

Refutation of the direct correspondence of quantum gates to reversible classical gates

© Copyright 2018 by Colin James III All rights reserved.

Taken from:

Faugère, J-C., Horan, K., Kahrobaei, D., Kaplan, M, Kashefi, E., Perret, L. (2017). "Fast quantum algorithm for solving multivariate quadratic equations". arxiv.org/pdf/1712.07211.pdf

"2.3 Quantum Gates: The following gates are quantum gates of interest which operate on qubits, each directly corresponding to reversible classical gates. For qubits $|x\rangle$, $|y\rangle$, $|z\rangle$ the gates perform the following operations:

- CNOT (XOR, Feynman) $CNOT|x\rangle|y\rangle = |x\rangle|x + y\rangle$ [1.1]
- Toffoli (AND) $T|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z + xy\rangle$ [2.1]
- X (NOT) $X|x\rangle = |\bar{x}\rangle = |1 + x\rangle$ [3.1]
- n-qubit Toffoli (AND) $T_n|x_1\rangle \dots |x_n\rangle = |x_1\rangle \dots |x_{n-1}\rangle|x_n + (x_1 \dots x_{n-1})\rangle$ [4.1]
- Swap $S|x\rangle|y\rangle = |y\rangle|x\rangle$ [5.1]

LET: $p\ q\ r\ |x\rangle\ |y\rangle\ |z\rangle$; also $p\ q\ r\ s\ |x_1\rangle\ |x_2\rangle\ |x_3\rangle\ |x_4\rangle$; $n\ 4$;
 \sim Not; $+$ Or; $\&$ And; $=$ Equivalence; $@$ Not Equivalence, XOR

T is tautology as the designated *proof* value, with F as contradiction
 The 16-valued truth tables are presented row-major and horizontally.

Using the Meth8/VL4 apparatus and method, we render Eqs. 1.1-5.1 as:

$$(p@q)=(p\&(p+q)) ; \quad \text{TTF F TTF F TTF F TTF F} \quad (1.2)$$

$$((p\&q)\&r)=((p\&q)\&(r+(p\&q))) ; \quad \text{TTTF TTTT TTTF TTTT} \quad (2.2)$$

$$\sim p=((p\backslash p)+p) ; \quad \text{TFTF TFTF TFTF TFTF} \quad (3.2)$$

$$(((p\&q)\&r)\&s)=(((p\&p)\&q)\&r)\&(s+(((p\&p)\&q)\&r))) ; \quad \text{TTTT TTTF TTTT TTTT} \quad (4.2)$$

$$(p\&q)=(q\&p) ; \quad \text{TTTT TTTT TTTT TTTT} \quad (5.2)$$

Eqs. 1.2-4.2 are *not* tautologous. This means those quantum gates do not directly correspond to reversible classical gates. (Eq. 5.2 is tautologous, although trivial.)

Remark: Eqs. 2.2 and 4.2 are nearly tautologous but not, due to the single F contradiction value.

What follows is that quantum gates *cannot* map to bivalent logic.

Remark: We obtained the above conclusion in unpublished work (2008) where: the qubit was proved to be a probabilistic vector (not bivalent); and the various quantum gates were mapped to non-bivalent truth tables to show where bivalent corrections *would be*. Hence, this paper demonstrates a shorter refutation of quantum gates as reversible bivalent operators.