Symbolic calculus for class of quantum computing circuits

F.Z. Hadjam and C. Moraga

A symbolic calculus to evaluate the output signals at the target line(s) of quantum computing subcircuits using controlled negations and controlled-\(Q\) gates is introduced, where \(Q\) represents the 4th root of \([0 \ 1; 1 \ 0]\), the unitary matrix of NOT, and \(k\) is a power of two. The controlling signals are GF(2) expressions possibly including Boolean expressions. The method does not require operating with complex-valued matrices. The method may be used to verify the functionality and to check for possible minimisation of a given quantum computing circuit using target lines. The method does not apply for a whole circuit if there are interactions among target lines. In this case the method applies for the independent subcircuits.

Introduction: Reversible switching theory represents a fast developing area, because of its possible applications in low power circuits, nano-electromechanical systems, superconducting interference devices, and because in the field of quantum computing, all basic operations must be reversible [1]. Much effort has been dedicated to develop methods to design reversible/quantum digital circuits (see e.g. [2–8]) focussing on benchmark databases (see e.g. [9]). One of the basic conditions to be fulfilled by a reversible/quantum circuit design system is to satisfy a given specification. A validation requires calculation of the outputs for specified, mostly all, inputs. A possibly semi-straightforward, formally correct method to do this resembles the ‘bit-slice’ architectures of the decade of the 1970s. A bit-slice architecture comprises independent gates at the same depth in a circuit. The transfer matrix of the bit-slice will be obtained as the top-down Kroncker product of the transfer matrices of its gates. A particularly severe constraint is the requirement that the controlling signals and the controlled gate must be in neighbour lines. This may require swapping some lines. Furthermore since the process is numerical, to evaluate the correct performance of a circuit with \(n\) inputs, all \(2^n\) possible input vectors must be considered.

A special class of quantum computing circuits comprises circuits with dedicated target lines to do the actual processing and give the result of computation; meanwhile all other lines do the controlling of the target gates. This kind of structure appears quite naturally when embedding a non-reversible function in a reversible one providing the target line(s). See examples below. To calculate the target output in this kind of circuit a low complexity symbolic calculus is introduced for circuits based on controlled-\(Q\) gates, which following the seminal work [5] are complex-valued matrices representing roots of NOT. Preliminary results of this work were presented at the 11th International Workshop on Boolean Problems [10].

Formalisms: Matrices giving formal representation to gates of a quantum computing circuit must be unitary, i.e. the product of a matrix and its adjoint must return the identity matrix. If the matrix is symmetric, the adjoint reduces to its complex conjugate. The matrix corresponding to the NOT operation is \([0 \ 1; 1 \ 0]\), which is trivially unitary, since it is real, symmetric and self-inverse. Therefore \(NOT* = NOT\), leading to \(NOT\) is the identity matrix. For any \(k\), power of 2, matrices \(Q\) such that \(Q^* = Q\), are also unitary and symmetric [1, 2]. Moreover, since \(NOT\) is self-inverse, \(Q^{-1} = NOT\) and \(Q^* = Q\). Moreover, NOT \(Q\) is \(NOT\) gate \(Q\) is \(Q\) gate \(Q^*\).\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)

\(Q^* = NOT\) gate \(Q\) is \(Q\) gate \(Q^*\).\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)\(\cdot\)

\(Q^*\) and \(Q\) are special cases of \(CNQ\), since as mentioned above, when \(k = 2\), \(Q = V\) and when \(k = 4\), \(Q = W\).

Lemma 1: Given a two-quantum bits (qubits)-controlled-\(Q\) gate with a binary control signal \(a\) and a target input \(t\), then the target output \(t'\) equals \(Q^{at}\cdot t\).

Proof: From the specification of a controlled gate, \(CQ\) of \(Q\) gate should be inhibited and behave as an identity, else, if \(a = 1\) the \(Q\) gate is active and it will be applied to \(t\).

It is this exactly expressed by \(t' = Q^{at}\cdot t\), since if \(a = 0\), then \(Q^* = Q^{0t} = I\) and therefore \(t' = t\); meanwhile if \(a = 1\), then \(Q^* = Q^t\) and \(t' = \eta t\).

Remark: Since \(\eta a_{\oplus}\{0, 1\}\) with \(1 \leq i \leq n\) holds

\(Q^\eta \cdot Q^\eta \cdot \ldots \cdot Q^\eta = Q^{\eta(\eta+\ldots+\eta)}\) (2)

and at the exponents level the sum is associative and commutative, this means that ‘for calculation purposes’ the individual \(Q\) matrices may be reordered. Whether in the circuit a reordering of the \(CQs\) is possible will depend on the relative independence of the controlling expressions.

Since the exponents of \(Q\) will be represented as \(GF(2)\) expressions possibly extended with Boolean operations, they will have to be translated to arithmetic expressions. Some basic elementary transformations are, e.g.:

\(1 \oplus a = 1 - a\); \(a \oplus b = a + b - 2ab\); \(a \oplus b \oplus ab = a + b - ab\); \(a + b - (a \oplus b) = 2ab\).

Examples

Example 1: Given a circuit with two cascaded Toffoli gates, as shown in Fig. 1, the question is: which is the lowest possible quantum cost for a realisation based on \(CNV\) gates?

From the functionality of the Toffoli gate it is simple to show that the target output will be \(t' = t \oplus ab \oplus bc = t \oplus b(a \oplus c)\). A straightforward approach to obtain a \(CNV\) realisation is to replace each Toffoli gate with the \(CNV\) circuit introduced in Barenco et al. [5], this leading to the circuit shown in Fig. 2.

In the circuits shown below, an empty square will denote a gate the unitary matrix of which is \(Q\), and a square with a diagonal line, a gate the unitary matrix of which is \(Q^\eta\). The circuits belong to the ‘\(CNQ\)’ family, where ‘\(C\)’ stands for ‘controlled’, ‘\(N\)’ for NOT and ‘\(Q\)’ for the gates introduced earlier. It is easy to understand that \(CNV\) and \(CNW\) are special cases of \(CNQ\), since as mentioned above, when \(k = 2\), \(Q = V\) and when \(k = 4\), \(Q = W\).

\(Q^\eta = NOT^{\eta b}(bc)\) and with (1), \(t' = V^{2k\eta(\eta+1)}\cdot t = NOT^{\eta b}bc\cdot t = t \oplus b(a \oplus c)\), as was to be expected. The realisation comprises 10 elementary controlled gates.

\(Q^\eta = NOT^{\eta b}(bc)\) and with (1), \(t' = V^{2k\eta(\eta+1)}\cdot t = NOT^{\eta b}bc\cdot t = t \oplus b(a \oplus c)\), as was to be expected. The realisation comprises 10 elementary controlled gates.
Note that the equation for $E$ may also be given by the following equivalent expression: $E = a + (b + b) - (a \oplus b) + c$, which represents moving gate 4 towards gate 2. That part of the circuit will have then a transfer of $P^{a}P^{b} = V^{ab} = \text{NOT}$. Hence, the two CV gates may be replaced by 'one' CNOT gate, thus reducing the total number of controlled gates to 9, as shown in Fig. 3.

Fig. 3 Realisation with nine elementary controlled gates

It should be recalled that since $P^{a}P^{b}$ also equals NOT, a Barenco et al. type of realisation for the second Toffoli gate (of Fig. 3) may be done using CV* gates at the places 4 and 5 and a CV gate at the place 6 (see [6]). In this case, gates 2 and 4 will produce an identity gate placed 6 (see [6]). In this case, gates 2 and 4 will produce an identity gate.

However, we claim that the realisation of Fig. 5 requires only 10 gates. Working at the level of exponents of controlled gates to 9, as shown in Fig. 3.

The output of the Toffoli gate with two control signals is correct. Note that the equation for $E$ may also be given by the following equivalent expression: $E = a + (b + b) - (a \oplus b) + c$, which represents moving gate 4 towards gate 2. That part of the circuit will have then a transfer of $P^{a}P^{b} = V^{ab} = \text{NOT}$. Hence, the two CV gates may be replaced by 'one' CNOT gate, thus reducing the total number of controlled gates to 9, as shown in Fig. 3.

The output of the Toffoli gate with two control signals is also correct. It should be pointed out that the realisation of Fig. 5 requires only 10 elementary controlled gates. If the control signal $c$ should be recovered, an additional CV Toffoli gate would be needed to add $ab$ to $c$ in mod 2 and recover $c$. The elements of the additional Toffoli gate may be reordered leaving the CNOT gate with target line $b$ in the first position, thus cancelling the CNOT gate on line $b$ at the end of the original circuit. This would lead to a realisation with 13 elementary gates, which is optimal, according to the classical CNW realisation [5].

Conclusion: A symbolic calculus has been introduced, which uses powers of the unitary matrices of the CNQ library. The exponents of the matrices are Boolean expressions. It has been shown that this is an appropriate formalism for the otherwise verbal specification of the behaviour of a controlled gate. The calculus was developed for the evaluation of the performance of target line oriented reversible quantum circuits based on the family of controlled-$Q$ gates. Although the considered circuits involve complex-valued matrices, the calculus only uses Boolean expressions and plain arithmetic. The proposed calculus is much simpler than the one presented in [7], and also much simpler than evaluations based on bit-slices.

Acknowledgment: The work of C. Moraga was partially supported by the CICYT Spain, under project TIN 2011-29827-C02-01.

© The Institution of Engineering and Technology 2015

17 October 2014

doi: 10.1049/el.2014.3623

F.Z. Hadjam (European Centre for Soft Computing, 33600 Mieres, Spain)

C. Moraga (European Centre for Soft Computing, 33600 Mieres, Spain)

E-mail: claudio.moraga@softcomputing.es

F.Z. Hadjam: Also with DÉpartement Informatique, Djillali Liabes University, Sidi Bel Abbes, Algeria

C. Moraga: Also with Faculty of Computer Science, TU Dortmund University, Dortmund, Germany

References

1. De Vos, A.: ‘Reversible computing: fundamentals, quantum computing, and applications’ (Wiley-VCH, Weinheim, 2010)

2. Sasanian, Z., and Miller, D.M.: ‘Transforming MCT circuits to NCWV circuits’, in ‘Reversible Computing’, De Vos, A., and Wille, R. (Eds.): (Springer, Heidelberg, 2012) (LNCS, 7165), pp. 77–88

3. Moraga, C.: ‘Hybrid GF(2)–Boolean expressions for quantum computing circuits’, in ‘Reversible Computing’, De Vos, A., and Wille, R. (Eds.): (Springer, Heidelberg, 2012) (LNCS, 7165), pp. 54–63, ISBN 978-3-642-29516-4

4. Szyprowski, M., and Kerntopf, P.: ‘Reducing quantum cost of pairs of multi-control Toffoli gates’, in Steinbach, B. (Ed.): ‘Recent progress in the Boolean domain’ (Cambridge Scholars Publishing, Newcastle upon Tyne, UK, 2014), pp. 359–368. ISBN 978-1-4438-5638-6

5. Barenco, A., Bennett, C.H., Cleve, R., et al.: ‘Elementary gates for quantum computation’, Phys. Rev. A, 1995, 52, pp. 3457–3467

6. Sasanian, Z.: ‘Technology mapping and optimization for reversible and quantum circuits’. PhD dissertation, University of Victoria, Canada, 2012

7. Lakac, M., Kameyama, M., Perkowski, M., and Kerntopf, P.: ‘Minimization of quantum circuits using quantum operator forms’. Proc. 21st Int. Workshop on Post-binary ULSI Systems, Tuusula, Finland, May 2012, pp. 88–95

8. Hadjam, F.Z., and Moraga, C.: ‘Introduction to RIMEP2. A multi-expression programming system for the design of reversible digital circuits’. ArXiv: 1405.2226

9. Wille, R., Große, D., Teuber, L., Dueck, G.W., and Drechsler, R.: ‘Revlib: an online resource for reversible functions and reversible circuits’. Proc. 38th IEEE Int. Symp. on Multiple-valued Logic, Dallas, TX, USA, May 2008, pp. 220–225

10. Moraga, C., and Hadjam, F.Z.: ‘Symbolic calculations in reversible CNQ subcircuits’. Proc. 11th Int. Workshop on Boolean Problems, Freiberg, Germany, September 2014, pp. 107–114, ISBN 978-3-86012-488-8