Zagadnienia Szczegółowe Dyskusji Panelu Ekspertów

(21 grudnia 2011 IITiS PAN, Gliwice)

pt. „Perspektywy rozwoju systemów obliczeń kwantowych do roku 2025"

1 Perspektywy produkcji dużych pamięci kwantowych

1.1 Zastosowanie pamięci kwantowych do przechowywania danych

Pamięci kwantowe są ważnym elementem w systemach kwantowego przetwarzania informacji.
Są one wykorzystywane m.in.

- w sieciach kwantowych [H.J. Kimble, Nature 453, 1023 (2008)]
- jako element powielaczy kwantowych (ang. quantum reapeters)
- w kwantowym przetwarzaniu danych z wykorzystanie optyki liniowej [Knill, Laflamme and Milburn Nature (London) 409 46 (2001)].

1.2 Wykorzystanie pamięci w repeaterach kwantowych

Bezpośrednia dystrybucja stanów splątanych na duże odległości jest ograniczona ze względu na straty. Szansę na rozwiązanie tego problemu dają powielacze kwantowe.
Zasada działania powielaczy kwantowych:

- pozwalają na podzielenie długich łączy na krótsze,
- tworzą i składują stany splątanie niezależnie,
- wykorzystują przenoszenie splątania (ang. entanglement swapping).

Takie podejście wymaga pamięci kwantowych.

1.3 Technologie tworzenia pamięci kwantowych

Pamięci kwantowe wykorzystywane są do magazynowania ale nie do przetwarzani informacji kwantowej.
Takie pamięci mogą być zrealizowane na kilka sposobów:

- atomowe zespoły statystyczne (atomic ensembles),
- pułapkowane optycznie atomy (cavity QED),
- pamięci w ciele stałym (solid state devices).

2 Algorytmy kwantowe na ponad 50 qubitów

2.1 Problemy prawne stosowania algorytmów kwantowych

- Natura obliczeń kwantowych jest probabilistyczna, zatem czy wynik obliczeń kwantowych może być dowodem przed sądem?
- Ciekawym problemem prawnym jest to czy: jeżeli stworzymy superpozycję wszystkich możliwych dzieł np. obrazów, to czy twórca takiej superpozycji uzyskuje prawa autorskie do każdego z dzieł?
- Czy przepisy np. dotyczące konkurencji lub obrotu giełdowego, które zakazują wymiany informacji pomiędzy stronami powinny być rozszerzone o zakaz korzystania ze stanów splątanych?

2.2 Kwantowe języki programowania i kompilatory kwantowe

Wraz z powstawaniem koncepcji i pierwszych realizacji komputerów kwantowych powstają liczne kwantowe języki programowania. Jak do tej pory rozszerzają one podejście klasyczny do domeny kwantowej.
Dwa problemy wydają się być interesujące:

- Czy możliwe jest efektywne stworzenie klasycznego kompilatora dla komputera kwantowego?
- Jakie fundamentalne nowe cechy mogą posiadać kwantowe języki programowania?

2.3 Technologie skalowalnych obliczeń kwantowych

Proponowane układy do realizacji obliczeń kwantowych.

- pułapkowane jony,
- neutralne atomy, cząsteczki i jamy kwantowo elekotrodynamiczne,
- obwody nadprzewodzące,
- kropki kwantowe półprzewodnikowe,
- optyka liniowa,
- zanieczyszczenia spinowe w ciele stałym pojedyncze klastry molekularne.

3 Symulatory kwantowe: symulacja problemów naukowych

Symulatory kwantowe mogą być pierwszym zastosowaniem komputerów kwantowych, ponieważ umożliwią symulacje zjawisk, których symulacja na klasycznych komputerach jest niemożliwa. Symulator kwantowy to układ kwantowy, którego dynamika może być tak dobrana, że zachowuje się on tak jak inny układ fizyczny, którego zachowanie chcemy poznać.

2 Algorytmy kwantowe na ponad 50 qubitów

2.1 Problemy prawne stosowania algorytmów kwantowych

- Natura obliczeń kwantowych jest probabilistyczna, zatem czy wynik obliczeń kwantowych może być dowodem przed sądem?
- Ciekawym problemem prawnym jest to czy: jeżeli stworzymy superpozycję wszystkich możliwych dzieł np. obrazów, to czy twórca takiej superpozycji uzyskuje prawa autorskie do każdego z dzieł?
- Czy przepisy np. dotyczące konkurencji lub obrotu giełdowego, które zakazują wymiany informacji pomiędzy stronami powinny być rozszerzone o zakaz korzystania ze stanów splątanych?

2.2 Kwantowe języki programowania i kompilatory kwantowe

Wraz z powstawaniem koncepcji i pierwszych realizacji komputerów kwantowych powstają liczne kwantowe języki programowania. Jak do tej pory rozszerzają one podejście klasyczny do domeny kwantowej.
Dwa problemy wydają się być interesujące:

- Czy możliwe jest efektywne stworzenie klasycznego kompilatora dla komputera kwantowego?
- Jakie fundamentalne nowe cechy mogą posiadać kwantowe języki programowania?

2.3 Technologie skalowalnych obliczeń kwantowych

Proponowane układy do realizacji obliczeń kwantowych.

- pułapkowane jony,
- neutralne atomy, cząsteczki i jamy kwantowo elekotrodynamiczne,
- obwody nadprzewodzące,
- kropki kwantowe półprzewodnikowe,
- optyka liniowa,
- zanieczyszczenia spinowe w ciele stałym pojedyncze klastry molekularne.

3 Symulatory kwantowe: symulacja problemów naukowych

Symulatory kwantowe mogą być pierwszym zastosowaniem komputerów kwantowych, ponieważ umożliwią symulacje zjawisk, których symulacja na klasycznych komputerach jest niemożliwa. Symulator kwantowy to układ kwantowy, którego dynamika może być tak dobrana, że zachowuje się on tak jak inny układ fizyczny, którego zachowanie chcemy poznać.

- osłabienie sygnału na łączu do satelity jest porównywalne z osłabieniem na odległości 5-8 km przy łączności w obrębie atmosfery,
- wykorzystanie łączy satelitarnych pozwala na dystrybucję stanów splątanych na bardzo duże odległości.

5.2 Zastosowanie kodowania super-gęstego do przesyłania informacji klasycznej

Gęste kodowanie pozwala na poprawę wydajność transmisji klasycznej poprzez transmisję informacji kwantowej.

- wykorzystanie gęstego kodowani pozwala na znaczną poprawę wydajności protokołów klasycznych
- rozwój sieci kwantowych wymaga rozwoju nowych protokołów kwantowych.

6 Kryptografia kwantowa

Najważniejszą cechą komputerów kwantowych jest możliwość efektywnego wykonania na nich faktoryzacji liczb naturalnych. Powstanie komputerów kwantowych spowoduje, iż część z powszechnie używanych systemów kryptograficznych przestanie być bezpieczna.
Rozwiązaniem, które jest już dostępne komercyjnie, może być Kwantowa Dystrybucja Klucza – protokół Benetta i Brassarda – który umożliwia ustalenie pomiędzy dwiema współpracującymi stronami wspólnego tajnego klucza. Protokół zapewnia, iż każda próba odkrycia, nawet części klucza, przez trzecią stronę będzie możliwa do wykrycia z dużym prawdopodobieństwem.

6.1 Łącza typu punkt – punkt

Dostępne na rynku rozwiązanie umożliwia ustalenie klucza pomiędzy dwiema stronami połączonymi ze sobą bezpośrednio światłowodem. Aby system mógł być wykorzystywany powszechnie, niezbędną funkcjonalnością jest możliwość zestawienia połączenia oraz uruchomienia protokołu na dowolnych dwóch węzłach w sieci.

6.2 Kryptografia kwantowa na zmiennych ciągłych

W ostatnich latach kwantowa teoria informacji rozważana jest na zmiennych ciągłych, czyli w nieskończenie wymiarowych przestrzeniach Hilberta.
Rozważane były przede wszystkim modele bozonowe – ze statystykami Gaussowskimi, ponieważ są dostępne eksperymentalnie oraz mają względnie prosty opis matematyczny.
Powstały uogólnienia protokołu Kwantowej Dystrybucji Klucza na zmienne ciągłe oraz protokoły wykorzystujące stany koherentne.

7 Wielowęzłowe sieci kwantowe

7.1 Interfejsy kwantowe

Zadaniem interfejsów kwantowych jest umożliwienie łączenie podzespołów kwantowych w większe systemy.
Główne przesłanki motywujące rozwój interfejsów kwantowych

- do stworzenia dużego systemu kwantowego przetwarzania informacji konieczne jest łącznie nośników (fotonów) z procesorami i pamięciami (atomami, jonami),
- przyszłe realizacje obliczeń kwantowych bedą wykorzystywały różnego rodzaju zjawiska fizyczne.

7.2 Zastosowanie infrastruktury sieci czysto optycznych do komunikacji kwantowej

Rozwój sieci czysto optycznych pozwala na ich wykozrsytanie do kwantowego przesyłania informacji
Zalety sieci czysto optycznych:

- przełanczanie i trasowanie sygnału na poziomie optycznym,
- między dwomo dowolnymi węzłami sieci może być zestawione łącze optyczne.

8 Realizacja nowych protokołów kwantowych

8.1 Perspektywy realizacji aukcji kwantowych

Aukcje kwantowe są relatywnie nową klasą algorytmów kwantowych obejmujących:

- Aukcje z zamkniętymi ofertami, w których np. tylko oferta wygrywająca jest znana.
- Aukcje kombinatoryczne.

8.2 Gry kwantowe — perspektywy wdrożenia

Prace wielu badaczy wykazały, że pozwolenie graczom na korzystanie z praw mechaniki kwantowej podczas wyboru strategii wielu gier, pozwala na osiągnięcie wyników znacząco różnych od klasycznych. Możliwość wykorzystania gier kwantowych do problemów rzeczywistych nie jest jasna, ale za to stworzenie „kwantowego kasyna", może być atrakcyjne dla szerokiego grona klientów.
Już teraz urządzenia generujące liczby losowe z wykorzystaniem praw mechaniki kwantowej są masowo kupowane przez internetowe kasyna.

8.3 Rozproszone kwantowe problemy decyzyjne w sytuacjach konfrontacyjnych i kooperacyjnych

Rozwój sieci kwantowych oraz osiągnięcia teoretyczne w zakresie kwantowej teorii gier pozwalają podejrzewać, że zostaną podjęte próby wykorzystania kwantowych protokołów

decyzyjnych do koordynacji działań stron, szczególnie kiedy przekazywanie informacji pomiędzy będzie niemożliwe np. z powodów prawnych.

8.4 Prognozowanie kwantowe

Liniowy charakter mechaniki kwantowej utrudnia modelowanie procesów nieliniowych, jakimi są procesy społeczno-gospodarcze. Ciekawe jest czy istnieje możliwość efektywnej symulacji procesów nieliniowych przez komputery kwantowe.

9 Perspektywy komercyjnego wdrożenia algorytmów kwantowych

9.1 Jakie algorytmy kwantowe gdzie mogą znaleźć zastosowanie

Jednym z głównych problemów w doprowadzeniu do powszechnego użycia komputerów kwantowych jest fakt, iż nie jest jasne jakie zastosowania komercyjne zostaną dla nich znalezione.

- Kwantowy algorytm wyszukiwania nie daje zbyt dużego przyspieszenia kwantowego, ale w połączeniu z kwantowym błądzeniem losowym może być relatywnie prosty do realizacji.
- Algorytm faktoryzacji liczb będzie miał głównie zastosowanie w kryptologii.
- Istnieje nadzieja na wykorzystanie algorytmów adiabatycznych do analizy rozległych grafów w stylu algorytmu PageRank.

10 Spin-off w innych dziedzinach nauki i techniki

10.1 Obliczenia kwantowe, a fundamentalne problemy nauki

Czy badania nad kwantową teorią informacji doprowadzą do rozwiązania problemu P =? NP.

Głównym problemem w dziedzinie informatyki jest przypuszczenie, że dwie klasy złożoności, P (czas wielomianowy) oraz NP (nie deterministyczny czas wielomianowy – problemy decyzyjne, dla których proponowane rozwiązanie może być sprawdzane w czasie wielomianowym), są różne w modelu obliczeń Turinga. W ogólności, można przyjąć, że dla każdej teorii fizycznej odpowiada pewien model obliczeniowy, którego moc jest ograniczona przez daną teorię fizyczną.

Pojawiają się przypuszczenia, iż nieabelowa kwantowa teoria pola może posiadać model obliczeniowy umożliwiający efektywne rozwiązanie problemów typu NP.

10.2 Obliczenia kwantowe, a fundamentalne problemy nauki

Czy dokładniejsze doświadczenia doprowadzą do stworzenia teorii post kwantowych? Temat do dyskusji.

10.3 Kwantowa metrologia - technologie i zastosowania

Mechanika kwantowa może zaoferować znaczne zwiększenie czułości instrumentów pomiarowych. Przykładem może być

- spektroskopia ultra wysokiej precyzji,
- synchronizacja zegarów przez użycie częstotliwościowo splątanych impulsów,
- zwiększenie dokładności zegarów przy użyciu splątania

Innym przykładem potencjalnych zastosowań jest obrazowanie kwantowe, gdzie splątanie wykorzystywane jest do zapisu, przetwarzania oraz przechowywania informacji dotyczącej punktów na obrazie optycznym. Ponadto techniki wywodzące się z teorii kwantów mogą poprawić czułość pomiarów obrazu poprzez zwiększenie rozdzielczości poza ograniczeni wynikające z długości fali świetlnej.

10.4 Perspektywy nowych odkryć w zakresie teorii kwantów i obliczeń kwantowych

- Nowe eksperymenty potwierdzające lub obalające mechanikę kwantową.
- Nowe materiały.
- Łamanie nierówności „silniejszych" niż nierówności Bella.