zakresie [5]; ograniczenia związane są tam głównie ze swobodnymi nośnikami informacji – mobilnymi qubitami, np. fotonami, i możliwościami utrzymania stabilnych ich kwantowych cech na dużych odległościach (ostatnie eksperymenty ze spowalnianiem i zatrzymywaniem światła wydają się tu też bardzo obiecujące).

#### Tabela 4. CNOT – sterowane zaprzeczenie

CNOT (*controlled-NOT*) – operacja dwu-qubitowa. Na prostej bazie przestrzeni  $H_1 \otimes H_2$  działa wg przepisu:

$$|00\rangle \Rightarrow |00\rangle \quad |01\rangle \Rightarrow |01\rangle \quad |10\rangle \Rightarrow |11\rangle \quad |11\rangle \Rightarrow |10\rangle$$

Spełnienie wyżej wymienionych wymagań wcale nie jest proste i nie każdy układ dwupoziomowy może być qubitami. Jako qubity proponuje się rozmaite układy fizyczne [5]: foton (*jest, nie ma* w danym modzie), ekscyton (*jest, nie ma* w kropce kwantowej), spin jądrowy lub elektronowy w polu magnetycznym (1/2, -1/2), prąd tunelowy w nadprzewodzącym złączu Josephsona (kierunek  $\rightarrow$  lub  $\leftarrow$ ). Bardziej zaawansowane koncepcje to pojedynczy qubit na wielocząstkowych stanach w układach spinowych [12], fermionowych, bozonowych a nawet anyonowych [11]. Poszukuje się zwłaszcza rozwiązań w obszarze nanotechnologii przy wykorzystaniu dobrze rozwiniętej technologii miniaturyzacji klasycznej informatyki (epitaksji, litografii i procesów samoorganizacji).

W obszarze nanotechnologii szczególnie interesujące są kropki kwantowe – układy o rozmiarach od kilku do kilkudziesięciu nanometrów, najczęściej w półprzewodnikowych heterostrukturach, mogące zawierać nawet pojedyncze elektrony. Stany elektronów zlokalizowanych w takich kropkach, z energią wiązania od kilku do kilkudziesięciu meV, mogą być (w przeciwieństwie do elektronów w atomach) łatwo modyfikowane polem magnetycznym (do 10 T) w zakresie do kilkudziesięciu procent, a także, w podobnym zakresie, łatwo osiągalnym technicznie polem elektrycznym. Stale rozwijane techniki wytwarzania kropek pozwalają na budowę skorelowanych układów kropek, takich jak molekuly, czy łańcuchy kropek – niezbędne dla procesorów kwantowych. Zarówno orbitalne (elektronowe lub ekscytonowe), jak i spinowe stopnie swobody nośników uwięzionych w kropkach brane są pod uwagę [12-16]. Całkowicie sterowana światłem ekscytonowa bramka logiczna na kwantowej molekule (sprężonej parze kropek) GaAs/InAs [14] jest całkiem realistyczna – zademonstrowano już splątanie stanów [15]. Czas relaksacji ekscytonów w kropkach jest rzędu nanosekundy, więc zastosowanie ultraszybkich femtosekundowych technik optycznych [17] daje szansę na korektę błędów. Zastrzeżenia powstały jednak ostatnio w związku z możliwością pikosekundowej dekoherencji ekscytonów poprzez kanał



niestabilnych polaronów [18], co mocno podważa przydatność takiej implementacji kwantowych bramek.

**Tabela 5. Implementacje komputera kwantowego**

Fizyka atomowa (zrealizowany 3-qubitowy)	Jony w pułapkach elektrycznych	Cirac, Zoller (1995) Monroe et al. (1995)
1. Optyka kwantowa	QED – kwantowa elektrodynamika mikrownek	Turchette et al. (1995) Imamoglu et al. (1999)
2. Jądrowy rezonans magnetyczny, NMR (zrealizowany 3-qubitowy)	Spiny jądrowe molekuł w cieczach	Cory et al. (1997) Gershenfeld et al. (1997)
3. Elektronowy rezonans magnetyczny, EPR	Spiny elektronowe	Kane (1998) Vrijen (2000)
4. Rezonansowa spektroskopia nadprzewodników	Nadprzewodzące złącza Josephsona	Averin et al. (1997) Shnirman et al. (1997) Mooij et al. (1999)
5. Fizyka elektronów	Elektrony na powierzchni He-4	Platzman, Dykman (1999)
6. Sterowane polem magnetycznym lub elektrycznym struktury nanoskopowe (kropki kwantowe)	Spinowe stopnie swobody kropek kwantowych	DiVincenzo et al. (1998) DiVincenzo et al. (2000) Tanamoto (2000) Jacak et al. (2001)
7. Optycznie sterowane struktury nanoskopowe (kropki kwantowe)	Orbitalne stopnie swobody kropek kwantowych (elektronowe lub ekscytonowe)	Zanardi, Rossi (1998) Li, Arakawa (2000) Bayer et al. (2001)
8. Automaty komórkowe, układy biologiczne	Automaty komórkowe	Lloyd (1993) Benjamin (2000)
9. Wzbudzenia topologiczne	Anyony, ułamkowy efekt Halla	Kitaev (1997)

Spinowe stopnie swobody mogą okazać się znacznie korzystniejsze [12,13]. Czas dekoherencji spinu pojedynczego elektronu w kropce szacuje się w skali mikrosekund (wobec bardzo słabego sprzężenia z fononami). Trudności w tym przypadku związane są raczej z komplikacjami uzyskania pojedynczego elektronu w kropce, oraz ze słabym rozszczepieniem Zeemana w tych układach (np. 0.03 meV/T w GaAs). Różnica energii stanów qubitu zadanego przez dwie orientacje spinu w polu magnetycznym jest zatem mała, a czas operacji jedno-qubitowych byłby niekorzystnie długi. W celu ominięcia tej trudności DiVincenzo [12] podał koncepcję qubitu spinowego na stanach trzech elektronów w trzech jedno-elektronowych kropkach i wykorzystanie do jedno-qubitowych operacji silnego oddziaływania wymiennego (oddziaływanie to komutuje z  $\hat{S}^2$  i  $\hat{S}_z$ ; dla 8-miu stanów trójki spinów, dwie pary stanów mają te same  $S$  i  $S_z$ , na jednej z tych par proponuje się rozpiąć



qubit; wcześniej proponowano też qubit na stanach singletowym i trypletowym pary elektronów w kropce [16]). Oddziaływanie wymienne, choć spinowe, jest pochodzenia orbitalnego (Tabela. 6) i wyraża się poprzez różnicę energii stanów trypletowego i singletowego pary elektronów. Dobrze znane przejście singlet-tryplet w polu magnetycznym (dla pola rzędu 1T, w przypadku dużych kropek kwantowych) umożliwia zaprojektowanie sterowanego polem magnetycznym splątania stanów spinowych, co przy dużej wartości rozszczepienia singlet-tryplet poza punktem krytycznym, może pozwolić na implementację bardzo szybkich dwu-qubitowych operacji, a także jedno-qubitowych dla wielo-spinowych qubitów.

Mimo wielkich wysiłków nie zbudowano jednak jeszcze pozwalającej na skalowanie bramki logicznej w technologii stało-ciałowej, nawet przy użyciu kropek kwantowych. Wobec skali trudności tego zadania, praktyczna konstrukcja dużego komputera kwantowego może nie być realistyczna w najbliższym czasie, jednakże gwałtowny postęp w zakresie eksperymentalnej mechaniki kwantowej doprowadzi z pewnością do wielu ważnych odkryć i praktycznych zastosowań, już dziś bardzo atrakcyjnych np. w zakresie zabezpieczeń i transmisji.

**Tabela 6. Zawansowanie technik informatyki kwantowej**

Rodzaj <i>hardwaru</i>	Liczba qubitów	Liczba kroków przed dekoherencją	status
Kwantowa kryptografia	1	1	<b>zaimplementowana</b>
Kwantowa kryptografia na stanach splątanych	2	1	<b>zaimplementowana</b>
Bramka CNOT	2	1	<b>zademonstrowana</b>
Układ bramek	2	2	<b>zademonstrowany</b>
Algorytm Deutscha	2	3	<b>zademonstrowany</b>
Zdwojenie pojemności kanału	2	2	<b>blisko realizacji</b>
Teleportacja	3	2	<b>zademonstrowana</b>
Wymiana splątania	4	1	<b>zademonstrowana</b>
<i>Repeater</i> dla kryptografii	kilka	kilka	<b>niekompletna teoria</b>
Kwantowa symulacja	kilka	kilka	<b>prosta demonstracja</b>
Algorytm Grovera z <i>toy-data</i>	3+	6+	<b>zademonstrowany</b>
Ultra-precyzyjny <i>standard</i> częstości	kilka	kilka	<b>przewidywany</b>
<i>Purifikacja</i> splątania	kilka	kilka	<b>przewidywana</b>
Algorytm Shora z <i>toy-data</i>	16+	100+	?
Kwantowa maszyna <i>faktoryzująca</i>	100+	< 1000	??
Uniwersalny komputer kwantowy	1000+	1000+	???



## 2. Zasady kwantowego opisu

Stan kwantowy zamkniętego (odosobnionego<sup>3</sup>) układu opisujemy funkcja falowa:

$|\Psi\rangle \in H$ , gdzie  $H$  jest przestrzenia Hilberta, tj. zupełną<sup>4</sup> przestrzenią metryczną z metryką zadaną przez iloczyn skalarny  $\langle \Psi | \Phi \rangle$  o własnościach :

- $\langle \Psi | \Psi \rangle \geq 0$ ,  $\langle \Psi | \Psi \rangle = 0 \Leftrightarrow |\Psi\rangle = 0$
- $\langle \Psi | a_1\Phi + a_2\Theta \rangle = a_1\langle \Psi | \Phi \rangle + a_2\langle \Psi | \Theta \rangle$
- $\langle \Psi | \Phi \rangle = \langle \Phi | \Psi \rangle^*$ .

$H$  jest zupełną wg normy  $\|\Psi\| = \sqrt{\langle \Psi | \Psi \rangle}$ . Przykładem może tu być przestrzeń  $L^2$ , funkcji całkowalnych z kwadratem, iloczyn skalarny zadany jest w tym przypadku całką  $\int \Psi(q)^* \Phi(q) dq$ .

Często zakłada się że  $H$  jest ośrodkowa, tzn., że istnieje gęsty<sup>5</sup> podzbiór przeliczalny.

Funkcje falowe różniące się o stały zespolony czynnik identyfikujemy (ograniczyć się można tylko do unormowanych funkcji, wówczas identyfikujemy funkcje różniące się o czynnik fazowy).

Moduł funkcji falowej identyfikujemy z gęstością prawdopodobieństwa znalezienia cząstki i tę wielkość traktujemy jako mierzalną.

Funkcja falowa spełnia równanie Schrödingera-Heisenberga

$$i\hbar \frac{\partial |\Psi\rangle}{\partial t} = \hat{H} |\Psi\rangle,$$

gdzie  $\hat{H}$  jest operatorem Hamiltona. Zakładamy że jest operatorem liniowym i z warunku, że nie wyprowadza poza normowanie otrzymujemy, że jest samosprzężony (hermitowski).

Z liniowością równania ruchu wiąże się zasada superpozycji: jeśli dwa stany są rozwiązaniem równania ruchu, to ich liniowa kombinacja także.

Ewolucja wg równania Schrödingera jest unitarną ewolucją (też wynika to z liniowości i hermitowskości hamiltonianu), tj.

$$|\Psi(t)\rangle = U(t) |\Psi(0)\rangle$$

<sup>3</sup> tzn. nieoddziałującego z innymi układami

<sup>4</sup> przestrzeń metryczna jest zupełna, jeśli wszystkie ciągi Cauchy'ego (wg metryki -- normy) są zbieżne

<sup>5</sup> zbiór gęsty to taki, którego domknięcie jest całą przestrzenią

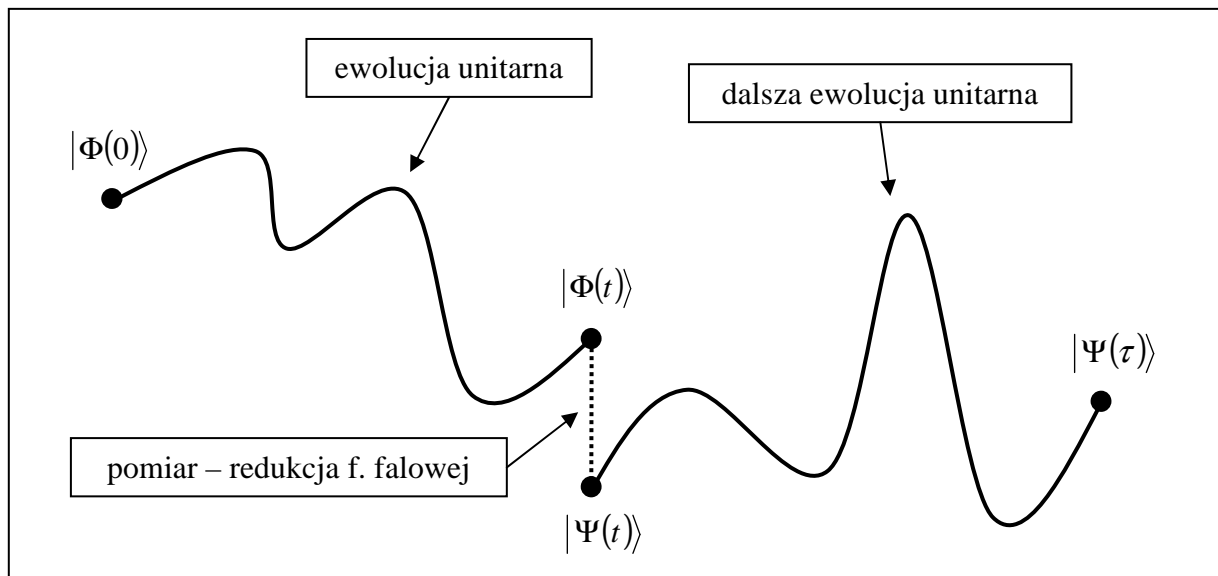


i dla hamiltonianu niezależnego od czasu

$$U(t) = e^{-i\hat{H}t/\hbar}.$$

Zatem dla ewolucji kwantowej zamkniętego układu mamy spełnioną zasadę determinizmu: hamiltonian jednoznacznie określa przyszłość (i przeszłość) układu kwantowego, jeśli zadany jest stan w chwili początkowej. Oznacza to jednoznaczność trajektorii układu w przestrzeni Hilberta<sup>6</sup>. Ten determinizm jest podstawą kwantowej informatyki, gdyż podobnie jak w przypadku klasycznym, pozwala na planowanie określonego zachowania układu kwantowego (wg programu).

W mechanice kwantowej zawarty jest jednak głęboki niedeterminizm związany z pomiarem. Ewolucja unitarna zostaje wówczas zakłócona w nieprzewidywalny i nieodwracalny sposób. Bezwrotnie tracona jest wtedy informacja kwantowa, a przynajmniej jej część. Bez pomiaru nie jesteśmy jednak w stanie dowiedzieć się niczego o kwantowym układzie. Można tu postawić pytanie, kto dokonuje pomiaru. W odpowiedzi można podać, obserwator za pomocą klasycznego, makroskopowego przyrządu (bo innego nie mógłby odczytać). Zatem pomiar tak rozumiany wymaga trzech składników: układu kwantowego, który będzie mierzony, klasycznego przyrządu pomiarowego, który na skutek oddziaływania zapisze w sobie wynik pomiaru w makroskopowy sposób i z obserwatora rejestrującego wynik (nie jest jasne, czy obserwatorem może być maszyna klasyczna i czy ten trzeci składnik jest niezbędny, jednakże rozwiązania informatyki klasycznej korzystają w pełni z obecności obserwatora).



Rys.1. Schematyczne przedstawienie ewolucji stanu kwantowego w przestrzeni Hilberta: unitarna ewolucja i rzutowanie von Neumanna

<sup>6</sup> nie ma jednak trajektorii w przestrzeni fazowej



### 3. Pomiar w mechanice kwantowej

Wielkości mierzalne nazywamy obserwabami i odpowiadają im liniowe operatory hermitowskie. Ich widmo (wartości własne) jest rzeczywiste – wartości własne są zatem dobrym kandydatem na wynik pomiaru (który klasycznie musi być wyrażony jako liczba rzeczywista).

Dla operatorów hermitowskich w przestrzeni Hilberta spełnione jest twierdzenie spektralne

$$\hat{A} = \sum_n a_n \hat{P}_n,$$

gdzie  $a_n$  jest  $n$ -tą wartością własną (rzeczywistą w przypadku operatora hermitowskiego) operatora  $\hat{A}$ . Operator  $\hat{P}_n$  jest operatorem rzutowania na podprzestrzeń własną odpowiadającą  $n$ -tej wartości własnej (w przypadku braku degeneracji jest to rzut na pojedynczy kierunek  $n$ -tego wektora własnego). Operator rzutowania posiada własności *nilpotentności* i hermitowskości

$$\begin{aligned}\hat{P}_n \hat{P}_m &= \delta_{nm} \hat{P}_n, \\ \hat{P}_n^+ &= \hat{P}_n.\end{aligned}$$

Dla operatorów ograniczonych jest to proste uogólnienie algebry liniowej w skończeniu wielowymiarowym przypadku. Natomiast dla operatorów nieograczonych występują dodatkowe subtelności, które jednak nie mają istotnego znaczenia w obszarze informatyki kwantowej. Warto dodać, że operator różniczkowania jest operatorem nieograczonym, co pociąga za sobą tę własność dla operatorów pędu i energii kinetycznej (wyrażających się przez gradient).

W wyniku pomiaru następuje redukcja funkcji falowej do przestrzeni rzutowej (jest to tzw. *kolaps von Neumanna*), przy czym wybór operatora rzutu (podprzestrzeni, na którą następuje rzutowanie) jest zupełnie przypadkowy. Określone jest tylko prawdopodobieństwo tego wyboru, a mianowicie,

$$p_n = \|\hat{P}_n |\Psi\rangle\|^2 = \langle \Psi | \hat{P}_n^+ \hat{P}_n | \Psi \rangle = \langle \Psi | \hat{P}_n | \Psi \rangle.$$

W wyniku pomiaru uzyskuje się wynik  $a_n$  z prawdopodobieństwem  $p_n$ , natomiast funkcja

falowa  $|\Psi\rangle$  redukuje się (kolapsuje) do funkcji  $\frac{\hat{P}_n |\Psi\rangle}{(\langle \Psi | \hat{P}_n | \Psi \rangle)^{1/2}}$ .

Jeśli szybko (natychmiastowo) powtórzyć pomiar tej samej wielkości, to kolaps już nie nastąpi, gdyż z prawdopodobieństwem jeden określony jest już wynik takiego pomiaru. Zatem ciągły pomiar utrzymuje układ kwantowy w jednym stanie – zatrzymana jest ewolucja kwantowa (mówimy wtedy o kwantowym efekcie Zenona)



Ewolucja układu kwantowego składa się zatem z elementów deterministycznych, gdy odbywa on dynamikę jako układ zamknięty zgodnie z równaniem Schrödingera,

$$|\Psi(t)\rangle = e^{-i\hat{H}t/\hbar}|\Psi(0)\rangle,$$

gdy Hamiltonian nie zależał jawnie od czasu. Gdy Hamiltonian zależy jawnie od czasu możemy opisać ewolucję przy pomocy złożenia (scalkowania) unitarnych operatorów ewolucji w czasie  $dt$ . Zgodnie z równaniem Schrödingera,

$$|\Psi(t+dt)\rangle = \left(1 - \frac{i}{\hbar}\hat{H}(t)dt\right)|\Psi(t)\rangle,$$

czyli

$$|\Psi(t+dt)\rangle = U(t, dt)|\Psi(t)\rangle,$$

gdzie  $U(t, dt) = \left(1 - \frac{i}{\hbar}\hat{H}(t)dt\right)$ ,  $U^+U = UU^+ = 1$ , z dokładnością do liniowych członów w  $dt$ .

Zawsze jest to jednoznaczna unitarna ewolucja zamkniętego układu. Jeśli jednak chcemy dowiedzieć się o istnieniu i stanie tego układu, musimy dokonać pomiaru jakiejś wielkości. Wówczas następuje kolaps (redukcja) funkcji falowej do wektora własnego (z podprzestrzeni własnej). Ta redukcja gubi nieodwracalnie i zupełnie losowo informację kwantową (chyba że stan był akurat własny dla operatora mierzonej wielkości).

Wybór kierunku rzutowania (podprzestrzeni własnej i funkcji własnej) jest zupełnie przypadkowy, podane jest tylko prawdopodobieństwo tego wyboru – zawarte jest ono w danym stanie w danym momencie poprzez kwadraty modułów współczynników rozwinięcia tego stanu w tym momencie na bazie wektorów własnych operatora wielkości mierzonej (co jest tożsame z  $p_n = \|\hat{P}_n|\Psi\rangle\|^2 = \langle\Psi|\hat{P}_n^+\hat{P}_n|\Psi\rangle = \langle\Psi|\hat{P}_n|\Psi\rangle$ ).

Rzutowanie to (redukcja w wyniku pomiaru) jest niedeterministycznym elementem kwantowej ewolucji, jednak już (w momencie pomiaru) niezamkniętego układu. Kwantowy pomiar oznacza bowiem wejście w oddziaływanie z przyrządem i tego oddziaływania nie można uczynić dowolnie małym (jak przy pomiarach klasycznych wielkości<sup>7</sup>). Jakikolwiek zatem oddziaływanie będące istotą pomiaru układu kwantowego zaburzy stan mierzonego układu i w czasie gdy układ ten oddziałuje z przyrządem nie jest już zamknięty. Nic więc dziwnego, że jego unitarna ewolucja jako zamkniętego układu jest w tym momencie przerwana.

Po pomiarze i wycofywaniu przyrządu układ znowu podejmuje swoją unitarną ewolucję, jednak już z innym warunkiem początkowym, a mianowicie startuje teraz ze stanu w jakim

<sup>7</sup> to jest zasadnicza różnica między klasycznym a kwantowym pomiarem – w klasycznym przypadku oddziaływanie w czasie pomiaru można uczynić dowolnie małym, tzn. nie zaburza ono mierzonej wielkości; w przypadku kwantowym jest to niemożliwe



znalazł się w wyniku pomiaru. Startuje z przypadkowo wybranego stanu własnego operatora mierzonej wielkości. W ogólnym przypadku informacja kwantowa w sensie funkcji falowej układu przed pomiarem została zatem stracona (przynajmniej w dużym stopniu). Ewolucję kwantową z obiema jej aspektami można przedstawić na rysunku 1.

### 3.1. Pomiar w sensie von Neumanna – superwybór Żurka

Założmy, że dwa stany  $|1\rangle, |2\rangle$  są dwoma wektorami własnymi pewnej obserwabli  $A$ , której operator hermitowski zadany jest przez  $\hat{A}$ <sup>8</sup>, tzn.

$$\hat{A}|1\rangle = \lambda_1|1\rangle \text{ oraz } \hat{A}|2\rangle = \lambda_2|2\rangle.$$

Wtedy stan (superpozycja koherentna)  $|\Psi\rangle = c_1|1\rangle + c_2|2\rangle$ ,  $|c_1|^2 + |c_2|^2 = 1$ , gdzie  $c_i \in \mathbb{C}$ ,  $C$  oznacza liczby zespolone (można wybrać  $c_1 = x, c_2 = \sqrt{1-x^2}e^{i\varphi}$ ,  $x, \varphi \in \mathbb{R}$ ,  $x \in [0,1]$ ,  $\varphi \in [0,2\pi)$ ), określa dowolny stan czysty z dwuwymiarowej przestrzeni Hilberta rozpiętej na stanach  $|1\rangle, |2\rangle$ .

W wyniku pomiaru na stanie  $|\Psi\rangle = c_1|1\rangle + c_2|2\rangle$  wielkości  $A$ , z prawdopodobieństwem  $|c_1|^2 = x^2$  otrzymujemy wynik  $\lambda_1$  i zamianę stanu  $|\Psi\rangle$  w stan  $|1\rangle$ , oraz z prawdopodobieństwem  $|c_2|^2 = 1-x^2$  otrzymujemy wynik  $\lambda_2$ , a stan  $|\Psi\rangle$  przechodzi w stan  $|2\rangle$ .

Stan czysty  $|\Psi\rangle = c_1|1\rangle + c_2|2\rangle$  można zapisać przy pomocy macierzy gęstości:

$$\begin{aligned} \hat{\rho} &= |\Psi\rangle\langle\Psi| = (c_1|1\rangle + c_2|2\rangle)(c_1^*\langle 1| + c_2^*\langle 2|) \\ &= x^2|1\rangle\langle 1| + x\sqrt{1-x^2}e^{-i\varphi}|1\rangle\langle 2| + x\sqrt{1-x^2}e^{i\varphi}|2\rangle\langle 1| + (1-x^2)|2\rangle\langle 2|. \end{aligned}$$

Jest to operator rzutowania na stan czysty  $|\Psi\rangle$  (ponieważ  $|\Psi\rangle\langle\Psi|\Phi\rangle = \langle\Psi|\Phi|\Psi\rangle$ ). Macierz gęstości można przepisać w postaci macierzowej,

$$\hat{\rho} = \begin{pmatrix} x^2 & x\sqrt{1-x^2}e^{-i\varphi} \\ x\sqrt{1-x^2}e^{i\varphi} & 1-x^2 \end{pmatrix}.$$

Ślad macierzy gęstości,  $Tr\hat{\rho} = 1$  (dla każdej macierzy gęstości musi być spełniony ten warunek), zauważamy też, że na diagonalu macierzy gęstości stoją prawdopodobieństwa wyników pomiaru wielkości  $A$ , natomiast pozadiagonalne elementy zawierają różnice faz  $\varphi$ .

<sup>8</sup> zakładamy, że wielkość ta ma tylko dwie wartości własne, np. zwrot spinu na wybranym kierunku



Wyniki pomiaru wielkości  $A$  nie dają zatem żadnej informacji o tej różnicy faz (różnicy faz między  $c_1$  i  $c_2$ ) decydującej o koherentnym charakterze superpozycji. Pomiar niszczy tę koherencję, likwidując w nieodwracalny sposób informację zawartą w różnicy faz współczynników superpozycji. Można to zapisać macierzowo:

$$\rho = \begin{pmatrix} x^2 & x\sqrt{1-x^2}e^{-i\varphi} \\ x\sqrt{1-x^2}e^{i\varphi} & 1-x^2 \end{pmatrix} \Rightarrow \rho_0 = \begin{pmatrix} x^2 & 0 \\ 0 & 1-x^2 \end{pmatrix}.$$

Strzałka oznacza tutaj pomiar. W jego rezultacie traci się informację zawartą w niediagonalnych elementach macierzy gęstości. Traci się informację o różnicy faz, tzn. następuje zupełna *dekoherencja fazowa*.

W ogólności macierz gęstości danego układu (niekoniecznie rozpatrywanego wyżej) może zmieniać się pod wpływem oddziaływania z innym układem (wyżej rozpatrujemy wynik oddziaływania z przyrządem pomiarowym), wówczas mogą zmieniać się diagonalne elementy macierzy gęstości (tzn. zachodzić będzie *dekoherencja amplitudowa*), lub niediagonalne (*dekoherencja fazowa*). Pomiar jest w naszym przypadku całkowitą (zmiana do zera) *dekoherencją fazową*.

Zawartość diagonalnych elementów nie ulega zmianie – są to bowiem prawdopodobieństwa wyników pomiaru i dla wielokrotnego powtórzenia tego samego pomiaru na takim samym stanie tę informację można (tj. wielkości tych prawdopodobieństw) uzyskać.

Jeśli teraz przyjrzymy się dokładniej, jak zachodzi znikanie elementów niediagonalnych macierzy gęstości, to poznamy lepiej mechanizm kolapsu funkcji falowej w wyniku pomiaru. Przyrząd pomiarowy  $P$  dokonujący pomiaru wielkości  $A$  na stanie  $|\Psi\rangle = c_1|1\rangle + c_2|2\rangle$ , jest układem makroskopowym (tzn. o liczbie stopni swobody rzędu liczby Avogadro). Jest to konieczny warunek, gdyż wynik pomiaru ma być czytelny dla człowieka (obserwatora), a ten rozumie tylko klasyczną informację. Taka informacja, np. wychylenie jakiejś wskazówki wymaga zmiany położenia ogromnej liczby mikrocząstek (atomów), a zatem zmiany stopni swobody w ilości rzędu liczby Avogadro, tzn.  $10^{23}$  (w najmniejszej nawet wskazówce jest mniej więcej tyle atomów).

Pomiar to wpisywanie w przyrząd  $P$  informacji o ogromnej ilości cząstek o stanie  $|1\rangle$  lub  $|2\rangle$  danego mierzonego układu. Wczytywanie to możliwe jest na skutek oddziaływania układu z przyrządem.

Założmy, że przed pomiarem (gdy przyrząd  $P$  jest oddalony od układu) stan przyrządu opisywała jego funkcja falowa  $|\Phi_0\rangle$  (funkcja ogromnej ilości zmiennych). Nieoddziaływający przyrząd  $P$  i nasz układ  $U$  tworzą razem większy układ, który przed pomiarem jest w stanie czystym,

$$|\Omega_0\rangle = |\Psi\rangle \otimes |\Phi_0\rangle.$$

Macierz gęstości układu  $U$  można wyrazić jako ślad po stanach przyrządu z pełnej macierzy gęstości,



$$\rho = Tr_P(|\Omega_0\rangle\langle\Omega_0|) = \begin{pmatrix} x^2\langle\Phi_0|\Phi_0\rangle & x\sqrt{1-x^2}e^{-i\varphi}\langle\Phi_0|\Phi_0\rangle \\ x\sqrt{1-x^2}e^{i\varphi}\langle\Phi_0|\Phi_0\rangle & (1-x^2)\langle\Phi_0|\Phi_0\rangle \end{pmatrix},$$

gdzie całka  $\langle\Phi_0|\Phi_0\rangle$  zjawiała się w wyniku wzięcia śladu po stanach przyrządu  $P$ . Wobec unormowania  $\langle\Phi_0|\Phi_0\rangle=1$ , czyli rzeczywiście mamy naszą wyjściową macierz gęstości.

Jeśli stan układu  $U$  byłby  $|1\rangle$ , to z całą pewnością otrzymalibyśmy po pomiarze ten sam stan (bo w takim przypadku  $x=1$ ), podobnie gdyby stan  $U$  był  $|2\rangle$ , to po pomiarze stan też pozostałby niezmienny. W pierwszym przypadku stan przyrządu  $P$  po pomiarze byłby  $|\Phi_1\rangle$ , a w drugim przypadku  $|\Phi_2\rangle$ , przy czym obie te funkcje falowe przyrządu muszą być różne w makroskopowy sposób (tzn. różnią się na makroskopowej liczbie zmiennych, rzędu liczby Avogadro) – to w tych funkcjach jest zapisana informacja odpowiednio o stanie  $|1\rangle$  i  $|2\rangle$  układu  $U$ .

Czyli można napisać,

$$\begin{aligned} |1\rangle \otimes |\Phi_0\rangle &\Rightarrow |1\rangle \otimes |\Phi_1\rangle, \\ |2\rangle \otimes |\Phi_0\rangle &\Rightarrow |2\rangle \otimes |\Phi_2\rangle. \end{aligned}$$

Jeśli pomiaru dokonujemy na stanie  $|\Psi\rangle = c_1|1\rangle + c_2|2\rangle$  układu  $U$ , to możemy zapisać,

$$\Omega_0 = (c_1|1\rangle + c_2|2\rangle) \otimes |\Phi_0\rangle \Rightarrow c_1|1\rangle \otimes |\Phi_1\rangle + c_2|2\rangle \otimes |\Phi_2\rangle = \Omega_1$$

(strzałka oznacza pomiar, po pomiarze znowu przyrząd znajduje się dalej od układu, ale ma już zapisaną w sobie informację). Widać, że przed pomiarem zarówno przyrząd jak i układ były w swoich stanach czystych. Po pomiarze nie są one w stanach czystych, chociaż razem tworzą stan czysty  $|\Omega_1\rangle$  całego układu  $U+P$ .

W tym stanie układ  $U$  jest trochę w stanie  $|1\rangle$ , a trochę w stanie  $|2\rangle$ , natomiast przyrząd jest trochę w stanie  $|\Phi_1\rangle$ , a trochę w stanie  $|\Phi_2\rangle$ . Jest to nieseparowalny element iloczynu tensorowego, inaczej mówiąc stan splątany układu i przyrządu.

Łatwo jednak napisać macierz gęstości całego układu  $U+P$ , tj.  $|\Omega_1\rangle\langle\Omega_1|$ , i biorąc ślad po stanach przyrządu określić można postać macierzy gęstości dla układu po pomiarze, tj.,

$$Tr_P|\Omega_1\rangle\langle\Omega_1| = \begin{pmatrix} x^2\langle\Phi_1|\Phi_1\rangle & x\sqrt{1-x^2}e^{-i\varphi}\langle\Phi_2|\Phi_1\rangle \\ x\sqrt{1-x^2}e^{i\varphi}\langle\Phi_1|\Phi_2\rangle & (1-x^2)\langle\Phi_2|\Phi_2\rangle \end{pmatrix}.$$



Funkcje  $|\Phi_1\rangle$  i  $|\Phi_2\rangle$  są unormowane, zatem  $\langle\Phi_i|\Phi_i\rangle=1$ . Natomiast o całce  $\langle\Phi_1|\Phi_2\rangle$  możemy wnioskować tylko na podstawie różnicy między obiema funkcjami na makroskopowej liczbie stopni swobody. W. Żurek argumentował w swojej słynnej pracy o *superwyborze*, że całka ta jest całką wielokrotną o krotności rzędu liczby Avogadro i w podobnej ilości przypadków dotyczy różnej zależności funkcyjnej obu funkcji. Jeśli w tych różnych przypadkach każda całka daje tylko nieznacznie mniejszą od 1 wartość, to cała całka jest równa 0, wobec przemnożenia przez siebie ogromnej liczby nawet niewiele mniejszych od jedności czynników.

W ten sposób znikają niediagonalne elementy macierzy gęstości i w istocie otrzymujemy macierz gęstości po pomiarze zgodnie ze schematem von Neumanna, czyli,

$$\hat{\rho}_0 = \begin{pmatrix} x^2 & 0 \\ 0 & 1-x^2 \end{pmatrix}.$$

Warto dodać, że ten opis pomiaru pozwala na prześledzenie go zgodnie z zasadami dynamiki kwantowej – funkcja stanu całego układu  $U + P$  przechodzi bowiem swoją unitarną ewolucję (z całym Hamiltonianem zależnym wprawdzie od czasu, gdyż obserwator przysuwa, a następnie odsuwa przyrząd, czyli włącza i wyłącza oddziaływanie  $U$  i  $P$ ) od stanu  $|\Omega_0\rangle$  do stanu  $|\Omega_1\rangle$ . To wyjaśnia w pewnym stopniu pozornie sztuczny i dodatkowy w stosunku do unitarnej dynamiki charakter *ansatzu von Neumanna*.

Znikanie elementów pozadiagonalnych w macierzy gęstości zachodzi w rzeczywistości w ciągu skończonego czasu związanego z dynamiką pomiaru, tzn. z zależnym od czasu oddziaływaniem między układem i przyrządem, pozwalającym na dopłytywanie do układu coraz to nowych stopni swobody przyrządu, aż ich liczba osiągnie makroskopową wielkość (pozwalającą na makroskopowe odróżnienie wpisanych w przyrząd informacji o mierzonym układzie). Proces ten zachodzi jednak bardzo szybko (w szczególności, np. dla stanów koherentnych oscylatora, może być opisany czynnikiem czasowym typu  $e^{-x(\lambda_2-\lambda_1)^2 t}$ ).

#### 4. Macierz gęstości

Jeśli układ A jest w stanie czystym  $|\Psi\rangle \in H$ , to można wprowadzić operator rzutowania na ten stan i nazwać go macierzą gęstości:

$$\hat{\rho} = |\Psi\rangle\langle\Psi|.$$

Dla dowolnej obserwabli  $M$  w układzie A mamy wtedy:



$$\langle \widehat{M} \rangle = \langle \Psi | \widehat{M} | \Psi \rangle = \text{Tr}(\widehat{M} \widehat{\rho}).$$

Rzeczywiście,  $\text{Tr}$  oznacza wzięcie śladu z operatora w jego macierzowej postaci (nie zależy on od wyboru bazy) i przy danej bazie ON (ortonormalnej) w  $H$  np.  $\{|i\rangle\}$ , mamy

$$\text{Tr}(\widehat{A}) = \sum_i \langle i | \widehat{A} | i \rangle.$$

Dla  $\widehat{A} = \widehat{M} \widehat{\rho}$  mamy zatem <sup>9</sup>

$$\text{Tr}(\widehat{M} \widehat{\rho}) = \sum_i \langle i | \widehat{M} \widehat{\rho} | i \rangle = \sum_i \langle i | \widehat{M} | \Psi \rangle \langle \Psi | i \rangle = \sum_i \langle \Psi | i \rangle \langle i | \widehat{M} | \Psi \rangle = \langle \Psi | \widehat{M} | \Psi \rangle.$$

Zapisy stanu czystego w postaci operatora rzutu na ten stan, czyli w postaci macierzy gęstości, i w postaci funkcji falowej, są zatem w pełni ekwiwalentne (dają te same średnie dla dowolnych obserwabli).

Macierz gęstości można jednak wprowadzić ogólniej, tzn. nie tylko dla stanów czystych układu A, wtedy nie będzie ona operatorem rzutu na jakiś stan (bo układ A nie jest wtedy w określonym stanie czystym).

Taką sytuację mamy gdy układ A oddziałuje z układem B i razem tworzą zamknięty układ A+B, który jako całość jest już w stanie czystym,

$$|\Psi\rangle_{AB} \in H_A \otimes H_B.$$

Wspólna macierz gęstości układu A+B dla tego stanu jest równa:

$$\rho_{AB} = |\Psi\rangle_{AB} \langle \Psi|_{AB}.$$

W przestrzeniach Hilberta  $H_A$ ,  $H_B$  wybieramy bazy ON  $\{|i\rangle_A\}$ ,  $\{|r\rangle_B\}$ ,

Wtedy  $|\Psi\rangle_{AB} = \sum_{i,r} a_{ir} |i\rangle_A \otimes |r\rangle_B$ , zgodnie z definicją iloczynu tensorowego obu przestrzeni<sup>10</sup>.

Jasne, że  $\sum_{i,r} |a_{ir}|^2 = 1$ , gdyż funkcja  $|\Psi\rangle_{AB} \in H_A \otimes H_B$  jest unormowana.

<sup>9</sup> Tę równość można sprawdzić rozpisując w bazie  $\{|i\rangle\}$  macierz gęstości,  $\widehat{\rho} = |\Psi\rangle \langle \Psi| = \sum_{i,j} c_i c_j^* |i\rangle \langle j|$ .

Wtedy:  $\text{Tr}(\widehat{M} \widehat{\rho}) = \sum_i \langle i | \widehat{M} \widehat{\rho} | i \rangle = \sum_i \langle i | \widehat{M} | \Psi \rangle \langle \Psi | i \rangle = \sum_{i,j,k} c_j c_k^* \langle i | \widehat{M} | j \rangle \langle k | i \rangle = \sum_{i,j} c_j c_i^* \langle i | \widehat{M} | j \rangle$

ale także  $\langle \Psi | \widehat{M} | \Psi \rangle = \sum_{i,j} c_j c_i^* \langle i | \widehat{M} | j \rangle$ .

<sup>10</sup> Jeśli tworzymy iloczyn tensorowy dwóch przestrzeni Hilberta  $H_A \otimes H_B$ , to bazą tej przestrzeni jest





Jeśli z macierzy gęstości dla pełnego układu A+B (będącego w stanie czystym) wziąć teraz ślad po układzie B, to otrzymamy macierz gęstości dla układu A oddziałującego z B (i przez to nie będącego w stanie czystym). Mianowicie<sup>11</sup>:

$$\hat{\rho}_A = Tr_B \hat{\rho}_{AB} = \sum_r \langle r | \hat{\rho}_{AB} | r \rangle_B = \sum_{r,i,j,p,s} a_{i,p} a_{j,s}^* \langle r | p \rangle_B \langle s | r \rangle_B | i \rangle_A \langle j | = \sum_{i,j,r} a_{i,r} a_{j,r}^* | i \rangle_A \langle j |.$$

Mamy zatem dwie sytuacje odnośnie macierzy gęstości stanu A. Dla stanu czystego układu A

$$\hat{\rho}_A = |\Psi\rangle_{AA} \langle \Psi| = \sum_{i,j} c_i c_j^* | i \rangle_{AA} \langle j |$$

i dla stanu układu A będącego częścią złożonego układu A+B (nie jest to stan czysty układu A)

$$\hat{\rho}_A = Tr_B \hat{\rho}_{AB} = \sum_{i,j,r} a_{i,r} a_{j,r}^* | i \rangle_{AA} \langle j |.$$

Różnica polega tu na dodatkowym indeksie  $r$  i sumowaniu po nim w przypadku stanu układu będącego częścią układu A+B. W pierwszym przypadku macierz gęstości jest operatorem rzutowania, w drugim nie.

W obu przypadkach macierz gęstości posiada jednak trzy własności:

- jest operatorem hermitowskim,
- jest operatorem dodatnio określonym,
- ślad macierzy gęstości jest równy 1.

Te ogólne własności dowolnej macierzy gęstości można sprawdzić w obu wymienionych wyżej przypadkach. W obydwu mamy  $\hat{\rho}_A^+ = \hat{\rho}_A$  bezpośrednio z powyższych wyrażeń (np. w drugim przypadku

$$\hat{\rho}_A^+ = \sum_{i,j,r} a_{i,r}^* a_{j,r} | j \rangle_{AA} \langle i | = \hat{\rho}_A, \text{ co dowodzi hermitowskości macierzy gęstości.}$$

Druga własność oznacza że  $\forall_{|\Psi\rangle_A} \langle \Psi | \hat{\rho}_A | \Psi \rangle_A \geq 0$ , wynika to z faktu, że

zbiór  $|i\rangle_A \otimes |r\rangle_B$ . Gdy wymiary obu przestrzeni są skończone  $n$  i  $m$ , to wymiar ich iloczynu tensorowego jest  $nm$ .

<sup>11</sup> w zapisie tensorowym można zmieniać kolejność czynników, tzn.,  $|i\rangle_A \otimes |r\rangle_B$  można utożsamić z

$|r\rangle_B \otimes |i\rangle_A$ , tak jak przy zwykłym mnożeniu



$${}_A \langle \Psi | \hat{\rho}_A | \Psi \rangle_A = {}_A \langle \Psi | \left( \sum_{i,j,r} a_{i,r} a_{j,r}^* |i\rangle_A \langle j| \right) | \Psi \rangle_A = \sum_r \left| \sum_i a_{i,r} \langle \Psi | i \rangle_A \right|^2 \geq 0.$$

Ostatnią własność można bezpośrednio sprawdzić w obu powyższych przypadkach, np. w drugim:

$$Tr_A \hat{\rho}_A = \sum_k {}_A \langle k | \left( \sum_{i,j,r} a_{i,r} a_{j,r}^* |i\rangle_A \langle j| \right) | k \rangle_A = \sum_{k,r} |a_{k,r}|^2 = 1, \quad \text{z unormowania funkcji } |\Psi\rangle_{AB} \in H_A \otimes H_B \text{ (lub funkcji } |\Psi\rangle_A \in H_A, \text{ w pierwszym przypadku).}$$

Z powyższych trzech własności macierzy gęstości wynika, że operator ten można zdiagnozować przez odpowiedni wybór bazy w przestrzeni Hilberta  $H_A$  (wynika to z hermitowskości macierzy gęstości), przy czym wartości własne tego operatora są rzeczywiste (jak każdego operatora hermitowskiego), oraz nieujemne (co wynika z drugiej własności). Ślad tego operatora jest zawsze 1 i nie zależy to od reprezentacji (tj. od wyboru bazy), więc suma wartości własnych (stoją one na diagonalu w reprezentacji diagonalnej) jest równa 1. Czyli istnieje taka baza w  $H_A$   $\{|\Phi_i\rangle_A\}$ , że

$$\hat{\rho}_A = \sum_i p_i |\Phi_i\rangle_A \langle \Phi_i|,$$

gdzie  $0 \leq p_i \leq 1$ , oraz  $\sum_i p_i = 1$  (są tymi wartościami własnymi).

W przypadku stanu czystego  $\hat{\rho}_A = |\Psi\rangle_A \langle \Psi|$ , jest tylko jedna wartość własna różna od zera, równa 1, i wtedy macierz gęstości jest operatorem rzutowania na ten stan czysty układu A. W ogólnym przypadku, zgodnie z powyższą formułą macierz gęstości jest sumą (liniową kombinacją o dodatnich współczynnikach) operatorów rzutowania na ortogonalne wektory własne (taka suma nie jest już operatorem rzutowania<sup>12</sup>).

W tym ogólnym przypadku, gdy macierz gęstości nie jest operatorem rzutowania, tzn. gdy układ A nie jest w stanie czystym, mówimy, że jest on w stanie mieszanym (z prawdopodobieństwem  $p_i$  jest on w stanie  $|\Phi_i\rangle_A$ ). Chociaż sam układ A nie jest w stanie czystym (a w stanie mieszanym), cały układ A+B jest w stanie czystym. Mieszanie wynika z oddziaływania układów A i B i oznacza ich kwantową korelację, którą nazywamy kwantowym splątaniem.

<sup>12</sup> operator rzutowania spełnia warunek  $\hat{P}^2 = \hat{P}$ , a stąd  $Tr(\hat{P}^2) = Tr(\hat{P})$ ; dla macierzy gęstości w ogólnej

postaci  $\hat{\rho}_A = \sum_i p_i |\Phi_i\rangle_A \langle \Phi_i|$  ten warunek nie jest spełniony, gdyż

$$Tr(\hat{\rho}^2) = \sum_i p_i^2 < 1 = Tr(\hat{\rho}), \text{ czyli dla macierzy gęstości dla stanu mieszanego } \hat{\rho}^2 \neq \hat{\rho}.$$



Warto zauważyć, że dla macierzy gęstości układu A w stanie mieszanym,

$$\hat{\rho}_A = Tr_B \hat{\rho}_{AB} = \sum_{i,j,r} a_{i,r} a_{j,r}^* |i\rangle_A \langle j|,$$

dla dowolnego operatora obserwabli M w układzie A, której operator jest równy  $\hat{M}_A$  mamy równość  $\langle \hat{M}_A \rangle_{AB} = \langle \Psi | \hat{M}_A \otimes \hat{1}_B | \Psi \rangle_{AB} = Tr_A (\hat{M}_A \hat{\rho}_A)$ , co uzasadnia sensowność wprowadzenia macierzy gęstości dla stanu mieszanego (w analogii do macierzy gęstości dla stanu czystego).

## 5. Reprezentacja Schmidta i liczba Schmidta, stany splątane

Na podstawie trzech wyżej wymienionych własności każdej macierzy gęstości możemy zawsze założyć, że w przypadku stanu mieszanego dla układu A będącego częścią układu A+B, możemy wybrać bazę w przestrzeni Hilberta  $H_A$  taką, w której macierz gęstości układu A jest diagonalna, tj.,

$$\hat{\rho}_A = \sum_i p_i |i\rangle_A \langle i|.$$

Możemy teraz zapisać także funkcję falową stanu czystego układu A+B, używając tej bazy w przestrzeni Hilberta układu A, tj.,

$$|\Psi\rangle_{AB} = \sum_{i,r} a_{i,r} |i\rangle_A \otimes |r\rangle_B = \sum_i |i\rangle_A \otimes \left( \sum_r a_{i,r} |r\rangle_B \right) = \sum_i |i\rangle_A \otimes |\tilde{i}\rangle_B,$$

gdzie  $|\tilde{i}\rangle_B = \sum_r a_{i,r} |r\rangle_B$ . Wektory te nie są bazą w  $H_B$ , w przeciwieństwie do  $\{|r\rangle_B\}$ .

Okazuje się jednak, że wektory  $\{|\tilde{i}\rangle_B\}$  są ortogonalne (ale nie unormowane).

W reprezentacji diagonalnej w  $H_A$  mamy bowiem:

$$\hat{\rho}_A = \sum_i p_i |i\rangle_A \langle i| = Tr_B \left( |\Psi\rangle_{AB} \langle \Psi| \right) = \sum_r \langle r| \left( \sum_{i,j} |i\rangle_A \otimes |\tilde{i}\rangle_B \langle \tilde{j}| \otimes \langle i| \right) |r\rangle_B$$

czyli

$$\hat{\rho}_A = \sum_{i,j} \langle \tilde{j} | \tilde{i} \rangle_B |i\rangle_A \langle j|.$$



Z porównania obu powyższych wierszy wynika, że  ${}_B \langle \tilde{j} | \tilde{i} \rangle_B = p_i \delta_{i,j}$ , co dowodzi ortogonalności wektorów  $\{|\tilde{i}\rangle_B\}$ . Można je unormować i w ten sposób wprowadzić bazę ON w  $H_B$  w postaci wektorów,

$$|\tilde{i}\rangle_B = \sqrt{p_i} |i'\rangle_B,$$

tylko dla niezerowych  $p_i$ .

W tej bazie można zapisać funkcję falową stanu czystego układu A+B w postaci

$$|\Psi\rangle_{AB} = \sum_i \sqrt{p_i} |i\rangle_A \otimes |i'\rangle_B,$$

przy czym obie bazy w przestrzeniach dla układu A i B, tj. w  $H_A$  i w  $H_B$  są ON. Są one jednak wybrane dla konkretnego stanu całego układu i np. dla dwóch różnych stanów czystych układu A+B nie istnieje z reguły wspólne przedstawienie jak wyżej (dla każdego z osobna istnieje, ale w różnych bazach). Powyższe przedstawienie stanu czystego układu złożonego z dwóch podukładów nazywamy reprezentacją Schmidta.

Korzystając z tej reprezentacji mamy macierz gęstości dla stanu mieszanego układu A w postaci diagonalnej,

$$\hat{\rho}_A = Tr_B (|\Psi\rangle_{AB} \langle\Psi|) = \sum_i p_i |i\rangle_A \langle i|,$$

ale także i diagonalną postać macierzy gęstości dla układu B, tzn.,

$$\hat{\rho}_B = Tr_A (|\Psi\rangle_{AB} \langle\Psi|) = \sum_i p_i |i'\rangle_B \langle i'|.$$

W tej reprezentacji (przy takim wyborze baz w obu przestrzeniach, jak w reprezentacji Schmidta) obie macierze gęstości są zatem diagonalne i co istotne mają takie same wartości własne (jest ich tyle samo, chociaż wymiary  $H_A$  i  $H_B$  mogą być różne, wtedy obie macierze gęstości różnią się stopniem degeneracji wartości własnej równej zero).

Dalszy wniosek z powyższej reprezentacji jest taki, że obie macierze gęstości  $\hat{\rho}_A$  i  $\hat{\rho}_B$  jednoznacznie wyznaczają funkcje  $|\Psi\rangle_{AB}$ , pod warunkiem, że nie ma zdegenerowanych, innych niż zero, wartości własnych. Wystarczy bowiem zdiagnozować obie macierze gęstości  $\hat{\rho}_A$  i  $\hat{\rho}_B$  i wektory własne odpowiadające tym samym wartościom własnym zestawić w postaci  $|\Psi\rangle_{AB} = \sum_i \sqrt{p_i} |i\rangle_A \otimes |i'\rangle_B$ . Jeśli któraś z niezerowych wartości własnych jest zdegenerowana, to nie ma już jednoznaczności, bo można rozmaicie zestawić funkcje z odpowiednich podprzestrzeni własnych.



Można dodać jeszcze uwagę, że przy zestawianiu reprezentacji Schmidta nie ma dowolności przyjmowania faz funkcji z obu baz (za wyjątkiem możliwych przeciwnych lub zerowych dla par odpowiadających tej samej wartości własnej, co wynika z zapisu reprezentacji Schmidta).

Liczbę niezerowych (wspólnych) wartości własnych macierzy gęstości  $\hat{\rho}_A$  i  $\hat{\rho}_B$  nazywamy liczbą Schmidta. Jeśli liczba Schmidta jest większa od 1 to stan  $|\Psi\rangle_{AB}$  nazywamy stanem splątany (wobec jednakowych wartości własnych obu układów możemy powiedzieć, że oba układy są splątane ze sobą w takim samym stopniu). W przeciwnym przypadku jest to stan niesplątany, czyli separowalny (tzn. można go przedstawić w postaci iloczynu tensorowego dwóch stanów czystych obu układów).

Liczby Schmidta nie można zwiększyć przez lokalne operacje tylko na jednym z układów. Splątanie (czyli stan mieszany) obu układów powstaje wyłącznie na skutek oddziaływania obu podukładów. Liczbę Schmidta można jednak zmniejszyć przez operacje lokalne na jednym z podukładów.

Splątanie kwantowe jest zatem zjawiskiem nielokalnym i typowo kwantowym (nie ma klasycznego odpowiednika – jest związane z algebrą przestrzeni Hilberta).

## 6. Geometryczne własności macierzy gęstości

Macierz gęstości ma następujące własności

- $\hat{\rho}^\dagger = \hat{\rho}$  (hermitowski operator),
- $\forall |\Psi\rangle_A, \quad \langle \Psi | \hat{\rho} | \Psi \rangle_A \geq 0$  (nieujemność),
- $\text{tr}_A \hat{\rho} = 1$ .

Jeśli operator liniowy spełnia te własności, to jest on macierzą gęstości dla układu A.

W skończonej wielo-wymiarowej przestrzeni Hilberta, np.  $n$ -wymiarowej, operatory liniowe przedstawić można jako macierze  $n \times n$  o stałych wyrazach (zespolonych). Zbiór macierzy gęstości jest wtedy podzbiorem zespolonych macierzy  $n \times n$ .

Jeśli  $\hat{\rho}_1$  i  $\hat{\rho}_2$  są macierzami gęstości to wypukła kombinacja liniowa,<sup>13</sup>

$$\hat{\rho} = \lambda \hat{\rho}_1 + (1 - \lambda) \hat{\rho}_2, \quad 0 \leq \lambda \leq 1, \lambda \in R,$$

<sup>13</sup> linowa wypukła kombinacja dwóch punktów w przestrzeni liniowej jest punktem z odcinka łączącego te dwa punkty



jest też macierzą gęstości. Rzeczywiście, przez bezpośrednie sprawdzenie przekonać się można, że taka kombinacja spełnia wyżej wymienione własności macierzy gęstości. Oznacza to, że zbiór macierzy gęstości jest zbiorem wypukłym w zbiorze wszystkich operatorów liniowych (zawiera wszystkie punkty odcinków łączących dowolne dwa punkty tego zbioru).

Można zatem zapytać, czym różnią się macierze gęstości z wnętrza zbioru (wypukłego) wszystkich macierzy gęstości danego układu od macierzy gęstości z brzegu tego zbioru. Łatwo zauważyć, że na brzegu zbioru macierzy gęstości (w przypadku  $n$  wymiarowej przestrzeni Hilberta) leżą takie macierze gęstości, które mają co najmniej jedną zerową wartość własną (są one na granicy między dodatnimi i ujemnymi wartościami własnymi i wobec własności nieujemności macierzy gęstości, leżą one na granicy zbioru macierzy gęstości). W szczególnym przypadku, gdy wszystkie (za wyjątkiem jednej<sup>14</sup>) wartości własne macierzy gęstości są równe zero – wtedy macierz gęstości odpowiada operatorowi rzutowania na jeden stan, czyli jest macierzą gęstości stanu czystego, również taka macierz leży na brzegu zbioru macierzy gęstości i dodatkowo jest jego punktem ekstremalnym<sup>15</sup>. Oznacza to, że stan czysty (jego macierz gęstości) nie może być przedstawiona jako wypukła kombinacja innych macierzy gęstości; rzeczywiście, gdyby

$$\hat{\rho} = |\Psi\rangle\langle\Psi| = \lambda\hat{\rho}_1 + (1-\lambda)\hat{\rho}_2, \quad \text{to dla dowolnego stanu } \langle\Phi|, \text{ ortogonalnego do } \langle\Psi| \text{ mamy}$$

$$\langle\Phi|\hat{\rho}|\Phi\rangle = 0 = \lambda\langle\Phi|\hat{\rho}_1|\Phi\rangle + (1-\lambda)\langle\Phi|\hat{\rho}_2|\Phi\rangle, \quad \text{i wobec nieujemności wszystkich macierzy gęstości mamy } \langle\Phi|\hat{\rho}_i|\Phi\rangle = 0, \quad i = 1, 2, \text{ a wobec dowolności } \langle\Phi|, \text{ otrzymujemy } \hat{\rho}_1 = \hat{\rho}_2 = \hat{\rho}.$$

Stany czyste są więc ekstremalne i odwrotnie stany ekstremalne są stanami czystymi. W przypadku dwuwymiarowej przestrzeni Hilberta (jak dla qubitu) wszystkie stany brzegowe są ekstremalne (bo tylko jedna wartość własna może być zero w tym przypadku), co nie jest jednak prawdą w więcej wymiarowych przypadkach. Stany mieszane nie są z pewnością punktami ekstremalnymi, bo ich przedstawienie w postaci diagonalnej jest przykładem rozkładu wypukłego na inne macierze gęstości. Stany mieszane mogą być zatem punktami wewnętrznymi wypukłego zbioru wszystkich macierzy gęstości danego układu lub punktami brzegowymi, ale nie ekstremalnymi (w przypadku więcej niż dwuwymiarowym).

Dla stanu mieszanego macierz gęstości może być zatem przedstawiona jako wypukła kombinacja dwóch innych macierzy gęstości (w szczególności stanów czystych – punktów ekstremalnych). Przedstawienie to nie jest jednoznaczne. Każde takie przedstawienie można traktować jako różne przygotowanie macierzy gęstości – jest ono jednak nierozpoznawalne przy pomocy pomiarów, ponieważ niezależnie od sposobu przygotowania danej macierzy gęstości mamy dla dowolnej obserwabli  $M$ :

$$\langle\hat{M}\rangle = \text{tr}_A(\hat{\rho}\hat{M}) = \lambda\text{tr}_A(\hat{\rho}_1\hat{M}) + (1-\lambda)\text{tr}_A(\hat{\rho}_2\hat{M})$$

<sup>14</sup> wtedy ta jedna wartość własna musi być 1, wobec własności śladu macierzy gęstości

<sup>15</sup> punkt ekstremalny zbioru wypukłego to taki punkt jego brzegu, który nie może być przedstawiony jako wypukła kombinacja innych punktów tego zbioru; przykładem punktów ekstremalnych są wierzchołki wielościanów wypukłych, lub punkty z powierzchni kuli



i wynik nie zależy od wypukłego przedstawienia. Dla stanów mieszanych mamy zatem wiele możliwych przygotowań macierzy gęstości (nieskończenie wiele), których jednak nie możemy zidentyfikować pomiarami. Stan czysty, jako punkt ekstremalny, nie dopuszcza żadnych różnych przygotowań tego stanu. Ta ukryta niejednoznaczność (nieostępna pomiarami) dla stanów mieszanych jest kolejną istotną cechą kwantowej informacji zawartej w stanach mieszanych danego układu i nie posiadającą klasycznego odpowiednika<sup>16</sup>.

## 7. Zbiór wypukły macierzy gęstości qubitu (sfera Blocha)

Najprostszym układem kwantowym jest qubit, dla którego przestrzeń Hilberta jest dwuwymiarowa. Operatory liniowe są więc zespolonymi macierzami  $2 \times 2$  (w ogólnym przypadku zadanymi przez 8 rzeczywistych parametrów).

Nałożenie warunku hermitowskości operatora powoduje ograniczenie rzeczywistych parametrów takiej macierzy do czterech<sup>17</sup>. Można zatem wybrać cztery niezależne liniowo macierze hermitowskie i dowolna macierz hermitowska  $2 \times 2$ , będzie liniową kombinacją tych czterech. Wygodnie wybrać jest cztery macierze hermitowskie:

$$\hat{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

trzy ostatnie macierze to macierze Pauliego – składowe wektora, który jest operatorem spinu  $\hat{\vec{\sigma}} = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)$ . Te macierze są liniowo niezależne, gdyż wyznacznik transformacji

macierzy  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$  w wyżej wymienione macierze jest różny od zera.

Macierze Pauliego są bezśladowe, więc hermitowska macierz ze śladem jeden (jak dla macierzy gęstości) musi mieć postać:

$$\hat{\rho} = \frac{1}{2}(\hat{1} + \vec{P} \cdot \hat{\vec{\sigma}}) = \frac{1}{2} \begin{pmatrix} 1 + P_z & P_x - iP_y \\ P_x + iP_y & 1 - P_z \end{pmatrix},$$

<sup>16</sup> Klasyczny bit probabilistyczny może być przygotowany tylko w jeden sposób (0 z prawdopodobieństwem p i 1 z prawdopodobieństwem 1-p). Podobnie rozkład prawdopodobieństwa n elementowy jest także jednoznaczny tj., dopuszcza tylko jedno przedstawienie przy pomocy prawdopodobieństw poszczególnych elementów rozkładu – jest to też wypukła kombinacja liniowa stanów pojedynczych elementów. Takie jednoznaczne przedstawienia przy pomocy określonych stanów tworzą również bryłę wypukłą – *sympleks*, którego wierzchołkami są te stany. W świetle tej uwagi, zbiór wypukły macierzy gęstości nie może być *sympleksem*.

<sup>17</sup> Hermitowskie sprzężenie dla macierzy oznacza transponowanie i zespolone sprzężenie, więc hermitowskość oznacza równość:

$$\begin{pmatrix} a + ib & c + id \\ e + if & g + ih \end{pmatrix} = \begin{pmatrix} a - ib & e - if \\ c - id & g - ih \end{pmatrix}, \text{ czyli } b = h = 0, e = c, f = -d; \text{ pozostają zatem tylko cztery}$$

niezależne parametry rzeczywiste



gdzie  $\vec{P} = (P_x, P_y, P_z)$  jest rzeczywistym wektorem.

Warunek nieujemności macierzy gęstości narzuca dodatkowe ograniczenie. W przypadku macierzy  $2 \times 2$ , sytuacja jest prosta, gdyż warunek nieujemności macierzy gęstości (równoważny z nieujemnością jej wartości własnych), w przypadku tylko dwóch wartości własnych  $\lambda_1, \lambda_2$ , sprowadza się do warunku  $\lambda_1 \lambda_2 \geq 0$  (gdyż równocześnie dla macierzy gęstości  $\text{tr}_A \hat{\rho} = \lambda_1 + \lambda_2 = 1$ ). Iloczyn wartości własnych macierzy równy jest jej wyznacznikowi. Wobec przedstawienia macierzy gęstości jak wyżej, mamy  $\det \hat{\rho} = \frac{1}{4}(1 - P^2)$ , czyli warunek  $\det \hat{\rho} \geq 0 \Leftrightarrow 0 \leq P^2 \leq 1$ . Oznacza to, że zbiór macierzy gęstości qubitów jest izomorficzny z kulą jednostkową (w tym kontekście jest ona nazywana kulą Blocha).

Zgodnie z ogólnymi własnościami zbiorów (wypukłych) macierzy gęstości, wewnątrz sfery (kuli) Blocha stanowią stany mieszane, natomiast powierzchnia tej kuli (sfera) to stany czyste.

Jeśli rozważyć dowolny punkt z powierzchni kuli Blocha, to odpowiada on wektorowi  $\vec{P}_{pow} = (\sin \Theta \cos \varphi, \sin \Theta \sin \varphi, \cos \Theta)$  we współrzędnych sferycznych ( $\Theta \in [0, \pi]$ ,  $\varphi \in [0, 2\pi]$ ). Wtedy macierz gęstości,

$$\hat{\rho} = \frac{1}{2}(\hat{1} + \vec{P}_{pow} \cdot \vec{\hat{\sigma}}) = \frac{1}{2} \begin{pmatrix} 1 + \cos \Theta & \sin \Theta e^{-i\varphi} \\ \sin \Theta e^{i\varphi} & 1 - \cos \Theta \end{pmatrix} = |\Psi\rangle\langle\Psi|,$$

gdzie stan czysty qubitów<sup>18</sup> (co można sprawdzić bezpośrednim prostym rachunkiem<sup>19</sup>),

$$|\Psi\rangle = \cos \frac{\Theta}{2} e^{-i\varphi/2} |1\rangle + \sin \frac{\Theta}{2} e^{i\varphi/2} |2\rangle.$$

Stany czyste odpowiadają więc powierzchni kuli Blocha i zgodnie z ogólnymi własnościami wypukłych zbiorów macierzy gęstości są punktami ekstremalnymi (dla kuli punkty ekstremalne leżą na sferze). Punkty wewnętrzne kuli Blocha odpowiadają macierzom gęstości dla stanów mieszanych qubitów i mogą być one przedstawione (w przeciwieństwie do punktów ekstremalnych) jako wypukłe kombinacje innych punktów kuli (na nieskończenie wiele sposobów). W szczególności mogą być przedstawione (też na nieskończenie wiele sposobów) jako wypukłe kombinacje pary punktów ekstremalnych – końców cięciwy kuli przechodzącej przez dany punkt wewnętrzny. Punkt środkowy kuli odpowiada wektorowi  $\vec{P}_0 = 0$ , i wtedy macierz gęstości,

<sup>18</sup> stan ten jest określony z dokładnością do czynnika fazowego  $e^{i\alpha}$

<sup>19</sup> stan ten otrzymuje się bezpośrednio w wyniku diagonalizacji macierzy  $\hat{\rho}$ , jest on wektorem własnym tej macierzy dla wartości własnej 1





$$\hat{\rho} = \frac{1}{2} \hat{1}.$$

Ta macierz gęstości również może być przedstawiona na nieskończenie wiele sposobów jako wypukła kombinacja punktów ekstremalnych (macierzy gęstości stanów czystych), wyznaczonych przez końce dowolnej średnicy kuli. W tym przypadku mamy zawsze jednakowy udział obu tych stanów czystych – mówimy wtedy o maksymalnym zmieszaniu stanów<sup>20</sup>. Końce średnicy wyznaczają parę stanów czystych, które po zmieszaniu w proporcjach  $\frac{1}{2}$  tworzą maksymalnie zmieszany stan mieszany (można to zrobić, czyli przygotować, na nieskończenie wiele sposobów). Stany na przeciwnych końcach średnicy kuli mają  $\tilde{\Theta} = \pi - \Theta$  i  $\tilde{\varphi} = \varphi + \pi$ , można je zatem zapisać jako:

$$|\Psi\rangle = \cos \frac{\Theta}{2} e^{-i\varphi/2} |1\rangle + \sin \frac{\Theta}{2} e^{i\varphi/2} |2\rangle, \quad |\tilde{\Psi}\rangle = \cos \frac{\pi - \Theta}{2} e^{-i(\varphi + \pi)/2} |1\rangle - \sin \frac{\pi - \Theta}{2} e^{i(\varphi + \pi)/2} |2\rangle.$$

Przez bezpośrednie sprawdzenie łatwo się przekonać, że stany  $|\Psi\rangle$  i  $|\tilde{\Psi}\rangle$  są ortogonalne.

Jeśli np.  $|\Psi\rangle = |1\rangle \equiv |\uparrow\rangle_z$  (czyli  $\Theta = 0$ ,  $\varphi = 0$ ), to  $|\tilde{\Psi}\rangle = -i|2\rangle = |\downarrow\rangle_z$  i wtedy,

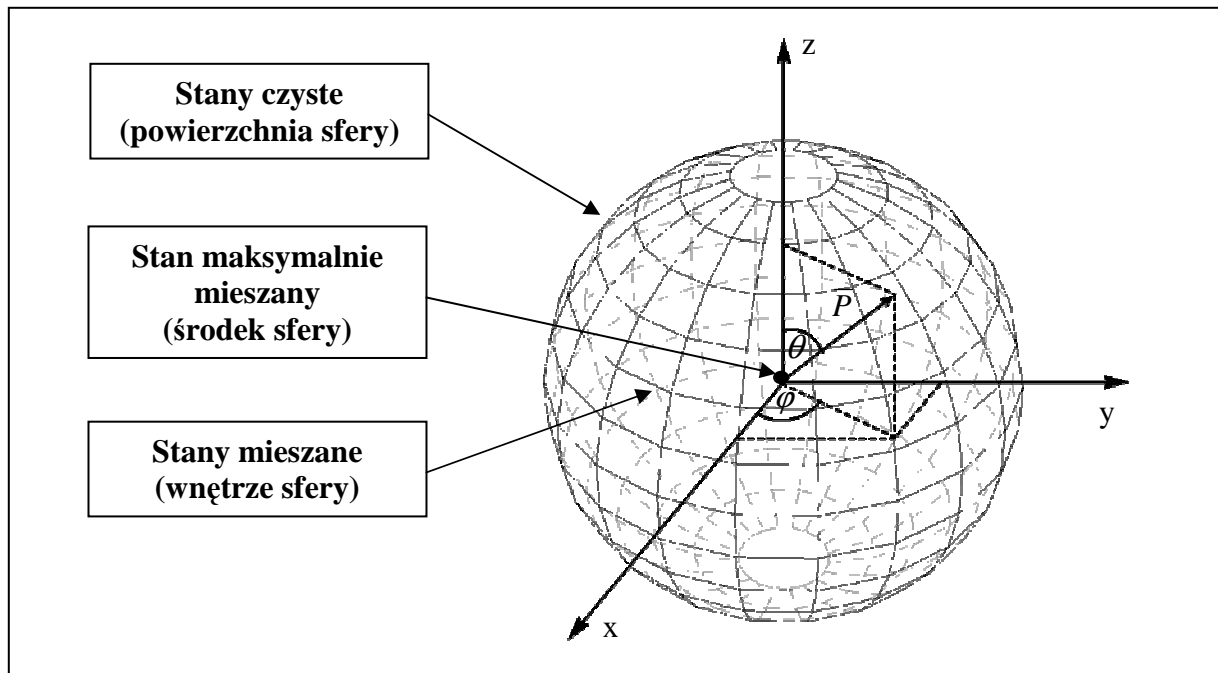
$$\hat{\rho} = \frac{1}{2} \hat{1} = \frac{1}{2} |\uparrow\rangle_z \langle\uparrow| + \frac{1}{2} |\downarrow\rangle_z \langle\downarrow| = \frac{1}{2} |1\rangle\langle 1| - \frac{1}{2} |2\rangle\langle 2|.$$

Dla stanów maksymalnie zmieszanych (w przypadku qubitu – ze środka kuli Blocha) można wybrać rozmaite pary wzajemnie ortogonalnych stanów czystych (na nieskończenie wiele sposobów – w przypadku qubitu będą to stany wyznaczone przez końce rozmaitych średnic kuli Blocha), których maksymalne zmieszanie (tj. zmieszanie w równych proporcjach – w przypadku qubitu w proporcji  $\frac{1}{2}$ ) da ten stan maksymalnie zmieszany (w przypadku qubitu  $\frac{1}{2} \hat{1}$ )<sup>21</sup>. Dla innych stanów mieszanych (nie maksymalnie zmieszanych) jest tylko jedna para (w przypadku qubitu) wzajemnie ortogonalnych stanów czystych, których zmieszanie w nierównych proporcjach daje ten stan mieszany (są to stany na końcach średnicy przechodzącej przez punkt wewnętrzny kuli Blocha, nie będący jej środkiem).

<sup>20</sup> Stan maksymalnie zmieszany to stan opisany macierzą gęstości, która ma całkowicie zdegenerowane widmo wartości własnych (wszystkie niezerowe wartości własne są równe). Taki stan mieszany odpowiada (w niejednoznaczny sposób – zgodnie z reprezentacją Schmidta) splątany stan czystym układem A+B, które nazywamy wtedy maksymalnie splątanymi stanami (jest to słuszne dla dowolnego  $n$ ). Maksymalnie zmieszane stany osiągają maksimum *entropii von Neumanna*  $S = -\text{tr}_A(\hat{\rho} \ln \hat{\rho})$  (uogólnienie entropii informacyjnej Schannona  $S = -\sum p_i \ln p_i$ , dla rozkładu prawdopodobieństwa) – maksimum jest osiągnięte dla jednorodnego rozkładu w obu przypadkach (entropię von Neumanna można traktować zatem jako miarę zmieszania stanu mieszanego opisanego macierzą gęstości, a przez to i splątania stanu czystego całego układu).

<sup>21</sup> W przypadku więcej wymiarowej przestrzeni macierz gęstości stanu maksymalnie zmieszanego jest postaci

$$\hat{\rho} = \frac{1}{n} \hat{1} \quad (\text{odpowiada to zmieszaniu stanów czystych w równych proporcjach } \frac{1}{n})$$



Rys. 2. Sfera Blocha jest kulą jednostkową w abstrakcyjnej przestrzeni 3D (tradycyjnie używa się nazwy sfera)

Kierunek wektora  $\vec{P}$  można identyfikować z kierunkiem spinu. Jest on także kierunkiem wzdłuż którego prowadzić można średnicę, na końcach której leżą stany czyste dające po zmieszaniu dany stan mieszany  $\hat{\rho} = \frac{1}{2}(\hat{1} + \vec{P} \cdot \hat{\sigma})$ . Gdy  $\vec{P}$  jest zero, jak dla maksymalnie zmieszanego stanu qubitów, kierunek spinu (i średnicy) można wybrać dowolnie. W szczególności istnieją zatem 3 wzajemnie prostopadłe kierunki spinu: x, y i z, którymi można charakteryzować zmieszanie (przygotowanie) stanu maksymalnie splątanego w interpretacji spinowej, tzn.:

$$\begin{aligned}\hat{\rho} &= \frac{1}{2}\hat{1} = \frac{1}{2}|\uparrow\rangle_{xx}\langle\uparrow| + \frac{1}{2}|\downarrow\rangle_{xx}\langle\downarrow|, \\ \hat{\rho} &= \frac{1}{2}\hat{1} = \frac{1}{2}|\uparrow\rangle_{yy}\langle\uparrow| + \frac{1}{2}|\downarrow\rangle_{yy}\langle\downarrow|, \\ \hat{\rho} &= \frac{1}{2}\hat{1} = \frac{1}{2}|\uparrow\rangle_{zz}\langle\uparrow| + \frac{1}{2}|\downarrow\rangle_{zz}\langle\downarrow|.\end{aligned}$$

Są to trzy różne przygotowania (zmieszania) prowadzące do tego samego stanu mieszanego, spośród nieskończenie wielu innych możliwych, odróżniają się one jednak interpretacją w języku spinu – tzn. odpowiadają trzem ortogonalnym kierunkom wektora spinu, a stany  $|\uparrow\rangle_{\alpha}$  i  $|\downarrow\rangle_{\alpha}$ , można interpretować jako rzut spinu na kierunek  $\alpha$ .

Stany splątane dwóch qubitów to stany z przestrzeni Hilberta 4-wymiarowej, która jest iloczynem dwóch przestrzeni qubitów (2-wymiarowych), takie że nie można ich separować na prosty iloczyn tensorowy stanów obu qubitów. W 4-wymiarowej przestrzeni Hilberta pary



qubitów można wybrać bazę złożoną z samych stanów splątanych. Standardowa baza tej przestrzeni składa się ze stanów niesplątanych:

$$|1\rangle_A \otimes |1\rangle_B, \quad |2\rangle_A \otimes |1\rangle_B, \quad |1\rangle_A \otimes |2\rangle_B, \quad |2\rangle_A \otimes |2\rangle_B.$$

Stany te tworzą bazę ON w  $H_A \otimes H_B$ . Bazę tę można jednak zmienić na dowolną inną bazę (przy pomocy unitarnej transformacji), w szczególności na bazę złożoną z maksymalnie splątanych stanów (tj. odpowiadających maksymalnie zmieszanemu stanowi zarówno układu A jak i B – wszystkie stany splątane odpowiadają temu samemu stanowi zmieszanemu podukładu A i B).

Taką bazę można wybrać w postaci:

$$\begin{aligned} |\Psi^+\rangle_{AB} &= \frac{1}{\sqrt{2}} (|1\rangle_A \otimes |2\rangle_B + |2\rangle_A \otimes |1\rangle_B), \\ |\Psi^-\rangle_{AB} &= \frac{1}{\sqrt{2}} (|1\rangle_A \otimes |2\rangle_B - |2\rangle_A \otimes |1\rangle_B), \\ |\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}} (|1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B), \\ |\Phi^-\rangle_{AB} &= \frac{1}{\sqrt{2}} (|1\rangle_A \otimes |1\rangle_B - |2\rangle_A \otimes |2\rangle_B). \end{aligned}$$

Wektory te nazywane są *stanami Bella*, a baza – *bazą Bella*<sup>22</sup>. Łatwo zauważyć, że baza Bella ma specjalną własność – stany qubitów A wchodzi do wszystkich wektorów Bella w taki sam sposób. Oznacza to, że można uzyskać wszystkie wektory Bella z jednego z nich (np. pierwszego) manipulując tylko stanami qubitów B, a więc przy pomocy tylko lokalnych operacji na układzie B.

Ta własność jest ściśle kwantowa (wynika ze splątania kwantowego – czyli w zasadzie z prostych własności algebraicznych 4-wymiarowej przestrzeni liniowej) i nie ma swojego odpowiednika klasycznego. Ten fakt nosi nazwę *supergęstego kodowania*.

## 8. Protokoły kwantowe

### 8.1. Super gęste kodowanie

Z postaci stanów Bella wynika, że następujące operacje lokalne na qubicie B pozwalają otrzymać wszystkie stany Bella z jednego, np.

<sup>22</sup> ortonormalność bazy Bella można sprawdzić bezpośrednim rachunkiem wykorzystując ON bazy standardowej



$$|1\rangle_B \Rightarrow |1\rangle_B, \quad |2\rangle_B \Rightarrow |2\rangle_B \quad (\text{operacja tożsamosciowa}) \Leftrightarrow |\Psi^+\rangle_{AB} \Rightarrow |\Psi^+\rangle_{AB},$$

$$|1\rangle_B \Rightarrow -|1\rangle_B, \quad |2\rangle_B \Rightarrow |2\rangle_B \quad (\text{obrot o } \pi) \Leftrightarrow |\Psi^+\rangle_{AB} \Rightarrow |\Psi^-\rangle_{AB},$$

$$|1\rangle_B \Rightarrow |2\rangle_B, \quad |2\rangle_B \Rightarrow |1\rangle_B \quad (\text{zamiana}) \Leftrightarrow |\Psi^+\rangle_{AB} \Rightarrow |\Phi^+\rangle_{AB},$$

$$|1\rangle_B \Rightarrow -|2\rangle_B, \quad |2\rangle_B \Rightarrow |1\rangle_B \quad (\text{zamiana i obrot o } \pi) \Leftrightarrow |\Psi^+\rangle_{AB} \Rightarrow |\Phi^-\rangle_{AB},$$

Oznacza to zdwojenie możliwości kodowania informacji w stosunku do klasycznej pary bitów: 00, 01, 10, 11. W tym przypadku, aby otrzymać wszystkie cztery stany pary bitów, należy kodować obydwa bity. Zauważmy, że podobną własność ma także baza standardowa przestrzeni  $H_A \otimes H_B$ , tj. baza:  $|1\rangle_A \otimes |1\rangle_B$ ,  $|2\rangle_A \otimes |1\rangle_B$ ,  $|1\rangle_A \otimes |2\rangle_B$ ,  $|2\rangle_A \otimes |2\rangle_B$  (także należy kodować na obu qubitach).

Własność supergęstego kodowania związana jest zatem ze splątaniem kwantowym.

## 8.2. Teleportacja kwantowa

Innym przykładem prostego wykorzystania splątania kwantowego jest zjawisko teleportacji kwantowej. Można opisać je w następujący sposób.

Jeśli mamy stan cząstki A (qubitu A) w postaci:

$$|\varphi\rangle_A = c_1|1\rangle_A + c_2|2\rangle_A, \quad (|c_1|^2 + |c_2|^2 = 1),$$

i chcemy przesłać (teleportować) ten stan na cząstkę B (qubit B), odległą od cząstki A, to możemy posłużyć się cząstką pomocniczą C (qubitem C), w taki sposób, że przygotowujemy parę cząstek CB w stanie splątanim. Najlepiej w jednym z maksymalnie splątanych stanów

Bella – np. w stanie  $|\Psi^-\rangle_{CB} = \frac{1}{\sqrt{2}}(|1\rangle_C \otimes |2\rangle_B - |2\rangle_C \otimes |1\rangle_B)$ . Można to zrobić posługując

się przyrządem pomiarowym realizującym pomiar na parze cząstek (w tym przypadku CB), tak zorganizowanym, że jego operator hermitowski ma przedstawienie spektralne w postaci operatorów rzutowania na cztery stany Bella qubitów C i B. Taki pomiar – ortogonalne rzutowanie na stany Bella – prowadzi do oddziaływania cząstek (qubitów) C i B, w wyniku którego powstaje jeden ze stanów Bella. Nie wiadomo który – może powstać każdy z jednakowym prawdopodobieństwem, ale z pewnością któryś powstanie. Taki pomiar na parze nieoddziaływujących cząstek prowadzi zatem do ich splątania, czyli jest ich oddziaływaniem. Zakładając zatem, że przygotowaliśmy parę qubitów C i B w stanie

$$|\Psi^-\rangle_{CB} = \frac{1}{\sqrt{2}}(|1\rangle_C \otimes |2\rangle_B - |2\rangle_C \otimes |1\rangle_B), \text{ cały układ ABC jest w stanie czystym}$$



$$\begin{aligned} |\Phi\rangle_{ABC} = |\varphi\rangle_A \otimes |\Psi^-\rangle_{CB} &= (c_1|1\rangle_A + c_2|2\rangle_B) \otimes \frac{1}{\sqrt{2}}(|1\rangle_C \otimes |2\rangle_B - |2\rangle_C \otimes |1\rangle_B) = \\ &= \frac{1}{2} \{ |\Psi^+\rangle_{AB} \otimes (-c_1|1\rangle_C + c_2|2\rangle_C) + \\ &+ |\Psi^-\rangle_{AB} \otimes (-c_1|1\rangle_C - c_2|2\rangle_C) + \\ &+ |\Psi^+\rangle_{AB} \otimes (c_1|2\rangle_C - c_2|1\rangle_C) + \\ &+ |\Psi^-\rangle_{AB} \otimes (c_1|2\rangle_C + c_2|1\rangle_C) \}. \end{aligned}$$

Ostatnia równość jest oczywistym tożsamościowym związkiem wynikającym z możliwości zapisu tego samego wektora w przestrzeni liniowej (w tym przypadku ośmiowymiarowej  $H_A \otimes H_B \otimes H_C$ ) w rozłożeniu na inne wektory (zmiana bazy). Jasne jest, że wektor

$|\Phi\rangle_{ABC} = |\varphi\rangle_A \otimes |\Psi^-\rangle_{CB}$ , może być przedstawiony w bazie przestrzeni  $H_A \otimes H_B \otimes H_C$  o postaci:

$$\begin{aligned} &|\Psi^+\rangle_{AB} \otimes |0\rangle_C, \quad |\Psi^-\rangle_{AB} \otimes |0\rangle_C, \quad |\Phi^+\rangle_{AB} \otimes |0\rangle_C, \quad |\Phi^-\rangle_{AB} \otimes |0\rangle_C, \\ &|\Psi^+\rangle_{AB} \otimes |1\rangle_C, \quad |\Psi^-\rangle_{AB} \otimes |1\rangle_C, \quad |\Phi^+\rangle_{AB} \otimes |1\rangle_C, \quad |\Phi^-\rangle_{AB} \otimes |1\rangle_C. \end{aligned}$$

Oczywiście wtedy współczynniki  $c_1$  i  $c_2$  znajdą się przy qubicie (częstce C), ale w wielu różnych kombinacjach. Można powiedzieć, że w tym sensie (nadmiarowo) te współczynniki są od razu przy częstce C (choć wprowadziliśmy je z częstką A) – tak samo jak przy dowolnej innej częstce – wynika to z możliwości zmiany bazy w przestrzeniach Hilberta wielo-cząstkowych (wielo-qubitowych) układów.

Jeśli uważać, że nie ma żadnego oddziaływania między cząstkami A, B, i C, ani też oddziaływania otoczenia na te trzy cząstki, to można oddalić cząstkę B (nawet znacznie) od cząstki C, pozostawiając je jednak dalej w stanie splątanym,

$$|\Psi^-\rangle_{CB} = \frac{1}{\sqrt{2}}(|1\rangle_C \otimes |2\rangle_B - |2\rangle_C \otimes |1\rangle_B).$$

Następnie można zbliżyć do siebie cząstki A i C i dokonać na tej parze ortogonalnego pomiaru stanów Bella, tzn. wprowadzić ich oddziaływanie za pośrednictwem tego pomiaru. W wyniku tego pomiaru zostanie wybrany (z równym prawdopodobieństwem) któryś z czterech możliwych stanów Bella pary AC, ale równocześnie, wobec powyższego przedstawienia, zostanie wtedy wybrany stan czysty cząstki B. Na przykład gdy po rzutowaniu na stany Bella pary AC znajdzie się ona w stanie  $|\Psi^-\rangle_{AC}$ , cząstka B będzie wtedy z pewnością w stanie  $c_1|2\rangle_B + c_2|1\rangle_B$ . Wystarczy wtedy lokalnie na częstce B (odległej) wykonać zamianę stanów  $|1\rangle_B$  i  $|2\rangle_B$ , by otrzymać ten sam stan, jaki na początku miała cząstka A. Z góry nie wiadomo było jednak, który z wyników rzutowania na stany Bella się zrealizuje (tu założyliśmy dla przykładu, że czwarty) i dopiero po jego zrealizowaniu

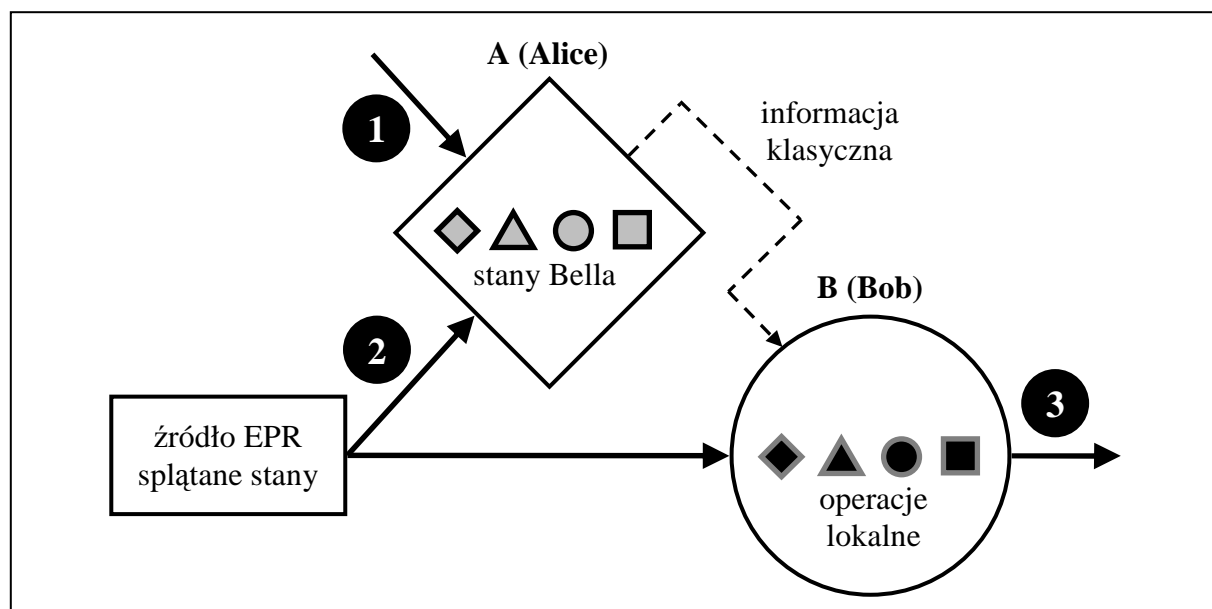
wiadomo co zrobić lokalnie na qubicie B (odległym), żeby otrzymać pożądany stan, taki jak wyjściowy na qubicie A. Tę informację, który ze stanów Bella zrealizował się w pomiarze (zupełnie losowo – zgodnie z *ansatzem* von Neumanna), należy przesłać do obserwatora przy qubicie B (Bob), za pomocą klasycznych kanałów łączności (informacje te wysła obserwator qubitu A, który dokonał pomiaru stanów Bella na parze AC - Alice).

Ten fakt konieczności przesłania dodatkowej informacji klasycznej powoduje

- ograniczenie prędkości teleportacji kwantowej przez prędkość światła (w kanale klasycznym), chociaż kwantowa informacja znalazła się na cząstce B natychmiastowo, ale w nieczytelny dla Boba sposób,
- układ z informacją klasyczną oznacza co innego, niż układ bez tej informacji klasycznej,
- konieczność uczestnictwa obserwatora (Boba) i obserwatora (Alice) w całym procesie teleportacji.

Pomiar dokonany przez Alice na parze AC powoduje splątanie cząstek A i C, ale równocześnie rozplątanie cząstek C i B – po tym pomiarze cząstka B jest już w stanie czystym. Natomiast cząstka A jest wtedy w stanie splątany z C (i para AC nie ma już żadnej informacji o współczynnikach  $c_1$  i  $c_2$  -- ta informacja jest już w całości na B – jest to wynik *rzutowania von Neumanna*). Jest tu spełniona zasada *no cloning* – stan czysty znika z cząstki A i pojawia się na cząstce C, nie ma więc kopiowania stanu kwantowego, ale jego przesyłanie (teleportacja).

Schemat teleportacji przedstawiony jest na rysunku:



Rys.3. Schematyczne przedstawienie procesu teleportacji kwantowej: do cząstki 2, splątanej kwantowo z cząstką 3, doplatuje się, przez pomiar na parze 1-2, cząstkę 1, wtedy cząstka 3 odplątuje się, a stan z cząstki 1 może być przeniesiony na cząstkę 3, pod warunkiem



wykonania odpowiedniego pomiaru na tej cząstce (skorelowanego z wcześniej nie znanym wynikiem pomiaru na parze 1-2).

## 9. Ewolucja w czasie macierzy gęstości

Macierz gęstości opisująca stan mieszany (w szczególności także czysty) danego układu odbywa ewolucję czasowa zgodnie z zasadami mechaniki kwantowej, która określa unitarną ewolucję całego układu A+B, tzn.

$$i\hbar \frac{\partial |\Psi(t)\rangle_{AB}}{\partial t} = H_{AB} |\Psi(t)\rangle_{AB},$$

gdzie  $H_{AB} = H_A + H_B + H_{int AB}$ , jest hamiltonianem całego układu A+B, uwzględniając oddziaływanie między podukładami. Z powyższego równania wynika ewolucja czasowa macierzy gęstości podukładu A, gdyż:

$$\hat{\rho}_A(t) = \text{tr}_B |\Psi(t)\rangle_{AB} \langle \Psi(t)|.$$

Jest jasne, że zależność czasowa macierzy gęstości podukładu A będzie zatem determinowana zarówno przez Hamiltonian układu A jak i B, oraz ich oddziaływanie. W ogólnym przypadku jest to złożona zależność, nie dająca się przełożyć na proste równanie dynamiczne w obrębie tylko podukładu A. W niektórych przypadkach szczegółowych, przy spełnieniu dodatkowych warunków, można jednak ewolucję macierzy gęstości wyrazić poprzez charakterystyki tylko podukładu A (będzie to przybliżenie) – nie będzie to jednak ewolucja unitarna, za wyjątkiem sytuacji gdy nie ma oddziaływania podukładów A i B (tzn. gdy  $H_{int AB} = 0$ ).

W tym ostatnim przypadku ewolucja macierzy gęstości podukładu A jest unitarna i daje się prosto opisać.

W przypadku braku oddziaływania między podukładami A i B, każdy z podukładów jest niezależny i w każdym odbywa się unitarna ewolucja stanów podukładów zgodnie ze swoimi hamiltonianami, tj.

$$i\hbar \frac{\partial |\varphi\rangle_A}{\partial t} = H_A |\varphi\rangle_A, \quad i\hbar \frac{\partial |\varphi\rangle_B}{\partial t} = H_B |\varphi\rangle_B.$$

Równania te zadają unitarne ewolucje dla każdego z podukładów (i łącznie dla całego układu A+B) – operatory tych unitarnych ewolucji to  $\hat{U}_A(t)$  i  $\hat{U}_B(t)$ <sup>23</sup>, a całego układu A+B

<sup>23</sup> gdy hamiltonian nie zależy jawnie od czasu, to operator ewolucji ma postać  $\hat{U}(t) = e^{-iHt/\hbar}$



$\hat{U}_{AB}(t) = \hat{U}_A(t) \otimes \hat{U}_B(t)$ . Te ewolucje można zapisać w postaci ewolucji macierzy gęstości<sup>24</sup> (analogicznie jak dla macierzy gęstości stanu czystego). W ogólnym przypadku macierz gęstości podukładu A ma postać (w dowolnej bazie przestrzeni Hilberta układu A):

$$\hat{\rho}_A = \sum_{i,j,k} a_{ik} a_{jk}^* |i\rangle_{AA} \langle j|,$$

lub w bazie, w której jest ona diagonalna,

$$\hat{\rho}_A = \sum_r p_r |r\rangle_{AA} \langle r|.$$

Macierz ta jest wynikiem wzięcia śladu po układzie B z macierzy gęstości stanu czystego całego układu A+B, tj.  $\hat{\rho}_A = \text{tr}_B |\Psi\rangle_{AB} \langle \Psi|$ , gdzie w dowolnych bazach przestrzeni Hilberta układu A i B  $|\Psi\rangle_{AB} = \sum_{i\alpha} a_{i\alpha} |i\rangle_A \otimes |\alpha\rangle_B$ . W przypadku unitarnej ewolucji podukładów A i B (tzn. gdy one nie oddziałują) mamy,

$$|\Psi(t)\rangle_{AB} = \hat{U}_{AB}(t) |\Psi(0)\rangle_{AB} = \sum_{i,\alpha} a_{i\alpha} \hat{U}_A(t) |i(0)\rangle_A \otimes \hat{U}_B(t) |\alpha(0)\rangle_B = \sum_{i,\alpha} a_{i\alpha} |i(t)\rangle_A \otimes |\alpha(t)\rangle_B.$$

Wektory  $|i(t)\rangle_A$ ,  $|\alpha(t)\rangle_B$  są w każdym momencie  $t$  bazami w swoich przestrzeniach (ponieważ unitarne transformacje – operatory ewolucji – przekształcają bazy w bazy), zatem w każdym momencie można wziąć ślad z macierzy gęstości stanu czystego układu A+B, i uzyskać macierz gęstości układu A z tymi samymi współczynnikami (niezależnymi od czasu), tj.,

$$\begin{aligned} \hat{\rho}_A(t) &= \text{tr}_B |\Psi(t)\rangle_{AB} \langle \Psi(t)| = \sum_{i,j,k} a_{ik} a_{jk}^* |i(t)\rangle_{AA} \langle j(t)| = \sum_{i,j,k} a_{ik} a_{jk}^* \hat{U}_A(t) |i(0)\rangle_{AA} \langle j(0)| \hat{U}_A^\dagger(t) \\ &= \sum_r p_r |r(t)\rangle_{AA} \langle r(t)| = \sum_r p_r \hat{U}_A(t) |r(0)\rangle_{AA} \langle r(0)| \hat{U}_A^\dagger(t) = \hat{U}_A(t) \hat{\rho}_A(0) \hat{U}_A^\dagger(t) \end{aligned}$$

zarówno w dowolnej jak i w diagonalnej reprezentacji.

Zatem **unitarna** ewolucja macierzy gęstości ma postać<sup>25</sup>,

$$\hat{\rho}_A(t) = \hat{U}_A(t) \hat{\rho}_A(0) \hat{U}_A^\dagger(t).$$

<sup>24</sup> w zasadzie w takim przypadku macierz gęstości podukładu A powinna być macierzą gęstości jego stanu czystego (bo brak jest oddziaływania z układem B, które mogło by wprowadzić zmieszania stanów); w ogólności jednak można rozważać ewolucję **unitarną** macierzy gęstości stanu mieszanego, gdyż taki stan mieszany mógł być przygotowany (traktować to można jako warunek początkowy) w wyniku oddziaływań, które zostały następnie wyłączone i już dalej podukład A ewoluuje samodzielnie

<sup>25</sup> operator ewolucji jest unitarny, więc  $\hat{U}_A^\dagger(t) = \hat{U}_A^{-1}(t)$





Można także napisać to w postaci równania różniczkowego, którego rozwiązaniem jest powyższy związek,

$$i\hbar \frac{\partial \hat{\rho}}{\partial t} = [\hat{H}_A, \hat{\rho}].$$

Równanie to łatwo uzyskać zapisując unitarną ewolucję w postaci równania Schrödingera-Heisenberga (dla wektorów bazy):

$$i\hbar |i(t)\rangle_A = \hat{H}_A |i(t)\rangle_A \quad i - i\hbar \langle j(t)|_A = \langle j(t)| \hat{H}_A.$$

Równanie różniczkowe dla unitarnej ewolucji macierzy gęstości nazywa się równaniem Louville'a (zwłaszcza w odniesieniu do uogólnienia macierzy gęstości na przypadek operatora statystycznego w kwantowej fizyce statystycznej).

Ewolucję unitarną macierzy gęstości można zilustrować geometrycznie dla macierzy gęstości qubitu posługując się kulą Blocha. Szczególnie interesujący<sup>26</sup> jest przypadek qubitu zdefiniowanego przez dwa stacjonarne stany<sup>27</sup> pewnego Hamiltonianu  $\hat{H}_0$

$$\begin{aligned} |\Phi_1(\vec{r}, t)\rangle_A &= e^{-iE_1 t/\hbar} |\varphi_1(\vec{r})\rangle_A, & \hat{H}_A |\Phi_1\rangle_A &= E_1 |\Phi_1\rangle_A, \\ |\Phi_2(\vec{r}, t)\rangle_A &= e^{-iE_2 t/\hbar} |\varphi_2(\vec{r})\rangle_A, & \hat{H}_A |\Phi_2\rangle_A &= E_2 |\Phi_2\rangle_A. \end{aligned}$$

Jeśli qubit jest w stanie czystym  $|\Psi(t)\rangle_A = c_1 e^{-iE_1 t/\hbar} |\varphi_1\rangle_A + c_2 e^{-iE_2 t/\hbar} |\varphi_2\rangle_A$ , to macierz gęstości ma postać,

$$\hat{\rho}_A(t) = \begin{bmatrix} |c_1|^2 & c_1 c_2^* e^{i\omega_0 t} \\ c_1^* c_2 e^{-i\omega_0 t} & |c_2|^2 \end{bmatrix},$$

gdzie  $\omega_0 = \frac{E_2 - E_1}{\hbar}$ .

Można także ogólniej, gdy Hamiltonian układu qubitu:  $\hat{H}_A = \hat{H}_0 + \hat{H}'_A(t)$  i qubit rozpięty jest na dwóch stanach stacjonarnych Hamiltonianu  $\hat{H}_0$ . Macierz gęstości qubitu spełnia w tym przypadku równanie unitarnej ewolucji:

$$i\hbar \frac{\partial \hat{\rho}_A(t)}{\partial t} = [(\hat{H}_0 + \hat{H}'_A), \hat{\rho}(t)].$$

<sup>26</sup> ze względu na zastosowania do opisu dwupoziomowego układu laserującego [np. K.Shimoda, *Wstęp do fizyki laserów*, PWN Warszawa 1993]

<sup>27</sup> w ogólności qubit nie musi być rozpięty na stanach stacjonarnych, ale w przypadku takich stanów ewolucja czasowa tych stanów jest wyjątkowo prosta



Równanie to można przepisać w postaci (w reprezentacji Hamiltonianu  $\hat{H}_0$ ),

$$i\hbar \frac{\partial \rho_{ij}}{\partial t} = E_i \rho_{ij} - E_j \rho_{ij} + \sum_k (H'_{ik} \rho_{kj} - \rho_{ik} H'_{kj}),$$

gdzie  $i, j, k = 1, 2$ ,  $H'_{ik} = \langle \Phi_i | \hat{H}_A | \Phi_k \rangle_A$ . Pamiętając, że macierz gęstości jest operatorem hermitowskim o śladzie 1, tylko dwa (dla qubitu) elementy macierzowe  $\rho_{ij}$  są niezależne, np.  $\rho_{11}$  (rzeczywisty) i  $\rho_{12}$  (zespolony). Spełniają one równania:

$$\begin{aligned} \frac{\partial \rho_{11}}{\partial t} &= \frac{i}{\hbar} (\rho_{12} H'_{21} - c.c.), \\ \frac{\partial \rho_{12}}{\partial t} &= i\omega_0 \rho_{12} - \frac{i}{\hbar} (1 - 2\rho_{11}) H'_{12} - \frac{i}{\hbar} \rho_{12} (H'_{11} - H'_{22}) \end{aligned}$$

zauważmy, że  $\rho_{22} = 1 - \rho_{11}$ ,  $\rho_{21} = \rho_{12}^*$ .

Łatwo też podać powyższe równanie ruchu w reprezentacji wektora z kuli Blocha (ze sfery Blocha – gdy rozważamy stan czysty). Wektor Blocha wyraża się następująco:

$$\begin{aligned} P_x &= 2 \operatorname{Re} \rho_{12}, \\ P_y &= -2 \operatorname{Im} \rho_{12}, \\ P_z &= \rho_{11} - \rho_{22}. \end{aligned}$$

Wtedy równanie unitarnej ewolucji macierzy gęstości qubitu można zapisać w postaci

$$\frac{\partial \vec{P}}{\partial t} = \vec{F} \times \vec{P}, \quad \vec{F} = \left( \frac{1}{\hbar} (H'_{12} + H'_{21}), \frac{i}{\hbar} (H'_{12} - H'_{21}), -\omega_0 - \frac{1}{\hbar} (H'_{22} - H'_{11}) \right).$$

Widzimy, że wektor  $\vec{F}$  jest rzeczywisty ( $F_x = \frac{2}{\hbar} \operatorname{Re} H'_{12}$ ,  $F_y = -\frac{2}{\hbar} \operatorname{Im} H'_{12}$ ). Często (z przyczyn symetrii)  $H'_{11} = H'_{22} = 0$ , wtedy  $F_z = -\omega_0$ . Powyższe równanie opisuje precesję wektora Blocha wokół wektora  $\vec{F}$ . Zatem unitarna (koherentna) ewolucja macierzy gęstości qubitu to precesja jęgo wektora Blocha wokół wektora  $\vec{F}$ .

## 10. Sterowanie qubitem – oscylacje Rabięgo

Oscylacje Rabięgo odnoszą się do ściśle dwupoziomowego układu kwantowego – zatem do qubitu. Są obserwowane eksperymentalnie (głównie w pomiarach spektroskopii atomowej),



gdy dwa poziomy energetyczne są oddalone i przejścia kwantowe do innych poziomów są zaniedbywalnie małe (dodatkowo zablokowane np. przez reguły wyboru). W przypadku dwupoziomowego układu zapisać można jego stany stacjonarne:

$$\begin{aligned} H_0|1\rangle &= E_1|1\rangle, \\ H_0|2\rangle &= E_2|2\rangle. \end{aligned}$$

Zewnętrzne zależne od czasu zaburzenie przyjąć można w postaci pola elektrycznego fali elektro-magnetycznej, o potencjale wektorowym,

$$V(t) \approx V_0 \cos(\omega t),$$

i jeśli spełnione są warunki przybliżenia dipolowego (tzn., gdy długość fali odpowiadająca częstości  $\omega$ , jest dużo większa od rozmiarów układu<sup>28</sup>) i wyrazić można poprzez operator

$$H' = \mu_z E_0 (e^{i\omega t} + c.c.) / 2,$$

gdzie,  $\mu_z$  jest z-tową składową momentu dipolowego (elektronu w atomie lub kropce) przy polaryzacji fali e-m wzdłuż osi z.

Takie zaburzenie powoduje niestacjonarną ewolucję układu, której odpowiada funkcja falowa  $|\Psi(t)\rangle$ . Funkcję tę można jednak w każdym momencie,  $t$ , rozłożyć w przestrzeni Hilberta rozpiętej na stanach  $|1\rangle$  i  $|2\rangle$ , t.j.,

$$|\Psi(t)\rangle = a_1(t)|1\rangle + a_2(t)|2\rangle,$$

oraz,

$$i\hbar \frac{\partial |\Psi(t)\rangle}{\partial t} = (H + H')|\Psi(t)\rangle.$$

Zakładając (dla uproszczenia), że stany  $|1\rangle$  i  $|2\rangle$  są symetryczne na odbicie współrzędnych (wtedy  $\langle 1|\mu_z|1\rangle = \langle 2|\mu_z|2\rangle = 0$ ), otrzymać można następujące równania na współczynniki zależne od czasu,

$$i\hbar \frac{\partial a_1}{\partial t} = a_2 \left\langle \tilde{1} \left| -\frac{1}{2} \mu_z E_0 \right| \tilde{2} \right\rangle \left[ e^{i(\omega - \omega_0)t} + e^{-i(\omega + \omega_0)t} \right],$$

<sup>28</sup> tak jest w przypadku stanów elektronu w atomie (dla zakresu widzialnego częstości odpowiadającego atomowym odległościom energetycznym) lub w kropce kwantowej (dla zakresu podczerwonego odpowiadającego odległościom energetycznym w kropce), lub protonu w jądrze atomowym (dla zakresu rentgenowskiego)



$$i\hbar \frac{\partial a_2}{\partial t} = a_1 \langle \tilde{1} | -\frac{1}{2} \mu_z E_0 | \tilde{2} \rangle \left[ e^{i(\omega+\omega_0)t} + e^{-i(\omega-\omega_0)t} \right]$$

gdzie,  $\omega_0 = \frac{E_2 - E_1}{\hbar}$  wiąże się ze stacjonarną ewolucją stanów,  $|i\rangle = e^{iE_i t} |\tilde{i}\rangle$ .

W powyższych równaniach mamy zatem czynniki czasowe szybkozmienne,  $e^{\pm i(\omega+\omega_0)t}$ , oraz wolno zmienne  $e^{\pm i(\omega-\omega_0)t}$  (przy założeniu, że  $\omega \approx \omega_0$ ). W przypadku równań różniczkowych z istotnie różnymi skalami czasowymi, dominujący wpływ na rozwiązanie wywiera wolno-zmienna funkcja, natomiast szybkozmienna powoduje niewielkie dodatkowe oscylacje o dużej częstotliwości nałożone na wolno-zmienny przebieg rozwiązania. Z powodu rozdzielczości czasowej ewentualnej obserwacji oscylacje te nie wnoszą żadnego wkładu przy uśrednieniu po czasie i można je zaniedbać. Przybliżenie takie nosi nazwę przybliżenia wirujących osi (i jest wykorzystywane w obliczeniach dwupoziomowych układów laserujących). W ramach takiego przybliżenia układ równań różniczkowych zapisać można w postaci równania drugiego rzędu:

$$\frac{\partial^2 a_1}{\partial t^2} - i(\omega - \omega_0) \frac{\partial a_1}{\partial t} + \frac{|x|^2}{4} a_1 = 0,$$

gdzie,  $x = \frac{\langle \tilde{1} | \mu_z E_0 | \tilde{2} \rangle}{\hbar}$ .

To równanie (liniowe) ma rozwiązanie w postaci,

$$a_1 = (A_1 e^{i\Omega t/2} + B_1 e^{-i\Omega t/2}) e^{i(\omega-\omega_0)t/2},$$

gdzie,  $\Omega = \sqrt{(\omega - \omega_0)^2 + |x|^2}$ .

Dla warunków początkowych,  $a_1(0) = 0$  (wtedy,  $a_2(0) = 1$  [wybrane rzeczywiste], gdyż  $|a_1|^2 + |a_2|^2 = 1$ ) łatwo ustalić wartości stałych  $A_1$  i  $B_1$ . Wtedy,

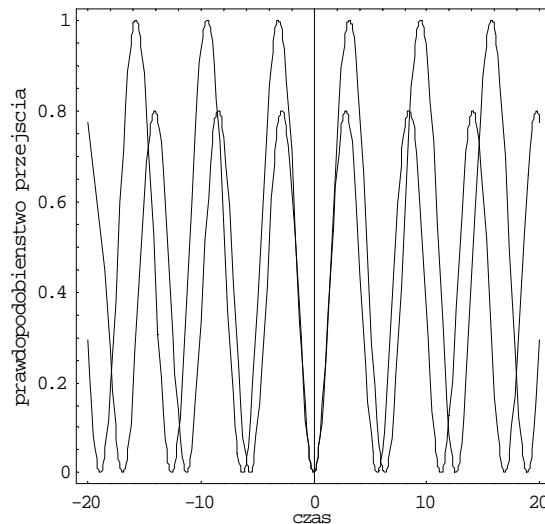
$$a_1(t) = \frac{ix}{\Omega} \sin \frac{\Omega t}{2} e^{i(\omega-\omega_0)t/2},$$

$$a_2(t) = \left( \cos \frac{\Omega t}{2} - \frac{\omega - \omega_0}{2\Omega} \sin \frac{\Omega t}{2} \right) e^{i(\omega-\omega_0)t/2}.$$

Z powyższych zależności określić można prawdopodobieństwo znalezienia układu w stanie  $|1\rangle$ ,

$$|a_1(t)|^2 = \frac{|x|^2}{\Omega^2} \left( \sin \frac{\Omega t}{2} \right)^2.$$

Wynik ten przedstawia oscylacje Rabiego – periodyczne przechodzenie układu między dwoma stanami – zostało to zobrazowane na rysunku.



Rys. 4. Oscylacje Rabiego – prawdopodobieństwo znalezienia układu w stanie  $|1\rangle$  zmienia się periodycznie w zakresie od 0 do 1, w przypadku rezonansu,  $\omega = \omega_0$ ; poza rezonansem oscylacje Rabiego nie osiągają 1 (i mają większą częstość)

Cyklicznym przejściom między stanami qubitów towarzyszy emisja i absorpcja kwantu energii (fotonu) [oscylacje Rabiego nazywane są czasem kwantowym dudnienia z powodu podobieństwa do dudnienia w wyniku interferencji fal]. Częstość oscylacji Rabiego,  $\Omega = x$ , dla idealnego rezonansu, jest tym większa im większy jest element macierzowy sprzężenia (zależny od  $E_0$ ). Czas, po którym qubit przechodzi całkowicie ze jednego do drugiego stanu nazywany jest czasem  $\pi$  impulsu i wynosi on  $\frac{\pi}{\Omega}$ . Wyłączenie zaburzenia w odpowiednim momencie pozwala na ustalenie dowolnie wybranej koherentnej superpozycji qubitów – zatem oscylacje Rabiego to technika sterowania qubitami.

Należy zauważyć, że oscylacje Rabiego wymagają rezonansowego monochromatycznego sygnału sterującego, który może być włączony lub wyłączony w dowolnie krótkim czasie. Nie jest możliwe jednak włączanie i wyłączanie sygnału ściśle monochromatycznego – obwiednia sterowania sygnałem spowoduje rozmycie częstości (zgodnie z fourierowską reprezentacją czasowej obwiedni sterującej). Z praktycznego punktu widzenia, nie jest także łatwo osiągać krótkie czasy przełączania – są one ograniczone, w przypadku sterowania elektrycznego, przez LC obwodu sterującego.

Oscylacje Rabiego występują dla każdego dwupoziomowego układu, jeśli zależny od czasu sygnał sprzęga się z układem poprzez niezerowy element macierzowy między stanami



stacjonarnymi układu (qubitu). W przypadku dwóch orientacji spinu (np. w kierunku zewnętrznego stałego pola magnetycznego) dwa te stany rozpinają qubit o z-towych składowych spinu. Oscylacje Rabiego można w tym przypadku osiągnąć przy pomocy poprzecznego ( w kierunku np.  $x$  lub  $y$  ) zmiennego w czasie pola magnetycznego, dla którego odpowiedni człon Pauliego ma niezerowy element macierzowy z funkcjami spinu wzdłuż osi  $z$ .

## 11. Twierdzenia No-cloning, No-broadcasting oraz No-deleting

### 11.1. Twierdzenie No-cloning

Twierdzenie No-cloning brzmi następująco:

Nieznany stan kwantowy nie może być skopiowany [Wootters W. K., Żurek W. H., Nature **299** 802-803 (1982)].

Należy tutaj wyjaśnić, co oznacza „nieznany stan kwantowy”. Rozważmy pojedynczy qubit. Jest to stan rozpięty na bazie dwu-wektorowej. W ogólnym przypadku baza ta jest dowolna, ale jej wektory uważane są za stany „znane”, natomiast qubit z dowolnymi współczynnikami występującymi w kombinacji liniowej wektorów bazowych wybranej bazy nazywany jest stanem „nieznanym”. Nieznany stan odpowiada nieznanym wartościom współczynników definiujących qubit – w przypadku gdy wartości te wynoszą (0,1) lub (1,0) to stan qubitu odpowiada stanom bazy i uważany jest za „znany”.

To twierdzenie można łatwo udowodnić. Wystarczy zauważyć, że gdyby twierdzenie No-cloning nie było prawdziwe to istniałaby możliwość pomiaru niekomutujących wielkości na kopiach stanu, a to przeczyłoby schematowi von Neumanna kwantowego kolapsu na skutek pomiaru.

#### Dowód (1)

Bardziej precyzyjny dowód można przeprowadzić w następujący sposób. Załóżmy (nie wprost), że istnieje operator kopiowania  $\hat{A}$ , zdefiniowany następująco:

$$\hat{A}(|\Psi\rangle \otimes |s\rangle) = |\Psi\rangle \otimes |\Psi\rangle.$$

Więc,

$$\begin{aligned} \hat{A}[(\alpha|1\rangle + \beta|2\rangle) \otimes |s\rangle] &= (\alpha|1\rangle + \beta|2\rangle) \otimes (\alpha|1\rangle + \beta|2\rangle) \\ &= \alpha^2|1\rangle \otimes |1\rangle + \alpha\beta|1\rangle \otimes |2\rangle + \beta\alpha|2\rangle \otimes |1\rangle + \beta^2|2\rangle \otimes |2\rangle. \end{aligned}$$



Okazuje się, że ten operator jest nieliniowy i tym samym narusza warunek liniowości nakładany przez zasadę superpozycji. W konsekwencji taki operator nie może istnieć w ramach liniowej mechaniki kwantowej. Jeżeli jednak założyć jego liniowość, to

$$\hat{A}[(\alpha|1\rangle + \beta|2\rangle) \otimes |s\rangle] = \alpha \hat{A}[|1\rangle \otimes |s\rangle] + \beta \hat{A}[|2\rangle \otimes |s\rangle] = \alpha|1\rangle \otimes |1\rangle + \beta|2\rangle \otimes |2\rangle,$$

co stoi w sprzeczności z poprzednim równaniem. Oba równania można ze sobą uzgodnić tylko w przypadku gdy  $\beta = 0$ ,  $\alpha = 1$ , lub  $\alpha = 0$ ,  $\beta = 1$ , co oznacza, że kopiowany jest stan znany (wektor z bazy). To kończy dowód.

## Dowód (2)

Założmy (ponownie nie wprost), że kopiowanie jest możliwe. Jako wejście można rozważyć nieznaną stan  $|\psi\rangle$ , jako wyjście ten sam stan, który zastąpi wcześniejszy stan czysty aparatury kopiującej. Więc początkowy stan aparatury kopiującej oraz kopiowanego stanu można zapisać w następującej formie:

$$|\psi\rangle \otimes |s\rangle,$$

gdzie  $\otimes$  oznacza iloczyn tensorowy. Założmy dodatkowo, że proces kopiowania jest pewną operacją unitarną  $U$  aparatury kopiującej, czyli:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle.$$

Można rozważyć kopiowanie dwóch stanów czystych  $|\psi\rangle$  oraz  $|\varphi\rangle$ , zatem:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle,$$

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle.$$

Jeżeli teraz rozważyć iloczyn skalarny obu powyższych równań,

$$\begin{aligned} (U(|\psi\rangle \otimes |s\rangle), U(|\varphi\rangle \otimes |s\rangle)) &= (\psi \otimes \psi, \varphi \otimes \varphi), \\ L = (U(|\psi\rangle \otimes |s\rangle), U(|\varphi\rangle \otimes |s\rangle)) &= \left( (\psi \otimes |s\rangle), \underbrace{U^\dagger U}_{=1}(|\varphi\rangle \otimes |s\rangle) \right) \\ &= (\psi \otimes |s\rangle, \varphi \otimes |s\rangle) = (\psi, \varphi) \underbrace{(|s\rangle, |s\rangle)}_{=1} = (\psi, \varphi), \\ P = (\psi \otimes \psi, \varphi \otimes \varphi) &= (\psi, \varphi)(\psi, \varphi) = (\psi, \varphi)^2, \\ L = P &\Leftrightarrow (\psi, \varphi) = (\psi, \varphi)^2 \Leftrightarrow \langle \psi | \varphi \rangle = (\langle \psi | \varphi \rangle)^2, \end{aligned}$$

to uzyska się następujący warunek:



$$\langle \psi | \varphi \rangle = (\langle \psi | \varphi \rangle)^2.$$

Powyższe równanie jest postaci:

$$x = x^2 \Rightarrow x = 0 \vee x = 1.$$

Stąd, albo  $|\psi\rangle = |\varphi\rangle$  albo  $|\psi\rangle$  i  $|\varphi\rangle$  są prostopadłe. To odpowiada stanom bazy, a stany bazy mogą być kopiowane, w odróżnieniu od innych. Np. stan  $|\psi\rangle = |0\rangle$  oraz  $|\varphi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  nie mogą zostać skopiowane, ponieważ nie są ortogonalne. Zatem operacja U nie dopuszcza kopiowania dowolnych nieznanych stanów. To kończy dowód.

W bardzo podobny sposób można dowieść braku możliwości skasowania nieznannej kwantowej informacji (*No-Deleting*<sup>29</sup>) – wynika to z nieliniowego charakteru kasowania, co stoi w sprzeczności z liniowością mechaniki kwantowej. Twierdzenie *No-Cloning*<sup>30</sup> prowadzi także do braku możliwości rozprzestrzeniania (*broadcasting*) kwantowej informacji, co byłby nierozzerwalnie związane z tworzeniem kopii. Ta idea wyrażona jest w twierdzeniu *No-Broadcasting*<sup>31</sup>. Wymienione twierdzenia znacząco odróżniają informację kwantową od klasycznej, która w przeciwieństwie kwantowej może być kopiowana, kasowana oraz rozprzestrzeniana. Jest to silny dowód na to, że kwantowa informacja jest zupełnie innym obiektem niż jej klasyczny odpowiednik.

### Konsekwencje dla QIP (kwantowego przetwarzania informacji)

- brak możliwości tworzenia kopii kwantowych rejestrów
- bezużyteczność klasycznych metod korekcji błędów (bazujących na zwielokrotnieniu kopii informacji)
- umożliwienie całkowicie bezpiecznej komunikacji kwantowej (bezpieczeństwo przed atakami hakerów)
- umożliwienie natychmiastowej identyfikacji dowolnej formy ataków hakerskich
- potwierdzenie zasady nieoznaczoności
- potwierdzenie destruktywnego charakteru pomiaru kwantowego

<sup>29</sup> Pati A. K., Braunstein S. L., *Impossibility of deleting an unknown quantum state*, Nature **404**, 164 (2000); Pati A. K., Braunstein S. L., *Quantum deleting and signalling*, arXiv:quant-ph/0305145v1 (2003), Żurek W., *Quantum cloning: Schrödinger's sheep* Nature **404**, 130 (2000)

<sup>30</sup> Wootters W. K., Żurek W. H., *A single quantum cannot be cloned*, Nature **299** 802-803 (1982)

<sup>31</sup> Barnum H. et al, *Noncommuting mixed states cannot be broadcast*, Phys. Rev. Lett. **76**, 2818-2821 (1996); Gottesman D., Chuang I. L., *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature **402**, 390 (1999); Bennett C. H., DiVincenzo D., *Quantum information and computation*, Nature, **404** (2000); DiVincenzo D., *Quantum Computation*, Science **270**, 255 (1995)





- w przypadku gdyby możliwe było kopiowanie wtedy dopuszczalna byłaby natychmiastowa komunikacja (co naruszałoby ograniczenia relatywistyczne) zgodnie z poniższym schematem:
  - przygotowanie pary splątanych fotonów – para EPR (związek nazwy ze znanym paradoksem Einsteina-Podolskiego-Rosena)
  - na jednej z cząstek dokonywany jest pomiar w wybranej bazie - założmy, że jest to pomiar polaryzacji
  - druga cząstka posiadać będzie identyczną polaryzację, na skutek splątania – zgodnie z argumentacją paradoksu EPR
  - następnie kopiowany jest drugi foton i dokonywany jest pomiar kopii
  - w ten sposób można określić, w której bazie został zmierzony pierwszy foton
  - czyli natychmiastowa komunikacja byłaby możliwa

## 11.2. Twierdzenie No-broadcasting – konsekwencje

Jak zauważyliśmy wyżej, w informatyce kwantowej można także wprowadzić twierdzenie o braku możliwości rozprzestrzeniania (*No-Broadcasting*) informacji kwantowej, które wynika z twierdzenia Żurka *No-Cloning*. Wykluczenie możliwości kopiowania informacji skutkuje silnym ograniczeniem narzuconym na kantową komunikację. Kwantowa komunikacja musi przebiegać w trybie jeden-do-jednego, w odróżnieniu od klasycznych systemów np. transmisji telewizyjnej, druku książek, czy kopiowania lub transmitowania dokumentów elektronicznych.

## 11.3. Twierdzenie No-deleting – konsekwencje

Zagadnienia dotyczące usuwania (kasowania) informacji są silnie związane z bezpieczeństwem informacji. W przypadku klasycznego przetwarzania informacji mamy do czynienia z dwoma możliwymi schematami kasowania informacji. Proces kasowania odbywający się przy zachowaniu kopii (ten proces jest odwracalny). Drugi schemat to proces nieodwracalnego wymazania informacji. Taki nieodwracalny proces musi odbywać się zgodnie z prawami fizyki statystycznej – potrzebuje energii<sup>32</sup> – związane z tym rozważania doprowadziły do sformułowania zasady Landauera<sup>33</sup>.

W przypadku kwantowego przetwarzania informacji nieodwracalne wymazanie stanu pojedynczego qubitu może zostać wykonane np. poprzez dekoherencję spowodowaną otoczeniem.

Proces kasowania przy zachowaniu kopii – odwracalne wymazywanie jest procesem odwrotnym do procesu kopiowania nieznanego stanu – więc także nie jest możliwe.

Założmy, że dysponujemy pewną liczbą kopii nieznannej informacji. W przypadku klasycznym możliwe jest skasowanie jednej kopii przy zachowaniu drugiej, po czym

<sup>32</sup> wymazywanie informacji jest procesem *dyssypatywnym* w sensie fizycznym; wykonanie takiej operacji wymaga zmniejszenia objętości fazowej układu i przez to redukcji entropii – jest to zatem proces nieodwracalny i niesamorzutny, konieczne jest wykonanie pracy, żeby taki proces przeprowadzić

<sup>33</sup> Landauer R., *Irreversibility and heat generation in the computing process*. IBM Journal of Research & Development **5**, 183-191 (1961)



odtworzenie informacji następuje przy wykorzystaniu pozostałej kopii. W przypadku kwantowym sytuacja jest zupełnie inna.

Są tu dwie możliwe sytuacje:

- Wymazanie informacji – posiadana jest tylko jedno kopia stanu i ten stan może być zniszczony (przez pomiar, decoherencje) w sposób nieodwracalny (informacje zostaje całkowicie utracona)
- Skasowanie z zachowaniem kopii – w przypadku posiadania przynajmniej dwóch kopii tego samego stanu. Ta sytuacja nie jest jednak możliwa w kwantowym przypadku, ponieważ jest to odwrotny proces do procesu kopiowania.

Związane publikacje: *No-Deleting* [Pati A. K., Braunstein S. L., *Impossibility of deleting an unknown quantum state*, Nature **404**, 164 (2000); Pati A. K., Braunstein S. L., *Quantum deleting and signalling*, arXiv:quant-ph/0305145v1 (2003), Żurek W., *Quantum cloning: Schrödinger's sheep* Nature **404**, 130 (2000)]

### Dowód (1)

Rozważmy dwu-qubitowy układ oraz pewne otoczenie. Stany dwóch qubitów należą odpowiednio do przestrzeni  $H_1$ ,  $H_2$  natomiast stan otoczenia do przestrzeni  $H_3$ . Czyli stan całego układu należy do przestrzeni  $H_1 \otimes H_2 \otimes H_3$  (będącej iloczynem tensorowym przestrzeni poszczególnych podukładów). Załóżmy, że oba qubity znajdują się w tym samym nieznanym stanie kwantowym  $|\psi\rangle$  natomiast otoczenie znajduje się w pewnym stanie  $|A\rangle$ . Załóżmy, że transformacja usuwająca informację względem jej kopii jest transformacją liniową  $L$ ,

$$L : H_1 \otimes H_2 \otimes H_3 \rightarrow H_1 \otimes H_2 \otimes H_3,$$

oraz

$$|\psi\rangle \otimes |\psi\rangle \otimes |A\rangle \xrightarrow{L} |\psi\rangle \otimes |\Sigma\rangle \otimes |A_\psi\rangle,$$

gdzie  $|\Sigma\rangle$  jest stanem „pustym” (dowolnie wybranym), stan  $|A_\psi\rangle$  jest pomocniczym stanem otoczenia, zależnym od stanu  $|\psi\rangle$ . Ogólnie, rozpatrywana transformacja zdefiniowana jest na układzie trzech niesplątanych stanów i zamienia stan  $|\psi\rangle$  wobec jego kopii w stan  $|\Sigma\rangle$ . Dla ortogonalnych stanów bazy qubitu mamy:

$$\begin{aligned} |0\rangle \otimes |0\rangle \otimes |A\rangle &\rightarrow |0\rangle \otimes |\Sigma\rangle \otimes |A_0\rangle, \\ |1\rangle \otimes |1\rangle \otimes |A\rangle &\rightarrow |1\rangle \otimes |\Sigma\rangle \otimes |A_1\rangle. \end{aligned}$$

Należy zwrócić uwagę na to, że jawna postać transformacji dotyczy wyłącznie dwóch identycznych kopii. W przypadku, gdy stany poszczególnych qubitów są różne, transformacja



pozostaje niezdefiniowana (dla dwóch różnych stanów nie możemy mówić o odwróceniu w czasie transformacji kopiowania).

W ogólnym przypadku należy rozważyć dowolny stan qubitów:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Zgodnie z definicją transformacji,

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \otimes |A\rangle \xrightarrow{L} (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |A_\psi\rangle.$$

Zatem,

$$\begin{aligned} & \alpha^2|0\rangle \otimes |0\rangle \otimes |A\rangle + \beta^2|1\rangle \otimes |1\rangle \otimes |A\rangle + \alpha\beta|0\rangle \otimes |1\rangle \otimes |A\rangle + \beta\alpha|1\rangle \otimes |0\rangle \otimes |A\rangle \\ & \xrightarrow{L} (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |A_\psi\rangle. \end{aligned}$$

Dla zwięzłości zapisu przyjmijmy, że  $|X\rangle \otimes |X\rangle = |XX\rangle$ , czyli,

$$\begin{aligned} & \alpha^2|00\rangle \otimes |A\rangle + \beta^2|11\rangle \otimes |A\rangle + \alpha\beta[|01\rangle + |10\rangle] \otimes |A\rangle \\ & \xrightarrow{L} (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |A_\psi\rangle. \end{aligned}$$

Jak wspomniane zostało wcześniej, rozpatrywana transformacja  $L$  nie posiada jawnej postaci dla różnych stanów, dlatego można założyć dla stanu mieszanego, że,

$$\begin{aligned} & \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle] \otimes |A\rangle \xrightarrow{L} |\varphi\rangle \\ & \Downarrow \\ & \alpha\beta[|01\rangle + |10\rangle] \otimes |A\rangle \xrightarrow{L} \sqrt{2}\alpha\beta|\varphi\rangle. \end{aligned}$$

Zatem,

$$\begin{aligned} & \alpha^2|0\rangle \otimes |\Sigma\rangle \otimes |A_0\rangle + \beta^2|1\rangle \otimes |\Sigma\rangle \otimes |A_1\rangle + \sqrt{2}\alpha\beta|\varphi\rangle \\ & = (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |A_\psi\rangle. \end{aligned}$$

Wiadomo, z postaci  $|\varphi\rangle$ , że nie występuje tam zależność od współczynników  $\alpha$  i  $\beta$ . Aby powyższe równanie było spełnione dla dowolnych  $\alpha$  i  $\beta$  stan  $|A_\psi\rangle$  musi od nich liniowo zależeć. Stąd to równanie ma rozwiązanie jedynie gdy:



$$|\varphi\rangle = \frac{|0\rangle \otimes |\Sigma\rangle \otimes |A_1\rangle + |1\rangle \otimes |\Sigma\rangle \otimes |A_0\rangle}{\sqrt{2}},$$

$$|A_\psi\rangle = \alpha|A_0\rangle + \beta|A_1\rangle.$$

Stan końcowy całego układu przyjmuje postać:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes (\alpha|A_0\rangle + \beta|A_1\rangle).$$

Z warunku normalizacji uzyskuje się:

$$([\alpha|0\rangle + \beta|1\rangle] \otimes |\Sigma\rangle \otimes [\alpha|A_0\rangle + \beta|A_1\rangle], [\alpha|0\rangle + \beta|1\rangle] \otimes |\Sigma\rangle \otimes [\alpha|A_0\rangle + \beta|A_1\rangle]) = 1.$$

Zgodnie z definicją iloczynu skalarnego,

$$\begin{aligned} &([\alpha|0\rangle + \beta|1\rangle] \otimes |\Sigma\rangle \otimes [\alpha|A_0\rangle + \beta|A_1\rangle], [\alpha|0\rangle + \beta|1\rangle] \otimes |\Sigma\rangle \otimes [\alpha|A_0\rangle + \beta|A_1\rangle]) \\ &=([\alpha|0\rangle + \beta|1\rangle], [\alpha|0\rangle + \beta|1\rangle]) (|\Sigma\rangle, |\Sigma\rangle) ([\alpha|A_0\rangle + \beta|A_1\rangle], [\alpha|A_0\rangle + \beta|A_1\rangle]) \\ &= 1. \end{aligned}$$

Równocześnie,

$$\begin{aligned} &(|\Sigma\rangle, |\Sigma\rangle) = 1, \\ &([\alpha|0\rangle + \beta|1\rangle], [\alpha|0\rangle + \beta|1\rangle]) = |\alpha|^2 + |\beta|^2 = 1. \end{aligned}$$

Zatem,

$$\begin{aligned} &([\alpha|A_0\rangle + \beta|A_1\rangle], [\alpha|A_0\rangle + \beta|A_1\rangle]) \\ &= \alpha^2 (|A_0\rangle, |A_0\rangle) + \beta^2 (|A_1\rangle, |A_1\rangle) + \alpha\beta^* (|A_0\rangle, |A_1\rangle) + \beta\alpha^* (|A_1\rangle, |A_0\rangle) = 1 \\ &\quad \Downarrow \\ &\alpha^2 \langle A_0 | A_0 \rangle + \beta^2 \langle A_1 | A_1 \rangle + \alpha\beta^* \langle A_1 | A_0 \rangle + \beta\alpha^* \langle A_0 | A_1 \rangle = 1. \end{aligned}$$

Zakładając unormowanie  $A_0$  oraz  $A_1$ , można zapisać,

$$\begin{aligned} &\underbrace{\alpha^2 \langle A_0 | A_0 \rangle + \beta^2 \langle A_1 | A_1 \rangle}_{=1} + \alpha\beta^* \langle A_1 | A_0 \rangle + \beta\alpha^* \langle A_0 | A_1 \rangle \\ &\quad \Downarrow \\ &\alpha\beta^* \langle A_0 | A_1 \rangle + \beta\alpha^* \langle A_1 | A_0 \rangle = 0. \end{aligned}$$



Z powyższego wynika, że aby ostatnia równość była spełniona dla dowolnych  $\alpha$  i  $\beta$ , to stany  $A_0$  i  $A_1$  muszą być ortogonalne. Ortogonalność i unormowanie stanów  $A_0$  i  $A_1$  oznacza, że stan  $|A_\psi\rangle = \alpha|A_0\rangle + \beta|A_1\rangle$  zawiera tyle samo informacji co stan  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Czyli informacja nie została usunięta a jedynie przesunięta, co kończy dowód.

## Dowód (2)

Rozważmy liniowy operator  $\hat{A}$ , zdefiniowany następująco,

$$\hat{A}(|\psi\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |\varepsilon_\psi\rangle.$$

Dla dowolnego stanu qubitu  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  mamy,

$$\hat{A}([\alpha|0\rangle + \beta|1\rangle] \otimes [\alpha|0\rangle + \beta|1\rangle]) = [\alpha|0\rangle + \beta|1\rangle] \otimes |\varepsilon_\psi\rangle.$$

Ale można zapisać, że,

$$\begin{aligned} & \hat{A}([\alpha|0\rangle + \beta|1\rangle] \otimes [\alpha|0\rangle + \beta|1\rangle]) \\ &= \alpha^2 \hat{A}(|0\rangle \otimes |0\rangle) + \beta^2 \hat{A}(|1\rangle \otimes |1\rangle) + \alpha\beta \hat{A}([|0\rangle \otimes |1\rangle] + [|1\rangle \otimes |0\rangle]) \\ & \left| \begin{array}{l} \hat{A}(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |\varepsilon_0\rangle \\ \hat{A}(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |\varepsilon_1\rangle \\ \hat{A}([|0\rangle \otimes |1\rangle] + [|1\rangle \otimes |0\rangle]) = |\varphi\rangle \end{array} \right| \\ &= \alpha^2 |0\rangle \otimes |\varepsilon_0\rangle + \beta^2 |1\rangle \otimes |\varepsilon_1\rangle + \alpha\beta |\varphi\rangle. \end{aligned}$$

Czyli uzyskujemy równość,

$$\alpha^2 |0\rangle \otimes |\varepsilon_0\rangle + \beta^2 |1\rangle \otimes |\varepsilon_1\rangle + \alpha\beta |\varphi\rangle = [\alpha|0\rangle + \beta|1\rangle] \otimes |\varepsilon_\psi\rangle.$$

Jeśli  $|\varphi\rangle$  niezależny jest od  $\alpha$  i  $\beta$ , to dla dowolnych  $\alpha$  i  $\beta$ , to stan  $|\varepsilon_\psi\rangle$  musi być liniową funkcją tych parametrów. Rozwiązanie tego równania przyjmuje zatem postać:

$$\begin{aligned} |\varphi\rangle &= |0\rangle \otimes |\varepsilon_1\rangle + |1\rangle \otimes |\varepsilon_0\rangle, \\ |\varepsilon_\psi\rangle &= \alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle. \end{aligned}$$

Stan końcowy będzie postaci:

$$[\alpha|0\rangle + \beta|1\rangle] \otimes [\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle].$$



Z warunku normalizacji wynika, że,

$$\begin{aligned} &([\alpha|0\rangle + \beta|1\rangle] \otimes [\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle], [\alpha|0\rangle + \beta|1\rangle] \otimes [\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle]) = 1, \\ &([\alpha|0\rangle + \beta|1\rangle], [\alpha|0\rangle + \beta|1\rangle])([\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle], [\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle]) = 1, \\ &\left(\underbrace{|\alpha|^2 + |\beta|^2}_{=1}\right)([\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle], [\alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle]) = 1, \\ &\alpha^2 \langle \varepsilon_0 | \varepsilon_0 \rangle + \beta^2 \langle \varepsilon_1 | \varepsilon_1 \rangle + \alpha\beta^* \langle \varepsilon_1 | \varepsilon_0 \rangle + \alpha^* \beta \langle \varepsilon_0 | \varepsilon_1 \rangle = 1. \end{aligned}$$

Zakładając unormowanie  $\varepsilon_0$  oraz  $\varepsilon_1$ , można zapisać,

$$\underbrace{\alpha^2 \langle \varepsilon_0 | \varepsilon_0 \rangle + \beta^2 \langle \varepsilon_1 | \varepsilon_1 \rangle}_{=1} + \alpha\beta^* \langle \varepsilon_1 | \varepsilon_0 \rangle + \alpha^* \beta \langle \varepsilon_0 | \varepsilon_1 \rangle = 1.$$

Zatem,

$$\alpha\beta^* \langle \varepsilon_1 | \varepsilon_0 \rangle + \alpha^* \beta \langle \varepsilon_0 | \varepsilon_1 \rangle = 0.$$

To prowadzi do warunku  $\langle \varepsilon_1 | \varepsilon_0 \rangle = \langle \varepsilon_0 | \varepsilon_1 \rangle = 0$ , więc  $\varepsilon_0$  i  $\varepsilon_1$  tworzą bazę, oraz  $|\varepsilon_\psi\rangle = \alpha|\varepsilon_0\rangle + \beta|\varepsilon_1\rangle$  jest tym samym co  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . To kończy dowód.

## Konsekwencje

- Bezpieczeństwo kwantowej informacji
- Informacja kwantowa jest odporna na różne metody jej usuwania przy zachowaniu kopii

## 12. Bramki jedno-qubitowe

Unitarne macierze dwuwymiarowe opisują jedno-qubitowe operacje. Niektóre z nich nazywane są jedno-qubitowymi bramkami. Standardowo używane do konstruowania programów kwantowych bramki jedno-qubitowe zostaną przedstawione poniżej.

### 12.1. Macierze Pauliego

Macierze Pauliego definiowane są następująco:

$$\vec{\sigma} = (X, Y, Z),$$



$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Operator spinu (1/2) definiowany jest przy wykorzystaniu macierzy Pauliego:

$$\hat{S} = \frac{1}{2} \hat{\sigma}.$$

W mechanice kwantowej spin wprowadzany jest w ramach relatywistycznego podejścia w postaci równania Diraca w obecności pola magnetycznego, prowadzącym do pojawienia się członu Pauliego w Hamiltonianie,

$$-\mu_B \hat{S} \cdot \vec{B}.$$

Własności macierzy Pauliego:

$$\begin{aligned} \det(\sigma_i) &= -1, \\ \text{Tr}(\sigma_i) &= 0, \\ \sigma_i^2 &= I. \end{aligned}$$

Dla macierzy Pauliego można zapisać:

$$\sigma_i \sigma_j = i \varepsilon_{ijk} \sigma_k + \delta_{ij} I,$$

Łatwo jest wyprowadzić reguły komutacji dla macierzy Pauliego (pozostają one w pełnej analogii do reguł komutacji dla składowych operatora momentu pędu  $[M_i, M_j] = i \varepsilon_{ijk} M_k$ ):

$$[\sigma_i, \sigma_j] = 2i \varepsilon_{ijk} \sigma_k,$$

## 12.2. Bramka Pauliego $X$

Ta jedno-kubitowa bramka zdefiniowana jest jako unitarna operacja liniowa zadana przez macierz Pauliego  $X$ :

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

Bramka  $X$  zamienia wzajemnie stany bazowe  $|0\rangle$  oraz  $|1\rangle$ :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{X} |1\rangle, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{X} |0\rangle.$$



Dla dowolnego stanu qubitów, działanie bramki  $X$  sprowadza się do zamiany współczynników,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{X} \beta|0\rangle + \alpha|1\rangle.$$

Bramka ta jest bramką samo odwracalną (odwrotna do niej operacja jest tą samą operacją), ponieważ:

$$X^2 = I.$$

### 12.3. Bramka Pauliego $Y$

Ta jedno-qubitowa bramka zdefiniowana jest jako unitarna operacja liniowa zadana przez macierz Pauliego  $Y$ :

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Działanie tej bramki na stany bazy obliczeniowej przebiega zgodnie z poniższym zapisem,

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{Y} i|1\rangle, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{Y} -i|0\rangle.$$

Dla dowolnego stanu qubitów,

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -i\beta \\ i\alpha \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{Y} -i\beta|0\rangle + i\alpha|1\rangle.$$

Bramka ta jest również bramką samo-odwracalną, ponieważ

$$Y^2 = I.$$

### 12.4. Bramka Pauliego $Z$

Ta bramka jedno-qubitowa zdefiniowana jest jako unitarna operacja liniowa zadana przez macierz Pauliego  $Z$ :

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Działanie tej bramki na stany bazowe  $|0\rangle$  and  $|1\rangle$  jest następujące:





$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{Z} |0\rangle, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{Z} -|1\rangle.$$

Dla dowolnego stanu qubitu,

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{Z} \alpha|0\rangle - \beta|1\rangle.$$

Bramka ta także jest bramką samo-odwracalną, ponieważ,

$$Z^2 = I.$$

Warto podkreślić, że macierze Pauliego są hermitowskie (określają obserwable – składowe spinu),

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow X^+ = \left[ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^* \right]^T = X,$$

$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \Rightarrow Y^+ = \left[ \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}^* \right]^T = Y,$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow Z^+ = \left[ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^* \right]^T = Z.$$

Macierze Pauliego są równocześnie unitarne jak zostało pokazane wcześniej,

$$X^+X = XX^+ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I,$$

$$Y^+Y = YY^+ = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = I,$$

$$Z^+Z = ZZ^+ = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I.$$

## 12.5. Bramka Hadamarda

Ta jedon-qubitowa bramka jest zdefiniowana przez unitarną liniową macierz postaci:

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

Na stany bazowe bramka ta działa następująco:



$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle),$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

Można powiedzieć, że bramka ta przekształca stany bazy  $|0\rangle$  i  $|1\rangle$  na stany maksymalnej superpozycji (bramka Hadamarda przekształca  $|0\rangle$  i  $|1\rangle$  w stany leżące „w połowie drogi” sfery Blocha – dlatego nazywa się ją pierwiastkiem negacji, ale  $H^2 = I \neq \sigma_x$ ). Działanie bramki Hadamarda można interpretować, jako obrót sfery o  $\frac{\pi}{2}$  wokół osi  $y$ , a następnie obrót o  $\pi$  wokół osi  $x$ .

Dla dowolnego stanu qubitu działanie bramki jest następujące:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha + \beta \\ \alpha - \beta \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{H} \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle,$$

Macierz Hadamarda jest hermitowska,

$$H^+ = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H,$$

i równocześnie unitarna,

$$H^+ H = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I = H H^+.$$

Warto podkreślić, że dla dowolnej macierzy, która jest hermitowska i unitarna, jej odwrotność jest tą samą macierzą.

Łatwo zauważyć, że,

$$H = \frac{X + Z}{\sqrt{2}}.$$

## 12.6. Bramka fazy

Ta jedno-qubitowa bramka bramka zdefiniowana jest przez macierz,



$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Działanie na stany bazowe  $|0\rangle$  lub  $|1\rangle$  przebiega następująco:

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{S} |0\rangle, \quad \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{S} i|1\rangle.$$

Dla dowolnego stanu qubitu,

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ i\beta \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{S} \alpha|0\rangle + i\beta|1\rangle.$$

Można sprawdzić, że  $S^2 = Z \neq I$ , więc nie jest to bramka samo-odwracalna – ponieważ bramka ta nie jest hermitowska,

$$S^+ = \left[ \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}^* \right]^T = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \neq S.$$

Unitarność bramki fazy można łatwo sprawdzić,

$$S^+ S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = I,$$

$$S S^+ = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = I.$$

## 12.7. Bramka $\frac{\pi}{8}$

Ta bramka jedno-qubitowa jest zdefiniowana przez unitarną, niehermitowską macierz,

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, \quad T = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}.$$

Działanie tej bramki na stany bazowe  $|0\rangle$  and  $|1\rangle$  jest następujące:



$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{T} |0\rangle, \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ e^{i\frac{\pi}{4}} \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{T} e^{i\frac{\pi}{4}} |1\rangle.$$

Dla dowolnego stanu qubitu,

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ e^{i\frac{\pi}{4}} \beta \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{T} \alpha|0\rangle + e^{i\frac{\pi}{4}} \beta|1\rangle.$$

Jak łatwo sprawdzić  $T^2 = S \neq I$ , nie jest to bramka samo-odwracalna, ponieważ nie jest hermitowska,

$$T^+ = \left[ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}^* \right]^T = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} \neq T.$$

Unitarność bramki fazy można łatwo sprawdzić,

$$T^+T = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = I,$$

$$TT^+ = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} = I.$$

## 12.8. Bramka $e^{i\phi}$ (przesunięcie fazy o $\phi$ )

Ta bramka jedno-qubitowa jest zdefiniowana przez unitarna, niehermitowską macierz:

$$\Phi = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

Działanie tej bramki na stany bazowe  $|0\rangle$  and  $|1\rangle$  jest następujące:

$$\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} e^{i\phi} \\ 0 \end{bmatrix} \Leftrightarrow |0\rangle \xrightarrow{\Phi} e^{i\phi} |0\rangle, \quad \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ e^{i\phi} \end{bmatrix} \Leftrightarrow |1\rangle \xrightarrow{\Phi} e^{i\phi} |1\rangle,$$

a dla dowolnego stanu qubitu,

$$\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} e^{i\phi} \alpha \\ e^{i\phi} \beta \end{bmatrix} = e^{i\phi} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \Leftrightarrow \alpha|0\rangle + \beta|1\rangle \xrightarrow{\Phi} e^{i\phi} \alpha|0\rangle + e^{i\phi} \beta|1\rangle = e^{i\phi} (\alpha|0\rangle + \beta|1\rangle).$$



Widać, że działanie tej bramki sprowadza się do przesunięcia w fazie qubitów o  $\phi$ . Ta bramka posiada parametr  $\phi$ , dlatego powyższą definicję należy traktować, jako definicję rodziny takich bramek.

## 12.9. Rotacje na sferze Blocha

Jak zostało wcześniej opisane, qubit jest zdefiniowany przez dwie liczby rzeczywiste określające dwa współczynniki liniowej kombinacji,  $\alpha|0\rangle + \beta|1\rangle$ ,

$$\begin{aligned} |\alpha|^2 + |\beta|^2 &= 1, \\ \alpha &= x, \\ \beta &= e^{i\varphi} \sqrt{1-x^2}. \end{aligned}$$

Zatem,

$$\begin{aligned} x &= \cos\left(\frac{\theta}{2}\right), \\ \sqrt{1-x^2} &= \sin\left(\frac{\theta}{2}\right). \end{aligned}$$

Stąd, dla dowolnego qubitów, można zapisać,

$$\begin{aligned} &\alpha|0\rangle + \beta|1\rangle \text{ lub} \\ &\cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \sin\frac{\theta}{2}|1\rangle. \end{aligned}$$

Ta reprezentacja kątowa odpowiada współrzędnym sferycznym jednostkowego wektora,

$$\hat{n} = [\cos\varphi \sin\theta, \sin\varphi \sin\theta, \cos\theta],$$

na sferze Blocha. Stan  $|0\rangle$  odpowiada punktowi  $[0,0,1]$ , a  $|1\rangle$  odpowiada punktowi  $[0,0,-1]$ .

$$\begin{aligned} n_x &= |\hat{n}| \cos\varphi \sin\theta, \quad |\hat{n}| = 1, \\ n_y &= |\hat{n}| \sin\varphi \sin\theta, \quad |\hat{n}| = 1, \\ n_z &= |\hat{n}| \cos\theta, \quad |\hat{n}| = 1. \end{aligned}$$

Można zapisać postaci operatory obrotów względem osi  $\hat{x}, \hat{y}, \hat{z}$  o dowolny kąt  $\theta$ ,

$$\begin{aligned} R_x(\theta) &= e^{-i\frac{\theta}{2}X}, \\ R_y(\theta) &= e^{-i\frac{\theta}{2}Y}, \\ R_z(\theta) &= e^{-i\frac{\theta}{2}Z}, \end{aligned}$$



gdzie  $X, Y, Z$  są macierzami Pauliego. Z hermitowskości  $X, Y, Z$  wynika unitarność operatorów  $R_x, R_y, R_z$ .

Funkcje od operatorów zazwyczaj definiuje się poprzez rozwinięcie w szereg potęgowy. W ogólnym przypadku można wykorzystać rozwinięcie Taylora:

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x-x_0)^1 + \frac{f''(x_0)}{2!}(x-x_0)^2 + \dots,$$

i dla funkcji  $e^A$  (w  $x_0 = 0$ ), można zapisać,

$$e^A = 1 + \frac{A}{1} + \frac{A^2}{2!} + \frac{A^3}{3!} + \dots$$

Można zatem operator  $R_x(\theta) = e^{-i\frac{\theta}{2}X}$  rozwinąć w szereg. Zakładając,

$$A = -\frac{i\theta}{2}X = -\frac{i\theta}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

uzyska się:

$$A^2 = -\frac{\theta^2}{4} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -\frac{\theta^2}{4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -\frac{\theta^2}{4} I,$$

$$A^3 = A^2 A = -\frac{\theta^2}{4} \begin{pmatrix} -i\theta \\ -i\theta \end{pmatrix} I \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{i\theta^3}{8} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{i\theta^3}{8} A.$$

Zatem, dla parzystych potęg  $A^{2k} = I$ , a dla nieparzystych potęg  $A^{2k+1} = A$ . Stąd,

$$R_x(\theta) = \sum_{n=0}^{\infty} \frac{1}{n!} \left(-\frac{i\theta}{2}\right)^n X^n$$

$$= \sum_{k \in \mathbb{N}} \frac{1}{(2k)!} \left(-\frac{i\theta}{2}\right)^{2k} I + \sum_{k \in \mathbb{N}} \frac{1}{(2k+1)!} \left(-\frac{i\theta}{2}\right)^{2k+1} X.$$

W związku z  $(i)^{2k} = (-1)^k$  oraz  $(i)^{2k+1} = i(-1)^k$  można zapisać:

$$R_x(\theta) = \sum_{k \in \mathbb{N}} \frac{1}{(2k)!} (-1)^k \left(\frac{\theta}{2}\right)^{2k} I + \sum_{k \in \mathbb{N}} \frac{1}{(2k+1)!} (-i)(-1)^k \left(\frac{\theta}{2}\right)^{2k+1} X.$$

Ale, można skorzystać z zależności,



$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1},$$

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n}.$$

W wyniku można zapisać końcową postać:

$$R_x(\theta) = I \underbrace{\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} \left(\frac{\theta}{2}\right)^{2n}}_{=\cos\left(\frac{\theta}{2}\right)} + (-i) X \underbrace{\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} \left(\frac{\theta}{2}\right)^{2n+1}}_{=\sin\left(\frac{\theta}{2}\right)}$$

$$= \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X.$$

Można to bezpośrednio sprawdzić, że dla dowolnej funkcji postaci  $e^{-iAx}$ , zachodzi

$e^{-iAx} = \cos xI - i \sin xA$ , przy założeniach, że  $x \in R$  oraz  $A^2 = I$ , np.,

$$e^{-iAx} = \sum_{n=0}^{\infty} \frac{(-iAx)^n}{n!} = \sum_{k=0}^{\infty} \frac{(-iAx)^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{(-iAx)^{2k+1}}{(2k+1)!} = \sum_{k=0}^{\infty} \frac{(-i)^{2k} x^{2k} I}{(2k)!} + \sum_{k=0}^{\infty} \frac{(-i)^{2k+1} x^{2k+1} A}{(2k+1)!},$$

$$\sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)!} I + \sum_{k=0}^{\infty} \frac{(-1)^{2k} x^{2k+1}}{(2k+1)!} (-i) A = \cos xI - i \sin xA.$$

Zatem, można zapisać nową postać dla każdego z trzech obrotów:

$$R_x(\theta) = e^{-i\frac{\theta}{2}X} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i \sin\left(\frac{\theta}{2}\right) \\ -i \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix},$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix},$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Z =$$



$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) - i \sin\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) + i \sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}.$$

Można ogólniej,

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\bar{\sigma}} = \cos\left(\frac{\theta}{2}\right)I - i \sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z),$$

gdzie  $\hat{n} = (n_x, n_y, n_z)$  jest rzeczywistym wektorem jednostkowym, oraz  $\bar{\sigma} = (X, Y, Z)$  - co odpowiada rotacji wokół dowolnej osi na sferze Blocha.

Można przypomnieć, że np. bramkę Hadamarda można interpretować, jako obrót na sferze o  $\frac{\pi}{2}$  wokół osi y, a potem obrót o  $\pi$  wokół osi x - czyli macierz Hadamarda można zapisać jako złożenie dwóch obrotów,

$$\begin{aligned} R_x(\pi)R_y\left(\frac{\pi}{2}\right) &= \begin{pmatrix} \cos\frac{\pi}{2} & -i\sin\frac{\pi}{2} \\ -i\sin\frac{\pi}{2} & \cos\frac{\pi}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{\pi}{4} & -\sin\frac{\pi}{4} \\ \sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{pmatrix} \\ &= \frac{-i}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \frac{-i}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = -iH. \end{aligned}$$

Zauważmy, że  $-i = e^{i\frac{3}{2}\pi}$ .

Alternatywnie, można wyrazić bramkę Hadamarda jako złożenie obrotu wokół osi z oraz wokół osi x o  $\frac{\pi}{2}$  z dokładnością do globalnego czynnika fazowego,

$$\begin{aligned} R_x\left(\frac{\pi}{2}\right)R_z\left(\frac{\pi}{2}\right) &= \begin{pmatrix} \cos\frac{\pi}{4} & -i\sin\frac{\pi}{4} \\ -i\sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{pmatrix} \left( \cos\frac{\pi}{4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - i \sin\frac{\pi}{4} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right) \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1-i & 0 \\ 0 & 1+i \end{pmatrix} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1-i & -i+1 \\ -i+1 & 1+i \end{pmatrix} = \frac{1}{\sqrt{2}} (1-i) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{(1-i)}{\sqrt{2}} H, \end{aligned}$$





$$\left| \frac{(1-i)}{\sqrt{2}} \right| = \frac{1}{\sqrt{2}} \sqrt{(1+i)(1-i)} = \frac{1}{\sqrt{2}} \sqrt{2} = 1 \Leftrightarrow e^{i\frac{7}{4}\pi}.$$

Oraz podobnie, wykorzystując  $R_y$  i  $R_z$ ,

$$\begin{aligned} R_y\left(\frac{\pi}{2}\right)R_z(\pi) &= \begin{pmatrix} \cos\frac{\pi}{4} & -\sin\frac{\pi}{4} \\ \sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{pmatrix} \left( \cos\frac{\pi}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - i \sin\frac{\pi}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right) \\ &= -i \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = i \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = iH. \end{aligned}$$

Tutaj wykorzystano,  $i = e^{i\frac{\pi}{2}}$ .

Bramkę  $T$ , czyli bramkę  $\frac{\pi}{8}$ , z dokładnością do globalnej fazy, można przedstawić jako:

$$T = R_z\left(\frac{\pi}{4}\right) = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}, \quad e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}.$$

Można teraz uogólnić wprowadzając definicję obrotu wokół dowolnej osi wyznaczonej przez rzeczywisty wektor jednostkowy  $\hat{n} = (n_x, n_y, n_z)$ ,

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\cdot\bar{\sigma}} = \cos\left(\frac{\theta}{2}\right)I - i \sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z),$$

gdzie  $\bar{\sigma} = (X, Y, Z)$ . Dowód przeprowadza się analogicznie jak pokazano wcześniej poprzez rozłożenie w szereg Taylora. Należy tylko zauważyć, że,

$$\begin{aligned} (\hat{n} \cdot \bar{\sigma})^2 &= I, \\ \sigma_i \sigma_j &= i \varepsilon_{ijk} \sigma_k + \delta_{ij} I, \\ n_i n_j (\delta_{ij} I + i \varepsilon_{ijk} \sigma_k) &= n_i n_j \delta_{ij} I + i n_i n_j \varepsilon_{ijk} \sigma_k = n_i n_i I + \underbrace{i n_i n_j \varepsilon_{ijk} \sigma_k}_{=0}. \end{aligned}$$

Załóżmy, że qubit jest w stanie  $\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$  i zadziałał na niego operator obrotu o kąt  $\alpha$  względem osi  $\hat{n}$ , czyli,



$$\begin{aligned}
& \left( \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)(n_x X + n_y Y + n_z Z) \right) \left( \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \right) \\
&= \cos\frac{\alpha}{2}\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\cos\frac{\alpha}{2}\sin\frac{\theta}{2}|1\rangle - i\sin\frac{\alpha}{2}(n_x X + n_y Y + n_z Z)\cos\frac{\theta}{2}|0\rangle + \\
&\quad -ie^{i\varphi}\sin\frac{\alpha}{2}(n_x X + n_y Y + n_z Z)\sin\frac{\theta}{2}|1\rangle \\
&= \cos\frac{\alpha}{2}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}(n_x X|0\rangle + n_y Y|0\rangle + n_z Z|0\rangle) + \\
&\quad -ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}(n_x X|1\rangle + n_y Y|1\rangle + n_z Z|1\rangle) \\
&= \cos\frac{\alpha}{2}\left(\cos\frac{\theta}{2}|0\rangle + \cos\frac{\alpha}{2}e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}(n_x|1\rangle + n_y i|1\rangle + n_z|0\rangle) + \\
&\quad -ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}(n_x|0\rangle - n_y i|0\rangle - n_z|1\rangle) = \\
&\quad \cos\frac{\alpha}{2}\cos\frac{\theta}{2}|0\rangle + \cos\frac{\alpha}{2}e^{i\varphi}\sin\frac{\theta}{2}|1\rangle - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_x|1\rangle - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_y i|1\rangle \\
&\quad -i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_z|0\rangle - ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_x|0\rangle + ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_y i|0\rangle + ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_z|1\rangle \\
&= \left[ \cos\frac{\alpha}{2}\cos\frac{\theta}{2} - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_z - ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_x + ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_y i \right] |0\rangle \\
&\quad + \left[ \cos\frac{\alpha}{2}e^{i\varphi}\sin\frac{\theta}{2} - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_x - i\sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_y i + ie^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_z \right] |1\rangle \\
&= \left[ \cos\frac{\alpha}{2}\cos\frac{\theta}{2} - e^{i\varphi}\sin\frac{\alpha}{2}\sin\frac{\theta}{2}n_y - i\sin\frac{\alpha}{2}\left(\cos\frac{\theta}{2}n_z + e^{i\varphi}\sin\frac{\theta}{2}n_x\right) \right] |0\rangle \\
&\quad + \left[ \cos\frac{\alpha}{2}e^{i\varphi}\sin\frac{\theta}{2} + \sin\frac{\alpha}{2}\cos\frac{\theta}{2}n_y - i\sin\frac{\alpha}{2}\left(\cos\frac{\theta}{2}n_x - e^{i\varphi}\sin\frac{\theta}{2}n_z\right) \right] |1\rangle
\end{aligned}$$

$$(\text{niech } A = \cos\frac{\theta}{2} \text{ a } B = e^{i\varphi}\sin\frac{\theta}{2})$$

$$\begin{aligned}
&= \left[ A\cos\frac{\alpha}{2} - B\sin\frac{\alpha}{2}n_y - i\sin\frac{\alpha}{2}(An_z + Bn_x) \right] |0\rangle \\
&\quad + \left[ B\cos\frac{\alpha}{2} + A\sin\frac{\alpha}{2}n_y - i\sin\frac{\alpha}{2}(An_x - Bn_z) \right] |1\rangle,
\end{aligned}$$

$$A|0\rangle + B|1\rangle \rightarrow$$

$$\begin{aligned}
&\left[ A\cos\frac{\alpha}{2} - B\sin\frac{\alpha}{2}n_y - i\sin\frac{\alpha}{2}(An_z + Bn_x) \right] |0\rangle \\
&\quad + \left[ B\cos\frac{\alpha}{2} + A\sin\frac{\alpha}{2}n_y - i\sin\frac{\alpha}{2}(An_x - Bn_z) \right] |1\rangle,
\end{aligned}$$

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\sigma} = R_x(\alpha)R_y(\beta)R_z(\gamma) = e^{-i\frac{\theta}{2}X} e^{-i\frac{\theta}{2}Y} e^{-i\frac{\theta}{2}Z}.$$



## 12.10. Twierdzenie o przedstawieniu dowolnej operacji jedno-qubitowej za pomocą operatorów obrotu

Dowolny jedno-qubitowy unitarny operator może zostać przedstawiony w postaci:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta),$$

dla ustalonych rzeczywistych parametrów  $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ . (jest to tzw. dekompozycja Z-Y)

$$\begin{aligned} U &= e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix} = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} e^{-i\frac{\beta}{2}} \\ e^{i\frac{\beta}{2}} \sin\frac{\gamma}{2} & e^{i\frac{\beta}{2}} \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix} \\ &= e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} e^{-i\frac{\delta}{2}} \cos\frac{\gamma}{2} & -e^{-i\frac{\beta}{2}} e^{i\frac{\delta}{2}} \sin\frac{\gamma}{2} \\ e^{i\frac{\beta}{2}} e^{-i\frac{\delta}{2}} \sin\frac{\gamma}{2} & e^{i\frac{\beta}{2}} e^{i\frac{\delta}{2}} \cos\frac{\gamma}{2} \end{pmatrix} = \begin{pmatrix} e^{i\left(\alpha - \frac{\beta}{2} - \frac{\delta}{2}\right)} \cos\frac{\gamma}{2} & -e^{i\left(\alpha - \frac{\beta}{2} + \frac{\delta}{2}\right)} \sin\frac{\gamma}{2} \\ e^{i\left(\alpha + \frac{\beta}{2} - \frac{\delta}{2}\right)} \sin\frac{\gamma}{2} & e^{i\left(\alpha + \frac{\beta}{2} + \frac{\delta}{2}\right)} \cos\frac{\gamma}{2} \end{pmatrix}. \end{aligned}$$

Postać macierzy,

$$\begin{pmatrix} e^{i\left(\alpha - \frac{\beta}{2} - \frac{\delta}{2}\right)} \cos\frac{\gamma}{2} & -e^{i\left(\alpha - \frac{\beta}{2} + \frac{\delta}{2}\right)} \sin\frac{\gamma}{2} \\ e^{i\left(\alpha + \frac{\beta}{2} - \frac{\delta}{2}\right)} \sin\frac{\gamma}{2} & e^{i\left(\alpha + \frac{\beta}{2} + \frac{\delta}{2}\right)} \cos\frac{\gamma}{2} \end{pmatrix},$$

wynika, z faktu że dla dowolnej jednostkowej macierzy  $U$ , zawsze można znaleźć takie cztery liczby rzeczywiste  $\alpha, \beta, \gamma, \delta$ , że powyższa reprezentacja będzie poprawna.

Dowód:

$$\begin{aligned} U &= \begin{pmatrix} r_1 e^{i\alpha_1} & r_2 e^{i\alpha_2} \\ r_3 e^{i\alpha_3} & r_4 e^{i\alpha_4} \end{pmatrix}, \quad U^\dagger = \begin{pmatrix} r_1 e^{-i\alpha_1} & r_3 e^{-i\alpha_3} \\ r_2 e^{-i\alpha_2} & r_4 e^{-i\alpha_4} \end{pmatrix} \\ UU^\dagger &= \begin{pmatrix} r_1 e^{i\alpha_1} & r_2 e^{i\alpha_2} \\ r_3 e^{i\alpha_3} & r_4 e^{i\alpha_4} \end{pmatrix} \begin{pmatrix} r_1 e^{-i\alpha_1} & r_3 e^{-i\alpha_3} \\ r_2 e^{-i\alpha_2} & r_4 e^{-i\alpha_4} \end{pmatrix} = I, \quad U^\dagger U = \begin{pmatrix} r_1 e^{-i\alpha_1} & r_3 e^{-i\alpha_3} \\ r_2 e^{-i\alpha_2} & r_4 e^{-i\alpha_4} \end{pmatrix} \begin{pmatrix} r_1 e^{i\alpha_1} & r_2 e^{i\alpha_2} \\ r_3 e^{i\alpha_3} & r_4 e^{i\alpha_4} \end{pmatrix} = I \\ &\Downarrow \\ (1) \begin{cases} r_1^2 + r_3^2 = 1 \\ r_2^2 + r_4^2 = 1 \\ r_1 r_2 e^{i(\alpha_2 - \alpha_1)} + r_3 r_4 e^{i(\alpha_4 - \alpha_3)} = 0 \\ r_1 r_2 e^{i(\alpha_1 - \alpha_2)} + r_3 r_4 e^{i(\alpha_3 - \alpha_4)} = 0 \end{cases}, \quad (2) \begin{cases} r_1^2 + r_2^2 = 1 \\ r_3^2 + r_4^2 = 1 \\ r_1 r_3 e^{i(\alpha_1 - \alpha_3)} + r_2 r_4 e^{i(\alpha_2 - \alpha_4)} = 0 \\ r_1 r_3 e^{i(\alpha_3 - \alpha_1)} + r_2 r_4 e^{i(\alpha_4 - \alpha_2)} = 0 \end{cases} \\ &\Downarrow \end{aligned}$$



$$r_1 = \cos \frac{A}{2}, \quad r_2 = \sin \frac{A}{2}, \quad r_3 = \sin \frac{A}{2}, \quad r_4 = \cos \frac{A}{2},$$

z (1) wynika, że:

$$\begin{cases} \frac{1}{2} \sin A \left( e^{i(\alpha_2 - \alpha_1)} + e^{-i(\alpha_3 - \alpha_4)} \right) = 0 \\ \frac{1}{2} \sin A \left( e^{-i(\alpha_2 - \alpha_1)} + e^{i(\alpha_3 - \alpha_4)} \right) = 0 \end{cases}.$$

Stąd,

$$\begin{aligned} \begin{cases} e^{i(\alpha_2 - \alpha_1)} = a \\ e^{i(\alpha_3 - \alpha_4)} = b \end{cases} &\Rightarrow \begin{cases} a + \frac{1}{b} = 0 \\ b + \frac{1}{a} = 0 \end{cases} \Leftrightarrow ab + 1 = 0 \Rightarrow ab = -1, \\ e^{i(\alpha_2 - \alpha_1 + \alpha_3 - \alpha_4)} &= e^{i\pi} \Rightarrow \alpha_2 - \alpha_1 + \alpha_3 - \alpha_4 = \pi. \end{aligned}$$

Podobnie, z (2),

$$\begin{aligned} \begin{cases} \frac{1}{2} \sin A \left( e^{i(\alpha_1 - \alpha_3)} + e^{-i(\alpha_4 - \alpha_2)} \right) = 0 \\ \frac{1}{2} \sin A \left( e^{-i(\alpha_1 - \alpha_3)} + e^{i(\alpha_4 - \alpha_2)} \right) = 0 \end{cases}, \\ e^{i(\alpha_2 - \alpha_1 + \alpha_3 - \alpha_4)} &= e^{-i\pi} \text{ oraz} \\ \alpha_1 - \alpha_3 + \alpha_4 - \alpha_2 &= -\pi. \end{aligned}$$

Jest to jedno równanie:

$$\alpha_2 - \alpha_1 + \alpha_3 - \alpha_4 = \pi.$$

Istnieją trzy rzeczywiste liczby  $\alpha, \beta, \gamma$ , takie, że,

$$\begin{cases} \alpha_1 = \alpha - \frac{\beta}{2} - \frac{\gamma}{2} \\ \alpha_3 = \alpha + \frac{\beta}{2} - \frac{\gamma}{2}, \\ \alpha_4 = \alpha + \frac{\beta}{2} + \frac{\gamma}{2} \end{cases}$$

oraz  $\alpha_2$  z równania odnalezionego wcześniej.

Ten układ równań posiada nietrywialne rozwiązanie, ponieważ



$$\begin{vmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 1 & \frac{1}{2} & -\frac{1}{2} \\ 1 & \frac{1}{2} & \frac{1}{2} \end{vmatrix} = 1,$$

co kończy dowód.

Istnieje analogiczna reprezentacja dowolnej unitarnej macierzy, ale z wykorzystaniem tylko operatorów  $R_x$  i  $R_y$  (tzw. dekompozycja X-Y). Ogólnie można napisać, że dowolną unitarną macierz  $2 \times 2$  można przedstawić w postaci:

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta),$$

gdzie

$$R_{\hat{m}}(\theta) = e^{-i\frac{\theta}{2}\hat{m}\vec{\sigma}} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(m_x X + m_y Y + m_z Z),$$

oraz  $\hat{m} = (m_x, m_y, m_z)$  jest rzeczywistym wektorem jednostkowym, a  $\vec{\sigma} = (X, Y, Z)$ , oraz

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\vec{\sigma}} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z),$$

gdzie  $\hat{n} = (n_x, n_y, n_z)$  jest rzeczywistym wektorem jednostkowym, ale nierównoległym do  $\hat{m}$ .

Wykorzystując powyższą dekompozycję, można sformułować następujące twierdzenie.

Dla dowolnej unitarnej operacji jednoqubitowej  $U$  istnieją takie trzy operatory jednoqubitowe  $A, B, C$ , że zachodzi związek,

$$ABC = I, \\ U = e^{i\alpha} AXBXC,$$

gdzie  $\alpha$  jest nieistotnym globalnym przesunięciem fazowym.

Dowód:

Niech  $A, B, C$  będą postaci:

$$A = R_z(\beta) R_y\left(\frac{\gamma}{2}\right),$$



$$B = R_y \left( -\frac{\gamma}{2} \right) R_z \left( -\frac{\delta + \beta}{2} \right),$$

$$C = R_z \left( \frac{\delta - \beta}{2} \right).$$

Rozważmy teraz złożenie tych trzech operatorów,

$$\begin{aligned} ABC &= R_z(\beta) R_y \left( \frac{\gamma}{2} \right) R_y \left( -\frac{\gamma}{2} \right) R_z \left( -\frac{\delta + \beta}{2} \right) R_z \left( \frac{\delta - \beta}{2} \right) \\ &= e^{-i\frac{\beta}{2}Z} \underbrace{e^{-i\frac{\gamma}{4}Y} e^{i\frac{\gamma}{4}Y}}_{=I} e^{-i\left(\frac{\delta+\beta}{4}\right)Z} e^{-i\left(\frac{\delta-\beta}{4}\right)Z} = e^{-i\frac{\beta}{2}Z} e^{i\left(\frac{\delta+\beta}{4}\right)Z} e^{i\left(\frac{\delta-\beta}{4}\right)Z} \\ &= e^{-i\frac{\beta}{2}Z} e^{i\frac{\delta}{4}Z} e^{i\frac{\beta}{4}Z} e^{-i\frac{\delta}{4}Z} e^{i\frac{\beta}{4}Z} = e^{i\left(-\frac{\beta}{2} + \frac{\delta}{4} + \frac{\beta}{4} - \frac{\delta}{4} + \frac{\beta}{4}\right)Z} = I. \end{aligned}$$

Można także pokazać, że

$$\begin{aligned} XR_y(\theta)X &= R_y(-\theta), \\ X \left( \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Y \right) X &= \cos \frac{\theta}{2} XIX - i \sin \frac{\theta}{2} XYX = \cos \left( \frac{\theta}{2} \right) I - i \sin \left( \frac{\theta}{2} \right) XYX, \\ XYX &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = -Y, \\ \cos \left( -\frac{\theta}{2} \right) I - i \sin \left( -\frac{\theta}{2} \right) Y &= R_y(-\theta). \end{aligned}$$

A ogólniej,

$$XBX = XR_y \left( -\frac{\gamma}{2} \right) \underbrace{I}_{=XX} R_z \left( -\frac{\delta + \beta}{2} \right) X = XR_y \left( -\frac{\gamma}{2} \right) XX \left( -\frac{\delta + \beta}{2} \right) X = R_y \left( \frac{\gamma}{2} \right) R_z \left( \frac{\delta + \beta}{2} \right).$$

Korzystając z powyższego można napisać,

$$AXBXC = R_z(\beta) R_y \left( \frac{\gamma}{2} \right) R_y \left( \frac{\gamma}{2} \right) R_z \left( \frac{\delta + \beta}{2} \right) R_z \left( \frac{\delta - \beta}{2} \right) = R_z(\beta) R_y(\gamma) R_z(\delta).$$

Zatem,

$$e^{i\varphi} AXBXC = e^{i\varphi} R_z(\beta) R_y(\gamma) R_z(\delta) = U,$$

co kończy dowód.

Dla przykładu można podać wartości współczynników dla dekompozycji Z-Y bramki Hadamarda,



$$H = e^{i\frac{\pi}{2}} R_z(0) R_y\left(\frac{\pi}{2}\right) R_z(\pi).$$

Można także odszukać odpowiednie macierze A,B,C,

$$H = e^{i\frac{\pi}{2}} R_z(0) R_y\left(\frac{\pi}{2}\right) R_z(\pi) = e^{i\frac{\pi}{2}} R_z(0) \underbrace{X R_y\left(-\frac{\pi}{2}\right) X}_{=R_y\left(\frac{\pi}{2}\right)} R_z(\pi),$$

$$A = R_z(0),$$

$$B = R_y\left(-\frac{\pi}{2}\right),$$

$$C = R_z(\pi),$$

$$\alpha = \frac{\pi}{2}.$$

Warto wspomnieć także o prostych tożsamościach, które są pomocne przy obliczeniach na bramkach kwantowych,

Cccccf m

$$HXH = Z,$$

$$HYH = -Y,$$

$$HZH = X,$$

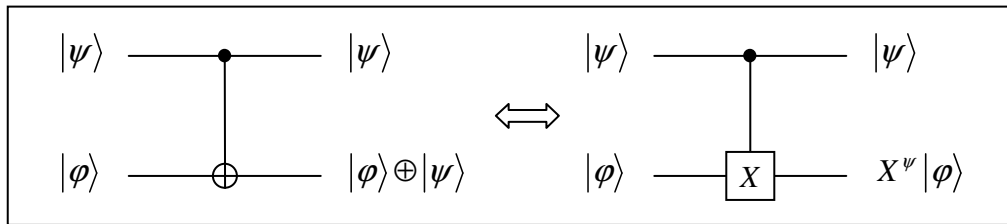
$$HTH = R_x\left(\frac{\pi}{4}\right), \text{ z dokładnością do przesunięcia fazowego.}$$

## 13. Bramki wielo-qubitowe

Zasadniczą własnością macierzy unitarnych, umożliwiającą rozważanie kwantowych programów, jest możliwość dokonania dekompozycji dowolnej wielowymiarowej unitarnej ewolucji na proste elementarne składowe, których wykonanie kolejno w czasie byłoby ekwiwalentne wykonaniu całościowej operacji. Okazuje się, że wystarczy w tym celu wykorzystać jednoqubitowe operacje oraz jedną uniwersalną bramkę dwuqubitową. Wybór uniwersalnej bramki jest dowolny. Często, jako taką bramkę wybiera się bramkę kontrolowanej negacji *CNOT* (*controlled-NOT*).

### 13.1. Bramka kontrolowanej negacji (CNOT)

Bramkę *CNOT* można rozpatrywać jako unitarną operację na dwóch qubitach – qubicie kontrolnym (control qubit) oraz qubicie docelowym (target qubit). Prezentacja graficzna bramki *CNOT* przedstawiona została poniżej,



Górna linia reprezentuje qubit kontrolny, dolna reprezentuje qubit docelowy, znak  $\oplus$  - suma modulo 2.

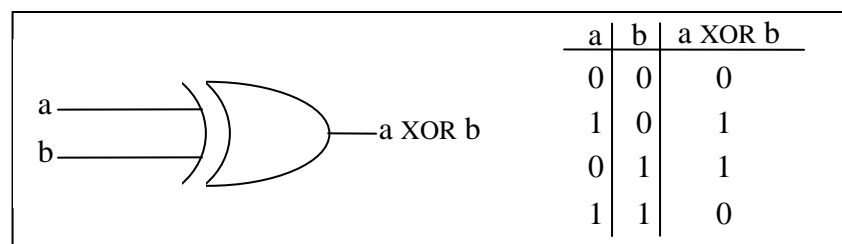
Działanie bramki *CNOT* na stany qubitów kontrolnego i docelowego z bazy obliczeniowej  $\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\}$  wygląda następująco:

- jeżeli qubit kontrolny znajduje się w stanie  $|0\rangle$ , to stan qubit docelowego nie ulega zmianie;
- jeżeli qubit kontrolny znajduje się w stanie  $|1\rangle$ , to stan qubit docelowego zmieni się na przeciwny.

Można to zapisać w postaci:

$$\begin{aligned} |0\rangle \otimes |0\rangle &\xrightarrow{CNOT} |0\rangle \otimes |0\rangle, \\ |0\rangle \otimes |1\rangle &\xrightarrow{CNOT} |0\rangle \otimes |1\rangle, \\ |1\rangle \otimes |0\rangle &\xrightarrow{CNOT} |1\rangle \otimes |1\rangle, \\ |1\rangle \otimes |1\rangle &\xrightarrow{CNOT} |1\rangle \otimes |0\rangle. \end{aligned}$$

Można także bramkę *CNOT* interpretować w odniesieniu do klasycznej operacji logicznej *XOR*. Bramka *XOR* jest klasyczną bramką dwubitową, zdefiniowaną następująco:



Bramka *CNOT* jest pewnym uogólnieniem klasycznej bramki *XOR* (kwantowe bramki działają nie tylko na stany z bazy, ale także na pełny iloczyn tensorowy przestrzeni Hilberta, w wyniku liniowości; bramka klasyczna zdefiniowana jest wyłącznie na dyskretnym zbiorze logicznych wartości bitów). Wynik działania bramki *CNOT*, podobnie jak bramki *XOR* sprowadza się do sumy modulo 2 ( $\oplus$ ), co ma sens wyłącznie w stosunku do stanów bazowych (w przypadku bramki kwantowej). Dla wektorów z bazy obliczeniowej można zapisać,





$$|\psi\rangle \otimes |\varphi\rangle \xrightarrow{CNOT} |\psi\rangle \otimes (|\varphi\rangle \oplus |\psi\rangle).$$

Operację unitarną  $CNOT$  można przedstawić jako czterowymiarową unitarną macierz,

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Można pokazać, że powyższa macierz jest unitarna,

$$U_{CNOT} U_{CNOT}^+ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I = U_{CNOT}^+ U_{CNOT}.$$

Macierz  $U_{CNOT}$  jest także hermitowska (jest macierzą rzeczywistą i symetryczną), czyli  $U_{CNOT} = U_{CNOT}^+$ . Z równoczesnej hermitowskości i unitarności wynika, że macierz odwrotna jest tą samą macierzą (czyli  $CNOT^2 = I$ ).

Iloczyn tensorowy dwóch qubitów jest opisany przez czterovektor w bazie obliczeniowej iloczynu tensorowego przestrzeni układów dwóch qubitów,  $\{|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2\}$  i można go zapisać następująco:

$$\begin{aligned} & (\alpha_1 |0\rangle_1 + \beta_1 |1\rangle_1) \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) \\ &= \alpha_1 \alpha_2 |0\rangle_1 \otimes |0\rangle_2 + \alpha_1 \beta_2 |0\rangle_1 \otimes |1\rangle_2 + \beta_1 \alpha_2 |1\rangle_1 \otimes |0\rangle_2 + \beta_1 \beta_2 |1\rangle_1 \otimes |1\rangle_2 \\ & \quad \updownarrow \\ & \left. \begin{aligned} \alpha_1 |0\rangle_1 \otimes \alpha_2 |0\rangle_2 &= \alpha_1 \alpha_2 |0\rangle_1 \otimes |0\rangle_2 \Leftrightarrow \begin{bmatrix} \alpha_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \alpha_2 \\ \beta_1 \beta_2 \end{bmatrix} \\ \alpha_1 |0\rangle_1 \otimes \beta_2 |1\rangle_2 &= \alpha_1 \beta_2 |0\rangle_1 \otimes |1\rangle_2 \Leftrightarrow \alpha_1 \beta_2 \\ \beta_1 |1\rangle_1 \otimes \alpha_2 |0\rangle_2 &= \beta_1 \alpha_2 |1\rangle_1 \otimes |0\rangle_2 \Leftrightarrow \beta_1 \alpha_2 \\ \beta_1 |1\rangle_1 \otimes \beta_2 |1\rangle_2 &= \beta_1 \beta_2 |1\rangle_1 \otimes |1\rangle_2 \Leftrightarrow \beta_1 \beta_2 \end{aligned} \right\} \end{aligned}$$

Baza tensorowa dla dwóch qubitów może zostać przedstawiona wektorami,

$$|0\rangle_1 \otimes |0\rangle_2 \Leftrightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |0\rangle_1 \otimes |1\rangle_2 \Leftrightarrow \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |1\rangle_1 \otimes |0\rangle_2 \Leftrightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |1\rangle_1 \otimes |1\rangle_2 \Leftrightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$



Można teraz zapisać sposób działania bramki  $CNOT$  na powyżej zdefiniowane stany bazy iloczynu tensorowego. Działanie na stan  $|0\rangle_1 \otimes |0\rangle_2$ :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Leftrightarrow |0\rangle_1 \otimes |0\rangle_2.$$

Działanie na stan  $|0\rangle_1 \otimes |1\rangle_2$ :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \Leftrightarrow |0\rangle_1 \otimes |1\rangle_2.$$

Działanie na stan  $|1\rangle_1 \otimes |0\rangle_2$ :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \Leftrightarrow |1\rangle_1 \otimes |1\rangle_2.$$

Działanie na stan  $|1\rangle_1 \otimes |0\rangle_2$ :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \Leftrightarrow |1\rangle_1 \otimes |0\rangle_2.$$

Działanie macierzy  $4 \times 4$  na wektory bazy obliczeniowej  $\{|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2\}$  układu dwóch qubitów jest zadane przez kolumny macierzy. Kolejne kolumny macierzy odpowiadają działaniu macierzy na kolejne wektory bazy. W przypadku, gdy rozpatrywany jest dowolny dwu-qubitowy stan, będący liniową kombinacją wektorów bazy iloczynu tensorowego, wyniki dla poszczególnych elementów bazy są mnożone przez odpowiednie współczynniki i sumowane.

Dla stanu  $(\alpha_1|0\rangle_1 + \beta_1|1\rangle_1) \otimes (\alpha_2|0\rangle_2 + \beta_2|1\rangle_2)$  można zapisać:



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} \alpha_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \alpha_2 \\ \beta_1 \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \beta_2 \\ \beta_1 \alpha_2 \end{bmatrix}$$

$$= \alpha_1 \alpha_2 |0\rangle_1 \otimes |0\rangle_2 + \alpha_1 \beta_2 |0\rangle_1 \otimes |1\rangle_2 + \beta_1 \beta_2 |1\rangle_1 \otimes |0\rangle_2 + \beta_1 \alpha_2 |1\rangle_1 \otimes |1\rangle_2$$

$$= \alpha_1 |0\rangle_1 \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) + \beta_1 |1\rangle_1 \otimes (\beta_2 |0\rangle_2 + \alpha_2 |1\rangle_2).$$

W ogólnym przypadku stan końcowy nie jest stanem separowalnym (w odróżnieniu od początkowego stanu). Jest to zobrazowanie bramki wprowadzającej splątanie (w rzeczywistości splątanie powodowane jest między-qubitowym oddziaływaniem). Gdy  $\alpha_1 = 1, \beta_1 = 0$ , wtedy stan qubitów docelowego nie ulega zmianie, natomiast gdy  $\alpha_1 = 0, \beta_1 = 1$ , stan qubitów docelowego działa jednoqubitowa bramka negacji (bramka Pualiego  $X$ ), zmieniając miejscami współczynniki,

$$\beta_2 |0\rangle_2 + \alpha_2 |1\rangle_2 = X (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2),$$

Zatem, bramkę  $CNOT$  można zapisać w następującej postaci:

$$\begin{pmatrix} I_{2 \times 2} & 0 & 0 \\ 0 & 0 & X \\ 0 & 0 & 0 \end{pmatrix}.$$

Oraz dla dowolnych stanów:

$$|\psi\rangle \otimes |\varphi\rangle \xrightarrow{CNOT} |\psi\rangle \otimes X^\psi |\varphi\rangle.$$

## 13.2. Układ kopiujący

Pomimo tego, że twierdzenie No-cloning wskazuje na brak możliwości kopiowania nieznanego stanu kwantowego, można rozważyć układ kopiujący wykorzystując przedstawioną powyżej bramkę w celu zilustrowania twierdzenia No-cloning.

Dla stanu qubitów docelowego  $|0\rangle$  oraz dla stanu qubitów kontrolnego  $\alpha|0\rangle + \beta|1\rangle$  (dowolny nieznanany stan kwantowy), działanie bramki  $CNOT$  można zapisać następująco:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |0\rangle)$$

$$\xrightarrow{CNOT} \alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |1\rangle).$$



Jak widać, otrzymany wynik końcowy nie jest iloczynem tensorowym dwóch identycznych nieznanych stanów, tak jak by należało oczekiwać od procesu kopiowania:

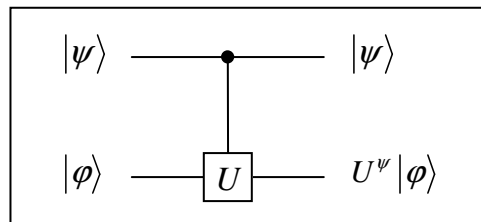
$$\alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |1\rangle) \neq \alpha^2(|0\rangle \otimes |0\rangle) + \alpha\beta(|0\rangle \otimes |1\rangle) + \beta\alpha(|1\rangle \otimes |0\rangle) + \beta^2(|1\rangle \otimes |1\rangle).$$

Jednakże, powyższe równanie jest spełnione dla  $\alpha = 1, \beta = 0$  lub  $\alpha = 0, \beta = 1$ , co pozostaje w zgodzie z możliwością kopiowania znanych stanów (zgodnie z twierdzeniem No-cloning). Posługując się macierzowym zapisem można zapisać działanie dla stanu wejściowego  $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle$ ,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix}, \text{ ale oczekiwany wynik procedury kopiowania jest postaci: } \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \beta\alpha \\ \beta^2 \end{bmatrix}.$$

### 13.3. Bramka kontrolowanej operacji $U$

Można podać ogólną postać dowolnej dwu-qubitowej bramki kontrolowanej. Dwu-qubitowa kontrolowana operacja  $U$  może być rozumiana, jako dwu-qubitowa bramka z qubitem kontrolującym działanie jedno-qubitowej operacji  $U$  na qubicie docelowym. Jeżeli qubit kontrolny jest w stanie state  $|1\rangle$ , wtedy operacja  $U$  jest stosowana na qubicie docelowym. Gdy qubit kontrolny jest w stanie  $|0\rangle$  stan qubitu docelowego nie ulega zmianie. Graficznie bramka kontrolowanej operacji  $U$  ma postać:

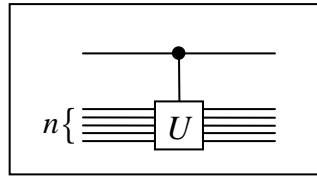


gdzie  $U^\psi$  oznacza operację  $U$  gdy  $\psi$  jest stanem  $|1\rangle$ , oraz  $U^\psi = I$ , w przypadku gdy  $\psi$  jest stanem  $|0\rangle$ . W ogólnym przypadku, można zapisać  $|\psi\rangle \otimes |\phi\rangle \xrightarrow{\text{controlled-}U} |\psi\rangle \otimes U^\psi |\phi\rangle$ , lub podać postać macierzową bramki kontrolowanej operacji  $U$ :

$$U_{\text{controlled-}U} = \begin{pmatrix} I_{2 \times 2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & U \end{pmatrix}.$$

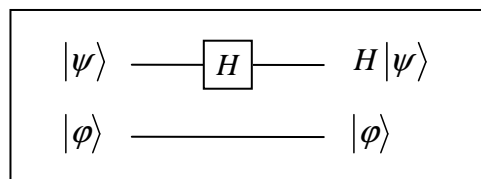


Można także uogólnić operacje kontrolowaną  $U$  na operację  $n$ -qubitową, czyli,

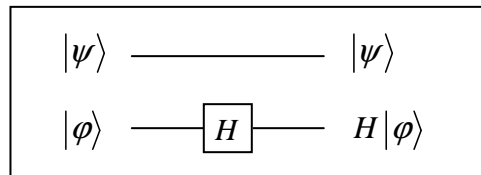


Kolejnym krokiem jest reprezentacja dowolnej dwuqubitowej operacji.

Przykładowo można rozważyć dwa przypadki:



oraz



Pierwszy przypadek można opisać w następujący sposób,

$$|\psi\rangle \otimes |\phi\rangle \rightarrow H|\psi\rangle \otimes |\phi\rangle.$$

Działanie tej operacji można przedstawić także jako,

$$H|\psi\rangle \otimes I|\phi\rangle = (H \otimes I)(|\psi\rangle \otimes |\phi\rangle).$$

Macierz  $H \otimes I$  ma postać:

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \cdot I & 1 \cdot I \\ 1 \cdot I & -1 \cdot I \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

W drugim przypadku operacja jest postaci:

$$|\psi\rangle \otimes |\phi\rangle \rightarrow |\psi\rangle \otimes H|\phi\rangle = (I \otimes H)(|\psi\rangle \otimes |\phi\rangle).$$



A odpowiadająca jej macierz:

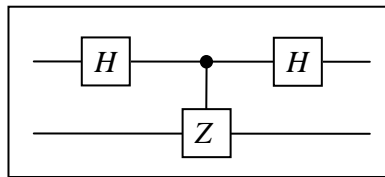
$$I \otimes H = \begin{pmatrix} 1 \cdot H & 0 \cdot H \\ 0 \cdot H & 1 \cdot H \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Można teraz spróbować skonstruować bramkę *CNOT* za pomocą kontrolowanej bramki *Z* :

$$U_{\text{controlled-Z}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

oraz dwóch bramek Hadamarda *H* .

Rozważmy następujący układ:



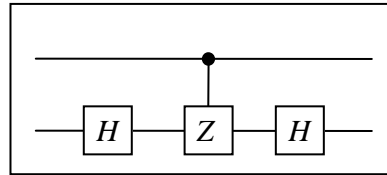
Działanie powyższego układu bramek jest następujące,

$$(H \otimes I)(U_{\text{controlled-Z}})(H \otimes I)(|\psi\rangle \otimes |\phi\rangle).$$

Można sprawdzić czy  $(H \otimes I)(U_{\text{controlled-Z}})(H \otimes I) \stackrel{?}{=} U_{\text{CNOT}}$  . W reprezentacji macierzowej:

$$\begin{aligned} & \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Wynik nie odpowiada macierzy  $CNOT$ . Okazuje się jednak, że jest to bramka kontrolowanej negacji, ale z zamienionymi qubitami kontrolnym oraz docelowym. Dlatego teraz rozważmy inny układ bramek:



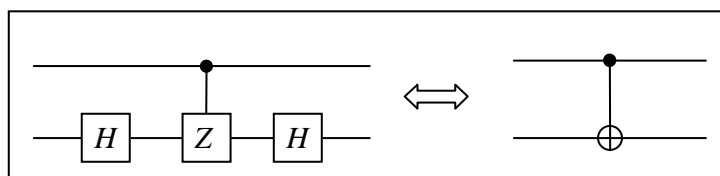
Dla tego układu można zapisać:

$$(I \otimes H)(U_{\text{controlled-Z}})(I \otimes H)(|\psi\rangle \otimes |\varphi\rangle).$$

Ponownie sprawdzamy, czy  $(I \otimes H)(U_{\text{controlled-Z}})(I \otimes H) \stackrel{?}{=} U_{CNOT}$ ,

$$\begin{aligned} & \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \end{aligned}$$

Wynik wskazuje, że rozważany układ bramek jest tożsamy z bramką  $CNOT$ , czyli,



### 13.4. Działanie bramki $CNOT$ na macierz gęstości układu dwóch qubitów

Macierz gęstości spełnia następujące warunki:

$$\rho_A^\dagger = \rho_A \text{ - warunek hermitowskości}$$

$$\text{Tr} \rho_A = 1 \text{ - warunek normalizacji}$$

$$\langle \psi | \rho_A | \psi \rangle \geq 0 \text{ - warunek dodatniej określoności}$$

Macierz gęstości dla stanu czystego,



$$\hat{\rho}_A = |\psi\rangle\langle\psi|,$$

jest operatorem rzutowania na ten stan.

Dla stanu czystego pary qubitów można zapisać:

$$\begin{aligned} |\psi\rangle_{AB} &= \sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B, \\ \hat{\rho}_{AB} &= |\psi\rangle_{AB} \langle\psi|_{AB} = \sum_{i,j} \sum_{p,q} c_{ij} c_{pq}^* |i\rangle_A \otimes |j\rangle_B \langle p|_A \otimes \langle q|_B \\ &= \sum_{i,j} \sum_{p,q} c_{ij} c_{pq}^* (|i\rangle_A \langle p|_A) \otimes (|j\rangle_B \langle q|_B). \end{aligned}$$

Pojedynczy qubit ogólności nie jest jednak w stanie czystym i odpowiadająca mu stan mieszany jest opisany przez następującą macierz gęstości:

$$\begin{aligned} \hat{\rho}_A &= Tr_B \hat{\rho}_{AB} \\ Tr_B \hat{\rho}_{AB} &= \sum_n \langle n|_B \hat{\rho}_{AB} |n\rangle_B = \sum_{i,j,p,q,n} c_{ij} c_{pq}^* |i\rangle_A \langle p|_A \underbrace{\langle n|_B |j\rangle_B}_{=\delta_{nj}} \underbrace{\langle q|_B |n\rangle_B}_{=\delta_{qn}} \\ &= \sum_{i,n,p} c_{in} c_{pn}^* |i\rangle_A \langle p|_A = \sum_{i,n,p} c_{ipn} |i\rangle_A \langle p|_A. \end{aligned}$$

Przypomnijmy, że dla stanu czystego było:

$$\begin{aligned} \hat{\rho}_A &= |\psi\rangle_A \langle\psi|_A = \sum_{i,j} c_i c_j^* |i\rangle_A \langle j|_A \\ |\psi\rangle_A &= \sum_i c_i |i\rangle_A. \end{aligned}$$

Macierz gęstości qubitu w stanie czystym ma następującą strukturę:

$$\hat{\rho} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix} \Leftrightarrow \alpha_1 |0\rangle\langle 0| + \alpha_2 |0\rangle\langle 1| + \alpha_3 |1\rangle\langle 0| + \alpha_4 |1\rangle\langle 1|.$$

Dla stanu mieszanego,

$$\hat{\rho}_A = Tr_B \hat{\rho}_{AB} = \sum_{i,n,p} c_{in} c_{pn}^* |i\rangle_A \langle p|_A.$$

Łatwo jest sprawdzić własności macierzy gęstości,

$${}_A \langle\psi| \hat{\rho}_A |\psi\rangle_A = {}_A \langle\psi| \left( \sum_{i,n,p} c_{in} c_{pn}^* |i\rangle_A \langle p|_A \right) |\psi\rangle_A = \sum_n \left| \sum_i c_{in} \langle\psi|i\rangle_A \right|^2 \geq 0$$





$$\text{Tr}_A \hat{\rho}_A = \sum_k \langle k | \left( \sum_{i,n,p} c_{in} a_{np}^* |i\rangle_{AA} \langle p| \right) |k\rangle_A = \sum_{kn} |a_{kn}|^2 = 1 \Leftrightarrow \text{normalizacja } |\psi\rangle_{AB}$$

Dla dwukubitowej macierzy gęstości można napisać:

$$\begin{aligned} \hat{\rho}_{12} &= \left[ \alpha_1 \alpha_2 (|0\rangle_1 \otimes |0\rangle_2) + \alpha_1 \beta_2 (|0\rangle_1 \otimes |1\rangle_2) + \beta_1 \alpha_2 (|1\rangle_1 \otimes |0\rangle_2) + \beta_1 \beta_2 (|1\rangle_1 \otimes |1\rangle_2) \right] \\ &\left[ \alpha_1^* \alpha_2^* ({}_1\langle 0| \otimes {}_2\langle 0|) + \alpha_1^* \beta_2^* ({}_1\langle 0| \otimes {}_2\langle 1|) + \beta_1^* \alpha_2^* ({}_1\langle 1| \otimes {}_2\langle 0|) + \beta_1^* \beta_2^* ({}_1\langle 1| \otimes {}_2\langle 1|) \right] \\ &= \alpha_1 \alpha_2 \alpha_1^* \alpha_2^* (|0\rangle_{11} \langle 0|) \otimes (|0\rangle_{22} \langle 0|) + \alpha_1 \alpha_2 \alpha_1^* \beta_2^* (|0\rangle_{11} \langle 0|) \otimes (|0\rangle_{22} \langle 1|) \\ &+ \alpha_1 \alpha_2 \beta_1^* \alpha_2^* (|0\rangle_{11} \langle 1|) \otimes (|0\rangle_{22} \langle 0|) + \alpha_1 \alpha_2 \beta_1^* \beta_2^* (|0\rangle_{11} \langle 1|) \otimes (|0\rangle_{22} \langle 1|) \\ &+ \alpha_1 \beta_2 \alpha_1^* \alpha_2^* (|0\rangle_{11} \langle 0|) \otimes (|1\rangle_{22} \langle 0|) + \alpha_1 \beta_2 \alpha_1^* \beta_2^* (|0\rangle_{11} \langle 0|) \otimes (|1\rangle_{22} \langle 1|) \\ &+ \alpha_1 \beta_2 \beta_1^* \alpha_2^* (|0\rangle_{11} \langle 1|) \otimes (|1\rangle_{22} \langle 0|) + \alpha_1 \beta_2 \beta_1^* \beta_2^* (|0\rangle_{11} \langle 1|) \otimes (|1\rangle_{22} \langle 1|) \\ &+ \beta_1 \alpha_2 \alpha_1^* \alpha_2^* (|1\rangle_{11} \langle 0|) \otimes (|0\rangle_{22} \langle 0|) + \beta_1 \alpha_2 \alpha_1^* \beta_2^* (|1\rangle_{11} \langle 0|) \otimes (|0\rangle_{22} \langle 1|) \\ &+ \beta_1 \alpha_2 \beta_1^* \alpha_2^* (|1\rangle_{11} \langle 1|) \otimes (|0\rangle_{22} \langle 0|) + \beta_1 \alpha_2 \beta_1^* \beta_2^* (|1\rangle_{11} \langle 1|) \otimes (|0\rangle_{22} \langle 1|) \\ &+ \beta_1 \beta_2 \alpha_1^* \alpha_2^* (|1\rangle_{11} \langle 0|) \otimes (|1\rangle_{22} \langle 0|) + \beta_1 \beta_2 \alpha_1^* \beta_2^* (|1\rangle_{11} \langle 0|) \otimes (|1\rangle_{22} \langle 1|) \\ &+ \beta_1 \beta_2 \beta_1^* \alpha_2^* (|1\rangle_{11} \langle 1|) \otimes (|1\rangle_{22} \langle 0|) + \beta_1 \beta_2 \beta_1^* \beta_2^* (|1\rangle_{11} \langle 1|) \otimes (|1\rangle_{22} \langle 1|) \end{aligned}$$

Lub w postaci macierzowej,

$$\begin{aligned} \hat{\rho}_{12} &= \begin{pmatrix} \alpha_1 \alpha_2 \alpha_1^* \alpha_2^* & \alpha_1 \alpha_2 \alpha_1^* \beta_2^* & \alpha_1 \alpha_2 \beta_1^* \alpha_2^* & \alpha_1 \alpha_2 \beta_1^* \beta_2^* \\ \alpha_1 \beta_2 \alpha_1^* \alpha_2^* & \alpha_1 \beta_2 \alpha_1^* \beta_2^* & \alpha_1 \beta_2 \beta_1^* \alpha_2^* & \alpha_1 \beta_2 \beta_1^* \beta_2^* \\ \beta_1 \alpha_2 \alpha_1^* \alpha_2^* & \beta_1 \alpha_2 \alpha_1^* \beta_2^* & \beta_1 \alpha_2 \beta_1^* \alpha_2^* & \beta_1 \alpha_2 \beta_1^* \beta_2^* \\ \beta_1 \beta_2 \alpha_1^* \alpha_2^* & \beta_1 \beta_2 \alpha_1^* \beta_2^* & \beta_1 \beta_2 \beta_1^* \alpha_2^* & \beta_1 \beta_2 \beta_1^* \beta_2^* \end{pmatrix} \\ &= \begin{pmatrix} |\alpha_1|^2 |\alpha_2|^2 & |\alpha_1|^2 \alpha_2 \beta_2^* & \alpha_1 \beta_1^* |\alpha_2|^2 & \alpha_1 \alpha_2 \beta_1^* \beta_2^* \\ |\alpha_1|^2 \beta_2 \alpha_2^* & |\alpha_1|^2 |\beta_2|^2 & \alpha_1 \beta_1^* \beta_2 \alpha_2^* & \alpha_1 \beta_1^* |\beta_2|^2 \\ \alpha_1^* \beta_1 |\alpha_2|^2 & \alpha_1^* \beta_1 \alpha_2 \beta_2^* & |\beta_1|^2 |\alpha_2|^2 & |\beta_1|^2 \alpha_2 \beta_2^* \\ \alpha_1^* \beta_1 \alpha_2^* \beta_2 & \alpha_1^* \beta_1 |\beta_2|^2 & |\beta_1|^2 \alpha_2^* \beta_2 & |\beta_1|^2 |\beta_2|^2 \end{pmatrix}. \end{aligned}$$

Złożenie macierzy *CNOT* wraz z macierzą gęstości można wyrazić w następujący sposób:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} |\alpha_1|^2 |\alpha_2|^2 & |\alpha_1|^2 \alpha_2 \beta_2^* & \alpha_1 \beta_1^* |\alpha_2|^2 & \alpha_1 \alpha_2 \beta_1^* \beta_2^* \\ |\alpha_1|^2 \beta_2 \alpha_2^* & |\alpha_1|^2 |\beta_2|^2 & \alpha_1 \beta_1^* \beta_2 \alpha_2^* & \alpha_1 \beta_1^* |\beta_2|^2 \\ \alpha_1^* \beta_1 |\alpha_2|^2 & \alpha_1^* \beta_1 \alpha_2 \beta_2^* & |\beta_1|^2 |\alpha_2|^2 & |\beta_1|^2 \alpha_2 \beta_2^* \\ \alpha_1^* \beta_1 \alpha_2^* \beta_2 & \alpha_1^* \beta_1 |\beta_2|^2 & |\beta_1|^2 \alpha_2^* \beta_2 & |\beta_1|^2 |\beta_2|^2 \end{pmatrix}$$



$$= \begin{pmatrix} |\alpha_1|^2 |\alpha_2|^2 & |\alpha_1|^2 \alpha_2 \beta_2^* & \alpha_1 \beta_1^* |\alpha_2|^2 & \alpha_1 \alpha_2 \beta_1^* \beta_2^* \\ |\alpha_1|^2 \beta_2 \alpha_2^* & |\alpha_1|^2 |\beta_2|^2 & \alpha_1 \beta_1^* \beta_2 \alpha_2^* & \alpha_1 \beta_1^* |\beta_2|^2 \\ \alpha_1^* \beta_1 \alpha_2^* \beta_2 & \alpha_1^* \beta_1 |\beta_2|^2 & |\beta_1|^2 \alpha_2^* \beta_2 & |\beta_1|^2 |\beta_2|^2 \\ \alpha_1^* \beta_1 |\alpha_2|^2 & \alpha_1^* \beta_1 \alpha_2 \beta_2^* & |\beta_1|^2 |\alpha_2|^2 & |\beta_1|^2 \alpha_2 \beta_2^* \end{pmatrix}.$$

Można zauważyć, iloczyn macierzy *CNOT* z macierzą gęstości sprowadza się do wzajemnej zamiany rzędów 3 i 4 w macierzy gęstości.

Dla dowolnej transformacji unitarnej  $U$  (w ogólnym przypadku, odpowiadającej zmianie bazy przestrzeni), można zapisać,

$$\begin{aligned} Ax &= y, \\ Uy &= y' \Rightarrow y = U^{-1} y', \\ Ux &= x' \Rightarrow x = U^{-1} x', \\ AU^{-1} x' &= U^{-1} y' \Rightarrow UAU^{-1} x' = y' \Rightarrow A' x' = y'. \end{aligned}$$

Można taką transformację *CNOT* zastosować do macierzy gęstości:

$$\begin{aligned} \hat{\rho}'_{AB} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} |\alpha_1|^2 |\alpha_2|^2 & |\alpha_1|^2 \alpha_2 \beta_2^* & \alpha_1 \beta_1^* |\alpha_2|^2 & \alpha_1 \alpha_2 \beta_1^* \beta_2^* \\ |\alpha_1|^2 \beta_2 \alpha_2^* & |\alpha_1|^2 |\beta_2|^2 & \alpha_1 \beta_1^* \beta_2 \alpha_2^* & \alpha_1 \beta_1^* |\beta_2|^2 \\ \alpha_1^* \beta_1 |\alpha_2|^2 & \alpha_1^* \beta_1 \alpha_2 \beta_2^* & |\beta_1|^2 |\alpha_2|^2 & |\beta_1|^2 \alpha_2 \beta_2^* \\ \alpha_1^* \beta_1 \alpha_2^* \beta_2 & \alpha_1^* \beta_1 |\beta_2|^2 & |\beta_1|^2 \alpha_2^* \beta_2 & |\beta_1|^2 |\beta_2|^2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} |\alpha_1|^2 |\alpha_2|^2 & |\alpha_1|^2 \alpha_2 \beta_2^* & \alpha_1 \beta_1^* |\alpha_2|^2 & \alpha_1 \alpha_2 \beta_1^* \beta_2^* \\ |\alpha_1|^2 \beta_2 \alpha_2^* & |\alpha_1|^2 |\beta_2|^2 & \alpha_1 \beta_1^* \beta_2 \alpha_2^* & \alpha_1 \beta_1^* |\beta_2|^2 \\ \alpha_1^* \beta_1 \alpha_2^* \beta_2 & \alpha_1^* \beta_1 |\beta_2|^2 & |\beta_1|^2 \alpha_2^* \beta_2 & |\beta_1|^2 |\beta_2|^2 \\ \alpha_1^* \beta_1 |\alpha_2|^2 & \alpha_1^* \beta_1 \alpha_2 \beta_2^* & |\beta_1|^2 |\alpha_2|^2 & |\beta_1|^2 \alpha_2 \beta_2^* \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} |\alpha_1|^2 |\alpha_2|^2 & |\alpha_1|^2 \alpha_2 \beta_2^* & \alpha_1 \alpha_2 \beta_1^* \beta_2^* & \alpha_1 \beta_1^* |\alpha_2|^2 \\ |\alpha_1|^2 \beta_2 \alpha_2^* & |\alpha_1|^2 |\beta_2|^2 & \alpha_1 \beta_1^* |\beta_2|^2 & \alpha_1 \beta_1^* \beta_2 \alpha_2^* \\ \alpha_1^* \beta_1 \alpha_2^* \beta_2 & \alpha_1^* \beta_1 |\beta_2|^2 & |\beta_1|^2 |\beta_2|^2 & |\beta_1|^2 \alpha_2^* \beta_2 \\ \alpha_1^* \beta_1 |\alpha_2|^2 & \alpha_1^* \beta_1 \alpha_2 \beta_2^* & |\beta_1|^2 |\alpha_2|^2 & |\beta_1|^2 \alpha_2 \beta_2^* \end{pmatrix}. \end{aligned}$$

Należy podkreślić, że przedstawiony powyżej opis bramek podany był w bazie obliczeniowej. W przypadku wyboru dowolnej innej bazy, działanie bramek (np. działanie *CNOT*) będzie raczej nieintuicyjne. W szczególności, w przypadku *CNOT* stan qubit kontrolnego nie ulega zmianie tylko w przypadku bazy obliczeniowej. Aby to zobrazować, przyjmijmy poniższą postać bazy:



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

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

Oraz dla układów dwu-qubitowych:

$$|+\rangle \otimes |+\rangle = \left( \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \right) \otimes \left( \frac{|0\rangle_2 + |1\rangle_2}{\sqrt{2}} \right) \Rightarrow \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix},$$

$$|-\rangle \otimes |+\rangle = \left( \frac{|0\rangle_1 - |1\rangle_1}{\sqrt{2}} \right) \otimes \left( \frac{|0\rangle_2 + |1\rangle_2}{\sqrt{2}} \right) \Rightarrow \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix},$$

$$|+\rangle \otimes |-\rangle = \left( \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \right) \otimes \left( \frac{|0\rangle_2 - |1\rangle_2}{\sqrt{2}} \right) \Rightarrow \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix},$$

$$|-\rangle \otimes |-\rangle = \left( \frac{|0\rangle_1 - |1\rangle_1}{\sqrt{2}} \right) \otimes \left( \frac{|0\rangle_2 - |1\rangle_2}{\sqrt{2}} \right) \Rightarrow \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}.$$

Dla bramki *CNOT* można zapisać:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \Leftrightarrow |+\rangle \otimes |+\rangle \xrightarrow{CNOT} |+\rangle \otimes |+\rangle,$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \Leftrightarrow |-\rangle \otimes |+\rangle \xrightarrow{CNOT} |-\rangle \otimes |+\rangle,$$



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} \Leftrightarrow |+\rangle \otimes |-\rangle \xrightarrow{CNOT} |-\rangle \otimes |-\rangle,$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \Leftrightarrow |-\rangle \otimes |-\rangle \xrightarrow{CNOT} |+\rangle \otimes |-\rangle.$$

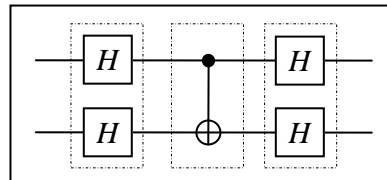
Z powyższego wynika, że w rozważanej przykładowej bazie, qubit kontrolny zamienił się rolą z qubitem docelowym. Qubit docelowy nie zmienia stanu na skutek działania bramki  $CNOT$ . Dla stanu  $|+\rangle$  qubitu docelowego stan qubitu kontrolnego ulega zmianie na przeciwny. To w prosty sposób obrazuje wpływ wyboru bazy na działanie bramek kwantowych.

Stany bazowe przedstawione powyżej można uzyskać działając bramką Hadamarda na stany bazy obliczeniowej:

$$H|0\rangle = |+\rangle,$$

$$H|1\rangle = |-\rangle.$$

Wykorzystując powyższe formuły można zaprojektować układ bramek, który spowoduje zadziałanie bramki  $CNOT$  w nowej bazie  $\{|+\rangle, |-\rangle\}$ , a następnie zamieni bazę ponownie na bazę obliczeniową  $\{|0\rangle, |1\rangle\}$ . Taki układ ma następującą postać:



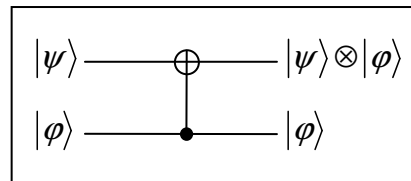
Macierze odpowiadające trzem kolejnym częściom powyższego układu mają postać:

$$H \otimes H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H \otimes H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Zatem wynikowa macierz opisująca cały układ jest postaci:

$$\frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

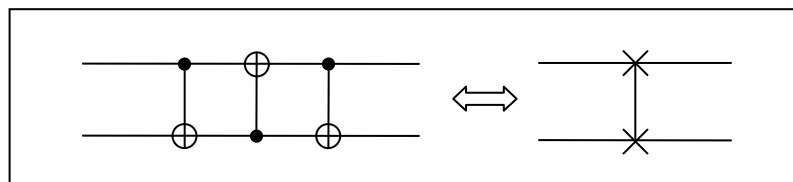
Powyższa macierz opisuje operację *CNOT* przy zamienionych rolami qubitach: kontrolnym i docelowym. Taką operację można przedstawić następująco:



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} |0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |0\rangle \\ |1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |0\rangle \\ |0\rangle \otimes |1\rangle \rightarrow |1\rangle \otimes |1\rangle \\ |1\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |1\rangle \end{matrix}.$$

### 13.5. Bramka SWAP

Operacja *SWAP* została wprowadzona w celu zrealizowania zamiany stanów dwóch qubitów. Bramka *SWAP* oznaczana jest w następujący sposób,



Działanie tej bramki można przeanalizować na podstawie kolejnych kroków:

$$\begin{aligned} & |\psi\rangle \otimes |\phi\rangle \\ & \xrightarrow{CNOT} |\psi\rangle \otimes (|\phi\rangle \oplus |\psi\rangle) \\ \xrightarrow{\text{reversed } CNOT} & [|\psi\rangle \oplus (|\phi\rangle \oplus |\psi\rangle)] \otimes (|\phi\rangle \oplus |\psi\rangle) = |\phi\rangle \otimes (|\phi\rangle \oplus |\psi\rangle) \\ & \xrightarrow{CNOT} |\phi\rangle \otimes [(|\phi\rangle \oplus |\psi\rangle) \oplus |\phi\rangle] = |\phi\rangle \otimes |\psi\rangle, \end{aligned}$$



Przyjęto tutaj, że  $a \oplus b = b \oplus a$  oraz  $a \oplus (a \oplus b) = b$ . Macierzowa reprezentacja unitarnej operacji *SWAP* jest następująca:

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

Można zweryfikować działanie bramki wykorzystując postać macierzową. Rozważmy dwa qubity w dowolnym stanie, które poddane zostaną działaniu operacji *SWAP*:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} \alpha_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \alpha_2 \\ \beta_1 \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 \alpha_2 \\ \beta_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \beta_2 \end{bmatrix} \Leftrightarrow [\alpha_2 |0\rangle_1 + \beta_2 |1\rangle_1] \otimes [\alpha_1 |0\rangle_2 + \beta_1 |1\rangle_2].$$

Można zauważyć, że nastąpiła zamiana współczynników. Odpowiada to wzajemnej wymianie kwantowej informacji pomiędzy qubitami. Operacja *SWAP* w pewien sposób jest powiązana z twierdzeniem *No-Deleting* – próba usunięcia nieznanej informacji skutkuje tylko przesunięciem tej informacji.

### 13.6. Bramka *CNOT* w reprezentacji dowolnej kontrolowanej bramki *U*

Należy podkreślić, że bramka *CNOT*, jako bramka dwu-qubitowa, jest szczególnie istotna z punktu widzenia twierdzenia o dekompozycji bramki. Wykorzystując wyłącznie bramkę *CNOT* oraz operacje jedno-qubitowe jest możliwe skonstruowanie dowolnej kontrolowanej bramki *U*. Przypominamy, że dowolna unitarna jedno-qubitowa operacja *U* może zostać przedstawiona następująco:

$$ABC = I, \\ U = e^{i\alpha} AXBXC.$$

Najpierw rozważmy jedno-qubitową operację zmiany fazy. Przypomnijmy, że konstruowana jest bramka kontrolowana – więc rozważana bramka fazy także powinna być kontrolowana qubitem kontrolnym. Jeżeli qubit kontrolny będzie w stanie  $|0\rangle$ , to stan qubitu docelowego nie ulegnie zmianie, natomiast jeśli qubit kontrolny będzie w stanie  $|1\rangle$ , to stan qubitu docelowego zostanie pomnożony przez czynnik fazowy  $e^{i\alpha}$ , zatem:

$$\begin{aligned} |0\rangle \otimes |0\rangle &\rightarrow |0\rangle \otimes |0\rangle \\ |0\rangle \otimes |1\rangle &\rightarrow |0\rangle \otimes |1\rangle \\ |1\rangle \otimes |0\rangle &\rightarrow |1\rangle \otimes e^{i\alpha} |0\rangle \\ |1\rangle \otimes |1\rangle &\rightarrow |1\rangle \otimes e^{i\alpha} |1\rangle \end{aligned}$$

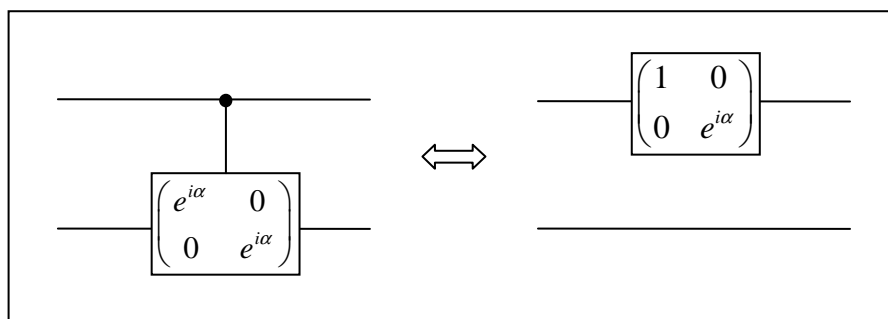
W reprezentacji macierzowej kontrolowana bramka fazy będzie miała postać:

$$\begin{pmatrix} I_{2 \times 2} & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}$$

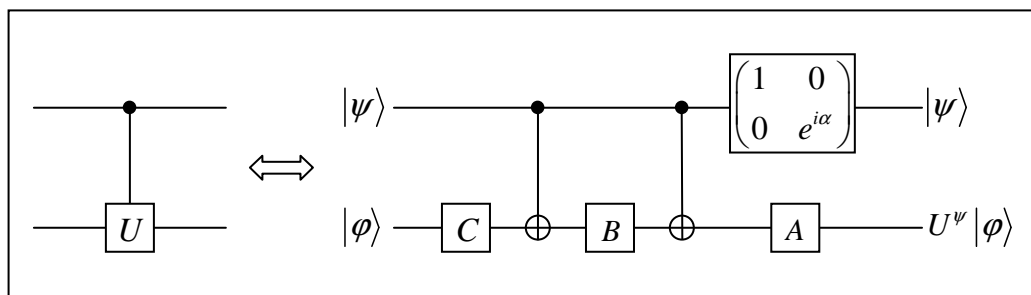
Można to zapisać następująco

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \otimes I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}$$

Zatem, można przedstawić kontrolowaną bramkę fazy w następującej postaci:



Wykorzystując powyższe oraz możliwą dekompozycję operacji  $U$ , można przedstawić kontrolowaną bramkę  $U$  w postaci:



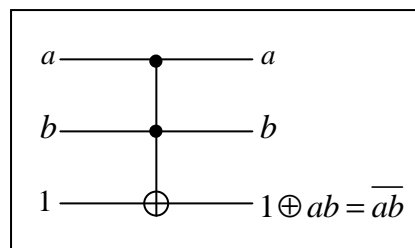
Jeżeli qubit kontrolny jest w stanie  $|\psi\rangle = |1\rangle$  wtedy stan qubitu docelowego podlegać będzie operacji  $U = e^{i\alpha}AXBXC$ , a w przypadku, gdy qubit kontrolny będzie w stanie  $|\psi\rangle = |0\rangle$ , wtedy na stan qubitu docelowego będzie działała operacja  $ABC = I$ .

### 13.7. Bramka Toffoli

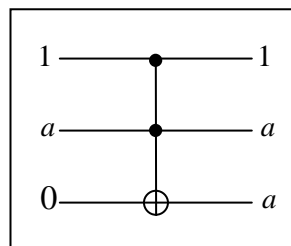
Bramka Toffoli jest klasyczną bramką odwracalną zdefiniowaną następująco:

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Negacja trzeciego bitu zachodzi w przypadku, gdy oba bity kontrolne są w stanie wysokim. Bity kontrolne nie ulegają zmianie podczas działania bramki. Bramka Toffoli jest bramką odwracalną. Ta bramka może zostać wykorzystana do realizacji bramki NAND – wystarczy aby bit docelowy był w wysokim stanie,

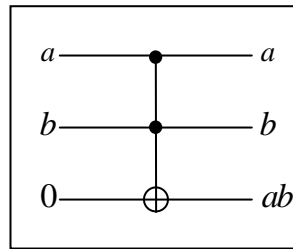


Bramka Toffoli może także realizować bramkę FANOUT (czyli, rozdwojenie klasycznego przewodu – skopiowanie bitu). Wystarczy, aby bit docelowy był w stanie niskim a pierwszy bit kontrolny w stanie wysokim.





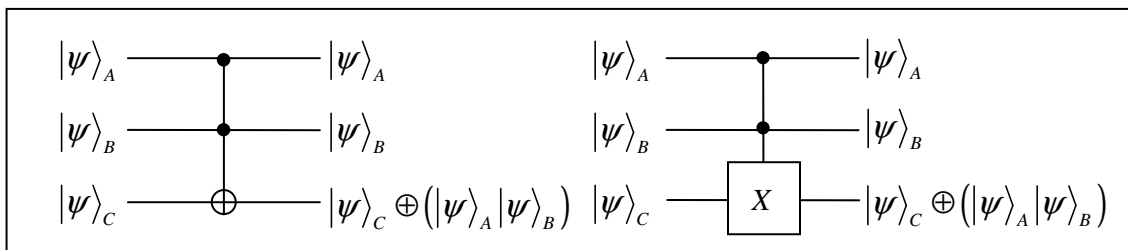
Oczywiście można także zrealizować bramkę AND,



Kwantową realizację bramki Toffoli jest możliwa dla układu dwóch qubitów kontrolnych i jednego qubitów docelowego. Stany poszczególnych qubitów zapisywane są w bazie obliczeniowej – co umożliwia posługiwanie się sumą modulo 2 (dzięki interpretacji stanów z bazy obliczeniowej na bity klasyczne). Operację Toffoli (można ją oznaczać jako bramkę *CCNOT*) na qubitach można zapisać następująco,

$$|\psi\rangle_A \otimes |\psi\rangle_B \otimes |\psi\rangle_C \xrightarrow{CCNOT} |\psi\rangle_A \otimes |\psi\rangle_B \otimes (|\psi\rangle_C \oplus (|\psi\rangle_A |\psi\rangle_B)).$$

Należy zwrócić uwagę, że powyższy zapis jest umowny, ponieważ suma  $\oplus$ , oraz iloczyn stanów  $(|\psi\rangle_A |\psi\rangle_B)$  odnoszą się do rachunku klasycznego bitów – ma to jedynie sens dla stanów obliczeniowych bazy.



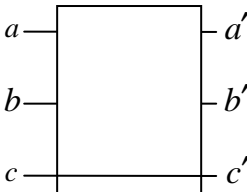
Korzystając z własności iloczynu tensorowego, oraz z wartości dla poszczególnych wektorów z bazy obliczeniowej układu trzech qubitów, można otrzymać postać macierzową operatora podwójnie kontrolowanej negacji – jest to macierz  $8 \times 8$ :

$$CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

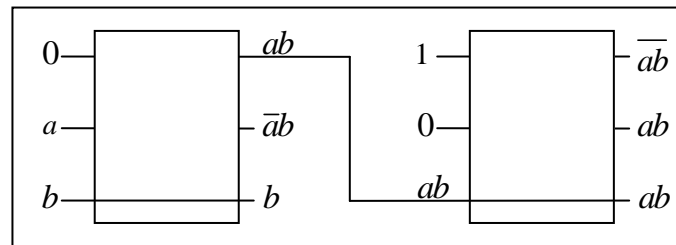
### 13.8. Bramka Fredkina

Bramka Fredkina jest także klasyczną odwracalną bramką:

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1



Klasyczna bramka Fredkina jest odpowiednikiem kontrolowanej bramki zamiany (SWAP). Bitem kontrolnym zazwyczaj jest bit ostatni – zależy to głównie od definicji. Podobnie jak w przypadku bramki Toffoliego, korzystając z bramki Fredkina można przedstawić bramkę NAND:



W przypadku kwantowym można zrealizować bramkę Fredkina w oparciu o kwantową kontrolowaną bramkę SWAP. Operacji SWAP odpowiada następująca definicja:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{\text{SWAP}} \begin{bmatrix} \alpha_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \alpha_2 \\ \beta_1 \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 \alpha_2 \\ \beta_1 \alpha_2 \\ \alpha_1 \beta_2 \\ \beta_1 \beta_2 \end{bmatrix} \Leftrightarrow [\alpha_2 | 0\rangle_1 + \beta_2 | 1\rangle_1] \otimes [\alpha_1 | 0\rangle_2 + \beta_1 | 1\rangle_2].$$

Można zaproponować postać macierzową dla kontrolowanej bramki SWAP:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

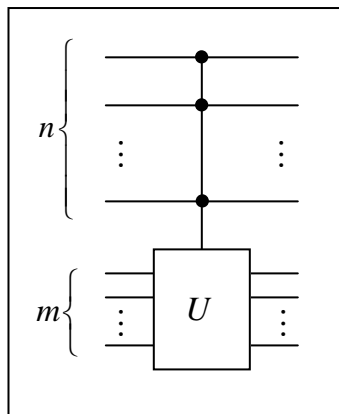
W powyższym przypadku qubitem kontrolnym jest pierwszy qubit. Jeżeli qubit kontrolny jest w stanie  $|1\rangle$  wtedy zamieniane są dwa pozostałe qubity. Natomiast, w przypadku gdy qubit kontrolny będzie w stanie  $|0\rangle$  wtedy stany wszystkie qubity pozostaną bez zmian.

### 13.9. Dowolna kontrolowana operacja $U$

Można rozważyć układ  $n$  qubitów kontrolnych i  $m$  qubitów docelowych, które zostaną poddane działaniu operacji unitarnej  $U$ , gdy wszystkie qubity kontrolne znajdą się w odpowiednich stanach. Taka operację można zapisać następująco,

$$C^n(U)|x_1x_2\dots x_n\rangle|\psi\rangle = |x_1x_2\dots x_n\rangle U^{x_1x_2\dots x_n}|\psi\rangle,$$

gdzie  $U$  oznacza unitarną operację na  $m$  qubitach, a  $x_1x_2\dots x_n$  jest iloczynem bitów  $x_1, x_2, \dots, x_n$ . Reprezentacja graficzna jest następującej postaci:

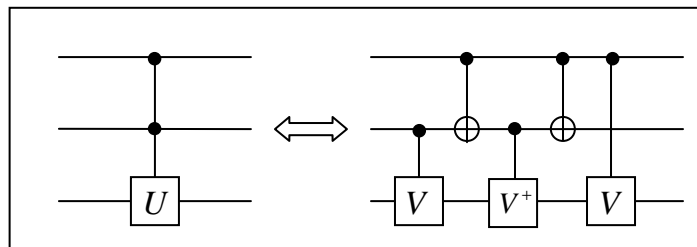


Dla ułatwienia można przyjąć, że  $m=1$ . Dla większych  $m$  można zastosować podobne rozważanie i otrzymać postać odpowiednich bramek.

Ogólną postać macierzy kontrolowanej operacji  $U$ , dla układu  $n$  qubitów kontrolnych, oraz  $m$  docelowych można przedstawić jako:

$$C^n(U^{(m)}) = \begin{pmatrix} I_{(2^{n+m}-2^m) \times (2^{n+m}-2^m)} & 0 \\ 0 & U_{2^m \times 2^m} \end{pmatrix}.$$

Natomiast, dowolna podwójnie kontrolowana operacja  $U$  jest postaci:



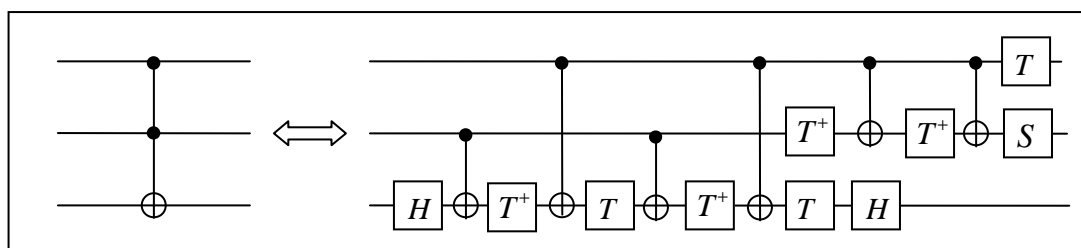
gdzie  $V^2 = U$ . W przypadku gdy,

$$V = \frac{(1-i)(I-iX)}{2}$$

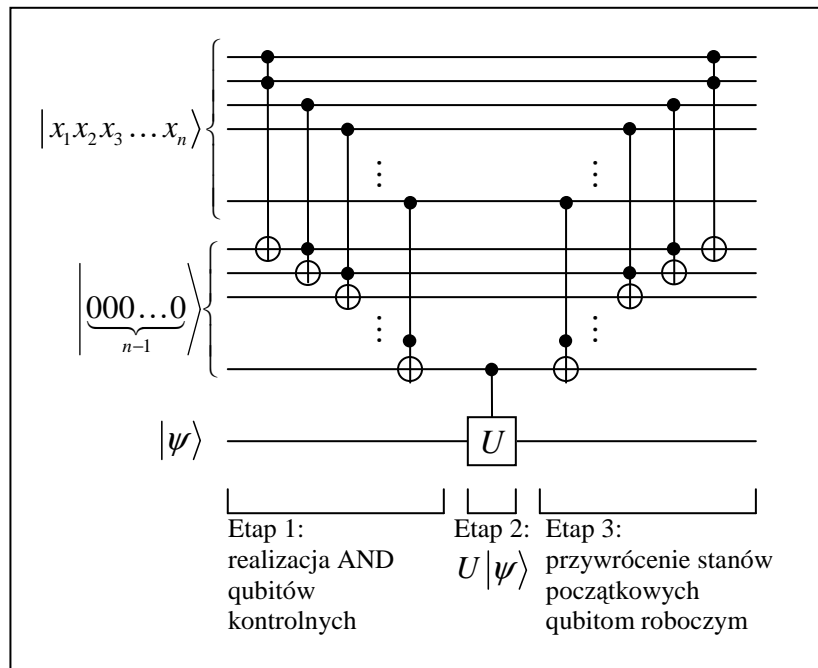
$$\Rightarrow V^2 = X,$$

powyższa realizacja odpowiada bramce Toffoliego zrealizowanej za pomocą bramek jedno-qubitowych oraz dwu-qubitowych. Warto zwrócić uwagę na fakt, że w przypadku informatyki klasycznej nie jest możliwe zrealizowanie za pomocą jedno- i dwu-bitowych odwracalnych bramek bramki Toffoliego, czy dowolnych układów.

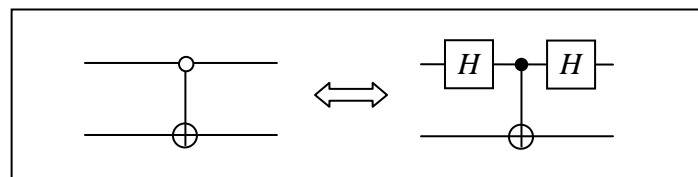
Jak zostanie niżej pokazane, dowolną unitarną operację można zrealizować (z dowolną dokładnością) za pomocą bramki Hadamarda, fazy, CNOT,  $\frac{\pi}{8}$ . Dla przykładu można przedstawić realizację bramki Toffoliego:



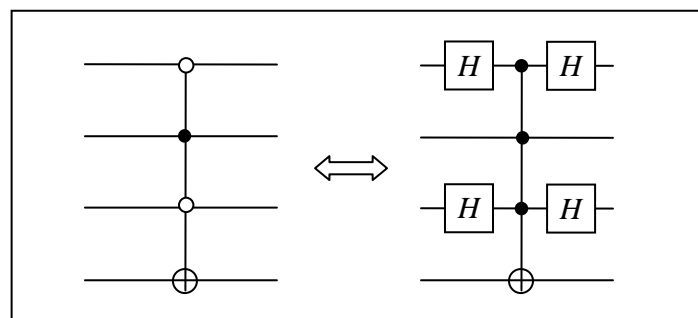
Realizacja dowolnej operacji  $C^n(U)$ , gdzie  $U$  jest unitarną operacją jednoqubitową ma postać trzy-stopniową, oraz wykorzystuje  $n-1$  qubitów roboczych, które na początku i na końcu działania operacji znajdują się w stanie  $|0\rangle$ .



Bramka kontrolna, działająca gdy qubit kontrolny jest w stanie  $|0\rangle$  ma postać:

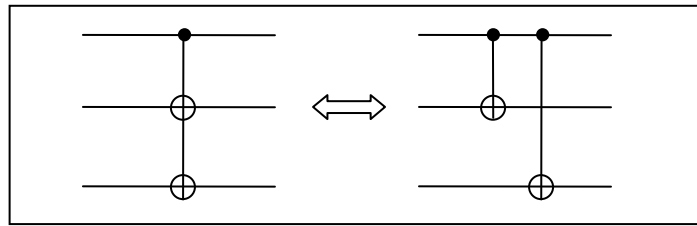


Przykład bramki kontrolowanej:



Pierwszy i trzeci qubit muszą być w stanie  $|0\rangle$ , a drugi qubit musi być w stanie  $|1\rangle$ , aby operacja  $U$  została zastosowana do czwartego qubit.

Można także rozważyć bramki kontrolne, które mają wiele qubitów docelowych:



Notacja ta oznacza, że jeżeli qubit kontrolny jest w stanie  $|1\rangle$ , wtedy do obu qubitów docelowych zostaną zastosowane operacje kwantowej negacji. W przypadku, gdy qubit kontrolny będzie w stanie  $|0\rangle$ , wtedy stany qubitów docelowych nie ulegną zmianie. Macierzowa postać takiej bramki jest następująca:

$$\begin{array}{l}
 |000\rangle \rightarrow |000\rangle \\
 |001\rangle \rightarrow |001\rangle \\
 |010\rangle \rightarrow |010\rangle \\
 |011\rangle \rightarrow |011\rangle \\
 |100\rangle \rightarrow |111\rangle \\
 |101\rangle \rightarrow |110\rangle \\
 |110\rangle \rightarrow |101\rangle \\
 |111\rangle \rightarrow |100\rangle
 \end{array}
 \Rightarrow
 \begin{pmatrix}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
 \end{pmatrix}$$

### 13.10. Operacje wielo-qubitowe – bramki uniwersalne

Można sformułować następujące twierdzenie:

Każda wielo-qubitowa unitarna operacja może zostać zrealizowana za pomocą uniwersalnego zbioru kwantowych bramek, np. bramki Hadamarda, fazy,  $CNOT$ ,  $\frac{\pi}{8}$ .

Dowód tego twierdzenia opiera się na połączeniu trzech konstrukcji:

- **Pierwsza konstrukcja** wskazuje na możliwość dokładnego przedstawienia dowolnej operacji unitarnej, jako iloczynu operatorów unitarnych działających nietrywialnie na wyłącznie dwa stany (lub mniej) z bazy obliczeniowej (operatory te reprezentowane są przez tzw. macierze dwu-poziomowe).
- **Druga konstrukcja** wskazuje, że dowolny unitarny operator opisany macierzą dwu-poziomą można przedstawić za pomocą wyłącznie bramek jedno-qubitowych, oraz bramek  $CNOT$ .
- **Trzecia konstrukcja** wskazuje, że każdą wielo-qubitową operację można przedstawić (z dowolną dokładnością) za pomocą bramek Hadamarda, fazy,  $CNOT$ ,  $\frac{\pi}{8}$ .



## Pierwsza konstrukcja

Rozważmy unitarną macierz  $U_{3 \times 3}$

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix},$$

$$U_3 U_2 U_1 U = I \Rightarrow U = U_1^+ U_2^+ U_3^+.$$

Poszukujemy macierzy  $U_1, U_2, U_3$ .

Konstrukcja macierzy  $U_1$ ,

$$b=0 \Rightarrow U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad b \neq 0 \Rightarrow U = \begin{pmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

W obu powyżej wskazanych przypadkach, macierz  $U_1$  macierzą dwupoziomową. Iloczyn  $U_1 U$  ma postać:

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & i' \end{pmatrix}.$$

Konstrukcja macierzy  $U_2$ ,

$$c'=0 \Rightarrow U = \begin{pmatrix} a^{**} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad c' \neq 0 \Rightarrow U = \begin{pmatrix} \frac{a^{**}}{\sqrt{|a|^2+|c|^2}} & 0 & \frac{c^{**}}{\sqrt{|a|^2+|c|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a|^2+|c|^2}} & 0 & \frac{-a'}{\sqrt{|a|^2+|c|^2}} \end{pmatrix}.$$

Iloczyn  $U_2 U_1 U$  ma postać:

$$U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & i'' \end{pmatrix}.$$



Z unitarności  $U, U_1, U_2$  wynika, że  $U_2 U_1 U$  jest macierzą unitarną i z unormowania pierwszego rzędu,

$$d'' = g'' = 0.$$

Konstrukcja macierzy  $U_3$ ,

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & i''^* \end{pmatrix}.$$

Widać, że iloczyn  $U_3 U_2 U_1 U = I$ , oraz,

$$U_3 U_2 U_1 U = I \Rightarrow U = U_1^+ U_2^+ U_3^+.$$

Dla dowolnej macierzy unitarnej  $U$  w  $d$ -wymiarowej przestrzeni Hilberta można zastosować analogiczną do powyższej metodę. Można znaleźć macierze  $U_1, \dots, U_{d-1}$  takie, że iloczyn  $U_{d-1} U_{d-2} \dots U_1 U$  ma w lewym górnym rogu 1, a w pozostałej części pierwszej kolumny i pierwszego rzędu zera. Następnie należy powtórzyć procedurę dla macierzy o rozmiarach  $(d-1) \times (d-1)$ , która znajduje się w prawej dolnej części macierzy  $U_{d-1} U_{d-2} \dots U_1 U$ . W końcu będzie można zapisać,

$$U = V_1 \dots V_k, \quad k \leq (d-1) + (d-2) + \dots + 1 = \frac{d(d-1)}{2}.$$

Zatem,

$$k \leq \frac{2^n(2^n-1)}{2} = 2^{n-1}(2^n-1).$$

## Druga konstrukcja

Można pokazać, że przy wykorzystaniu wyłącznie jedno-qubitowych bramek oraz bramek *CNOT* można zrealizować dowolną dwu-poziomą unitarną macierz.

Założmy, że  $U$  jest dwu-poziomą unitarną macierzą, która działa nietrywialnie na stany  $|a\rangle$  i  $|b\rangle$ , gdzie  $a = a_1 \dots a_n$ ,  $b = b_1 \dots b_n$  są binarnymi rozwinięciami stanów. Niech  $\tilde{U}$  będzie nietrywialną macierzą  $2 \times 2$  – operacją jedno-qubitową.

Dla ułatwienia można zastosować kod Gray'a. Niech  $a = a_1 \dots a_n$  i  $b = b_1 \dots b_n$  będą odległymi liczbami binarnymi. Kod Gray'a, łączący liczby  $a = a_1 \dots a_n$  i  $b = b_1 \dots b_n$ , jest ciągiem liczb binarnych, w którym kolejna liczba różni się dokładnie na jednym miejscu od poprzedniej.





Niech  $g_1, \dots, g_m$  będą elementami kodu Gray'a takimi, że  $g_1 = a$ ,  $g_m = b$  ( $m \leq n+1$ , bo  $a$  i  $b$  mogą się różnić maksymalnie na  $n$  pozycjach). Idea implementacji  $U$  polega na zrealizowaniu zmiany stanów,

$$|g_1\rangle \rightarrow |g_2\rangle \rightarrow \dots \rightarrow |g_{m-1}\rangle,$$

a następnie, na zastosowania kontrolowanej operacji  $\tilde{U}$ , na qubicie docelowym, który odpowiada miejscu w zapisie binarnym, gdzie różnią się stany  $|g_{m-1}\rangle$  i  $|g_m\rangle$ , oraz finalnie na powrocie operacjami

$$|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle \rightarrow \dots \rightarrow |g_1\rangle.$$

Dla przykładu,

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & c_1 & 0 & 0 & 0 & 0 & c_2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & c_3 & 0 & 0 & 0 & 0 & c_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \tilde{U} = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}.$$

Powyższa macierz działa nietrywialnie na dwa stany:

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Leftrightarrow |001\rangle \xrightarrow{U} c_1|001\rangle + c_3|110\rangle \Rightarrow \begin{bmatrix} 0 \\ c_1 \\ 0 \\ 0 \\ 0 \\ 0 \\ c_3 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \Leftrightarrow |110\rangle \xrightarrow{U} c_2|001\rangle + c_4|110\rangle \Rightarrow \begin{bmatrix} 0 \\ c_2 \\ 0 \\ 0 \\ 0 \\ 0 \\ c_4 \\ 0 \end{bmatrix}$$

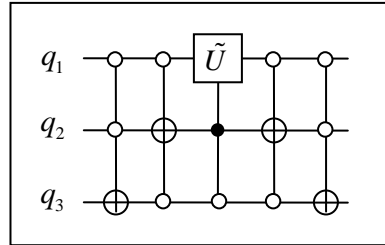
Koda Graya dla tych stanów jest następujący

	$q_1$	$q_2$	$q_3$
$a = g_1$	0	0	1
$g_2$	0	0	0



$g_3$	0	1	0
$b = g_4$	1	1	0

Czyli układ będzie miał postać



Jako, że zbiór operacji unitarnych jest ciągły, nie istnieje możliwość przedstawienia go za pomocą dyskretnego zbioru elementów. Można raczej tu mówić o przedstawieniu z dowolnie dobrym przybliżeniem.

### Trzecia konstrukcja – uniwersalność skończonego zbioru bramek

Wykorzystując bramki Hadamarda i bramki  $\frac{\pi}{8}$  można zbudować (z odpowiednim przybliżeniem) dowolną jedno-qubitową unitarną bramkę. Bramka  $T$  jest obrotem wokół osi  $z$  o kąt  $\frac{\pi}{4}$  (z dokładnością do nieistotnego czynnika fazowego) natomiast bramka  $HTH$  jest obrotem wokół osi  $x$  także o  $\frac{\pi}{4}$ . Czyli można zapisać,

$$e^{-i\frac{\pi}{8}Z} e^{-i\frac{\pi}{8}X} = \left( \cos \frac{\pi}{8} I - i \sin \frac{\pi}{8} Z \right) \left( \cos \frac{\pi}{8} I - i \sin \frac{\pi}{8} X \right)$$

$$= \cos^2 \frac{\pi}{8} I - \left( i \cos \frac{\pi}{8} (X + Z) - i \sin \frac{\pi}{8} ZX \right) \sin \frac{\pi}{8}.$$

Jest to obrót wokół osi  $\vec{n} = \left( \cos \frac{\pi}{8}, \sin \frac{\pi}{8}, \cos \frac{\pi}{8} \right)$  (gdzie  $\hat{n}$  jest wersorem tego kierunku) o kąt  $\theta$ , określony przez  $\cos \frac{\theta}{2} = \cos^2 \frac{\pi}{8}$ . Czyli używając wyłącznie bramki Hadamarda i bramki  $\frac{\pi}{8}$  można skonstruować bramkę  $R_{\vec{n}}(\theta)$  (można pokazać, że  $\theta$  jest niewymierną wielokrotności  $2\pi$ ). Wielokrotne złożenie  $R_{\vec{n}}(\theta)$  może być wykorzystane do dowolnie dokładnego przybliżenia dowolnej rotacji  $R_{\vec{n}}(\alpha)$ . Niech  $\delta > 0$ ,  $\delta$  ustalona dokładność,

$$N > \frac{2\pi}{\delta}, \quad N \in \mathbb{Z},$$

$$\theta_k \in [0, 2\pi), \quad \theta_k = (k\theta) \bmod 2\pi.$$



Można zapisać, że,

$$\exists_{j,k \in \{1, \dots, N\}} |\theta_k - \theta_j| \leq \frac{2\pi}{N} < \delta.$$

Bez straty ogólności założyć można, że  $k > j$ , wtedy,

$$|\theta_{k-j}| < \delta.$$

W związku z tym, że  $k \neq j$  oraz, że  $\theta$  jest niewymierną wielokrotności  $2\pi$  mamy  $\theta_{k-j} \neq 0$ . Wynika z tego, że  $\theta_{l(k-j)}$  wypełnia przedział  $[0, 2\pi)$  przy zmianie  $l$ , w taki sposób, że dwa sąsiednie elementy ciągu nie są oddalone od siebie bardziej niż o  $\delta$ ; można więc napisać

$$\forall_{\varepsilon > 0} \exists_n E(R_{\hat{n}}(\alpha), [R_{\hat{n}}(\theta)]^n) < \frac{\varepsilon}{3}.$$

Zatem,

$$HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha),$$

gdzie  $\hat{m}$  jest wersorem wektora  $\left(\cos \frac{\pi}{8}, -\sin \frac{\pi}{8}, \cos \frac{\pi}{8}\right)$ , z czego wynika

$$E(R_{\hat{m}}(\alpha), [R_{\hat{m}}(\theta)]^n) < \frac{\varepsilon}{3}.$$

Wykorzystując fakt, że dowolna unitarna jedno-qubitowa operacja  $U$  może być przedstawiona, z dokładnością do fazy, w postaci,

$$U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta),$$

mamy,

$$E\left(U, [R_{\hat{n}}(\theta)]^{n_1} H [R_{\hat{m}}(\theta)]^{n_2} H [R_{\hat{n}}(\theta)]^{n_3}\right) < \varepsilon.$$

Wynika z powyższego, że można przybliżyć (z dowolną dokładnością  $\varepsilon > 0$ ) dowolną unitarną jedno-qubitową operacją  $U$  za pomocą jedynie bramek Hadamarda i bramek  $\frac{\pi}{8}$ .

Oznacza to, że zbiór: bramka Hadamarda, bramka  $\frac{\pi}{8}$ , bramka fazy i bramka  $CNOT$  tworzą zbiór uniwersalny.

## 14. Układ bramek kwantowych realizujący splątane stany (stany Bella)

Rozważmy układ dwóch qubitów. Maksymalnie splątane stany rozpięte na bazie obliczeniowej układu dwóch qubitów  $\{|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2\}$  nazywane są stanami Bella i są następującej postaci,

$$|\psi^+\rangle_{12} = \frac{1}{\sqrt{2}} (|1\rangle_1 \otimes |2\rangle_2 + |2\rangle_1 \otimes |1\rangle_2),$$

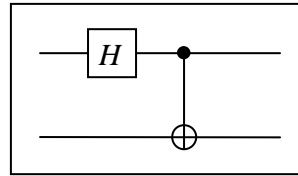
$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}} (|1\rangle_1 \otimes |2\rangle_2 - |2\rangle_1 \otimes |1\rangle_2),$$

$$|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}} (|1\rangle_1 \otimes |1\rangle_2 + |2\rangle_1 \otimes |2\rangle_2),$$

$$|\phi^-\rangle_{12} = \frac{1}{\sqrt{2}} (|1\rangle_1 \otimes |1\rangle_2 - |2\rangle_1 \otimes |2\rangle_2).$$

Te stany są czasem nazywane stanami EPR w związku z paradoksem Einsteina-Podolskiego-Rosena. Stany Bella są maksymalnie zmieszonymi stanami układu dwóch qubitów (ze środka odpowiedniej sfery Blocha).

Można rozważyć układ, który splątuje dwa qubity w stany Bella.



$$(H \otimes I)(CNOT) = \left( \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes I \right) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Działanie powyższej macierzy na stany z bazy obliczeniowej jest następujące:

$$|0\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = |\phi^+\rangle_{12}$$

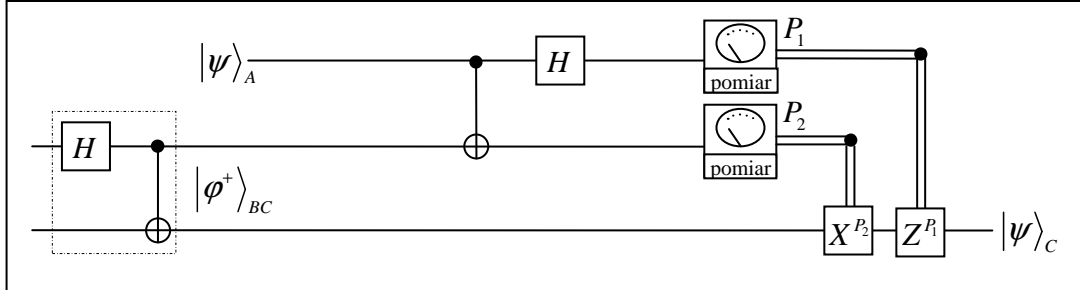
$$|0\rangle \otimes |1\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) = |\psi^+\rangle_{12}$$

$$|1\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) = |\phi^-\rangle_{12}$$

$$|1\rangle \otimes |1\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) = |\psi^-\rangle_{12}$$

## 15. Układ bramek kwantowych realizujący teleportację kwantowych stanów

Można zrealizować układ teleportujący kwantowe stany, oparty na bramkach kwantowych.:



W pierwszym kroku realizujemy stan maksymalnie splątany na qubitach  $B$  i  $C$ , przy wykorzystaniu układu przedstawionego wcześniej. Załóżmy, że qubity  $B$  i  $C$  są w stanie  $|\phi^+\rangle_{BC}$ , natomiast qubit  $A$  jest w dowolnym nieznanym stanie  $|\psi\rangle_A$  (który ma zostać przeteleportowany). Więc stan całego układu

$$\begin{aligned} |\psi\rangle_{ABC}^{(0)} &= |\psi\rangle_A \otimes |\phi^+\rangle_{BC} = \frac{1}{\sqrt{2}} (\alpha|0\rangle_A + \beta|1\rangle_A) \otimes (|0\rangle_B \otimes |0\rangle_C + |1\rangle_B \otimes |1\rangle_C) \\ &= \frac{1}{\sqrt{2}} [\alpha|0\rangle_A \otimes (|0\rangle_B \otimes |0\rangle_C + |1\rangle_B \otimes |1\rangle_C) + \beta|1\rangle_A \otimes (|0\rangle_B \otimes |0\rangle_C + |1\rangle_B \otimes |1\rangle_C)] \end{aligned}$$

Po zadziałaniu bramki  $CNOT$  na qubity  $A$  i  $B$  stan całego układu ulegnie zmianie:

$$|\psi\rangle_{ABC}^{(1)} = \frac{1}{\sqrt{2}} [\alpha|0\rangle_A \otimes (|0\rangle_B \otimes |0\rangle_C + |1\rangle_B \otimes |1\rangle_C) + \beta|1\rangle_A \otimes (|1\rangle_B \otimes |0\rangle_C + |0\rangle_B \otimes |1\rangle_C)]$$

Następnie na qubit  $A$  jest poddany działaniu bramki Hadamarda, co zmieni stan układu na:

$$\begin{aligned} |\psi\rangle_{ABC}^{(2)} &= \frac{1}{2} [\alpha(|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B \otimes |0\rangle_C + |1\rangle_B \otimes |1\rangle_C) \\ &\quad + \beta(|0\rangle_A - |1\rangle_A) \otimes (|1\rangle_B \otimes |0\rangle_C + |0\rangle_B \otimes |1\rangle_C)] \end{aligned}$$

Powyższe można zapisać w postaci:

$$\begin{aligned} |\psi\rangle_{ABC}^{(2)} &= \frac{1}{2} [\alpha(|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B \otimes |0\rangle_C + |1\rangle_B \otimes |1\rangle_C) \\ &\quad + \beta(|0\rangle_A - |1\rangle_A) \otimes (|1\rangle_B \otimes |0\rangle_C + |0\rangle_B \otimes |1\rangle_C)] \\ &= \frac{1}{2} [(|0\rangle_A \otimes |0\rangle_B) \otimes \alpha|0\rangle_C + (|0\rangle_A \otimes |1\rangle_B) \otimes \alpha|1\rangle_C \\ &\quad + (|1\rangle_A \otimes |0\rangle_B) \otimes \beta|0\rangle_C + (|1\rangle_A \otimes |1\rangle_B) \otimes \beta|1\rangle_C] \end{aligned}$$



$$\begin{aligned}
 & + (|1\rangle_A \otimes |0\rangle_B) \otimes \alpha |0\rangle_C + (|1\rangle_A \otimes |1\rangle_B) \otimes \alpha |1\rangle_C \\
 & (|0\rangle_A \otimes |1\rangle_B) \otimes \beta |0\rangle_C + (|0\rangle_A \otimes |0\rangle_B) \otimes \beta |1\rangle_C \\
 & + (|1\rangle_A \otimes |1\rangle_B) \otimes (-\beta) |0\rangle_C + (|1\rangle_A \otimes |0\rangle_B) \otimes (-\beta) |1\rangle_C ] \\
 = & \frac{1}{2} [ (|0\rangle_A \otimes |0\rangle_B) \otimes (\alpha |0\rangle_C + \beta |1\rangle_C) + (|0\rangle_A \otimes |1\rangle_B) \otimes (\alpha |1\rangle_C + \beta |0\rangle_C) \\
 & + (|1\rangle_A \otimes |0\rangle_B) \otimes (\alpha |0\rangle_C - \beta |1\rangle_C) + (|1\rangle_A \otimes |1\rangle_B) \otimes (-\beta |0\rangle_C + \alpha |1\rangle_C) ] .
 \end{aligned}$$

Można więc zapisać,

$$\begin{aligned}
 |0\rangle_A \otimes |0\rangle_B & \rightarrow \alpha |0\rangle_C + \beta |1\rangle_C \\
 |0\rangle_A \otimes |1\rangle_B & \rightarrow \beta |0\rangle_C + \alpha |1\rangle_C \\
 |1\rangle_A \otimes |0\rangle_B & \rightarrow \alpha |0\rangle_C - \beta |1\rangle_C \\
 |1\rangle_A \otimes |1\rangle_B & \rightarrow -\beta |0\rangle_C + \alpha |1\rangle_C .
 \end{aligned}$$

Jeżeli pomiary  $P_1$  oraz  $P_2$  wskażą na stan  $|0\rangle_A \otimes |0\rangle_B$ , wtedy stan qubitu  $C$  przyjmie postać z odpowiednią kombinacją współczynników stanu teleportowanego. W przypadku  $|0\rangle_A \otimes |1\rangle_B$  należy zadziałać na qubit  $C$  bramką negacji  $X$ . W przypadku  $|1\rangle_A \otimes |0\rangle_B$  należy zadziałać na qubit  $C$  bramką  $Z$ , a w przypadku  $|1\rangle_A \otimes |1\rangle_B$  należy zadziałać najpierw bramką  $X$  a potem  $Z$ . W ogólnym przypadku należy zadziałać operacją  $Z^{P_1} X^{P_2}$  na stan qubitu  $C$  w celu otrzymania odpowiedniej kombinacji współczynników. Informacja, jaki rodzaj lokalnej operacji należy wykonać na qubicie  $C$ , nie jest wcześniej znana – ta klasyczna informacja musi zostać przekazana kanałem klasycznym odległemu obserwatorowi, znajdującemu się przy qubicie  $C$ .

## 16. Równoległość kwantowa

Kwantowa równoległość jest szeroko wykorzystywana w różnych kwantowych algorytmach. W dużym uproszczeniu można powiedzieć, że równoległość przetwarzania kwantowego polega na jednoczesnym obliczeniu wartości funkcji dla różnych argumentów (obliczeniu w sensie kwantowym, niedostępnym dla klasycznego obserwatora).

Założmy, że funkcja  $f(x)$  jest zdefiniowana następująco:

$$f(x) : \{0,1\} \rightarrow \{0,1\} .$$



Rozważmy dwu-qubitowy komputer kwantowy. Stan początkowy komputera kwantowego niech będzie postaci  $|a\rangle \otimes |b\rangle$ . Zakładamy, że realizowana będzie operacja, której wynik jest postaci  $|a\rangle \otimes (|b\rangle \oplus |f(a)\rangle)$ . Czyli można zapisać,

$$\begin{aligned} &|a\rangle \text{ rejestr wejściowy} \\ &|b\rangle \text{ rejestr wyjściowy} \\ U_f : &|a\rangle \otimes |b\rangle \rightarrow |a\rangle \otimes (|b\rangle \oplus |f(a)\rangle). \end{aligned}$$

Jeśli  $|b\rangle = |0\rangle$  wtedy wynikiem jest  $|f(a)\rangle$ .

Założmy, że stan wejściowy  $|a\rangle$  będzie postaci,

$$|a\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Zatem, wynik działania operacji  $U_f$  będzie postaci,

$$\frac{|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle}{\sqrt{2}}.$$

Z powyższego widać, że funkcja jest równocześnie obliczana dla dwóch argumentów.

Warto wskazać, że:

1. W związku z wymogiem odwracalności operacji komputery kwantowe muszą posiadać rejestry wejściowe i wyjściowe równych rozmiarów.
2. Rejestr wejściowy składa się z:
  - $n$  qubitów definiujących liczbę całkowitą  $x$  – w reprezentacji bitowej zapisaną za pomocą  $n$  bitów (dla  $n$  qubitów można wyreprezentować liczby całkowite do  $2^n$ )
  - $m$  qubitów potrzebnych do wyreprezentowania wyników określonej funkcji  $f(x)$
3. Rejestr wyjściowy składa się z:
  - niezmiennych  $n$  qubitów wejściowych
  - $m$  qubitów, które przyjmą wartości funkcji  $f(x)$ .

Gdyby nie uwzględnić dodatkowych  $m$  qubitów (oprócz  $n$  qubitów) pojawiłby się problem z odwracalnością operacji dla funkcji nieróżnowartościowych – operacja taka nie byłaby unitarna. Dla funkcji różnowartościowej  $m = n$ .

Założmy, że

$$U_f (|x\rangle_n \otimes |y\rangle_m) = |x\rangle_n \otimes |y \oplus f(x)\rangle_m,$$



gdzie  $|a\rangle_b$  oznacza  $b$ -bitową liczbę całkowitą  $a$ . W przypadku gdy  $y = 0$ , mamy

$$U_f(|x\rangle_n \otimes |0\rangle_m) = |x\rangle_n \otimes |0 \oplus f(x)\rangle_m = |x\rangle_n \otimes |f(x)\rangle_m.$$

$$U_f U_f(|x\rangle \otimes |y\rangle) = U_f(|x\rangle \otimes |y \oplus f(x)\rangle) = |x\rangle \otimes |y \oplus f(x) \oplus f(x)\rangle = |x\rangle \otimes |y\rangle,$$

ponieważ, dla dowolnego  $a$  mamy  $a \oplus a = 0$ .

Rozpatrzmy następujące działanie:

$$(H \otimes H)(|0\rangle \otimes |0\rangle) = H|0\rangle \otimes H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Można to uogólnić na  $n$ -krotny iloczyn tensorowy bramek Hadamarda  $H^{\otimes n}$ ,

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n} |x\rangle_n.$$

Otrzymany stan jest równowagową superpozycją wszystkich możliwych kombinacji liniowych, które może przyjąć stan  $|x\rangle_n$ . Zatem można napisać,

$$(H^{\otimes n} \otimes I_m)(|0\rangle_n \otimes |0\rangle_m) = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n} (|x\rangle_n \otimes |0\rangle_m).$$

Następnie można do powyższego stanu zastosować następującą operację unitarną,

$$U_f \left( \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n} (|x\rangle_n \otimes |0\rangle_m) \right) = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n} U_f(|x\rangle_n \otimes |0\rangle_m) = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n} (|x\rangle_n \otimes |f(x)\rangle_m).$$

Uzyskany stan, w przypadku klasycznego obliczania wartości funkcji  $f$ , wymagałby obliczenia wartości dla wszystkich  $x$  – w przypadku kwantowym stan ten otrzymany jest natychmiastowo.

Można dokonać obliczeń np. dla 100 qubitów, czyli  $|0\rangle_{100}$  oraz  $|0\rangle_m$ , po zastosowaniu 100-krotnego iloczynu tensorowego bramek Hadamarda, oraz po zastosowaniu operacji unitarnej, uzyskana zostanie superpozycja  $2^{100}$  stanów, a to odpowiada około  $10^{30}$  obliczeń wartości funkcji  $f$ .

Jednakże, pojawia się tutaj problem – wynikowy stan jest nieznanym, a klasycznie możliwe jest odczytanie tylko jego małego fragmentu. Np. po dokonaniu pomiaru uzyskana zostanie tylko





jedna losowa wartość (w związku z równowagowym rozkładem prawdopodobieństwa w równowagowej superpozycji).

## 17. Kwantowa transformata Fouriera

Kwantowe procedury realizowane na komputerach kwantowych mogą znacznie przyspieszyć niektóre obliczenia matematyczne. Bardzo istotną transformacją z punktu widzenia kwantowych algorytmów jest transformata Fouriera.

Dyskretna transformata Fouriera jest zdefiniowana jako operator,

$$F = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{i \frac{2\pi nk}{N}},$$

w  $N$ -wymiarowej przestrzeni. Jej działanie na zespolony wektor  $x_0, \dots, x_{N-1}$  można zapisać w postaci,

$$\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{i \frac{2\pi nk}{N}} x_n = y_k,$$

gdzie  $y_0, \dots, y_k$  jest wyjściowym zespolonym wektorem.

Działanie kwantowej transformaty Fouriera jest podobne. Kwantowa transformacja Fouriera, zdefiniowana jako operator liniowy, w działaniu na wektor  $|x_k\rangle$  należący do bazy ortonormalnej (rozpinającej przestrzeń  $N$ -wymiarową)  $|0\rangle, \dots, |N-1\rangle$  przekształca go w kombinację liniową wszystkich wektorów z innej bazy tej samej przestrzeni, o współczynnikach danych postacią operatora,

$$F|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i \frac{2\pi jk}{N}} |k\rangle = |\tilde{j}\rangle.$$

W związku z liniowością można zapisać działanie transformaty na dowolny wektor,

$$\sum_{k=0}^{N-1} \alpha_j |j\rangle \xrightarrow{F} \sum_{k=0}^{N-1} \beta_k |k\rangle,$$

Gdzie  $\beta_k$  są dyskretnymi transformatami Fouriera  $\alpha_j$ ,

$$\beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{i \frac{2\pi jk}{N}} \alpha_j.$$



Transformata Fouriera jest operatorem unitarnym, czyli zachowuje iloczyn skalarny  $\langle j_2 | j_1 \rangle$ ,

$$\begin{aligned} |j_1\rangle &= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{N-1} e^{i\frac{2\pi j_1 k_1}{N}} |k_1\rangle, \\ |j_2\rangle &= \frac{1}{\sqrt{N}} \sum_{k_2=0}^{N-1} e^{i\frac{2\pi j_2 k_2}{N}} |k_2\rangle, \\ \langle j_2 | j_1 \rangle &= \frac{1}{\sqrt{N}} \frac{1}{\sqrt{N}} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} e^{i\frac{2\pi j_1 k_1}{N}} e^{-i\frac{2\pi j_2 k_2}{N}} \langle k_2 | k_1 \rangle \\ &= \frac{1}{N} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} e^{i\frac{2\pi j_1 k_1}{N}} e^{-i\frac{2\pi j_2 k_2}{N}} \delta_{12} = \frac{1}{N} \sum_{k_1=0}^{N-1} e^{i\frac{2\pi j_1 k_1}{N}} e^{-i\frac{2\pi j_2 k_1}{N}} \\ &= \frac{1}{N} \sum_{k_1=0}^{N-1} e^{i\frac{2\pi k_1}{N}(j_1-j_2)}, \\ j_1 = j_2 &\Rightarrow \frac{1}{N} \sum_{k_1=0}^{N-1} e^{i\frac{2\pi k_1}{N}(j_1-j_2)} = \frac{1}{N} \sum_{k_1=0}^{N-1} e^0 = \frac{N}{N} = 1, \\ j_1 \neq j_2 &\Rightarrow \frac{1}{N} \sum_{k_1=0}^{N-1} e^{i\frac{2\pi k_1}{N}(j_1-j_2)} \end{aligned}$$

W przypadku gdy  $j_1 \neq j_2$  rozważana suma jest sumą szeregu geometrycznego,

$$S = a_1 \frac{1-q^n}{1-q},$$

oraz dla rozważanego szeregu:

$$\begin{aligned} a_1 = \frac{1}{N} \Leftrightarrow k_1 = 0 &\Rightarrow \frac{1}{N} e^{i\frac{2\pi 0}{N}(j_1-j_2)} = \frac{1}{N}, \quad q = e^{i\frac{2\pi}{N}(j_1-j_2)}, \\ \frac{1-q^N}{1-q} &= \frac{1-e^{i\frac{2\pi}{N}(j_1-j_2)N}}{1-e^{i\frac{2\pi}{N}(j_1-j_2)}} = \frac{1-e^{i2\pi(j_1-j_2)}}{1-e^{i\frac{2\pi}{N}(j_1-j_2)}} = \frac{1-1}{1-e^{i\frac{2\pi}{N}(j_1-j_2)}} = 0. \end{aligned}$$

Można wprowadzić odwrotną transformatę Fouriera:

$$\begin{aligned} |k\rangle &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-i\frac{2\pi jk}{N}} |\tilde{j}\rangle, \\ |k_x\rangle &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-i\frac{2\pi jk_x}{N}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i\frac{2\pi jk}{N}} |k\rangle = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{-i\frac{2\pi jk_x}{N}} e^{i\frac{2\pi jk}{N}} |k\rangle \end{aligned}$$



$$\begin{aligned}
 &= \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{-i\frac{2\pi j k_x}{N}} e^{i\frac{2\pi j k}{N}} |k\rangle = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{i\frac{2\pi j}{N}(k-k_x)} |k\rangle \\
 &\qquad\qquad\qquad k = k_x \\
 &= \frac{1}{N} \sum_{j=0}^{N-1} e^{i\frac{2\pi j}{N}(k-k_x)} |k\rangle = \frac{N}{N} |k_x\rangle \\
 &\qquad\qquad\qquad k \neq k_x \\
 &= \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{i\frac{2\pi j}{N}(k-k_x)} |k\rangle = \frac{1}{N} \sum_{k=0}^{N-1} |k\rangle \underbrace{\sum_{j=0}^{N-1} e^{i\frac{2\pi j}{N}(k-k_x)}}_{\substack{\text{suma szeregu geom.} \\ =0}} = 0
 \end{aligned}$$

W ramach kwantowej transformaty Fouriera można rozważyć układ  $n$  qubitów. Odpowiadająca mu przestrzeń Hilberta będzie miała wymiar  $2^n$ . Stany bazy obliczeniowej tej przestrzeni można zapisać w konwencji rozwinięć bitowych,

$$|j\rangle \in \{|0\rangle, \dots, |2^n - 1\rangle\},$$

Dla bazy obliczeniowej,

$$\begin{aligned}
 |j\rangle &= |j_1\rangle \otimes \dots \otimes |j_n\rangle = |j_1 \dots j_n\rangle, \quad i = 1, \dots, n \quad j_i \in \{0, 1\} \\
 \Rightarrow j_k &= j_1 \dots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_{n-1} 2^1 + j_n 2^0
 \end{aligned}$$

(w przyjętej konwencji zapisu dwójkowego).

Działanie kwantowej transformaty Fouriera na stan  $|j\rangle$  można zapisać w postaci:

$$\begin{aligned}
 F|j\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{i\frac{2\pi j k}{2^n}} |k\rangle = \left| |k\rangle = |k_1\rangle \otimes \dots \otimes |k_n\rangle \right| \\
 &\stackrel{(***)}{=} \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 e^{i2\pi j \left( \sum_{q=1}^n \frac{k_q}{2^q} \right)} (|k_1\rangle \otimes \dots \otimes |k_n\rangle) \\
 &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 \prod_{q=1}^n e^{i2\pi j \frac{k_q}{2^q}} |k_q\rangle \\
 &= \frac{1}{\sqrt{2^n}} \prod_{q=1}^n \left( \sum_{k_q=0}^1 e^{i2\pi j \frac{k_q}{2^q}} |k_q\rangle \right) \\
 &= \frac{1}{\sqrt{2^n}} \prod_{q=1}^n \left( |0\rangle + e^{i\frac{2\pi j}{2^q}} |1\rangle \right)
 \end{aligned}$$



$$= \frac{1}{\sqrt{2^n}} \left[ \left( |0\rangle + e^{i2\pi(j_n 2^{-1})} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_{n-1} 2^{-1} + j_n 2^{-2})} |1\rangle \right) \otimes \dots \otimes \left( |0\rangle + e^{i2\pi(j_1 2^{-1} + j_2 2^{-2} + \dots + j_n 2^{-n})} |1\rangle \right) \right]$$

Krok (\*\*\*) w powyższym wyprowadzeniu można przykładowo przedstawić dla  $n=3$ .  
Można zapisać:

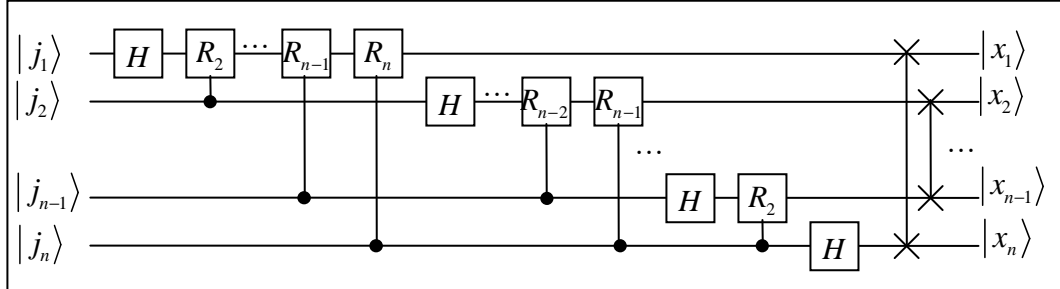
$$\begin{aligned} & \frac{1}{\sqrt{2^3}} \sum_{k=0}^7 e^{i2\pi j \frac{k}{2^3}} |k_1 k_2 k_3\rangle \\ &= \frac{1}{\sqrt{2^3}} \left[ e^{i2\pi j \cdot 0} |000\rangle + e^{i2\pi j \cdot \frac{1}{2^3}} |001\rangle + e^{i2\pi j \cdot \frac{2}{2^3}} |010\rangle + e^{i2\pi j \cdot \frac{3}{2^3}} |011\rangle \right. \\ & \quad \left. + e^{i2\pi j \cdot \frac{4}{2^3}} |100\rangle + e^{i2\pi j \cdot \frac{5}{2^3}} |101\rangle + e^{i2\pi j \cdot \frac{6}{2^3}} |110\rangle + e^{i2\pi j \cdot \frac{7}{2^3}} |111\rangle \right] \\ &= \sum_{k_1=0}^1 \left( e^{i2\pi j \cdot \lceil k_1 2^{-1} \rceil} |k_1 00\rangle + e^{i2\pi j \cdot \lceil k_1 2^{-1} + \frac{1}{2^3} \rceil} |k_1 01\rangle + e^{i2\pi j \cdot \lceil k_1 2^{-1} + \frac{2}{2^3} \rceil} |k_1 10\rangle + e^{i2\pi j \cdot \lceil k_1 2^{-1} + \frac{3}{2^3} \rceil} |k_1 11\rangle \right) \\ &= \sum_{k_1=0}^1 \sum_{k_2=0}^1 \left( e^{i2\pi j \cdot \lceil k_1 2^{-1} + k_2 2^{-2} \rceil} |k_1 k_2 0\rangle + e^{i2\pi j \cdot \lceil k_1 2^{-1} + k_2 2^{-2} + \frac{1}{2^3} \rceil} |k_1 k_2 1\rangle \right) \\ &= \sum_{k_1=0}^1 \sum_{k_2=0}^1 \sum_{k_3=0}^1 e^{i2\pi j \cdot \lceil k_1 2^{-1} + k_2 2^{-2} + k_3 2^{-3} \rceil} |k_1 k_2 k_3\rangle = \sum_{k_1=0}^1 \sum_{k_2=0}^1 \sum_{k_3=0}^1 e^{i2\pi j \cdot \lceil \sum_{q=1}^3 k_q 2^{-q} \rceil} |k_1 k_2 k_3\rangle \\ &= \sum_{k_1=0}^1 \sum_{k_2=0}^1 \sum_{k_3=0}^1 \prod_{q=1}^3 (\otimes) e^{i2\pi j k_q 2^{-q}} |k_q\rangle = \prod_{q=1}^3 (\otimes) \left( \sum_{k_q=0}^1 e^{i2\pi j k_q 2^{-q}} |k_q\rangle \right) = \prod_{q=1}^3 (\otimes) \left( |0\rangle + e^{i2\pi j 2^{-q}} |1\rangle \right) \\ &= \left( |0\rangle + e^{i2\pi j 2^{-1}} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi j 2^{-2}} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi j 2^{-3}} |1\rangle \right) \\ &= \left. \begin{array}{l} j = j_1 2^2 + j_2 2^1 + j_3 2^0 \\ \frac{j}{2} = j_1 2^1 + j_2 2^0 + j_3 2^{-1} \\ \frac{j}{4} = j_1 2^0 + j_2 2^{-1} + j_3 2^{-2} \\ \frac{j}{8} = j_1 2^{-1} + j_2 2^{-2} + j_3 2^{-3} \end{array} \right| \\ &= \left( |0\rangle + e^{i2\pi(j_1 2^1 + j_2 2^0 + j_3 2^{-1})} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_1 2^0 + j_2 2^{-1} + j_3 2^{-2})} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_1 2^{-1} + j_2 2^{-2} + j_3 2^{-3})} |1\rangle \right) \\ &= \left( |0\rangle + e^{i2\pi j_3 2^{-1}} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_2 2^{-1} + j_3 2^{-2})} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_1 2^{-1} + j_2 2^{-2} + j_3 2^{-3})} |1\rangle \right). \end{aligned}$$

Postać iloczynowa kwantowej transformacji Fouriera,



$$\frac{1}{\sqrt{2^n}} \left[ \left( |0\rangle + e^{i2\pi(j_n 2^{-1})} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_{n-1} 2^{-1} + j_n 2^{-2})} |1\rangle \right) \otimes \dots \otimes \left( |0\rangle + e^{i2\pi(j_1 2^{-1} + j_2 2^{-2} + \dots + j_n 2^{-n})} |1\rangle \right) \right],$$

umożliwia konstrukcję wydajnego układu kwantowego realizującego transformację,



gdzie stan  $|x_n\rangle = |0\rangle + e^{i2\pi(\frac{j_1 + \dots + j_n}{2^n})} |1\rangle, \dots, |x_1\rangle = |0\rangle + e^{i2\pi \frac{j_n}{2}} |1\rangle$ .

Powyższy układ składa się z  $n$  bramek Hadamarda, z  $(n-1) + (n-2) + \dots + 1 = \frac{(n-1)(n-2)}{2}$

z dwu-qubitowych kontrolowanych bramek  $R_k$ , oraz z  $\frac{n}{2}$  bramek SWAP (pierwszy z ostatnim, drugi z przedostatnim, itd.). Bramki typu  $R_k$  odpowiadają unitarnej transformacji,

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^k}} \end{pmatrix}.$$

Można prześledzić działanie powyższego układu na przykładowym stanie  $|j_1\rangle \otimes \dots \otimes |j_n\rangle = |j_1 \dots j_n\rangle$ . Rozważmy działanie układu na ostatni qubit  $|j_n\rangle$

$$H|j_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \frac{j_n}{2}} |1\rangle \right) \begin{matrix} \xrightarrow{j_n=0} e^0 \\ \xrightarrow{j_n=1} e^{i\pi} \end{matrix}.$$

Następnie pierwszy qubit zamienia się z ostatnim, czyli,

$$|j_n\rangle \leftrightarrow |j_1\rangle.$$

Czyli końcowy stan pierwszego qubitów wynosi

$$|x_1\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \frac{j_n}{2}} |1\rangle \right).$$



Na przedostatni qubit  $|j_{n-1}\rangle$  najpierw działa bramka Hadamarda, a następnie kontrolowana bramka  $R_2$  oraz zostaje on zamieniony z qubitem 2.

$$H|j_{n-1}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \frac{j_{n-1}}{2}} |1\rangle \right).$$

Bramka  $R_2$  jest kontrolowana przez ostatni qubit i posiada postać,

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{4}} \end{pmatrix}.$$

Zatem można zapisać,

$$R_2^{(j_n)} H|j_{n-1}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \frac{j_{n-1}}{2}} e^{i2\pi \frac{j_n}{4}} |1\rangle \right) = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \left( \frac{j_{n-1}}{2} + \frac{j_n}{4} \right)} |1\rangle \right).$$

W wyniku zamiany z drugim qubitem

$$|j_{n-1}\rangle \leftrightarrow |j_2\rangle.$$

stan końcowy drugiego qubitu ma postać,

$$|x_2\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \left( \frac{j_{n-1}}{2} + \frac{j_n}{4} \right)} |1\rangle \right).$$

Podobnie dla stanu  $|j_{n-2}\rangle$ ,

$$R_3^{(j_n)} R_2^{(j_{n-1})} H|j_{n-2}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \left( \frac{j_{n-2}}{2} + \frac{j_{n-1}}{4} + \frac{j_n}{8} \right)} |1\rangle \right), |j_{n-2}\rangle \leftrightarrow |j_3\rangle,$$

$$\Rightarrow |x_3\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \left( \frac{j_{n-2}}{2} + \frac{j_{n-1}}{4} + \frac{j_n}{8} \right)} |1\rangle \right).$$

Powtarzając tą procedurę dla kolejnych stanów otrzyma się wyrażenie na stan  $|j_1\rangle$ ,

$$R_n^{(j_n)} R_{n-1}^{(j_{n-1})} \dots R_3^{(j_3)} R_2^{(j_2)} H|j_1\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi \left( \frac{j_1}{2} + \frac{j_2}{4} + \dots + \frac{j_n}{2^n} \right)} |1\rangle \right).$$

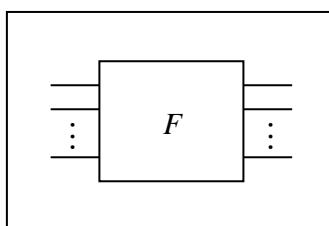
Po zastosowaniu operacji SWAP uzyska się stan wyjściowy  $|x_n\rangle$ ,

$$|x_n\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi\left(\frac{j_1}{2} + \frac{j_2}{4} + \dots + \frac{j_n}{2^n}\right)} |1\rangle \right).$$

Zatem, stan końcowy całego układu przyjmuje postać,

$$\begin{aligned} |x\rangle &= |x_1\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_n\rangle \\ &= \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi\frac{j_1}{2}} |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi\left(\frac{j_{n-1}}{2} + \frac{j_n}{4}\right)} |1\rangle \right) \otimes \dots \otimes \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2\pi\left(\frac{j_1}{2} + \frac{j_2}{4} + \dots + \frac{j_n}{2^n}\right)} |1\rangle \right) \\ &= \frac{1}{\sqrt{2^n}} \left[ \left( |0\rangle + e^{i2\pi(j_n 2^{-1})} |1\rangle \right) \otimes \left( |0\rangle + e^{i2\pi(j_{n-1} 2^{-1} + j_n 2^{-2})} |1\rangle \right) \otimes \dots \otimes \left( |0\rangle + e^{i2\pi(j_1 2^{-1} + j_2 2^{-2} + \dots + j_n 2^{-n})} |1\rangle \right) \right]. \end{aligned}$$

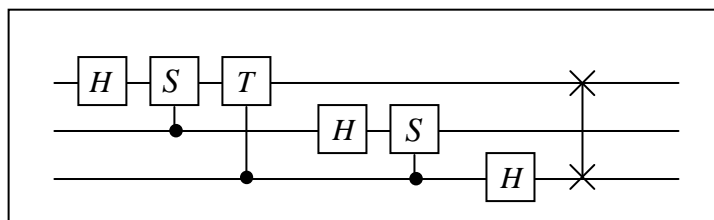
Można wprowadzić oznaczenie dla wielo-qubitowej bramki realizującej kwantową transformatę Fouriera (QTF):



Jako przykład, można wykorzystać bramkę fazy oraz bramkę  $\frac{\pi}{8}$  do zrealizowania układu wykonujący kwantową transformatę Fouriera dla trzech qubitów. Bramka fazy posłuży jako bramka  $R_2$  a bramka  $\frac{\pi}{8}$  jako  $R_3$ ,

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} = R_2, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = R_3.$$

Taki układ ma następującą postać,



Dla powyższego układu można podać postać macierzową operatora kwantowej transformaty Fouriera,



$$\frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & e^{i\frac{2\pi}{8}} & e^{i\frac{2\pi}{4}} & e^{i2\pi\frac{3}{8}} & e^{i2\pi\frac{1}{2}} & e^{i2\pi\frac{5}{8}} & e^{i2\pi\frac{6}{8}} & e^{i2\pi\frac{7}{8}} \\ 1 & e^{i\frac{2\pi}{4}} & e^{i2\pi\frac{1}{2}} & e^{i2\pi\frac{6}{8}} & 1 & e^{i\frac{2\pi}{4}} & e^{i2\pi\frac{1}{2}} & e^{i2\pi\frac{6}{8}} \\ 1 & e^{i2\pi\frac{3}{8}} & e^{i2\pi\frac{6}{8}} & e^{i\frac{2\pi}{8}} & e^{i2\pi\frac{1}{2}} & e^{i2\pi\frac{7}{8}} & e^{i\frac{2\pi}{4}} & e^{i2\pi\frac{5}{8}} \\ 1 & e^{i2\pi\frac{1}{2}} & 1 & e^{i2\pi\frac{1}{2}} & 1 & e^{i2\pi\frac{1}{2}} & 1 & e^{i2\pi\frac{1}{2}} \\ 1 & e^{i2\pi\frac{5}{8}} & e^{i\frac{2\pi}{4}} & e^{i2\pi\frac{7}{8}} & e^{i2\pi\frac{1}{2}} & e^{i\frac{2\pi}{8}} & e^{i2\pi\frac{6}{8}} & e^{i2\pi\frac{3}{8}} \\ 1 & e^{i2\pi\frac{6}{8}} & e^{i2\pi\frac{1}{2}} & e^{i\frac{2\pi}{4}} & 1 & e^{i2\pi\frac{6}{8}} & e^{i2\pi\frac{1}{2}} & e^{i\frac{2\pi}{4}} \\ 1 & e^{i2\pi\frac{7}{8}} & e^{i2\pi\frac{6}{8}} & e^{i2\pi\frac{5}{8}} & e^{i2\pi\frac{1}{2}} & e^{i2\pi\frac{3}{8}} & e^{i\frac{2\pi}{4}} & e^{i\frac{2\pi}{8}} \end{pmatrix}.$$

W ogólnym przypadku całkowita liczba bramek potrzebnych do realizacji układu kwantowej transformaty Fouriera jest rzędu:

$$n + (n-1) + (n-2) + \dots + 1 + \frac{n}{2} = \frac{n(n-1)}{2} + \frac{n}{2} \approx n^2.$$

Wynika z tego, że układ kwantowej transformacji Fouriera jest wydajny (w sensie teorii złożoności), ponieważ jego złożoność jest wielomianowa –  $O(n^2)$ .

W przypadku klasycznym, liczba operacji realizowanych przez klasyczną transformatę Fouriera,

$$X_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{i\frac{2\pi nk}{N}} x_n.$$

odpowiada złożoności  $O(N^2) = O(2^{2n})$ .

Pomimo tego, że możliwe jest przyspieszenie algorytmu klasycznej transformaty Fouriera poprzez zastosowanie tzw. szybkiej transformaty Fouriera, jej złożoność (choć znacznie zmniejszona) pozostaje nadal rzędu eksponentialnego  $O(N \log_2 N) = O(n2^n)$ . W związku z tym w przypadku klasycznym nie istnieje efektywny algorytm transformaty Fouriera.

Należy jednak podkreślić, że w związku z fundamentalnym charakterem schematu pomiaru w mechanice kwantowej dostęp do informacji kwantowej jest znacznie ograniczony. W związku z tym nie wszystkie współczynniki wyliczone kwantową transformatą Fouriera są dostępne dla klasycznego obserwatora, w odróżnieniu od rezultatów klasycznej transformaty Fouriera. Jednakże, zastosowanie kwantowej transformaty Fouriera jest niezmiernie przydatne w różnych algorytmach kwantowych, gdzie klasyczny dostęp do wynikowych współczynników nie jest potrzebny.





## 18. Algorytm Grovera – poszukiwanie igły w stogu siana (*finding needle in a haystack*)

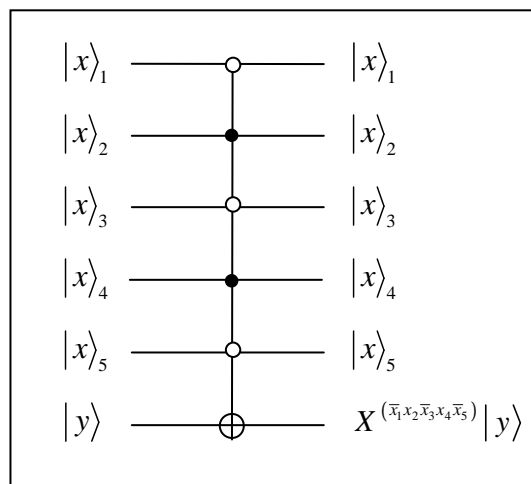
Klasyczne przeszukiwanie zbioru (np. bazy danych) w poszukiwaniu danego elementu (przy założeniu występowania tylko jednej kopii szukanego elementu) skaluje się liniowo z liczbą elementów – odpowiada to złożoności  $O(N)$ . Grover podał algorytm kwantowy, który proces wyszukiwania przyspieszenie pierwiastkowe, zmieniając złożoność do  $O(\sqrt{N})$ . Algorytm Grovera zakłada istnienie kwantowej procedury określającej, czy poszukiwany element został znaleziony, czyli czy wyreprezentowana przez  $n$  qubitów liczba całkowita jest poszukiwaną liczbą, zwracając odpowiedź poprzez funkcję  $f(x)$

$$f(x) = \begin{cases} 0, & x \neq a \\ 1, & x = a \end{cases}$$

Grover pokazał, że jego algorytm kwantowy – w najgorszym przypadku – nie wymaga sprawdzenia wszystkich (dla poszukiwanej  $n$ -bitowej liczby całkowitej)  $2^n$  elementów, tak jak jego klasyczny odpowiednik. Implementacja tego algorytmu opiera się na unitarnej operacji  $U_f$ , która działa na  $n$ -qubitowy rejestr wejściowy reprezentujący liczbę  $x$ , oraz posiada 1-qubitowy rejestr wyjściowy, którego stan zmienia wartość w przypadku gdy  $x = a$  lub pozostaje niezmienny w przeciwnym przypadku. Czyli

$$U_f(|x\rangle_n |y\rangle_1) = |x\rangle_n |y \oplus f(x)\rangle_1$$

Przykładowa realizacja takiego układu może mieć postać:





W ogólnym przypadku układ działa ja czarna skrzynka i nie jest wiadome, które qubity kontrolują w sposób prosty, a które w sposób odwrotny, działanie bramki  $X$  – ta informacja jest określona przez nieznaną liczbę całkowitą  $a$ . W przypadku klasycznym, należałoby sprawdzać wszystkie możliwe kombinacje do momentu, gdy nastąpi zamiana rejestru wyjściowego (dla poszukiwanej  $n$ -bitowej liczby całkowitej, w najgorszym przypadku będzie to  $2^n$  kroków). Ale w przypadku algorytmu Grovera wystarczy wykonać mniej niż  $2^{\frac{n}{2}} = \sqrt{N}$  kroków – dokładniej  $\left(\frac{\pi}{4}\right)2^{\frac{n}{2}}$ , gdy  $N$  jest dostatecznie duże (wtedy prawdopodobieństwo sukcesu jest równe prawie 1).

Przydatne jest odwrócenia operacji zamiany stanu rejestru wyjściowego na operację tylko zmiany znaku stanu wyjściowego. W tym celu wystarczy, aby rejestr wyjściowy był w stanie:

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

To spowoduje odpowiednią zmianę znaku, jak poniżej:

$$U_f(|x\rangle \otimes H|1\rangle) = (-1)^{f(x)}|x\rangle \otimes H|1\rangle,$$

ponieważ,

$$\begin{aligned} U_f(|x\rangle \otimes H|1\rangle) &= \frac{1}{\sqrt{2}}(|x\rangle \otimes [(|0\rangle - |1\rangle) \oplus |f(x)\rangle]) = \frac{1}{\sqrt{2}}(|x\rangle \otimes [|0\rangle \oplus |f(x)\rangle - |1\rangle \oplus |f(x)\rangle]) \\ &= \begin{cases} x = a \Rightarrow \frac{1}{\sqrt{2}}(|x\rangle \otimes [|0\rangle \oplus |1\rangle - |1\rangle \oplus |1\rangle]) = \frac{1}{\sqrt{2}}(|x\rangle \otimes [|1\rangle - |0\rangle]) = (-1)^{f(x)}(|x\rangle \otimes H|1\rangle) \\ x \neq a \Rightarrow \frac{1}{\sqrt{2}}(|x\rangle \otimes [|0\rangle \oplus |0\rangle - |1\rangle \oplus |0\rangle]) = \frac{1}{\sqrt{2}}(|x\rangle \otimes [|0\rangle - |1\rangle]) = (-1)^{f(x)}(|x\rangle \otimes H|1\rangle) \end{cases} \end{aligned}$$

Zatem, w przypadku  $x = a$ , stan całego układ zostanie pomnożony przez czynnik -1.

Z powyższego wynika, że rozważana operacja odpowiada działaniu tylko na rejestr wejściowy pewną operacją unitarną  $V$ , która działa na bazie obliczeniowej w następujący sposób,

$$V|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle, & x \neq a \\ -|a\rangle, & x = a \end{cases}$$

Można więc zapisać  $V$  jako,

$$V = I - 2|a\rangle\langle a|,$$

ponieważ,



$$V|x\rangle = |x\rangle - 2|a\rangle\langle a|x\rangle = \begin{cases} |x\rangle, & \langle a|x\rangle = 0 \\ -|a\rangle, & x = a \end{cases}.$$

(liniowość  $V$  wynika z liniowości  $U_f$ ). W przypadku działania na dowolny stan  $|\psi\rangle$  będący superpozycją stanów  $|x\rangle_n$  bazy obliczeniowej, operacja  $V$  zmienia znak składowej  $|a\rangle$ , a pozostałe składowe pozostawia niezmiennione,

$$V|\psi\rangle = |\psi\rangle - 2|a\rangle\langle a|\psi\rangle.$$

Czyli, dla ogólnego przypadku można zapisać,

$$U_f(|\psi\rangle \otimes H|1\rangle) = [|\psi\rangle - 2|a\rangle\langle a|\psi\rangle] \otimes H|1\rangle.$$

Można zauważyć, że operacja  $U_f$  pozostawia stan  $H|1\rangle$  niesplątany z resztą układu i stan ten pozostaje niesplątany z rejestrem wejściowym przez cały czas działania algorytmu – dlatego można stan  $H|1\rangle$  pominąć w reszcie rozważań, co ułatwi zapis.

Rozważmy dowolny stan układu wejściowego. Można go przyjąć, jako superpozycję wszystkich możliwych stanów wejściowych – wykorzystując operacje Hadamarda,

$$|\varphi\rangle = H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n.$$

Oprócz operacji  $V$  potrzebna jest także operacji  $W$ , która działa podobnie do  $V$ , ale nie jest zależna od  $a$ . Unitarna transformacja  $W$  zachowuje znak współczynnika stojącego przy stanie  $|\varphi\rangle$  zmieniając znak wszystkich innych stanów na przeciwny:

$$W = 2|\varphi\rangle\langle\varphi| - I.$$

Algorytm Grovera sprowadza się do wielokrotnego powtarzania operacji  $WV$ . Rozważmy działanie  $WV$  na stan początkowy  $|\varphi\rangle$ . Wiadomo, że  $\langle a|\varphi\rangle = \langle\varphi|a\rangle = \frac{1}{\sqrt{2^n}}$ ,

$$\begin{aligned} V|a\rangle &= -|a\rangle, \\ V|\varphi\rangle &= |\varphi\rangle - \frac{2}{\sqrt{2^n}}|a\rangle, \\ W|\varphi\rangle &= |\varphi\rangle, \\ W|a\rangle &= \frac{2}{\sqrt{2^n}}|\varphi\rangle - |a\rangle. \end{aligned}$$

Przykładowo, można zapisać,

$$\begin{aligned} WVWVWV|\varphi\rangle &= WVWVW\left(|\varphi\rangle - \frac{2}{\sqrt{2^n}}|a\rangle\right) = WVWV\left(W|\varphi\rangle - \frac{2}{\sqrt{2^n}}W|a\rangle\right) \\ &= WVWV\left(|\varphi\rangle - \frac{2}{\sqrt{2^n}}\left(\frac{2}{\sqrt{2^n}}|\varphi\rangle - |a\rangle\right)\right) = WVWV\left(|\varphi\rangle\left[1 - \frac{2}{\sqrt{2^n}} \cdot \frac{2}{\sqrt{2^n}}\right] + \frac{2}{\sqrt{2^n}} \cdot \frac{2}{\sqrt{2^n}}|a\rangle\right). \end{aligned}$$

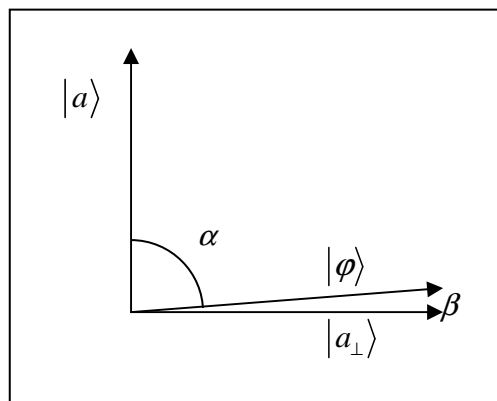
Z postaci  $|\varphi\rangle$  wynika, że  $|a\rangle$  i  $|\varphi\rangle$  są prawie prostopadłe, ponieważ,

$$\cos \alpha = \langle a|\varphi\rangle = \frac{1}{\sqrt{2^n}} \leq \frac{1}{\sqrt{N}}.$$

Można zdefiniować stan  $|a_{\perp}\rangle$  będący znormalizowaną liniową kombinacją stanów  $|a\rangle$  i  $|\varphi\rangle$ , która jest ortogonalna do stanu  $|a\rangle$  i tworzy mały kąt  $\beta = \frac{\pi}{2} - \alpha$  ze stanem  $|\varphi\rangle$ . Obliczając sinus kąta  $\beta = \frac{\pi}{2} - \alpha$  mamy,

$$\sin \beta = \cos \alpha = \langle a|\varphi\rangle = \frac{1}{\sqrt{2^n}} \leq \frac{1}{\sqrt{N}},$$

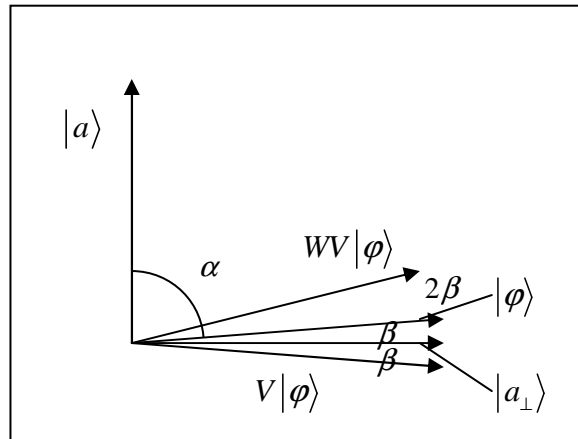
oraz dla dostatecznie dużego  $N$  można przyjąć, że  $\beta \approx \frac{1}{\sqrt{2^n}}$ .



Ponieważ operacja  $W$  pozostawia stan  $|\varphi\rangle$  niezmieniony, a dowolny wektor, który jest prostopadły do stanu  $|\varphi\rangle$  zmienia na przeciwny, więc operację  $W$  można traktować jako odbicie lustrzane względem prostej przechodzącej przez środek i wyznaczonej przez stan  $|\varphi\rangle$ . Operacja  $V$  zmienia stan  $|a\rangle$  na przeciwny, a dowolny inny wektor prostopadły do stanu  $|a\rangle$  pozostawia niezmieniony. Czyli operację  $V$  można z kolei traktować jako odbicie lustrzane



względem prostej wyznaczonej przez stan  $|a_{\perp}\rangle$ . Operacja  $WV$  jest złożeniem dwóch odbić – czyli jest dwuwymiarowym obrotem. Efekt rotacji  $WV$  stanu  $|a_{\perp}\rangle - V$  pozostawia stan niezmienny, a  $W$  odbija go względem stanu  $|\varphi\rangle$ .



Czyli jest to rotacja o kąt  $2\beta$ . Operacja  $WV$  obróci dowolny wektor o  $2\beta$  w kierunku od  $|a_{\perp}\rangle$  do  $|\varphi\rangle$  (rys. powyżej). Działając  $WV$  na stan  $|\varphi\rangle$  otrzymamy stan obrócony o  $3\beta$  od stanu  $|a_{\perp}\rangle$ , bo początkowo  $|\varphi\rangle$  było obrócone o  $\beta$  od stanu  $|a_{\perp}\rangle$ . Kolejne zastosowanie  $WV$  oddala wynikowy stan od  $|a_{\perp}\rangle$  o  $2\beta$ . Jako, że  $\beta \approx \frac{1}{\sqrt{2^n}}$ , to po całkowitej liczbie kroków,

która jest najbliższa  $\frac{\pi}{4} 2^{\frac{n}{2}}$ , wektor wynikowy będzie prawie równoległy do wektora  $|a\rangle$ .

Liczbę powtórzeń  $k$  można wyznaczyć z warunku,

$$\frac{\pi}{2} = \frac{1}{\sqrt{2^n}} + 2k \frac{1}{\sqrt{2^n}} \Rightarrow 1 + 2k = \frac{\pi}{2} \sqrt{2^n} .$$

Dla odpowiednio dużych  $k$  można zapisać,  $k = \left[ \frac{\pi}{4} \sqrt{2^n} \right]$ .

Zatem, w wyniku pomiaru w bazie obliczeniowej końcowego stanu, z prawdopodobieństwem bliskim 1 uzyska się poszukiwany wynik  $|a\rangle$ . Można sprawdzić czy  $f(a) = 1$ . Jeśli nie, to w celu zwiększenia dokładności można powtórzyć procedurę kilka razy.

## 19. Algorytm Shora – łamanie szyfru RSA

Co wie BOB?	Co wie ALICE?	Co jest publicznie znane?
Dwie liczby pierwsze: $p$ i $q$ ,	Wiadomość $a$ do	Zakodowana wiadomość $b$



oraz liczby $c$ i $d$ , takie, że $cd = 1 \pmod{(p-1)(q-1)}$	zakodowania. Tylko $c$ (nie zna $d$ ), oraz tylko $N = pq$ (nie zna poszczególnych mnożników $p$ i $q$ ) Zakodowana wiadomość: $b = a^c \pmod{N}$	Tylko $c$ (nie jest znane $d$ ), oraz tylko $N = pq$ (nie są znane poszczególne mnożniki)
Dekodowanie: $a = b^d \pmod{N}$		Komputer kwantowy znajduje $r$ : $b^r = 1 \pmod{N}$ Klasyczny komputer znajduje $d'$ $cd' = 1 \pmod{r}$ $a = b^{d'} \pmod{N}$

Jeśli  $c$  nie posiada wspólnego dzielnika z  $(q-1)(p-1)$  to istnieje takie  $d$ , dla którego powyższe jest spełnione.

Wiadome jest, że  $a^{1+s(q-1)(p-1)} = a \pmod{pq}$ , to jeżeli  $cd = 1 + s(p-1)(q-1)$ , zatem

$$a^{cd} = a \pmod{pq}$$

$$b = a^c \pmod{pq} \text{ (z małej teorii Fermata)}$$

$$b^d = a \pmod{pq}$$

Szyfr RSA można złamać, jeśli posiada się szybką metodę wyszukiwania okresu  $r$  znanej funkcji okresowej:

$$f(x) = b^x \pmod{N}$$

Wydawałoby się, że jest to dość proste, szczególnie, że z okresowości funkcji mamy:

$$f(x+s) = f(x) \Leftrightarrow s = kr,$$

gdzie  $k$  jest liczbą całkowitą. Jeśli znanych jest kilka różnych wielokrotności okresu, to można z dużym prawdopodobieństwem znaleźć sam okres  $r$  (np. wykorzystując algorytm Euklidesa).

### Algorytm Euklidesa

W celu znalezienia wspólnego dzielnika dwóch liczb  $A$  i  $B$ , należy wykonać następujące kroki:

$$\frac{A}{B} = l.\text{całkowita} + \frac{a_1}{B} \Rightarrow \frac{B}{a_1} = l.\text{całkowita} + \frac{a_2}{B} \Rightarrow \dots$$



Np.

$$\left. \begin{aligned} \frac{168}{35} &= 4 + \frac{28}{35} \Rightarrow \frac{35}{28} = 1 + \frac{7}{28} \Rightarrow \frac{28}{7} = 4 + \frac{0}{7} \\ \frac{170}{35} &= 4 + \frac{30}{35} \Rightarrow \frac{35}{30} = 1 + \frac{5}{30} \Rightarrow \frac{30}{5} = 6 + \frac{0}{5} \end{aligned} \right\} 5,7$$

### Przykłady

$$N = 15, \quad y = 8$$

$n$	0	1	2	3	4	5	6
$y^n$	1	8	64	512	4096	32768	262144
$y^n \bmod N$	1	8	4	2	1	8	4

$$r = 4$$

$$\left. \begin{aligned} y^{\frac{r}{2}} - 1 &= 63 = 3^2 \cdot 7 \\ y^{\frac{r}{2}} + 1 &= 65 = 5 \cdot 13 \end{aligned} \right\} \Rightarrow 3,5$$

$$N = 15, \quad y = 7$$

$n$	0	1	2	3	4	5	6
$y^n$	1	7	49	343	2041	16807	117694
$y^n \bmod N$	1	7	4	13	1	7	4

$$r = 4$$

$$\left. \begin{aligned} y^{\frac{r}{2}} - 1 &= 48 = 2^4 \cdot 3 \\ y^{\frac{r}{2}} + 1 &= 50 = 2 \cdot 5^2 \end{aligned} \right\} \Rightarrow 3,5$$

$$N = 35, \quad y = 13$$

$n$	0	1	2	3	4	5	6
$y^n$	1	13	169	2197	28561	371293	4826809
$y^n \bmod N$	1	13	29	27	1	13	29

$$r = 4$$

$$y^{\frac{r}{2}} - 1 = 168 = 2^3 \cdot 3 \cdot 7$$

$$y^{\frac{r}{2}} + 1 = 170 = 2 \cdot 5 \cdot 17$$

Zgodnie z algorytmem Euklidesa,

$$\frac{A}{B} = l.calkowita + \frac{a_1}{B} \Rightarrow \frac{B}{a_1} = l.calkowita + \frac{a_2}{B} \Rightarrow \dots$$

Czyli dla powyższych liczb można zapisać:



$$\left. \begin{aligned} \frac{168}{35} &= 4 + \frac{28}{35} \Rightarrow \frac{35}{28} = 1 + \frac{7}{28} \Rightarrow \frac{28}{7} = 4 + \frac{0}{7} \\ \frac{170}{35} &= 4 + \frac{30}{35} \Rightarrow \frac{35}{30} = 1 + \frac{5}{30} \Rightarrow \frac{30}{5} = 6 + \frac{0}{5} \end{aligned} \right\} 5,7$$

Należy jednak zwrócić uwagę na fakt, że wartości rozważanej funkcji  $f(x) = b^x \pmod{N}$  w odróżnieniu od prostych, gładkich funkcji periodycznych (np.  $\sin$ ,  $\cos$ , itp.) nie wskazują na żadną prawidłowość – można powiedzieć, że jest to funkcja losowego szumu z okresem. Żaden zakres wartości między okresami nie wskazuje na prawdopodobną wartość okresu funkcji. Z tego powodu w przypadku klasycznym, próba określenia okresu takiej funkcji sprowadza się do wyliczania wartości  $f$  dla losowego zbioru liczb całkowitych do momentu aż nie zostanie znaleziona wartość funkcji identyczna do wyliczonej wcześniej.

### Skalowanie

Niech  $n_0$  będzie liczbą bitów w reprezentacji binarnej liczby  $N = pq$ , wtedy  $2^{n_0}$  to najniższa potęga 2 przekraczająca  $N = pq$ . Dla liczby 500 znakowej w reprezentacji dziesiętnej (typowy rozmiar dla wykorzystania kryptograficznych), liczba bitów w reprezentacji binarnej wynosi około 1700. Podobne skale można przyjąć dla  $a$ ,  $b$ , oraz okresu  $\pmod{N}$   $r$ . Czyli złożoność problemu znalezienia okresu skaluje się eksponentalnie z  $n_0$ .

W przypadku kwantowym, w związku z istnieniem kwantowej równoległości, procedura wyliczenia okresu (z prawdopodobieństwem bliskim 1) skaluje się wielomianowo z  $n_0$ .

Można rozważyć układ kwantowy, który posiada rejestr wejściowy oraz rejestr wyjściowy. Aby umożliwić reprezentację  $x$  i  $f(x)$  w przedziale od 0 do  $N$ , należy przyjąć rozmiary obu rejestrów nie mniejsze niż  $n_0$ . Dla odpowiedniej efektywności przyjmuje się rejestr wejściowy o rozmiarze  $n = 2n_0$ . Podwojenie rejestru wejściowego zapewne zawieranie przynajmniej  $N$  pełnych okresów funkcji  $f$ .

Działanie rozpoczyna się od skonstruowania stanu:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle_n |f(x)\rangle_{n_0}.$$

Czyli najpierw wprowadzamy rejestr wejściowy i wyjściowy w superpozycję bramkami Hadamarda  $H^{\otimes n}$  (z dokładnością do globalnego czynnika fazowego), a następnie działamy operacją  $U_f (|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$ .





Założmy, że po dokonaniu pomiaru stanu  $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle_n |f(x)\rangle_{n_0}$  otrzymamy wartość  $f_0$ , wtedy można zapisać stan rejestru wejściowego w postaci:

$$|\psi\rangle_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n,$$

gdzie  $x_0$  jest najmniejszą wartością  $x$  ( $0 \leq x_0 < r$ ) dla której  $f(x_0) = f_0$ , a  $m$  jest najmniejszą liczbą całkowitą dla której  $mr + x_0 \geq 2^n$ , zatem,

$$m = \left\lceil \frac{2^n}{r} \right\rceil, \quad m = \left\lceil \frac{2^n}{r} \right\rceil + 1,$$

w zależności od liczby  $x_0$ . Gdyby posiadać kilka kopii stanu  $|\psi\rangle_n$  to można by wykonać parę pomiarów, następnie wziąć ich różnicę i w ten sposób otrzymać zbiór różnych wielokrotności okresu, co umożliwiłoby obliczenie okresu (np. algorytmem Euklidesa). Jest to jednak niemożliwe zgodnie z twierdzeniem No-cloning. Pojedynczy pomiar zwróci jedynie wartość  $x_0 + kr$  dla zupełnie losowego  $x_0$ , co uniemożliwi wydobycie jakiegokolwiek informacji o okresie.

Należy podkreślić, że wykonanie pomiaru  $f_0$  nie jest konieczne – można pracować na całym stanie wejściowym, co w rezultacie da dodatkową sumę. Taki pomiar można rozważyć teoretycznie i pominąć niepotrzebne człony, nie wpływające na działanie algorytmu.

Należy następnie zastosować kwantową transformatę Fouriera,

$$U_{FT} = \left( \sum_{x=0}^{2^n-1} \alpha(x) |x\rangle \right) = \sum_{x=0}^{2^n-1} \beta(x) |x\rangle,$$

$$\beta(x) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{i2\pi xy}{2^n}} \alpha(x).$$

Działanie kwantowej transformaty Fouriera  $U_{FT}$  na stan  $|\psi\rangle_n$  będzie postaci,

$$U_{FT} \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{\frac{i2\pi(x_0+kr)y}{2^n}} |y\rangle$$

$$= \sum_{y=0}^{2^n-1} e^{\frac{i2\pi x_0 y}{2^n}} \frac{1}{\sqrt{2^n m}} \sum_{k=0}^{m-1} \left( e^{\frac{i2\pi k r y}{2^n}} \right) |y\rangle.$$



Jeżeli teraz zostanie przeprowadzony pomiar, to prawdopodobieństwo  $p(y)$  otrzymania stanu  $y$  jest kwadratem współczynnika stojącego przy  $|y\rangle$ . Czynniki  $e^{\frac{i2\pi x_0 y}{2^n}}$  zniknie pod modułem (problem z losowym  $x_0$  także). Czyli można zapisać prawdopodobieństwo,

$$p(y) = \frac{1}{2^n m} \left| \sum_{k=0}^{m-1} e^{\frac{i2\pi k r y}{2^n}} \right|^2$$

$$\left| \sum_{k=0}^{m-1} e^{\frac{i2\pi k r y}{2^n}} \right|^2 = \left| \frac{1 - e^{\frac{i2\pi r y}{2^n} m}}{1 - e^{\frac{i2\pi r y}{2^n}}} \right|^2$$

$$\begin{aligned} |1 - e^{i\alpha}|^2 &= (1 - e^{i\alpha})(1 - e^{-i\alpha}) = 1 - e^{i\alpha} - e^{-i\alpha} + 1 = 2 - 2\cos\alpha \\ &= 2(1 - \cos\alpha) = 2\left(1 - \cos 2\frac{\alpha}{2}\right) \end{aligned}$$

$$\begin{aligned} \cos 2x &= 1 - 2\sin^2 x \\ 2\left(1 - \cos 2\frac{\alpha}{2}\right) &= 2\left(1 - 1 + 2\sin^2 \frac{\alpha}{2}\right) = 4\sin^2 \frac{\alpha}{2} \end{aligned}$$

$$\left| \sum_{k=0}^{m-1} e^{\frac{i2\pi k r y}{2^n}} \right|^2 = \left| \frac{1 - e^{\frac{i2\pi r y}{2^n} m}}{1 - e^{\frac{i2\pi r y}{2^n}}} \right|^2 = \frac{4\sin^2 \frac{\frac{i2\pi r y}{2^n} m}{2}}{4\sin^2 \frac{\frac{i2\pi r y}{2^n}}{2}} = \frac{\sin^2 \frac{\pi r m y}{2^n}}{\sin^2 \frac{\pi r y}{2^n}}$$

Prowadzi to do postaci:

$$p(y) = \frac{1}{2^n m} \frac{\sin^2 \frac{\pi r m y}{2^n}}{\sin^2 \frac{\pi r y}{2^n}}$$

Okazuje się, że powyższa funkcja prawdopodobieństwa osiąga maksimum przy  $y$  bliskim całkowitej wielokrotności  $\frac{2^n}{r}$ . Można rozważyć otoczenie całkowitej wielokrotności  $\frac{2^n}{r}$  (np. rzędu  $\frac{1}{2}$ ), czyli przyjąć  $y = y_j = j\frac{2^n}{r} + \delta_j$ , gdzie  $|\delta_j| \leq \frac{1}{2}$ . (prawdopodobieństwo powyżej 40%)

$$p(y_j) = \frac{1}{2^n m} \frac{\sin^2 \frac{\pi r m \delta_j}{2^n}}{\sin^2 \frac{\pi r \delta_j}{2^n}}$$



Wiemy, że  $m$  jest liczbą całkowitą bliską  $\frac{2^n}{r}$  oraz, że  $\frac{2^n}{r} \geq \frac{N^2}{r} > N$ , można zastąpić  $\frac{mr}{2^n}$  przez 1, oraz zamienić dolny sinus przez bardzo mały argument,

$$p(y_j) \approx \frac{1}{2^n m} \left[ \frac{\sin \pi \delta_j}{\frac{\pi r \delta_j}{2^n}} \right]^2 = \frac{2^{2n}}{2^n m r^2} \left[ \frac{\sin \pi \delta_j}{\pi \delta_j} \right]^2 = \frac{1}{r} \left[ \frac{\sin \pi \delta_j}{\pi \delta_j} \right]^2.$$

Dla  $0 \leq x \leq \frac{\pi}{2}$  wiemy, że  $\frac{2x}{\pi} \leq \sin x$ , a skoro  $\delta_j \leq \frac{1}{2}$ , to

$$p(y_j) \approx \frac{1}{r} \left[ \frac{2}{\pi} \right]^2.$$

Należy zauważyć, że istnieje przynajmniej  $r-1$  różnych wartości  $j$ , okres może być bardzo duża liczbą, więc widać, że z prawdopodobieństwa minimum 40% ( $\frac{4}{\pi^2} = 0,4053$ ) otrzymamy założoną wartość  $y$ , która znajduje się w otoczeniu  $\frac{1}{2}$  całkowitej wielokrotności  $\frac{2^n}{r}$ .

Jeżeli znaleźliśmy  $y$ , które jest właśnie w takim otoczeniu to, można zapisać:

$$\left| \frac{y}{2^n} - \frac{j}{r} \right| \leq \frac{1}{2^{n+1}},$$

Znając  $y$  oraz  $n$ , otrzymujemy zatem przybliżenie na  $\frac{j}{r}$ .



## 20. Literatura

- [1] M. B. Menskij, Usp. Fiz. Nauk **169**, 1017 (1998)
- [2] W. Żurek, Phys.Rev.D **26**, 1862 (1982)
- [3] D. Aharonov, *Quantum computation*, arxiv quant-ph/98 12037 (1999)
- [4] J. Preskill, *Quantum Information and Computation*,  
[http:// www.theory.caltech.edu/~preskill/ph229](http://www.theory.caltech.edu/~preskill/ph229) (1998)
- [5] D. Bouwmeester, A. Ekert, A. Zeilinger, *The Physics of Quantum Information*, Springer Verlag (2000)
- [6] W. Wootters, W. Żurek, Nature **299**, 802 (1982)
- [7] H. Barnum et al, Phys.Rev.Lett. **76**, 2818 (1996)
- [8] A. K. Pati, S. L. Braunstein, Nature **404**, 184 (2000); W. Żurek, Nature **404**, 130 (2000)
- [9] D. Gottesman, I. L. Chuang, Nature **402**, 390 (1999)
- [10] Ch. Bennet, D. DiVincenzo, Nature, **404** (2000); D. DiVincenzo, Science **270**, 255 (1995);
- [11] M. H. Friedman, arxiv quant-ph/0101025 (2001); A. Kitaev, Russian Math. Survey, **52**, 1191 (1997)
- [12] D. DiVincenzo et al, Nature **408**, 339 (2000)
- [13] D. Loss, D. DiVincenzo, Phys. Rev. A **57**, 120 (1998); G. Burkard et al, Phys. Rev. B **59**, 2070 (1999)
- [14] P. Zanardi, F. Rossi, Phys. Rev. Lett. **81**, 4752 (1998); Phys. Rev. B **59**, 6170 (1999); E. Biolatti et al, Phys. Rev. Lett. **85**, 564 7 (2000)
- [15] M. Bayer et al, Nature **405**, 923 (2000); Science **291**, 451 (2001); G. Chen et al, Science **289**, 1906 (2000)
- [16] L. Jacak et al, Acta Phys.Pol. A **99**, 277 (2001); Phys. Rev. B **72**, 245309 (2005)
- [17] J. M. Kikkawa, D. D. Awschalom, Nature **397**, 139 (1999); Physics Today, June, 33 (1999)
- [18] O. Verzeelen et al, Phys. Rev. B **62**, R4809 (2000)
- [19] ARDA Report (*Advanced Research & Development Activity – roadmap in Quantum Information* 2002), [http:// www.qist.lanl.gov](http://www.qist.lanl.gov)
- [20] N. Gershenfeld, *The Physics of Information Technology*, Cambridge U.P. 2000
- [21] M. A. Nielsen, I. L. Chuang, *Quantum Computation & Quantum Information*, Cambridge UP 2000
- [22] K. A. Suominen, *Quantum Approach to Informatics*, Wiley-Interscience, New Jersey, 2005
- [23] N. D. Mermin, *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007
- [24] W. Jacak, R. Gonczarek, L. Jacak, *Defazowanie orbitalnych i spinowych stopni swobody w kropkach kwantowych*, OW PWr 2010