

A Quantum Algorithm for finding Minimal Exclusive-Or Expressions for incompletely specified Boolean Functions

M. Sampson, D. Voudouris, M. Kalathas, G. Papakonstantinou
 Dept of Electrical and Computer Engineering
 Division of Computer Science
 Computing Systems Laboratory
 National Technical University of Athens
 157 80, Zografou Campus, Greece

Abstract— This paper presents a quantum algorithm for finding minimal ESCT (Exclusive-or Sum of Complex Terms) or ESOP (Exclusive-or Sum Of Products) expressions for any arbitrary incompletely specified switching function. The proposed algorithm takes advantage of the inherent massive parallelism of quantum circuits in order to achieve better complexity than the conventional ones. The proposed xor expressions such as ESCT can be used to implement an arbitrary Boolean function into a reversible or even a quantum circuit.

I. INTRODUCTION

Quantum circuits have already begun to establish themselves as the future in the computer design technology. Despite the technical difficulties in implementing a complete quantum computer, quantum circuits are already being studied thoroughly. Many algorithms, specifically designed for quantum computers, have been proposed and some of them prove that, in certain kind of problems, a quantum computer can achieve far better complexity than a conventional one. The three algorithms that constitute, so far, the foundations of quantum algorithms are the Shor's [1], the Grover's [2] and the Quantum Fourier Transformation [3] algorithms. In particular the Shor's algorithm can find the periodicity of a function in polynomial time, providing exponential speedup which, in principle, renders RSA and related cryptography algorithms obsolete. Grover's algorithm is the optimal quantum searching algorithm even though it doesn't achieve the spectacular speedup of the previous one. Finally, the quantum Fourier Transform is actually the implementation of the Discrete Fourier Transform as a quantum circuit and has many applications in quantum algorithms as it provides the theoretical basis to the phase estimation procedure and is a key feature for many important quantum algorithms.

Finding minimal ESCT (Exclusive-or Sum of Complex Terms) or ESOP (Exclusive-or Sum Of Products) expressions for an arbitrary completely specified switching function is a very difficult problem for a conventional computer. Finding minimal ESCT or ESOP expressions for an incompletely specified function is even more difficult.

An ESCT or ESOP expression of a boolean function is $Q = P_1 \oplus P_2 \oplus \dots \oplus P_n$, where $P_i = (\dots((x_1^* \odot x_2^*) \odot x_3^*) \dots x_n^*)$, x_i^* is a variable literal and \odot represents the logical AND, OR or XOR function. If \odot represents only the logical AND function, then Q is an ESOP expression, otherwise it is an ESCT expression. A minimal ESCT or ESOP expression is the one with the least possible number of P_i terms.

An interesting property of the ESCT and ESOP expressions is that they can be directly mapped to cellular architectures like the Maitra Cellular Architecture (Fig. 1) which has been proved to be reversible [4]. Therefore expressing a Boolean function in ESCT or ESOP form results in a reversible circuit and may help in designing quantum circuits [4].

Some algorithms for finding minimal ESOP or ESCT expressions for an arbitrary completely specified switching function, but with limitations on its number of input variables or the number of terms in its minimal forms, have been presented in the past [5], [6], [7], [8], [15], [14], [11]. Others have been designed in order to detect almost minimal ESOP or ESCT expressions but for more input variables [4], [9], [10], [14], [11], [13]. Algorithms for finding almost minimal ESCT or ESOP expressions for incompletely specified functions are significantly less [16], [17], [18], [19].

In [12] a quantum algorithm for finding FPRM (Fixed Polarity Reed Muller) expressions with number of terms less than a specified threshold is described. It proposes the construction of a specialized quantum operator (oracle) which evaluates FPRM expressions. It then uses this oracle in conjunction with Grover's algorithm [2] in order to find the FPRM expressions with the desired characteristics. In [20] a quantum algorithm for finding ESCT or ESOP expressions with number of terms less than a specified threshold is described (and if the threshold is appropriately selected, it finds minimal expressions). QMin algorithm uses a modified oracle for Grover's algorithm and detects minimal ESCT or ESOP expressions for an arbitrary completely specified Boolean function.

In this work the previously mentioned QMin algorithm [20] is extended in order to detect minimal ESCT or ESOP expressions for incompletely specified Boolean functions (QMin is designed for completely specified Boolean functions). To the best of the authors' knowledge, this is the first quantum

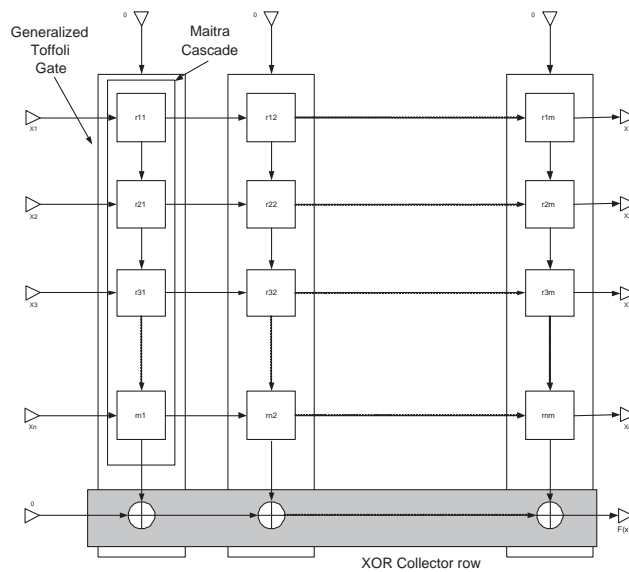


Fig. 1. Reversible wave cascade CA

algorithm that detects minimal ESCT or ESOP expressions for an arbitrary incompletely specified Boolean function.

REFERENCES

- [1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Computing* 26, pp. 1484-1509 (1997).
- [2] L.K. Grover, "A fast quantum mechanical algorithm for database search", *Proc. 28th Ann. ACM Symp. on Theory of Comput.*, 212219, 1996.
- [3] D. E. Knuth "The Art of Computer Programming", Vol. 2: Seminumerical Algorithms, Second ed., Addison-Wesley, 1981.
- [4] A. Mishchenko, M. Perkowski, "Logic Synthesis of Reversible Wave Cascades", *International Workshop on Logic And Synthesis 2002*, New Orleans, Louisiana, June 4-7, 2002.
- [5] G. Papakonstantinou, "Synthesis of cutpoint cellular arrays with exclusive-OR collector row", *Electronic Letters*, 13(1977).
- [6] D. Voudouris, S. Stergiou, G. Papakonstantinou "Minimization of reversible wave cascades", *IEICE Trans. on Fund.*, Vol E88-A, No. 4, pp. 1015-1023, 2005/04.
- [7] D. Voudouris, G. Papakonstantinou "Maitra Cascade Minimization", *6th IWSBP*, 2005, Freiberg (Sachsen), Germany.
- [8] D. Voudouris, M. Sampson, G. Papakonstantinou "Exact ESCT Minimization for functions of up to six input variables", accepted to be published in *Integration, The VLSI Journal*, Elsevier.
- [9] D. Voudouris, M. Kalathas, G. Papakonstantinou "Decomposition of Multi-output Boolean Functions", *HERCMA 2005*, Athens, Hellas.
- [10] G. Lee "Logic synthesis for cellular architecture FPGA using BDD", *ASP-DAC 97*, pp 253-258 Jan 1997.
- [11] A. Gaidukov, "Algorithm to derive minimum esop for 6 variable function", *5th IWSBP*, September 2002.
- [12] Lun Li, Mitch Thornton and Marek Perkowski "A Quantum CAD Accelerator based on Grover's algorithm for finding the minimum Fixed Polarity Reed-Muller form", *ISMVL'06, Proc. of the ISMVL'06 vol. 00*, pp. 33- 33, 17-20 May 2006.
- [13] A. Mishchenko, M. Perkowski "Fast Heuristic Minimization of Exclusive-Sums-of-Products", *5th International Reed-Muller Workshop*, Starkville, Mississippi, August, 2001
- [14] Stergiou S., Voudouris D., Papakonstantinou G., "Multiple-Value Exclusive-Or Sum-Of-Products Minimization Algorithms", *IEICE Trans. on Fund.*, 2004, vol 87, part 5, pp. 1226-1234.
- [15] T. Hirayama, Y. Nishitani, T. Sato "A Faster Algorithm of Minimizing AND-EXOR Expressions", *IEICE Trans. on Fund.*, Vol E85-A, No. 12, pp. 2708-2714, 2002/12.
- [16] M. Kalathas, D. Voudouris, G. Papakonstantinou "A heuristic algorithm to minimize ESOPs for multiple output incompletely specified functions", *GLSVLSI 2006*, Philadelphia, USA, 2006.
- [17] T. Kozłowski, E. L. Dagless, J. M. Saul "An enhanced algorithm for the minimization of exclusive-or sum-of-products for incompletely specified functions", *1995 IEEE Intern. Conf. on Computer Design (ICDD'95)*, pp. 244, 1995.
- [18] N. Song, M. A. Perkowski "Minimization of exclusive sum-of-products expressions for multiple-valued input, incompletely specified functions", *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, vol. 15, Nr. 4, April 1996.
- [19] G. Lee, R. Drechsler "ETDD-based Synthesis of term-based FPGAs for incompletely specified boolean functions", *ASP-DAC 1998*.
- [20] M. Sampson, D. Voudouris, G. Papakonstantinou "A Quantum Algorithm for Finding Minimum Exclusive-Or Expressions", to be presented in *ISVLSI 2007*, May 2007, Porto Alegre, Brazil.