Roman GIELERAK, Przemysław RATAJCZAK
UNIWERSYTET ZIELONOGÓRSKI, INSTYTUT STEROWANIA I SYSTEMÓW INFORMATYCZNYCH

Efektywnie symulowalne układy quditowe

Prof. dr hab. Roman GIELERAK

Wszystkie stopnie i tytuły naukowe uzyskał na Uniwersytecie Wrocławskim w okresie od 1976 do 1999(profesura). Brał udział w licznych projektach badawczych we współpracy z wieloma ośrodkami zagranicznymi (ETH Zurych; ZIBJ Dubna; MGU Moskwa; Bochum-Bonn-Bielefeld Uniwersytety; Instytut Galileusza, Paryż; Uniwersytet w Lisbonie). Autor licznych prac i opracowań monograficznych z podstaw teorii kwantowej i jej zastosowań.

e-mail: r.gielerak@issi.uz.zgora.pl

Mgr inż. Przemysław RATAJCZAK

Ukończył studia na Wydziale Elektrotechniki, Informatyki i Telekomunikacji Uniwersytetu Zielonogórskiego. W roku 2006 obronił pracę magisterską pt. Protokoły kryptografii kwantowej i ich symulacje komputerowe. Aktualnie jest doktorantem na Wydziale Elektrotechniki, Informatyki i Telekomunikacji UZ.

e-mail: P.Ratajczak@weit.uz.zgora.pl

Streszczenie

Przedstawiono wyniki symulacji losowych obliczeń kwantowych zrealizowanych za pomocą obwodów unitarnych klasy CHP dla obwodów quditowych. Potwierdzone teoretyczne oszacowania dotyczące złożoności obliczeniowej symulacji tego typu układów kwantowych. Symulacje przeprowadzono poprzez implementacje w języku C algorytmu Aaronsona-Gottesmana .

Słowa kluczowe: obwody kwantowe, qudity, algorytm CHP.

Effectively simulable qudit circuits

Abstract

Simulations of random quantum calculations schemes realized within the class of CHP circuits are being performed and the results of them are being presented. In particular the theoretical estimations of computational complexity of the systems analyzed are being confirmed. The C language version of the Aaronson-Gottesman algorithm has been used for the analyzed simulation process.

Keywords: quantum circuits, qudits, CHP algorithm.

1. Wstęp

Postępująca miniaturyzacja w technologii układów scalonych nieuchronnie zbliża nas do bariery, gdzie zjawiska specyficzne dla mikroświata, zjawiska kwantowe zaczną odgrywać dominującą rolę. Załamie to ostatecznie trend opisywany tzw. prawem Moore'a. Wyjściem z tej sytuacji jest możliwość użycia praw fizyki kwantowej do przeprowadzania procesów przetwarzania informacji, jej przechowywania oraz jej transferu. Ten nowy obszar badawczy znany pod nazwą Informatyka Kwantowa przeżywa w ostatnich latach swoistą erupcję w sferze badań teoretycznych. Jednakowoż problem zbudowania wielkoskalowej maszyny kwantowej ciągle jeszcze wydaje się być poza zasięgiem dzisiejszej technologii. Nowe wyłaniające się technologie jak np. inżynieria molekularno-atomowa, czego szczególnym przypadkami są np. inżynieria genetyczna, czy też nanoinżynieria wymagają bardzo kosztownych badań laboratoryjnych i dlatego problem symulacji procesów technologicznych w skalach tu rozważanych jest bardzo istotny. Okazuje się jednak, że złożoność obliczeniowa procesów symulacji układów kwantowych na maszynach klasycznych narasta eksponencjalnie wraz ze stopniem złożoności takiego układu [1, 2].

Jednakże istnieją pewne układy quasikwantowe, których zachowania można symulować na maszynach klasycznych w czasie wielomianowym. Ogólne twierdzenia wiążące efektywną symulowalność ze stopniem splątania stanu układu podaje [3, 4, 8]. W zakresie obwodów kwantowych wyselekcjonowano pewne klasy takich układów, których zachowanie (czyli proces obliczeniowy) można efektywnie symulować na maszynach klasycznych. Najbardziej znana klasa układów kwantowych tego typu to układy CHP [5, 6, 7, 8]. Są to obwody kwantowe, w których dopuszczalne bramki kwantowe to: C-Not, bramka Hadamarda oraz specjalna bramka zmiany bramka fazy P. Dodatkowo dopuszczamy bramki nieunitarne implementujące proces pomiaru stanów jednoqubitowych w bazach kanonicznych. W niniejszej pracy podjęto próbę opisania obwodów kwantowych opierających się na wyższych jednostkach kwantowych tzw. quditach będących odpowiednikami qubitowych obwodów klasy CHP i których jak udowadniamy poniżej symulacja na maszynach klasycznych jest możliwa w czasie wielomianowym, przy czym o ile nie pojawiają się bramki pomiaru to złożoność obliczeniowa tych symulacji jest liniowa, a przy obecności bramek pomiaru stanu złożoność w używanej obecnie wersji algorytmu do symulacji jest ograniczone z góry potęgą 3. W przypadku układów qubitowych pojawiły się ostatnio wersje algorytmów symulacji obliczeń realizowanych na tego typu obwodach z wykładnikami znacznie mniejszymi [11].

Inna klasa efektywnie symulowalnych obwodów kwantowych implementujących tryb obliczeń kwantowych znany pod nazwą „one way quantum computing" została opisana w pracach [12, 13, 14, 15].

2. Układy klasy CHP zbudowane na quditach i ich symulowalność

Niech d >= 2 będzie liczba naturalną. Dowolny układ kwantowy dla którego odpowiednia przestrzeń stanów jest izomorficzna z d-wymiarową przestrzenią zespoloną Euklidesa C^d będzie nazywany quditem. Dla d=2 mamy do czynienia z dobrze znanymi qubitami. Kanoniczna baza ortonormalna przestrzeni C^d będzie oznaczona jako system ketów ($|j\rangle$, j=0,..., d-1). Dla rejestru złożonego z n quditów odpowiednia przestrzeń stanów to d^n wymiarowa przestrzeń Hilberta C^{d^n}, baza kanoniczna której jest oznaczona jako system ketów ($|j_1 j_2 ... j_n\rangle$, j =0,..., d-1).

Podstawowe jednoquditowe operatory unitarne generujące grupę Pauliego P(d) to naturalne uogólnienia odpowiednich macierzy X i Z dobrze znanych dla d=2 i zdefiniowanych poprzez swoje działania na wektorach bazy:

$$X|j\rangle = |j+1\rangle; \quad Z|j\rangle = \omega^j |j\rangle \tag{2.1}$$

gdzie ω to prymitywny pierwiastek z 1 stopnia d, tzn. $\omega^d = 1$.

Wprost z (2.1) wynika, że $X^d = Z^d = 1$ oraz, że następujące relacje komutacji są spełnione:

$$X * Z = \omega^{-1} * Z * X \tag{2.2}$$

Multiplikatywna grupa operatorów generowana przez operacje X i Z jest zwana jednoquditową grupą Pauliego P(d). Wprost z definicji i relacji (2.1) i (2.2) wynika, że:

$$P(d) = \left\{\omega^i * X^j * Z^k, \ i,j,k = 0,...,d-1\right\} \tag{2.3}$$

a zatem grupa ta zawiera dokładnie d^3 elementów.

Iloczyn tensorowy grupy Pauliego P(d) działający w produkcie tensorowym, produktowa grupa Pauliego P(d, n) jest nazywana n–quditową grupą Pauliego. Łatwo sprawdzić, iż ta grupa zawiera dokładnie $d*d^{2n}$ elementów. Korzystając ze znanych twierdzeń o grupach dyskretnych wnosimy, że istnieją układy G(d, n) generujące grupy P(d, n) i składające się z nie więcej niż z $\log_2(d*d^{2n}) = \log_2(d)*(1 + 2n)$ elementów.

Z idempotentności macierzy X i Z wynika, że ich wartości spektralne to zbiór wszystkich pierwiastków stopnia d z jedności. Biorąc dowolny element W grupy P(d, n) łatwo udowodnić, iż jego spektrum jest podzbiorem zbioru pierwiastków stopnia d z jedynki. Jeżeli d jest liczbę pierwszą to wtedy krotność degeneracji każdej z wartości własnej operatora W wynosi $(1/d)*n^d$ i jest taka sama dla każdej wartości spektralnej.

Typowy element grupy Pauliego P(d, n) ma następującą postać:

$$\widetilde{X} = \omega^{\alpha} \underline{X}^{\underline{\gamma}} \underline{Z}^{\underline{\delta}} \tag{2.4}$$

gdzie $\alpha \in \{0,...,d-1\}$, $\underline{\gamma} \in \{0,...,d-1\}^{\{1,...,n\}}$, $\underline{\delta} \in \{0,...,d-1\}^{\{1,...,n\}}$ to odpowiednie multindeksy, oraz gdzie jest zastosowana notacja: $\underline{X}^{\underline{\gamma}} = X_1^{\gamma_1} \otimes ... \otimes X_n^{\gamma_n}$, $\underline{Z}^{\underline{\delta}} = Z_1^{\delta_1} \otimes ... \otimes Z_n^{\delta_n}$ i gdzie X_i, Z_i oznaczają $X_i = 1 \otimes ... \otimes X \otimes ... \otimes 1$, X na i-tej pozycji i podobnie dla Z_i.

W przypadku n=1 operacje $X^{\alpha}Z^{\beta}$ i $X^{\alpha'}Z^{\beta'}$ są przemienne wtedy i tylko wtedy, gdy $\beta\alpha' = \alpha\beta' \bmod(d)$, a w przypadku n>1 odpowiedni warunek komutacji to: dla $\widetilde{Y} = \underline{X}^{\underline{\gamma}} \underline{Z}^{\underline{\delta}}$, $\widetilde{Y}' = \underline{X}^{\underline{\gamma}'} \underline{Z}^{\underline{\delta}'}$ zachodzi $\widetilde{Y} * \widetilde{Y}' = \widetilde{Y}' * \widetilde{Y}$ wtedy i tylko wtedy, gdy $\sum_{i=1}^{n} \gamma_i * \delta_i' = \sum_{i=1}^{n} \gamma_i' * \delta_i \bmod(d)$.

Dla zadanego wektora $|\Psi\rangle \in C^d$ określamy jego stabilizator

$$Stab(|\Psi\rangle) = \{A \in U(d): \; A|\Psi\rangle = |\Psi\rangle\} \tag{2.5}$$

gdzie U(d) oznacza grupę unitarnych transformacji przestrzeni C^d. Łatwo udowodnić, że dla każdego wektora $|\Psi\rangle$ zbiór $Stab(|\Psi\rangle)$ stanowi podgrupę grupy U(d) oraz dla dowolnej pary wektorów $|\Psi\rangle$ i $|\Psi'\rangle$ odpowiednie grupy $Stab(|\Psi\rangle)$ i $Stab(|\Psi'\rangle)$ są sprzężone, a wiec w szczególności zawierają tą samą liczbę elementów oraz dla $\Psi \neq \Psi'$ grupy stabilizatorów są różne. Dla zadanego wektora $|\Psi\rangle$ przecięcie grupy $Stab(|\Psi\rangle)$ z grupą P(d, n) jest podgrupą grupy P(d, n) i właśnie o tej podgrupie będziemy mówić jako właściwej grupie stabilizacyjnej i oznaczać ją jako $STAB(|\Psi\rangle)$.

Normalizator grupy P(d, n) w grupie unitarnej $U(d^n)$ nosi nazwę grupy Clifforda rejestru n-quditowego i odgrywa fundamentalna rolę w konstrukcji kodów korekcji błędów kwantowych [17]. Nas będą natomiast interesować stany rejestru, które cechują się tym, że ich stabilizatory są podgrupami grupy Pauligo. Stany takie są interesujące z tego powodu, iż można je opisać za pomocą znacznie mniejszej ilości współrzędnych niż standardowy opis wektorowy, który wymaga n^d współrzędnych oraz fakt, iż takie stany można opisać za pomocą generatorów grupy Clifforda, które opisujemy poniżej. Kluczem do tego jest uwaga ze stan taki jest opisany jednoznacznie za pomocą swojego stabilizatora STAB, a z kolei grupa STAB jest generowana przez O(n) elementów dla dowolnej wartości d. Przypadek d=2 jest dobrze rozpoznany, a cała klasa tego rodzaju wektorów zwanych wektorami stabilizatorowymi została dokładnie opisana wraz z odpowiednimi algorytmami do ich konstrukcji. Jest to treść twierdzenia Knilla-Gottesmana [5, 6, 7].

Zdefiniujemy teraz pewne bramki kwantowe będące naturalnymi uogólnieniami odpowiednio bramek C-NOT, bramki Hadamarda i bramki fazowej P - dobrze znanych w przypadku qubitów. I tak, d-wymiarowe uogólnienie bramki Hadamarda jest zdefiniowane poprzez :

$$H: |j\rangle \rightarrow \sum_{k=0}^{d-1} \omega^{jk} |k\rangle \tag{2.6}$$

bramka zmiany fazy :

$$P: |j\rangle \rightarrow \omega^{j(j-1)/2} |j\rangle \tag{2.7}$$

i wreszcie dwuquditowa bramka C-NOT ;

$$C: |i, j\rangle \rightarrow |i, i + j \bmod(d)\rangle \tag{2.8}$$

Zanotujmy następujące związki, które łatwo udowodnić wprost z definicji:

$$HXH^{-1} = Z, \; HZH^{-1} = X^{d-1} \tag{2.9}$$

$$PXP^{-1} = XZ, \; PZP^{-1} = Z \tag{2.10}$$

$$(C-NOT)(X \otimes Z)(C-NOT)^{-1} = XZ^{d-1} \otimes XZ \tag{2.11}$$

i podobnie dla $X \otimes X$, $Z \otimes Z$, $Z \otimes X$.

Potrzebujemy też operacji unitarnych $S_{a,b}$ takich, że:

$$S_{a,b} X S^{-1} = X^a, \; S_{a,b} Z S_{a,b}^{-1} = Z^b \tag{2.12}$$

dla każdej pary (a,b) spełniającej warunek ab=1 mod(d).

Jeżeli a jest takie, że generuje grupę multiplikatywną Z^*_d to wystarczy wybrać jedną parę (a,b) taką, że ab=1 mod(d) i wtedy ominąć dolne indeksy dla S określonego poprzez

$$S|j\rangle = |aj\rangle \; . \tag{2.13}$$

Dla zupełności naszego opisu musimy zdefiniować też operację pomiaru stanu wyróżnionego quditu w hipotetycznym n-quditowym rejestrze. Niech E(i) to projektor ortogonalny w C^d na podprzestrzeń generowaną przez wektor bazowy |i>. Wtedy operator $M = \sum_{i=0}^{d-1} E(i)$ jest i mplementacją operatorową pomiaru stanu quditu w bazie kanonicznej. W przypadku rejestru n-quditowego, operator $M_k = 1 \otimes ... \otimes M \otimes ... \otimes 1$, gdzie M zajmuje pozycję k-tą, jest operacja pomiaru stanu quditu o numerze k. Przypomnijmy, że jeżeli rejestr n-quditowy znajduje się w stanie $|\psi\rangle$ którego rozkład w bazie kanonicznej przestrzeni C jest dany poprzez formułę:

$$|\Psi\rangle = \sum_{j_1,...,j_n=0}^{d-1} C_{j_1...j_n} |j_1...j_n\rangle \tag{2.14}$$

Po wykonaniu pomiaru rejestr znajdzie się w jednym ze stanów

$$|\Psi'\rangle = \sum_{j_1...j_{k-1}j_{k+1}...j_n} C_{j_1...j_{k-1}k^*j_{k+1}...j_n} |j_1...j_{k-1}k^*j_{k+1}...j_n\rangle \tag{2.15}$$

dla k^*=0,..., d-1 z prawdopodobieństwem równym $\sum_{j_1...j_n=0}^{d-1} |C_{j_1...j_n}|^2$.

Podobnie jak w przypadku d=2 wszystkie stany, które można otrzymać poprzez zastosowanie dowolnej skończonej kombinacji operatorów H, P i C-NOT oraz operatorów M_k do stanu próżniowego |0,...0>, a zwane uogólnionymi stanami stabilizatorowymi, cechują się tym, że ich grupy Stab pokrywają się z grupami STAB. Poniżej formułujemy jedno z podstawowych twierdzeń uzyskanych przez nas, a którego kompletny dowód zostanie przedstawiony w innej publikacji [16].

Twierdzenie 2.1.

Niech n i d będą ustalone. Wtedy następujące warunki są równoważne:

(1) stan $|\Psi\rangle$ można otrzymać poprzez zastosowanie skończonej ilości operacji H, P, S i C-Not zastosowanych do stanu próżniowego rejestru |0,...0>.

(2) stan $|\Psi\rangle$ można otrzymać poprzez zastosowanie skończonej ilości operacji H, P, S i C-Not oraz dodatkowo operacji pomiarów M_k zastosowanych do stanu próżniowego rejestru |0,...0> jako stanu początkowego rejestru.

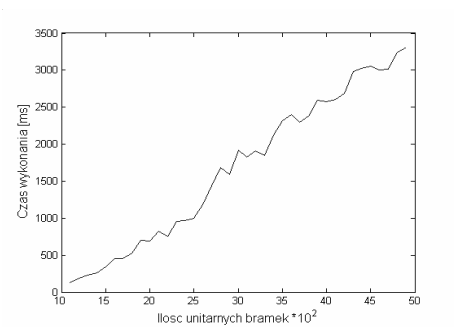
(3) stan $|\Psi>$ jest jednoznacznie określony poprzez równość $Stab(|\Psi>) = STAB(|\Psi>)$.
(4) Grupa $STAB(|\Psi>)$ składa się dokładnie z d^n elementów.

Zatem działanie wyróżnionych bramek z algebry Clifforda na stanach rejestru możemy opisywać za pomocą zmian stabilizatora odpowiedniego stanu. Biorąc bramkę U stabilizator wektora $U|\Psi>$ jest równy $U^{-1}*STAB(|\Psi>) * U$ i ta równość stanowi klucz do napisania odpowiedniego algorytmu za pomocą którego można opisywać ewolucje stanu rejestru i to w czasie liniowym.

3. Symulacje komputerowe

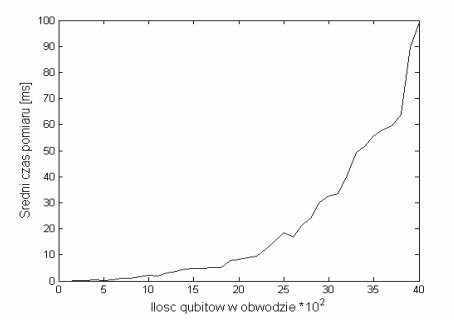
W symulacjach zastosowano implementację wzorowaną na implementacji Aaronsona [7]. Ponadto zastosowano maszynę o następujących parametrach: procesor AMD Athlon 2500+, 512MB RAM, system operacyjny Windows XP. Wykorzystany kompilator kodu źródłowego to gcc.

Dla d=2 symulacje podzielono na dwa etapy. Mając na uwadze, iż czas przetwarzania dla pojedynczej bramki różni się w zależności od tego czy mamy do czynienia z bramką pomiaru dającą wynik deterministyczny, czy też dowolną inną bramką. Dlatego w pierwszym eksperymencie rozpatrujemy czasy przetwarzania układów losowo wygenerowanych, zawierających bramki CNOT, Hadamarda i fazy w równych proporcjach. Dla układu 1000 qubitów zastosowaliśmy rosnącą liczbę unitarnych bramek w zakresie od 1000 do 20000 ze wzrostem co 500. Wynik pomiaru czasów prezentuje rys. 1. Widać tu wyraźną liniową zależność czasu wykonania od liczby bramek.



Rys. 1. Zależność czasu przetwarzania obwodu od liczby bramek unitarnych
Fig. 1. CPU occupation time necessary to simulate random CHP class circuit composed of n unitary gates

W drugim przypadku rozpatrywany był czas pomiarów. Przeprowadzane one były po wykonaniu na układzie n*log(n) unitarnych operacji, których celem było przeprowadzenie mierzonego rejestru w stan, którego wynik pomiaru jest deterministyczny. Liczba rozpatrywanych qubitów znajdowała się w zakresie od 100 do 4000 z krokiem 100. Rysunek 2 przedstawia zależność średniego czas wykonania pojedynczej operacji pomiaru w zależności od ilości qubitów w rejestrze. Widać wielomianowy wzrost potrzebnego czasu zbliżający się do krzywej n^2.



Rys. 2. Zależność średniego czasu pojedynczego pomiaru od wielkości układu kwantowego
Fig. 2. Average time necessary to simulate measurement of a single qubit as function of the the number n of qubits forming the circuit

Głównym powodem stosowania układów CHP opartych o zapis oparty o grupę stabilizatorów w przeciwieństwie do symulatorów stosujących pełen opis stanu układu jest możliwość wielokrotnego zwiększenia ilości przetwarzanych qubitów. Jednak wydajność zależy od rodzaju symulowanych układów, stąd czas dla pojedynczego pomiaru mieści się pomiędzy wartościami liniowo, a kwadratowo zależnymi od n.

4. Podsumowanie

W przedstawionej pracy przedstawiono próbę uogólnienia znanego dla przypadku qubitowego twierdzenia oraz algorytmu Aaronsona-Knilla-Gottesmana o wielomianowej symulowalności kwantowych obwodów klasy CHP na przypadek wyższych jednostek kwantowych. W szczególności podano opis odpowiednich grup Pauliego i grup Clifforda dla układów quditów, a także sformułowano podstawowe twierdzenie opisujące stany stabilizatorowe w terminach generatorów grupy Clifforda, co umożliwia sformułowanie odpowiednich algorytmów do symulacji analizowanych obwodów kwantowych o wielomianowych złożonościach obliczeniowych.

Ponieważ jednak znany w przypadku układów qubitowych formalizm oparty na stanach gronowych i macierzowych stanach produktowych [11, 14, 15] umożliwia daleko idącą optymalizację procedur symulacyjnych, dlatego podjęta też została próba przeniesienia wymienionych technik na przypadek układów quditowych, a odpowiednie wyniki zostaną sformułowane w innej publikacji [16].

5. Literatura

[1] Feynman R.P.: Simulating physics with computers, International Journal of Theoretical Physics 21, 467-488 1982.
[2] Feynman R.P.: Quantum mechanical computers, Foundations of physics 16, 507-531 1986.
[3] Vidal G.: Efficient classical simulation of slightly entangled quantum computations, Phys. Rev. Lett. 91, 147902 2003, quant-ph/0301063 2003.
[4] Vidal G.: A class of quantum many-body states that can be efficiently simulated, quant-ph/0610099 2006.
[5] Gottesman D.: An introduction to quantum error correction, in Quantum Computation : A Grand Mathematical Challenge for the Twenty-First Century and the Millennium, ed. S.J. Lomonaco Jr, 221-235, AMS, Providence 2002, quant-ph/0004072 2000.
[6] Knill E., Laflamme R.: Theory of quantum error-correcting codes, Phys. Rev. A 55, 900-911 1997.
[7] Aaronson S., Gottesman D.: Improved Simulation of Stabilizer Circuits, Phys. Rev. A 70, 052326 (2004), quant-ph/0406196 2004.
[8] Jozsa R.: On the simulation of quantum circuits, quant-ph/0603163 2006.
[9] Markov I., Shi Y.: Simulating quantum computations by contracting tensor networks, quant-phys/0511069 2006.
[10] Teszner M.: Effectively simulable quantum systems (in Polish), Master Thesis, University of Zielona Góra 2006.
[11] Anders S., Briegel H.J.: Fast simulation of stabilizer circuits using a graph state representation, quant-ph/0504117 2006.
[12] Nielsen M.A., Chuang I.L.: Quantum Computation and Quantum Information, Cambridge University Press 2000.
[13] Anders S.: A guide to the local Clifford group, w przygotowaniu.
[14] Van den Nest M., Dür W., Vidal G., Briegel H.J.: Classical simulation versus universality in measurement based quantum computation, quant-ph/0608060 2006.
[15] Browne D., Briegel H.: One-way Quantum Computation, quant-ph/0603226 2006.
[16] Gielerak R., Ratajczak P.: praca w przygotowaniu.
[17] Hostens E., Dehaene J., De Moor B.: Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic, quant-ph/0408190 2005.
[18] Ashikhmin A., Knill E.: Nonbinary Quantum Stabilizer Codes, IEEE Trans. Inform Theory 47, 3065-3072 2001.
[19] Grassl M., Roetteler M., Beth T.: Efficient Quantum Circuits for Non-Qubit Quantum Error-Correcting Codes, Intern. J. of Found. Of Computer Sciences (IJFCS) 14(5), 757-775 2003.

Artykuł recenzowany