QUBITS - KUBITY

Kubit to najprostszy układ kwantowy. Posiada tylko 2 stany własne. Do tej klasy układów szczególnie przydaje się notacja Diraca.

Omówmy ją, przy okazji przypominając kilka faktów dotyczących wektorów.

Przestrzeń liniowa, lub inaczej przestrzeń wektorowa, to uogólnienie przestrzeni, z jaką mieliśmy do czynienia do tej pory.
Wektory, jakie znamy z fizyki klasycznej np $\vec{a} = [a_x, a_y, a_z]$ są szczególnym przypadkiem takiej przestrzeni. W mech. kwant. przestrzeń funkcji stanu jest przestrzenią liniową (tzw. przestrzenią Hilberta).

SLAJD2 W notacji Diraca stosuje się nawiasy ket $|...\rangle$ i bra $\langle ...|$ (od bracket - nawias)
Za pomocą nawiasów bra zapisuje się wektory z tzw przestrzeni dualnej, wektor $\langle V|$ jest hermitowskim sprzężeniem wektora $|V\rangle$.

Czyli np. zapis $\langle v | w \rangle$ oznacza iloczyn skalarny wektorów $|v\rangle$ i $|w\rangle$.

Kolejne slajdy przedstawiają aksjomaty, które powinny wyglądać znajomo, ponieważ są prawdziwe również dla zwykłych wektorów z geometrii. Tutaj są zapisane w sposób bardziej ogólny.

SLAJD OSTATNI

Omówmy formę, w jakiej będziemy zapisywać wektory opisujące stany układów kwantowych.

$$|v\rangle = \sum_{i=1}^{n} v_i |i\rangle$$

$(n=3)$

załóżmy, że rozważana przestrzeń ma wymiar 3. Czyli każdy wektor tej przestrzeni możemy zapisać w postaci:

$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle + \gamma|3\rangle$$

Oznaczenia 1, 2, 3 w tym zapisie to nie są liczby, tylko etykiety. Nie muszą mieć nic wspólnego z liczbowymi wartościami tych etykiet. To etykiety elementów bazy.

Możemy wprowadzić dowolne etykiety elementów bazy. Np prawidłowym wektorem może być:

$$|\psi\rangle = \alpha\,|\text{☼}\rangle + \beta\,|\text{☾}\rangle + \gamma\,|\text{✡}\rangle$$

Liczbami (zespolonymi) są współczynniki α, β i γ.

Załóżmy, że ψ jest funkcją falową o postaci

$$|\psi\rangle = \alpha\,|1\rangle + \beta\,|2\rangle + \gamma\,|3\rangle.$$

Oznacza to, że wykonując pomiar możemy otrzymać jedynie wartości własne odpowiadające tym 3 ortogonalnym (czyli wzajemnie wykluczającym się) stanom. Prawdopodobieństwo znalezienia układu w stanie $|1\rangle$ wynosi α^2, w stanie $|2\rangle$ wynosi β^2, w $|3\rangle$ – γ^2.

Kubit to system (układ) kwantowy, który posiada wyłącznie 2 stany własne (ortogonalne). Czyli baza przestrzeni stanów ma 2 elementy. Najprostszy układ klasyczny to np bit (który może mieć wartość 0 lub 1) lub moneta (orzeł lub reszka). Kubit jest kwantowym odpowiednikiem takich 2-stanowych układów. Różnica polega na tym, że stan kubitu jest superpozycją stanów własnych. Stan kwantowej monety zapiszemy np

$$\alpha |orzeł\rangle + \beta |reszka\rangle .$$

JAK DZIAŁA POMIAR STANU?

① Jeśli kwantowa moneta jest w jednym ze swoich stanów własnych (np $\beta = 0$), to w wyniku pomiaru otrzymamy na pewno ten stan (np orzeł). W ogólności otrzymamy stan orzeł z pstwem α^2, reszka z pstwem β^2.

② Pomiar zmienia stan układu!

Pomiar to oddziaływanie z otoczeniem, więc wpływa na stan. Jeśli przed pomiarem stan układu jest

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

to po pomiarze stan układu będzie

$|\psi\rangle = |0\rangle$ (z pstwem α^2), lub

$|\psi\rangle = |1\rangle$ (z pstwem β^2).

Następuje tzw kolaps (collapse), dekoherencja funkcji falowej.

kubit to abstrakcyjny model układu o dwóch stanach własnych. Może to być np foton o polaryzacji pionowej lub poziomej

$$|\psi\rangle = \alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle,$$

lub elektron o spinie góra lub dół

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

lub częściej +1, -1

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$$

PODSTAWOWE OPERACJE NA KUBITACH

(brak slajdów do tej części)

Baza przestrzeni stanów pojedynczego kubitu składa się z wektorów $|0\rangle$ i $|1\rangle$.

Zdefiniujmy te elementy jako wektory kolumnowe:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{i} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Wektory te są ortogonalne, tzn

$$\langle 0 | 1 \rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

$$\langle 1 | 0 \rangle = 0$$

$$\langle 0 | 0 \rangle = 1$$

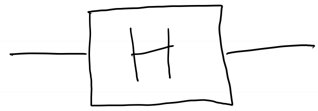
$$\langle 1 | 1 \rangle = 1$$

Zdefiniujmy kilka operatorów (bramek logicznych) za pomocą których będziemy wykonywać operacje na kubitach.

BRAMKA HADAMARDA (Hadamard gate)

Jest to pierwsza z tzw uniwersalnych bramek.
Jest to bramka jednokubitowa. Ozn: $\hat{H}$

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



ozn. graficzne

Sprawdźmy wynik działania tej bramki na stany własne.

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+0 \\ 1-0 \end{pmatrix} =$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right)$$

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0+1 \\ 0-1 \end{pmatrix} =$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right)$$

Warto zauważyć, że stany $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ i $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ również są stanami ortogonalnymi, a więc stanowią alternatywną bazę.

Możemy je np oznaczyć

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

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

$$\hat{H}|0\rangle = |+\rangle \quad \text{i} \quad \hat{H}|1\rangle = |-\rangle$$

Najważniejszą funkcją bramki Hadamarda jest właśnie zmiana bazy wektora.

BRAMKI PAULIEGO

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$\hat{X}$ to kwantowy NOT $-\!\!\oplus\!\!-$

$$\hat{X}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\hat{X}|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

w ogólności $\hat{X}(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$

$$XX|0\rangle = |0\rangle \qquad XX|1\rangle = |1\rangle$$

$$XX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$ macierz jednostkowa

$$I|0\rangle = |0\rangle$$

$$I|1\rangle = |1\rangle$$

$\hat{Y}$ nie będziemy używać w moich przykładach

$\hat{Z}$ jest szczególnym przypadkiem bramki przesunięcia fazy $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$ $\varphi = \pi$

$$\hat{Z}|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$\hat{Z}|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

Stany dwukubitowe

Wymieńmy stany własne układu składającego się z 2 kubitów. Jest ich 4. Oznaczmy je:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

BRAMKA CNOT - controlled NOT

- jest to bramka dwukubitowa
- w zależności od stanu pierwszego kubitu (kubit kontrolny lub sterujący) zmienia stan drugiego kubitu (docelowego)

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

$$CNOT|00\rangle = |00\rangle$$

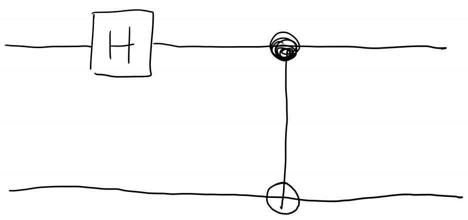
$$CNOT|10\rangle = |11\rangle$$

$$CNOT|01\rangle = |01\rangle$$

$$CNOT|11\rangle = |10\rangle$$

SPLĄTANIE KWANTOWE

Rozważmy następujący układ złożony z dwóch bramek: $\hat{H}$ i $\hat{CNOT}$



Prześledźmy działanie tego układu na stan $|00\rangle$

$\hat{H}$ działa wyłącznie na pierwszy kubit, więc:

$$\hat{H}|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Teraz ten pierwszy kubit jest kontrolny:

$$\frac{1}{\sqrt{2}} CNOT(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$$

analogicznie dla pozostałych:

$$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$$

$$|10\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \to \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$$

$$|11\rangle \to \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \to \frac{1}{\sqrt{2}}|01\rangle - |10\rangle) = |\Psi^-\rangle$$

Uzyskane stany $|\Phi^+\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$ i $|\Psi^-\rangle$ to tzw stany Bella.

PRACA DOMOWA: udowodnij, że stany Bella są ortogonalne.

Spróbujmy teraz wyrazić jeden ze stanów Bella jako iloczyn dwóch stanów kubitów. Czyli spróbujmy rozseparować ten stan dwukubitowy na dwa stany jednokubitowe.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \left(\alpha|0\rangle + \beta|1\rangle\right)\left(\gamma|0\rangle + \delta|1\rangle\right)$$

$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Czyli iloczyny $\alpha\delta$ i $\beta\gamma$ muszą być zerowe, a $\alpha\gamma$ i $\beta\gamma$ niezerowe. Nie jest to możliwe!

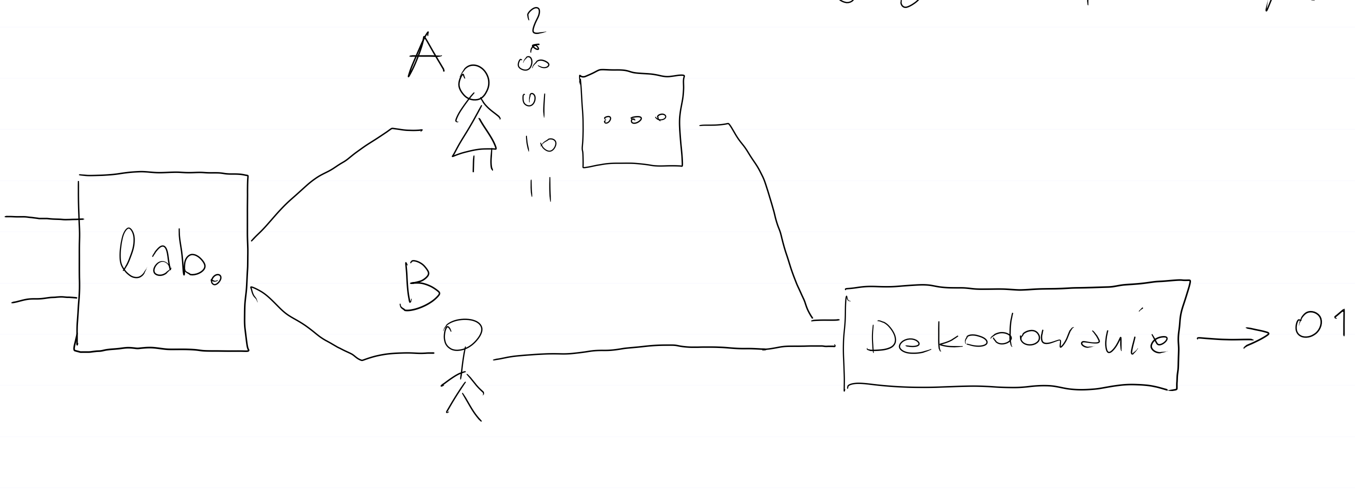
Kubity opisane tym stanem (i jakimkolwiek ze stanów Bella) są splątane. Funkcji falowej opisującej ich stan nie da się rozseparować na dwie funkcje jednocząstkowe (jednokubitowe). Tzn że jeśli zmienimy stan jednego kubitu, automatycznie zmieni się stan drugiego.

Splątanie kwantowe i zmiana bazy pomiaru to podstawowe elementy wielu algorytmów kwantowych (teleportacja kwant., kryptografia kw.).

PRZYKŁAD 1. - gęste kodowanie

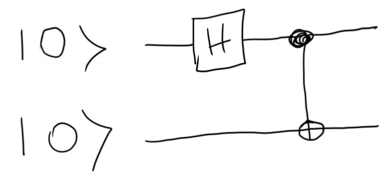
Jest to przykład protokołu pozwalającego przesłać 2 klasyczne bity w jednym kubicie.

Ogólny schemat jest następujący: mamy dwoje uczestników komunikacji: Alicja chce przesłać 2 klasyczne bity do Boba. W pierwszym kroku zostają przygotowane w laboratorium 2 splątane kubity, jeden z nich otrzymuje Alicja, drugi Bob. Następnie Alicja wykonuje na swoim kubicie pewną operację, zależną od tego, co chce zakodować, po czym przesyła swój kubit do Boba. Bob wykonuje operację dekodowania na obu kubitach i odczytuje informację.



CZĘŚĆ 1. - przygotowanie splątanych kubitów (stan Bella)

W laboratorium są przygotowane 2 kubity z wykorzystaniem omówionego wcześniej układu złożonego z bramek H i CNOT.



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

CZĘŚĆ 2. - kodowanie

Do Alicji trafił pierwszy z kubitów. Następnie Alicja wykonuje na kubicie jedną z 4 operacji, zależnie od informacji, jaką chce przesłać.

	informacja (2 klasyczne bity)	operacja
a)	0 0	I
b)	0 1	X
c)	1 0	Z
d)	1 1	X Z

a) 0 0 : Alicja robi I, czyli nie zmienia stanu.

b) 0 1 : X, czyli zmiana $0 \to 1$ i $1 \to 0$

Stan 2-kubitowy po tej operacji to

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

c) 1 0 : Z, czyli odwrócenie fazy, otrzymujemy

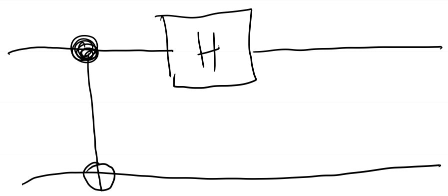
$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

d) 1 1 : XZ, czyli b) + zmiana fazy

$$\frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle)$$

CZĘŚĆ 3. - dekodowanie

Bob otrzymuje od Alicji kubit, a następnie na obu kubitach przeprowadza operację dekodowania, która jest odwrotna do tej, za pomocą której przygotowano stan splątany Bella w laboratorium



kolejne przypadki (pomińmy to $\frac{1}{\sqrt{2}}$)

a) $|00\rangle + |11\rangle \xrightarrow{CNOT} |00\rangle + |10\rangle \xrightarrow{H}$

$\rightarrow |00\rangle + |10\rangle + |00\rangle - |10\rangle = |00\rangle$

b) $|10\rangle + |01\rangle \xrightarrow{CNOT} |11\rangle + |01\rangle \xrightarrow{H}$

$\rightarrow |01\rangle - |11\rangle + |01\rangle + |11\rangle = |01\rangle$

c) $|00\rangle - |11\rangle \xrightarrow{CNOT} |00\rangle - |10\rangle \xrightarrow{H}$

$\rightarrow |00\rangle + |10\rangle - |00\rangle + |10\rangle = |10\rangle$

d) $-|10\rangle + |01\rangle \xrightarrow{CNOT} -|11\rangle + |01\rangle \xrightarrow{H}$

$\rightarrow -|01\rangle + |11\rangle + |01\rangle + |11\rangle = |11\rangle$

CZĘŚĆ 4. – pomiar

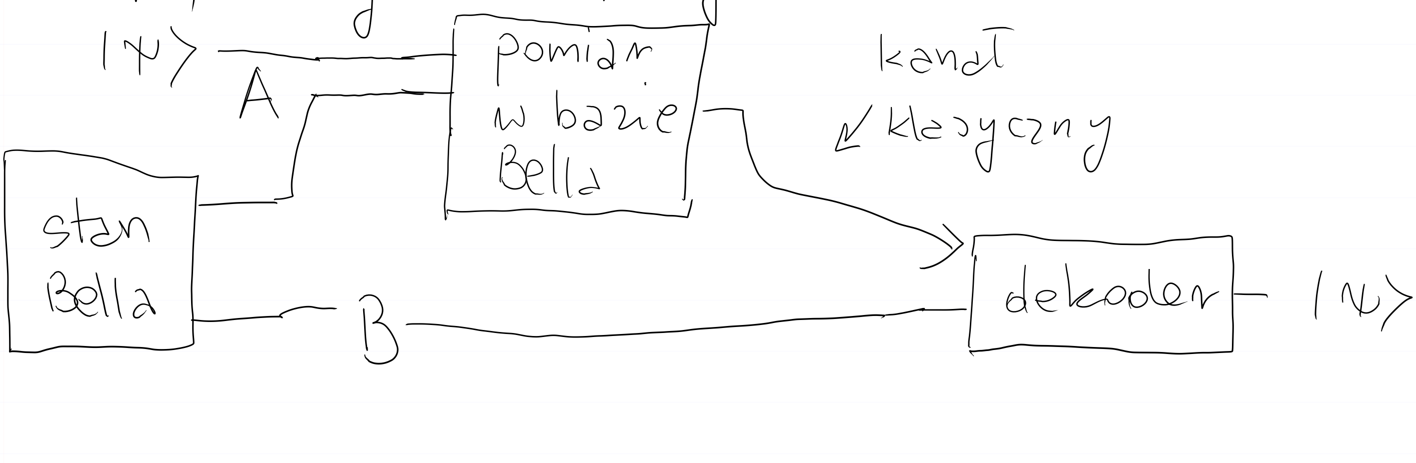
Bob po operacji dekodowania w każdym przypadku otrzymuje jeden ze stanów własnych. Jeśli otrzymał stan dwukubitowy $|01\rangle$ to z p-stwem 1 w wyniku pomiaru otrzyma bity 0 i 1, czyli to, co zakodowała Alicja.

PRZYKŁAD 2. - kwantowa teleportacja

Protokół kwantowej teleportacji pozwala przesłać informację kwantową (czyli stan kwantowego układu) za pomocą klasycznego kanału.

Ogólny schemat:

Alicja posiada pewien układ kwantowy w stanie $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Posiada też jeden ze splątanych kubitów, przygotowanych wcześniej w laboratorium. Drugi ze splątanych kubitów ma Bob (podobnie jak w przykładzie 1.) Następnie Alicja dokonuje pomiaru stanu swoich obu kubitów w bazie stanów Bella, a wynik pomiaru (klasyczny) przesyła do Boba. Bob wykonuje dekodowanie i odtwarza stan kubitu, który miała Alicja.



stan układu Alicji $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

wspólny stan Bella $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

(Alicja otrzymała pierwszy kubit, Bob - drugi).

Stan łączny: (pomińmy $\frac{1}{\sqrt{2}}$)

$$* = (\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle) =$$

$$= \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle$$

Następnie stan dwóch pierwszych kubitów musimy wyrazić w bazie stanów Bella, czyli stanów

$|\Phi^+\rangle = |00\rangle + |11\rangle$

$|\Psi^+\rangle = |01\rangle + |10\rangle$

$|\Phi^-\rangle = |00\rangle - |11\rangle$

$|\Psi^-\rangle = |01\rangle - |10\rangle$

I kolejno:

$|00\rangle = |\Phi^+\rangle + |\Phi^-\rangle$

$|01\rangle = |\Psi^+\rangle + |\Psi^-\rangle$

$|10\rangle = |\Psi^+\rangle - |\Psi^-\rangle$

$|11\rangle = |\Phi^+\rangle - |\Phi^-\rangle$

kont. równanie $* = \alpha|\Phi^+\rangle|0\rangle + \alpha|\Phi^-\rangle|0\rangle +$

$+ \alpha|\Psi^+\rangle|1\rangle + \alpha|\Psi^-\rangle|1\rangle + \beta|\Psi^+\rangle|0\rangle - \beta|\Psi^-\rangle|0\rangle +$

$+ \beta|\Phi^+\rangle|1\rangle - \beta|\Phi^-\rangle|1\rangle =$

$$= \Big[|\phi^+\rangle (\alpha|0\rangle + \beta|1\rangle) + |\psi^+\rangle (\alpha|1\rangle + \beta|0\rangle)$$
$$+ |\phi^-\rangle (\alpha|0\rangle - \beta|1\rangle) + |\psi^-\rangle (\alpha|1\rangle - \beta|0\rangle)\Big] \frac{1}{2}$$

po uwzględnieniu pomijanych czynników $\frac{1}{\sqrt{2}}$

można zauważyć, że wyrażenia w nawiasach to

$$\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$
$$\alpha|1\rangle + \beta|0\rangle = \hat{X}|\psi\rangle$$
$$\alpha|0\rangle - \beta|1\rangle = \hat{Z}|\psi\rangle$$
$$\alpha|1\rangle - \beta|0\rangle = \hat{Z}\hat{X}|\psi\rangle$$

Alicja wykonuje pomiar i klasycznym kanałem przesyła do Boba, czyli przesyła informację, który ze stanów ortogonalnych Bella otrzymała. Teraz wystarczy, że Bob na swoim kubicie wykona odpowiednią operację ($\hat{I}$, $\hat{X}$, $\hat{Z}$ lub $\hat{Z}\hat{X}$), by odtworzyć stan $|\psi\rangle$ Alicji.

W protokole tym układ o stanie $|\psi\rangle$ nie jest kopiowany, ani nawet przenoszony. Jego stan jest niszczony, a następnie odtwarzany w innym układzie.