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

Metody konstrukcji optymalnych układów odwracalnych

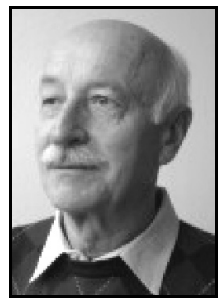
Mgr inż. Marek SZYPROWSKI

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 oraz w Katedrze Fizyki Teoretycznej i Informatyki na Wydziale Fizyki i Informatyki Teoretycznej Uniwersytetu Łódzkiego. Zainteresowania naukowe: synteza układów logicznych, układy odwracalne, układy kwantowe, binarne i wielowartościowe diagramy decyzyjne.



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

Streszczenie

Dopiero w 2010 roku, po całej dekadzie badań, opracowano pierwszą metodę syntezy optymalnych układów odwracalnych dla dowolnych funkcji czterech zmiennych. Układy te budowane były ze standardowej biblioteki bramek odwracalnych NCT, mających wyłącznie tzw. pozytywne sterowanie. W pracy opisujemy wyniki naszych rozszerzeń tej metody na przypadek minimalizowania kosztu kwantowego dla układów o zadanej liczbie bramek, a także na układy budowane z bramek NCT o mieszanym sterowaniu (tzn. zarówno o pozytywnym, jak i negatywnym).

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

Techniques for constructing optimal reversible circuits

Abstract

Synthesis of reversible logic circuits is the most intensively studied topic of reversible computation (i.e. bijective mapping). This emerging research area 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 in low power computation. Recent advances consist in reducing numbers of gates, garbage bits or quantum cost. Synthesis of optimal reversible circuits is a very hard problem even for small input/output circuits. In 2010 a method for construction of 4-input/output optimal circuits was developed for circuits constructed using reversible gates from NCT library [5]. In the paper we present a summary of the results of our extensions to this method. We have developed an approach for minimization of quantum cost of the 4-input/output circuits [7]. Our computational experiments have been conducted for two sets of reversible gates: a standard NCT library and extended mixed-polarity NCT library, which consists of gates with both positive and negative control lines. Using our tools we have found circuits for the known reversible benchmarks which have lower quantum cost than any of the best known implementations so far. Based on the data of our experiments we have made a statistical comparison of the optimal circuits built from standard NCT and mixed-polarity NCT libraries.

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, 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 innych 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. Na przykład, w klasycznych technologiach półprzewodnikowych CMOS [2] zbudowano m.in. eksperymentalne procesory odwracalne oraz rozmaite układy arytmetyczne [1], zaś w toku są prace nad budową odwracalnego mikroprocesora w technologii CMOS we współpracy uniwersytetów w Gandawie i Kopenhadze. Z drugiej strony, układy kwantowe, które ze swej natury pracują w sposób odwracalny, umożliwiłyby wykładnicze przyspieszenie obliczeń dla wielu ważnych zastosowań, np. faktoryzacji dużych liczb naturalnych i obliczania logarytmów dyskretnych [3].

Z punktu widzenia projektowania układów kwantowych istotne jest rozwiązanie problemu projektowania układów odwracalnych, które są podklasą układów kwantowych [4]. 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. Nawet dla bramek z pozytywnym sterowaniem problem konstruowania optymalnych układów pod względem liczby bramek dopiero niedawno został rozwiązany dla układów o czterech wejściach i wyjściach [5]. Dzięki opracowanym przez nas narzędziom, po raz pierwszy w literaturze problem ten rozwiązaliśmy dla przypadku minimalizacji kosztu kwantowego oraz dla bramek z tzw. sterowaniem mieszanym. Prace te mają bardzo ważne znaczenie dla znalezienia lepszych niż dotychczas benchmarków, które pozwolą na bardziej wiarygodne testowanie algorytmów projektowania układów odwracalnych.

W niniejszej pracy przedstawiamy wyniki konstrukcji optymalnych odwracalnych układów o czterech wejściach i wyjściach dla różnych funkcji kosztu, jak również dla różnych bibliotek bramek odwracalnych. Podstawowe pojęcia z dziedziny syntezy układów odwracalnych czytelnik znajdzie w [1, 2], zaś dalsze informacje o układach kwantowych – w monografii [4].

2. Minimalizacja układów o 4 wejściach

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. Zatem, dla dwóch zmiennych istnieją 24 (4!) takie funkcje, dla trzech zmiennych jest ich 40320 (8!), a dla czterech zmiennych ponad $2 \cdot 10^{13}$ (16!).

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 $k \leq n$.

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,
- bramka Toffoliego o czterech wejściach/wyjściach.

Powyższe bramki oznaczane są w skrócie jako N, C, T3 i T4.

Tab. 1. Definicje bramek odwracalnych N, C, T3 i T4
Tab. 1. Definition of reversible N, C, T3 and T4 gates

NOT	CNOT	Bramka T3	Bramka T4
$y_1 = 1 \oplus x_1$	$y_1 = x_1$ $y_2 = x_1 \oplus x_2$	$y_1 = x_1$ $y_2 = x_2$ $y_3 = x_3 \oplus x_1x_2$	$y_1 = x_1$ $y_2 = x_2$ $y_3 = x_3$ $y_4 = x_4 \oplus x_1x_2x_3$

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 T3, 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 T3, y_4 w bramce T4). O bramkach z tabeli 1 mówi się, że mają wejścia sterujące pozytywne. W literaturze rozpatrywane są również wejścia bramek ze sterowaniem negatywnym (w których we wzorach definiujących funkcje wyjściowe wszystkie wejścia występują w postaci zanegowanej w stosunku do wzorów z tab. 1) oraz mieszanym (ang. *gates with mixed-polarity control*), gdy tylko część linii sterujących jest zanegowana.

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 (GC). Najczęściej stosowaną jest tzw. koszt kwantowy (QC), odpowiadający minimalnej liczbie elementarnych bramek kwantowych, użytych do budowy danego układu. Przyjmuje się [8], że koszt kwantowy bramek N, C, T3 i T4 wynosi odpowiednio 1, 1, 5 i 13, zarówno dla sterowania pozytywnego jak i mieszanego, zaś dla sterowania negatywnego jest o jeden większy [11, 12]. 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 narzędzia do optymalizacji układów

W pracy [5] po raz pierwszy zaproponowana została metoda konstruowania układów optymalnych dla dowolnych funkcji czterech zmiennych. Metoda ta jest pewną formą algorytmu typu brute-force, jednak nawet rozwiązanie tego problemu dla funkcji czterech zmiennych wymagało zastosowania zaawansowanych pomysłów algorytmicznych, aby wykonać przeszukiwanie na współczesnych komputerach.

Jednym z najważniejszych pomysłów zaproponowanego rozwiązania jest optymalizacja danych przechowywanych w pamięci komputera. Autorzy zauważyli, że układy odwracalne można pogrupować w klasy równoważności względem jednoczesnej zmiany (permutacji) nazw zmiennych wejściowych i wyjściowych oraz zmianę kolejności bramek na odwrotną. Dzięki tej obserwacji w pamięci przechowywana jest informacja tylko o jednym, wybranym reprezentancie klasy, co redukuje problem prawie 48 razy (4! = 24 możliwych permutacji nazw zmiennych oraz możliwość odwrócenia porządku bramek).

Kluczową rolę w działaniu opisanego w [5] algorytmu odgrywa to, że układy optymalne mogą być skonstruowane z dwóch części, z których każda również jest optymalna. Dzięki temu, konstruując bazę optymalnych układów dla funkcji wymagających k bramek, można znajdować układy dla funkcji wymagających $2k$ bramek – poprzez złożenie odpowiednich par układów z już istniejącej bazy.

Ważną rolę odgrywa również zwarty sposób przechowywania informacji o analizowanych układach w pamięci komputera. Autorzy zaproponowali, aby funkcja odwracalna czterech zmiennych była zapisana jako liczba 64-bitowa, przy czym wartości kolejnych wierszy tabeli prawdy zapisane są w kolejnych czwórkach bitów. Dla takiego zapisu możliwe jest bardzo szybkie wykonanie operacji złożenia funkcji oraz znalezienie funkcji odwrotnej. Analizowane funkcje zapisywane są w tablicach mieszających, osobnych dla różnych długości układów odwracalnych. Autorzy prac [5, 6] pokazali, że ich algorytm jest w stanie znaleźć układy optymalne pod względem liczby bramek dla znanych odwracalnych benchmarków czterech zmiennych. Obliczenia wymagały zbudowania bazy optymalnych układów do 8 bramek włącznie. Taka baza zajmuje w pamięci ponad 2GiB.

W naszych pracach nad syntezą układów odwracalnych wykorzystaliśmy zaproponowaną metodę do optymalizacji kosztu kwantowego. Ponieważ ze względu na ograniczony rozmiar pamięci współczesnych komputerów nie jest możliwe skonstruowanie analogicznej bazy dla układów optymalnych pod względem kosztu kwantowego, postanowiliśmy wykorzystać bazy skonstruowane wcześniej dla kosztu bramkowego. W pracy [7] pokazaliśmy, jak wykonując algorytm pełnego przeszukiwania takich baz skonstruować wszystkie istniejące układy optymalne o zadanej liczbie bramek. Następnie wśród tak znalezionych układów wybierany był układ o najmniejszym koszcie kwantowym. Liczba bramek poszukiwanego układu była sukcesywnie zwiększana, gdyż układy optymalne pod względem kosztu kwantowego mają więcej bramek niż układy dla tych samych funkcji, ale optymalne pod względem liczby bramek. Mimo prostoty, algorytm ten pozwolił na zredukowanie kosztu kwantowego dla znanych benchmarków średnio o 44,7% [7, 8].

W kolejnych pracach nad rozszerzeniem algorytmu syntezy optymalnych układów odwracalnych dla funkcji czterech zmiennych rozszerzyliśmy dostępną bibliotekę bramek odwracalnych. W pracy [7] używana była standardowa biblioteka bramek NCT, sterowanych pozytywnie. Po drobnych zmianach w algorytmie możliwe było skonstruowanie bazy optymalnych układów dla biblioteki bramek NCT, ale sterowanych sygnałami mieszanymi. Zwiększenie liczby dostępnych bramek odwracalnych spowodowało również wzrost rozmiaru bazy optymalnych układów: np. tablica mieszająca zawierająca funkcje posiadające układ optymalny z siedmiu bramek NCT sterowanych pozytywnie zajmuje 128MiB, zaś analogiczna tablica mieszająca dla bramek ze sterowaniem mieszanym – 32 GiB.

4. Nasze wyniki

W tab. 2 zestawione są wyniki przeprowadzonych przez nas eksperymentów obliczeniowych. W kolumnie I podane są nazwy benchmarków [9, 10]. Kolumna II zawiera zebrane z literatury wartości kosztu bramkowego (GC) i kwantowego (QC) dla znanych układów o najmniejszej liczbie bramek. Kolumny III i IV zawierają wartości GC oraz QC dla wygenerowanych przez nas układów przy założeniu optymalizacji kosztu kwantowego (III) oraz kosztu bramkowego (IV). Wszystkie układy opisane w kolumnach II-IV konstruowane są tylko z bramek NCT ze sterowaniem pozytywnym. W kolumnie V podane są wartości GC i QC dla wygenerowanych układów zbudowanych z bramek NCT z mieszanym sterowaniem (w skrócie m-NCT).

Porównując kolumny II z III i IV, widać, że za pomocą naszych narzędzi skonstruowane zostały układy o lepszych parametrach kosztu niż znane z literatury. Z porównania kolumn III i IV widać wyraźnie, że układy o mniejszym koszcie kwantowym zbudowane są z większej liczby bramek niż układy o minimalnym koszcie bramkowym. Równocześnie, porównując kolumny IV i V, można zauważyć, że rozszerzenie dostępnej biblioteki bramek odwracalnych o bramki z mieszanym sterowaniem powoduje zauważalny spadek kosztu bramkowego układów optymalnych (średnio z 11,08 do 8,23).

Tab. 2. Wartości kosztu układów odwracalnych dla znanych benchmarków
Tab. 2. Cost values of reversible circuits for known benchmarks

I	II		III		IV		V	
benchmark	**literatura (NCT) [9,10]**		**opt. QC (NCT)**		**opt. GC (NCT)**		**opt. GC (m-NCT)**	
	GC	**QC**	**GC**	**QC**	**GC**	**QC**	**GC**	**QC**
4b15g_1	15	47	15	39	15	39	11	48
4b15g_2	15	61	15	31	15	31	11	37
4b15g_3	15	53	15	33	15	33	11	37
4b15g_4	15	47	15	35	15	35	11	46
4b15g_5	15	43	15	31	15	31	10	37
nth_prime4_inc	15	51	14	26	11	53	8	56
4_49	12	32	14	28	12	30	9	30
decode42	10	30	10	28	10	28	6	39
hwb4	11	21	13	19	11	21	10	22
imark	7	19	9	17	7	19	6	19
mperk	9	15	9	13	9	13	8	17
oc5	11	39	12	34	11	39	9	38
oc6	12	42	13	37	12	38	9	38
oc7	13	41	14	34	13	35	10	41
oc8	12	48	13	35	12	40	9	43
primes4	10	42	12	22	10	42	8	33
mini_alu	6	62	8	16	6	30	6	30
aj_e11	10	30	10	28	10	28	6	39
mod10_171	10	56	12	32	9	53	5	46
mod10_176	7	41	9	21	7	35	5	33
4_49+hwb4	12	30	14	26	12	28	9	34
msaee	16	72	14	34	12	40	9	43
gyang	19	103	14	36	10	52	5	50
dmasl	16	128	10	24	9	25	7	31
App2.2	18	102	13	35	11	39	9	38
App2.11	14	82	12	26	9	45	7	32
średnia:	**12,50**	**51,42**	**12,46**	**28,46**	**11,08**	**34,69**	**8,23**	**36,81**

Zbadaliśmy też zmiany parametrów kosztu bramkowego dla ważnej klasy liniowych układów odwracalnych w zależności od użytej biblioteki bramek (NCT oraz m-NCT, tab. 3).

Tab. 3. Liczba optymalnych układów o danej liczbie bramek dla wszystkich odwracalnych funkcji liniowych.
Tab. 3. Number of optimal circuits for the given number of gates for all linear affine 4-bit functions.

Liczba bramek	NCT [6]	m-NCT
0	1	1
1	16	28
2	162	438
3	1206	4340
4	6589	25761
5	26182	82680
6	72062	129016
7	118424	71096
8	84225	9104
9	13555	96
10	138	
Średnia długość układu:	6,88	5,82

5. Podsumowanie

Przedstawiliśmy rozszerzenia wcześniej zaprezentowanego podejścia do rozwiązania problemu minimalizacji układów o czterech wejściach. Pierwsze rozszerzenie dotyczy minimalizacji kosztu kwantowego. Następnie obydwa powyżej wspomniane problemy zostały zastosowane do układów budowanych z bramek ze sterowaniami mieszanymi (tzn. z pozytywnymi i negatywnymi zmiennymi sterującymi). Tego rodzaju rozszerzenia zostały zaproponowane po raz pierwszy w literaturze. Wykorzystując stworzone narzędzia programowe przeprowadziliśmy szereg eksperymentów obliczeniowych, których efektem są ulepszone układy dla znanych benchmarków. Obliczenia te potwierdziły, jak złożonym problemem jest optymalizacja układów odwracalnych.

Praca była wykonana w ramach realizacji grantu MNiSzW nr 4180/B/T02/2010/38.

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] Shor P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. of Computing, vol. 26, pp.1484-1509, 1997.
[4] Nielsen M., Chuang I.: Quantum Computation and Quantum Information. Cambridge University Press 2000.
[5] Golubitsky O., Falconer S.M., Maslov D.: Synthesis of the optimal 4-bit reversible circuits. Design Automation Conf., pp. 653-656, 2010.
[6] Golubitsky O., Maslov D.: A study of optimal 4-bit reversible Toffoli circuits and their synthesis. IEEE Trans. on Computers, 2012, accepted, dostępny jako arXiv:1103.2686.
[7] Szyprowski M., Kerntopf P.: Reducing quantum cost in reversible Toffoli circuits, Proc. 10th International Reed-Muller Workshop, pp. 127-136, 2011.
[8] Szyprowski M., Kerntopf P.: An approach to reducing quantum cost in reversible circuits, Proc. 11th IEEE International Conference on Nanotechnology, pp. 1521-1526, 2011.
[9] Maslov D.: Reversible Logic Synthesis Benchmarks Page, http://www.cs.uvic.ca/~dmaslov.
[10] Wille R., Grosse D., Teuber L., Dueck G. W. and Drechsler R., RevLib: An online resourse for reversible functions and reversible circuits, http://www.revlib.org.
[11] Markov I.L., Saeedi M.: Constant-optimized quantum circuits for modular multiplication and exponentiation, arXiv:1202.6614, 2012.
[12] Maslov D., Saeedi M.: Reversible circuit optimization via leaving the Boolean domain, IEEE Trans. on CAD, vol. 30, pp. 806-816, 2011.

otrzymano / received: 26.04.2012
przyjęto do druku / accepted: 01.06.2012 *artykuł recenzowany / revised paper*