Marek SZYPROWSKI, Paweł KERNTOPF
POLITECHNIKA WARSZAWSKA, WYDZIAŁ ELEKTRONIKI I TECHNIK INFORMACYJNYCH, INSTYTUT INFORMATYKI

Porównanie efektywności heurystycznych miar złożoności odwracalnych funkcji boolowskich

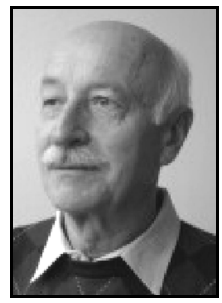
Mgr inż. Marek SZYPROWSKI

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, których synteza stanowiła 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 PW w Instytucie Informatyki na tym Wydziale. Jego zainteresowania naukowe to synteza układów logicznych, odwracalne układy logiczne, kwantowe układy logiczne, binarne i wielowartościowe diagramy decyzyjne oraz logiki wielowartościowe.



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

Streszczenie

Funkcja boolowska jest nazywana odwracalną, gdy jest wzajemnie jednoznaczna. W literaturze zaproponowano kilka heurystyk służących do syntezy odwracalnych układów logicznych, jednak do tej pory nie znaleziono rozwiązania, które dawałoby zadowalające wyniki. Przy pracach nad ulepszaniem tych algorytmów potrzebne jest dobre kryterium oceny jakości poszczególnych heurystyk. W pracy pokazano jak wykorzystać bazę optymalnych układów odwracalnych do oceny działania heurystyk oraz przedstawiono wyniki obliczeń pozwalających na porównanie ich efektywności.

Słowa kluczowe: odwracalne układy logiczne, miary złożoności funkcji odwracalnych.

Comparison of Heuristic Complexity Measure Quality for Reversible Boolean Functions

Abstract

A Boolean logic function is reversible if it is a bijective mapping. Synthesis of such functions is motivated by advances in quantum computing, nanotechnologies and low power design. Several heuristic synthesis algorithms has been proposed, but so far none of them produces circuits of good quality in acceptable time. All of them are based on exploration of the search tree guided by a complexity measure function. Search for better algorithms is important and for this aim a good evaluation criterion of a heuristic complexity measure quality is needed. In this article the comparison of reversible function complexity measures known from the literature is made. Their accuracy is checked on the library of the optimal circuits of 3 inputs/outputs. The results are presented in Table 1. The numeric factor Q is introduced on the basis of calculating the probability of taking a wrong way in the search tree by a synthesis algorithm for every reversible function. This factor was calculated for five heuristic complexity measures and shown in Table 2. According to it the Reed-Muller spectrum based complexity measure gives best synthesis results, however there is still a lot of space for improvements.

Keywords: reversible logic circuits, reversible function complexity measure.

1. Wstęp

Projektowanie kombinacyjnych układów logicznych realizujących odwracalne funkcje boolowskie (tj. wzajemnie jednoznaczne) jest stosunkowo nową dziedziną. Główną motywacją do zajmowania się takimi układami są zastosowania w obliczeniach i komputerach kwantowych, nanotechnologii oraz układach o małym poborze energii. Do tej pory nie zostały jednak znalezione zadowalające rozwiązania problemu syntezy takich układów. Wśród zaproponowanych w literaturze rozwiązań istotną grupę stanowią heurystyki, mimo że najczęściej nie jest możliwe sformułowanie dowodu poprawności czy zbieżności takich algorytmów. Często jednak czas ich działania jest znacznie krótszy niż czas działania nieheurystycznych algorytmów znanych z literatury, które generują układy porównywalnej jakości. Takie algorytmy polegają bowiem na projektowaniu wieloetapowym, gdzie w pierwszym kroku znajdywany jest najczęściej układ daleki od optymalnego, a w kolejnych etapach jest on redukowany. W pracach nad ulepszaniem algorytmów heurystycznych potrzebne jest dobre kryterium oceny jakości poszczególnych heurystyk. Takie kryterium umożliwia również szybkie sprawdzanie hipotez lub modyfikacji miary złożoności bez potrzeby ponownej syntezy wszystkich testowych układów.

2. Podstawowe pojęcia

Definicja 1: Boolowska funkcja logiczna o jednakowej liczbie wejść i wyjść jest nazywana odwracalną gdy jest wzajemnie jednoznaczna.

Funkcja odwracalna realizuje permutację elementów ze swojej dziedziny. Istnieje zatem dokładnie $2^n!$ różnych boolowskich funkcji odwracalnych o n argumentach. Dla takiej funkcji możliwe jest pełne odtworzenie wartości wejściowych na podstawie wartości wyjściowych (stąd nazwa – odwracalna).

Definicja 2: Bramka logiczna jest odwracalna, gdy realizuje funkcję odwracalną (z reguły bardzo prostą).

Dla takiej bramki stan wyjść można w pełni określić na podstawie wartości wejściowych oraz odwrotnie – stan wejść można określić na podstawie tylko wartości wyjściowych.

Definicja 3: Układem odwracalnym nazywany kaskadowe połączenie dowolnej liczby bramek.

Każdy układ odwracalny realizuje pewną funkcję odwracalną. W układzie takim nie mogą występować rozgałęzienia sygnału z jednego wyjścia do wielu wejść bramek (ang. fan-out). Układ odwracalny ma z definicji taką samą liczbę wejść i wyjść.

Definicja 4: Biblioteką bramek nazywamy zbiór bramek odwracalnych, z których mogą być zbudowane układy odwracalne.

W literaturze zaproponowano wiele różnych bramek odwracalnych, jednak zdecydowana większość prac dotyczy układów zbudowanych z bramek należących do biblioteki NCT, w skład której wchodzą następujące bramki:

- **N**OT (klasyczny inwerter – jedno wejście i jedno wyjście),
- **C**NOT (sterowany inwerter – 2 wejścia i 2 wyjścia, linia sterująca przechodzi przez bramkę niezmieniona, a linia sterowana jest negowana, gdy na wejściu sterującym jest sygnał o wartości 1)
- bramka **T**offoliego (3 wejścia, w tym 2 wejścia sterujące i jedno sterowane, które jest negowane, gdy na obu wejściach sterujących wystąpią sygnały o wartości 1).

W niektórych pracach wyróżnia się jeszcze uogólnioną bramkę Toffoliego. Pierwsze n-1 sygnałów wejściowych jest przez taką bramkę przekazywane na pierwsze n-1 wyjść bez jakiejkolwiek modyfikacji. Wszystkie te sygnały są nazywane sterującymi. Wartość ostatniego, n-tego wejścia jest przekazywana na n-te wyjście w postaci zanegowanej, gdy wartość wszystkich linii sterujących wynosi 1, albo w postaci niezmienionej w przeciwnym wypadku.

3. Synteza układów odwracalnych

Schemat działania wszystkich zaproponowanych w literaturze algorytmów heurystycznych jest bardzo podobny. W każdym kolejnym kroku algorytmu wybierana jest konkretna bramka (lub bramki), która jest dołączana do aktualnej kaskady bramek, a następnie algorytm jest powtarzany dla nowej kaskady. Jeżeli po dodaniu danej bramki nie udaje się znaleźć układu realizującego zadaną funkcję odwracalną, przeprowadzana jest próba dla kolejnej bramki z biblioteki. Głównym elementem różniącym poszczególne heurystyki jest kryterium wykorzystywane przy wyborze bramek w kolejnych krokach algorytmu – nazywane miarą złożoności. Realizacja algorytmu sprowadza się do zbudowania drzewa przeszukiwań i następnie jego efektywnego przeglądania według zadanej miary złożoności.

Definicja 5: Częściową realizacją funkcji odwracalnej nazywamy dowolną kaskadę bramek, która po dodaniu kolejnych bramek odwracalnych będzie łącznie realizowała zadaną funkcję odwracalną.

Definicja 6: Funkcja resztowa to funkcja, jaką ma zrealizować układ bramek, który należy dodać do częściowej realizacji funkcji w celu uzyskania układu realizującego zadaną funkcję odwracalną.

Definicja 7: Miara złożoności to funkcja, która przyporządkowuje każdej funkcji odwracalnej pewną liczbę.

Idealna miara złożoności przyporządkowuje wartości monotonicznie malejące (lub rosnące) funkcjom resztowym po każdej kolejnej bramce odwracalnej w optymalnym układzie realizującym zadaną funkcję odwracalną oraz wartości malejące (rosnące) niemonotonicznie funkcjom resztowym po każdej kolejnej bramce dla układów realizujących zadaną funkcję odwracalną, ale nie będącymi optymalnymi według zadanych kryteriów oceny jakości układu (np. liczba bramek, czy suma kosztów wszystkich bramek w układzie).

W literaturze stosowane są następujące miary złożoności:

- **odległość Hamminga** między wierszami tabel prawdy dla funkcji resztowej i funkcji tożsamościowej [1],
- **liczba wyrazów** w opisie funkcji resztowej za pomocą wyrażeń **PPRM** (ang. Positive Polarity Reed-Muller expressions) [2],
- **rozmiar współdzielonego binarnego diagramu decyzyjnego z zanegowanymi krawędziami** (ang. Complemented-edge Shared Binary Decision Diagrams, w skrócie **diagramy CSBDD**) funkcji resztowej [3],
- **rozmiar widma Reeda-Mullera** funkcji resztowej [4].

Wartość tych miar złożoności maleje dla coraz to prostszych (wymagających mniejszej liczby bramek do ich realizacji) funkcji. W literaturze rozpatrywana była również miara złożoności oparta na **widmach Rademachera-Walsha** funkcji resztowej [5], której wartości rosną dla coraz to prostszych funkcji, dlatego przyjęliśmy jej wartości ze znakiem minus, aby móc używać w dalszej części określeń mniejsze lub większe wartości miary złożoności w tym samym znaczeniu do wszystkich rozpatrywanych miar.

4. Kryteria oceny jakości układów

Dla każdej funkcji odwracalnej istnieje wiele układów odwracalnych realizujących ją. Układy te różnią się typami oraz kolejnością występowania poszczególnych bramek odwracalnych. Żeby możliwa była ocena jakości poszczególnych układów, istnieje potrzeba zdefiniowania kosztu układu, co pozwoli ocenić, który z zaproponowanych układów jest układem optymalnym. Zakłada się, że koszt układu jest równy sumie kosztów bramek.

Koszty bramek przyjmuje się najczęściej jako wartości względne, pozwalające ocenić poziom skomplikowania każdej z bramek względem pozostałych, przy założeniu, że koszt najprostszej bramki wynosi 1. W literaturze spotyka się wiele propozycji kosztu każdej bramki dla różnych przewidywanych technologii, jednak obecnie nie można jeszcze określić, która z nich umożliwi zbudowanie rzeczywistych układów odwracalnych.

Najprostszym ze stosowanych kryteriów jest liczba bramek potrzebnych do zbudowania układu, co oznacza, że przyjmuje się taki sam koszt każdej z bramek. Jest to kryterium bardzo ogólne, jednak wydaje się być pewne, że układ zbudowany (w dowolnej technologii) z 3 bramek, będzie lepszy od układu realizującego taką samą funkcję, a zbudowanego np. z 8 bramek. Kryterium to jest często spotykane w literaturze i służy za punkt odniesienia przy porównywaniu różnych algorytmów syntezy układów odwracalnych.

Mając określone kryterium optymalności oraz bibliotekę dostępnych bramek, poprzez proste rekurencyjne przeszukiwanie wszystkich możliwych kaskad bramek odwracalnych zbudowaliśmy bazę wszystkich układów optymalnych o 3 wejściach i wyjściach (wszystkich takich układów jest 8! = 40320). Na współczesnych komputerach nie jest możliwe obliczenie takiej bazy dla układów o większej liczbie wejść i wyjść.

5. Wyniki obliczeń

Wykorzystując naszą bazę optymalnych układów dla biblioteki NCT i kosztu układu określonego liczbą bramek, wykonaliśmy obliczenia przedstawionych wcześniej miar złożoności dla wszystkich funkcji odwracalnych z tej bazy. Uzyskane wyniki (tabela 1) pokazują zależność wartości miar złożoności od kosztu optymalnego układu realizującego daną funkcję. W każdej komórce tabeli podana jest liczba funkcji, dla których układy optymalne mają długość podaną w nagłówku kolumny i wartość miary złożoności podaną w pierwszej komórce danego wiersza.

Tab. 1. Zależność wartości miar złożoności od kosztu optymalnego układu realizującego daną funkcję (biblioteka NCT)

Tab. 1. Correlation between values of complexity measures and the cost of optimal circuit realizing a given function (NCT library)

		koszt układu (liczba bramek)								
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
miara oparta na odległości Hamminga	**0**	1	0	0	0	0	0	0	0	0
	2	0	3	6	0	3	0	0	0	0
	4	0	6	15	30	24	30	9	0	0
	6	0	0	27	111	173	200	158	195	12
	8	0	3	21	147	507	1044	1191	846	96
	10	0	0	12	120	774	2160	3720	2181	129
	12	0	0	18	66	600	2799	5583	3126	220
	14	0	0	0	84	330	1650	4338	2598	96
	16	0	0	3	42	219	774	1689	1104	24
	18	0	0	0	12	132	180	349	203	0
	20	0	0	0	12	6	84	12	0	0
	22	0	0	0	0	12	0	0	0	0
	24	0	0	0	1	0	0	0	0	0
miara oparta na widmach Rademachera-Walsha	**-456**	1	3	3	4	12	9	2	14	0
	-452	0	6	30	42	30	78	102	0	0
	-448	0	0	12	87	183	225	69	0	0
	-444	0	0	6	42	90	108	42	0	0
	-440	0	0	0	12	78	54	0	0	0
	-380	0	3	21	63	78	180	129	102	0
	-378	0	0	6	48	126	108	258	30	0
	-376	0	0	12	90	216	342	456	36	0
	-374	0	0	0	21	210	531	366	24	0
	-370	0	0	0	12	114	288	150	12	0
	-308	0	0	0	3	39	141	237	156	0
	-306	0	0	6	60	258	570	912	480	18
	-304	0	0	6	84	534	1350	1950	684	0
	-302	0	0	0	12	144	684	1044	420	0
	-300	0	0	0	12	156	750	1206	180	0
	-234	0	0	0	0	32	476	2090	1891	119
	-232	0	0	0	12	165	1086	3810	3837	306
	-230	0	0	0	6	153	1284	3312	2037	120
	-228	0	0	0	15	162	657	914	350	14
miara oparta na diagram. CSBDD	**0**	1	6	20	40	58	83	66	14	0
	1	0	4	34	132	254	361	231	40	0
	2	0	2	31	193	573	1040	1085	244	0
	3	0	0	14	172	944	2297	3092	1052	13
	4	0	0	3	62	510	1980	3484	1952	73
	5	0	0	0	25	399	2679	7316	5496	405
	6	0	0	0	1	39	445	1605	1286	80
	7	0	0	0	0	3	36	170	169	6

Tab. 1. ciąg dalszy
Tab. 1. continued

		koszt układu (liczba bramek)								
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
miara oparta na liczbie składników wyrażenia PPRM	**3**	1	0	0	3	0	0	2	0	0
	4	0	12	6	0	30	12	6	6	0
	5	0	0	54	54	51	93	48	24	0
	6	0	0	42	145	156	303	174	50	0
	7	0	0	0	258	399	405	594	126	0
	8	0	0	0	102	606	915	951	330	12
	9	0	0	0	51	800	1332	1587	574	36
	10	0	0	0	12	426	2001	2568	1335	84
	11	0	0	0	0	228	2049	3546	2007	108
	12	0	0	0	0	66	1050	3605	2559	160
	13	0	0	0	0	12	579	2346	1965	102
	14	0	0	0	0	6	144	1122	912	66
	15	0	0	0	0	0	32	378	274	6
	16	0	0	0	0	0	6	90	81	3
	17	0	0	0	0	0	0	30	6	0
	18	0	0	0	0	0	0	2	4	0
miara oparta na rozmiarze widma Reeda-Mullera	**0**	1	0	0	0	0	0	0	0	0
	1	0	12	0	0	0	0	0	0	0
	2	0	0	54	0	0	0	0	0	0
	3	0	0	48	103	0	0	0	0	0
	4	0	0	0	288	75	0	0	0	0
	5	0	0	0	126	564	57	0	0	0
	6	0	0	0	78	821	471	72	0	0
	7	0	0	0	30	513	1653	324	24	0
	8	0	0	0	0	498	1935	1449	96	0
	9	0	0	0	0	171	1845	2972	450	0
	10	0	0	0	0	90	1500	3462	1194	0
	11	0	0	0	0	36	657	3309	2112	48
	12	0	0	0	0	6	494	2393	2269	120
	13	0	0	0	0	6	189	1476	1911	174
	14	0	0	0	0	0	78	981	1071	108
	15	0	0	0	0	0	24	383	689	64
	16	0	0	0	0	0	12	153	312	24
	17	0	0	0	0	0	6	54	78	36
	18	0	0	0	0	0	0	18	34	0
	19	0	0	0	0	0	0	0	12	3
	20	0	0	0	0	0	0	3	0	0
	21	0	0	0	0	0	0	0	1	0

6. Ocena jakości heurystyk

Dla idealnej miary złożoności spełniona powinna być proporcjonalna zależność wartości miary złożoności funkcji od kosztu układu optymalnego realizującego daną funkcję. Oznacza to, że w częściach tabeli 1 odpowiadających poszczególnym miarom złożoności większość funkcji powinna znajdować się blisko przekątnej przechodzącej z lewego górnego do prawego dolnego rogu.

Jakość poszczególnych heurystyk można dokładniej ocenić na podstawie liczby funkcji, dla których algorytm syntezy będzie wybierał nieprawidłową gałąź w drzewie przeszukiwań. Dla funkcji odwracalnej o koszcie równym i oraz złożoności j prawdopodobieństwo wybrania błędnej ścieżki w drzewie przeszukiwań wynosi:

$$P_{i,j} = \frac{\left\| S\left(C\left(f\right) < i\right) \cap S\left(V\left(f\right) < j\right) \right\|}{\left\| S\left(V\left(f\right) < j\right) \right\|} \qquad (1)$$

gdzie $C(f)$ – koszt optymalnego układu dla funkcji f, $V(f)$ – miara złożoności funkcji f, $S(w)$ – zbiór wszystkich funkcji spełniających warunek w, $\|\ \|$ – moc zbioru.

Prawdopodobieństwo to obliczane jest na podstawie liczby niepoprawnych dróg (tj. takich, dla których wartość miary złożoności maleje, a optymalny układ ma większy koszt) oraz liczby wszystkich możliwych ścieżek w danym węźle drzewa przeszukiwań (tj. wszystkich funkcji o mniejszej wartości miary złożoności).

Licząc średnią arytmetyczną prawdopodobieństw P dla wszystkich funkcji odwracalnych uzyskuje się współczynnik Q, który określa jakość danej heurystyki. Dla idealnej miary złożoności (ściśle monotoniczna zależność między wartością miary złożoności a kosztem funkcji) współczynnik ten wynosi zero. W tabeli 2 znajdują się wartości współczynnika Q obliczone dla analizowanych heurystycznych miar złożoności.

Tab. 2. Wartości współczynnika Q dla pięciu heurystycznych miar złożoności
Tab. 2. Values of the Q factor for five heuristic complexity measures

Miara złożoności	**Współczynnik Q**
odległość Hamminga	0,5685
rozmiar widma Rademachera-Walsha	0,5199
liczba składników wyrażeń PPRM	0,4986
rozmiar diagramu CSBDD	0,4930
rozmiar widma Reeda-Mullera	0,3807

7. Wnioski

Dla poprawnego działania heurystycznych algorytmów syntezy istotne jest, aby w tabeli 1 nie występowały komórki, odpowiadające małej mierze złożoności i dużemu kosztowi optymalnego układu. Istnienie takich przypadków powoduje, że algorytm, który podczas syntezy jest kierowany tylko wartościami miary złożoności, będzie generował układy znacznie dłuższe od optymalnych lub nawet może w ogóle nie odnaleźć układu realizującego zadaną funkcję.

Z praktycznego punktu widzenia dobrze jest również, gdy miara złożoności posiada możliwie dużo wartości, bowiem może to wpłynąć w znacznym stopniu na ograniczenie drzewa przeszukiwań. Natomiast, gdy miara złożoności ma mało wartości, wówczas może okazać się, że istnieje bardzo dużo gałęzi o tej samej wartości miary złożoności i działanie algorytmu nie będzie się różniło od zwykłego przeszukiwania wszystkich możliwych kombinacji bramek.

Z tabeli 1 widać, że najlepiej spełnia powyższe warunki miara złożoności oparta na widmach RM. Do wartości 10 i długości układu równej czterem bramkom w bardzo dużym stopniu spełniony jest warunek skupiania się wyników na przekątnej. Dla pozostałych miar złożoności występują znaczne odchylenia od wartości na przekątnej oraz istnieją kolumny zawierające bardzo krótkie układy, dla których miara złożoności jest stosunkowo duża oraz układy o relatywnie dużej liczbie bramek i bardzo małej wartości miary złożoności. Z tabeli 1 widać również, że wadą miary opartej na rozmiarze diagramów CSBDD jest bardzo mała liczba wartości, czego efektem jest bardzo duża liczba funkcji, dla których miara złożoności jest równa 0, mimo że ich optymalne realizacje wymagają nawet 7 bramek. Obserwacje te potwierdzają wartości współczynnika Q obliczone dla każdej z miar złożoności.

Wprowadzony w pracy współczynnik Q pozwolił na porównanie jakości poszczególnych miar złożoności. Pokazał on, że dotychczas zaproponowane miary złożoności są dalekie od idealnej, a zatem że należy nadal pracować nad ulepszaniem algorytmów heurystycznych. Może to przyczynić się do opracowania lepszych niż istniejące algorytmów syntezy układów odwracalnych.

8. Literatura

[1] G.W. Dueck, D. Maslov: Reversible Function Synthesis with Minimum Garbage Outputs, Proceedings of the 6th International Symposium on Representations and Methodology of Future Computing Technology, Trier, Germany, March 2003, pp. 154-161.

[2] P. Gupta, A. Agrawal, N.K. Jha: An Algorithm for Synthesis of Reversible Logic Circuits, IEEE Transactions on Computer-Aided Design, 25, November 2006, pp. 2317-2330.

[3] P. Kerntopf: A New Heuristic Algorithm for Reversible Logic Synthesis, Proceedings of the 41st Design Automation Conference, San Diego, CA, June 2004, pp. 834-837.

[4] D. Maslov, G.W. Dueck, D.M. Miller: Techniques for the Synthesis of Reversible Toffoli Networks, ACM Transactions on Design Automation of Electronic Systems vol. 12, no. 4, September 2007, article 42, pp. 1-28.

[5] D.M. Miller, D. Maslov: Spectral Techniques for Reversible Logic Synthesis, Proceedings of the 6th International Symposium on Representations and Methodology of Future Computing Technology, Trier, Germany, March 2003, pp. 56-62.

Artykuł recenzowany