Gry kwantowe i programowanie komputerów kwantowych

Jarosław Miszczak

Instytut Informatyki Teoretycznej i Stosowanej PAN w Gliwicach

Perspektywy informatyki kwantowej
Wrocław, 25.IV.2008

Prace Zespołu Kwantowych Systemów Informatyki

Kwantowa teoria gier

- Dylemat więźnia
- Paradoks Parrondo
  - Wykorzystanie programowania kwantowego
- Gra w magiczne kwadraty

Rozróżnialność stanów i miary odległości

- Miary odległości między stanami
- Rozróżnialność stanów jako gra kwantowa
- Ograniczenia na fidelity

Podsumowanie

Projekt Quantiki

Prace Zespołu Kwantowych Systemów Informatyki

Skład: 2 pracowników + 2 doktorantów + 1 post-doc

Tematy:

- **Gry kwantowe:** Badanie wpływy zasada mechaniki kwantowej na teorię gier oraz wykorzystanie teorii gier do opisu kwantowego przetwarzania informacji.

Prace Zespołu Kwantowych Systemów Informatyki

Skład: 2 pracowników + 2 doktorantów + 1 post-doc

Tematy:

- **Gry kwantowe:** Badanie wpływy zasada mechaniki kwantowej na teorię gier oraz wykorzystanie teorii gier do opisu kwantowego przetwarzania informacji.
- **Kwantowe języki programowania:** Zastosowanie metod informatycznych (gramatyki formalne) do opisu algorytmów i protokołów kwantowych.

Prace Zespołu Kwantowych Systemów Informatyki

Skład: 2 pracowników + 2 doktorantów + 1 post-doc

Tematy:

- **Gry kwantowe:** Badanie wpływy zasada mechaniki kwantowej na teorię gier oraz wykorzystanie teorii gier do opisu kwantowego przetwarzania informacji.
- **Kwantowe języki programowania:** Zastosowanie metod informatycznych (gramatyki formalne) do opisu algorytmów i protokołów kwantowych.
- **Miary odległości między stanami:** Badanie fidelity, dyskryminacja stanów kwantowych.

Kwantowa teoria gier

Krótkie wprowadzenie

Teoria gier opisuje sytuacje współzawodnictwa z udziałem wielu agentów (graczy). Każdy gracz ma do dyspozycji określony zestaw ruchów i wie jaka jest funkcja wypłaty w zależności o wykonanych ruchów.

Kwantowa teoria gier

Krótkie wprowadzenie

Teoria gier opisuje sytuacje współzawodnictwa z udziałem wielu agentów (graczy). Każdy gracz ma do dyspozycji określony zestaw ruchów i wie jaka jest funkcja wypłaty w zależności o wykonanych ruchów.

Kwantowa teoria gier – podobnie jak teoria obliczeń kwantowych – uwzględnia w opis takich sytuacji fizyczny opis układu. Gracze mają do dyspozycji większy zbiór możliwych ruchów.

Kwantowa teoria gier

Wykorzystanie

Do czego przydatna jest kwantowa teoria gier?

[1] Du *et al.*, Phys. Rev. Lett. 88, 137902 (2002)

Kwantowa teoria gier

Wykorzystanie

Do czego przydatna jest kwantowa teoria gier?

- Daje przykłady pokazujące wpływ mechaniki kwantowej na algorytmy klasyczne – np. kwantowy dylemat więźnia, gra w magiczne kwadraty.

[1] Du *et al.*, Phys. Rev. Lett. 88, 137902 (2002)

Kwantowa teoria gier

Wykorzystanie

Do czego przydatna jest kwantowa teoria gier?

- Daje przykłady pokazujące wpływ mechaniki kwantowej na algorytmy klasyczne – np. kwantowy dylemat więźnia, gra w magiczne kwadraty.
- Umożliwia opis pewnych problemów typowych dla informatyki kwantowej – np. problem dyskryminacji stanów.

[1] Du *et al.*, Phys. Rev. Lett. 88, 137902 (2002)

Kwantowa teoria gier

Wykorzystanie

Do czego przydatna jest kwantowa teoria gier?

- Daje przykłady pokazujące wpływ mechaniki kwantowej na algorytmy klasyczne – np. kwantowy dylemat więźnia, gra w magiczne kwadraty.
- Umożliwia opis pewnych problemów typowych dla informatyki kwantowej – np. problem dyskryminacji stanów.
- Pozwala na zaproponowanie prostych scenariuszy do realizacji eksperymentalnych[1].

[1] Du *et al.*, Phys. Rev. Lett. 88, 137902 (2002)

Kwantowa teoria gier

Najprostszy przykład – dylemat więźnia

Dwóm osobom grozi kara wiezienia. Mogą one zmniejszyć swoje wyroki zeznając przeciwko sobie.

Kwantowa teoria gier

Najprostszy przykład – dylemat więźnia

Dwóm osobom grozi kara wiezienia. Mogą one zmniejszyć swoje wyroki zeznając przeciwko sobie.

- jeżeli jeden z nich poda dowód obciążający drugiego, to jego kara zostanie zmniejszona o 5 lat,
- jeżeli obaj podadzą dowody to ich kara zostanie zmniejszona o 1 rok,
- jeżeli żaden nie poda dowodu to ich kara zostanie zmniejszona o 3 lata.

	Bob: W	Bob: Z
Alicja: W	(3,3)	(0,5)
Alicja: Z	(5,0)	(1,1)

Kwantowa teoria gier

Najprostszy przykład – dylemat więźnia

W przypadku klasycznym nie jest możliwe wykonanie ruchu optymalnego dla obojga graczy jeżeli nie mają oni możliwości komunikowania się.

Średnio opłaca się podać dowody przeciwko współwięźniowi, ale nie jest to wybór optymalny.

	Bob: W	Bob: Z
Alicja: W	(3,3)	(0,5)
Alicja: Z	(5,0)	(1,1)

Kwantowa teoria gier

Kwantowy dylemat więźnia

Kwantowa wersja dylematu więźnia zezwala na wykonywanie ruchów opisanych macierzami unitarnymi. Gracze wpółdzielą też stan maksymalnie splątany.

Grając z wykorzystaniem stanów kwantowych gracze mogą uzyskać optymalny efekt. Rozwiązuje to klasyczny paradosk. Klasycznym ruchom odpowiadają macierze

$$W \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ oraz } Z \sim \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

[2] J. Eisert *et al* Phys. Rev. Lett., 83, 3077 (1999).

Kwantowa teoria gier

Kwantowy dylemat więźnia

Kwantowa wersja dylematu więźnia zezwala na wykonywanie ruchów opisanych macierzami unitarnymi. Gracze współdzielą też stan maksymalnie splątany.

Grając z wykorzystaniem stanów kwantowych gracze mogą uzyskać optymalny efekt. Rozwiązuje to klasyczny paradosk. Klasycznym ruchom odpowiadają macierze

$$W \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ oraz } Z \sim \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Optymalne posunięcie jest opisane macierzą[2]

$$Q = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

[2] J. Eisert *et al* Phys. Rev. Lett., 83, 3077 (1999).

Kwantowa teoria gier

Przykład: Paradoks Parrondo

Paradoks Parrondo to klasyczna gra jednoosobowa – celem jest zmaksymalizowanie zysku.

Gracz może w każdym kroku wykonać wybrać czy gra w grę **A** czy **B**. Gra **A** to rzut nieuczciwą monetą. Gra **B** to rzut jedną z monet $\mathbf{B}_1$ (wygrywającą) bądź $\mathbf{B}_2$ (przegrywającą) w zależności czy zgromadzona suma jest podzielna przez 3 czy nie.

Kwantowa teoria gier

Przykład: Paradoks Parrondo

Paradoks Parrondo to klasyczna gra jednoosobowa – celem jest zmaksymalizowanie zysku.

Gracz może w każdym kroku wykonać wybrać czy gra w grę **A** czy **B**. Gra **A** to rzut nieuczciwą monetą. Gra **B** to rzut jedną z monet $\mathbf{B}_1$ (wygrywającą) bądź $\mathbf{B}_2$ (przegrywającą) w zależności czy zgromadzona suma jest podzielna przez 3 czy nie.

Grając zawsze **A** bądź zawsze **B** gracz przegra.

Kwantowa teoria gier

Przykład: Paradoks Parrondo

Paradoks Parrondo to klasyczna gra jednoosobowa – celem jest zmaksymalizowanie zysku.

Gracz może w każdym kroku wykonać wybrać czy gra w grę **A** czy **B**. Gra **A** to rzut nieuczciwą monetą. Gra **B** to rzut jedną z monet $\mathbf{B}_1$ (wygrywającą) bądź $\mathbf{B}_2$ (przegrywającą) w zależności czy zgromadzona suma jest podzielna przez 3 czy nie.

Grając zawsze **A** bądź zawsze **B** gracz przegra.

Można tak dobrać strategię (ciąg gier **A** i **B**) aby uzyskać dodatnią wartość oczekiwaną wygranej.

Paradoks Parrondo

Algorytm Grovera

W przypadku algorytmu Grovera wykonywane są naprzemiennie dwie operacje – zaznaczenie i obrót wokół średniej. Każda z nich stosowana samodzielnie nie prowadzi do zwiększenia wybranej amplitudy.

Natomiast stosowane oddzielnie prowadzą do stanu w którym z dużym prawdopodobieństwem zmierzymy szukaną wartość.

Paradoks Parrondo

Wykorzystanie programowania kwantowego

W oryginalnej wersji paradosku gra **B** wymaga operacji mnożenia modulo. Wykonywanie operacji na liczbach zakodowanych w stanach jest kłopotliwe w modelu bramek kwantowych – konieczne jest wykonywanie operacji na pojedynczych qubitach.

Kwantowe języki programowania pozwalają na ominięcie pewnych ograniczeń modelu bramek kwantowych

- łatwiejszy opis działań na liczbach – gotowe funkcje do operacji na liczbach lub wbudowanie podstawowej arytmetyki w gramatykę języka.
- kontrolę nad wykonaniem programu kwantowego – kwantowe instrukcje warunkowe.

Paradoks Parrondo

Wykorzystanie programowania kwantowego

- Kwantową wersję paradoksu Parrondo można uzyskać wykorzystując wysokopoziomowy język programowania – np. QCL (Quantum Computation Language)[3].
- Zaletą tej realizacji jest złozoność pamięciowa $O(\log n)$, gdzie n to liczba wykonywanych kroków.
- Dodatkową zaletą jest możliwość symulacji gry Parrondo – QCL dostarcza wydajnego symulatora obliczeń kwantowych.

[3] P. Gawron, JM, Fluctuation and Noise Letters, Vol. 5, No. 4 (2005).

QCL (Quantum Computation Language)

QCL został opracowany i zaimplementowany przez B. Ömera[4].
Pozwala on na tworzenie programów w których obliczenia kwantowe są kontrolowane klasycznie.
Cechy języka

- znane z języka C konstrukcje warunkowe, pętle, funkcje...
- możliwość definiowania własnych operatorów,
- łatwość łączenia obliczeń klasycznych i kwantowych – do zapisu wykorzystywana jest jednolita składnia,
- kwantowe instrukcje warunkowe – uogólnienie operacji kontrolowanych.

[4] http://tph.tuwien.ac.at/~oemer/qcl.html

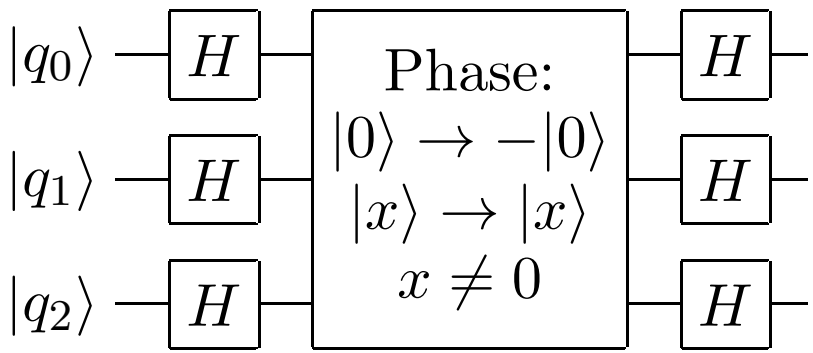
QCL (Quantum Computation Language)

Przykład

Algorytm Grover wykorzystuje tzw. operator obrotu wokół średniej.

$$D = 2|0\rangle\langle 0| - 1$$

która jest równoważna złożeniu dwóch bramek – H i kontrolowanej fazy.



QCL (Quantum Computation Language)

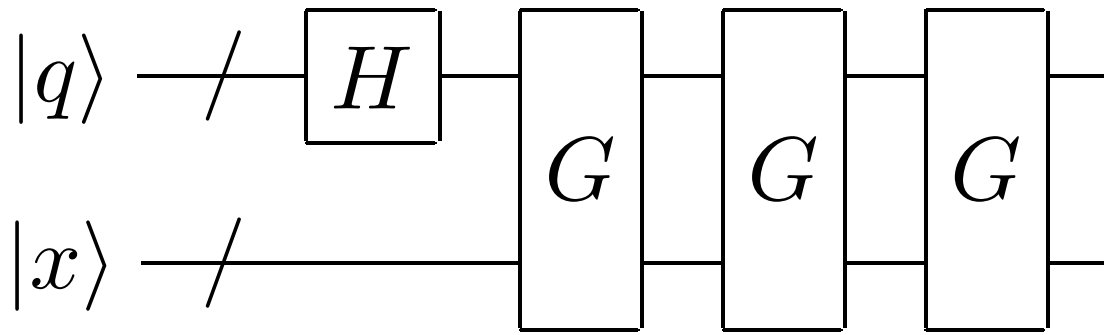
Przykład

W języku QCL operacja ta może być zapisana jako operator

```
operator diffuse(qureg q) {
  H(q);                    // operacja Hadamarda
  Not(q);                  // negacja
  CPhase(pi,q);            // obrót dla q=1111..
  !Not(q);                 // odwrotna negacja
  !H(q);                   // odwrotna operacja Hadamarda
}
```

QCL (Quantum Computation Language)

Przykład




```
for i=1 to ceil(sqrt(2^#q)) {
  query(q,f,n);
  CPhase(pi,f);
  !query(q,f,n);
  diffuse(q);
}
```

gdzie query implementuje wyrocznię stosowaną w algorytmie.

Gra w magiczne kwadraty

Zasady gry

Gra ta jest przykładem gry dwuosobowej. Alicja dostaje od arbitra numer wiersza, Bob dostaje numer kolumny. Ich zadaniem jest wypełnienie tablicy 3 na 3 liczbami 0 lub 1. Suma w wierszu musi być nieparzysta a w kolumnie parzysta. Alicja wypełnia wiersz a Bob kolumnę.

Gra w magiczne kwadraty

Zasady gry

Gra ta jest przykładem gry dwuosobowej. Alicja dostaje od arbitra numer wiersza, Bob dostaje numer kolumny. Ich zadaniem jest wypełnienie tablicy 3 na 3 liczbami 0 lub 1. Suma w wierszu musi być nieparzysta a w kolumnie parzysta. Alicja wypełnia wiersz a Bob kolumnę.

W przypadku klasycznym Alicja i Bob mogą tak uzgodnić ruchy przed rozpoczęcie m gry aby szansa wygranej wynosiła $\frac{8}{9}$.

Gra w magiczne kwadraty

Wersja kwantowa

Kwantowa wersja gry wymaga współdzielenia przez Alicje i Bob stanu czteroqubitowego. W zależności od otrzymanego numeru wiersza/kolumny Alicja i Bob wykonują jedną z operacji dwuqubitowych unitarnych opisanych w protokole[5] a następnie wykonują pomiar.

Współdzielenie stanu kwantowego pozwala im zawsze wygrać.

[5] G. Brassard *et al.*, Found. Phys. 35, 1877 (2005).

Gra w magiczne kwadraty

Wpływ szumów na wyniki gry

Cechy protokołu kwantowego

- pozwala pokazać jak splątanie wypływa na wyniki – współdzielenie stanu kwantowego daje lepsze wyniki niż najlepsza strategia klasyczna,
- gra jest bardzo wrażliwa na błędy kwantowe pojawiające się w trakcie przesyłania stanu – nawet przy małych zakłóceniach lepiej wybrać strategię klasyczną.

Miary odległości między stanami

Rozróżnialność stanów wynika z odległości między stanami.

- Odległość Buresa $D_B(A,B) = \sqrt{2-2\sqrt{F}}$ (oparta na fidelity $F(A,B) = [\mathrm{tr}|\sqrt{A}\sqrt{B}|]^2$)

[6] B.-G. Englert, Phys. Rev. Lett. 77, 2154 (1996).

Miary odległości między stanami

Rozróżnialność stanów wynika z odległości między stanami.

- Odległość Buresa $D_B(A,B) = \sqrt{2-2\sqrt{F}}$ (oparta na fidelity $F(A,B) = [\mathrm{tr}|\sqrt{A}\sqrt{B}|]^2$)
- Odległość śladowa $D_{\mathrm{tr}}(A,B) = \frac{1}{2}\mathrm{tr}|A-B|$ – określana także jako *rozróżnialność stanów*[6].

[6] B.-G. Englert, Phys. Rev. Lett. 77, 2154 (1996).

Miary odległości między stanami

Rozróżnialność stanów wynika z odległości między stanami.

- Odległość Buresa $D_B(A,B) = \sqrt{2-2\sqrt{F}}$ (oparta na fidelity $F(A,B) = [\mathrm{tr}|\sqrt{A}\sqrt{B}|]^2$)
- Odległość śladowa $D_{\mathrm{tr}}(A,B) = \frac{1}{2}\mathrm{tr}|A-B|$ – określana także jako *rozróżnialność stanów*[6].

Wielkości te są powiązane nierównością

$$1-\sqrt{F} \leq D_{\mathrm{tr}} \leq \sqrt{1-F}$$

[6] B.-G. Englert, Phys. Rev. Lett. 77, 2154 (1996).

Rozróżnialność stanów

Dany jest zbiór stanów kwantowych.

Zadanie: Naszym zadaniem jest określenie który z tych stanów mamy w swoim posiadaniu.

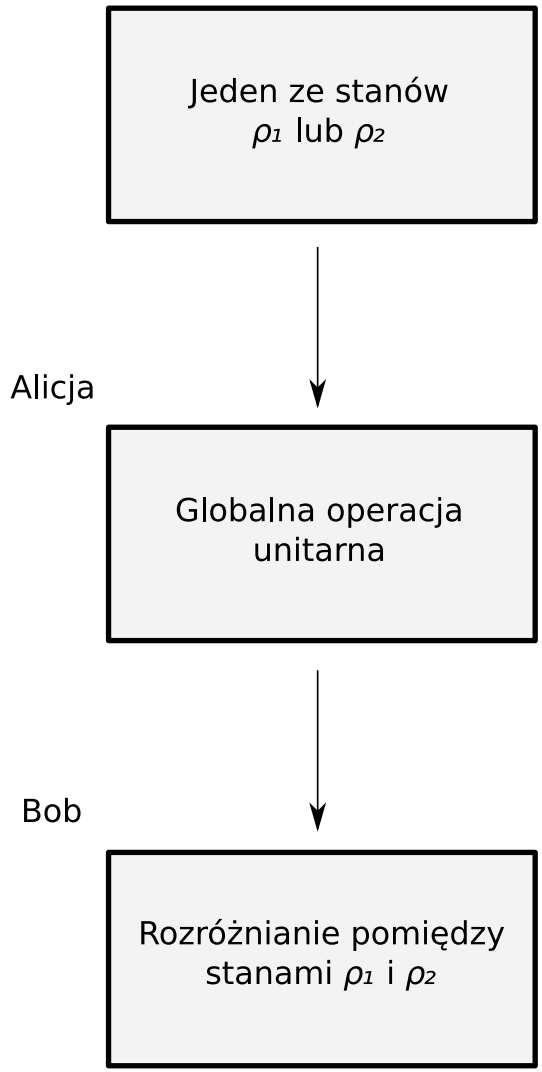
Utrudnienie: Co się stanie jeżeli na stanach jest wykonywana jakaś operacja unitarnych.

Rozróżnialność stanów jako gra kwantowa

Rozróżnianie pomiędzy stanami kwantowymi może być opisane jako gra kwantowa.

Rozróżnialność stanów jako gra kwantowa

Rozróżnianie pomiędzy stanami kwantowymi może być opisane jako gra kwantowa.



Rozróżnialność stanów jako gra kwantowa

Alicja przeszkadzając Bobowi stara się zminimalizować odległość pomiędzy ρ_1 i ρ_2 poprzez wykonanie operacji unitarnych.

$$\min_{V,U} D_B(V\rho_1 V^\dagger, U\rho_2 U^\dagger) = D_B(p_i^\uparrow q_i^\uparrow)$$

Analogicznie minimum jest osiągane dla odległości śladowej[7].

[7] D. Markham, JM, Z. Puchala, K. Zyczkowski, Phys. Rev. A 77, 042111 (2008)

Rozróżnialność stanów jako gra kwantowa

Alicja przeszkadzając Bobowi stara się zminimalizować odległość pomiędzy ρ_1 i ρ_2 poprzez wykonanie operacji unitarnych.

$$\min_{V,U} D_B(V\rho_1 V^\dagger, U\rho_2 U^\dagger) = D_B(p_i^\uparrow q_i^\uparrow)$$

Analogicznie minimum jest osiągane dla odległości śladowej[7].

Zatem najlepsza strategia dla Alicji to wykonać operację unitarna która przeprowadza wekroty własne ρ_1 na wektory własne ρ_2 z uwzględnieniem uporządkowania wartości własnych.

[7] D. Markham, JM, Z. Puchala, K. Zyczkowski, Phys. Rev. A 77, 042111 (2008)

Rozróżnialność stanów jako gra kwantowa

Podobnie ograniczeni górne wynosi dla odległości Buresa

$$\max_{U,V} D_B(V\rho_1 V^\dagger, U\rho_2 U^\dagger) = D_B(p_i^\uparrow q_i^\downarrow)$$

oraz dla odległości śladowej

$$\max_{U,V} D_{\mathrm{tr}}(V\rho_1 V^\dagger, U\rho_2 U^\dagger) = \frac{1}{2}\sum_i |p_i^\uparrow - q_i^\downarrow|$$

Rozróżnialność stanów jako gra kwantowa

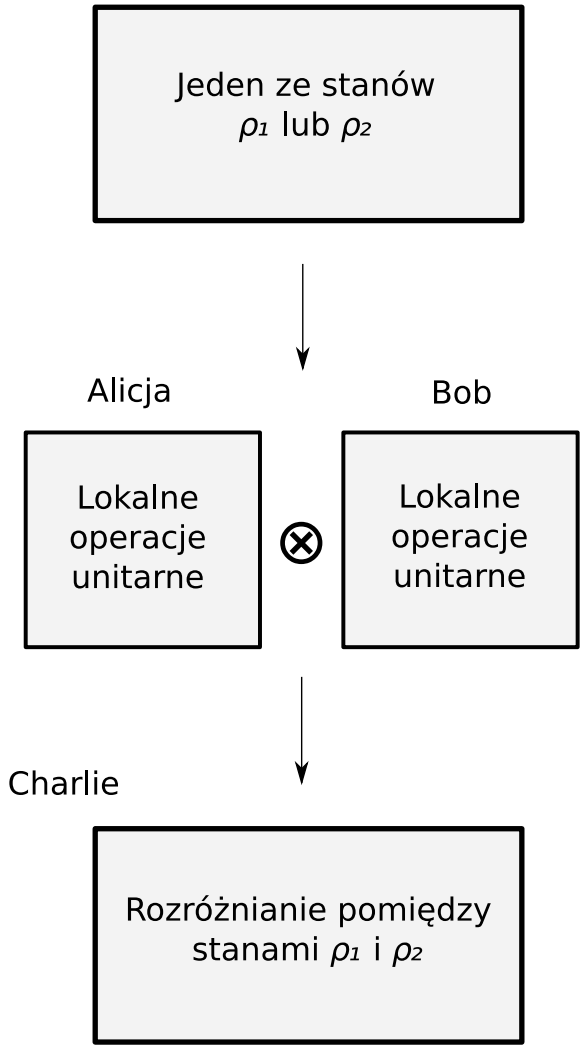
Wersja lokalna

Podobne pytanie można zadać w przypadku gdy Alicja i Bob grają przeciwko trzeciemu graczowi.

Rozróżnialność stanów jako gra kwantowa

Wersja lokalna

Podobne pytanie można zadać w przypadku gdy Alicja i Bob grają przeciwko trzeciemu graczowi.



Miary odległości między stanami

Alternatywne odległości

Problemem jest wyliczenie fidelity dla dowolnych macierzy gęstości – wymaga to znajomości spectrum operatorów. Można ją oszacować innymi wielkościami, które mogą być zmierzone w laboratorium[8].

[8] JM, Z. Puchała, P. Horodecki, A. Uhlmann, K. Życzkowski, *Sub– and super–fidelity as bounds for quantum fidelity*, w przygotowaniu

Miary odległości między stanami

Alternatywne odległości

Problemem jest wyliczenie fidelity dla dowolnych macierzy gęstości – wymaga to znajomości spectrum operatorów. Można ją oszacować innymi wielkościami, które mogą być zmierzone w laboratorium[8].

- super-fidelity $G(A,B) = \mathrm{tr}AB + \sqrt{(1-\mathrm{tr}A^2)(1-\mathrm{tr}B^2)}$
- sub-fidelity $E(A,B) = \mathrm{tr}AB + \sqrt{2(\mathrm{tr}AB\mathrm{tr}AB - \mathrm{tr}ABAB)}$

[8] JM, Z. Puchała, P. Horodecki, A. Uhlmann, K. Życzkowski, *Sub– and super–fidelity as bounds for quantum fidelity*, w przygotowaniu

Miary odległości między stanami

Alternatywne odległości

Problemem jest wyliczenie fidelity dla dowolnych macierzy gęstości – wymaga to znajomości spectrum operatorów. Można ją oszacować innymi wielkościami, które mogą być zmierzone w laboratorium[8].

- super-fidelity $G(A,B) = \mathrm{tr}AB + \sqrt{(1-\mathrm{tr}A^2)(1-\mathrm{tr}B^2)}$
- sub-fidelity $E(A,B) = \mathrm{tr}AB + \sqrt{2(\mathrm{tr}AB\mathrm{tr}AB - \mathrm{tr}ABAB)}$

Wielkości te powiązane są z fidelity nierównościami

$$E \leq F \leq G$$

a w przypadku jednoqubitowym

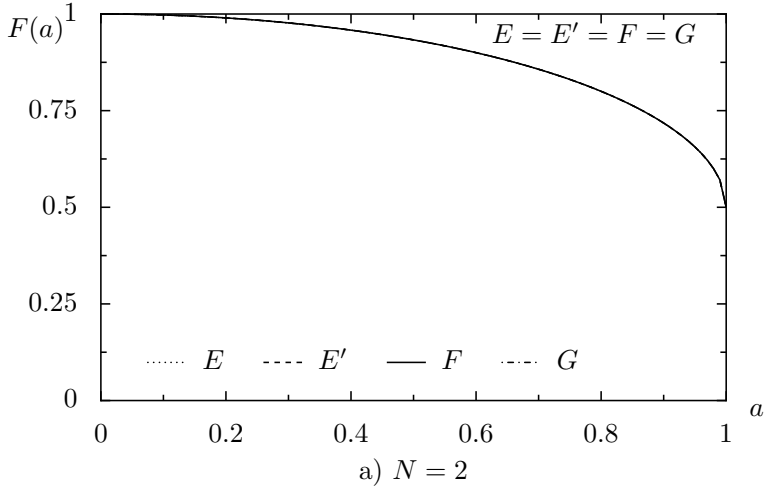
$$E = F = G$$

[8] JM, Z. Puchała, P. Horodecki, A. Uhlmann, K. Życzkowski, *Sub– and super–fidelity as bounds for quantum fidelity*, w przygotowaniu

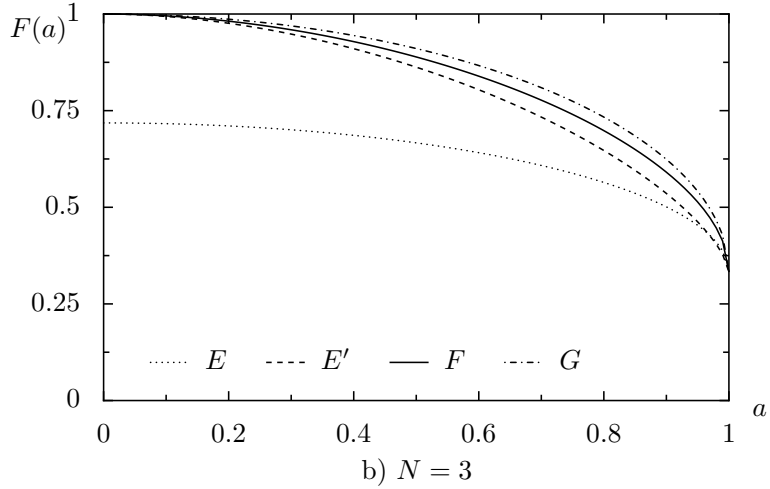
Miary odległości między stanami

Porównanie zachowania dla małych wymiarów

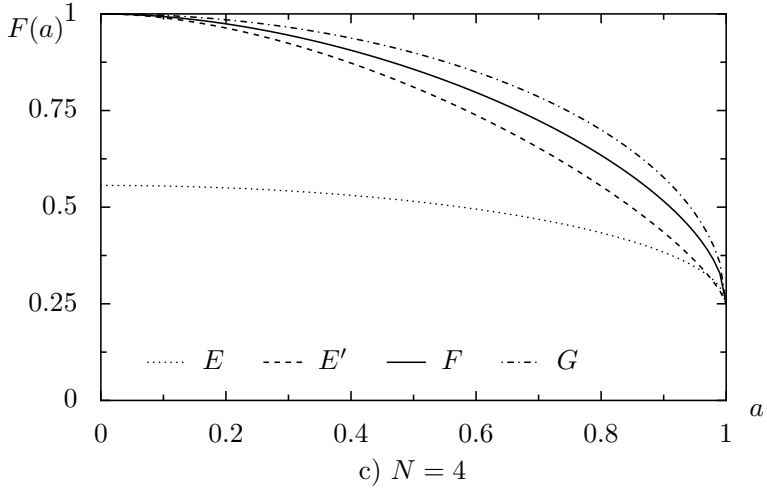
Ograniczenia dla fidelity w niskich wymiarach



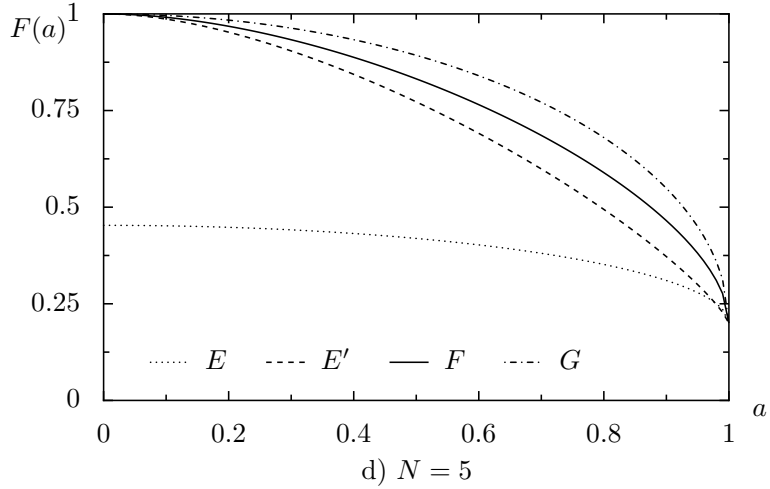
a) $N = 2$



b) $N = 3$



c) $N = 4$



d) $N = 5$

Podsumowanie

- gry kwantowe mogą być użyte jako ilustracja wpływy mechaniki kwantowej na algorytmy i protokoły,
- wygodnym narzędziem do ich opisu są kwantowe języki programowania,

Podsumowanie

- gry kwantowe mogą być użyte jako ilustracja wpływy mechaniki kwantowej na algorytmy i protokoły,
- wygodnym narzędziem do ich opisu są kwantowe języki programowania,
- zagadnienie takie jak rozróżnialność stanów mogą być rozpatrywane jako przykłady gier – takie scenariusze maja zastosowanie do badania związków między odległościami na przestrzeni stanów.

Projekt Quantiki

Wiki i portal poświęcone informatyce kwantowej

- Portal poświęcone informatyce kwantowej oraz encyklopedia informatyki kwantowej.

Projekt Quantiki

Wiki i portal poświęcone informatyce kwantowej

- Portal poświęcone informatyce kwantowej oraz encyklopedia informatyki kwantowej.
- Możliwość dodawania informacji o ofertach prac, konferencjach oraz baza grup pracujących na kwantową teorią informacji.

Projekt Quantiki

Wiki i portal poświęcone informatyce kwantowej

- Portal poświęcone informatyce kwantowej oraz encyklopedia informatyki kwantowej.
- Możliwość dodawania informacji o ofertach prac, konferencjach oraz baza grup pracujących na kwantową teorią informacji.
- Projekt finansowany w ramach projektu ERA-Pilot *Quantum Information Science and Technology*, tworzony przy współpracy National University of Singapore.

Projekt Quantiki

Wiki i portal poświęcone informatyce kwantowej

- Portal poświęcone informatyce kwantowej oraz encyklopedia informatyki kwantowej.
- Możliwość dodawania informacji o ofertach prac, konferencjach oraz baza grup pracujących na kwantową teorią informacji.
- Projekt finansowany w ramach projektu ERA-Pilot *Quantum Information Science and Technology*, tworzony przy współpracy National University of Singapore.
- Więcej na: http://www.quantiki.org/

Dziękuję za uwagę