

ПРОЕКТИРОВАНИЕ СПЕЦИФИКАЦИЙ КВАНТОВОЙ ЦЕПИ НА ОСНОВЕ АНАЛИЗА СТАТИСТИЧЕСКОЙ ИНФОРМАЦИИ

Матвеева И. В.¹, Власова К. В.², Линник М. А.³, Синявская Е. Д.⁴, Фокин Л. А.⁵

¹Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», Санкт-Петербург, Россия (197376, Санкт-Петербург, ул. Проф. Попова, д.5), e-mail: ir_mat@mail.ru

²Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Балтийская государственная академия рыбопромыслового флота», г. Калининград, Россия (236029, г. Калининград, ул. Молодежная, д. 6), e-mail: rector@bga.gazinter.net, kantzbgga@bga.gazinter.net

³Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тихоокеанский государственный университет», г. Хабаровск, Россия (680035, Хабаровский край, г. Хабаровск, ул. Тихоокеанская, 136), e-mail: khstu@khstu.ru

⁴Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет», г. Ростов-на-Дону, Россия (344006, г. Ростов-на-Дону, ул. Большая Садовая, 105/42), e-mail: info@sfedu.ru

⁵Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Южно-Уральский государственный университет», г. Челябинск, Россия (454080, г. Челябинск, проспект Ленина, 76), e-mail: admin@susu.ac.ru

В статье приводится методика проектирования спецификаций квантовой цепи на основе таблично заданных булевых функций. Методика рассматривается на примере построения набора квантовых булевых цепей, синтезированных на основе поляризованных полиномов Рида – Маллера (FPRM) с выбором оптимальных полиномиальных форм на основе предварительного статистического анализа определенных характеристик FPRM всех полярностей. Описывается матричная запись и программная реализация базовых квантовых преобразователей: NOT, C¹NOT, C²NOT, SWAP. Описан пример построения набора квантовых цепей для булевой квантовой функции по заданной таблице истинности. Показано, что задачи синтеза и оптимизации квантовой цепи могут быть сведены к традиционным логическим решениям. Приведены иллюстрации, которые наглядно демонстрируют переход от автоматически синтезированных квантовых цепей для различных полярностей полиномов Рида – Маллера к квантовым цепям, имеющим меньшее число преобразователей и меньшую глубину.

Ключевые слова: квантовые цепи, кубиты, полиномы Рида – Маллера, SWAP-преобразователи.

DESIGN SPECIFICATIONS OF QUANTUM CIRCUIT BASED ON ANALYSIS OF STATISTICS

Matveeva I. V.¹, Vlasova K. V.², Linnik M. A.³, Sinyavskaya E. D.⁴, Fokin L. A.⁵

¹Saint-Petersburg State Electrotechnical University, Saint-Petersburg, Russia. (197376, 5, Professora Popova st., Saint-Petersburg, Russia), e-mail: ir_mat@mail.ru

¹ Baltic Fishing Fleet State Academy (BFFSA), Kaliningrad, Russia. (236039, 6, Molodezhnaja st., Kaliningrad, Russia), e-mail: rector@bga.gazinter.net, kantzbgga@bga.gazinter.net

³Pacific State University, Khabarovsk, Russia. (680035, 136, Tikhookeanskaya St., Khabarovsk, Russia), e-mail: khstu@khstu.ru

⁴Southern Federal University, Rostov-on-Don, Russia (344006, 105/42, Bolshaya Sadovaya st., Rostov-on-Don, Russia), e-mail: info@sfedu.ru

⁵South Ural State University, Chelyabinsk, Russia (454080, 76, Lenin ave, Chelyabinsk, Russia), e-mail: admin@susu.ac.ru

The article describes the method of design of quantum circuit specifications, based on tabulated Boolean functions data. The method is considered as an example of building a set of new Boolean quantum circuits synthesized based on Reed – Muller polarized polynomials (FPRM) to have the best polynomial forms on the basis of preliminary statistical analysis of certain FPRM characteristics at all polarities. Matrix entry and software implementation of basic quantum converters is described, including: NOT, C¹NOT, C²NOT, SWAP. An example of the construction of a set of quantum circuits for quantum Boolean function for a given 1–0 table presented. The article shows, that the problem of synthesis and optimization of quantum circuits can be reduced to the traditional logical decisions. Illustrations, demonstrating transitions from automatically synthesized quantum cir-

Введение

Квантово-механические явления играют в последнее время все возрастающую роль в области представления и обработки информации, так как размеры транзистора приблизились к нанометрическому уровню. Стремительный прогресс компьютерных технологий должен сопровождаться соответствующим развитием методов проектирования. Это позволит в полной мере использовать потенциал возможностей все более усложняющихся аппаратных средств и одновременно адаптировать их для решения вполне определенных задач. При рассмотрении современных тенденций в области компьютерных технологий в качестве отправной точки следует использовать такие устоявшиеся классические понятия, как виртуализация аппаратных средств, иерархические программы, типы данных, управление памятью, поток управление и др., которые остаются применимыми и для представления новых подходов (например, квантовые вычисления).

Рассмотрение неклассических подходов (алгоритмов) для определения новых способов решения задач в принципиально иной аппаратной среде строится на основе замены и адаптации традиционных концептуальных положений. Для представления явления с конечным числом состояний привлекается модель квантовых цепей [7].

Вопрос об увеличении мощности вычислений по сравнению с классическим компьютером рассмотрен в 1992 г. в работах Deutsch D. и Jozsa R. [6], а также Berthiaume A. и Brassard G. [5]. Они показали, что имеются задачи, эффективно решаемые на основе квантовых подходов (асимптотически быстрее, чем классически). Отметим, что примеры задач несколько искусственные (без практической применимости), но позволяют представить суть подхода и проводить реальные физические эксперименты по их реализации.

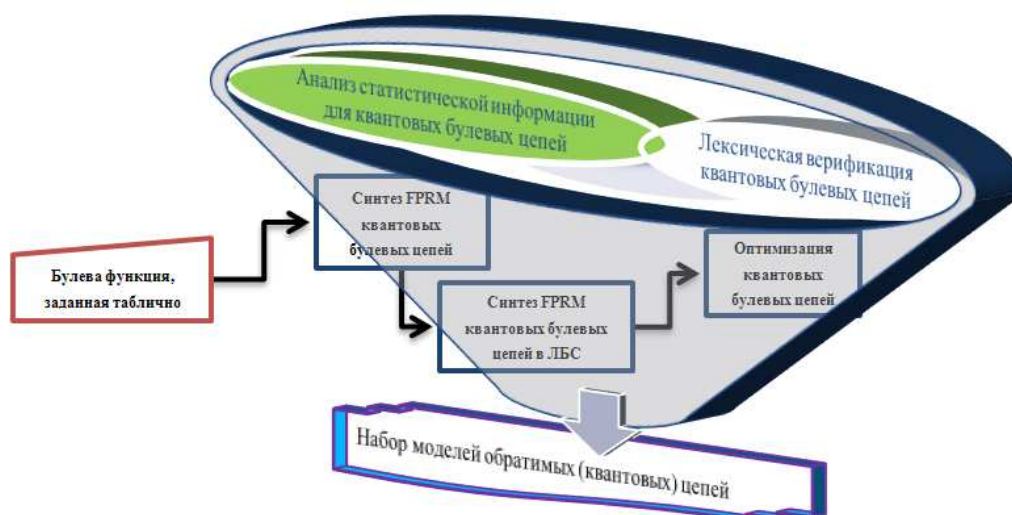


Рисунок 1. Фрагмент применяемого маршрута проектирования квантовых булевых цепей

При проектировании [4] обратимых и квантовых цепей может быть использован класс квантовых цепей (квантовые булевы цепи) с логикой на базе AND/EXOR, которая на основе полиномиальных нормальных форм позволяет получить представление булевых функций меньшей сложности и упростить верификацию синтезированных цепей. В статье рассмотрен пример построения набора квантовых булевых цепей, синтезированных на основе поляризованных полиномов Рида – Маллера (FPRM) с выбором оптимальных полиномиальных форм на основе предварительного статистического анализа определенных характеристик FPRM всех полярностей. Фрагмент применяемого маршрута проектирования квантовых булевых цепей представлен на рис. 1.

FPRM-представление [1] булевых функций (n входов и 1 выход) – это «сложение по модулю 2» EXOR от AND минитермов, в которых каждая булева переменная либо в прямой,

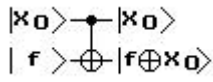
либо в инверсной форме, но не в обеих: $f(x_0, \dots, x_{n-1}) = \bigoplus_{i=0}^{2^n-1} b_i \varphi_i$, где $\varphi_i = \prod_{k=0}^{n-1} x_k^{i_m}$, $x_k = x_k$

или $\overline{x_k}$ и $x_m, b_i \in \{0, 1\}$ и i_m представляют собой двоичные числа в m ; φ_i известны как произведения термов, а b_i определяет, представлено произведение термов или нет. Символ \oplus обозначает операцию EXOR и символ умножения – точка обозначает операцию AND.

Описание решения

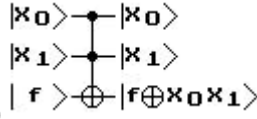
Рассмотрим этап синтеза, на котором по заданной таблице истинности для n булевых переменных строится поляризованный полином Рида – Маллера (нулевой полярности) и формируется набор поляризованных полиномов FPRM фиксированной полярности (от 1 до $2^n - 1$). На основе полученных полиномов в нотации Рида – Маллера генерируются наборы квантовых булевых схем в нотации квантовых преобразователей. Преобразователь NOT инвертирует входной кубит, что реализуется операцией EXOR с логической 1. Преобразователь CNOT инвертирует целевой кубит, если управляющий кубит в 1, при этом выполняется операция EXOR для обоих кубитов. Преобразователь Тоффоли инвертирует целевой кубит, когда оба управляющих кубита имеют значение 1, что реализуется операциями EXOR для целевого кубита и AND для обоих управляющих кубитов. Синтез соответствующей квантовой цепи осуществляется на основе сопоставления фрагментов FPRM представления и нотации квантовых преобразователей. Матричная запись и программная реализация графического представления библиотеки базовых квантовых преобразователей имеет следующий вид (символ \oplus в графической нотации обозначает операцию EXOR, а символ \bullet – управляющий кубит):

а) преобразователь NOT $|x_0\rangle \oplus |x_0\rangle$ для кубита имеет вид: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$;



б) преобразователь $C^1\text{NOT}$ для двух кубитов имеет вид:

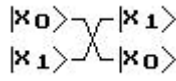
$$\begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} ab \\ ad \\ cb \\ cd \end{bmatrix} \xrightarrow{\text{CNOT}} \begin{bmatrix} ab \\ cd \\ cb \\ ad \end{bmatrix} = \begin{bmatrix} c \\ a \end{bmatrix} \otimes \begin{bmatrix} 0 \\ d \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ 0 \end{bmatrix};$$



в) преобразователь $C^2\text{NOT}$ (Тоффоли) для трёх кубитов имеет вид:

$$\begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ d \end{bmatrix} \otimes \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} abe \\ abf \\ ade \\ adf \\ cbe \\ cbf \\ cde \\ cdf \end{bmatrix} \xrightarrow{\text{Tof}} \begin{bmatrix} abe \\ abf \\ ade \\ cdf \\ cbe \\ cbf \\ cde \\ adf \end{bmatrix} =$$

$$= \begin{bmatrix} c \\ a \end{bmatrix} \otimes \begin{bmatrix} 0 \\ d \end{bmatrix} \otimes \begin{bmatrix} 0 \\ f \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ 0 \end{bmatrix} \otimes \begin{bmatrix} e \\ 0 \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} 0 \\ d \end{bmatrix} \otimes \begin{bmatrix} e \\ 0 \end{bmatrix} + \begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ f \end{bmatrix};$$



г) преобразователь SWAP для двух кубитов имеет вид

$$\begin{bmatrix} a \\ c \end{bmatrix} \otimes \begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} ab \\ ad \\ cb \\ cd \end{bmatrix} \xrightarrow{\text{SWAP}} \begin{bmatrix} ba \\ bc \\ da \\ dc \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ c \end{bmatrix}.$$

вход	выход	Polarity	NOT	5	4	3	2	1	NOT	C'gates+S	SWAPs	C'gates+	SWAPs	C'gates+	SWAPs	C'gates+	SWAPs	Отнош	Имен.			
			-x	control	control	control	control	control	-f	gates	SWAPs	SWAPs(1)	SWAPs(1)	SWAPs(2)	SWAPs(2)	QCost	Глубина	gates	глубины			
00000	1	0	0	0	1	3	1	1	1	7	22	29	1141	18	25	14	21	1101	17	27,586%	19,048%	
00001	0	1	2	0	1	3	3	2	0	11	36	47	1267	26	37	20	31	1187	27	34,043%	12,903%	
00010	1	2	2	0	1	4	4	0	1	12	54	66	1498	40	52	30	42	1378	35	36,364%	16,667%	
00011	1	3	4	0	1	4	6	3	1	19	80	99	1695	54	73	50	69	1545	57	30,303%	17,391%	
00100	1	4	2	0	1	2	0	1	1	7	12	19	943	12	19	12	19	943	14	0,000%	26,316%	
00101	0	5	4	0	1	2	2	1	0	10	24	34	1054	16	26	16	26	1014	21	23,529%	19,231%	
00110	1	6	4	0	1	3	2	1	1	12	32	44	1220	26	38	22	34	1170	27	22,727%	20,588%	
00111	0	7	6	0	1	3	4	3	0	17	56	73	1401	34	51	30	47	1271	38	35,616%	19,149%	
01000	1	8	2	0	1	4	2	1	1	11	38	49	1373	26	37	20	31	1283	26	36,735%	16,129%	
01001	0	9	4	0	1	4	2	2	0	13	36	49	1369	26	39	22	35	1299	29	28,571%	17,143%	
01010	1	10	4	0	1	5	6	1	1	18	88	106	1850	68	86	44	62	1630	48	41,509%	22,581%	
01011	1	11	6	0	1	5	6	2	1	21	82	103	1827	56	77	46	67	1647	53	34,951%	20,896%	
01100	1	12	4	0	1	3	0	1	1	10	20	30	1110	14	24	14	24	1080	15	20,000%	37,500%	
01101	0	13	6	0	1	3	2	1	0	13	32	45	1221	18	31	18	31	1151	23	31,111%	25,806%	
01110	1	14	6	0	1	4	3	1	1	16	50	66	1462	34	50	28	44	1352	33	33,333%	25,000%	
01111	0	15	8	0	1	4	5	3	0	21	74	95	1643	42	63	36	57	1453	44	40,000%	22,807%	
10000	1	16	2	0	1	4	1	1	1	10	34	44	1328	18	28	16	26	1238	22	40,909%	15,385%	
10001	0	17	4	0	1	4	3	1	0	13	46	59	1439	24	37	20	33	1309	27	44,068%	18,182%	
10010	1	18	4	0	1	5	5	2	1	18	80	98	1790	40	58	36	54	1570	45	44,898%	16,667%	
10011	0	19	6	0	1	5	7	4	0	23	104	127	1971	52	75	48	71	1691	60	44,094%	15,493%	
10100	1	20	4	0	1	3	1	1	1	11	18	29	1125	12	23	12	23	1095	15	20,690%	34,783%	
10101	0	21	6	0	1	3	3	2	0	15	32	47	1251	18	33	18	33	1181	26	39,787%	21,212%	
10110	1	22	6	0	1	4	4	0	1	16	46	62	1462	26	42	24	40	1352	32	35,484%	20,000%	
10111	1	23	8	0	1	4	6	3	1	25	72	95	1659	36	59	34	57	1469	47	40,000%	17,544%	
11000	1	24	4	0	1	5	3	2	1	16	56	72	1620	30	46	28	44	1480	36	38,889%	18,182%	
11001	0	25	6	0	1	5	1	2	0	15	44	59	1511	24	39	22	37	1401	29	37,288%	21,622%	
11010	0	26	6	0	1	6	8	5	0	26	124	150	2226	70	96	66	92	1936	72	38,667%	21,739%	
11011	1	27	8	0	1	6	6	3	1	25	100	125	2049	52	77	48	73	1789	55	41,600%	24,658%	
11100	1	28	6	0	1	4	2	1	1	15	30	45	1337	16	31	16	31	1267	23	31,111%	25,806%	
11101	0	29	8	0	1	4	2	2	0	17	36	53	1373	18	35	18	35	1283	26	33,962%	25,714%	
11110	1	30	8	0	1	5	6	1	1	22	72	94	1774	36	58	36	58	1594	46	38,298%	20,690%	
11111	1	31	10	0	1	5	6	2	1	25	82	107	1831	40	65	38	63	1611	46	41,121%	26,984%	
			NOT	5	4	3	2	1	NOT	C'gates+S	SWAPs	C'gates+	SWAPs	C'gates+	SWAPs	C'gates+	SWAPs	Отнош	Имен.			
			-x	control	control	control	control	control	-f	gates	SWAPs	SWAPs(1)	SWAPs(1)	SWAPs(2)	SWAPs(2)	QCost	Глубина	gates	глубины			
			Вс:							7	12	19	943	12	19	12	19	943	14	0,000%	12,903%	
										max	26	124	150	2226	70	96	66	92	1936	72	44,898%	37,500%
										avg	15,875	53,500	69,375	1494,4	31,938	47,813	28,188	44,063	1367,8	34,813	33,664%	21,369%

Рисунок 2. Таблица истинности пяти переменных

Рассмотрим пример построения набора квантовых цепей для булевой квантовой функции по заданной таблице истинности 5 переменных на основе анализа характеристик квантовых цепей (рис. 2). По таблице истинности проводится последовательный синтез логической функции в нотациях полиномов FPRM с последующей трансляцией в нотацию квантовой цепи. В итоге автоматически генерируется набор эквивалентных квантовых цепей, которые имеют разный состав (качественный и количественный) преобразователей. Задача синтеза и оптимизации квантовой цепи может быть сведена к традиционным логическим решениям на основе полиномов FPRM различной полярности. Полином 0-й полярности имеет вид:

$$f(x_0, x_1, x_2, x_3, x_4) = x_0x_1x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4 \oplus x_4 \oplus 1.$$

Результаты первичного синтеза и анализа цепей автоматически передаются в Excel (рис. 2) с формированием столбцов: «Polarity» – номер полярности, «NOT-x» – количество преобразователей NOT для обрабатываемых кубитов $|x_0\rangle \dots |x_{n-1}\rangle$, где n – число управляющих кубитов, столбцы k -control (число $k \in \{1, n\}$) – количество C^k NOT, «NOT-f» – количество NOT, воздействующих на функциональный кубит $|f\rangle$, «gates» – количество преобразователей в цепи, «SWAPs» – количество преобразователей SWAP, необходимых для приведения преобразования цепи с точки зрения близкого соседства без учета возможной оптимизации, «gates+SWAPs» – количество преобразователей в цепи с учетом SWAP, «QCost» – квантовая стоимость цепи. За единицу квантовой стоимости выбран однокубитовый преобразователь, в примере – NOT. Стоимость двухкубитового преобразователя зависит от технологии его реализации и определяется на основе стандартного разложения на однокубитовые преобразова-

тели со значением 5. Аналогично для преобразователей большей мерности. В примере для функции на рис. 2 оптимальной с точки зрения разных критериев оказалась цепь Polarity 4. По числу преобразователей также оптимальна цепь Polarity 20. По глубине (определяется по числу уровней преобразователей, где каждый уровень содержит набор тех преобразователей, которые могут быть реализованы параллельно) и квантовой стоимости – цепь Polarity 4, а по глубине к ней близки Polarity 12 и 20. Дальнейший выбор цепи будет зависеть от того, в какой технологии предполагается ее реализации, а также от типа используемой оптимизации.

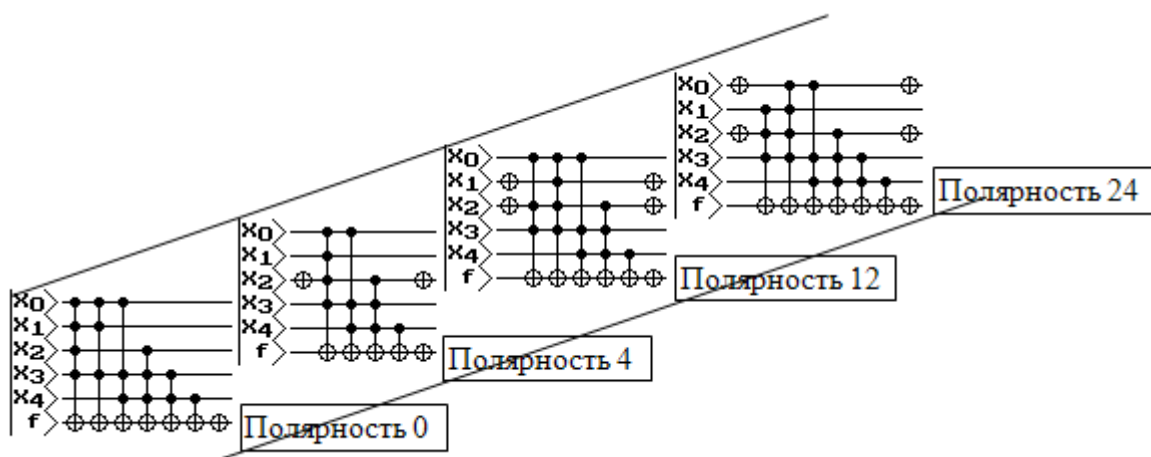


Рисунок 3. Экранные формы результата автоматического синтеза квантовых цепей

На рис. 3 представлены экранные формы результата автоматического синтеза квантовых цепей для различных полярностей полиномов Рунда – Маллера с наиболее оптимальными предварительно проанализированными характеристиками – полярности 0, 4, 12 и 20.

Для физической реализации возможна дальнейшая оптимизация набора схем [2], например, с точки зрения близкого соседства в зависимости от технологии реализации. Синтез квантовых логических цепей основан на библиотеке, состоящей из NOT, CNOT, C^2 NOT и SWAP преобразователей. Использование SWAP-преобразователей обусловлено требованием смежности входов квантовых преобразователей в схемах близкого соседства.

Простая предварительная оптимизации с точки зрения близкого соседства рассмотрена на примере цепи нулевой полярности. В этом случае применено 18 преобразователей SWAP (рис.4, слева). Минимизация по размещению каскадных SWAP выполняется на основе анализа их типового размещения. Шаблоны замещения каскадных SWAP приведены в [3]. Многопроходная минимизация с использованием шаблонов приводит к значительному сокращению преобразователей SWAP, уменьшая общее число преобразователей квантовой цепи (рис.4, справа) и ее глубину.

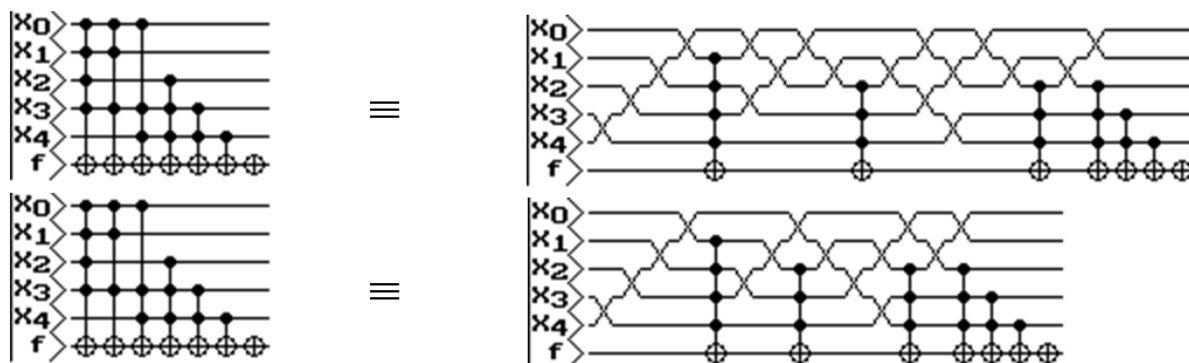


Рисунок 4. Многопроходная минимизация квантовых цепей

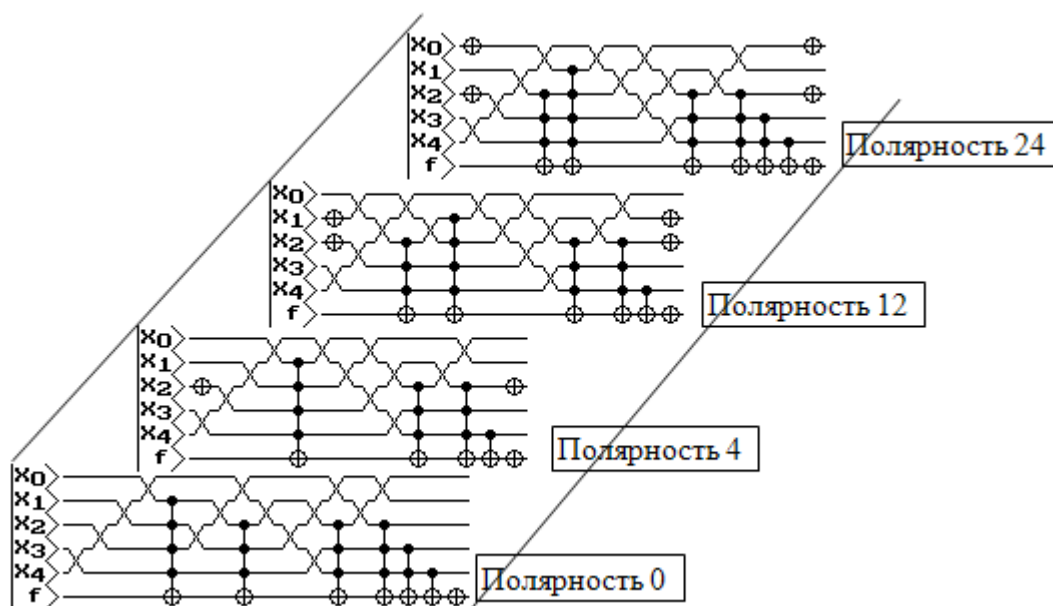


Рисунок 5. Спецификации оптимизированных квантовых цепей

Результирующие представления спецификаций после замещения каскадных SWAP для полярностей 0, 4, 12 и 20 представлены на рис. 5.

Заключение

Разработана и апробирована методика проектирования спецификаций квантовой цепи на основе таблично заданных булевых функций. Наглядно продемонстрировано, что многопроходная минимизация приводит к значительному сокращению преобразователей SWAP, тем самым уменьшая общее число преобразователей и глубину моделируемой квантовой цепи.

Работа выполнена при поддержке Министерства образования и науки РФ в рамках Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России на 2009–2013 годы» (Государственный контракт № 14.В37.21.2021 от 11 ноября 2012 г.).

Список литературы

1. Закревский А. Д., Торопов Н. Р. Полиномиальная реализация частичных булевых функций и систем. – 2-е изд. – М.: Изд-во «Едиториал УРСС», 2003. – 200 с.

2. Закревский А. Д., Торопов Н. Р. Быстрые алгоритмы оптимизации FPRM-представления систем булевых функций // Логическое проектирование. – Минск: Институт технической кибернетики, 1998. – С.4–18.
3. Калмычков В. А., Матвеева И. В. Модельные представления в проектировании высокопроизводительных квантовых вычислений. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2012.
4. Матвеева И. В., Калмычков В. А., Матвеева Л. И. Оптимизация проектирования квантовых цепей // Всероссийская научно-техническая конференция «Общество – наука – инновации»: сборник материалов: в 4 т. – Т. 2. ФАВТ, ФПМТ, ЭТФ. – 364 с. – Киров: Изд-во ГОУ ВПО «ВятГУ», 2010. – С. 48–52.
5. Berthiaume A., Brassard G. The quantum challenge to structural complexity theory // Proc. of the Seventh Annual Structure in Complexity Theory Conference. LosAlamos, CA: IEEE Computer Society Press, 1992. – P.132–137.
6. Deutsch D., Jozsa R. Rapid solution of problems by quantum computation // Proc. Roy. Soc. Ser. A. 1992. – Vol. 439. – P. 553–558.
7. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. – Cambridge: Cambridge Univ. Press, 2000.

Рецензенты:

Водяхо Александр Иванович, д.т.н., профессор кафедры вычислительной техники. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», г. Санкт-Петербург.

Пузанков Дмитрий Викторович, д.т.н., зав. кафедрой вычислительной техники. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», г. Санкт-Петербург.