Original scientific paper

THE FREDKIN GATE IN REVERSIBLE AND QUANTUM ENVIRONMENTS

Claudio Moraga[1], Fatima Z. Hadjam[2]

[1]Technical University of Dortmund, Dortmund, Germany
[2]University of Djillali Liabes, Sidi Bel Abbes, Algeria

Abstract. *Reversible Computing circuits are characterized by low power consumption and their proximity to circuits for quantum computing. The Fredkin gate was one of the earliest proposed controlled reversible circuits, which however, was soon superseded by the Toffoli gate, the NOT, and CNOT gates, which constituting a flexible functionally complete set could also realize the Fredkin gate as a building block. In quantum computing circuits, the Fredkin gate (under the name controlled SWAP) plays an important role regarding the superposition of states. The present paper studies extensions of the Fredkin gate in terms of mixed polarity in the reversible domain and an application in quantum computing.*

Keywords: Fredkin gate, Reversible circuits, Quantum computing circuits

1. INTRODUCTION

The earliest contributions to the development of reversible computing circuits may be traced back to E. Fredkin [6] and T. Toffoli [26] who introduced the first controlled reversible gates. A reversible gate realizes a bijection. Therefore, it does not lose information. If the outputs are known, then the inputs may be precisely recovered. The realization of reversible circuits as fanout-free and feedback-free cascades of reversible gates was stimulated by R. Landauer's Theorem [9] stating that erasing or deleting information in a circuit produces heat dissipation. Moreover, C. Bennet [2] showed that a computer could work with low power dissipation if all its circuits would be reversible.

Since the early times most work on the synthesis of reversible circuits has been based on the set of gates {NOT, CNOT, Toffoli}, known as *NCT,* which is functionally complete. The symbols and functionality of these gates in a common environment of two (eventually) controlling lines and a target line are shown in Fig. 1.
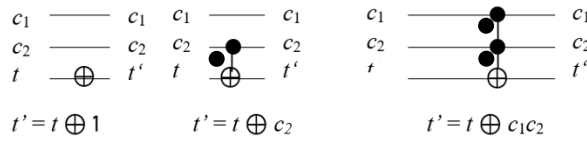
Fig. 1 Symbols and functionality for the reversible gates NOT, Controlled NOT and Toffoli

The NOT gate (represented with an EXOR symbol) is not controlled and acts directly on its target line. In the CNOT and Toffoli gates, control signals and target signals are distinguished. The NOT component acts on the target signal whenever the control signals have the value 1. Black dots identify which signal or signals are controlling the NOT component.

The design of minimal Boolean circuits is known to be NP-complete, and the design of minimal reversible circuits is NP-Hard [20]. This has led to the development of different heuristics to synthesize reversible circuits [4], [17], [21], [24], [25], and also to post-processing strategies to improve the minimization of circuits [19], [23].

In the last 25 years there have been important developments that have contributed to the improvement of the synthesis methods. Among the most relevant from the hardware point of view are the increasing speed of computers and the increasing size of memories. This has opened the possibility of including search [12], evolutionary algorithms [7], [8], [10] or SAT solvers [17] for the synthesis of reversible/quantum circuits. At the software side, the development of specialized efficient Libraries may be mentioned. At the level of gates, both the use of the value 0 for control signals identified by "white dots" [23], [14], frequently referred to as "mixed polarity", and the use of disjoint control signals [13], [15] may be mentioned. In what follows, the "generalization" of Fredkin gates in the reversible domain and a relevant application in the quantum domain will be analyzed. It may be mentioned that in [5] the term "Generalized Fredkin Gate" is used, referring to Fredkin gates with multiple control lines.

2. THE REVERSIBLE DOMAIN

It is not known whether the Fredkin gate ever had an own representation symbol (other than a box with three inputs and three outputs). Possibly a first symbolic representation was introduced in [11], which has been later replaced by the symbol used in circuits for quantum computing, as in e.g. [5]. In the literature this gate appears frequently as a Toffoli and CNOTs building block, as shown in Fig. 2 (left). In what follows, this building block will frequently be called simply Fredkin "gate" and will be used to illustrate the effects of mixed polarity. At the output side, variables will have a prime apostroph sign. (Complemented variables, on the other hand, will have a dash over their names, as frequently used in switching theory.) In the Barenco et al. based quantum model [1], Fig. 2 (right), a white box represents a V gate, whose functionality equals the square root of NOT and the box with a diagonal represents the adjoint of V.
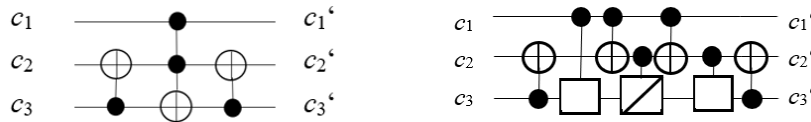

Fig. 2 Representation of the Fredkin gate as an *NCT* building block with positive control (left) and its Barenco et al. based quantum model (right)

The functionality of the building block representing the Fredkin gate is given by:

$$c'_3 = c_3 \oplus c_1(c_2 \oplus c_3) = c_3 \oplus c_1 c_2 \oplus c_1 c_3 = c_1 c_2 \oplus \bar{c}_1 c_3,$$
$$c'_2 = c_2 \oplus c_3 \oplus c'_3 = c_2 \oplus c_3 \oplus c_1 c_2 \oplus \bar{c}_1 c_3 = \bar{c}_1 c_2 \oplus c_1 c_3, \qquad (1)$$
$$c'_1 = c_1 .$$

Equations (1) may be expressed in the following summary:

	$c_1 = 0$	$c_1 = 1$
c_2'	c_2	c_3
c_3'	c_3	c_2

The tableau expressed in words means that whenever c_1 has the value 0, the Fredkin gate behaves as an identity, whereas when c_1 has the value 1, then the target signals c_2 and c_3 are exchanged. This means that the Fredkin gate behaves as a "controlled SWAP" although this name is hardly used in the community working on reversible circuits.

An important property of the Fredkin gate is its completeness. In (1), let $c_2 = 1$. Then:

$$c_2' = \bar{c}_1 \oplus c_1 c_3 = 1 \oplus c_1 \oplus c_1 c_3 = 1 \oplus c_1 \bar{c}_3 = \bar{c}_1 \vee c_3 = c_1 \to c_3$$

On the other hand, if for some x $c_1 \to (x \to 0)$ then $c_1 \to (\bar{x} \vee 0) = c_1 \to (\bar{x}) = \bar{c}_1 \vee \bar{x} = \overline{c_1 x} = \mathrm{NAND}(c_1, x)$.

Since NAND is functionally complete, so is also Fredkin complete.

A different formal representation of the Fredkin gate, appropriate to determine e.g. the performance of (simulated) circuits [28], is that of a transfer matrix.

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\cdot
\begin{matrix}
c_1\ c_2\ c_3 \\
\begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0 \\
0 & 1 & 1 \\
1 & 0 & 0 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 1 & 1
\end{bmatrix}
\end{matrix}
=
\begin{matrix}
c_1\text{'}c_2\text{'}c_3\text{'} \\
\begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0 \\
0 & 1 & 1 \\
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 0 & 1 \\
1 & 1 & 1
\end{bmatrix}
\end{matrix}
. \qquad (2)
$$

Equation (2) shows a Fredkin-Matrix as a blockdiag(I_4, SWAP), where I_4 denotes the 4×4 identity matrix. It becomes clear that the product of the Fredkin-Matrix with a matrix of all possible inputs preserves c_1, c_2 and c_3 when $c_1 = 0$, since the I_4 submatrix is active and $c_1\text{'}c_2\text{'}c_3\text{'} = c_1\ c_3\ c_2$ when $c_1 = 1$, since then the SWAP submatrix is active.

If a white dot is placed on the c_1 line of the original Fredkin gate, it is fairly obvious, that this will change the polarity of the control. The gate will become active when $c_1 = 0$ and it will remain inhibited, behaving as an identity, when $c_1 = 1$.

The circuit and the quantum model of a Fredkin gate, which is active when the control signal c_1 has the value 0 is shown in Fig. 3, where the quantum model uses the same two-qubit-gates as in Fig. 2, but in a different order.

Fig. 3 A Fredkin gate with negative control and its quantum model

Since the quantum cost of a reversible gate is obtained as the gate count of the Barenco et al. quantum model of the gate [22], [27], it becomes apparent that Fredkin gates with positive or negative control have the same quantum cost of 7.

A set of new behaviors is obtained if white dots are introduced in the lines c_2 or c_3, indicating that a signal is effective if it has the value 0. A first pair of equivalent variations is shown in Fig. 4.
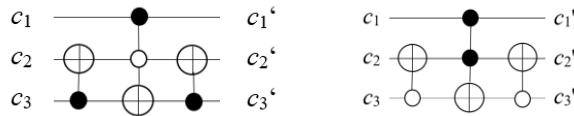

Fig. 4 Fredkin gate equivalent variations

The functionality of the building block at the left of Fig. 4 is given by:

$$c_3' = c_3 \oplus c_1(\bar{c}_3 \oplus c_2) = c_3 \oplus c_1\bar{c}_3 \oplus c_1c_2 = 1 \oplus \bar{c}_3 \oplus c_1\bar{c}_3 \oplus c_1c_2 =$$
$$= 1 \oplus \bar{c}_1\bar{c}_3 \oplus c_1c_2, \qquad (3)$$
$$c_2' = (c_3 \oplus c_2) \oplus c_3' = 1 \oplus c_3 \oplus \bar{c}_1\bar{c}_3 \oplus c_2 \oplus c_1c_2 = \bar{c}_1c_2 \oplus c_1\bar{c}_3,$$
$$c_1' = c_1 .$$

Equations (3) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	c_2	$\bar{c}_3$
c_3'	c_3	$\bar{c}_2$

In words: If $c_1 = 0$ the building block behaves as an identity and if $c_1 = 1$ both targets will be exchanged <u>and</u> complemented.

It is straightforward to show that the gate at the right of Fig. 4 has the same functionality. Further variations, and eventually their equivalent *NCT* reversible circuits are analyzed below.
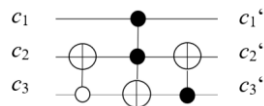

Fig. 5 Second Fredkin gate variation

The functionality of the building block of Fig. 5 is given by:

$$c_3' = c_3 \oplus c_1(c_2 \oplus \bar{c}_3) = 1 \oplus \bar{c}_3 \oplus c_1 c_2 \oplus c_1 \bar{c}_3 = c_1 c_2 \oplus \bar{c}_1 \bar{c}_3 \oplus 1,$$
$$c_2' = c_2 \oplus \bar{c}_3 \oplus c_3' = c_2 \oplus c_1 c_2 \oplus \bar{c}_3 \oplus \bar{c}_1 \bar{c}_3 \oplus 1 = \bar{c}_1 c_2 \oplus c_1 \bar{c}_3 \oplus 1, \quad (4)$$
$$c_1' = c_1.$$

Equations (4) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	$\bar{c}_2$	c_3
c_3'	c_3	$\bar{c}_2$

In words: If $c_1 = 0$ then c_2 will be complemented and c_3 will be preserved. If $c_1 = 1$ then the complement of c_2, and c_3 will be swapped.
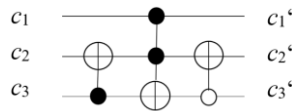
A third variation is shown in Fig. 6.

Fig. 6 Third variation of the Fredkin gate

The functionality of the building block of Fig. 6 is given by:

$$c_3' = c_3 \oplus c_1(c_2 \oplus c_3) = c_1 c_2 \oplus c_1 c_3 \oplus c_3 = c_1 c_2 \oplus \bar{c}_1 c_3,$$
$$c_2' = (c_2 \oplus c_3) \oplus (c_3' \oplus 1) = c_2 \oplus c_3 \oplus c_1 c_2 \oplus \bar{c}_1 c_3 \oplus 1 = \quad (5)$$
$$= \bar{c}_1 c_2 \oplus c_1 c_3 \oplus 1,$$
$$c_1' = c_1 .$$

Equations (5) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	$\bar{c}_2$	$\bar{c}_3$
c_3'	c_3	c_2

In words: If $c_1 = 0$ then c_3 will be preserved, but c_2 will be complemented. If $c_1 = 1$ then the signal c_3 will be complemented and swapped with c_2.

From all former variations follows that a variation comprising two white dots at the bottom and a white dot at the center of the middle line will have the same functionality as the original Fredkin gate. This is illustrated in Fig. 7.
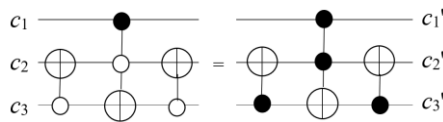

Fig. 7 Equivalent Fredkin gates

For the same reasons, the following variations on the Fredkin gate are equivalent, as illustrated in Fig. 8.
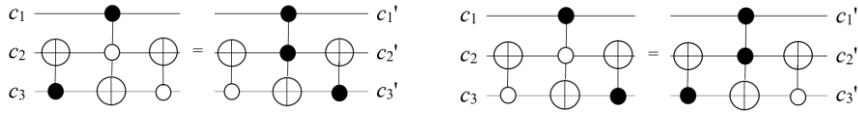

Fig. 8 Further equivalence of Fredkin variations

An additional way of introducing variations on the Fredkin gate consists of replacing the classical Toffoli gate with a disjunct controlled Toffoli gate [13], [15] possibly called "OR-Toffoli". For this gate, up-side-down triangles –(black or white)– are used instead of dots to identify the effectivity of driving control signals with value 1 and 0, respectively. Up-side-down triangles are used, based on their similarity with "∨", the disjunction symbol in mathematical logic.

A different variation, based on the OR-Toffoli gate, is shown in Fig. 9 and may be called "OR-Fredkin". Notice that the quantum model based on [1] does not use an adjoint V gate, but otherwise it uses the same gates as in the quantum model of the classical Fredkin gate. Therefore, it has the same quantum cost, 7.
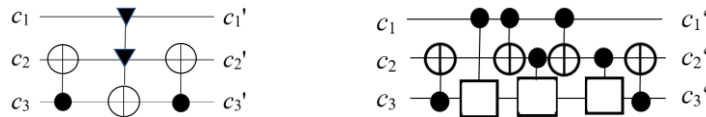

Fig. 9 The OR-Fredkin gate and its quantum model

The functionality of the building block of Fig. 9 (left) is given by:

$$c_3' = c_3 \oplus (c_1 \vee (c_2 \oplus c_3)) = c_3 \oplus c_1 \oplus c_2 \oplus c_3 \oplus c_1(c_2 \oplus c_3) =$$
$$= c_1 \oplus c_2 \oplus c_1(c_2 \oplus c_3) = c_1 \oplus c_2 \oplus c_1 c_2 \oplus c_1 c_3 = \bar{c}_1 c_2 \oplus c_1 \bar{c}_3, \quad (6)$$
$$c_2' = c_3 \oplus c_2 \oplus c_3' = c_3 \oplus c_2 \oplus \bar{c}_1 c_2 \oplus c_1 \bar{c}_3 = 1 \oplus \bar{c}_1 \bar{c}_3 \oplus c_1 c_2,$$
$$c_1' = c_1.$$

Equations (6) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	c_3	$\bar{c}_2$
c_3'	c_2	$\bar{c}_3$

An equivalent *NCT* circuit may be obtained, as shown in Fig. 10, where the two gates in the middle have the functionality of the OR-Toffoli gate.
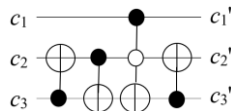

Fig. 10 An *NCT* equivalent circuit for the OR-Fredkin gate

Another variation is illustrated in Fig. 11, where for an OR-Toffoli gate, a white dot at the input side is introduced.
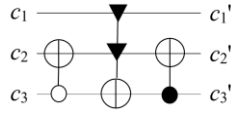

Fig. 11 A simple variation of the OR-Fredkin gate

The functionality of the building block of Fig. 11 is given by:

$$c_3' = c_3 \oplus \left(c_1 \vee (c_2 \oplus \bar{c}_3)\right) = c_3 \oplus \left(c_1 \oplus (c_2 \oplus \bar{c}_3) \oplus c_1(c_2 \oplus \bar{c}_3)\right) =$$
$$= c_3 \oplus c_1 \oplus c_2 \oplus \bar{c}_3 \oplus c_1(c_2 \oplus \bar{c}_3) = 1 \oplus c_2 \oplus c_1(c_2 \oplus c_3) =$$
$$= 1 \oplus \bar{c}_1 c_2 \oplus c_1 c_3 , \tag{7}$$
$$c_2' = c_2 \oplus \bar{c}_3 \oplus c_3' = c_2 \oplus \bar{c}_3 \oplus 1 \oplus \bar{c}_1 c_2 \oplus c_1 c_3 = c_1 c_2 \oplus \bar{c}_1 c_3 ,$$
$$c_1' = c_1.$$

Equations (7) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	c_3	c_2
c_3'	$\bar{c}_2$	$\bar{c}_3$

In words: If $c_1 = 0$ then c_2 will be complemented and swapped with c_3, whereas if $c_1 = 1$ there will be no swapping, but c_3 will be complemented. Fig. 12 shows an equivalent *NCT* circuit for the modified Fredkin gate of Fig. 11.
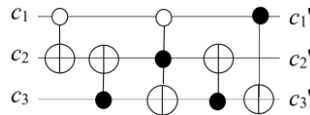

Fig. 12 Equivalent (more complex) *NCT* circuit for the gate of Fig. 11

Two equivalent variations are shown in Fig. 13, with a different distribution of the white dots/triangle.
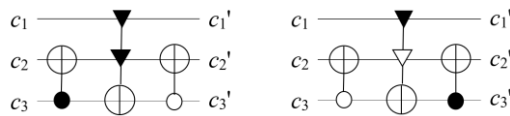

Fig. 13 Equivalent variations of the OR-Fredkin gate

The functionality of the building block at the left of Fig. 13 is given by:

$$c_3' = c_3 \oplus c_1 \vee (c_2 \oplus c_3) = c_1 \oplus c_2 \oplus c_1 c_2 \oplus c_1 c_3 = \bar{c}_1 c_2 \oplus c_1 \bar{c}_3 ,$$
$$c_2' = c_2 \oplus c_3 \oplus c_3' \oplus 1 = c_2 \oplus \bar{c}_3 \oplus \bar{c}_1 c_2 \oplus c_1 \bar{c}_3 = c_1 c_2 \oplus \bar{c}_1 \bar{c}_3 , \tag{8}$$
$$c_1' = c_1.$$

Equations (8) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	$\bar{c}_3$	c_2
c_3'	c_2	$\bar{c}_3$

In words: c_3 will be complemented and if $c_1 = 0$ then it will be swapped with c_2. If $c_1 = 1$ then no swapping takes place. It is simple to show that the circuit shown at the right of Fig. 13 has the same functionality. An *NCT* circuit equivalent to the variation, is shown in Fig. 14. It may be seen that its quantum cost [22], [27] and depth is higher by 1 with respect to the variations in Fig. 13.
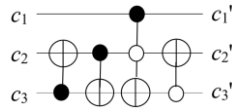

Fig. 14 Equivalent *NCT* circuit of the OR-Fredkin variation of Fig. 13

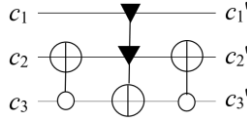Another variation is possible, with both bottom dots white, as shown in Fig. 15.

Fig. 15 Another OR- Fredkin variation

The functionality of the building block of Fig. 15 is given by:

$$c_3' = c_3 \oplus c_1 \vee (c_2 \oplus \bar{c}_3) = c_3 \oplus c_1 \oplus (c_2 \oplus \bar{c}_3) \oplus c_1(c_2 \oplus \bar{c}_3) =$$
$$= 1 \oplus c_1 \oplus c_2 \oplus c_1 c_2 \oplus c_1 \bar{c}_3 = \bar{c}_1 c_2 \oplus c_1 c_3 \oplus 1 = \bar{c}_1 \bar{c}_2 \oplus c_1 \bar{c}_3 , \quad (9)$$
$$c_2' = (c_2 \oplus \bar{c}_3) \oplus c_3' \oplus 1 = c_2 \oplus \bar{c}_3 \oplus \bar{c}_1 c_2 \oplus c_1 c_3 =$$
$$= c_1 c_2 \oplus \bar{c}_1 c_3 \oplus 1 = c_1 \bar{c}_2 \oplus = \bar{c}_1 \bar{c}_3 ,$$
$$c_1' = c_1 .$$

Equations (9) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	$\bar{c}_3$	$\bar{c}_2$
c_3'	$\bar{c}_2$	$\bar{c}_3$

In words: If $c_1 = 0$ then c_2 and c_3 will be complemented and swapped, whereas if $c_1 = 1$, c_2 and c_3 will be just complemented.

Equivalent circuits not using OR-Fredkin variations are shown in Fig. 16. It is easy to see that these equivalent *NCT* circuits are more complex than the OR-Fredkin variation.
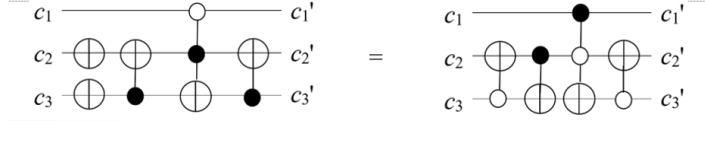
Fig. 16 Equivalent *NCT* circuits for the OR-Fredkin variation of Fig. 15

Another variation is shown in Fig. 17, where in analogy to the white dot, a white triangle is introduced, meaning that the corresponding control signal will be complemented before calculating the disjunction.
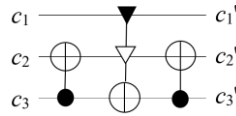

Fig. 17 A mixed-polarity OR-Fredkin variation

The functionality of the building block of Fig. 17 is given by:

$$c_3' = c_3 \oplus (c_1 \vee (c_3 \oplus c_2 \oplus 1)) = c_3 \oplus c_1 \oplus c_3 \oplus \bar{c}_2 \oplus c_1(\bar{c}_3 \oplus c_2) =$$
$$c_1(\bar{c}_3 \oplus \bar{c}_2) \oplus \bar{c}_2 = c_1\bar{c}_3 \oplus \bar{c}_1\bar{c}_2 \,, \tag{10}$$
$$c_2' = c_2 \oplus c_3 \oplus c_3' = c_2 \oplus c_3 \oplus c_1\bar{c}_3 \oplus \bar{c}_1\bar{c}_2 = \bar{c}_1\bar{c}_3 \oplus c_1\bar{c}_2 \,,$$
$$c_1' = c_1 \,.$$

Equations (10) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	$\bar{c}_3$	$\bar{c}_2$
c_3'	$\bar{c}_2$	$\bar{c}_3$

It becomes apparent that equations (9) and (10) are equal. This means that the corresponding OR-Fredkin variations are equivalent. Moreover, it may be noticed that the distribution of "white elements" in these variations is the same as the distribution of white dots shown in Fig. 4 for variations of the classical Fredkin gate.

An additional OR-Fredkin variation is shown in Fig. 18.
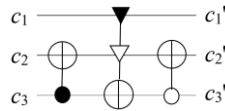
Fig. 18 OR-Fredkin variation

The functionality of the circuit is:

$$c_3' = c_3 \oplus \big(c_1 \vee (c_2 \oplus \bar{c}_3)\big) = c_3 \oplus c_1 \oplus c_2 \oplus \bar{c}_3 \oplus c_1(c_2 \oplus \bar{c}_3) =$$
$$= 1 \oplus c_1 \oplus c_2 \oplus c_1c_2 \oplus c_1\bar{c}_3 = c_1c_3 \oplus \bar{c}_1c_2 \oplus 1 \,, \tag{11}$$
$$c_2' = c_2 \oplus c_3 \oplus c_3' \oplus 1 = c_2 \oplus c_3 \oplus c_1c_3 \oplus \bar{c}_1c_2 = c_1c_2 \oplus \bar{c}_1c_3 \,,$$
$$c_1' = c_1 \,.$$

Equations (11) may be summarized as follows:

	$c_1 = 0$	$c_1 = 1$
c_2'	c_3	c_2
c_3'	$\bar{c}_2$	$\bar{c}_3$

It may be seen, that Eqs. (7) and (11) are equal. Therefore, the corresponding Fredkin variations are equivalent. They have the same distribution of white elements as the variations shown in Fig. 8. The comparison is shown in Fig. 19.
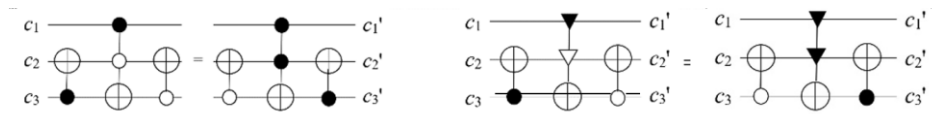

Fig. 19 Pairs of equivalent Fredkin variations

3. THE QUANTUM DOMAIN

In the domain of circuits for quantum computing, the Fredkin gate is not known under this name, but as "controlled SWAP", possibly because in the case of quantum circuits there is a very simple symbol for the swap of two "qubits" (= quantum bits). (See Fig. 19). Without knowing whether in some "quantum technology" the controlled SWAP is also realized as in the reversible domain, i.e. CNOT-Toffoli-CNOT, no variations as presented in the former section will be discussed. However, some changes in the surroundings of the controlled SWAP may be considered.

A relevant example of an effective use of the controlled SWAP was introduced in [3] to efficiently determine whether two qubits are equal or have an inner product with absolute value $\geq \varphi$, a threshold in [0, 1]. (See Fig. 20). A detailed analysis follows. In the Dirac notation [16], let $|0\rangle$ and $|1\rangle$ be the basis states of the working Hilbert space [16]. Let $|\gamma\rangle$ denote the state of a control qubit and let $\boldsymbol{H}$ denote the Hadamard gate $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

If $|\gamma\rangle = |0\rangle = [\ 1\ 0\ ]^T$ (in the vector notation), then :

$$\boldsymbol{H}|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{12}$$

This represents a superposition of states and a quantum circuit will work *in both states simultaneously*, which is one of the main characteristics of circuits for quantum computing.
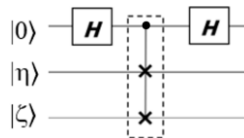

Fig. 20 Circuit to compare two qubits, in the dotted box, the symbol for the controlled SWAP

At the output side the circuit of Fig. 20, produces

$$(\boldsymbol{H} \otimes I_4)(C\mathrm{SWAP})(\boldsymbol{H} \otimes I_4)\,|0\rangle|\eta\rangle|\zeta\rangle\,, \tag{13}$$

where I_4 represents the 4×4 Identity matrix.

Lemma 1: The output of the circuit of Fig. 20 is given by:

$$(1/2)[\,|0\rangle(|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle) + |1\rangle(|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle)\,]. \tag{14}$$

Proof:

Considering the most general case, let $|\eta\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle)$, with $|\alpha_1|^2 + |\beta_1|^2 = 1$ and $|\zeta\rangle = (\alpha_2|0\rangle + \beta_2|1\rangle)$, with $|\alpha_2|^2 + |\beta_2|^2 = 1$.

Recall that $\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and let $\mathbf{Q} = (\boldsymbol{H} \otimes I_4)(C\mathrm{SWAP})(\boldsymbol{H} \otimes I_4)$.

Let S stand for SWAP. Then

$$\mathbf{Q} = \frac{1}{\sqrt{2}} \begin{bmatrix} I_4 & I_4 \\ I_4 & -I_4 \end{bmatrix} \cdot \begin{bmatrix} I_4 & 0_4 \\ 0_4 & S \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} I_4 & I_4 \\ I_4 & -I_4 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} I_4 & S \\ I_4 & -S \end{bmatrix} \cdot \begin{bmatrix} I_4 & I_4 \\ I_4 & -I_4 \end{bmatrix} =$$

$$= \frac{1}{2} \begin{bmatrix} I_4 + S & I_4 - S \\ I_4 - S & I_4 + S \end{bmatrix}. \tag{15}$$

Moreover,

$$|\eta\rangle|\zeta\rangle = [\alpha_1\ \beta_1]^T \otimes [\alpha_2\ \beta_2]^T = [\alpha_1\alpha_2\ \ \alpha_1\beta_2\ \ \beta_1\alpha_2\ \ \beta_1\beta_2]^T. \tag{16}$$

$$|\zeta\rangle|\eta\rangle = [\alpha_2\ \beta_2]^T \otimes [\alpha_1\ \beta_1]^T = [\alpha_2\alpha_1\ \ \alpha_2\beta_1\ \ \beta_2\alpha_1\ \ \beta_2\beta_1]^T. \tag{17}$$

Therefore,

$$|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle =$$

$$= [(\alpha_1\alpha_2 + \alpha_2\alpha_1)\ (\alpha_1\beta_2 + \alpha_2\beta_1)\ (\beta_1\alpha_2 + \beta_2\alpha_1)\ (\beta_1\beta_2 + \beta_2\beta_1)]^T. \tag{18}$$

$$|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle =$$

$$= [(\alpha_1\alpha_2 - \alpha_2\alpha_1)\ (\alpha_1\beta_2 - \alpha_2\beta_1)\ (\beta_1\alpha_2 - \beta_2\alpha_1)\ (\beta_1\beta_2 - \beta_2\beta_1)]^T. \tag{19}$$

Since α and β are possibly complex values, the products $\alpha_1\alpha_2$ and $\beta_1\beta_2$ are commutative. Therefore, the first and last components of the vector in (18) equal $2\alpha_1\alpha_2$ and $2\beta_1\beta_2$ respectively, and the first and last components of the vector in (19) equal 0. Therefore,

$$|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle = [(2\alpha_1\alpha_2)\ (\alpha_1\beta_2 + \alpha_2\beta_1)\ (\beta_1\alpha_2 + \beta_2\alpha_1)\ (2\beta_1\beta_2)]^T. \tag{20}$$

$$|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle = [\quad 0\quad\ (\alpha_1\beta_2 - \alpha_2\beta_1)\ (\beta_1\alpha_2 - \beta_2\alpha_1)\quad 0\quad]^T. \tag{21}$$

To calculate $\mathbf{Q}\,|0\rangle|\eta\rangle|\zeta\rangle$ the explicit expression for (15) will be needed, where "**T**" will be used to represent -1 and preserve the format of the matrix.

$$\mathbf{Q}\,|0\rangle|\eta\rangle|\zeta\rangle = \frac{1}{2}\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & \mathbf{T} & 0 \\ 0 & 1 & 1 & 0 & 0 & \mathbf{T} & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & \mathbf{T} & 0 & 0 & 1 & 1 & 0 \\ 0 & \mathbf{T} & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2\alpha_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ 2\beta_1\beta_2 \\ 0 \\ \alpha_1\beta_2 - \beta_1\alpha_2 \\ -\alpha_1\beta_2 + \beta_1\alpha_2 \\ 0 \end{bmatrix}. \tag{22}$$

The resulting vector in (22) may be additively divided into two vectors as follows:

$$\frac{1}{2}\begin{bmatrix} 2\alpha_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ 2\beta_1\beta_2 \\ 0 \\ \alpha_1\beta_2 - \beta_1\alpha_2 \\ -\alpha_1\beta_2 + \beta_1\alpha_2 \\ 0 \end{bmatrix} = \frac{1}{2}\left(\begin{bmatrix} 2\alpha_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ 2\beta_1\beta_2 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \alpha_1\beta_2 - \beta_1\alpha_2 \\ -\alpha_1\beta_2 + \beta_1\alpha_2 \\ 0 \end{bmatrix}\right). \tag{23}$$

From Eq. (21), with (18.b) and (19.b) follows that the first vector of (21) equals

$$(1/2)|0\rangle(\,|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle\,)$$

and the second vector of (21) equals

$$(1/2)|1\rangle(\,|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle\,).$$

This ends the proof that

$$\mathbf{Q}\,|0\rangle|\eta\rangle|\zeta\rangle = \; (1/2)[\;|0\rangle(|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle) + |1\rangle(|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle)\;]\,.$$

□

Notice that if $(|\eta\rangle = |\zeta\rangle)$ then $(|\eta\rangle|\zeta\rangle = |\zeta\rangle|\eta\rangle)$ and $(|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle) = 0$. This means that in this case, $|1\rangle$ would be measured with probability 0, whereas $|0\rangle$ would be measured with a non-zero probability. The equality of two state vectors may be obtained in one step, whereas a classical algorithm would require two comparisons.

A possible "variation" may consider $|\gamma\rangle = |1\rangle = [\,0\;\;1\,]^T$ (in the vector notation), then

$$H|1\rangle = \; \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{24}$$

Lemma 2: If in the circuit of Fig. 20 $|\gamma\rangle$ is set to $|1\rangle$, then

$$\mathbf{Q}|1\rangle|\eta\rangle|\zeta\rangle = (1/2)[(|0\rangle(|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle) + |1\rangle(|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle)].$$

Proof: At the output side the circuit with $|\gamma\rangle = |1\rangle$ now gives

$$(\boldsymbol{H} \otimes I_4)(C\,\mathrm{SWAP})(\boldsymbol{H} \otimes I_4)\,|1\rangle|\eta\rangle|\zeta\rangle = \mathbf{Q}|1\rangle|\eta\rangle|\zeta\rangle =$$

$$= \mathbf{Q}([\,0\;\;1]^T \otimes [\,\alpha_1\alpha_2\;\;\;\alpha_1\beta_2\;\;\;\beta_1\alpha_2\;\;\;\beta_1\beta_2\,]^T\,) =$$

$$= \frac{1}{2} \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & T & 0 \\ 0 & 1 & 1 & 0 & 0 & T & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & T & 0 & 0 & 1 & 1 & 0 \\ 0 & T & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 \\ \alpha_1\beta_2 - \beta_1\alpha_2 \\ -\alpha_1\beta_2 + \beta_1\alpha_2 \\ 0 \\ 2\alpha_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ \alpha_1\beta_2 + \beta_1\alpha_2 \\ 2\beta_1\beta_2 \end{bmatrix} . \qquad (25)$$

As in the former case, (recall Eq. (23)), the final vector of Eq. (25) may be split into two components associated to $|0\rangle$ and $|1\rangle$ respectively, leading to:

$$\mathbf{Q}|1\rangle|\eta\rangle|\zeta\rangle = (1/2)[(|0\rangle(|\eta\rangle|\zeta\rangle - |\zeta\rangle|\eta\rangle) + |1\rangle(|\eta\rangle|\zeta\rangle + |\zeta\rangle|\eta\rangle)] . \qquad (26)$$

In this case, if $|\eta\rangle = |\zeta\rangle$, $|0\rangle$ would be measured with probability 0.

A (pseudo) variation may be introduced if a signal, not the Controlled SWAP, is modified. Recall that the Pauli $\mathbf{X}$ matrix [18] equals $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and behaves as a quantum inverter.

It is fairly obvious that if Pauli $\mathbf{X}$ gates are included, as shown in Fig. (21), then the complement of $|\eta\rangle$ will be compared with $|\zeta\rangle$, which is equivalent to compare $|\eta\rangle$ with the complement of $|\zeta\rangle$.
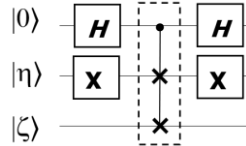

Fig. 21. Modified swap test circuit to compare one state with the complement of another.

The modified swap test may be expressed as:

$$(\mathbf{H} \otimes \mathbf{X} \otimes \mathrm{I}_2)(C\,\mathrm{SWAP})(\mathbf{H} \otimes \mathbf{X} \otimes \mathrm{I}_2)\,|0\rangle|\eta\rangle|\zeta\rangle. \qquad (27)$$

The proof of effectiveness, i.e. measuring $|1\rangle$ with probability 0, follows the same steps as in the former first case.

4. CONCLUSIONS

Variations on the Fredkin gate, based on mixed polarity, have been analyzed in the reversible domain. The OR-Fredkin gate is introduced and in all shown variation cases their circuits showed a lower complexity (quantum cost [22], [27], i.e. number of elementary gates on two qubits in the quantum model, and depth) than equivalent classical *NCT* circuits. A wide range of functionalities of the Fredkin gate under mixed polarity were shown, thus adding flexibility to the design of reversible circuits. Some equivalent variations were found and associated patterns of distribution of the white elements could be detected. In the quantum domain an application of the Controlled SWAP to efficiently test whether two states are equivalent was given a step by step calculation of behaviour and one possible extension of the *test circuit* was shown.

REFERENCES

[1]   A. Barenco, C. H. Bennett, R. Cleve, D. P. Di Vincenzo, N. Margolus, P. Shor, T. Sleator, J. A. = Smolin, and H. Weinfurter, "Elementary gates for quantum computation", *Phys. Rev.* A, vol. 52, pp. 3457-3467, 1995.
[2]   C. Bennett, "Logical reversibility of computation", *IBM J. Res. Develop.*, vol. 17, pp. 525-532, 1973.
[3]   H. Buhrman, R. Cleve, J. Watrous and R. De Wolf, "Quantum Fingerprinting", *Phys. Rev. Lett.*, vol. 87, no. 16, p. 167902-1-4, 2001.
[4]   C. S. Cheng and A. K. Singh, "Heuristic Synthesis of Reversible Logic – A Comparative Study", *Theoretical Appl. Electr. Eng.*, vol. 12, no. 3, pp. 210-225, 2014.
[5]   O. Dovhamuk and V. Deibuk, "CMOS simulation of mixed-polarity Generalized Fredkin Gates", In Proceedings of the 12th International Conference on Advanced Computer Information Technologies (ACIT), IEEE Press, 2022.
[6]   E. Fredkin and T. Toffoli, "Conservative logic", *Int. Jr. Theor. Phys.*, vol. 21, no. 3/4, pp. 219-253, 1982.
[7]   F. Z. Hadjam and C. Moraga, "RIMEP2. Evolutionary Design of Reversible Digital Circuits", *ACM J. Emerg. Technol. Comput. Syst.*, vol. 11, no. 3, pp. 27:1-27:23, 2014.
[8]   F. Z. Hadjam and C. Moraga, "A hierarchical distributed linear evolutionary system for the synthesis of 4-bit reversible circuits" in R. Seising and H. Allende-Cid (Eds.), *Studies in Fuzziness and Soft Computing* 349, pp. 233-249. Springer, 2017.
[9]   R. Landauer, "Irreversibility and heat generation in the computing process" *IBM J. Res. Develop.*, vol. 5, pp. 183-191, 1961.
[10] M. Lukac, M. A. Perkowski, H. Goi, M. Pivtoraiko, Ch. H. Yu, K. Chung, H. Jeech, B.-G. Kim and Y. D. Kim, "Evolutionary Approach to Quantum and Reversible Circuits Synthesis", *Artif. Intell. Rev.*, vol. 20, no. 3-4, pp. 361-417, 2003.
[11] D. Maslov, G. W. Dueck and D. M. Miller, "Synthesis of Fredkin-Toffoli Reversible Networks", *IEEE Trans. Very Large Scale Integ. (VLSI) Syst.*, vol. 13, no. 6, pp. 765-769, 2005.
[12] M. D. Miller and G. W. Dueck, "Search-Based Transformation Synthesis for 3-valued Reversible Circuits" in I. Lanese, and M. Rawski (Eds.)*, Reversible Computation,* LNCS 12227*,* 218-236, Springer, 2020.
[13] C. Moraga, "Hybrid GF(2)-Boolean Expressions for Quantum Computing Circuits", in A. De Vos and R. Wille (Eds.), *RC 2011*, LNCS 7165, pp. 54-63, Springer, 2012.
[14] C. Moraga, "Using negated control signals in quantum computing circuits", *FU Elec. Energ.*, vol. 24, no. 3, pp. 423-435, 2011.
[15] C. Moraga, "OR-Toffoli and OR-Peres Reversible Gates", in S. Yamashita and T. Yokoyama (Eds.) *Reversible Computation*, LNCS 12805, pp. 266-273, Springer, 2021.
[16] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge Univ. Press, UK, 2000.
[17] Ph. Niemann, L. Müller and R. Drechsler, "Finding Optimal Implementations of Non-native CNOT gates using SAT", in S. Yamashita, T. Yokoyama, (Eds.), *Reversible Computation,* LNCS 12805, pp. 242-255, Springer, 2021.
[18] W. Pauli, *Handbuch der Physik*, Chapter 24, Springer, Berlin, 1933.
[19] M. Rahman and G. W. Dueck, "An algorithm to find quantum Templates" In Proceedings of the IEEE Congress on Evolutionary Computing, IEEE Press, 2012, pp. 623-629.
[20] I. Rahul, B. Loff and I. C. Oliveira, "NP-hardness of circuit minimization for multi-output functions", In Proceedings of the 35th Computational Complexity Conference (CCC), 2020, pp. 22:1–22:36.
[21] M. Saeedi and I. L. Markov, "Synthesis and optimization of reversible circuits – A survey", *ACM Comput. Surveys*, vol. 45, no. 2, pp. 1-34, 2013.
[22] Z. Sasanian and D. M. Miller, "NCV Realization of MCT Gates with Mixed Control", In Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), 2011, pp. 567-571.
[23] M. Soeken and M. K. Thomsen, "White Dots *do* Matter: Rewriting Reversible Logic Circuits", in G. W. Dueck and D. M. Miller (Eds.), *Reversible Computation*, LNCS 7948, pp. 196-208, Springer, 2013.
[24] M. Soeken, G. W. Dueck and M. D. Miller, "A fast symbolic transformation-based algorithm for reversible logic synthesis", in S. Devitt and I. Lanese I. (Eds.), *Reversible Computation*, LNCS 9720, pp. 307-321, Springer, 2016.
[25] S. Stojković, M. M. Stanković and C. Moraga, "Complexity reduction of Toffoli networks based on FDD", *FU: Elec. Energ.*, vol. 28, no. 2, pp. 251-262, 2015.
[26] T. Toffoli, "Reversible Computing", in J. W. Baker and J. Van Leeuwen (Eds.), ALP 1980, LNCS 84, pp. 632-644, Springer, 1980.
[27] R. Wille, M. Saeedi and R. Drechsler, "Synthesis of Reversible Functions beyond Gate Count and Quantum Cost", 2010, pp. 1-7.
[28] A. Zulehner and R. Wille, "Simulation and Design of Quantum Circuits", in I. Ulidowski, I. Lanese, U. P. Schulz and C. Ferreira, (Eds.), *Reversible Computation: Extending Horizons of Computing*, LNCS 12070, pp. 60-82, Springer Open, 2020.