Komputery kwantowe - brudnopis notatek do wykladu

http://th.if.uj.edu.pl/∼ufjacekd/KK-wyklad.pdf(.ps)

Jacek Dziarmaga[1]

[1]*Instytut Fizyki UJ, ul.Reymonta 4, 30-059 Kraków*
tel: 012-6635662
e-mail: dziarmaga@th.if.uj.edu.pl

I. PRZESTRZEN STANOW.

Przestrzen stanow w mechanice kwantowej jest przestrzenia Hilberta. Przestrzen Hilberta jest napinana przez baze wektorow ortonormalnych, ktore oznaczamy w notacji Diraca przez ,,kety"

$$|m\rangle \tag{1}$$

numerowane indeksem m. Zakladamy, ze baza jest ortonormalna czyli

$$\langle m|n\rangle = \delta_{m,n} \tag{2}$$

W tym wzorze pojawily sie ,,bra", czyli $\langle m| = |m\rangle^\dagger$. Wybor bazy nie jest jednoznaczny, bo wektory powstale z ketow $|m\rangle$ w wyniku przeksztalcenia unitarnego

$$|m^{'}\rangle = \sum_n U_{mn}|n\rangle \tag{3}$$

sa rowniez baza ortonormalna. Stan ukladu fizycznego jest opisywany wektorem w przestrzeni Hilberta, ktory jest kombinacja liniowa stanow bazowych

$$|\psi\rangle = \sum_m c_m|m\rangle \ . \tag{4}$$

Zespolone wspolczynniki c_m nazywamy w mechanice kwantowej ,,amplitudami prawdopodobienstwa".

Dzialanie komputerow kwantowych najczesciej opisuje sie w bazie znormalizowanych wektorow wlasnych macierzy Pauliego $Z = \sigma_z$

$$|1\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , |0\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ . \tag{5}$$

Mozna rowniez uzywac bazy wektorow wlasnych macierzy $X = \sigma_x$ tj.

$$|+\rangle \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \ , |-\rangle \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \ . \tag{6}$$

Te dwie bazy sa powiazane za pomoca transformacji unitarnej

$$|+\rangle = \frac{1}{\sqrt{2}} \left(|1\rangle + |0\rangle\right) \ , \tag{7}$$

$$|-\rangle = \frac{1}{\sqrt{2}} \left(|1\rangle - |0\rangle\right) \ . \tag{8}$$

Odnotujmy rowniez kilka prostych tozsamosci, ktorych w dalszej czesci bedziemy uzywac do znudzenia:

$$Z|0\rangle = -|0\rangle \ , \quad Z|1\rangle = |1\rangle \ , \tag{9}$$

$$X|-\rangle = -|-\rangle \ , \quad X|+\rangle = |+\rangle \ , \tag{10}$$

$$X|0\rangle = |1\rangle \ , \quad X|1\rangle = |0\rangle \ , \tag{11}$$

$$Z|+\rangle = |-\rangle \ , \quad Z|-\rangle = |+\rangle \ . \tag{12}$$

Te tozsamosci pokazuja jak operatory Z, X dzialaja na wektory bazy. Znajac dzialanie operatorow na wektory bazy, wiemy jak te operatory dzialaja na dowolny wektor np.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ , \tag{13}$$

$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \ , \tag{14}$$

$$Z|\psi\rangle = -\alpha|0\rangle + \beta|1\rangle \ , \tag{15}$$

Powyzsze tozsamosci oraz ortonormalnosc bazy pozwala nam zapisac operatory jako

$$Z = -|0\rangle\langle 0| + |1\rangle\langle 1| \ , \tag{16}$$

$$X = -|-\rangle\langle -| + |+\rangle\langle +| \ , \tag{17}$$

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \ , \tag{18}$$

$$Z = |+\rangle\langle -| + |-\rangle\langle +| \ . \tag{19}$$

Od tej notacji mozemy przejsc do notacji macierzowej definiujac elemety macierzowe operatora O w bazie $|m\rangle$ jako

$$O_{mn} = \langle m|O|n\rangle \ . \tag{20}$$

Na przyklad operator Z ma w bazie $|1\rangle, |0\rangle$ elementy $Z_{11} = 1, Z_{00} = -1, Z_{01} = Z_{10} = 0$, ktore mozna zebrac w macierz

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z \ . \tag{21}$$

Ten sam operator w bazie $|+\rangle, |-\rangle$ ma elementy macierzowe $Z_{++} = Z_{--} = 0, Z_{+-} = Z_{-+} = 1$, co mozna zebrac w macierz

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x \ . \tag{22}$$

Macierz operatora oczywiscie zalezy od wyboru bazy. W dalszym ciagu jesli bedzie mowa o macierzy operatora bez okreslenia bazy to znaczy, ze domyslnie chodzi o baze $|1\rangle, |0\rangle$.

II. HAMILTONIAN.

Zauwazmy, ze operatory Z, X sa hermitowskie, bo np.

$$Z^\dagger = (-|0\rangle\langle 0| + |1\rangle\langle 1|)^\dagger = -|0\rangle\langle 0| + |1\rangle\langle 1| = Z \quad (23)$$

$$X^\dagger = (|0\rangle\langle 1| + |1\rangle\langle 0|)^\dagger = |1\rangle\langle 0| + |0\rangle\langle 1| = X \ . \quad (24)$$

Jesli $|\psi\rangle$ opisuje stan kwantowy ukladu, to jego ewolucja w czasie jest opisywana przez rownanie Schrödingera

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H\ |\psi\rangle \ . \quad (25)$$

W dalszej czesci bede uzywal jednostek czasu, w ktorych efektywnie stala Plancka ,,$\hbar = 1$". Operator Hamiltona H, lub krotko ,,Hamiltonian", jest operatorem hermitowskim. Jesli H nie zalezy od czasu, to formalne rozwiazanie powyzszego rownania ma postac

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle = U(t)\ |\psi(0)\rangle \ . \quad (26)$$

Gdzie $U(t) = e^{-iHt}$ jest operatorem unitarnym.

Dla przykladu, jesli $H = X = |0\rangle\langle 1| + |1\rangle\langle 0|$, to

$$U(t) = e^{-itX} = 1\ \cos(t) - i \sin(t)\ X = \quad (27)$$

$$(|1\rangle\langle 1| + |0\rangle\langle 0|)\cos(t) - i\,(|1\rangle\langle 0| + |0\rangle\langle 1|)\sin(t) \quad (28)$$

Operator ewolucji $U(t)$ ewoluuje stan poczatkowy $|\psi(0)\rangle = |0\rangle$ w

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle = U(t)|0\rangle = |0\rangle\cos(t) - i|1\rangle\sin(t) \ . \quad (29)$$

Ewolucja z hamiltonianem $H = X$ polega na oscylacjach pomiedzy poczatkowym stanem $|0\rangle$ a stanem $|1\rangle$.

Kolejny przyklad to $H = Z = -|0\rangle\langle 0| + |1\rangle\langle 1|$. Ten hamiltonian ewoluuje stanu poczatkowy $|\psi(0) = \alpha|1\rangle + \beta|0\rangle$ w stan

$$|\psi(t)\rangle = e^{-it}\alpha|1\rangle + e^{it}\beta|0\rangle \ , \quad (30)$$

czyli powoduje oscylacje wzglednej fazy pomiedzy stanami $|0\rangle$ i $|1\rangle$.

Wszystkie operacje wykonywane na kwantowych bitach w koputerze kwantowym sa transformacjami unitarnymi. Zauwazmy, ze transfromacje unitarne sa odwracalne, bo po zastosowaniu operacji U mozemy zastosowac rowniez unitarna transformacje $U^\dagger$ i powrocic do stanu poczatkowego.

Oprucz transformacji unitarnych, generowanych jako ewolucja z pewnym hamiltonianem, musimy rowniez od czasu do czasu wykonac pomiar chocby po to, aby sie przekonac jaki jest wynik obliczen. Pomiar w mechanice kwantowej nie jest operacja odwracalna.

III. POMIAR W MECHANICE KWANTOWEJ.

Jeden z postulatow mechaniki kwantowej glosi, ze jesli stanem ukladu jest

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ , \quad (31)$$

to prawdopodobienstwo, ze pomiar w bazie $|0\rangle, |1\rangle$, da wynik 0 lub 1 wynosi odpowiednio

$$P_0 = |\alpha|^2 \ , \quad P_1 = |\beta|^2 \ . \quad (32)$$

Jest to tzw. regula Borna, ze prawdopodobienstwo jest kwadratem amplitudy prawdopodobienstwa. Ten sam stan zapisany w bazie $|+\rangle, |-\rangle$ ma postac

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \ , \quad (33)$$

i prawdopodobienstwa wynikow $+, -$ wynosza

$$P_+ = \left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2 \ , \quad P_- = \left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2 \ . \quad (34)$$

W ogolnosci prawdopodobienstwo, ze pomiar stanu $|\psi\rangle$ da wynik ,,m" w bazie $|m\rangle$ wynosi

$$P_m = |\langle m|\psi\rangle|^2 \quad (35)$$

czyli kwadrat modulu amplitudy prawdopodobienstwa, ze stan $|\psi\rangle$ jest w stanie $|m\rangle$.

W wyniku pomiaru nastepuje ,,kolaps funkcji falowej" do stanu, ktory zostal zmierzony np. wynik pomiaru ,,0" powoduje, ze stan kolapsuje do stanu $|0\rangle$

$$\alpha|0\rangle + \beta|1\rangle \to |0\rangle \ . \quad (36)$$

Tajemniczy ,,kolaps" oznacza tylko tyle, ze jesli zmierzylem, ze stan jest 0 to stan jest 0.

IV. KUBITY, ODDZIALYWANIA KUBITOW.

Uklad fizyczny o dwuwymiarowej przestrzeni Hilberta (np. spin 1/2 elektronu, polaryzacja fotonu, stan zlacza Josephsona) nazywamy kwantowym bitem albo kubitem (ang. qubit). Stan kubitu to

$$\alpha|0\rangle + \beta|1\rangle \ . \quad (37)$$

Na ogol ten stan nie jest ani $|0\rangle$ ani $|1\rangle$, ale jest superpozycja tych stanow. Informacja jest zakodowana w zespolonych amplitudach α i β. Poniewaz, z dokladnoscia do normalizacji $|\alpha|^2 + |\beta|^2$, sa to ciagle parametry, informacja w kubicie jest zapisywana w sposob analogowy. Analogowy zapis informacji powoduje wrazliwosc na zaklucenia (szum otoczenia, niedokladne wykonanie bramek logicznych). Mimo to mozna wykonywac obliczenia kwantowe dzieki algorytmom kwantowej korekcji bledu.

Na jednym kubicie mozemy wykonac prosta jednobitowa bramke NOT realizowana przez transformacje unitarna $U = X$. Zauwazmy, ze ta transfromacja mozemy dzialac na superpozycje stanow $|0\rangle$ i $|1\rangle$

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle \quad (38)$$

Innymi slowy na wejscie komputera kwantowego podajemy jednoczesnie stan $|0\rangle$ i stan $|1\rangle$ i na tych stanach jednoczesnie wykonujemy operacje negacji logicznej. Jedna z zalet komputera kwantowego jest, ze wykonuje swoje operacje rownolegle, ale bez angazowania dodatkowego hardware'u.

Powazne obliczenia beda wymagaly wielu kubitow. Stan rejestru zlozonego z N kubitow jest superpozycja wektorow bazowych postaci

$$|0_1\rangle|0_2\rangle|1_3\rangle|0_4\rangle|1_5\rangle\ldots|0_N\rangle \equiv |00101\ldots0\rangle , \quad (39)$$

gdzie dolny indeks jest numerem kubitu. Takich wektorow bazowych jest 2^N. W ogolnosci stan rejestru N kubitow jest superpozycja

$$\sum_{i_1,i_2,\ldots,i_N=0,1} c_{i_1,i_2,\ldots,i_N}|i_1 i_2 ... i_N\rangle . \quad (40)$$

Informacja jest zawarta w 2^N zespolonych amplitudach prawdopodobienstwa $c_{i_1,i_2,\ldots,i_N}$. Zasada superpozycji oznacza, ze na N-kubitowe wejscie procesora kwantowego mozna jednoczesnie podac 2^N roznych stanow wejsciowych i wszystkie te stany beda przetwarzane rownolegle na tym samym jednym procesorze. Takie same rownolegle obliczenia wymagalyby 2^N klasycznych procesorow.

Nietrywialne obliczenia wymagaja bramek dwubitowych. Przykladem moze byc bramka CNOT (ang. conditional NOT) warunkowej negacji logicznej, ktorej tabelka w bazie dwubitowej ma postac

$$U_{\rm CNOT}|00\rangle = |00\rangle , \quad (41)$$
$$U_{\rm CNOT}|01\rangle = |01\rangle , \quad (42)$$
$$U_{\rm CNOT}|10\rangle = |11\rangle , \quad (43)$$
$$U_{\rm CNOT}|11\rangle = |10\rangle . \quad (44)$$
$$(45)$$

Krotko mowiac, jesli stan pierwszego kubitu jest $|0\rangle$, to nic sie nie dzieje, ale jesli stan pierwszego kubitu jest $|1\rangle$, to drugi kubit ulega negacji. Bramka CNOT wykonuje transformacje unitarna

$$U_{\rm CNOT} = |0_1\rangle\langle 0_1| \ 1_2 + |1_2\rangle\langle 1_2| \ X_2 . \quad (46)$$

Prosze sprawdzic, ze $U_{\rm CNOT}$ jest unitarne.

Podobnie jak bramka NOT takze bramka CNOT moze byc wykonywana na superpozycjach stanow dwubitowych:

$$U_{\rm CNOT} \quad (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle) \ = \ \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle . \quad (47)$$

Innymi slowy, bramka CNOT przetwarza rownolegle $2^2 = 4$ rozne stany wejsciowe.

V. ,,NO-CLONING THEOREM".

Proste twierdzenie (Wooters i Zurek, 1985) dowodzi, ze nie mozna sklonowac

$$|\psi\rangle \to |\psi\rangle|\psi\rangle \quad (48)$$

nieznanego stanu $|\psi\rangle$.

Dowod nie wprost jest bardzo prosty. Zalozmy, ze istnieje transformacja unitarna U_c, ktora klonuje nieznany stan $|\psi\rangle$ tj.

$$U_c|\psi\rangle|\phi\rangle = |\psi\rangle|\psi\rangle , \quad (49)$$

gdzie $|\phi\rangle$ jest poczatkowym stanem ,,papieru kserograficznego". $|\phi\rangle$ nie zalezy od stanu $|\psi\rangle$, bo stan $|\psi\rangle$ z zalozenia nie jest znany. Jesli tak jest, to U_c potrafi w szczegolnosci sklonowac stany 0 i 1:

$$U_c|0\rangle|\phi\rangle = |0\rangle|0\rangle , \quad (50)$$
$$U_c|1\rangle|\phi\rangle = |1\rangle|1\rangle . \quad (51)$$

Jesli tak to unitarne U_c odwzorowuje

$$U_c(\alpha|0\rangle + \beta|1\rangle)|\phi\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq \quad (52)$$
$$\neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \quad (53)$$

czyli dochodzimy do sprzecznosci.

To proste twierdzenie odgrywa wazna role w kryptografii kwantowej.

VI. SPLATANIE KWANTOWE

Stany dwu ukladow kwantowych (dwu kubitow) sa splatane, jesli nie da sie ich sprowadzic do iloczynu

$$|\psi_{AB}\rangle \neq |\psi_A\rangle|\psi_B\rangle , \quad (54)$$

czyli nie da sie powiedziec, ze uklad A ma okreslony stan $|\psi_A\rangle$, a uklad B ma stan $|\psi_B\rangle$. Klasycznym przykladem jest stan EPR (Einsteina-Podolskiego-Rosena) dwu kubitow

$$\frac{1}{\sqrt{2}}(|0_1 0_2\rangle + |1_1 1_2\rangle) \neq |\psi_1\rangle|\psi_2\rangle \quad (55)$$

Prosze sprobowac to rozplatac. :-) Jesli stan pierwszego kubitu jest 0(1) to drugiego tez jest 0(1), w tym sensie stany kubitow sa ,,splatane" lub ,,skorelowane".

Splatanie pojawia sie w wyniku oddzialywania kubitow, na przyklad w wyniku operacji CNOT:

$$\mathrm{CNOT}\frac{(|0_1\rangle + |1_1\rangle)}{\sqrt{2}}|0_2\rangle = \frac{(|0_1 0_2\rangle + |1_1 1_2\rangle)}{\sqrt{2}} . \quad (56)$$

CNOT zadzialal na stan separowalny (niesplatany) i wygenerowal stan splatany EPR.

Splatanie jest wlasnoscia czysto kwantowa, ktore nie wystepuje w swiecie klasycznym, w odroznienu od zasady superpozycji (liniowosci). Ma zasadnicze znaczenie dla kwantowej teleportacji, kryptografii, oraz mocy obliczeniowej komputerow kwantowych.

VII. ZREDUKOWANA MACIERZ GESTOSCI.

W tej czesci rozwiniemy proste narzedzia matematyczne pozwalajace opisywac splatanie kwantowe. Zalozmy, ze uklad fizyczny mozna podzielic na dwa podukłady: A i B. Niech $H_{\rm A}$ i $H_{\rm B}$ beda przestrzeniami Hilberta dla podukladow. W podprzestrzeni A wybieramy baze ortonormalna $|i_A\rangle$ z indeksem $i = 1, 2, ...$, podobnie w podprzestrzeni B wybieramy baze $|j_B\rangle$ z $j = 1, 2, ...$ Pelny uklad ma przestrzen stanow $H_A \otimes H_B$ napinana przez baze wektorow $|i_A\rangle|j_B\rangle$. Dowolny stan ukladu moze byc zapisany jako kombinacja liniowa wektorow bazy

$$|\Psi\rangle_{AB} = \sum_{i,j} c_{ij}|i_A\rangle|j_B\rangle \ , \tag{57}$$

gdzie $\sum_{ij} |c_{ij}|^2 = 1$ dla normalizacji stanu.

Jesli stan ukladu AB jest iloczynem stanow dla podukladow (stan nie jest splatany), to mozna go rozlozyc jako

$$\begin{aligned} |\Psi_{AB}\rangle \ &= \ |\psi_A\rangle|\psi_B\rangle = \\ &\left(\sum_i c_i^A|i_A\rangle\right)\left(\sum_j c_j^B|j_B\rangle\right) = \\ &\sum_{ij}\left(c_i^A c_j^B\right)|i_A\rangle|j_B\rangle \ , \end{aligned} \tag{58}$$

czyli $c_{ij} = c_i^A c_j^B$. Zatem jesli stan nie jest splatany, to istnieja takie wspolczynniki c_i^A oraz c_j^B, ze $c_{ij} = c_i^A c_j^B$. W praktyce trudno sprawdzic czy takie wspolczynniki istnieja, dlatego stosuje sie inne podejscie, oparte na zredukowanej macierzy gestosci.

Rozwazmy operator O_A, ktory dziala wylacznie w podprzestrzeni A. Wartosc oczekiwana tego operatora w stanie $|\Psi_{AB}\rangle$ wynosi

$$\begin{aligned} \langle O_A\rangle \ &= \ \langle\Psi_{AB}|O_A|\Psi_{AB}\rangle = \\ &\sum_{ij}\langle\Psi_{AB}|O_A|i_A\rangle|j_B\rangle\langle i_A|\langle j_B|\Psi_{AB}\rangle = \\ &\sum_{ij}\langle i_A|\langle j_B|\Psi_{AB}\rangle\langle\Psi_{AB}|O_A|j_B\rangle|i_A\rangle = \\ &Tr_A Tr_B\left(|\Psi\rangle_{AB\ AB}\langle\Psi|O_A\right) = \\ &Tr_A\left[(Tr_B|\Psi\rangle_{AB\ AB}\langle\Psi|)\,O_A\right] = Tr_A\left[\rho_A O_A\right] \ . \end{aligned} \tag{59}$$

W tym rachunku uzylem pojecia sladu operatora po podprzestrzeni B

$$Tr_B O = \sum_j \langle j_B|O|j_B\rangle \ = \sum_j O_{jj}, \tag{60}$$

czyli sumy diagonalnych elementow macierzowych operatora w bazie podprzestrzeni B. Zdefiniowalem takze zredukowana macierz gestosci dla podukladu A

$$\rho_A \ = \ Tr_B\ |\Psi_{AB}\rangle\langle\Psi_{AB}| \ , \tag{61}$$

ktora jest operatorem w podprzestrzeni A. Rachunek pokazal, ze wartosc oczekiwana operatora O_A dzialajacego w podprzestrzeni A jest rowna sladowi tego operatora ze zredukowana macierza gestosci

$$\langle O_A\rangle \ = \ Tr_A\ O_A\ \rho_A \ . \tag{62}$$

Wprowadzenie pojecia zredukowanej macierzy gestosci zostalo uzasadnione. Przyjrzyjmy sie teraz jej wlasnosciom.

ρ_A jest unormowane tzn.

$$Tr_A\ \rho_A \ = \ 1 \ . \tag{63}$$

Istotnie, podstawmy $O_A = 1_A$ w rownaniu (59), a otrzymamy $Tr_A\rho_A = \langle\Psi_{AB}|\Psi_{AB}\rangle$, czyli jesli stan $|\Psi_{AB}$ jest unormowany, to slad jego zredukowanej macierzy gestosci jest rowny 1.

ρ_A jest operatorem hermitowskim

$$\rho_A^\dagger \ = \ \rho_A \ , \tag{64}$$

bo $(Tr_B\ |\Psi_{AB}\rangle\langle\Psi_{AB}|)^\dagger = Tr_B\ |\Psi_{AB}\rangle\langle\Psi_{AB}|$.

Jesli $|\Psi_{AB}\rangle = |\psi_A\rangle|\psi_B\rangle$ nie jest splatany, to $\rho_A^2 = \rho_A$. Istotnie

$$\begin{aligned} \rho_A \ &= \ Tr_B\ |\Psi_{AB}\rangle\langle\Psi_{AB}| \ = \ |\psi_A\rangle\langle\psi_A|Tr_B\ |\psi_B\rangle\langle\psi_B| \ = \\ &|\psi_A\rangle\langle\psi_A| \ , \end{aligned} \tag{65}$$

a stad wynika

$$\begin{aligned} \rho_A^2 \ &= \ |\psi_A\rangle\langle\psi_A|\ |\psi_A\rangle\langle\psi_A| \ = \\ &= \ |\psi_A\rangle\langle\psi_A| \ = \ \rho_A \ . \end{aligned} \tag{66}$$

Prawdziwe jest takze stwierdzenie odwrotne: jesli $\rho_A^2 = \rho_A$, to stan $|\Psi_{AB}\rangle$ nie jest splatany. Krotko mowiac

$$\rho_A^2 \ = \ \rho_A \ \Leftrightarrow \ |\Psi_{AB}\rangle \text{ nie jest splatany} \ . \tag{67}$$

To twierdzenie stanowi kryterium czy stan jest splatany czy nie.

Dla dowodu zauwazmy, ze macierz hermitowska ρ_A mozna zdiagonalizowac. Jesli ρ_A ma wiecej niz jedna niezerowa wartosc wlasna, to $\rho_A^2 \neq \rho_A$ i stan musi byc splatany. Zalozmy zatem, ze istnieje tylko jedna niezerowa (i rowna 1) wartosc wlasna ρ_A, a zatem zachodzi $\rho_A^2 = \rho_A$.

Niech $|i_A\rangle$ bedzie baza stanow wlasnych ρ_A, przy czym przyjmujemy, ze $|1_A\rangle$ odpowiada niezerowej wartosci wlasnej, czyli $\rho_A = |1_A\rangle\langle 1_A|$. Zawsze mozemy stan AB zapisac jako

$$|\Psi_{AB}\rangle \ = \ \sum_{ij} c_{ij}\ |i_A\rangle|j_B\rangle \ . \tag{68}$$

Obliczmy wartosc oczekiwana operatorow rzutowych $|i_A\rangle\langle i_A|$ dla $i \neq 1$. Z jednej strony ta wartosc oczekiwana wynosi

$$Tr_A\rho_A|i_A\rangle\langle i_A| = Tr_A|1_A\rangle\langle 1_A|\ |i_A\rangle\langle i_A| \ = \ 0 \tag{69}$$

bo $i \neq 1$. Z drugiej strony ta sama wartosc oczekiwana

$$\langle \Psi_{AB}|1_A\rangle\langle 1_A|\Psi_{AB}\rangle = \sum_{ij} |c_{ij}|^2. \qquad (70)$$

Z porownania wzorow wynika, ze $\sum_j |c_{ij}|^2 = 0$ dla $i \neq 1$, czyli $c_{ij} = 0$ dla $i \neq 1$. A zatem

$$|\Psi_{AB}\rangle \;=\; \sum_j c_{1j}\ |1_A\rangle|j_B\rangle \;= |1_A\rangle \left(\sum_j c_{1j}\ |j_B\rangle \right) \;, \qquad (71)$$

czyli stan jest iloczynem stanow dla podukladow, czyli nie jest splatany, co konczy dowod.

VIII. ROZKLAD SCHMIDTA

Z powyzszego dowodu wynika jeszcze jeden pozyteczny wniosek. Przepiszmy rozklad stanu (68) w formie

$$|\Psi_{AB}\rangle \;=\; \sum_{ij} c_{ij}\ |i_A\rangle|j_B\rangle \;= \sum_i |i_A\rangle \sum_j c_{ij}\ |j_B\rangle \;\equiv\; \sum_i |i_A\rangle\ |\phi_i^B\rangle \qquad (72)$$

Skoro ρ_A jest z zalozenia diagonalne w stanach $|i_A\rangle$, to stany $|\phi_i^B\rangle$ musza byc ortogonalne. Istotnie

$$\rho_A \;=\; Tr_B\ |\Psi_{AB}\rangle\langle\Psi_{AB}| \;= Tr_B \sum_{ij} |i_A\rangle\ |\phi_i^B\rangle\langle\phi_j^B|\langle j_A| \;= \sum_{ij} |i_A\rangle\langle j_A| \sum_k \langle k_B|\phi_i^B\rangle\langle\phi_j^B|k_B\rangle \;, \qquad (73)$$

ale skoro ρ_A ma byc diagonalne w bazie $|i_A\rangle$, to dla $i \neq j$ musimy miec

$$0 \;=\; \sum_k \langle k_B|\phi_i^B\rangle\langle\phi_j^B|k_B\rangle \;= \sum_k \langle\phi_j^B|k_B\rangle\langle k_B|\phi_i^B\rangle \;= \langle\phi_j^B|\phi_i^B\rangle \;, \qquad (74)$$

co nalezalo dowiesc.

Pokazalismy, ze stany $|\phi_j^B\rangle$ sa baza ortogonalna. Normujac wektory $|\phi_j^B\rangle = \lambda_j|\tilde{j}_B$ otrzymujemy baze ortonormalna $|\tilde{j}_B\rangle$ i mozemy zapisac stan AB przy pomocy rozkladu Schmidta

$$|\Psi_{AB}\rangle \;=\; \sum_i \lambda_i\ |i_A\rangle|\tilde{j}_B\rangle \;. \qquad (75)$$

Bazy $|i_A\rangle$ oraz $|\tilde{j}_B\rangle$ sa ortonormalne, a wspolczynniki rozkladu λ_i mozna wybrac rzeczywiste i dodatnie. Jesli tylko jedno $\lambda_i \neq 0$ to stan nie jest splatany, w przeciwnym razie stan jest splatany.

IX. NIELOKALNOSC MECHANIKI KWANTOWEJ / ZMIENNE UKRYTE (?)

Niektorzy ludzie nie lubia przypadkowosci w wynikach pomiarow w mechanice kwantowej, powiadaja, ze ,,Pan Bog nie gra w kosci". Powiadaja, ze mechanika kwantowa nie opisuje calej rzeczywistosci. Ta nieopisywana przez MK czesc rzeczywistosci to tajemnicze ,,zmienne ukryte", ktorych wartosci determinuja wyniki pojedynczych pomiarow. Gdybysmy znali wartosci zmiennych ukrytych, to moglibysmy przewidziec wyniki pomiarow, ale poniewaz ich nie znamy, to wydaje nam sie, ze wyniki pomiarow sa przypadkowe. Zmienne ukryte sa postulowane na mocy filozoficznego zalozenia, ze fizyka musi byc deterministyczna, bo musi byc w stanie przewidywac (takze wyniki pomiarow).

Inne przekonanie lezace u podstaw fizyki, to lokalnosc, czyli brak oddzialywan na odleglosc. Gdyby wszystko ze wszystkim oddzialywalo na dowolnie duzych odleglosciach, to nie moglibysmy niczego przewidziec, bo niczego nie daloby sie wyizolowac myslowo z otoczenia. To nie jest tylko problem fizykow, mamuta tez by sie nie dalo upolowac. :-)

Einstein nie lubil mechaniki kwantowej i dlatego wraz z Podolskym i Rosenem wymyslil paradoks, ktory mial pokazac, ze mechanika kwantowa nie jest lokalna lub nie jest deterministyczna, a tym samym nie moze byc ostateczna teoria fizyczna. Zmienne ukryte i lokalnosc zostaly ,,splatane" w tzw. paradoksie Einsteina-Podolsky'ego-Rosena (EPR). Panowie EPR zaproponowali stan splatany

$$|EPR\rangle \;=\; \frac{1}{\sqrt{2}}\left(|0_1 0_2\rangle + |1_1 1_2\rangle\right) \;\neq\; |\psi_1\rangle|\psi_2\rangle \;. \qquad (76)$$

Zuwazmy, ze 0 i 1 jako wyniki pomiarow na kubicie 1 sa jednakowo pradopodobne. Podobnie 0 i 1 jako wyniki pomiarow na kubicie 2 sa jednakowo prawdopodobne. Jesli jednak wykonamy pomiar na kubicie 1 z wynikiem 0, to jednoczesne wykonanie pomiaru na kubicie 2 musi takze dac 0, bo tak wynika z korelacji w stanie EPR. Podobnie wynik 1 na jednym kubicie wymaga by wynika pomiaru na drugim kubicie dal 1.

Jednak jesli kubity sa bardzo oddalone w przestrzeni, to wedlug szczegolnej teorii wzglednosci (STW) rownoczesnosc jest wzgledna i wzgledna jest kolejnosc pomiarow na kubitach 1 i 2. A zatem nie moze byc tak, ze wynik pierwszego pomiaru wplywa na wynik drugiego pomiaru, bo kolejnosc pomiarow jest wzgledna. No i jest paradoks, bo jesli wyniki mimo to okazuja sie nielokalnie skorelowane, to moze oznaczac albo problemy z STW albo z lokalnoscia mechaniki kwantowej.

Panowie EPR, chcac ratowac lokalnosc i zarazem wprowadzic determinizm, zaproponowali, ze to lokalne zmienne ukryte determinuja wyniki pomiarow na kubitach 1 i 2, ale w taki sposob, zeby mozliwie dobrze zachowac korelacje pomiedzy wynikami pomiarow wynikajace ze splatania w stanie EPR.

W przypadku korelacji 2 fotonow hipoteza lokalnych zmiennych ukrytych prowadzi do slynnych nierownosci Bella. Nierownosci Bella opisuja odstepstwa od kwantowych korelacji wynikajace z lokalnego charakteru zmiennych ukrytych. Eksperyment Aspecta (20km swiatlowodu pod Jeziorem Genewskim) pokazal lamanie nierownosci Bella i tym samym sfalsyfikowal teorie lokalnych zmiennych ukrytych.

Hipoteze lokalnych zmiennych ukrytych najlatwiej zilustrowac na przykladzie splatanego stanu 3 kubitow

$$|GHZ\rangle \;=\; \frac{1}{\sqrt{2}}\left(|1_A\rangle|1_B\rangle|1_C\rangle - |0_A\rangle|0_B\rangle|0_C\rangle\right) \;. \quad (77)$$

Zauwazmy, ze stan GHZ jest stanem wlasnym o wartosci wlasnej 1 dla operatorow $X_AY_BY_C$, $Y_AX_BY_C$ oraz $Y_AY_BX_C$. Jednoczesnie jest stanem wlasnym o wartosci wlasnej -1 dla operatora $X_AX_BX_C$. Zatem jesli zmierzymy X_A, X_B, X_C, to mozemy dostac wyniki $x_A = 1, x_B = 1, x_c = -1$ lub $1, -1, 1$ lub $-1, 1, 1$ lub $-1, -1, -1$. Podobnie jesli zmierzymy dwa Y i jeden X to mozemy dostac wyniki: $1, 1, 1$ lub $1, -1, -1$ lub $-1, 1, -1$ lub $-1, -1, 1$, czyli zawsze iloczyn wynikow $yyx = +1$. Takie sa korelacje wynikajace ze splatania w stanie GHZ.

Poniewaz lokalne zmienne ukryte ,,nie wiedza" zawczasu co zostanie zmierzone na poszczegolnych kubitach (X czy Y), to musza byc przygotowane na kazda ewentualnosc. Przykladowy **lokalny** plan to

$$\begin{aligned} x_A = -1 \;,\;\; y_A = 1 \;, \\ x_B = 1 \;,\;\; y_B = -1 \;, \\ x_C = -1 \;,\;\; y_C = 1 \;. \end{aligned} \quad (78)$$

Jesli zostana zmierzone dwa Y i jeden X, to ten plan da wyniki o korelacjach wynikajacych ze splatania z stanie GHZ tj. $yyx = +1$. Jesli jednak we wszystkich trzech laboratoriach zostana zmierzone X, to zgodnie z planem $x_Ax_Bx_C = +1$, a ze splatania w stanie GHZ wynika $x_Ax_Bx_C = -1$.

Okazuje sie, ze nie tylko ten przyklad, ale zaden lokalny plan nie jest dobry. Dowod jest bardzo prosty. Splatanie w stanie GHZ naklada na wyniki pomiarow wiezy

$$\begin{aligned} y_Ay_Bx_C &= 1, \\ y_Ax_By_C &= 1, \\ x_Ay_By_C &= 1, \\ x_Ax_Bx_C &= -1 \end{aligned} \quad (79)$$

Te trzy wiezy sa w sprzecznosci. Aby sie o tym przekonac mnozymy stronami przez siebie pierwsze trzy linijki i dostajemy

$$y_A^2y_B^2y_C^2x_Ax_Bx_C = x_Ax_Bx_C = 1, \quad (80)$$

ale z drugiej strony powinno byc $x_Ax_Bx_C = -1$ co daje sprzecznosc.

Zatem jesli eksperyment zawsze daje wyniki skorelowane jak w rownaniu (79), to tym samym wyklucza lokalne zmienne ukryte.

A zatem nie sa mozliwe lokalne zmienne ukryte. Jesli nadal zakladac, ze mechanika kwantowa jest niekompletna i wymaga wprowadzenia zmiennych ukrytych, aby nadac jej deterministyczny charakter, to trzeba sie pogodzic z tym, ze zmienne ukryte musza byc nielokalne. Niezaleznie od tego czy zmienne ukryte sa, czy ich nie ma, nie mozemy uciec od nielokalnosci: albo przyjmiemy, ze sama mechanika kwantowa jest nielokalna, albo ze mechanika kwantowa uzupelniona z zmienne ukryte jest nielokalna.

Nielokalne korelacje nie sa natomiast sprzeczne ze STW, bo nie moga sluzyc do przekazywania informacji z predkoscia wieksza od predkosci swiatla.

X. GESTE KODOWANIE KWANTOWE

Stan kubitu jest superpozycja

$$|\psi\rangle \;=\; |0\rangle\cos\theta + |1\rangle\sin\theta e^{i\phi} \;. \quad (81)$$

Stan jest okreslony przez dwie fazy $\theta, \phi \in [0, 2\pi)$. Jesli przyjac, ze wartosci faz stanowia ,,informacje kwantowa", to wiekszosc tej kwantowej informacji jest niedostepna, bo pomiar w bazie $|0\rangle, |1\rangle$ da wynik 0 lub 1, podobnie jak dla klasycznego bitu. Innymi slowy dostepny jest jeden bit klasycznej informacji.

Podobnie stan N kubitow

$$\sum_{i_1,...,i_N=0,1} c_{i_1,...,i_N}\; |i_1, ..., i_N\rangle \quad (82)$$

zawiera informacje kwantowa w postaci 2^N liczb zespolonych, ale pomiar stanu daje jeden z mozliwych wynikow klasycznych np. $|0, 0, 1, 1, ..., 1$. Znowu wiekszosc kwantowej informacji nie jest dostepna.

Okazuje sie jednak, ze jesli kubit jest splatany z innym kubitem, to moze zostac uzyty to przekazania 2 bitow kwantowej informacji.

Niech A(licja) i B(artek) beda oddaleni w przestrzeni, ale niech wspolposiadaja pare splatanych kubitow np. w stanie EPR

$$|\psi^-\rangle \;=\; \frac{1}{\sqrt{2}}\left(|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle\right) \quad (83)$$

Kubity A i B sa oddalone w przestrzeni. Jak wiemy z dyskusji paradoksu EPR, samo splatanie nie wystarcza do przekazywania informacji pomiedzy A i B.

Uzupelnijmy stan $|\psi^-\rangle$ do tzw. bazy Bella

$$\begin{aligned} |\psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle\right) \;, \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|0_A\rangle|1_B\rangle + |1_A\rangle|0_B\rangle\right) \;, \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_B\rangle - |1_A\rangle|1_B\rangle\right) \;, \\ |\phi^+\rangle &= \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle\right) \;. \end{aligned} \quad (84)$$

Jest to baza ortonormalna i kazdy z tych stanow jest ,,maksymalnie splatany" tzn. ma dwa jednakowe wspolczynniki w rozkladzie Schmidta rowne $1/\sqrt{2}$.

Posiadajac wspolnie z B stan $|\psi^-\rangle$ Alicja moze przygotowac kazdy ze stanow bazy Bella wykonujac odpowiednie operacje unitarne wylacznie na swoim kubicie A. Operacje mozna ponumerowac jako U_{ij}:

$$\begin{aligned} U_{00} &= |0\rangle\langle 0| + |1\rangle\langle 1| = 1 , \\ U_{01} &= |0\rangle\langle 0| - |1\rangle\langle 1| = -Z , \\ U_{10} &= -|0\rangle\langle 1| - |1\rangle\langle 0| = -X , \\ U_{11} &= |1\rangle\langle 0| - |0\rangle\langle 1| . \end{aligned} \tag{85}$$

Zastosowanie tych operacji do kubitu A daje stany bazy Bella: $U_{00}|\psi^-\rangle = |\psi^-\rangle$, $U_{01}|\psi^-\rangle = |\psi^+\rangle$, $U_{10}|\psi^-\rangle = |\phi^-\rangle$, $U_{11}|\psi^-\rangle = |\phi^+\rangle$. Jesli zatem Alicja chce przekazac Bolkowi dwa klasyczne bity informacji i, j, to stosuje do kubitu A operacje U_{ij}, a nastepnie wysyla kubit A do Bolka. Bolek po otrzymaniu kubitu A ma obydwa splatane kubity A i B i wykonuje na nich pomiar w bazie Bella. Wynik tego pomiaru okresla wartosc bitow i, j: wynik $|\psi^-\rangle$ oznacza 00, $|\psi^+\rangle$ oznacza 01 itd..

Podsumowujac: Alicja wyslala do Bolka jeden kubit, ale przekazala dwa bity klasycznej informacji. Jest to mozliwe dzieki temu, ze wczesniej posiadali splatana pare kubitow.

XI. KWANTOWA TELEPORTACJA.

Powiedzmy, ze Alicja posiada nieznany stan $|\psi\rangle$ i chce go przekazac Bolkowi. Nie ma sensu go zmierzyc, bo wtedy skolapsuje stan do jednego ze stanow w bazie pomiarowej i nieodwracalnie zniszczy wiekszosc kwantowej informacji. Gdyby znala $|\psi\rangle$, to moglaby wyslac Bolkowi jego klasyczny opis podajac kolejne amplitudy prawdopodobienstwa, ale rozsadnie dokladne odtworzenie $|\psi\rangle$ przez Bolka w jego laboratorium wymagaloby transferu duzej ilosci klasycznej informacji tj. kolejnych pozycji dziesietnych amplitud prawdopodobienstwa. Gdyby Poczta Polska oferowala odpowiednie uslugi, to Alicja moglaby wyslac $|\psi\rangle$ kwantowym priorytetem z gwarantowanym czasem dekoherencji dluzszym niz czas doreczenia. Jesli jednak Alicja i Bolek zawczasu podzielili sie splatanymi parami kubitow (korzystajac z uprzejmosci genewskiego oddzialu Swiss Telecom), to moga teleportowac nieznany stan $|\psi\rangle$ w wygodny i bezpieczny sposob zwany kwantowa teleportacja.

Zalozmy, ze Alicja i Bob dziela stan splatany $|\psi^-\rangle$ pomiedzy kubitami A i B. Ponadto Alicja posiada dodatkowy kubit C w nieznanym stanie $|\psi\rangle$. Ten stan zawsze mozemy zapisac jako

$$|\psi_C\rangle = a|0_C\rangle + b|1_C\rangle , \tag{86}$$

gdzie amplitudy a i b sa nieznanymi liczbami zespolonymi. Laczny stan trzech kubitow to

$$|\Psi_{ABC}\rangle = |\psi_C\rangle|\psi^-_{AB}\rangle = \frac{1}{\sqrt{2}}\left(a|0_C\rangle + b|1_C\rangle\right)\left(|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle\right) \tag{87}$$

Ten stan mozna przepisac w bazie stanow Bella dla kubitow C i A:

$$\begin{aligned} 2\,|\Psi_{ABC}\rangle &= |\psi^-_{CA}\rangle\left(-a|0_B\rangle - b|1_B\rangle\right) \\ &+ |\psi^+_{CA}\rangle\left(-a|0_B\rangle + b|1_B\rangle\right) \\ &+ |\phi^-_{CA}\rangle\left(b|0_B\rangle + a|1_B\rangle\right) \\ &+ |\phi^+_{CA}\rangle\left(-b|0_B\rangle + a|1_B\rangle\right) . \end{aligned} \tag{88}$$

Zauwazmy, ze w ten sposob oddzielilismy stan kubitow C i A w posiadaniu Alicji od kubitu B w posiadaniu Bolka.

Na razie nie zostaly wykonane zadne operacje. Alicja wykonuje pierwsza operacje mierzac stan kubitow C i A w bazie Bella. Wszystkie wyniki sa jednakowo prawdopodobne z prawdopodobienstwem $\frac{1}{4}$ niezaleznie od stanu $|\psi\rangle$ (niezaleznie od jego amplitud a i b). Zatem ten pomiar nie daje Alicji zielonego pojecia o stanie $|\psi\rangle$, natomiast kubitu B w posiadaniu Bolka kolapsuje do odpowiednio

$$\begin{aligned} \left(-a|0_B\rangle - b|1_B\rangle\right) &= -U_{00}|\psi_B\rangle \\ \left(-a|0_B\rangle + b|1_B\rangle\right) &= -U_{01}|\psi_B\rangle \\ \left(b|0_B\rangle + a|1_B\rangle\right) &= -U_{10}|\psi_B\rangle \\ \left(-b|0_B\rangle + a|1_B\rangle\right) &= U_{11}|\psi_B\rangle , \end{aligned} \tag{89}$$

gdzie operacje unitarne U_{ij} zostaly zdefiniowane w rownaniu (85). Liczba binarna ij numeruje wyniki pomiarow kubitow CA w bazie Bella: $\psi^-, \psi^+, \phi^-, \phi^+$.

Krotko mowiac, stan kubitu B to

$$(-1)^{ij+1}U_{ij}\ |\psi_B\rangle . \tag{90}$$

A zatem Bolek jest juz w posiadaniu nieznanego stanu $|\psi\rangle$ z dokladnoscia do nieznanej mu transformacji unitarnej $(-1)^{ij+1}U_{ij}$. Krotki (klasyczny) SMS od Alicji przekazuje mu wartosci ij, co pozwala mu na odwrocenie transformacji $(-1)^{ij+1}U_{ij}$ i sprowadzenie kubitu B do nieznanego teleportowanego stanu $|\psi\rangle$.

Zauwazmy, ze Alicja i Bolek zuzyli splatana pare EPR w stanie $|\psi^-\rangle$ i wyslali jednego SMS-a (klasyczny kanal komunikacji). Alicja wysylajac jedynie 2 bity klasycznej informacji przekazala Bolkowi cala nieznana kwantowa informacje o stanie $|\psi\rangle$.

Zauwazmy, ze Alicja niczego przy okazji sie nie dowiedziala o ψ, dzieki czemu stan ψ nie zostal zaburzony. Zauwazmy rowniez, ze zgodnie z twierdzeniem o niemoznosci klonowania Bolek jest teraz w posiadaniu jedynej kopii nieznanego stanu ψ.

Splatane pary kubitow sa niezbednym zasobem dla kwantowej teleportacji. Musza byc przygotowane zawczasu. Na przyklad Alicja przygotowuje splatane pary kubitow a nastepnie wysyla po jednym kubicie z kazdej pary do Bolka. Przesylany kubit jest narazony na szum

otoczenia co spowoduje zniekształcenie splatanych par w porownaniu ze stanem ψ^-. Okazuje sie jednak, ze wykonujac jedynie lokane operacje w swoich laboratoriach i wysylajac SMS-y Alicja i Bob moga z posiadanych splatanych par ,,wydestylowac" mniejsza liczbe par w stanie $|\psi^-\rangle$.

XII. KRYPTOGRAFIA KWANTOWA.

Podstawowym elementem kryptografii klasycznej jest klucz krytograficzny. Klucz jest klasycznym ciagiem zer i jedynek np. $K = 011010$ sluzacym do kodowania sygnalow. Jezeli na przyklad ma byc wyslany sygnal $S = 100011$, to najpierw K i S zostaja zsumowane binarnie (tzn. kazdy bit jest sumowany niezaleznie modulo 2) dajac zakodowany sygnal $ZS = K \oplus S = 111001$. Nastepnie zakodowany sygnal ZS zostaje wyslany do odbiorcy, ktory jest rowniez w posiadaniu klucza K. Odbiorca odkodowuje sygnal dodajac do niego binarnie klucz K tj. $K \oplus ZS = S$. Osoba postronna nie znajaca klucza K nie moze odkodowac sygnalu ZS.

Klucz nie powinien byc uzywany wielokrotnie. Wezmy dwa sygnaly S_1 i S_2 i zakodujmy je tym samym kluczem: $ZS_1 = K \oplus S_1$ oraz $ZS_2 = K \oplus S_2$. Podsluchiwacz moze dodac binarnie podsluchane sygnaly

$$ZS_1 \oplus ZS_2 \;=\; K \oplus S_1 \oplus K \oplus S_2 \;=\; S_1 \oplus S_2 \qquad (91)$$

uzyskujac czesciowa informacje na temat wiadomosci S_1 i S_2, a mianowicie ich sume binarna. A zatem klucz nie powinien byc uzywany wielokrotnie. W szczegolnosci klucz K musi byc nie krotszy od sygnalu S, ktory ma byc zakodowany.

Kryptografia klasyczna jest calkowicie bezpieczna pod warunkiem, ze strony dysponuja dostatecznie dlugim wspolnym kluczem K, ktorego nie zna nikt poza nimi. A zatem kryptografia jest calkowicie bezpieczna pod warunkiem, ze istnieje bezpieczna metoda dystrybucji klucza pomiedzy strony. Metoda dystrybucji jest bezpieczna pod warunkiem, ze jest odporna na proby podsluchania klucza: klucz ma dotrzec do swojego adresata i tylko do niego.

Jedynym kwantowym elementem w kwantowej kryptografii jest kwantowa dystrybucja klucza. Bezpieczenstwo kwantowej dystrybucji klucza jest oparte na fundamentalnych prawach przyrody. Przewaga kwantowej dystrybucji klucza nad klasyczna wynika z faktu, ze pomiar zaburza stan kwantowy. Na przyklad pomiar stanu $\alpha|0\rangle + \beta|1\rangle$ w bazie $|0\rangle, |1\rangle$ kolapsuje stan do $|0\rangle$ lub $|1\rangle$. Oznacza to, ze kwantowo na ogol nie mozna ,,podsluchiwac" nie zaburzajac podsluchiwanej informacji. Z drugiej strony ,,no cloning theorem" nie pozwala sklonowac nieznanej informacji kwantowej, aby mozna bylo niepostrzezenie po(d)sluchac jej kopii.

Ponizej podaje przyklad algorytmu, ktory zostal zrealizowany doswiadczalnie [Los Alamos, Genewa].

A. Algorytm Bennetta i Brassarda.

A(licja) chce podzielic sie kluczem z B(olkiem), ale tak zeby E(wa) [eavesdropper] nie mogla tego podsluchac. A i B nie podziela sie z gory zalozonym kluczem, ale wygeneruja ciag przypadkowych zer i jedynek, aby nastepnie w wyniku dyskusji zadecydowac, ktore elementy tego ciagu wlaczyc do powstajacego klucza. Zakladamy, ze A i B dysponuja klasycznym i kwantowym kanalem informacji tzn. moga zarowno wysylac SMS-y jak i spolaryzowane fotony/spiny.

Kolejne kroki algorytmu sa nastepujace

- A i B ustalaja dopuszczalna czestosc bledow e_{max};
- A wysyla do B przypadkowy ciag fotonow/spinow w stanach $|0\rangle, |1\rangle, |+\rangle, |-\rangle$;
- dla kazdego fotonu/spinu w ciagu B wybiera przypadkowa baze pomiarowa 0/1 lub $+/-$;
- B mierzy kazdy spin i zapisuje wynik pomiaru (oraz baze);
- B oglasza swoje bazy pomiarowe tak, aby slyszala go A (nie oglasza wynikow pomiarow), ale dopiero po wykonaniu pomiarow;
- A dzwoni do B i mowi, ktore pomiary zostaly wykonane w poprawnych bazach;
- B wyrzuca wyniki uzyskane w zlych bazach;
- B przyjmuje ciag wynikow uzyskanych w dobrych bazach jako swoj surowy klucz K_B;
- A przyjmuje swoje wyniki w dobrych bazach jako swoj surowy klucz K_A [Gdyby nie bylo szumu ani zaklocen wynikajacych z podgladania, to $K_A = K_B$ i dystrubucja klucza bylaby juz zakonczona];
- A i B porownuja niektore wyniki uzyskane w bazie 1/0 oraz bazie $+/-$ i porownuja ich czestosci bledow z zalozona dopuszczalna czestoscia bledow e_{max}. Jesli $e_{1/0} < e_{max}$ i $e_{+/-} < e_{max}$, to traktuja pozostale wyniki jako surowe klucze K_A i K_B;
- A i B wybieraja podbloki kluczy K_A i K_B o takiej dlugosci, aby prawdopodobienstwo wystapienia bledu bylo male, a nastepnie porownuja przystosci podblokow starajac sie zlokalizowac blad. Jesli parzystosci okazuja sie zgodne, to akceptuja podbloki jako poprawne, ale odrzucaja ich ostatnie bity tak, aby Ewa nie dowiedziala sie niczego o parzystosci zaakceptowanych podblokow;
- aby wyeliminowac parzyste liczby bledow w podbloku wykonuja permutacje bitow, a nastepnie znowu dziela na podbloki i sprawdzaja parzystosc....;

- poniewaz Ewa moze miec czesciowa informacje o kluczu (bo czasami zmierzyla w dobrej bazie), to A i B stosuja do klucza K funkcje siekajaca zdefiniowana przez czesc klucza K (trzeba poswiecic czesc klucza). Funkcja siekajaca jest tylko czesciowo znana Ewie.

Wielokrotne powtarzanie ostatnich 3 punktow powoduje, ze wiedza Ewy na temat destylowanego klucza maleje eksponencjalnie.

Opisana powyzej strategia moze nie wystarczyc, jesli Ewa ze swej strony przyjmie bardziej skomplikowana strategie podsluchiwania i bedzie np. wykonywac nieloklane operacje unitarne na N kubitach. Wtedy pelne bezpieczenstwo moze zapewnic dopiero zastosowanie komputerow kwantowych.

XIII. KOMPUTERY KWANTOWE - PODSTAWY

Bit kwantowy moze byc w dwoch stanach bazowych $|0\rangle$ i $|1\rangle$ lub w ich dowolnej superpozycji kwantowej $\alpha|0\rangle + \beta|1\rangle$, okreslonej przez 2 liczby zespolone α i β. Rejestr kwantowy zlozony z N kubitow moze byc w jednym z 2^N stanow bazowych $|i_1 i_2 ... i_N\rangle$ lub w ich superpozycji $\sum_{i_1,i_2,...,i_N=0}^{1} c_{i_1 i_2 ... i_N} |i_1 i_2 ... i_N\rangle$ okreslonej przez 2^N liczb zespolonych $c_{i_1 i_2 ... i_N}$.

A. Bramki

Na kubitach mozna wykonywac znana juz brake NOT, $U_{NOT} = X$, a na parach kubitow bramke CNOT, $U_{CNOT} = |0_A\rangle\langle 0_A|1_B + |1_A\rangle\langle 1_A|X_B$. Ponadto w mechanice kwantowej mozna rozszerzyc pojecie bramki na operacje, ktore nie maja klasycznego odpowiednika. Bardzo uzyteczna bramka jest transformacja Hadamarda U_A o dzialaniu

$$\begin{aligned} U_A|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle , \\ U_A|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle . \end{aligned} \tag{92}$$

To jest transformacja unitarna, bo odwzorowuje jedna baze ortonormalna w druga baze ortonormalna. Ta operacja odwzorowuje stany 0/1 w superpozycje stanow 0/1 i jako taka nie ma odpowiednika klasycznego. Aby sie przekonac o uzytecznosci takiej bramki przygotujmy poczatkowo rejestr N kubitow w stanie

$$|00...0\rangle , \tag{93}$$

co zazwyczaj nie jest trudne. Nastepnie podzialajmy na kazdy z N kubitow transformacja Hadamarda U_A otrzymujac stan

$$\begin{aligned} |\psi\rangle &= U_A \otimes U_A \otimes ... U_A \, |00...0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes ... \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2^{N/2}} \sum_{x=0}^{2^N - 1} |x\rangle , \end{aligned} \tag{94}$$

gdzie x to liczba w N-bitowym zapisie binarnym. A zatem wykonujac N-krotnie transformacje Hadamarda otrzymujemy superpozycje $2^N = e^{2 \ln N}$ stanow rejestru. Dla porownania N klasycznych operacji pozwoliloby przygotowac dokladnie jeden stan rejestru. Stan $|\psi\rangle$ jest superpozycja wszystkich stanow bazowych rejestru N kubitow. Podany na wejscie komputera kwantowego pozwala wykonac rownolegle (unitarne) operacje na wszystkich eksponencjalnie wielu ($e^{2 \ln N}$) mozliwych stanach wejscia. Koszt przygotowania tego stanu jest jednak zaledwie liniowy w N.

B. Funkcje

Funkcja jest odwzorowaniem

$$f \, : \, \{0, 1, ..., 2^N - 1\} \, \rightarrow \, \{0, 1, ..., 2^N - 1\} . \tag{95}$$

Klasyczny komputer po prostu zastepuje kazdy stan wejscia $0, 1, ..., 2^N - 1$ przez odpowiadajacy mu stan wyjscia $f(0), f(1), ..., f(2^N - 1)$. Gdyby funkcja f byla bijekcja, to komputer kwantowy moglby dzialac podobnie, zastepujac stan bazowy $|x\rangle$ przez stan $|f(x)\rangle$:

$$U_f \, |x\rangle \stackrel{?}{=} |f(x)\rangle . \tag{96}$$

Dla bijekcji $f(x) \neq f(y)$ jesli $x \neq y$, a zatem dzialanie f sprowadza sie do przetasowania uporzadkowanej talii wektorow bazowych nr $0, 1, ..., 2^N - 1$ w talie pomieszana $f(0), f(1), ..., f(2^N - 1)$. Odwzorowanie bazy w baze jest oczywiscie unitarne. Jesli jednak f nie jest bijekcja, to istnieja takie (ortogonalne) stany bazy $|x\rangle$ i $|y\rangle$, ktore musialyby zostac odwzorowane w takie same stany $|f(x)\rangle = |f(y)\rangle$, co przeczyloby unitarnosci odwzorowania.

Aby ominac problem funkcji niedwracalnych komputer kwantowy realizuje funkcje przy pomocy dwu rejestrow: pierwszy rejestr przechowuje dane wejsciowe $|x\rangle$, a drugi zawiera wyniki obliczen dla tych danych wejsciowych. Funkcja jest obliczana przy pomocy transformacji unitarnej U_f, ktora dziala na obydwa rejestry w taki sposob, ze

$$U_f \, |x\rangle|0\rangle = |x\rangle|f(x)\rangle . \tag{97}$$

W ogolnosci

$$U_f \, |x\rangle|y\rangle = |x\rangle|x \oplus f(y)\rangle , \tag{98}$$

gdzie $\oplus$ to dodawanie wartosci kolejnych bitow modulo 2.

Komputer klasyczny musi wyliczac wartosci funcji $f(x)$ dla poszczegolnych x po kolei. Komputer kwantowy moze obliczyc wszystkie wartosci funcji jednoczesnie:

$$U_f \left(\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle \right) |0\rangle \; = \; \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle \, |f(x)\rangle \; . \quad (99)$$

Przygotowanie wejsciowej superpozycji kosztowalo N jednobitowych transformacji Hadamarda, obliczenie U_f zostalo wykonane tylko jeden raz, a usyskalismy stan zawierajacy informacje o wszystkich 2^N wartosciach funkcji. To jest zbyt piekne by moglo byc prawdziwe.

Faktycznie, jesli chcemy poznac wartosci $f(x)$ dla poszczegolnych x, to musimy wykonac pomiar obydwu rejestrow. Pomiar pierwszego rejestru moze dac z takim samym prawdopodobienstwem kazdy ze stanow bazowych $|x\rangle$. Po wykonaniu tego pomiaru znamy x, a wiec stan dwu rejestrow skolapsowal do $|x\rangle|f(x)\rangle$, zatem pomiar drugiego rejestru musi dac stan $|f(x)\rangle$. Poznajemy zatem tylko $f(x)$ dla jednej przypadkowo wybranej wartosci x. Aby poznac pozostale wartosci funkcji musielibysmy powtorzyc cala procedure (transformacje Hadamarda, obliczenie funkcji,pomiar rejestrow) okolo 2^N razy, az uda sie wylosowac wszystkie 2^N wartosci x i zmierzyc odpowiadajace im wartosci $f(x)$. Jeszcze raz okazuje sie, ze znakomita wiekszosc ogromnej informacji kwantowej jest niedostepna.

Mimo to istnieja bardziej wyrafinowane pomiary, ktore moga dostarczyc informacji na temat globalnych wlasnosci funkcji. W nastepnym rozdziale zilustruje to stwierdzenie elementarnym przykladem.

XIV. PROBLEM DEUTSCHA.

Rozwazmy wszystkie funkcje jednobitowe, czyli odwzorowania ze zbioru $\{0,1\}$ w zbior $\{0,1\}$. Istnieja tylko 4 mozliwosci:

$$\begin{aligned} &f_1(0) = f_1(1) = 0 \; , \\ &f_2(0) = f_2(1) = 1 \; , \\ &f_3(0) = 0, \; f_3(1) = 1 \; , \\ &f_4(0) = 1, \; f_4(1) = 0 \; . \end{aligned} \quad (100)$$

Problem polega na tym, aby ustalic czy nieznana funkja jest stala (f_1 lub f_2), czy zmienna (f_3 lub f_4). Jest to proste pytanie o globalna wlasnosc funkcji. Najprostsza strategia polega na wyliczeniu $f(0)$ i $f(1)$, a nastepnie porownaniu tych wartosci. W tym celu musimy obliczyc funkcje 2 razy.

Algorytm Deutscha rozwiazuje problem wyliczajac funkcje tylko 1 raz. Potrzebne sa dwa bity przygotowane w stanie poczatkowym $|01\rangle$. Nalezy do nich zastosowac transformacje

$$U_f \; (U_A \otimes U_A) \; |01\rangle \; . \quad (101)$$

Pierwsza (z prawej) transformacja Hadamarda generuje stan

$$\begin{aligned} &(U_A \otimes U_A) \; |01\rangle \; = \\ &\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \; = \\ &\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \; , \end{aligned} \quad (102)$$

ktory jest superpozycja wszystkich mozliwych stanow wejsciowych i pozwoli na rownolegle wyliczenie w nastepnym kroku wszystkich mozliwych wartosci funkcji f.

W nastepnym kroku stosujemy bramke dwubitowa U_f, ktorej dzialanie jest zdefiniowane przez

$$U_f \; |i,j\rangle \; = \; |i, j \oplus f(j)\rangle \; , \quad (103)$$

gdzie $i,j = 0,1$, a $\oplus$ oznacza dodawanie modulo 2. Zastosowanie U_f do stanu (102) daje stan

$$\frac{1}{2}|0\rangle \, (|0 \oplus f(0)\rangle - |1 \oplus f(0)) + \frac{1}{2}|1\rangle \, (|0 \oplus f(1)\rangle - |1 \oplus f(1)) \; . \quad (104)$$

Mozna zauwazyc, ze jesli funkcja jest stala, $f(0) = f(1)$, to stan (104) ma postac

$$\pm|+\rangle|-\rangle \; ,$$

a jesli funkcja jest zmienna, $f(0) \neq f(1)$, to stan (104) jest rowny

$$\pm|-\rangle|-\rangle \; .$$

A zatem juz w tym momencie mozna roztrzygnac czy funkcja jest stala czy zmienna mierzac stan pierwszego kubitu w bazie $+/-$. Wynik $+$ bedzie oznaczal funkcje stala, a wynik $-$ funkcje zmienna.

Ten algorytm pozwala zaklasyfikowac funkcje f po jej jednokrotnym obliczeniu, zamiast dwu obliczen klasycznych. Nie jest to eksponencjane przespieszenie, bo trudno o takim mowic dla funcji jednobitowej. Dlatego w nastepnym przykladzie rozwazymy funkcje N kubitow.

XV. PROBLEM SIMONA

Niech funkcja f bedzie odwzorowaniem

$$f \; : \; \{0, ..., 2^N - 1\} \; \rightarrow \; \{0, ..., 2^N - 1\} \; . \quad (105)$$

W tym kontekscie wygodnie jest stany oznaczac przez wektory o wartosciach binarnych np. $\vec{x} = (0,1,1,1,0,...,1)$. O funkcji $f(\vec{x})$ wiadomo, ze albo jest bijekcja, albo istnieje okres $\vec{c}$ taki, ze

$$f(\vec{x}) = f(\vec{y}) \Leftrightarrow \vec{x} = \vec{y} \oplus \vec{c} \; . \quad (106)$$

Funkcja f nie jest znana, nalezy znalezc jej okres $\vec{c}$.

Klasyczne rozwiazanie tego problemu wymaga 2^N obliczen funkcji dla 2^N roznych wartosci argumentu $\vec{x}$. Algorytm kwantowy jest wielomianowy w N.

Na poczatek uogolnijmy transformate Hadamarda do N bitow: $U_H = U_A \otimes U_A \otimes ...U_A$. Jej dzialanie mozna prosto opisac jako

$$U_H \ |\vec{x}\rangle \ = \ \frac{1}{2^{N/2}} \sum_{\vec{y}} (-1)^{\vec{x}\vec{y}} \ |\vec{y}\rangle \ . \qquad (107)$$

Suma przebiega po wszystkich wektorach binarnych $\vec{y}$. Iloczyn skalarny wektorow binarnych jest standardowy $\vec{x}\vec{y} = x_1 y_1 + ... + x_N y_N$. W szczegolnosci dla $\vec{x} = 0$ mamy jak poprzednio

$$U_H \ |\vec{0}\rangle \ = \ \frac{1}{2^{N/2}} \sum_{\vec{y}} |\vec{y}\rangle \ , \qquad (108)$$

czyli prosta superpozycje wszystkich 2^N stanow bazowych.

Algorytm Simona wymaga dwu rejestrow, poczatkowo przygotowanych w stanie $\vec{0}$

$$|\vec{0}\rangle|\vec{0}\rangle \ . \qquad (109)$$

Do pierwszego (lewego) rejestru stosujemy transformacje Hadamarda U_H przygotowujac superpozycje po wszystkich 2^N wartosciach argumentu funkcji

$$\frac{1}{2^{N/2}} \sum_{\vec{x}} |\vec{x}\rangle|\vec{0}\rangle \qquad (110)$$

Nastepnie obliczamy rownolegle wszystkie 2^N wartosci funkcji stosujac jeden raz transformacje U_f i otrzymujac stan

$$\frac{1}{2^{N/2}} \sum_{\vec{x}} |\vec{x}\rangle|f(\vec{x})\rangle \ . \qquad (111)$$

Nastepnie ponownie stosujemy transformacje Hadamarda U_H do pierszego rejestru otrzymujac stan

$$\frac{1}{2^{N/2}} \sum_{\vec{x}} \sum_{\vec{y}} (-1)^{\vec{x}\vec{y}} \ |\vec{y}\rangle|f(\vec{x})\rangle \ . \qquad (112)$$

Nastepnie mierzymy najpierw drugi, a potem pierwszy rejestr.

Mozliwe sa dwa przypadki:

- Jesli f jest bijekcja, to pomiar drugiego rejestru daje losowa liczbe $f(\vec{k})$, kolapsujac stan (112) do

$$\frac{1}{2^{N/2}} \left(\sum_{\vec{y}} (-1)^{\vec{k}\vec{y}} \ |\vec{y}\rangle \right) |f(\vec{k})\rangle \ . \qquad (113)$$

  Pomiar na pierwszym rejestrze da takze losowa liczbe $\vec{l}$ i nie bedzie mozna sie doszukac zadnej korelacji pomiedzy wynikami pomiarow na pierwszym i drugim rejestrze.

- Jesli f ma okres $\vec{c}$, to pomiar na drugim rejestrze da wynik $\vec{x}'$ taki, ze $\vec{x}' = f(\vec{k})$ lub $\vec{x}' = f(\vec{k} \oplus \vec{c}) = f(\vec{k})$, kolapsujac stan (112) do

$$\frac{1}{\sqrt{2}2^{N/2}} \sum_{\vec{y}} \left[(-1)^{\vec{k}\vec{y}} + (-1)^{(\vec{k}\oplus\vec{c})\vec{y}} \right] |\vec{y}\rangle|f(\vec{k})\rangle \ =$$

$$\frac{1}{\sqrt{2}2^{N/2}} \sum_{\vec{y}} (-1)^{\vec{k}\vec{y}} \left[1 + (-1)^{\vec{c}\vec{y}} \right] |\vec{y}\rangle|f(\vec{k})\rangle \ . \qquad (114)$$

  Zauwazmy, ze $1 + (-1)^{\vec{c}\vec{y}}$ jest rowne 0 lub 2, a wiec pomiar na pierwszym rejestrze moze dac tylko taki $\vec{y}$, ze $\vec{c}\vec{y} = 0$.

Algorytm Simona powtarza powyzsza procedure az do uzyskania N roznych wartosci $\vec{y}_i$ z $i = 1, ..., N$. Nastepnie trzeba rozwiazac uklad N rownan liniowych z N niewiadomymi $\vec{y}_i\vec{c} = 0$ i uzyskac rozwiazanie $\vec{c}$. Jesli funkcja jest okresowa, to $\vec{c}$ jest okresem tzn. $f(\vec{c} \oplus \vec{x}) = f(\vec{x})$ dla kazdego $\vec{x}$. Jesli natomiast f jest bijekcja, to dla uzyskanego rozwiazania $f(\vec{c} \oplus \vec{x}) \neq f(\vec{x})$ dla kazdego $\vec{x}$. Aby rozstrzygnac wystarczy porownac $f(\vec{x})$ i $f(\vec{x} \oplus \vec{c})$ dla jednej wartosci $\vec{x}$.

Powyzszy algortym jest wielomianowy w N w przeciwienstwie do klasycznego algorytmu, ktory wymagalby 2^N operacji.

XVI. ALGORYTM SHORA: ROZKLAD NA CZYNNIKI PIERWSZE.

A. Algorytm Euklidesa: najwiekszy wspolny dzielnik.

W roku 300 p.n.e. Euklides opublikowal nastepujacy algorytm. Mamy znalezc najwiekszy wspolny dzielnik liczb N_1 i N_2. Zalozmy dla ustalenia uwagi, ze $N_1 > N_2$. Podzielmy najpierw N_1 przez N_2 otrzymujac reszte z dzielenia R_1. Nastepnie podzielmy N_2 przez R_1 otrzymujac kolejna reszte z dzielenia R_2. Nastepnie podzielmy R_1 przez R_2 itd., tak dlugo, az uzyskamy w koncu zerowa reszte z dzielenia. Ostatnia niezerowa reszta z dzielenia R jest poszukiwanym najwiekszym wspolnym dzielnikiem liczb N_1 i N_2.

Dla dowodu, ze tak uzyskane R faktycznie jest najwiekszym wspolnym dzielnikiem zauwazmy, ze

- R dzieli wszystkie poprzednie reszty z dzielenia, a takze liczby N_1 i N_2.

  Dowod: dla ujednolicenia notacji oznaczmy $N_1 = R_{-1}$ i $N_2 = R_0$. Kolejny krok algorytmu, polegajacy na dzieleniu $R_j : R_{j+1}$, sprowadza sie do znalezienia wyniku dzielenia $q_j \geq 1$ oraz kolejnej reszty z dzielenia $R_{j+2} < R_{j+1}$, ktore spelniaja rownanie

$$R_j \ = \ q_j \ R_{j+1} \ + \ R_{j+2} \ . \qquad (115)$$

Dla pewnego $j = J$ musi sie okazac, ze reszta z dzielenia jest zerowa:

$$R_J \;=\; q_J\; R_{J+1} \;+\; 0\;. \tag{116}$$

W najgorszym razie $R_{J+1} = 1$. Zatem mozemy oznaczyc $R_{J+1} = R$ i przeiterowac te rownania wstecz otrzymujac $R_J = q_J R$, $R_{J-1} = R q_{J-1} q_J$, $R_{J-2} = R[q_{J-2} q_{J-1} q_J + q_J]$ itd. W ogolnosci

$$R_{J-s} \;=\; Q_s\; R\;, \tag{117}$$

co konczy dowod.

- Ponadto kazdy wspolny dzielnik N_1 i N_2 dzieli rowniez (bez reszty) wszystkie reszty z dzielenia.

  Dowod: Niech D bedzie dzielnikiem N_1 i N_2, czyli istnieja takie $q_1, q_2 \geq 1$, ze $N_1 = q_1 D$ i $N_2 = q_2 D$. W takim razie

$$N_1 : N_2 = (q_1 : q_2) D = (q \text{ reszta } r) D = qD \text{ reszta } rD\;. \tag{118}$$

  Jak widac reszta z dzielenia $R_1 = rD$ jest podzielna przez D.

W takim razie R musi byc najwiekszym wspolnym dzielnikiem.

Aby oszacowac efektywnosc algorytmu Euklidesa zauwazmy, ze

$$R_j \;=\; q_j\; R_{j+1} \;+\; R_{j+2}\;, \tag{119}$$

gdzie $q_j \geq 1$ i $R_{j+2} < R_{j+1}$. A zatem

$$R_{j+2} \;<\; \frac{1}{2} R_j\;, \tag{120}$$

czyli dwa kolejne dzielenia redukuja reszte z dzielenia przynajmniej o czynnik 2, a zatem potrzeba nie wiecej niz $2 \ln N_1$ dzielen, by reszta z dzielenia stala sie rowna 0.

Poniewaz rowniez kazde dzielenie jest wielomianowe w $\ln N_1$, bo liczba bitow jest proporcjonalna do $\ln N_1$, to calkowita liczba operacji jest wielomianowa w $\ln N_1$.

Wniosek: Koszt znalezienia najwiekszego wspolnego dzielnika liczb $N_1 > N_2$ jest wielomianowy w $\log N_1$.

B. Teoria grup

Zbior liczb $< N$ nie majacych wspolnego dzielnika, czyli wzglednie pierwszych z N jest skonczona grupa wzgledem mnozenia modulo N. Liczba elementow tej grupy to wartosc funkcji Eulera $\varphi(N) < N$. Uwaga: liczby 1 i N sa wzglednie pierwsze, 1 nalezy do zbioru.

Dowod:

- Niech A i B naleza do zbioru. Iloczyn AB mod N to reszta R z dzielenia AB przez N, czyli $AB = qN + R$ z $q \geq 1$. Gdyby R i N mialy wspolny dzielnik p, to wtedy $AB : p = q(N : p) + (R : p)$ byloby liczba calkowita. Z zalozenia jednak A ani B nie dzieli sie przez p, bo A i B nie maja wspolnego dzielnika z N. A zatem R nie moze miec wspolnego dzienika z N i R nalezy do zbioru. Mnozenie modulo N jest dzialaniem wewnetrznym.

- Aby przekonac sie o isnieniu elementu odwrotnego zauwazmy, ze dla kazdego ustalonego $A < N$ z tego zbioru, wyniki mnozenia AB mod N sa rozne dla dla roznych $B < N$ przebiegajacych zbior. Innymi slowy wyniki mnozenia AB mod N przebiegaja caly zbior. Istotnie, gdyby istnialy liczby $B_1 \neq B_2$ takie, ze $A(B_1 - B_2) = 0 \bmod N$, to N dzieliloby liczbe $A(B_1 - B_2)$. Poniewaz A nie dzieli sie przez N, to N musialoby dzielic liczbe $B_1 - B_2$, ktora jest $< N$. Otrzymujemy sprzecznosc.

  Zatem dla ustalonego A liczby AB mod N sa rozne i naleza do zbioru, a wiec musi isniec B takie, ze $AB = 1 \bmod N$. Dla kazdego A isnieje element odwrotny do A.

Kazdy element A tej grupy ma skonczony rzad $r > 0$, czyli najmniejsza liczbe calkowita taka, ze

$$A^r \;=\; 1 \bmod N\;. \tag{121}$$

Poniewaz $A^x \bmod N$ nalezy do naszej grupy skonczonej, to $r \leq \varphi(N)$ i jest skonczone.

Potegi $A^x \bmod N$ stanowia podgrupe o rzedzie (liczbie elementow) r.

Twierdzenie Eulera mowi, ze $\varphi(N)$ jest podzielne przez r dla kazdego A. Innymi slowy istnieje p takie, ze $\varphi(N) : r = p$ i co za tym idzie

$$A^{\varphi(N)} \bmod N \;=\; A^{pr} \bmod N \;=\; (A^r)^p \bmod N \;=\; 1 \bmod N\;. \tag{122}$$

C. Kryptografia RSA: bezpieczenstwo kart kredytowych.

W kryptografii RSA klucz kodujacy moze byc powszechnie znany, natomiast klucz dekodujacy jest slodka tajemnica np. banku. Odtworzenie klucza dekodujacego na podstawie klucza kodujacego wymaga umiejetnosci efektywnego rozkladu na czynniki pierwsze duzych liczba naturalnych. Wierzy sie, ze faktoryzacja jest eksponencjalnie kosztowna i na tej hipotezie zasadza sie bezpieczenstwo kryptografii z publicznym kluczem.

Aby skonstruowac publiczny klucz B(olek)-pracownik B(anku) wybiera dwie duze liczby pierwsze p i q, ktore zachowuje w tajemnicy. Zamiast tego oblicza ich iloczyn

$$N = pq. \tag{123}$$

Poniewaz Bolek zna rozklad N na czynniki pierwsze, to zna rowniez wartosc funkcji Eulera $\varphi(N)$, zdefiniowanej

jako liczba liczb mniejszych od N, ktore nie maja wspolnego dzielnika z N. W przypadku iloczynu liczb pierwszych $N = pq$ mamy

$$\varphi(N) = (N-1)-(p-1)-(q-1) = (p-1)(q-1) \ , \quad (124)$$

bo tylko wielokrotnosci p lub q maja wspolny dzielnik z $N = pq$. $\varphi(N)$ jest latwo znalezc jesli sie zna rozklad N na czynniki pierwsze, ale trudno gdy zna sie tylko N.

Bolek wybiera przypadkowa liczbe $e < \varphi(N)$, ktora nie ma wspolnego dzielnika z $\varphi(N)$. Nastepnie przekazuje Alicji (i przy okazji kazdemu kto zechce podsluchiwac) wartosci e oraz N.

Wiadomosc od Alicji (jej numer karty kredytowej) to $a < N$. Alicja ma zadbac by a nie mialo wspolnego dzielnika z N (nalezalo do grupy). Alicja koduje swoja wiadomosc obliczajac

$$b \ = \ a^e \bmod N \ . \quad (125)$$

b to zakodowana wiadomosc.

Bolek zna odwrotnosc d liczby e spelniajaca rownosc

$$e \ d \ = \ 1 \ (\mathrm{mod} \ \varphi(N)) \quad (126)$$

i trzyma ja w sejfie. Bolek dekoduje wiadomosc b obliczajac

$$b^d \ = \ a^{ed} \ = \ a \ \left[a^{\varphi(N)}\right]^{\text{calkowita}} \ = \ a \ , \quad (127)$$

gdzie wszystkie rownosci sa modulo N. Tutaj korzystamy z rownosci $ed = 1 \bmod \varphi(N)$ oraz z twierdzenia Eulera, ze $a^{\varphi(N)} = 1 \bmod N$.

Gdyby mozna bylo efektywnie faktoryzowac $N = pq$, to mozna by bylo efektywnie obliczyc $\varphi(N) = (p-1)(q-1)$, a nastepnie element odwrotny do e czyli d. Element odwrotny mozna efektywnie znalezc przy pomocy wariantu algorytmu Euklidesa.

D. Algorytm Shora.

W roku 1993 Shor podal kwantowy algorytm, ktory faktoryzuje duza liczbe calkowita N w czasie wielomianowym w N. Shor wykorzystal fakt, ze faktoryzacja moze zostac sprowadzona do szukania okresu pewnych funckji. Mianowicie znalezienie czynnikow pierwszych p i q liczby $N = pq$ sprowadza sie do znalezienia okresu funkcji

$$f_{A,N}(x) \ = \ A^x \ (\mathrm{mod} \ N) \ , \quad (128)$$

gdzie $A < N$ jest przypadkowa liczba wzglednie pierwsza z N. Obliczenie funkcji jest efektywne, jesli wykorzystac wielokrotne podnoszenie do kwadratu.

Zbior liczb $< N$ i wzglednie pierwszych z N jest skonczona grupa. Kazdy element A tej grupy ma skonczony rzad $r < \varphi(N)$, czyli najmniejsza liczbe calkowita r taka, ze

$$A^r \ = \ 1 \bmod N \ , \quad (129)$$

lub $A^r - 1$ jest podzielne przez N. Rzad r jest okresem funkcji $f_{A,N}(x)$, ktory moze zostac efektywnie znaleziony przy pomocy komputera kwantowego.

Jesli r okaze sie parzyste, to $A^r - 1 = (A^{r/2}-1)(A^{r/2}+1)$ jest podzielne przez N. Wiemy, ze $(A^{r/2}-1)$ nie jest podzielne przez N, bo wtedy rzad A wynosilby $r/2$ zamiast r. Jesli ponadto rowniez $(A^{r/2}+1)$ nie jest podzielne przez N, lub $A^{r/2} \neq -1 \bmod N$, to N musi miec nietrywialny wspolny dzielnik z kazdym z czynnikow $(A^{r/2} \pm 1)$. A zatem najwiekszy wspolny dzielnik N i $(A^{r/2}+1)$ rozny od 1 jest szukanym czynnikiem pierwszym liczby N. Mozna go obliczyc efektywnym algorytmem Euklidesa.

A zatem jesli znajdziemy okres funkcji r, to rowniez latwo znajdziemy dzielnik liczby N, o ile r jest parzyste i $A^{r/2}+1$ nie dzieli sie przez N. Jakie jednak jest prawdopodobienstwo, ze dla przypadkowo wybranej liczby A jej rzad r spelnia te dwa warunki? Po kilku stronach dowodu okazuje sie, ze to prawdopodobienstwo jest $> \frac{1}{2}$!

Aby zapisac liczbe N potrzeba L bitow. Na wszelki wypadek nasze rejestry beda mialy $2L$ bitow kazdy. Przygotowujemy je poczatkowo w stanie

$$|0\rangle \ |0\rangle \ . \quad (130)$$

Nastepnie stosujemy transformate Hadamarda do pierwszego rejestru

$$\frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} |x\rangle \ |0\rangle \quad (131)$$

przygotowujac superpozycje po wszystkich argumentach funkcji. W kolejnym kroku obliczamy rownolegle wszystkie wartosci funkcji

$$\frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} |x\rangle \ |f_{A,N}(x)\rangle \ . \quad (132)$$

Nastepnie mierzymy stan drugiego rejestru, a stan pierwszego rejestru kolapsuje do superpozycji wszystkich x, ktore daja zmierzona wartosc $f_{A,N}(x)$. Poniewaz $f_{A,N}(x)$ ma okres r, to stan pierwszego rejestru mozna zapisac, z dokladnoscia do normalizacji, jako

$$\sum_{j=0}^{\text{floor}[2^{2L}/r]} |jr + l\rangle \quad (133)$$

gdzie l to pewne nieznane (i nieciekawe) przesuniecie, a r to okres funkcji $f_{A,N}(x)$. Przesuniecia mozna sie pozbyc przy pomocy transformaty Fouriera.

E. Kwantowa transformata Fouriera.

Rowazmy transformacje unitarna

$$U_{\mathrm{FT}}|x\rangle \ = \ \frac{1}{2^L} \sum_{y=0}^{2^{2L}-1} \exp\left(2\pi i \frac{xy}{2^{2L}}\right) \ |y\rangle \ , \quad (134)$$

gdzie $2L$ jest wielkoscia rejestru.

Jesli ta transformacja podzialac na dowolny stan kwantowy

$$U_{\rm FT} \sum_{x=0}^{2^{2l}-1} c_x \, |x\rangle \;=\; \sum_{y=0}^{2^{2L}-1} c_y \, |y\rangle \;, \qquad (135)$$

gdzie nowe amplitudy c_y sa transformata Fouriera amplitud c_x:

$$c_y = \frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} \exp\left(2\pi i \frac{xy}{2^{2L}}\right) \; c_x \;. \qquad (136)$$

Zastosowanie tej transformaty do stanu (133) daje superpozycje

$$\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \exp\left(2\pi i l j/r\right) \; |j \; 2^{2L}/r\rangle \qquad (137)$$

o ile r dzieli 2^{2L}. Otrzymalismy stan o okresie $2^{2L}/r$. Przesuniecie l pojawia sie jedynie w czynniku fazowym. Pomiar tego stanu daje jeden z wynikow $j \; 2^{2L}/r$, skad mozna oszacowac okres r.

Jesli 2^{2L} nie dzieli sie przez r, to otrzymujemy amplitudy prawdopodobienstwa nieco rozmyte wokol stanow $j \; 2^{2L}/r$. Ich szerokosc jest proporcjonalna do 2^{-2L}, dlatego wielkosc pierwszego rejestru zostala podwojona: $2L$ zamiast L.

F. Implementacja kwantowej transformaty Fouriera.

XVII. ALGORYTM GROVERA.

W roku 1996 Grover opisal problem przeszukiwania bazy danych i zaproponowal kwantowy algorytm, ktory pozwala rozwiazac ten problem bardziej efektywnie niz jakikolwiek algorytm klasyczny, ale bez przyspieszenia eksponencjalnego. Zadanie polega na tym, by znalezc czyjes nazwisko w ksiazce telefonicznej w sytuacji, gdy znany jest tylko jego numer telefonu. Poniewaz ksiazki telefoniczne sa uporzadkowane alfabetycznie wedlug nazwisk, anie wedlug roznacych numerow, to wyszukiwanie numeru telefonu w ksiazce zawierajacej dane N abonentow wymaga przeszukania srednio $N/2$ numerow. Grover pokazal, ze to zadanie moze zostac wykonane przez komputer kwantowy w czasie, ktory sie skaluje jak $\sqrt{N}$, czyli o czynnik $\sim \sqrt{N}$ lepszy niz klasycznie.

Algorytm Grovera nie jest eksponencjalnie szybszy niz algortm klasyczny poniewaz nie wykorzystuje kwantowego splatania. Istnieje dowod, ze pomimo to algorytm Grovera jest optymalnym algorytmem kwantowym, tzn. nie da sie osiagnac lepszej efektywnosci niz $\sim \sqrt{N}$ nawet, gdyby wykorzystywac splatanie. Z drugiej strony brak splatania oznacza, ze mozna zaimplementowac algorytm Grovera w dowolnym klasycznym ukladzie liniowym, ktory spelnia zasade superpozycji. Nie jest potrzebna do tego mechanika kwantowa. Taki eksperyment zostal z powodzeniem wykonany.

Zadanie moze zostac nastepujaco sformalizowane. Rozwazmy $N = 2^L$ roznych stanow kwantowych $x = 0, .., 2^L - 1$. Rozwazmy ponadto warunek C_ν, ktory dla kazdego ν jest spelniony przez dokladnie jeden stan tj. $C_\nu(x) = 1$ wtedy i tylko wtedy gdy $x = \nu$, a poza tym 0. Naszym zadanie polega na znalezieniu ν sprawdzajac warunek C_ν minimalna liczbe razy.

A. Jak to dziala ?

Kwantowy algorytm Grovera rozpoczyna sie od przygotowania rejestru L kubitow w stanie

$$|0\rangle \;. \qquad (138)$$

Nastepnie do calego rejestru zostaje zastosowana transformacja Hadamarda U_H; w jej wyniku rejestr zostaje przygotowany w superpozycji

$$\frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} |x\rangle \;, \qquad (139)$$

gdzie wszystkie stany $|x\rangle$, reprezentujace S_x, sa jednakowo prawdopodobne. Jak mozna latwo sprawdzic, ten stan nie jest stanem splatanym.

Po tym standardowym przygotowaniu nalezy okolo $\mathcal{O}(\sqrt{N})$ razy powtorzyc nastepujacy ciag operacji:

- Zastosuj operator U_{C_ν} zdefiniowany przez

$$\begin{aligned} U_{C_\nu}|\nu\rangle &= -|\nu\rangle \;, \\ U_{C_\nu}|x\rangle &= |x\rangle \;, \text{ dla } x \neq \nu \;, \end{aligned} \qquad (140)$$

  lub bardziej zwiezle

$$U_{C_\nu} \;=\; 1 \;-\; 2 \, |\nu\rangle\langle\nu| \;. \qquad (141)$$

  Operator U_{C_ν} to czarna skrzynka (z ksiazka telefoniczna)- wiemy, ze odwraca znak amplitudy przy szukanym stanie $|\nu\rangle$, ale nie mozemy do skrzynki zagladac i sprawdzic ile wynosi ν;

- Zastosuj bramke

$$U_D \;=\; U_H \, U_{C_0} \, U_H \;. \qquad (142)$$

Po okolo $\mathcal{O}(\sqrt{N})$ powtorzeniach nalezy wykonac pomiar stanu rejestru. Wynik pomiaru bedzie rowny ν z prawdopodobienstwem $> 50\%$.

Zauwazmy, ze ani transformacja Hadamarda U_H, ktora jest iloczynem operacji jednokubitowych, ani operacja U_{C_ν} nie splatuja roznych kubitow w rejestrze.

Algorytm jest stochastyczny, bo uzyskany wynik pomiaru jest poprawna odpowiedzia ν z prawdopodobienstwem $> 50\%$. Aby zwiekszyc to prawdopodobienstwo, nalezy powtorzyc algorytm kilka razy. Prawdopodobienstwo uzyskania poprawnego wyniku bedzie zmierzalo eksponencjalnie do 100% wraz z liczba powtorzen.

B. Dlaczego to dziala ?

Centralna czesc algorytmu polega na wielokrotnym zastosowaniu operacji $U_H\, U_{C_0}\, U_H\, U_{C_\nu}$. Zauwazmy przedze wszystkim, ze w wyniku takich operacji zmieniaja sie znaki i wartosci amplitud pradopodobienstwa, ale amplitudy caly czas pozostaja rzeczywiste. Z tego powodu mozna wygodnie przedstawic graficznie chwilowe amplitudu **OBRAZEK**. Dzialanie U_{C_ν} sprowadza sie do odwrocenia amplitudy stanu $|\nu\rangle$.

Dzialanie bramki $U_D = U_H U_{C_0} U_H$ jest bardziej zlozone. Ta bramka realizuje odwrocenie amplitudy wzgledem sredniej. Konkretniej, niech na pewnym etapie rachunkow stan rejestru ma postac

$$|\psi\rangle = \sum_{x=0}^{2^L-1} \alpha_x\, |x\rangle\ , \tag{143}$$

gdzie α_x to rzeczywista amplituda stanu $|x\rangle$. Srednia amplitud to

$$\alpha\ =\ \frac{1}{2^L} \sum_{x=0}^{2^L-1} \alpha_x\ . \tag{144}$$

Dzialanie bramki U_D na stan $|\psi\rangle$ daje stan $|\psi^{'}\rangle = U_D|\psi\rangle$ o amplitudach

$$\alpha_x^{'}\ =\ \alpha\ -\ (\alpha_x - \alpha)\ . \tag{145}$$

Chwila zastanowienia pokazuje, ze U_D wzmacnia amplitudy, ktore odstaja od sredniej, a tlumi te, ktore sa blizej sredniej.

Laczny efekt dzialania operacji U_{C_ν} i U_D wzmacnia amplitude α_ν przy szukanym stanie $|\nu\rangle$. U_{C_ν} najpierw odwraca ta amplitude, powodujac, ze ona odstaje od sredniej, a nastepnie taka ,,odstajaca" amplituda jest wzmacniana przez U_D. I tak wiele razy. Jak z tego wynika stan rejestru po j iteracjach mozna zapisac jako

$$|\psi_j\rangle\ =\ \alpha_\nu(j)\ |\nu\rangle\ +\ \beta(j)\ \left[\sum_{x(\neq\nu)} \frac{1}{\sqrt{N-1}}\ |x\rangle\right] \tag{146}$$

bo wszystkie stany, z wyjatkiem szukanego stanu $|\nu\rangle$, maja taka sama amplitude prawdopodobienstwa. Udowodnimy teraz, ze

$$\alpha_\nu(j)\ =\ \sin\left[(2j+1)\theta\right]\ , \tag{147}$$

gdzie kat θ spelnia rownanie $\sin^2\theta = 1/2^L = 1/N$. Z normalizacji stanu (146) wynika, ze $\beta(j) = \sqrt{1-\alpha_\nu^2(j)} = \cos[(2j+1)\theta]$.

Dowod jest indukcyjny. Sprawdzamy najpierw, ze wartosc poczatkowa amplitudy, czyli ,,po 0 iteracjach", to

$$\alpha_\nu(0)\ =\ \sin\theta\ =\ \frac{1}{2^{L/2}}\ =\ \frac{1}{\sqrt{N}}. \tag{148}$$

Zalozmy teraz, ze wzor (147) jest sluszny dla pewnego j i sprawdzmy ten wzor dla $j+1$. Operacja U_{C_ν} daje stan posredni

$$U_{C_\nu}\ |\psi_j\rangle\ =\ -\,\alpha_\nu(j)\ |\nu\rangle\ +\ \beta(j)\ \left[\sum_{x(\neq\nu)} \frac{1}{\sqrt{N-1}}\ |x\rangle\right]\ . \tag{149}$$

Zastosowanie do tego stanu posredniego oparacji U_D, czyli odbicie wzgledem wartosci sredniej

$$\alpha\ =\ \frac{-\alpha_\nu(j) + (N-1)\frac{\beta}{\sqrt{N-1}}}{N}\ , \tag{150}$$

daje stan

$$|\psi_{j+1}\rangle\ =\ \alpha_\nu(j+1)\ |\nu\rangle\ +\ \beta(j+1)\ \left[\sum_{x(\neq\nu)} \frac{1}{\sqrt{N-1}}\ |x\rangle\right] \tag{151}$$

gdzie

$$\alpha_\nu(j+1) = \alpha - [-\alpha_\nu(j) - \alpha]\ =\ \frac{N-2}{N}\ \sin[(2j+1)\theta]\ +\ \frac{2\sqrt{N-1}}{N}\ \cos[(2j+1)\theta] \tag{152}$$

Korzystajac z zalozenia, ze $\sin^2\theta = 1/N$, mozna latwo sprawdzic, ze wspolczynniki

$$\frac{N-2}{N}\ =\ \cos(2\theta)\ ,\ \ \frac{2\sqrt{N-1}}{N}\ =\ \sin(2\theta)\ , \tag{153}$$

a co za tym idzie

$$\alpha_\nu(j+1)\ =\ \cos(2\theta)\ \sin[(2j+1)\theta]\ +\ \sin(2\theta)\ \cos[(2j+1)\theta]\ =\ \sin[(2(j+1)+1)\theta]\ , \tag{154}$$

co nalezalo dowiesc.

Dla $j=0$, czyli zanim zostanie wykonana jakakolwiek operacja, mamy $\alpha_\nu(0) = \frac{1}{2^{L/2}}$, czyli bardzo mala liczbe jesli $N = 2^L$ jest duze. W miare jak rosnie j amplituda $\alpha_\nu(j)$ takze rosnie i osiaga pierwsze maksimum, gdy $(2j+1)\theta = \frac{\pi}{2}$. Jesli $N = 2^L$ jest duze, to $\theta \approx 2^{-L/2}$ i pierwsze maksimum jest osiagane dla tej calkowitej wartosci j, ktora jest najblizsza

$$j_{\max}\ =\ \frac{\pi}{4}\ 2^{L/2}\ =\ \frac{\pi}{4}\ \sqrt{N}\ . \tag{155}$$

Jesli N jest duze, to maksymalna wartosc $\alpha_\nu(j)$ jest bliska 1 i wystarcza jeden pomiar, aby znalezc szukana wartosc ν. Jesli bedziemy iterowac dalej, to amplituda zacznie znowu malec i stanie sie znowu zaniedbywalnie mala dla $j \approx 2j_{\max}$. A zatem musimy bardzo dokladnie dobrac liczbe iteracji, mozliwie najblizej $j_{\max} \sim \sqrt{N}$.

XVIII. KWANTOWA KOREKCJA BLEDOW - METODA SHORA.

Informacja kwantowa jest zakodowana w amplitudach prawdopodobienstwa stanu

$$\alpha\ |0\rangle\ +\ \beta\ |1\rangle\ , \tag{156}$$

gdzie α i β sa podatnymi za zaklocenia liczbami zespolonymi. W pewnym sensie komputer kwantowy jest komputerem analogowym.

Zalozmy, ze kubit zostal przygotowany w stanie $|0\rangle$. Zaklucajacy wplyw otoczenia moze sie zamanifestowac dzialaniem na ten stan hamiltonianem $H = X$. Po czasie t dzialania takiego hamiltonianu stan przeewoluuje do stanu

$$|0\rangle\ \cos t\ -\ i\ |1\rangle\ \sin t\ . \tag{157}$$

Gdyby teraz zmierzyc stan kubitu to z prawdopodobinstwem $\cos^2 t$ otrzymalibysmy poczatkowa wartosc $|0\rangle$, lub z prawdopodobienstwem $\sin^2 t$ otrzymalibysmy wartosc bledna $|1\rangle$. W pierwszym wypadku nie stwierdzamy bledu, ale w drugim stwierdzamy, ze stan kubitu ulegl odwroceniu. W rzeczywistosci stan kubitu jest zarowno poprawny jak i bledny z pewnymi amplitudami prawdopodobienstwa i dopiero nasz pomiar powoduje, ze musi sie zdecydowac na jedna z tych opcji.

W dalszym ciagu bedziemy stosowac skrot myslowy: kwantowy bit albo ulegl blednemu odwroceniu albo nie.

W praktyce bedziemy musieli sie dowiedziec czy wystapil blad nie sprawdzajac bezposrednio czy informacja kwantowa w stanie jest poprawna. Gdybysmy zmierzyli informacje kwantowa to uleglaby ona zakluceniu. A wiec musimy wykrywac bledy nie mierzac stanu kubitu. Czy to sie wydaje niemozliwe? Owszem, ale tak wlasnie dziala metoda Shora.

Metoda Shora zaklada pewien model oddzialywania z otoczeniem. W modelu tym otoczenie moze niezaleznie oddzialywac na stany pojedynczych kubitow

A. Naprawa odwroconych kubitow.

Korekcja odwroconych kubitow staje sie mozliwa jesli kazdy kubit logiczny reprezentowac przez splatany stan 3 kubitow

$$\begin{aligned} |\bar{0}\rangle\ &=\ \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)\ , \\ |\bar{1}\rangle\ &=\ \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)\ . \end{aligned} \tag{158}$$

Tutaj $\bar{0}$ i $\bar{1}$ oznaczaja logiczne 0 i 1.

Stany logiczne mozna odroznic, gdyz sa one stanami wlasnymi operatora $X_1X_2X_3$:

$$\begin{aligned} X_1X_2X_3\ |\bar{0}\rangle\ &=\ +|\bar{0}\rangle\ , \\ X_1X_2X_3\ |\bar{0}\rangle\ &=\ -|\bar{0}\rangle\ . \end{aligned} \tag{159}$$

Co mozna latwo sprawdzic. Innymi slowy, pomiar operatora $X_1X_2X_3$ daje logiczna wartosc $\bar{0}$ lub $\bar{1}$.

Nie istnieje natomiast operator jedno- lub dwu-bitowy pozwalajacy odroznic stany $|\bar{0}\rangle$ i $|\bar{1}\rangle$. Na przyklad, pomiar Z_1 w stanie $|\bar{0}\rangle$ daje 0 lub 1 z takim samym prawdopodobienstwem 1/2. Oznacza to, ze informacja kwantowa jest zakodowana nielokalnie, nie mozna jej wydobyc z pojedynczego fizycznego kubitu. Tym samym informacji kwantowej nie mozna rowniez zniszczyc zaklucajac stan pojedynczego kubitu, a dzieki temu bledy pojedynczych kubitow mozna naprawic.

Przekonamy sie jak dziala korekcja odwroconych kubitow rozwazajac dowolny stan logicznego kubitu

$$\alpha\ |\bar{0}\rangle\ +\ \beta\ |\bar{1}\rangle\ . \tag{160}$$

Zalozmy, ze wystapil blad polegajacy na odwroceniu jednego z trzech fizycznych kubitow (na stan zadzialal jeden z operatorow X_k z $k = 1, 2, 3$).

Aby zdiagnozowac, ktory kubit zostal odwrocony mierzymy operatory Z_1Z_2 oraz Z_2Z_3. Dla tych operatorow stany $|\bar{0}\rangle$ i $|\bar{1}\rangle$ sa stanami wlasnymi o wartosci wlasnej $+1$, a wiec pomiar tych operatorow w stanie (160) da zawsze wynik $+1$ niezaleznie od amplitud α i β, a tym samym taki pomiar nie zmieni stanu (160). Innymi slowy, jesli nie bylo bledu, to pomiar Z_1Z_2 oraz Z_2Z_3 nie wplywa na stan logicznego kubitu. Jesli jednak jeden z kubitow w stanie (160) zostal odwrocony, to pomiar jednego lub dwu z operatorow Z_1Z_2 oraz Z_2Z_3 da wynik -1. Jesli na przyklad zmierzymy, ze $z_1z_2 = -1$ oraz $z_2z_3 = -1$, to zdiagnozujemy, ze ulegl odwroceniu fizyczny kubit numer 2 itd. Ustaliwszy, ze zostal odwrocony kubit numer k $(1, 2, 3)$ poprawiamy ten blad odwracajac (negujac) bledny kubit za pomoca operacji X_k.

Nalezy podkreslic, ze pomiar Z_1Z_2 oraz Z_2Z_3 pozostawia nieznana wartosc Z_1, czyli jeden bit informacji. Pomiar tych dwu operatorow nie jest pomiarem stanu logicznego, ktory nawet po zdiagnozowaniu bledu pozostaje nieznany.

B. Naprawa bledow fazy.

Powyzsza 3-kubitowa konkatenacja (158) wystarcza, aby korygowac stany odwroconych kubitow, ale nie wystarcza, jesli wystepuja rowniez bledy fazy, wynikajace z zadzialania na stan (160) jednym z operatorow Z_k:

$$Z_k\ |\bar{0}\rangle\ =\ -\,|\bar{1}\rangle\ , Z_k\ |\bar{1}\rangle\ =\ -\,|\bar{0}\rangle\ .$$

Dzialanie tego operatora na stan (160) daje bledny stan

$$Z_k\ \left[\alpha\ |\bar{0}\rangle\ +\ \beta\ |\bar{1}\rangle\right]\ =\ -\ \left[\alpha\ |\bar{1}\rangle\ +\ \beta\ |\bar{0}\rangle\right]\ . \tag{161}$$

Pomiar operatorow Z_1Z_2 oraz Z_2Z_3 da w obydwu wypadkach $+1$, tak jakby nie bylo zadnego bledu - istotnie stan zadnego kubitu nie zostal odwrocony.

Aby skutecznie korygowac odwroce fazy, mozna logiczny kubit konkatenowac 9-krotnie:

$$|\bar{0}\rangle = \frac{1}{\sqrt{8}} (|000\rangle + |111\rangle) (|000\rangle + |111\rangle) (|000\rangle + |111\rangle) ,$$
$$|\bar{1}\rangle = \frac{1}{\sqrt{8}} (|000\rangle - |111\rangle) (|000\rangle - |111\rangle) (|000\rangle - |111\rangle) . \quad (162)$$

Odwrocone pojedyncze kubity koryguje sie tak samo jak w przypadku 3-krotnej konkatenacji tzn. mierzac operatory Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8 oraz Z_8Z_9, by nastepnie skorygowac odwrocony kubit k dzialajac operatorem X_k.

Jesli chodzi o bledy fazy, to po pierwsze zauwazmy, ze stany $|\bar{0}\rangle$ oraz $|\bar{1}\rangle$ w rownaniu (162) sa stanami wlasnymi operatorow

$$X_{1...6} = X_1X_2...X_6 ,$$
$$X_{4...9} = X_4X_5...X_9 , \quad (163)$$

o wartosciach wlasnych $+1$. Ich pomiar nie zmienia poprawnego stanu (160). Z drugiej strony, jesli na przyklad w rejestrze kubitow 123 wystapil blad wynikajacy z zadzialania na ten rejestr operatora Z_1, to ulegnie zmianie na przeciwna wartosc wlasna operatora $X_1X_2X_3$ w tym rejestrze, a tym samym wartosc wlasna operatora $X_{1...6}$ w blednym stanie wyniesie -1. Zdiagnozowawszy blad fazy w obrebie rejestru kubitow 123, naprawiamy go dzialajac jednym z operatorow Z_1, Z_2 lub Z_3 w obrebie tego rejestru.

C. Bledy wielokrotne.

Caly czas zakladalismy, ze blad dotyczyl pojedynczego kubitu. Aby sie przekonac, ze metoda Shora nie zadziala poprawnie w przypadku bledu 2 kubitow, zobaczmy co sie stanie gdy na przyklad ulegly odwroceniu jednoczesnie dwa kubity o numerach 1 i 2. Pomiary diagnostyczne dadza $z_1z_2 = +1$ oraz $z_2z_3 = -1$. Zakladajac, ze odwrocony jest najwyzej jeden kubit wywnioskujemy, ze tym odwroconym kubitem jest kubit numer 3. Nastepnie, dzialajac w dobrej wierze, zadzialamy operatorem X_3, aby skorygowac stan trzeciego kubitu. W wyniku naszych dzialan zostana odwrocone stany wszystkich 3 kubitow. Pelni najlepszych checi pogorszymy jeszcze sytuacje.

Aby uniknac podwojnych bledow kwantowa korekcja bledow musi byc stosowana dostatecznie czesto. Czestosc powinna byc tak duza, by prawdopodobienstwo nagromadzenia sie dwu bledow w odstepie czasu pomiedzy kolejnymi operacjami korekcji bylo znikomo male.

Jesli uzyskanie dostatecznej duzej czestosci korekcji nie jest technicznie mozliwe, to stosujemy kaskadowa konkatenacje. Polega ona na tym, ze kazdy fizyczny kubit w stanie (162) zastepujemy przez 9 fizycznych kubitow powielajac schemat rownania (162).

D. Uwagi.

Metoda Shora nie jest optymalna w sensie liczby fizycznych kubitow koniecznych do zakodowania jednego kubitu logicznego. W rzeczywistosci zamiast 9 wystarczy 5 kubitow.

Powyzsza metoda zaklada, ze bramki kwantowe i pomiary kwantowe dzialaja w sposob idealny. To zalozenie nie jest sluszne, ale istnieja metody kwantowej korekcji dzialania bramek.

W kwantowej korekcji bledow informacja kwantowa jest korygowana bez koniecznosci pomiaru samej informacji kwantowej. Nie wiadomo, nawet w zasadzie, co jest korygowane.

XIX. STABILIZATOR 5-KUBITOWY.

W poprzednim rozdziale opisalem 9-kubitowy kod Shora, ktory nie jest optymalny, ale za to jego dzialanie jest proste do wyjasnienia. W tym rozdziale opisze optymalny kod 5-kubitowy. Jest on waznym przykladem tzw. ,,stabilizer codes" i dowod jego optymalnosci wynika z ogolnej teorii takich kodow, ktora tutaj pomine.

A. Generatory stabilizator.

Logiczne stany $|\bar{0}\rangle$ i $|\bar{1}\rangle$ koduje sie w rejestrze 5 fizycznych kubitow. Aby wykryc wszystkie mozliwe bledy wystarczy zmierzyc 4 operatory

$$M_1 = XZZX1 , \quad (164)$$
$$M_2 = 1XZZX , \quad (165)$$
$$M_3 = X1XZZ , \quad (166)$$
$$M_4 = ZX1XZ . \quad (167)$$
$$(168)$$

Sa to tzw. generatory stabilizatora. Mozna zauwazyc, ze operatory $M_{2,3,4}$ otrzymuje sie z M_1 przez cykliczna permutacje kubitow. Piaty operator $M_5 = ZZXIX = M_1M_2M_3M_4$, otrzymany przez kolejna cykliczna permutacje M_4, jest iloczynem pozostalych generatorow, wiec nie jest od nich niezalezny, ale jako iloczyn generatorow rowniez nalezy do stabilizatora.

Poniewaz cykliczna permutacja generatora jest rowniez generatorem, to caly kod jest cykliczny. W szczegolnosci logiczne stany $|\bar{0}\rangle$ i $|\bar{1}\rangle$ sa cykliczne, czyli nie zmieniaja sie przy cyklicznych permutacjach kubitow.

Dla kazdego $i = 1, 2, 3, 4$ mamy

$$M_i^2 = 1 , \quad (169)$$

co oznacza, ze wartosci wlasne kazdego M_i moga byc rowne jedynie ± 1.

Co wiecej generatory komutuja ze soba

$$[M_i , M_j] = 0 , \quad (170)$$

dla kazdego $i,j = 1,2,3,4$, a wiec generatory maja wspolne wektory wlasne.

Logiczne stany $|\bar{0}\rangle$ i $|\bar{1}\rangle$ nalezy wybrac jako wektory wlasne generatorow M_i o wartosciach wlasnych $+1$:

$$M_i \; |\bar{0}\rangle \; = \; |\bar{0}\rangle \; , \tag{171}$$

$$M_i \; |\bar{1}\rangle \; = \; |\bar{1}\rangle \; . \tag{172}$$

Dzieki temu pomiar dowolnego M_i w poprawnym stanie musi dac wynik $+1$.

Mozna powiedziec, ze dowolny blad jest generowany przez dzialanie pewnego generatora bledu. Na przyklad, geneator $X_1 = X1111$ dzialajac na poprawny stan $|\psi\rangle$ odwraca stan kubitu numer 1, czyli generuje blad pierwszego kubitu. Bledny stan $X_1|\psi\rangle$ moze zostac zdiagnozowany, o ile jest stanem wlasnym o wartosci wlasnej -1 dla jednego z generatorow M_i, czyli

$$M_i \; X_1 \; |\psi\rangle \; = \; - \; X_1 \; |\psi\rangle \; . \tag{173}$$

Z drugiej strony wiemy, ze

$$X_1 \; M_i \; |\psi\rangle \; = \; + \; X_1 \; |\psi\rangle \; . \tag{174}$$

Dodajac te rownania stronami otrzymujemy

$$(X_1 \; M_i \; + \; M_i \; X_1) \; |\psi\rangle \; = \; 0 \; . \tag{175}$$

A zatem jesli istnieje takie i, ze

$$X_1 \; M_i \; + \; M_i \; X_1 \; = \; 0 \; , \tag{176}$$

to blad generowany przez X_1 moze zostac zdiagnozowany. Ogolnie, blad moze byc zdiagnozowany, gdy jego generator antykomutuje z ktoryms z generatorow stabilizatora M_i. Latwo sprawdzic, ze $X_1 \; M_4 \; + \; M_4 \; X_1 \; = \; 0$, czyli blad X_1 zostanie zdiagnozowany, gdy pomiar M_4 da wynik -1. Taki blad bedzie mozna naprawic dzialajac na bledny stan $X_1|\psi\rangle$ generatorem X_1:

$$X_1 \; (X_1|\psi\rangle) \; = \; |\psi\rangle \; . \tag{177}$$

B. Syndrom bledu.

(Anty)komutatory generatorow M_i i generatorow bledu X_j mozna zebrac w nastepujacej tabelce.

	X_1	X_2	X_3	X_4	X_5
M_1	0	1	1	0	0
M_2	0	0	1	1	0
M_3	0	0	0	1	1
M_4	1	0	0	0	1

(178)

Kolumny sa numerowane przez generatory bledu X_j, a wiersze przez generatory stabilizatora M_i. 0 w pozycji ij oznacza, ze M_i komutuje z X_j. 1 w pozycji ij oznacza, ze M_i antykomutuje z X_j. Na przyklad, jesli wystapil blad generowany przez X_3, to pomiary $M_{1,2}$ dadza -1, a pomiary $M_{3,4}$ dadza $+1$.

Podobna tabelke mozna zapisac dla bledow fazy.

	Z_1	Z_2	Z_3	Z_4	Z_5
M_1	1	0	0	1	0
M_2	0	1	0	0	1
M_3	1	0	1	0	0
M_4	0	1	0	1	0

(179)

Zdefiniujemy $Y = ZX$ jako blad fazy polaczony z odwroceniem stanu kubitu. Tabelka dla Y, to

	Y_1	Y_2	Y_3	Y_4	Y_5
M_1	1	1	1	1	0
M_2	0	1	1	1	1
M_3	1	0	1	1	1
M_4	1	1	0	1	1

(180)

Nieprzypadkowo, tabelka Y jest suma (binarna) tabelek Z i X.

Mozna zauwazyc, ze zadna z 15 kolumn w trzech tabelkach sie nie powtarza, czyli dla kazdego rodzaju bledu mamy inny syndrom. O takim kodzie mowi sie, ze nie jest zdegenerowany.

Mozna rowniez zauwazyc, ze te 15 kolumn wyczerpuja wszystkie niezerowe 4-bitowe slowa binarne, co silnie sugeruje, ze ten kod jest optymalny.

C. Stany logiczne.

Stabilizator to zbior wszystkich nietrywialnych operatorow, ktore mozna otrzymac jako iloczynow generatorow $M_{1,2,3,4}$. W naszym przypadku stabilizator ma 15 elementow. Jest to operator M_1 wraz z czterema jego cyklicznymi permutacjami $M_{2,3,4,5}$. Stabilizator zawiera rowniez operator

$$M_3 M_4 = -YXXY1 \tag{181}$$

wraz z jego czterema cyklicznymi permutacjami oraz operator

$$M_2 M_5 = -ZYYZ1 \tag{182}$$

wraz z jego czterema cyklicznymi permutacjami. Wszystkie elementy stabilizatora komutuja ze soba. Stany poprawne sa stanami wlasnymi elemetow stabilizatora o wartosci wlasnej $+1$.

Jako operatory logiczne mozna wybrac operatory

$$\bar{Z} \; = \; ZZZZZ \; , \tag{183}$$

$$\bar{X} \; = \; XXXXX \; . \tag{184}$$

Operator $\bar{Z}$ nalezy zmierzyc, aby odroznic logiczne stany $|\bar{0}\rangle$ i $|\bar{1}\rangle$. Z kolei operator $\bar{X}$ dokonuje operacji NOT na stanach logicznych. Powyzszy wybor jest dopuszczalny ponieważ $\bar{Z}$ i $\bar{X}$ komutuja z generatorami stabilizatora

M_i, a wiec stany wlasne operatorow $\bar{Z}$ i $\bar{X}$ sa stanami wlasnymi M_i.

Aby zmierzyc $\bar{Z}$ mozna zmierzyc po kolei $Z_{1,2,3,4,5}$, a nastepnie pomnozyc wyniki. Alternatywne wyrazenia na $\bar{Z}$ i $\bar{X}$ mozna otrzymac mnozac te operatory przez generatory stabilizatora. Na przyklad mozemy wybrac

$$\bar{Z} = (ZZZZZ)(-ZYYZ1) = -1XX1Z \qquad (185)$$

oraz

$$\bar{X} = (XXXXX)(-YXXY1) = -Z11ZX \ . \qquad (186)$$

Mozna zauwazyc, ze w nowych opratorach logicznych wystepuja dwa opratory 1. A wiec, aby zmierzyc logiczne $\bar{Z}$ lub $\bar{X}$ wystarczy zmierzyc wartosc X lub Z jedynie dla 3 kubitow sposrod pieciu.

Aby skonstruowac stany logiczne $|\bar{0}\rangle$ i $|\bar{1}\rangle$ zauwazmy najpierw, ze z dowolnego stanu zaczatkowego $|\psi_0\rangle$ mozemy otrzymac stan

$$|\Psi_0\rangle = \sum_{M\in S} M|\psi_0\rangle \ , \qquad (187)$$

gdzie suma przebiega po wszystkich 15 elementach stabilizatora S. Taki stan jest stanem wlasnym elemntow stabilizatora o wartosci wlasnej $+1$,

$$M\ |\Psi_0\rangle \ = \ +\ |\Psi_0\rangle \ , \qquad (188)$$

dlatego ze pomnozenie przez M jedynie permutuje wyrazy w sumie (187).

Aby otzrymac logiczne $|\bar{0}\rangle$ mozemy wybrac jako stan zaczatkowy $|00000\rangle$, dla ktorego $\bar{Z} = +1$. Otrzymamy

$$\begin{aligned} |\bar{0}\rangle \ &= \ |00000\rangle \\ &+ \ (M_1 + \text{cykliczne permutacje})|00000\rangle \\ &+ \ (M_3M_4 + \text{c.p.})|00000\rangle \\ &+ \ (M_2M_5 + \text{c.p.})|00000\rangle \\ &= \ |00000\rangle \\ &+ \ (|10010\rangle + \text{c.p.}) \\ &- \ (|11110\rangle + \text{c.p.}) \\ &- \ (|01100\rangle + \text{c.p.}) \ . \end{aligned} \qquad (189)$$

W podobny sposob aby otzrymac logiczne $|\bar{1}\rangle$ wybieramy stan zaczatkowy $|11111\rangle$, dla ktorego $\bar{Z} = -1$ i otrzymujemy

$$\begin{aligned} |\bar{1}\rangle \ &= \ |11111\rangle \\ &+ \ (|01101\rangle + \text{c.p.}) \\ &- \ (|00001\rangle + \text{c.p.}) \\ &- \ (|10011\rangle + \text{c.p.}) \ . \end{aligned} \qquad (190)$$

XX. NMR.

Pierwsze eksperymentalne obliczenia kwantowe wykonano w technologii magnetycznego rezonansu jadrowego (ang.:NMR). W tej technologii podstawowym obiektem jest wieloatomowa molekula. Jadra atomowe atomow molekuly maja spiny, ktore odzialywuja wzajemnie sprzezeniem dipolowym oraz sprzegaja sie do zewnetrznych pol magnetycznych. Stanami kubitow (spinow) mozna manipulowac przy pomocy odpowiednich pol magnetycznych. Spiny jadrowe bardzo slabo sprzegaja sie do otoczenia, typowe czasy dekoherencji sa rzedu 1 sekundy.

W silnym polu magnetycznym w kierunku osi z hamiltonian molekuly dwuatomowej upraszcza sie do

$$H \ = \ \frac{1}{2}\hbar\omega_A\sigma_A^z \ + \ \frac{1}{2}\hbar\omega_B\sigma_B^z \ + \ \frac{1}{2}\hbar\omega_{AB}\sigma_A^z\sigma_B^z \ . \qquad (191)$$

W polu magnetycznym rzedu 10 T typowe czestosci precesji wokol osi z sa $\omega_A \approx \omega_B \simeq 100$ MHz, czyli w zakresie czestosci radiowych, podczas gdy typowa wartosc sprzezenia pomiedzy spinami jest rzedu $\omega_{AB} \simeq 100$Hz.

A. Operacje jednokubitowe.

Jesli czestosci rezonansowe poszczegolnych spinow jadrowych sa rozne, $\omega_A \neq \omega_B$, to mozna wykonac operacje na wybranym pojedynczym kubicie dostrajajac sie do jego czestosci rezonansowej. Zalozmy, ze przylozono pole magnetyczne w kierunku osi x, ktore oscyluje z czestoscia rezonansowa dla pewnego kubitu. Zakladajac, ze pole zewnetrzne jest znacznie silniejsze od sprzezen pomiedzy roznymi kubitami, na czas przylozenia pola zewnetrznego hamiltonian wybranego kubitu mozna przyblizyc przez

$$H \ = \ \frac{1}{2}\hbar\omega\sigma^z \ - \ \hbar\delta\sigma^x\cos(\omega t) \ . \qquad (192)$$

Poczatkowy stan kubitu (spinu) to $|\psi(0)\rangle$. Aby rozwiazac rownanie Schrodingera

$$i\hbar\frac{d}{dt}|\psi(t)\rangle \ = \ H\ |\psi(t)\rangle \qquad (193)$$

korzystnie jest przejsc do obrazu oddzialywania, gdzie stan spinu to

$$|\psi(t)\rangle \ = \ e^{-i\frac{1}{2}\omega\sigma^z t}\ |\chi(t)\rangle \ . \qquad (194)$$

Powyzsze podstawienie przeksztalca rownanie Schrodingera w

$$i\frac{d}{dt}|\chi(t)\rangle \ = \ -\delta\left(\frac{e^{i\omega t}+e^{-i\omega t}}{2}\right)\left(e^{i\omega t}\sigma^+ + e^{-i\omega t}\sigma^-\right)|\chi(t)\rangle \ , \qquad (195)$$

gdzie $\sigma^\pm = (\sigma^x \pm i\sigma^y)/2$. Jesli pominac wyrazy proporcjonalne do $e^{2i\omega t}$ oraz $e^{-2i\omega t}$, ktore bardzo szybko oscyluja i usredniaja w czasie sie do zera, to otrzymamy prostsze rownanie

$$i\frac{d}{dt}|\chi(t)\rangle \ = \ -\frac{\delta}{2}\sigma^x\ |\chi(t)\rangle \ , \qquad (196)$$

ktore opisuje precesje spinu wokol osi x. W wyniku precesji przez czas t spin ulega obrotowi wokol osi x o kat δt

$$|\chi(t)\rangle \;=\; e^{i\delta t\sigma^x/2}\,|\chi(0)\rangle\;. \tag{197}$$

Zauwazmy, ze gdy $\delta t=\pi$, to spin obraca sie wokol osi x o kat π, co jest rownowazne operacji NOT.

W podobny sposob, przykladajac pole magnetyczne w kierunku osi y oscylujace z czestoscia rezonansowa ω, mozna zrealizowac obroty wokol osi y. W szczegolnosci obrot wokol osi y o kat π jest rowniez operacja NOT. A zatem, na pojedynczym kubicie mozemy wykonywac dowolne obroty wokol osi w plaszczyznie $x-y$, a w szczegolnosci operacje NOT. W dalszym ciagu bede uzywal oznaczen, gdzie np. obrot spinu A wokol osi y o kat θ to $R^y_A(\theta)\equiv e^{i\theta\sigma^y_A/2}$. Co wiecej mozna wykonac dowolny obrot wokol osi z skladajac obroty wokol osi x i y:

$$R^z(\theta)=R^x(-\pi/2)R^y(\theta)R^x(\pi/2)\;. \tag{198}$$

Podsumowujac, jest mozliwe wykonanie dowolnego obrotu spinu, czyli dowolnej operacji unitarnej na pojedynczym kubicie.

B. Bramka CNOT.

Dla obliczen kwantowych konieczna jest mozliwosc wykonania dowolnej transformacji jednokubitowej oraz przynajmniej jednej operacji dwukubitowej. Mozna pokazac, ze takie minimum wystarcza, aby wykonac dowolna transformacje unitarna na rejestrze N kubitow. W tym podrozdziale, pokaze jak wykonac operacje CNOT w technologii NMR.

Na poczatek zauwazmy, ze czlon w hamiltonianie dla 2 kubitow

$$\frac{1}{2}\hbar\omega_{AB}\sigma^z_A\sigma^z_B\;. \tag{199}$$

generuje sprzezony obrot dwu kubitow wokol osi z:

$$R^z_{AB}(\omega_{AB}t) \;=\; e^{i\omega_{AB}t\sigma^z_A\otimes\sigma^z_B/2} \;=$$
$$\cos(\omega_{AB}t/2)+i\sin(\omega_{AB}t/2)\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{bmatrix} \tag{200}$$

Operacja CNOT na kubitach A i B, gdzie stan kubitu B kontroluje operacje wykonana na kubicie A, jest dana przez sekwencje obrotow

$$C_{AB} \;=\; R^y_A(-\pi/2)R^z_B(-\pi/2)R^z_A(-\pi/2)R^z_{AB}(\pi)R^y_A(\pi)\;, \tag{201}$$

o czym mozna sie latwo przekonac zapisujac te operacje w wersji macierzowej

$$\begin{aligned}C_{AB} \;=\;& \frac{1}{2^{5/2}}\\ &\times\begin{bmatrix}1&-1&0&0\\1&1&0&0\\0&0&1&-1\\0&0&1&1\end{bmatrix}\begin{bmatrix}1-i&0&0&0\\0&1-i&0&0\\0&0&1+i&0\\0&0&0&1+i\end{bmatrix}\\ &\times\begin{bmatrix}1-i&0&0&0\\0&1+i&0&0\\0&0&1-i&0\\0&0&0&1+i\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{bmatrix}\\ &\times\begin{bmatrix}1&1&0&0\\-1&1&0&0\\0&0&1&1\\0&0&-1&1\end{bmatrix}\\ =\;&\sqrt{-i}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\;.\end{aligned} \tag{202}$$

Ostatnia macierz rzeczywiscie odpowiada operacji CNOT

$$C_{AB} \;=\; |1_B\rangle\langle 1_B|1_A+|0_B\rangle\langle 0_B|X_A\;. \tag{203}$$

C. ,,Komputer kwantowy w filizance kawy".

Do tej pory zajmowalismy sie pojedyncza molekula tak jakby byla ona zawieszona w prozni. W rzeczywistosci obliczenia wykonuje sie na duzych zespolach molekul (10^{23} lub 1 cm^3) w roztworze wodnym w temperaturze pokojowej (,,filizance kawy"). Duza liczba molekul jest potrzebna, aby uzyskac mierzalny sygnal. Wada takiej technolgii jest, ze molekuly nie wystepuja w stanie czystym,

$$\rho \;\neq\; |0\rangle\langle 0| \tag{204}$$

ale w mieszanym stanie termicznym, opisywanym przez macierz gestosci

$$\rho \;\sim\; \sum_{s=0}^{2^N-1} e^{-E(s)/kT}\;|s\rangle\langle s|\;, \tag{205}$$

gdzie $|s\rangle = |s_1...s_N\rangle$ jest stanem rejestru N kubitow/spinow, k to stala Boltzmana, T to temperatura, a

$$E(s) \;=\; \sum_{i=1}^{N}\frac{1}{2}\hbar\omega_i s_i\;. \tag{206}$$

to energia stanu $|s\rangle$ w polu magnetycznym w kierunku osi z. W temperaturze pokojowej $kT\gg\hbar\omega_i$ i ten stan

jest bliski macierzy jednostkowej

$$\rho \;=\; \frac{1}{2^N}\sum_{s=0}^{2^N-1}|s\rangle\langle s|\;, \tag{207}$$

czyli stanowi calkowicie przypadkowemu.

Okazuje sie jednak, ze niewielkie odstepstwa od macierzy jednostkowej wystarcza, aby umozliwic obliczenia kwantowe. Dla przykladu rozwazmy molekule/rejestr o dwu spinach/kubitach. Molekuly sa poczatkowo w stanie mieszanym o macierzy gestosci

$$\rho \;=\; \begin{bmatrix} a & 0 & 0 & 0\\ 0 & b & 0 & 0\\ 0 & 0 & c & 0\\ 0 & 0 & 0 & d \end{bmatrix} \tag{208}$$

w bazie stanow $00, 01, 10, 11$. Na tych dwu spinach chcemy wykonac obliczenia polegajace na transformacji unitarnej U. Po wykonanu tej transformacji dostajemy macierz gestosci

$$\rho_1 = U\rho U^\dagger\;. \tag{209}$$

Nastepnie na innym zespole molekul wykonujemy najpierw permutacje stanow $01, 10, 11$, ktora prowadzi do macierzy gestosci

$$P_1(\rho) \;=\; \begin{bmatrix} a & 0 & 0 & 0\\ 0 & c & 0 & 0\\ 0 & 0 & d & 0\\ 0 & 0 & 0 & b \end{bmatrix}\;, \tag{210}$$

a nastepnie wykonujemy te same obliczenia otrzrymujac

$$\rho_2 = UP_1(\rho)U^\dagger\;. \tag{211}$$

Nastepnie na jeszcze jednym zespole molekul wykonujemy inna permutacje stanow $01, 10, 11$, ktora daje macierz gestosci

$$P_2(\rho) \;=\; \begin{bmatrix} a & 0 & 0 & 0\\ 0 & d & 0 & 0\\ 0 & 0 & b & 0\\ 0 & 0 & 0 & c \end{bmatrix}\;, \tag{212}$$

i znowu wykonujemy obliczenia unitarne otrzymujac

$$\rho_3 = UP_2(\rho)U^\dagger\;. \tag{213}$$

Na samym koncu sumujemy wyniki obliczen otrzymujac

$$\rho_1+\rho_2+\rho_3 \;=\; U\rho^{'}U^\dagger\;, \tag{214}$$

gdzie

$$\rho^{'} \;=\; \rho + P_1(\rho) + P_2(\rho) \tag{215}$$

$$\;=\; (b+c+d)1 + (3a-b-c-d)\begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{216}$$

$$\;=\; (b+c+d)1 + (3a-b-c-d)|0\rangle\langle 0|, \tag{217}$$

ktore jest efektywnie stanem czystym tzn. mierzony na koncu wynik obliczen jest taki jakby obliczenia zostaly wykonane przy stanie poczatkowym 00.

D. Uwagi.

W praktyce trudno skalowac ta technologie powyzej $N \approx 10$. Problem polega na tym, ze w miare gdy rosnie N w rownaniu (217) maleje stosunek stanu czystego $|0\rangle\langle 0|$ do macierzy jednostkowej i coraz trudniej uzyskac mierzalny sygnal.

$N = 7$ spinow w molekule aniliny wystarcza, aby faktoryzowac liczbe 15. Wykonano taki eksperyment.

$N = 7$ wystarcza takze by przetestowac 5-bitowy algorytm korekcji bledow i takze wykonano taki eksperyment.

Molekula o $N > 10$ spinach ma kwantowa moc obliczeniowa wieksza od jakiegokolwiek komputera klasycznego.