STUDIA INFORMATICA 2003
Volume 24 Number 2A (53)

Jarosław A. MISZCZAK
Instytut Informatyki Teoretycznej i Stosowanej PAN

MOŻLIWOŚCI PRZESYŁANIA INFORMACJI W SIECIACH Z WYKORZYSTANIEM EFEKTÓW KWANTOWYCH[1]

Streszczenie. Mechanika kwantowa umożliwia przesyłania informacji w sposób niemożliwy w modelu klasycznym. Przykładami wykorzystania efektów kwantowych jest teleportacja kwantowa oraz gęste kodowanie. Kwantowy charakter kanałów informacyjnych może także zapewnić bezpieczny przesył poufnych informacji.

Słowa kluczowe: splątanie, teleportacja, gęste kodowanie.

POSSIBILITIES OF TRANSMISSION IN NETWORKS WITH UTILIZATION OF THE QUANTUM EFFECTS

Summary. Quantum mechanics allows faster and more efficient communication that it is possible in the classical model. Two most important examples of quantum effects, which can be used in computer networks, are: quantum teleportation and dense coding. Quantum channels can also be applied to secure communication.

Keywords: entanglement, teleportation, dense coding.

1. Kanały kwantowe

Mechanika kwantowa w połączeniu z informatyką dały początek nowej gałęzi wiedzy nazwanej kwantową teorią informacji (ang. *quantum information theory*) [4,10,12,15]. Dwa najważniejsze aspekty tej teorii to obliczenia kwantowe i kwantowe przesyłanie informacji. Oba te podejścia można do pewnego stopnia połączyć, gdyż u ich podstaw leży ten sam formalizm matematyczny. Jest to szczególnie ważne z punktu widzenia złożoności przeprowadzanych operacji [6] oraz możliwości ponownego wykorzystania wyspecjalizowanej aparatu-

[1] Praca wykonana w ramach projektu KBN nr 7 T11C 017 21.

ry – np. urządzenia optyczne służące do symulacji obliczeń kwantowych mogą służyć do eksperymentów związanych z kwantowym przesyłaniem informacji.

Efekty kwantowe można wprowadzić także do rozważań dotyczących teorii gier i analizy rynku finansowego w ekonomii [16].

Różnice w przesyłaniu informacji droga klasyczną i kwantową wynikają z różnic w sposobie opisu mediów, którymi posługujemy się w tych przypadkach.

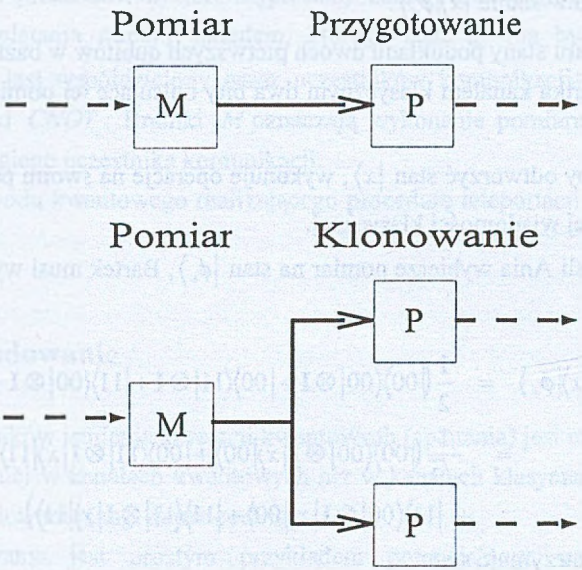
W odróżnieniu od kanałów klasycznych – tj. wykorzystujących jedynie media będące układami klasycznymi, czy też przesyłające informację zakodowaną symbolami alfabety klasycznego[2] – kanały wykorzystujące układy kwantowe nazywamy kanałami kwantowymi. Należy zaznaczyć, iż różnica tkwi tutaj w opisie, a nie w naturze fizycznej zjawiska. Stosowane obecnie technologie przesyłania informacji przy wykorzystaniu fotonów i elektronów nie operują na kwantowych własnościach tych obiektów.

Informacja w kanałach kwantowych może być zapisana za pomocą układów reprezentujących poprzez swój stan dowolny symbol będący superpozycją symboli klasycznych – wykorzystując alfabet kwantowy możemy zapisać symbole postaci $a0 + b1$. Układ odpowiadający klasycznemu bitowi to qubit.

Informacja kwantowa – czyli zapisana w postaci stanu układu kwantowego – jest nowym rodzajem informacji. Oznacza to, że nie ma możliwości dokonania teleportacja klasycznej – przesyłu informacji pomiędzy układami kwantowymi jedynie z wykorzystaniem kanałów klasycznych [12]. Możliwe jest natomiast przesyłanie stanów układów kwantowych, jeżeli zaangażowany jest w to kanał kwantowy – takie zjawisko nazywamy teleportacją kwantową.

Pewnym sposobem wyrażenia zależności między informacją klasyczną a kwantową jest zilustrowanie jej za pomocą konstrukcji maszyn realizujących przesyłanie informacji pomiędzy kanałami klasycznymi i kwantowymi. Rysunek 1 obrazuje dwie takie konstrukcje. Kanał kwantowy zaznaczony jest linią przerywaną, natomiast kanał klasyczny linią ciągłą. Możliwość konstrukcji urządzenia dokonującego przygotowania stanu kwantowego z informacji przesłanej do niego kanałem kwantowym (górna część rysunku) pozwala na sformułowanie zadania teleportacji klasycznej, co implikuje możliwość dokonania klonowania (dolna część rysunku). To zaś jest sprzeczne z obowiązującym w mechanice kwantowej twierdzeniem o nie-klonowaniu [1].

[2] Alfabetem klasycznym jest przykładowo zbiór $\{0,1\}$. System klasyczny może być opisany jednym z tych stanów lub może być opisany poprzez prawdopodobieństwo, iż jest w jednym z tych stanów.



Rys. 1. Teleportacja klasyczna i klonowanie
Fig. 1. Classical teleportation and cloning

Najciekawszym efektem kwantowym nie spotykanym w modelu klasycznym jest splątanie. Stany splątane odpowiadają rodzajowi korelacji wyników pomiarów, który nie ma odpowiednika w korelacjach obserwowanych w układach klasycznych. Stany te są znane w fizyce niemal od początku istnienia mechaniki kwantowej. Natomiast pierwsze eksperymentalne realizacje stanów zostały wykonane w latach siedemdziesiątych XX wieku.

Rozwój informatyki kwantowej spowodował wzrost zainteresowania stanami splątanymi, gdyż okazało się, iż splątanie jest odpowiedzialne między innymi za wykładnicze przyśpieszenie uzyskiwane przez algorytmy kwantowe.

2. Teleportacja stanów

Teleportacja kwantowa (ang. *quantum enhanced teleportation*) polega na możliwości przesłania informacji na temat stanu kwantowego z użyciem stanu splątanego i kanału klasycznego. Splątanie jest elementem koniecznym – teleportacja klasyczna, polegająca na przesyłaniu stanu tylko z wykorzystaniem kanału klasycznego, jest niemożliwa, gdyż wymaga odtworzenia stanu kwantowego jedynie z informacji klasycznej.

Załóżmy, ze Ania i Bartek mają do dyspozycji stan splątany $|\phi_+\rangle$. Aby przesłać dokładną kopie stanu $|x\rangle = a|0\rangle + b|1\rangle$, Ania musi wykonać następujące kroki:

1. Utworzyć układ w stanie $|x\rangle|\phi_+\rangle$.

2. Dokonać pomiaru stany podukładu dwóch pierwszych qubitów w bazie.

3. Przesłać do Bartka kanałem klasycznym dwa bity opisujące jej pomiar poprzez numer wektora bazowego.

Z kolei Bartek, aby odtworzyć stan $|x\rangle$, wykonuje operacje na swoim podukładzie, w zależności od otrzymanej wiadomości klasycznej.

Przykładowo, jeżeli Ania wybierze pomiar na stan $|\phi_+\rangle$, Bartek musi wykonać następujący ciąg operacji:

$$= \frac{1}{2}\left(|00\rangle\langle 00|\otimes \mathbf{I} + |00\rangle\langle 11|\otimes \mathbf{I} + |11\rangle\langle 00|\otimes \mathbf{I} + |11\rangle\langle 11|\otimes \mathbf{I}\right)|\phi_+\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|00\rangle\langle 00|\otimes \mathbf{I}|x\rangle|00\rangle + |00\rangle\langle 11|\otimes \mathbf{I}|x\rangle|11\rangle\right.$$

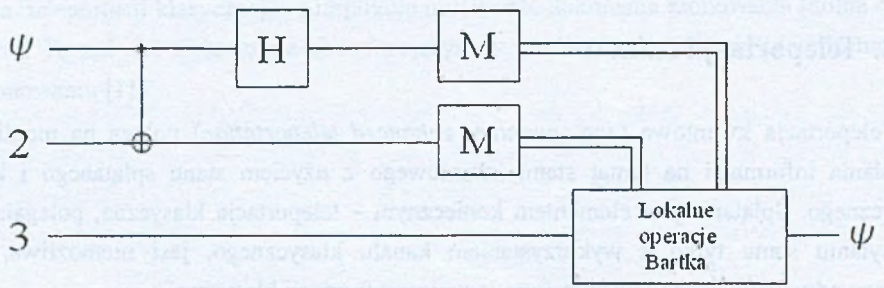
$$\left. + |11\rangle\langle 00|\otimes \mathbf{I}|x\rangle|00\rangle + |11\rangle\langle 11|\otimes \mathbf{I}|x\rangle|11\rangle\right).$$

W ten sposób Bartek otrzymuje stan:

$$\frac{1}{2\sqrt{2}}\left(\beta|001\rangle + \alpha|001\rangle + \alpha|110\rangle + \beta|111\rangle\right) = \frac{1}{2\sqrt{2}}\left(|00\rangle|x\rangle + |11\rangle|x\rangle\right),$$

czyli stan $|x\rangle$ zostanie przeniesiony do rejestru po stronie Bartka.

Wykonanie teleportacji jest zatem pewnego rodzaju obliczeniem kwantowym i może zostać zobrazowane za pomocą obwodu kwantowego. Elementem różniącym komunikację od obliczeń jest konieczność wykonania w pewnym kroku protokołu pomiaru stanu jednej z części układu (kanału). Pomiar jest dopuszczalną operacją podczas obliczenia kwantowego, ale zawsze można go dokonać dopiero w ostatnim kroku algorytmu. Tutaj natomiast jest on konieczny do realizacji protokołu, bowiem bez informacji od Ani, Bartek nie jest w stanie odtworzyć stanu, który ma być przeniesiony.



Rys. 2. Obwód kwantowy wykonujący procedurę teleportacji
Fig. 2. Quantum gate array for teleportation procedure

Na rysunku 2 przedstawiony jest najprostszy układ realizujący procedurę teleportacji. Wprowadzenie splątania między układem, którego stan ψ ma być przeteleportowany, a układem, który jest współdzielony przez uczestników komunikacji, odbywa się poprzez wykonanie bramki *CNOT*. Bramki *M* oznaczają wykonanie pomiaru, którego wynik jest przesyłany do drugiego uczestnika komunikacji.

Przykład obwodu kwantowego realizującego procedurę teleportacji można znaleźć także w [8].

3. Gęste kodowanie

Jednym z wyników istnienia korelacji kwantowych (splątania) jest możliwość przesyłania informacji wydajniej w kanałach kwantowych niż w kanałach klasycznych. Efekt ten znany jest jako gęste kodowanie (ang. *dense coding*).

Gęste kodowanie jest prostym przykładem potencjalnego wykorzystania stanów splątanych do przesyłania informacji. W tym wypadku splątanie pozwala na wydajniejsze kodowanie symboli podczas przesyłania informacji.

Załóżmy, że Ania i Bartek mają do dyspozycji stan splątany $|\phi_+\rangle$. Ania może wykonać na swoim podukładzie jedną z operacji unitarnych reprezentowanych przez macierze Pauliego: $\mathrm{I}, \sigma_x, \sigma_y$ bądź σ_z, odpowiadające w realizacji fizycznej np. elementom optycznym lub impulsom pola elektromagnetycznego. Powoduje to odpowiednio przejście w jeden ze stanów:

1. $|\phi_+\rangle = \mathrm{I} \otimes \mathrm{I}|\phi_+\rangle$
2. $|\psi_+\rangle = \sigma_x \otimes \mathrm{I}|\phi_+\rangle$
3. $|\psi_-\rangle = \sigma_y \otimes \mathrm{I}|\phi_+\rangle$
4. $|\phi_-\rangle = \sigma_z \otimes \mathrm{I}|\phi_+\rangle$

Każdy z nich może być rozpoznany jednoznacznie poprzez pomiar w bazie Bella $\{|\phi_\pm\rangle, |\psi_\pm\rangle\}$.

Zatem jeżeli teraz Bartek dokona pomiaru stanu układu powstałego z połączenia jego części i części, którą otrzymał od Ani w bazie $\{|\phi_\pm\rangle, |\psi_\pm\rangle\}$, jednoznacznie rozróżni operację, jaką wykonała Ania. Zatem przesłanie od Ani do Bartka jednego qubitu umożliwia przesłanie dwóch bitów informacji. Cała informacji jest tu zawarta w korelacjach pomiędzy stanami qubitów Ani i Bartka.

W przypadku klasycznym do przesłania dwóch bitów konieczne jest operowanie na dwóch układach – tutaj wystarczy operować na jednym z układów.

Teleportacja i gęste kodowanie są wzajemnie dopełniającymi się procedurami. W pierwszym przypadku korzystamy ze splątania do przenoszenia stanów przy wykorzystaniu informacji klasycznej, natomiast w drugim wykorzystujemy splątanie do przesyłania informacji klasycznej.

4. Możliwości wykorzystania

Kanały kwantowe mają kilka cech ograniczających ich potencjalne zastosowania praktyczne. Pierwszą z nich jest wrażliwość układów kwantowych na dekoherencję, czyli na utratę pod wpływem czynników zewnętrznych informacji zakodowanej w stanie cząstki. Wymaga to odseparowania nośników informacji kwantowej od środowiska[3].

Przeszkodą są także trudności w operowaniu stanem układów kwantowych, i co za tym idzie, trudności w uzyskiwaniu z dużą dokładnością określonego stanu.

Zaproponowany niedawno schemat teleportacji pomiędzy wieloma stronami [9] teoretycznie pozwala na rozszerzenie uzyskanych dotychczas efektów do komunikacji pomiędzy wieloma uczestnikami.

4.1. Systemy kryptograficzne

Pośrednie związki kwantowej teorii informacji z kryptografią wynikają z potencjalnej możliwości łamania niektórych szyfrów za pomocą maszyn kwantowych. Istnieje także możliwość bezpośredniego wykorzystania obwodów kwantowych do bezpiecznego przesyłania poufnych informacji. Wynikają one z niemożliwości uzyskania pełnej informacji o układzie poprzez wykonanie pojedynczego pomiaru lub z nielokalności stanów splątanych.

Splątanie, dzięki gęstemu kodowaniu, daje możliwości zupełnie odpornego na podsłuch przekazywania informacji. Gęste kodowanie pozwala na przesłanie informacji całkowicie poufnej, gdyż przesyłany qubit nie niesie informacji. Możliwe jest jedynie zakłócanie połączenia i tym samym zerwanie łączności pomiędzy stronami – unikamy jednak niebezpieczeństwa posługiwania się skompromitowanym kluczem.

4.2. Pamięci kwantowe

Możliwości wykorzystania teleportacji wynikają z potrzeb przetwarzania i przechowywania informacji kwantowej. Jednym z proponowanych zastosowań jest zapamiętywanie informacji przekazywanej kanałami kwantowymi – np. z wykorzystaniem fotonów – na trwałych nośnikach, takich jak spiny.

[3] Sytuacja ta dotyczy także obliczeń kwantowych.

Za pomocą teleportacji możliwe jest przenoszenie stanu z układu podlegającego szybkiej dekoherencji na układ trwały. Może mieć to zastosowanie do kumulacji danych w trakcie wykonania algorytmów kwantowych, a to można wykorzystać do zaoszczędzenia pamięci kwantowej.

Zastosowaniem teleportacji jest wykorzystywanie do kwantowej korekcji błędów występującej podczas obliczeń.

Przesyłanie informacji w sieciach lub układach opartych na nanotechnologiach może być wspierane efektami kwantowymi. Wynika to z konieczności operowania przy takich rozwiązaniach efektami w skali mikroskopowej.

Największe szanse na realizacje praktyczne mają systemy kwantowej dystrybucji klucza. Możliwość praktycznej realizacji kwantowego przesyłania informacji została potwierdzona poprzez wprowadzenie komercyjnych systemów przesyłania klucza z wykorzystaniem kanałów kwantowych. Kryptografia kwantowa może być wprowadzana jako uzupełnienie systemów symetrycznych takich, jak DES, IDEA czy AES. Ponieważ klucze używane w tych systemach mają zwykle długość nie większą niż 128 lub 256 bitów, nie jest konieczna wymiana dużej ilości informacji. W połączeniu z polityką kluczy jednorazowego użytku daje to bardzo bezpieczny system kryptograficzny.

4.3. Sieci czysto optyczne

Większość dotychczas przeprowadzonych doświadczeń związanych z występowaniem splątania dotyczyła fotonów. Pozwala to na powiązanie modelu sieci optycznych z efektami kwantowymi. Jest to sytuacja podobna jak w wypadku symulacji optycznych algorytmów kwantowych [6].

Jedną z trudności pojawiających się tutaj jest wrażliwość kanałów kwantowych na zakłócenia. Konieczne jest zatem wprowadzenie metod korekcji błędów powstałych podczas transmisji. Wiąże się to z małą przepustowością kanałów kwantowych – odpowiednia ilość transmisji np. pojedynczego fotonu jest z jednej strony konieczna do zapewnienia bezpieczeństwa przesyłania informacji, a z drugiej strony musimy uwzględnić szumy zakłócające i zniekształcające transmisję.

Do operowania na stanach splątanych przy przesyłaniu danych konieczne jest także wydajne źródło splątanych fotonów. Metody uzyskiwania takich źródeł omówione są w [3].

5. Podsumowanie

Rozwój komunikacji opartej na systemach kwantowych będzie dotyczył zapewne w pierwszym rzędzie systemów dystrybucji klucza. Systemy te mogą być zrealizowana z wykorzystaniem dostępnych dzisiaj technologii.

Natomiast realizacja metod wykorzystujących splątanie jest uzależniona od stopnia opanowania metod przetwarzania układów kwantowych. Podobnie sytuacja ma się z realizacją obliczeń kwantowych, gdzie konieczne jest operowania z dużą precyzją na układach mikroskopowych.

LITERATURA

1. Ballentiene L. E.: Quantum mechanics. A modern development, World Scientific, 2002.
2. Bennett C. H., Wiesner S. J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. 69, 20, 2881-2884 (1992).
3. Bouwmaster D., Ekert A., Zeilinger A.: The physics of quantum computation. Springer, 2000.
4. Bugajski S., Klamka J., Węgrzyn S.: Foundations of quantum computing. Part I, Archiwum Informatyki Teoretycznej i Stosowanej. 13, 2001, pp. 97-142.
5. Cerf N. J., Adami C., Kwiat P. G.: Optical Simulations of Quantum Logic. Phys. Rev. A 57, R1477 (1998).
6. Cleve R.: An Introduction to Quantum Complexity Theory. arXiv:quant-ph/9906111
7. Deutsch D. A., Ekert K.: Quantum communication moves into the unknown, Phys. World 6, 6, 22-23 (1993). http://www.consciousness.arizona.edu/quantum/qc4.htm.
8. Touchette H., Dumais P.: The quantum computation package for *Mathematica* 4.0. http://crypto.cs.mcgill.ca/QuCalc/.
9. Grudka, A.: Quantum teleportation between multiparties. arXiv:quant-ph/0303112
10. Hirvensalo M.: Quantum Computing. Springer-Verlag, 2001.
11. ID Quantique, Strona internetowa: http://www.idquantique.com/qkd.html.
12. Keyl, M.: Fundamentals of Quantum Information Theory, Physical Reports, 369, 5, (2002), arXiv:quant-ph/0202122.
13. MagiQ Technologies, Strona internetowa: http://www.magiqtech.com/.
14. Mosca, M.: Quantum Computer Algorithms, Praca doktorska dostępna na stronie http://www.cacr.math.uwaterloo.ca/~mosca/, 1999.
15. Nielsen M. A., Chuang, I. L.: Quantum Computation and Quantum Information. Cambridge University Press, 2002.

16. Piotrowski, E. W., Sladkowski, J.: An invitation to Quantum Game Theory, arXiv:quant-ph/0211191.

Recenzent: Prof. dr hab. inż. Jerzy Klamka

Wpłynęło do Redakcji 31 marca 2003 r.

Abstract

Quantum mechanical concepts involved in information processing lead to new model of communication – quantum communication. Quantum effects can be utilized to improve communication security and capacity of channels. They also lead to completely new aspects of communication such as quantum teleportation and dense coding. From the quantum mechanical point of view the most important issue responsible for those is entanglement – a kind of correlation, which is absent in classical theory.

This article describes simple protocols for quantum teleportation and dense coding. Some possible future applications of those two effects are proposed.

Adres

Jarosław A. MISZCZAK: Instytut Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk, ul. Bałtycka 5, 44-100 Gliwice, miszczak@iitis.gliwice.pl.