Internet kwantowy
(z krótkim wstępem do informatyki kwantowej)

Jarosław Miszczak

Instytut Informatyki Teoretycznej i Stosowanej PAN

16. stycznia 2012

Plan wystąpienia

1. Krótki wstęp do kwantowej teorii informacji
   - Skąd się biorą stany kwantowe?
   - Jak opisać układy złożone?
   - Co to jest splątanie?
   - Jak się buduje obwody kwantowe?
   - Jak działa teleportacja?
2. Komunikacja kwantowa i sieci kwantowe
   - Komunikacja kwantowa
   - Sieci kwantowe
3. Składniki intersieci kwantowych
   - Powielacze
   - Pamięci
   - Rutery
4. Modele intersieci kwantowych

Skąd się biorą stany kwantowe?

Zasada "zerowego" kwantowania

Przyjmijmy, że $0 \mapsto \binom{1}{0}$ oraz $1 \mapsto \binom{0}{1}$.

Notacja Diraca

$|0\rangle \equiv \binom{1}{0}$, $|1\rangle \equiv \binom{0}{1}$

Ponieważ $|0\rangle$ i $|1\rangle$ to wektory, więc nasz kwantowy bit może być w stanie

$$x_0|0\rangle + x_1|1\rangle, \quad x_0, x_1 \in \mathbb{C}, \tag{1}$$

np. $\frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle$.
Zatem "zerowa" zasada kwantowania przyjmuje postać

$$\{0,1\} + |\ \rangle \mapsto \mathrm{span}\{|0\rangle, |1\rangle\}. \tag{2}$$

Jak opisać układy złożone?

Zasada "zerowego" kwantowania dla układów złożonych

Jeżeli $(b_0, b_1) \in \{0,1\} \times \{0,1\}$ to przyjmujemy $(b_0, b_1) \mapsto |b_0\rangle \otimes |b_1\rangle$.

W przypadku dwóch bitów kwantowych, dozwolone stany to stany bazowe

$$|00\rangle \equiv |0\rangle \otimes |0\rangle,\ |01\rangle \equiv |0\rangle \otimes |1\rangle,\ |10\rangle \equiv |1\rangle \otimes |0\rangle,\ |11\rangle \equiv |1\rangle \otimes |1\rangle$$

oraz ich dowolne kombinacje $x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle$.

Co to jest splątanie?

Najważniejszym zasobem dostępnym w kwantowej teorii informacji jest splątanie.

Rozkład Schmidta

Macierz współczynników rozkładu w bazie

$$\begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix}$$

można zdiagonalizować unitarnie.

Stan jest splątany jeżeli po diagonalizacji macierz ma dwa elementy niezerowe, np.

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

Jak się buduje obwody kwantowe?

Zasada "zerowego" kwantowania operacji

Dla zadanej operacji, kwantowym odpowiednikiem jest takie przekształcenie wektorów, które działa odpowiednio na bazie $\{|0\rangle, |1\rangle\}$.

Przykładowo dla operacji NOT kwantowy odpowiednik to

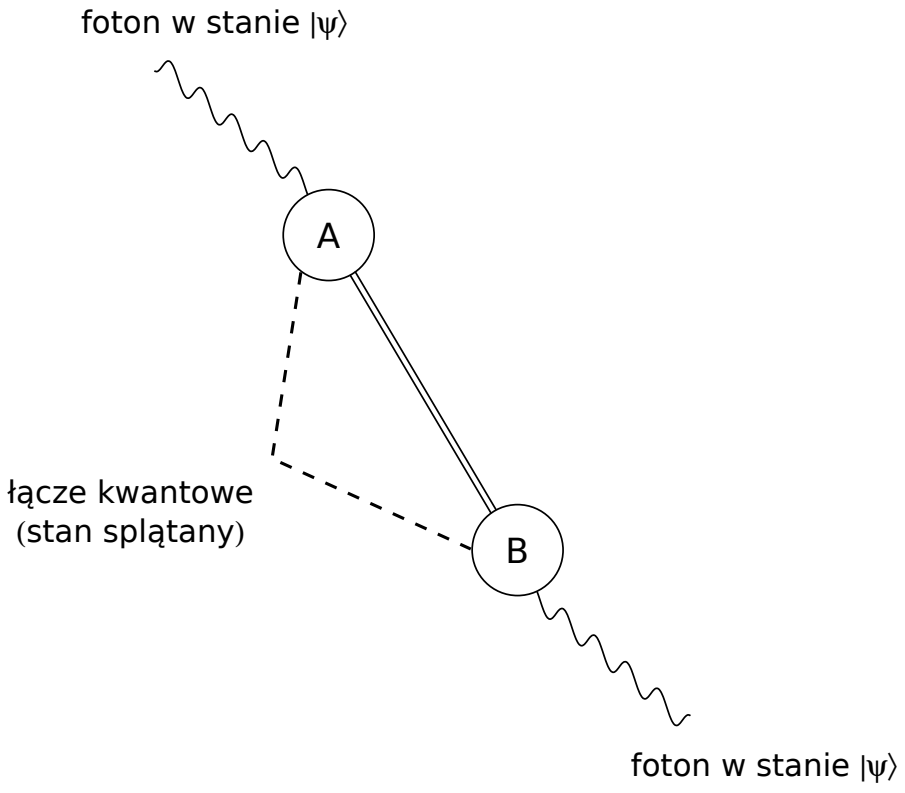
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv \sigma_x.$$

Możliwe jest natomiast wprowadzenie operacji, które nie mają odpowiedników klasycznych, np. operacja Hadamarda

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

Jak działa teleportacja?

Teleportacja pozwala na przesłanie stanu kwantowego poprzez wysłanie dwóch bitów.



Do przeprowadzenia teleportacji konieczne jest łącze kwantowe – współdzielenie pary maksymalnie splątanej. Tego typu łącza są kluczowym elementem sieci kwantowych.

Komunikacja kwantowa i sieci kwantowe

Komunikacja kwantowa to *sztuka* przesyłania stanów kwantowych.

Jest wykorzystywana do

- przesyłania nośników kwantowych na duże odległości
  - w kwantowej dystrybucji klucza,
  - w bezpośredniej komunikacji kwantowej,
- konstrukcji interfejsów między łączami kwantowymi a procesorami/pamięciami kwantowymi.

Komunikacja kwantowa i sieci kwantowe

Sieci kwantowe składają się z dużej liczby węzłów (np. procesorów kwantowych) komunikujących się za pomocą łączy kwantowych.

- Internet kwantowy (intersieć kwantowa) nie musi operować na dużych odległościach.
- W skład sieci wchodzić mogą urządzenia działające na różnych zasadach fizycznych.
- W obrębie sieci będą wymieniane zarówno dane klasyczne jak i kwantowe.
- Wraz ze wzrostem ilości węzłów w sieci zwiększa się
  - oferowana wydajność
  - złożoność zarządzania

Komunikacja kwantowa i sieci kwantowe

Z dużą ilością węzłów wiążą się wyzwania.

- Przesyłanie danych kwantowych pomiędzy węzłami kwantowymi wymaga metod zapewniających transmisję stanów kwantowych które zapewnią
  - niezawodność – np. poprzez uwzględnienie zerwanych łączy,
  - wydajność – np. zapewnienie optymalnych metod trasowania.
- Wykorzystując protokoły kwantowe należy wziąć pod uwagę złożoną strukturę sieci.
- Nie wiadomo czy i jak można wykorzystać protokoły kwantowe do poprawy wydajności sieci.

Składniki intersieci kwantowych

Dla budowy złożonych sieci operujących na wymianie nośników kwantowych kluczowe są

- powielacze kwantowe (ang. *quantum repeaters*) – możliwość dystrybucji stanów splątanych na duże odległości,
- pamięci kwantowe – ogromna poprawa wydajności powielaczy kwantowych, a co za tym idzie przepustowości sieci,
- interfejsy kwantowe – łącza pomiędzy nośnikiem informacji a pamięcią lub procesorem kwantowym,
- rutery kwantowe – nadzór złożonych intersieci kwantowych oraz łącza na styku kilku podsieci.

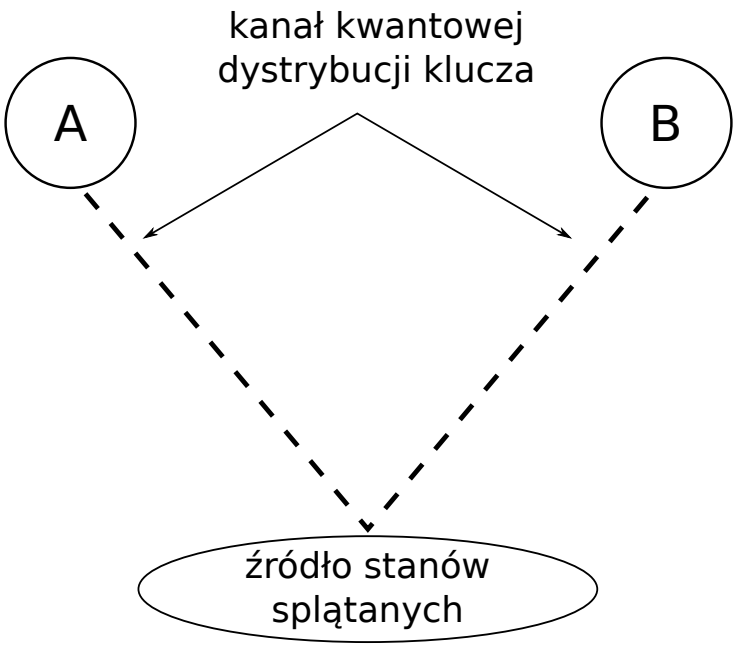
Powielacze kwantowe

Powielacze kwantowe są integralną częścią intersieci kwantowych.

- Obecnie główne problemy przy tworzeniu długodystansowych łączy to straty w światłowodach i błędy detektorów.
- Powielacze umożliwiają znaczne zwiększenie zasięgu na jakim może operować kwantowe przesyłanie danych.
- Dystrybucja stanów kwantowych na dużych odległościach jest konieczna do praktycznego zastosowania wielu protokołów kwantowych.

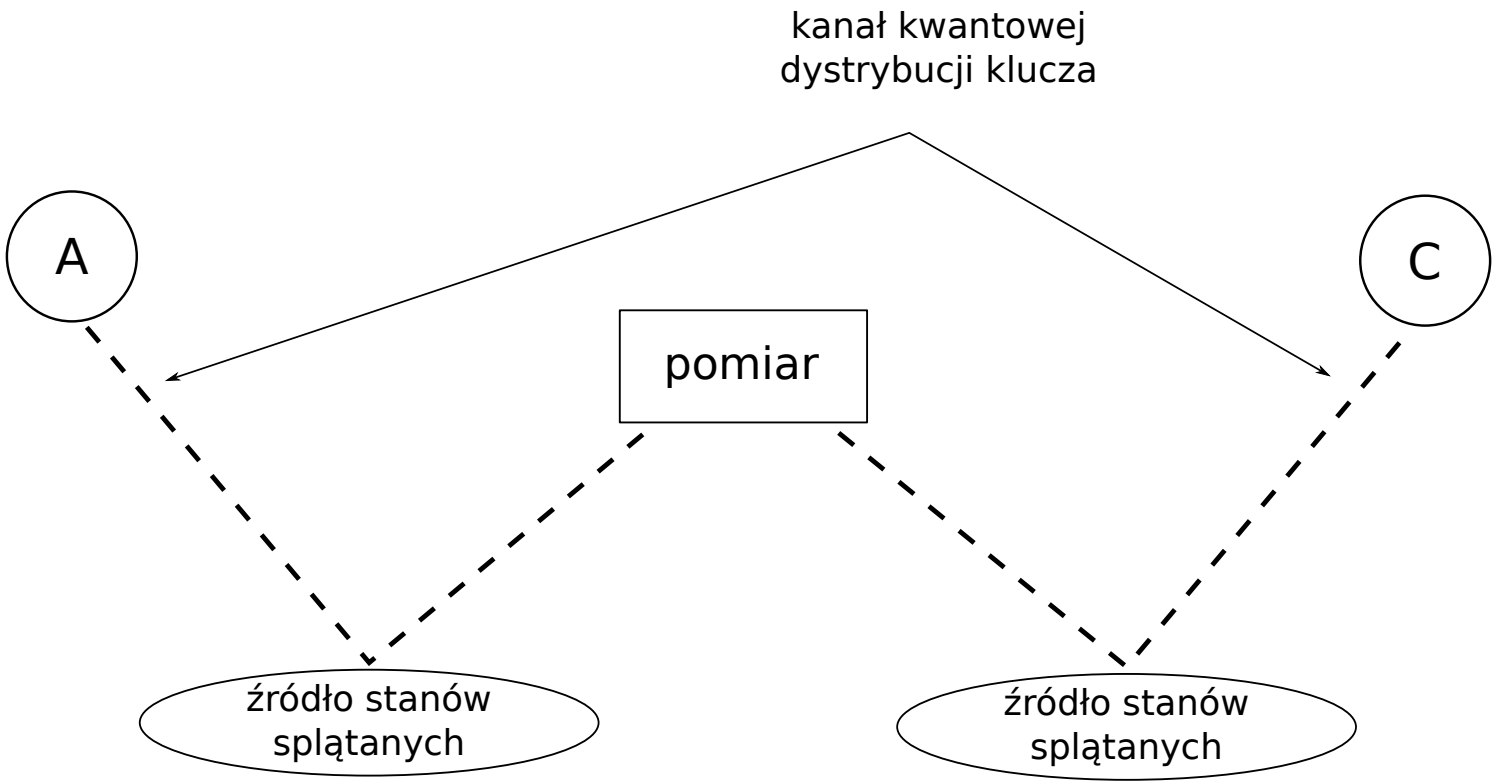
Przykład: kwantowa dystrybucja klucza

Współdzielenie stanów splatanych pozwala na utworzenie kanału kwantowej dystrybucji klucza.



Przykład: kwantowa dystrybucja klucza z powielaczem kwantowym

Zadaniem powielaczy kwantowych jest zwiększenie zasięgu łącza kwantowego.



Powielacze kwantowe

Zalety i wyzwania związane ze stosowaniem powielaczy kwantowych:

- pozwalają na podzielenie długich łączy na krótsze,
- niezależnie tworzą i składują stany splątane,
- wykorzystują przenoszenie splątania (ang. *entanglement swapping*),
- przy tworzeniu złożonych sieci konieczna jest synchronizacja i zarządzanie powielaczami,
- błędy w działaniu mogą mieć duży wpływ na wydajność transmisji.

Interfejsy i pamięci kwantowe

W sieciach klasycznych sygnał świetlny jest tłumaczony na impulsy elektryczne. Przejście takie nie jest możliwe w przypadku kwantowym – konieczne jest przeniesienie stanu kwantowego.

Użycie pamięci kwantowych wymaga

- opracowania metod tłumaczenia stanu z nośnika informacji kwantowej na pamięć kwantową,
- określenia ile pamięci jest potrzebne w implementacji danego protokołu/algorytmu,
- oszacowania czy użycie pamięci lub zwiększenie jej ilości poprawi wydajność pracy sieci.

Rutery kwantowe

W sytuacji gdy konieczne jest połączenie dwóch niezależnych podsieci, pojawia się problem trasowania stanów między nimi.

- Rutery kwantowe mają za zadanie wydajne przesyłanie informacji między podsieciami.
- W zależności od typu komunikacji, konieczne jest opracowanie różnych metod trasowania stanów.

Modele intersieci kwantowych

Uwzględnienie działania poszczególnych (wyidealizowanych) składników intersieci kwantowej pozwoli na zaplanowanie strategii działania w takiej sieci:

- ocena wydajności sieci z uwzględnieniem przesyłu danych klasycznych i kwantowych,
- wykrywanie wąskich gardeł – np. niewystarczająca pojemność pamięci,
- przygotowanie i modelowanie wykonania algorytmów rozproszonych – ocena efektywności, opracowanie i testowanie nowych algorytmów.

Modele intersieci kwantowych

Wykorzystanie modeli teoretycznych pozwala na optymalizację (oraz planowanie) realizacji fizycznych

- zaplanowanie topologii sieci,
- optymalizacja wykorzystania pamięci kwantowej,
- wykorzystanie klasycznych i kwantowych kanałów do optymalizacji protokołów – np. czy opłacalne jest wykorzystanie gęstego kodowania do przesyłania informacji klasycznej.

Dziękuję za uwagę!