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

Nowe reguły przesuwania bramek w układach odwracalnych

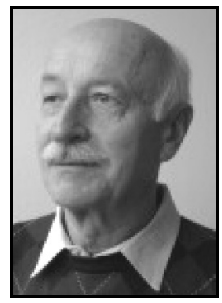
Mgr inż. Marek SZYPROWSKI

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

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 i w Katedrze Fizyki Teoretycznej i Informatyki na Wydziale Fizyki i Informatyki Teoretycznej Uniwersytetu Łódzkiego. Jego zainteresowania naukowe to synteza układów logicznych, odwracalne układy logiczne, kwantowe układy logiczne, binarne i wielowartościowe diagramy decyzyjne.



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

Streszczenie

Jedną z możliwości redukcji układów odwracalnych daje przesuwanie bramek. W pracy zaproponowano nowe reguły takich przesunięć dla układów budowanych ze standardowej biblioteki bramek odwracalnych NCT. Umożliwiają one eliminację bramek o dużej liczbie wejść/wyjść, które mają największy tzw. koszt kwantowy. Opracowane przez nas reguły mogą być stosowane dla dowolnej liczby wejść układu. Umożliwia to projektowanie układów odwracalnych o zredukowanym koszcie kwantowym. Podane przez nas przykłady pokazują, że oszczędności w porównaniu z układami publikowanymi w literaturze mogą być znaczne.

Słowa kluczowe: układy odwracalne, synteza logiczna, układy kwantowe.

New rules for moving gates in reversible circuits

Abstract

Synthesis of reversible logic circuits is the most intensively studied topic of the research area called reversible computation (circuits are reversible if they represent bijective mappings). This new research area has applications in many fields of computer science, e.g. quantum computing, nanotechnologies, optical computing, digital signal processing, communications, bioinformatics, cryptography as well as in low power computation. Recent advances consist in reducing numbers of gates, garbage bits or quantum cost. Some reversible circuit synthesis algorithms generate circuits in which majority of gates have large or even maximal size (i.e. equal to the number of inputs/outputs. However, quantum cost of multi-control generalized Toffoli gates is very high. In this paper it is shown how to reduce the quantum cost of circuits by eliminating most of large gates or even all of them. Namely, a new subset of moving rules useful for reducing the quantum cost is presented. Using this subset, it is possible to reduce the number of maximal-size gates to zero for even functions, and to one for odd functions, according to the known theorem. In the paper substantial savings in the quantum cost are presented for designs taken from recent publications.

Keywords: reversible circuits, logic synthesis, quantum circuits.

1. Wstęp

Układy odwracalne realizują wzajemnie jednoznaczne odwzorowania sygnałów wejściowych na sygnały wyjściowe. Badania nad takimi układami prowadzone są intensywnie, ponieważ wykazano, że ich stosowanie umożliwia zmniejszanie energii pobieranej przez układy cyfrowe [1]. Prace prowadzone w tym kierunku mają duże znaczenie przy opracowywaniu przyszłych technologii komputerowych, w tym technologii kwantowych, a także ze względu na potencjalną możliwość zastosowania układów odwracalnych w nanotechnologiach, układach optycznych, kryptografii, cyfrowym przetwarzaniu sygnałów, bioinformatyce i w wielu innych ważnych działach informatyki.

Najwięcej uwagi poświęca się problemom projektowania układów odwracalnych. Z jednej strony, wynika to z intensywnych prac nad konstrukcją prototypowych układów odwracalnych w różnych technologiach, w tym w klasycznych technologiach półprzewodnikowych CMOS [2]. Z drugiej strony, układy kwantowe, które ze swej natury pracują w sposób odwracalny, umożliwiają wykładnicze przyspieszenie obliczeń dla wielu ważnych zastosowań, np. faktoryzacji dużych liczb naturalnych.

Z punktu widzenia projektowania układów kwantowych istotne jest rozwiązanie problemu projektowania układów odwracalnych, które są podklasą układów kwantowych [1]. Otóż, wiele typowych podzespołów potrzebnych do budowy komputerów kwantowych, np. układy korygujące błędy i układy arytmetyczne, jest układami odwracalnymi, zaś w implementacji układów realizujących niektóre algorytmy kwantowe, duże ich części są układami odwracalnymi, a więc ważne jest, aby działały szybko.

Problem projektowania optymalnych układów odwracalnych jest problemem bardzo trudnym. Mimo opublikowania w ostatnich 10 latach kilkudziesięciu algorytmów projektowania, wciąż nie znaleziono metodologii pozwalającej na znajdowanie układów o praktycznym znaczeniu dla dowolnych funkcji odwracalnych. Dlatego stale pracuje się także nad metodami redukcji redundancyjnych układów generowanych przez obecne algorytmy syntezy. Dzięki opracowanym przez nas regułom, po raz pierwszy w literaturze zaprezentowany został zbiór przekształceń prowadzący do redukcji kosztu kwantowego w układach odwracalnych. Pozwoli to na ulepszanie parametrów układów generowanych przez algorytmy syntezy.

2. Bramki odwracalne i koszt kwantowy

Funkcja boolowska o n wejściach i n wyjściach (w skrócie $n*n$ funkcja) jest nazywana odwracalną, jeśli jest przekształceniem wzajemnie jednoznacznym. Dla n zmiennych istnieje $2^n!$ funkcji odwracalnych.

Bramka o n wejściach i n wyjściach (w skrócie $n*n$ bramka) jest nazywana odwracalną, jeśli realizuje $n*n$ funkcję odwracalną. Tę samą konwencję będziemy stosowali do układów. W układach odwracalnych rozgałęzienia sygnałów są zabronione, zatem $n*n$ układ jest kaskadą $k*k$ bramek odwracalnych, gdzie $k \le n$.

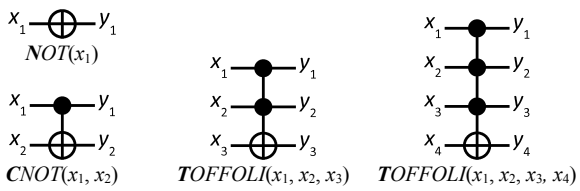
Zbiór bramek, które mogą być użyte do budowy układów jest nazywany biblioteką bramek. W niniejszej pracy omawiamy układy zbudowane z bramek biblioteki NCT (definicje w tab. 1):

- bramka NOT (inwerter) o jednym wejściu/wyjściu,
- bramka CNOT o dwóch wejściach/wyjściach,
- bramka Toffoliego o trzech wejściach/wyjściach,
- uogólniona bramka Toffoliego o n wejściach/wyjściach, n>3

Tab. 1. Definicje bramek odwracalnych N, C, T i Tn.
Tab. 1. Definition of reversible N, C, T i Tn gates.

Bramka N	Bramka C	Bramka T	Bramka Tn
$y_1 = 1 \oplus x_1$	$y_1 = x_1$ $y_2 = x_1 \oplus x_2$	$y_1 = x_1$ $y_2 = x_2$ $y_3 = x_3 \oplus x_1x_2$	$y_1 = x_1$ $y_2 = x_2$ …….. $y_n = x_n \oplus x_1x_2 \ldots x_{n-1}$

Powyższe bramki oznaczane są w skrócie jako N, C, T i T*n*. Ich symbole graficzne stosowane w literaturze podaje rys. 1.



Rys. 1. Graficzne reprezentacje bramek odwracalnych z biblioteki NCT
Fig. 1. Pictorial representations of reversible gates from NCT library

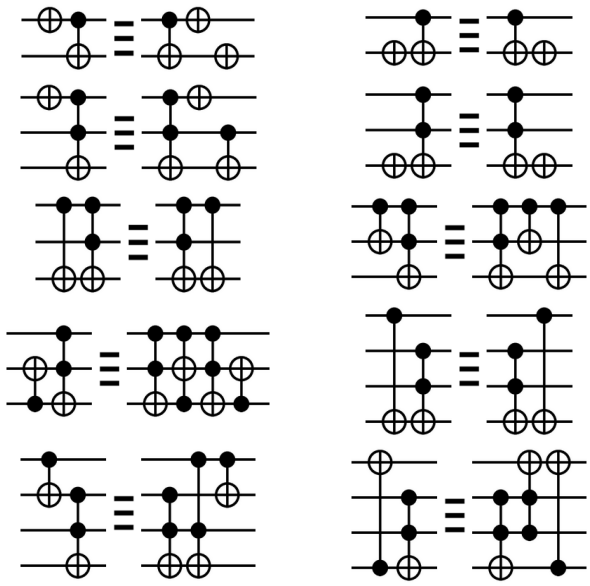
Wejścia, z których sygnały przechodzą bez zmiany na wyjścia o tych samych numerach, nazywane są wejściami sterującymi (dla definicji z tab. 1 są to: x_1 w bramce CNOT, x_1 i x_2 w bramce T, x_1, x_2 i x_3 w bramce T4). Te wyjścia, na których sygnały mogą zmienić się pod wpływem sygnałów na wejściach sterujących, nazywane są wyjściami sterowanymi (y_2 w bramce CNOT, y_3 w bramce T, y_4 w bramce T4).

Dla każdej funkcji odwracalnej istnieje wiele implementujących ją układów odwracalnych. Do oceny jakości układów stosowane są funkcje kosztu. Najprostszą jest liczba bramek w układzie, tzw. koszt bramkowy (ang. Gate Count, w skrócie GC). 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 N, C, T i T4 wynosi odpowiednio 1, 1, 5 i 13. Układ nazywamy optymalnym dla danej funkcji odwracalnej, jeśli ma najmniejszy koszt spośród wszystkich implementacji tej funkcji. Zbiór układów optymalnych zależy od funkcji kosztu i biblioteki bramek.

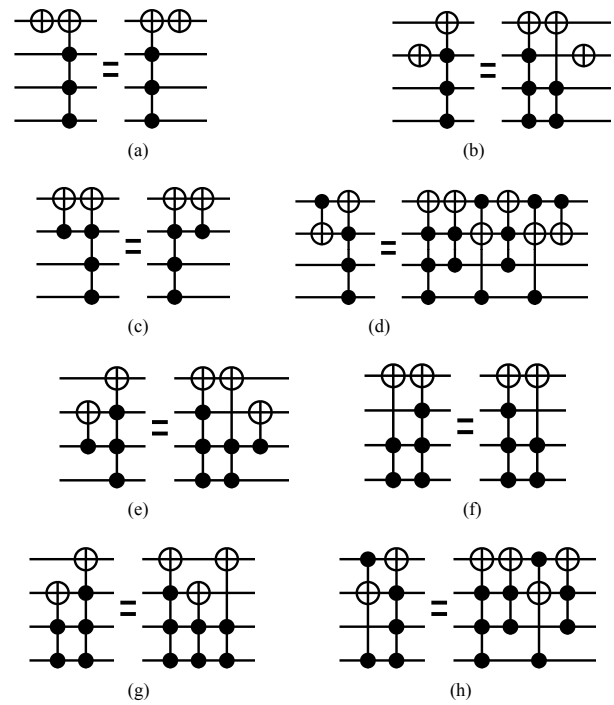
3. Nowe reguły przesuwania bramek

Reguły przesuwania bramek w układach odwracalnych zostały po raz pierwszy zaproponowane w [4]. W pracy tej chodziło o takie pogrupowanie bramek, które autorzy nazwali postacią kanoniczną, licząc na to, że przyda się ona do syntezy układów kwantowych. Nadzieje te nie spełniły się, ale koncepcja grupowania bramek została wkrótce potem uogólniona i wykorzystana w [5] do analizy możliwości dekompozycji układów odwracalnych na bloki, tzn. ciągi bramek zawierające bramki jednego rodzaju (N, C lub T). Reguły przesuwania bramek N, C i T stosowane w [5] do układów o 2, 3 i 4 wejściach przedstawione są na rys. 2. Wkrótce potem większy zbiór takich reguł zastosowany został w [6] do redukcji liczby bramek w redundancyjnych układach, które generował transformacyjny algorytm syntezy układów odwracalnych sformułowany w tej publikacji. Pary równoważnych układów nazwane zostały w niej wzorcami (ang. templates). Później zbiory wzorców były stopniowo rozszerzane na układy o większej liczbie wejść/wyjść i uogólniane na inne biblioteki bramek, a ostatnio także na układy kwantowe [7].

Zauważyliśmy, że analogiczne reguły przesuwania bramek wzdłuż układu odwracalnego mogą być stosowane także do bramek T*n* dla n>3. Najpierw opracowaliśmy zbiór reguł dla bramek T4, które podane są na rys. 3 (niektóre z nich były publikowane wcześniej, ale nie były stosowane do redukcji kosztu kwantowego). Jest to zbiór podstawowy, gdyż każdą z reguł można przekształcić na równoważną przez permutowanie linii i/lub odbicie zwierciadlane układu. Zbiór ten umożliwia redukcję liczby bramek T4, które mają znacznie większy koszt kwantowy niż bramki N, C i T. Mianowicie, dzięki tym regułom każdą parę najbliższych bramek T4 można tak przesunąć, aby stały się sąsiednimi, zaś parę jednakowych sąsiednich bramek można usunąć, bo jest równoważna przekształceniu identycznościowemu.

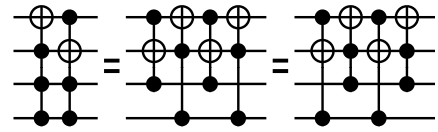


Rys. 2. Reguły przesuwania bramek odwracalnych z pracy [5]
Fig. 2. Moving rules for gates in reversible circuits from paper [5]

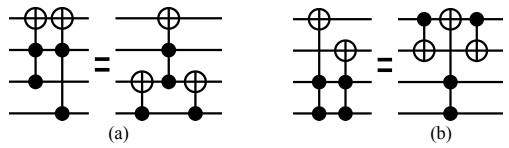


Rys. 3. Reguły przesuwania bramki T4 w 4*4 układach odwracalnych
Fig. 3. Moving rules for gate T4 in 4*4 reversible circuits

Parę różnych bramek T4 (QC=26) można przekształcić na cztery bramki T (QC=20), zgodnie z regułami z rys. 4, uzyskując zmniejszenie kosztu kwantowego układu o 6 jednostek. Poza tym, każdą parę sąsiednich bramek T (QC=10) można przekształcić na układ z jedną bramką T i dwiema bramkami C (QC=7), zmniejszając w ten sposób QC o 3 jednostki.



Rys. 4. Reguły przekształcania dwóch różnych bramek T4 na 4 bramki T
Fig. 4. Rules for transforming two different T4 gates into 4 T gates



Rys. 5. Reguły przekształcania 2 bramek T na 1 bramkę T i dwie bramki C
Fig. 5. Rules for transforming two T gates to one T gate and two C gates

Reguły podane na rys. 3-5 uogólniliśmy na przypadek przekształcania $n*n$ układów odwracalnych dla $n>4$. Lista tych reguł jest podana w wersji opisowej w tab. 2 (reguły nr 1-11 dotyczą przesuwania bramek Tn, zaś reguła nr 12 umożliwia przekształcenie par różnych sąsiednich bramek Tn na cztery bramki Tn-1). Łatwo można sprawdzić, że układy po obydwu stronach reguł są równoważne.

Tab. 2. Uogólnione reguły przesuwania bramek w układach odwracalnych
Tab. 2. Generalized rules for moving gates in reversible circuits

Reguła 1 $N(x_n)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ N(x_n)$

Reguła 2 $N(x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1},\ x_n)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-1};\ x_n)\ N(x_1)$

Reguła 3 $C(x_1;\ x_n)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ C(x_1;\ x_n)$

Reguła 4 $C(x_2;\ x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-1};\ x_n)\ C(x_2;\ x_1)$

Reguła 5 $C(x_n;\ x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-3},x_{n-1};\ x_1)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-3},x_{n-1};\ x_1)\ C(x_n;\ x_1)$

Reguła 6* $Tm(x_1,x_2,\ldots,x_{m-1};\ x_n)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tm(x_1,x_2,\ldots,x_{m-1};\ x_n)$

Reguła 7* $Tm(x_2,\ldots,x_m;\ x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-1};\ x_n)\ Tm(x_2,\ldots,x_m;\ x_1)$

Reguła 8* $Tm(x_2,\ldots,x_{m-1},x_n;\ x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-2},x_n;\ x_1)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-2},x_n;\ x_1)\ Tm(x_2,\ldots,x_{m-1},x_n;\ x_1)$

Reguła 9 $Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)$

Reguła 10 $Tn\text{-}1(x_2,\ldots,x_{n-1};\ x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-1};\ x_1)$

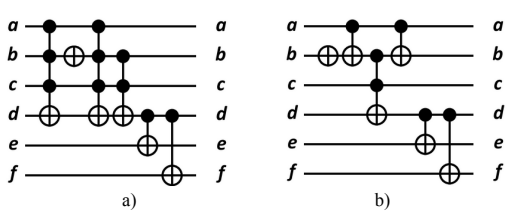
Reguła 11 $Tn\text{-}1(x_2,\ldots,x_{m-1},x_n;\ x_1)\ Tn(x_1,x_2,\ldots,x_{n-1};\ x_n) \Leftrightarrow Tn(x_1,x_2,\ldots,x_{n-1};\ x_n)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)\ Tn\text{-}1(x_2,\ldots,x_{n-3},x_{n-1};\ x_1)\ Tn\text{-}1(x_1,x_2,\ldots,x_{n-2};\ x_n)$

Reguła 12 $Tn(x_2,\ldots,x_n;\ x_1)\ Tn(x_1,x_3,\ldots,x_n;\ x_2) \Leftrightarrow Tn\text{-}1(x_1,x_3,\ldots,x_{n-1};\ x_2)\ Tn\text{-}1(x_2,\ldots,x_{n-2},x_n;\ x_1)\ Tn\text{-}1(x_1,x_3,\ldots,x_{n-1};\ x_2)\ Tn\text{-}1(x_2,\ldots,x_{n-2},x_n;\ x_1)$

*Reguły 6-8 mogą być stosowane tylko wtedy, gdy $m < n$-1.

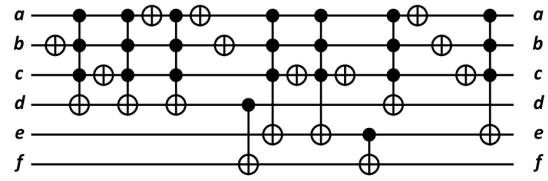
4. Przykłady

Pierwszy przykład wybraliśmy z pracy [8], której autorzy najpierw zaprojektowali układ odwracalny o QC=66, a następnie zastosowali swoją metodę redukcji kosztu kwantowego, uzyskując układ o QC=34 podany na rys. 6a. Stosując nasz zbiór reguł można ten układ przekształcić do podanego na rys. 6b mającego QC=10 (redukcja o 71%).

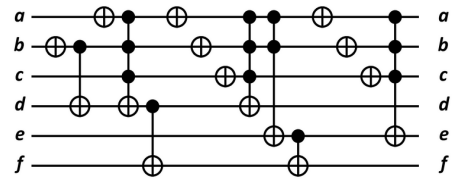


Rys. 6. a) układ z pracy [8] (QC=34), b) po naszej redukcji (QC=10)
Fig. 6. a) circuit from [8] (QC=34), b) after our reduction (QC=10)

W drugim przykładzie (rys. 7 i 8) uzyskaliśmy redukcję QC o 47%.



Rys. 7. Układ odwracalny z pracy [9] (QC=103)
Fig. 7. Reversible circuit from [9] (QC=103)



Rys. 8. Układ odwracalny z pracy [9] po naszej redukcji (QC=55)
Fig. 8. Reversible circuit from [9] after our reduction (QC=55)

5. Podsumowanie

Przedstawiliśmy nowy zbiór reguł przesuwania bramek w układach odwracalnych. Różni się on od wcześniej opracowanych reguł tym, że w naszym zbiorze każda reguła pozwala na redukcję kosztu kwantowego, podczas gdy w innych zbiorach reguły służyły do zmniejszania liczby bramek, co czasami zwiększa koszt kwantowy. Wykorzystując zaproponowany przez nas zbiór reguł przesuwania bramek przeprowadziliśmy redukcję kosztu kwantowego w układach znanych z literatury, które zostały zaprojektowane różnymi metodami, uzyskując w wielu przypadkach znaczną redukcję kosztu kwantowego (do 83%).

6. Literatura

[1] De Vos A.: Reversible Computing. Fundamentals, Quantum Computing and Applications. Wiley-VCH, Berlin 2010.
[2] Szyprowski M., Kerntopf P.: Realizacje układów odwracalnych w technologiach półprzewodnikowych. Pomiary Automatyka Kontrola, vol. 57, nr 8, ss. 911-913, 2011.
[3] Iwama K., Kambayashi Y., Ymashita S.: Transformation Rules for Designing CNOT-based Quantum Circuits. Proc. Design Automation Conf., pp. 419-424, 2002.
[4] Shende V.V., Prasad A.K., Markov I.L., Hayes J.P.: Synthesis of Reversible Logic Circuits. IEEE Trans. on CAD, vol. 22, pp.710-722, 2003.
[5] Miller D.M., Maslov D., Dueck G.W.: A Transformation Based Algorithm for Reversible Logic Synthesis. Proc. Design Automation Conf., pp. 318-323, 2003.
[6] Rahman M.M., Dueck G.W.: Properties of Quantum Templates. R. Glück, T. Yokoyama (eds.) Reversible Computation, vol. 7581, pp. 125-137, Springer-Verlag, Berlin Heidelberg, 2013.
[7] Nayeem N.M., Rice J.E.: A Shared-Cube Approach to ESOP-Based Synthesis of Reversible Logic. Facta Universitatis, Series: Electronics and Energetics, vol. 24, pp. 385-402, 2011.
[8] Sanaee Y., Dueck G.W.: Generating Toffoli Networks from ESOP Expresions. Proc. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 715-719, 2009.

otrzymano / received: 09.05.2013
przyjęto do druku / accepted: 03.07.2013 *artykuł recenzowany / revised paper*