Marek SZYPROWSKI [1], **Paweł KERNTOPF** [1,2]
[1] POLITECHNIKA WARSZAWSKA, WYDZIAŁ ELEKTRONIKI, INSTYTUT INFORMATYKI, ul. Nowowiejska 15/19, 00-665 Warszawa
[2] UNIWERSYTET ŁÓDZKI, WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ, ul. Pomorska 149/153, 90-236 Łódź

Projektowanie odwracalnych układów w architekturze LNN

Mgr inż. Marek SZYPROWSKI

Ukończył studia magisterskie na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Obecnie odbywa studia doktoranckie w Instytucie Informatyki na tym Wydziale. Jego zainteresowania naukowe koncentrują się wokół układów odwracalnych, które stanowiły temat jego pracy magisterskiej.

e-mail: M.Szyprowski@ii.pw.edu.pl

Streszczenie

Najnowszy kierunek w projektowaniu kwantowych układów odwracalnych uwzględnia fakt, że interakcje odbywają się tylko na sąsiadujących liniach. Ostatnio zaproponowano wiele algorytmów projektowania takich układów oraz zajmowano się ich optymalizacją. W pracy przedstawiony jest przegląd tych rozwiązań oraz perspektywy rozwoju tej ważnej dziedziny.

Słowa kluczowe: układy odwracalne, układy kwantowe, architektura LNN.

Designing reversible circuits in the LNN architecture

Abstract

Computation is called reversible if it is realized by circuits implementing bijective mappings. It is an emerging research area which has applications in many new areas of computer science, e.g. quantum computing, nanotechnologies, optical computing, digital signal processing, communications, bioinformatics, cryptography as well as low power computation. Quantum computation, which by nature is reversible, constitutes an especially attractive field of research due to a promise of an enormous speed-up of computing processes in the future. However, it has appeared that in some quantum technologies there are intrinsic limitations, namely, physically realizable operations would be only interactions between neighbor lines (also called qubits). As reversible circuits form a subset of quantum circuits there is a need to convert general reversible circuits into the so-called Linear Nearest Neighbor (LNN) architecture. In this architecture any gate operates between adjacent qubits only. Thus, recently there has been a new research objective to develop efficient methods for designing reversible circuits in the LNN architecture. This paper gives an overview of the present advances in this field.

Keywords: reversible circuits, quantum circuits, LLN architecture.

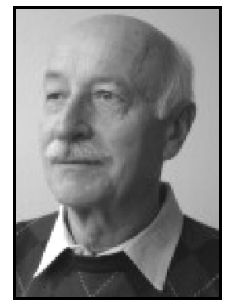
1. Wstęp

Układy odwracalne realizują wzajemnie jednoznaczne odwzorowania sygnałów wejściowych na sygnały wyjściowe, tj. nie prowadzące do strat informacji. Badania nad układami odwracalnymi prowadzone są bardzo intensywnie ze względu na potencjalną możliwość wykorzystania układów odwracalnych do konstrukcji urządzeń o małym poborze mocy, ponieważ umożliwiają one zmniejszanie energii pobieranej przez układy cyfrowe, a ponadto znajdują zastosowanie w nanotechnologiach, układach optycznych, kryptografii, cyfrowym przetwarzaniu sygnałów, bioinformatyce i w innych działach informatyki [1]. Jednak prace prowadzone w tym kierunku mają przede wszystkim ogromne znaczenie dla budowy komputerów kwantowych, co pozwoliłyby na znaczne przyspieszenie rozwiązywania niektórych problemów NP-trudnych, których nie można efektywnie rozwiązywać na dzisiejszych komputerach.

W ostatnich latach opublikowaliśmy kilka przeglądowych prac [2-6], aby wszystkich, którzy zajmują się w Polsce syntezą układów logicznych, zapoznać z nowymi wyzwaniami, jak również zachęcić i przygotować do badań w dziedzinie projektowania układów odwracalnych. W niniejszym przeglądzie omawiamy jeden z najnowszych kierunków tych badań – projektowanie układów w architekturze LNN, nazywanej tak od angielskiego określenia *Linear Nearest Neighbor* dla układów, w których zarówno wejścia, jak i wyjścia bramek znajdują się na sąsiednich liniach. Przedstawiamy w nim wyniki badań w tej dziedzinie.

Dr hab. inż. Paweł KERNTOPF

Ukończył studia na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Obecnie pracuje na stanowisku profesora nadzwyczajnego w Instytucie Informatyki na tym Wydziale oraz w Katedrze Fizyki Teoretycznej i Informatyki na Wydziale Fizyki i Informatyki Stosowanej Uniwersytetu Łódzkiego. Zainteresowania naukowe: synteza układów logicznych, układy odwracalne, układy kwantowe, binarne i wielowartościowe diagramy decyzyjne.



e-mail: P.Kerntopf@ii.pw.edu.pl

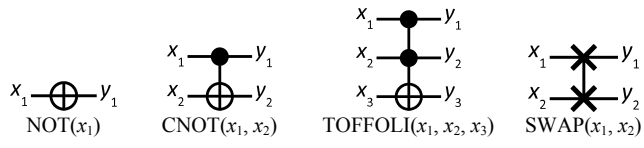
2. Pojęcia podstawowe

Poniżej podajemy podstawowe pojęcia z dziedziny syntezy układów odwracalnych. Funkcja boolowska o n argumentach i n wartościach (w skrócie $n*n$ funkcja) jest nazywana odwracalną, jeśli jest przekształceniem wzajemnie jednoznacznym. Bramka o n wejściach i n wyjściach (w skrócie $n*n$ bramka) jest nazywana odwracalną, jeśli realizuje $n*n$ funkcję odwracalną (tę samą konwencję stosujemy do układów). W układach odwracalnych rozgałęzienia sygnałów są zabronione, zatem $n*n$ układ jest kaskadą $k*k$ bramek odwracalnych, gdzie $k \le n$. Jak w tradycyjnych układach logicznych, dwa różne układy odwracalne mogą realizować tę samą funkcję odwracalną. W takim przypadku nazywane są układami równoważnymi.

W niniejszej pracy omawiamy układy zbudowane z bramek NOT (inwerter) o jednym wejściu/wyjściu, bramek CNOT (ang. *Controlled-NOT*,) i SWAP o dwóch wejściach/wyjściach oraz z bramek Toffoliego o trzech wejściach/wyjściach (ich definicje podane są w tab. 1, zaś symbole graficzne na rys. 1). Wejście x_1 w bramkach CNOT oraz wejścia x_1 i x_2 w bramkach Toffoliego nazywane są wejściami sterującymi, gdyż mogą zmieniać sygnały na pozostałych liniach.

Tab. 1. Definicje bramek odwracalnych
Tab. 1. Definitions of reversible gates

NOT	CNOT	Bramka Toffoliego	Bramka SWAP
$y_1 = x_1 \oplus 1$	$y_1 = x_1$ $y_2 = x_1 \oplus x_2$	$y_1 = x_1$ $y_2 = x_2$ $y_3 = x_3 \oplus x_1x_2$	$y_1 = x_2$ $y_2 = x_1$

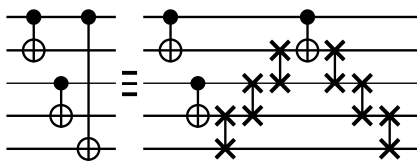


Rys. 1. Graficzne reprezentacje bramek odwracalnych
Fig. 1. Pictorial representations of reversible gates

Dla każdej funkcji odwracalnej istnieje wiele implementujących ją układów odwracalnych. Do oceny jakości tych układów stosowane są funkcje kosztu. Najczęściej stosowany jest tzw. koszt kwantowy (ang. *Quantum Cost*, w skrócie *QC*), odpowiadający minimalnej liczbie elementarnych bramek kwantowych, użytych

do budowy danego układu. Przyjmuje się, że koszt kwantowy bramek NOT i CNOT wynosi 1, zaś bramek Toffoliego i SWAP wynosi odpowiednio 5 i 3.

Dla architektury LNN wprowadzono nową funkcję kosztu zwaną NNC od angielskiej nazwy *Nearest Neighbor Cost*. Niech bramka o dwóch wejściach/wyjściach ma wejścia na liniach o numerach i oraz j ($1 \le i, j \le n$). Koszt NNC dla tej bramki jest równy $|i-j|$-1 (zatem najmniejszą wartością NNC jest 0). NNC dla układu odwracalnego jest sumą kosztów NNC jej wszystkich bramek. Dla lewego układu z rys. 2 mamy QC = 1 + 1+ 1 =3 oraz NNC = 0 + 0 + 3 = 3, zaś dla równoważnego mu prawego układu z Rys. 2 mamy QC = 1 + 1 + 3 + 3 + 3 + 1 + 3+ 3 + 3 = 21 oraz NNC = 0. Jak widać, stosując bramki SWAP do krzyżowania linii można zmniejszyć NNC do zera, jednak prowadzi to do zwiększania kosztu kwantowego.



Rys. 2. Dwa równoważne układy (prawy w architekturze LNN)
Fig. 2. Two equivalent circuits (the right one in the LNN architecture)

3. Bramki i układy kwantowe

W układach kwantowych jednostką informacji jest superpozycja stanów |0> i |1>:

$$q = c_0 |0\rangle + c_1 |1\rangle,$$

gdzie c_0 i c_1 są liczbami zespolonymi, spełniającymi warunek

$$|c_0|^2 + |c_1|^2 = 1.$$

Zaproponowano wiele bramek kwantowych, jednak w większości publikacji rozpatruje się tylko następujący zbiór czterech bramek: dwie wyżej zdefiniowane bramki NOT i CNOT oraz bramki CV i CV$^+$, których definicje podamy niżej.

Działanie n*n bramek odwracalnych i kwantowych może być opisane za pomocą macierzy kwadratowych o rozmiarach $2^n \times 2^n$, np. przekształcenie *NOT* opisywane jest przez macierz:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

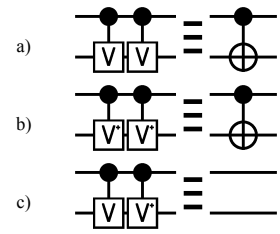
Reprezentacje macierzowe przekształceń V i V^+ [8]:

$$V = \frac{1+i}{2}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}, \qquad V^+ = V^{-1} = \frac{1-i}{2}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

Są one nazywane pierwiastkami kwadratowymi z *NOT*, gdyż $V \circ V = NOT$, $V^+ \circ V^+ = NOT$, gdzie symbol ∘ oznacza iloczyn macierzy, oraz $V \circ V^+ = Id$, gdzie Id oznacza macierz identycznościową.

Bramki CV i CV$^+$, nazywane sterowanymi bramkami V i V$^+$ (ang. *controlled-V*/*V*$^+$ gates), są elementarnymi 2*2 bramkami kwantowymi z jednym sygnałem sterującym. Symbole graficzne tych bramek przedstawia rys. 3. Jeśli sygnał sterujący jest równy 1, to bramki te stosują przekształcenie macierzowe, odpowiednio V i V^+, na drugiej linii, a gdy sygnał sterujący jest równy 0, to sygnał na drugiej linii nie jest zmieniany. Bramki CV i CV$^+$ są swoimi odwrotnościami. Zastosowanie dwóch operacji V lub V+ na tej samej linii jest tożsame wykonaniu operacji CNOT (rys. 4).

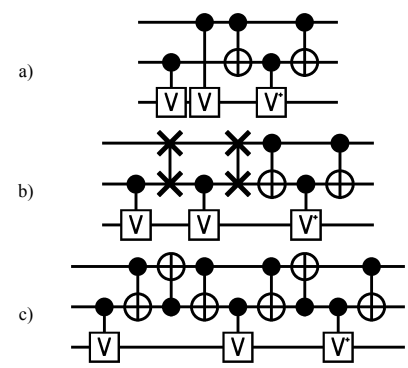
Rys. 3. Symbole graficzne dla bramek kwantowych CV i CV$^+$
Fig. 3. Pictorial symbols for CV and CV$^+$ quantum gates



Rys. 4. Upraszczanie par sąsiednich bramek kwantowych CV i CV$^+$
Fig. 4. Simplification of pairs of adjacent CV and CV$^+$ quantum gates

W ciągu ostatnich kilkunastu lat opracowano osiem technologii kwantowych [7, 8]. Każda z nich narzuca pewne ograniczenia na fizyczne realizacje układów kwantowych. Spośród nich najczęściej występującym jest ograniczenie interakcji do sąsiednich (czyli dwóch najbliższych geometrycznie) linii sygnałowych. Tak jest między innymi dla najpopularniejszych obecnie technologii: 1) opartej na nuklearnym rezonansie magnetycznym (ang. Nuclear Magnetic Resonance, w skrócie NMR) i 2) opartej na tzw. pułapkach jonowych (ang. ion traps). Uważa się bowiem, że te technologie dają największe szanse na opracowanie w niedalekiej przyszłości metodologii realizacji skalowalnych układów kwantowych.

Na rys. 5 przedstawiliśmy trzy implementacje kwantowe bramki Toffoliego, przy czym dwie pierwsze linie licząc od góry są liniami sterującymi. Rys. 5a pokazuje najbardziej rozpowszechniony w literaturze układ kwantowy o minimalnym koszcie kwantowym (QC = 5), mającym jednak NCC > 0. Dodając do niego dwie bramki SWAP (przed pierwszą bramką i po niej) otrzymujemy układ z rys. 5b, dla którego NCC = 0, ale koszt kwantowy wzrósł do 11. Jednakże istnieje równoważny układ kwantowy z NCC = 0, podany na Rys. 5c, w którym koszt kwantowy wynosi tylko 9. Takie dodawanie bramek SWAP na kolejnych liniach (jak na rys. 2) można zastosować do dowolnej bramki, dla której NCC > 0, jednak widzimy, że nie prowadzi to również do otrzymania optymalnych układów kwantowych.



Rys. 5. Trzy implementacje kwantowe bramki Toffoliego
Fig. 5. Three quantum implementations of the Toffoli gate

4. Wyniki prac na temat architektury LNN

Zagadnienie efektywnej realizacji algorytmów kwantowych w architekturze LNN jest aktualnie jednym z najbardziej intensywnie badanych. Pierwsze prace w tej dziedzinie dotyczyły projektowania kwantowych układów:

a) implementujących algorytm Shora do rozkładania w czasie wielomianowym dużych liczb naturalnych na czynniki pierwsze [9, 13],
b) sumatorów [19],
c) korygujących błędy [10],
d) implementujących transformatę Fouriera [12, 15].

Następnie badano wpływ ograniczeń architektury LNN na powiększanie się liczby bramek i kosztu kwantowego układów kwantowych i odwracalnych. W artykule [11] wykazano, że następuje wtedy zwiększenie liczby bramek prawie o rząd wielkości.

W pracy [14] pokazano, że przekształcenie dowolnego układu na układ mający NNC = 0 wymaga liniowego zwiększenia kosztu kwantowego względem liczby wejść do układu. Opracowano także heurystyczne metody przekształcania dowolnych układów na równoważne układy mające NNC = 0 [16, 17, 18, 21].

Wyraźny postęp stanowiła praca [20], w której zaproponowano rozszerzone podejście w stosunku do wcześniejszych publikacji, mające na celu opracowanie całościowego procesu projektowania układów z NNC = 0 w architekturze LNN. Obejmowało ono następujące nowe elementy:

a) redukcję wygenerowanych układów opartą na stosowaniu tzw. nowego typu wzorców (ang. templates), czyli par układów równoważnych, wzorowanych na wprowadzonych w 2003 r. wzorcach do redukcji liczby bramek w układach odwracalnych [8],
b) metodę projektowania układów LNN o minimalnym koszcie kwantowym dla prostych funkcji odwracalnych,
c) strategie permutowania linii, które przekształcają bramki z NNC > 0 na bramki o NNC = 0.

Kontynuacją pracy [20] była praca [23], w której podano trzy modele przekształcania bramek Toffoliego o dowolnej liczbie wejść sterujących na zredukowane układy LNN bez stosowania bramek SWAP. Wykorzystano do tego celu wzorce układów LNN. Dla wszystkich 3-wejściowych funkcji odwracalnych zbudowano w ten sposób układy o minimalnym koszcie kwantowym (w niektórych przypadkach uzyskano przy tym zmniejszenie liczby bramek o ponad 50%).

Żeby uniknąć stosowania bramek Toffoliego o więcej niż dwóch liniach sterujących, które mają bardzo duży koszt kwantowy, w pracy [22] przedstawiono metodę syntezy układów odwracalnych w architekturze LNN z bramek NOT, CNOT i Toffoliego (o dwóch liniach sterujących). Jednak wadą tej metody jest konieczność stosowania dodatkowych linii, co jest niekorzystne w układach kwantowych.

Inną istotną nowością było rozpatrzenie możliwości zmiany kolejności bramek w układach [24] w taki sposób, aby dodawać jak najmniejszą liczbę bramek SWAP. Dzięki wprowadzeniu specjalnego rodzaju grafu, zawierającego informację na temat zależności pomiędzy sąsiednimi bramkami, możliwe było ulepszenie wyników uzyskanych w pracy [20]. Algorytm jest bardzo efektywny w zastosowaniu do układów z niewielką liczba bramek SWAP, dlatego układy z większą liczbą takich bramek są dzielone na podukłady, które mogą być już efektywnie optymalizowane.

Wszystkie powyższe prace dotyczyły jednowymiarowych układów kaskadowych w architekturze LNN, jednakże rozpatrywano także inne architektury [8, 25]:

a) dwuwymiarowe kwadratowe siatki,
b) trójwymiarowe siatki (zbiory dwuwymiarowych siatek)
c) architektura typu Star,
d) architektura typu Cycle, która różni się od architektury LNN tym, że możliwa jest interakcja pomiędzy pierwszą i ostatnią linią.

5. Podsumowanie

W niniejszej pracy przedstawiono przegląd publikacji na temat projektowania układów odwracalnych i kwantowych w architekturze LNN. Jest to jeden z bardzo ważnych i aktualnie intensywnie rozwijanych kierunków badań w dziedzinie obliczeń odwracalnych i kwantowych. Problemy otwarte z tej dziedziny sformułowane zostały w niedawno opublikowanym artykule [8], do którego – z powodu braku miejsca – odsyłamy czytelników po informacje na ten temat.

6. Literatura

[1] De Vos A.: Reversible Computing. Fundamentals, Quantum Computing and Applications. Wiley-VCH, Berlin 2010.
[2] Kerntopf P.: Synteza odwracalnych układów logicznych. Pomiary Automatyka Kontrola, vol. 53, s.78-80, 2007.
[3] Szyprowski M., Kerntopf P.: Decompositions of reversible logic circuits. Pomiary Automatyka Kontrola, vol. 55, s. 609-611, 2009.
[4] Zagniński P., Kerntopf P.: Sekwencyjne odwracalne układy logiczne. Pomiary Automatyka Kontrola, vol. 56, s. 678-680, 2010.
[5] Szyprowski M., Kerntopf P.: Realizacje układów odwracalnych w technologiach półprzewodnikowych. Pomiary Automatyka Kontrola, vol. 57, s. 911-813, 2011.
[6] Szyprowski M., Kerntopf P.: Odwracalne układy programowalne. Pomiary Automatyka Kontrola, vol. 58, s. 644-646, 2012.
[7] Quantum Computation Roadmap. Los Alamos National Laboratory, http://qist.lanl.gov/qcomp_map.shtml, 2004.
[8] Saeedi M., Markov I.L.: Synthesis and optimization of reversible circuits – a survey. ACM Computing Surveys, vol. 45, no. 2, article 21, s. 1-34, 2013.
[9] Fowler A.G., Devitt S.J., Hollenberg L.C.: Implementation of Shor's algorithm on a linear neighbour qubit array. Quantum Information and Computation, vol. 4, s. 237-245, 2004.
[10] Fowler A.G., Hill C.D., Hollenberg L.C.: Quantum error correction on linear nearest neighbor qubit arrays. Physical Review A, vol. 69, s. 042314.1-042314.4, 2004.
[11] Shende V., Bullock S., Markov I.L.: Synthesis of quantum logic cir-cuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 25, s. 1000-1010, 2006.
[12] Takahashi Y., Kunihiro N., Ohta K.: The quantum Fourier transform on a linear nearest architecture. Quantum Information and Computation, vol. 7, s. 383-391, 2007.
[13] Kutin S.A.: Shor's algorithm on a nearest-neighbor machine. Proceedings of the Asian Conference on Quantum Information Science, s. 12-13, 2007.
[14] Cheung D., Maslov D., Severini S.: Translation techniques between quantum circuit architectures. Proceedings of the Workshop on Quantum Information Processing, s. 1-3, 2007.
[15] Maslov D.: Linear depth stabilizer and quantum Fourier transformation circuits with no auxiliary qubits in finite neighbor quantum architectures. Physical. Review A, vol. 76, s. 052310.1-052310.7, 2007.
[16] Chakrabarti, A., Sur-Kolay, S.: Rules for synthesizing quantum boolean circuits using minimized nearest-neighbour templates. Proceedings of the International Conference on Advanced Computing and Communications, s. 183–189, 2007.
[17] Chakrabarti A., Sur-Kolay S.: Nearest neighbour based synthesis of quantum boolean circuits. Engineering Letters, vol. 15, s. 356–361, 2007.
[18] Khan M.H.A.: Cost reduction in nearest neighbour based synthesis of quantum boolean circuits. Engineering Letters, vol. 16, s. 1–5, 2008.
[19] Choi B.S., Van Meter R.: Effects of interaction distance on quantum addition circuits. arXiv:0809.4317, 2008.
[20] Saeedi M., Wille R., Drechsler R.: Synthesis of quantum circuits for linear nearest neighbor architectures. Quantum Information Processing, vol. 10, s. 355-377, 2011.
[21] Hirata Y., Nakanishi M., Yamashita S., Nakashima Y.: An efficient conversion of quantum circuits to a linear nearest neighbor architecture. Quantum Information and Computation, vol. 11, s. 142-166, 2011.
[22] Perkowski M., Lukac M., Shah D., Kameyama M.: Synthesis of quantum circuits in linear nearest neighbor model using positive Davio lattices. Facta Universitatis, Series: Electronics and Energetics, vol. 24, s. 73-89, 2011.
[23] Rahman M.M., Dueck G.W.: Synthesis of linear nearest neighbor quantum circuits. Proceedings of the 11th International Workshop on Boolean Problems, s. 277-284, 2012.
[24] Matsuo A., Yamashita S.: Changing the gate order for optimal LNN conversion. A. De Vos, R. Wille (eds.) Reversible Computation, vol. 7165, s. 89-101, Springer-Verlag, Berlin Heidelberg, 2012.
[25] Rosenbaum D.: Optimal quantum circuits for nearest-neighbor architectures. arXiv:1205.0036, 2012.

otrzymano / received: 16.05.2013
przyjęto do druku / accepted: 03.07.2013 *artykuł recenzowany / revised paper*