Applied Mathematics & Information Sciences
An International Journal

On the Universality of n-bit Reversible Gate Libraries

Ahmed Younes[1,2,*]

[1] Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Alexandria, Egypt
[2] School of Computer Science, University of Birmingham, United Kingdom

Abstract: Many universal reversible libraries of gates that contain more than one gate type have been proposed in the literature. Synthesis of reversible circuits is much simpler and more practical if a single gate type is used in the circuit construction. This paper proposes a novel reversible n-bit gate that is universal for reversible circuits synthesis. The proposed gate is extendable according to the number of bits in the circuit. The paper shows that the size of the synthesized circuits using the proposed gate is comparable with the size of the synthesized circuits using the known reversible libraries of gates.

Keywords: reversible circuit, universal gate, circuit synthesis, circuit Optimization, group theory

1 Introduction

Reversible logic [1,2] is one of the hot areas of research. It has many applications in quantum computation [3,4], low-power CMOS [5,6] and many more. Synthesis of reversible circuits cannot be done using conventional ways [7].

A lot of work has been done trying to find an efficient reversible circuit for an arbitrary reversible function [8,9, 10,11]. A method is given in [12], where a very useful set of transformations for Boolean quantum circuits is shown. A lot of work has been done trying to find an efficient reversible circuit for an arbitrary multi-output Boolean functions by using templates [13,14] and data-structure-based optimization [15]. A method to generate an optimal 4-bit reversible circuits has been proposed [16]. Benchmarks for reversible circuits have been established [17]. In [18], it was shown that there is a direct correspondence between reversible Boolean operations and certain forms of classical logic known as Reed-Muller expansions. This shows the possibility of handling the problem of synthesis and optimization of reversible Boolean logic within the field of Reed-Muller logic.

Recently, the study of reversible logic synthesis problem using group theory is gaining more attention. Investigation on the universality of the basic building blocks of reversible circuit has been done [19,20]. A relation between Young subgroups and the reversible

logic synthesis problem has been proposed [21,22]. A comparison between the decomposition of reversible circuit and quantum circuit using group theory has been shown [23]. A GAP-based algorithms to synthesize reversible circuits for various types of gate with various gate costs has been proposed [24].

The aim of any reversible circuit synthesis algorithm is to synthesize a reversible circuit for a given specification with the smallest possible number of gates. The reversible circuit synthesis algorithm should specify a gate library to be used during the synthesis process. Many gate libraries have been suggested in the literature. All suggested gate libraries consist of more than one type of gates such as NOT (N), Feynman (C), Toffoli (T3), Fredkin (F) and Peres (P) gates. Gate libraries such as NCT, NCF and NCP have been studied. It can be easily shown that the larger the number of basic gates used in the gate library, the smaller the number of gates in the synthesized circuit. Assume that there is a gate library for n-bit circuits contain $2^n!$ gates, then all synthesized circuits will be of size one.

Another reason that all suggested gate libraries in the literature contain more than one gate type is that none of the suggested gates is universal for reversible computing. Toffoli and Fredkin gates are reversible gates that are proved to be universal for non-reversible computation by showing that they can function as NAND gate.

NAND gate is a classical non reversible gate that is universal for classical circuit design. NAND gate is

* Corresponding author e-mail: ayounes@alexu.edu.eg

preferred over other universal classical set of gates such as AND/OR/NOT and AND/XOR/NOT because using single type of gates in the synthesis process makes the circuit cheaper. NOR gate is another universal gate.

Although a digital circuit can be implemented with AND/OR/NOT, classical computers are built almost exclusively on NAND and NOR gates even with a little increase in the size of the circuit because of technology considerations; that is, using a single type of gates might be cheaper to implement, for example OR gate can be implemented by 3 NAND gates connected together.

The aim of this paper is to suggest a novel reversible gate that is universal for reversible circuit design. This is important as it is cheaper in practice to make lots of similar things than a bunch of different things (different gates). All results shown in the paper have been obtained using the group-theory algebraic software GAP [25]. Some results shown in this paper matches the results obtained by other methods such as [26,24].

The paper is organized as follows: Section 2 gives a short background on the synthesis of reversible circuit problem and shows the reduction of the problem to be handled by permutation group. Section 3 analyzes the universality properties of common universal reversible libraries in the literature. Section 4 introduces the proposed pure universal reversible library and shows its properties. The paper ends up with a conclusion in Section 5.

2 Basic Notation

In this section, the basic notions for reversible circuit synthesis, permutation group, the relationship between reversible logic circuits and permutation group theory will be reviewed.

A reversible Boolean function $f : X^n \to X^n$ is a function that maps an input vector $(x_1, \ldots, x_n) \in X^n$ to a unique output vector $(y_1, \ldots, y_n) \in X^n$ where $X = \{0, 1\}$ [27,28]. The one-to-one correspondence between a reversible Boolean function f and a permutation on $\{1, 2, \ldots, 2^n\}$ is established as done in [24]. In the permutation group references, a permutation begins from one, instead of zero, so, we have the following relation [24]: $< X_{2^n}, X_{2^n-1}, \ldots, X_1 >_2 = index(X_{2^n}, \ldots, X_1) - 1$ and since the function f is a bijection, then it can be represented as a permutation as follows,

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & 2^n \\ f(1) & f(2) & f(3) & \ldots & f(2^n) \end{pmatrix}. \quad (1)$$

If the top row is ordered, then it can be eliminated and f can be written as a specification of a function [27] as follows,

$$(f(1), f(2), f(3), \ldots, f(2^n)). \quad (2)$$

For n inputs, there are $2^n!$ possible reversible Boolean functions. For $n = 3$, there are 40,320 3-in/out reversible functions. A reversible gate (or circuit) with n-input(s) and n-output(s) (n-in/out) is a gate that realizes a reversible Boolean function with n input(s) [27]. A set of reversible gates that can be used to realize any reversible Boolean function with n-input(s) as a reversible circuit with n-in/out is called a universal reversible gate library L_n [27]. A universal reversible gate sub library SL_n is a set of reversible gates such that $SL_n \subseteq L_n$ that can be used to build any reversible circuit with n-in/out [27]. Let $|L_n|$ be the number of gates in L_n and $|SL_n|$ be the number of gates in SL_n, then the ratio $2^{|SL_n|}/2^{|L_n|}$ represents the utilization of gates in a universal sub library and the ratio $2^{\min(|SL_n|)}/2^{|L_n|}$ represents the utilization of gates in the smallest universal sub libraries from a universal library, where $2^{|A|}$ represents the number of subsets from a set A.

When an m-in/out reversible gate U is applied on an n-in/out reversible circuit such that $m \leq n$, then U will be denoted as $U^n_{i_1 i_2 \ldots i_m}$ where $\{i_1, i_2, \ldots, i_m\}$ are the m wires spanned by U in order [27]. The set of all permutations on f forms a symmetric group on f under composition of mappings [29], denoted by S_{2^n} [30]. A permutation group G is a subgroup [29] of the symmetric group S_{2^n}. A universal reversible gate library L_n is called the generators of the group. Another important notation of a permutation is the product of disjoint cycles [30]. For example, the specification $(3, 2, 5, 4, 6, 1, 8, 7)$ can be written as $(1, 3, 5, 6)(7, 8)$. The identity mapping "()" is called the unit element in a permutation group. A product $p * q$ of two permutations p and q means applying mapping p then q, which is equivalent to cascading p and q. In what follows, a $n \times n$ reversible gate is not distinguished from a permutation in S_{2^n}.

3 Universal Reversible Libraries

In this section, the functions of the known reversible gates will be explained briefly to be able to discuss the universality properties of the known universal reversible libraries. This section explains the reasons that make all known universal reversible libraries should contain more than one gate type.

3.1 1-bit Reversible Circuits

NOT (N) gate is a 1-bit gate that flips the input unconditionally. There are 2 possible reversible circuits with 1-in/out. $N^1_1 : (x_1) \to (x_1 \oplus 1) \equiv (1, 2)$ is sufficient to realize these two circuits, i.e. universal for 1-bit circuits. The action of the disjoint cycle of the N^1_1 gate can be seen on a hypercube of 2 nodes shown in (1-(a)) where the N^1_1 gate maps vertex-1 to vertex-2 and vice versa. The cascading of two N gates gives the identity.
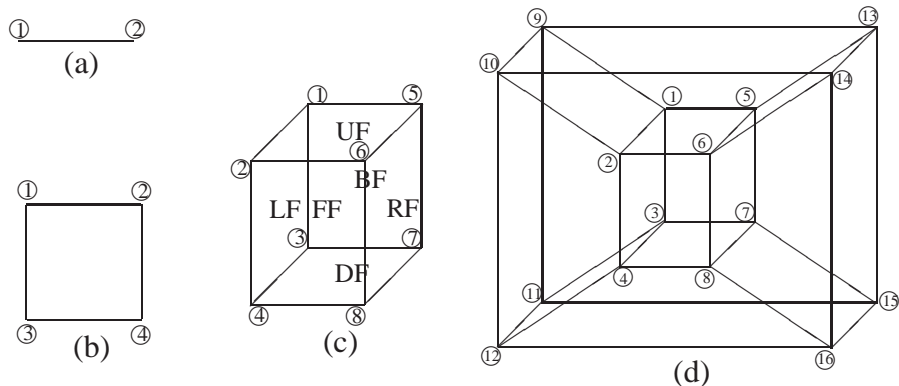
Fig. 1: A hypercube network with (a) 2 vertices, (b) 4 vertices, (c) 8 vertices and (d) 16 vertices.

3.2 2-bits Reversible Circuits

For 2-in/out reversible circuits, there are 24 possible circuits. The N gate cannot be used to synthesize all the 2-in/out reversible circuits. There are two possible N gates as follows,

$$
\begin{aligned}
N_1^2 &: (x_1, x_2) \rightarrow (x_1 \oplus 1, x_2) \equiv (1,3)(2,4), \\
N_2^2 &: (x_1, x_2) \rightarrow (x_1, x_2 \oplus 1) \equiv (1,2)(3,4).
\end{aligned}
\tag{3}
$$

These two N^2 gates can realize only 4 possible reversible circuits out of the 24 2-in/out reversible circuits. The action of the disjoint cycle of N_1^2 and N_2^2 gates can be seen on a hypercube of 4 nodes shown in (1-(b)) as edge mapping, where N_1^2 acts as a mapping between edge-$(1,2)$ and edge-$(3,4)$, while N_2^2 acts as a mapping between edge-$(1,3)$ and edge-$(2,4)$. No direct vertex mapping using N^2 gates which is the required mapping for the universality of a library.

Feynman (C) gate, also known as CNOT gate, is a 2-bit gate with a single control bit and a target bit. The C gate flips the target bit if the control bit is set to 1. There are two possible C gates for the 2-in/out reversible circuits as follows,

$$
\begin{aligned}
C_{12}^2 &: (x_1, x_2) \rightarrow (x_1, x_2 \oplus x_1) \equiv (3,4), \\
C_{21}^2 &: (x_1, x_2) \rightarrow (x_1 \oplus x_2, x_2) \equiv (2,4).
\end{aligned}
\tag{4}
$$

The action of the disjoint cycles of the C_{12}^2 and C_{21}^2 gates act as vertex mapping on the hypercube of 4 nodes between vertex-3 and vertex-4, and vertex-2 and vertex-4 respectively. A library that contains N_1^2, N_2^2, C_{12}^2 and C_{21}^2 is universal for 2-in/out reversible circuits. It can be shown using GAP that a permutation group with generators $\{N_1^2, C_{12}^2, C_{21}^2\}$ or $\{N_2^2, C_{12}^2, C_{21}^2\}$ is of size 24, i.e. a gate library that contains C_{12}^2 and C_{21}^2 with either of the N^2 gates is universal for 2-in/out reversible circuits.

3.3 3-bits Reversible Circuits

There are 40320 possible 3-in/out reversible circuits. The N gate and the C gate cannot be used to synthesize all the 3-in/out reversible circuits. There are 3 possible N gates, as shown in (2), for 3-in/out reversible circuits as follows,
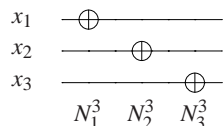

Fig. 2: The 3 possible N gates for 3-bit reversible circuits.

$$
\begin{aligned}
N_1^3 &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus 1, x_2, x_3) \equiv (1,5)(2,6)(3,7)(4,8), \\
N_2^3 &: (x_1, x_2, x_3) \rightarrow (x_1, x_2 \oplus 1, x_3) \equiv (1,3)(2,4)(5,7)(6,8), \\
N_3^3 &: (x_1, x_2, x_3) \rightarrow (x_1, x_2, x_3 \oplus 1) \equiv (1,2)(3,4)(5,6)(7,8).
\end{aligned}
\tag{5}
$$

The three N^3 gates act as face mapping on a hypercube of 8 nodes shown in (1-(c)). N_1^3 is a mapping between left face (LF) and right face (RF), N_2^3 is a mapping between upper face (UF) and down face (DF), and N_3^3 is a mapping between front face (FF) and back face (BF). The N gate is not universal for 3-in/out reversible circuits since it can realize only 8 possible circuits from the 40320 circuits. For n-in/out reversible circuits, there are n possible N gates.

There are 6 possible C gates for the 3-in/out reversible circuits as shown in (3). They act as edge mapping on a hypercube of 8 nodes shown in (1-(c)), for example, C_{12}^3 acts as a mapping between the upper edge and lower edge of RF. A gate library with C^3 gates can realize a total of 168 reversible circuits that constitute the linear 2-in/out circuits as shown in Table 1. The C gates for 3-in/out reversible circuits are as follows,
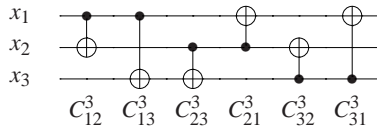
Fig. 3: The 6 possible *C* gates for 3-bit reversible circuits.

$$
\begin{aligned}
C_{12}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_2\oplus x_1,x_3) \equiv (5,7)(6,8),\\
C_{13}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_2,x_3\oplus x_1) \equiv (5,6)(7,8),\\
C_{23}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_2,x_3\oplus x_2) \equiv (3,4)(7,8),\\
C_{21}^3 &: (x_1,x_2,x_3) \rightarrow (x_1\oplus x_2,x_2,x_3) \equiv (3,7)(4,8),\\
C_{32}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_2\oplus x_3,x_3) \equiv (2,4)(6,8),\\
C_{31}^3 &: (x_1,x_2,x_3) \rightarrow (x_1\oplus x_3,x_2,x_3) \equiv (2,6)(4,8).
\end{aligned} \tag{6}
$$

Toffoli (*T*3) gate is a 3-bit with 2 control bits and a single target bit. *T*3 gate flips the target bit if the control bits are set to 1. There are 3 possible *T*3 gates, as shown in (4), for the 3-in/out reversible circuits as follows,
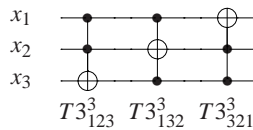

Fig. 4: The 3 possible *T* gates for 3-bit reversible circuit.

$$
\begin{aligned}
T3_{123}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_2,x_3\oplus x_1x_2) \equiv (7,8),\\
T3_{132}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_2\oplus x_1x_3,x_3) \equiv (6,8),\\
T3_{321}^3 &: (x_1,x_2,x_3) \rightarrow (x_1\oplus x_2x_3,x_2,x_3) \equiv (4,8).
\end{aligned} \tag{7}
$$

The *T*3 gate acts as a vertex mapping on a hypercube of 8 nodes shown in (1-(c)). The *T*3 gate is the smallest reversible gate that is proved to be universal for non-reversible computation by showing that it can function as NAND gate by initializing the target bit to 1. The *T*3 gate is not universal for reversible computation since a gate library with $T3^3$ gates can realize only 24 possible 3-in/out reversible circuits as shown in Table 1.

A library with $T3^3$ gates and N^3 gates form a universal library for 3-in/out reversible circuits known as NT library as shown in Table 1. The main NT library consists of 6 gates. There are 64 possible sub libraries from the main NT library, not every sub library is universal. There are only 4 sub libraries that are universal for 3-in/out reversible circuits as shown in Table 2. The smallest sub library contains 5 gates. There are only 3 universal sub libraries with 5 gates, these sub libraries contain the 3 T^3 gates with any 2 N^3 gates, for example, a

group with generators $\{N_1^3, N_2^3, T3_{123}^3, T3_{132}^3, T3_{321}^3\}$ is of size 40320 as shown in Table 3. The average size of the 40320 circuits synthesized with the NT library is 8.5 as shown in Table 4.

Using N^3 gates, C^3 gates and $T3^3$ gates form another universal library for 3-in/out reversible circuits known as NCT library Table 1. The main NCT library consists of 12 gates. There are 4096 possible sub libraries from the main NCT library. There are only 1960 sub libraries that are universal for 3-in/out reversible circuits as shown in Table 2. The smallest universal sub library contains 4 gates. There are only 21 universal sub libraries with 4 gates, for example, $\{N_1^3, C_{12}^3, C_{23}^3, T3_{321}^3\}$ and $\{N_2^3, C_{21}^3, T3_{123}^3, T3_{132}^3\}$ are universal sub libraries from the NCT library with 4 gates as shown in Table 3. The average size of the 40320 circuits synthesized with NCT library is 5.865 as shown in Table 4.

Fredkin (*F*) gate is another 3-bit gate which performs a conditional swap on two of its inputs if the third input is set to 1 as shown in (5). For 3-in/out reversible circuits, there are 3 possible *F* gates as follows,
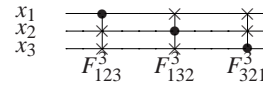

Fig. 5: The 3 possible *F* gates for 3-bit reversible circuits.

$$
\begin{aligned}
F_{123}^3 &: (x_1,x_2,x_3) \rightarrow (x_1,x_3,x_2) \equiv (6,7),\\
F_{132}^3 &: (x_1,x_2,x_3) \rightarrow (x_3,x_2,x_1) \equiv (4,7),\\
F_{321}^3 &: (x_1,x_2,x_3) \rightarrow (x_2,x_1,x_3) \equiv (4,6).
\end{aligned} \tag{8}
$$

The *F* gate introduces new type of mapping over the hypercube of 8 nodes shown in (1-(c)). The *F* gate maps vertices over the diagonal of a face, for example, F_{123}^3 is a mapping between vertex-6 and vertex-7 over the diagonal of RF. A gate library of F^3 gates is not universal since it can realize only 6 3-in/out reversible circuits as shown in Table 1. A gate library of N^3 gates and F^3 gates is also not universal since it can realize 1152 circuits out of the 40320 circuits.

The NCF library is a universal library with 12 gates as shown in Table 1. It has been introduced to get an average size of the 40320 synthesized circuits of 5.655 better than the NCT library as shown in Table 4. There are 4096 possible sub libraries of the main NCF library with 2460 universal sub libraries as shown in Table 2. The smallest universal sub library contains 4 gates better than the NCT and there are 60 universal sub libraries with 4 gates, for example, the gate libraries $\{N_1^3, C_{13}^3, F_{123}^3, F_{321}^3\}$ and $\{N_3^3, C_{32}^3, C_{32}^3, F_{132}^3\}$ are universal for 3-in/out reversible circuits as shown in Table 3.

Peres (*P*) gate is another 3-bit gate which combines the function of *T*3 gate and *C* gate in a single gate as shown in

(6). For 3-in/out reversible circuits, there are 6 possible *P* gates as follows,
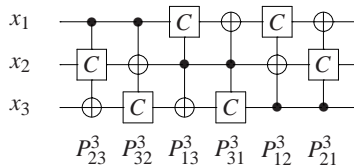

Fig. 6: The 6 possible *P* gates for 3-bit reversible circuits.

$$P_{23}^3 : (x_1,x_2,x_3) \rightarrow (x_1, x_2 \oplus x_1, x_3 \oplus x_1x_2) \equiv (5,7,6,8),$$
$$P_{32}^3 : (x_1,x_2,x_3) \rightarrow (x_1, x_2 \oplus x_1x_3, x_3 \oplus x_1) \equiv (5,6,7,8),$$
$$P_{13}^3 : (x_1,x_2,x_3) \rightarrow (x_1 \oplus x_2, x_2, x_3 \oplus x_1x_2) \equiv (3,7,4,8),$$
$$P_{31}^3 : (x_1,x_2,x_3) \rightarrow (x_1 \oplus x_2x_3, x_2, x_3 \oplus x_2) \equiv (3,4,7,8),$$
$$P_{12}^3 : (x_1,x_2,x_3) \rightarrow (x_1 \oplus x_3, x_2 \oplus x_1x_3, x_3) \equiv (2,6,4,8),$$
$$P_{21}^3 : (x_1,x_2,x_3) \rightarrow (x_1 \oplus x_2x_3, x_2 \oplus x_3, x_3) \equiv (2,4,6,8).$$
(9)

The *P* gate introduces another new type of mapping over the hypercube of 8 nodes shown in (1-(c)). It introduces a full path over the vertices of a plane through the diagonal to visit every vertex and return to the starting vertex. For example, P_{23}^3 and P_{32}^3 traverse RF starting from vertex-5, P_{13}^3 and P_{31}^3 traverse the DF starting from vertex-3, while P_{12}^3 and P_{21}^3 traverse FF starting from vertex-2. A gate library of P^3 gates is not universal since it can realize only 5040 3-in/out reversible circuits as shown in Table 1. A gate library of P^3 gates and N^3 gates is universal since it can realize the 40320 circuits. The NP library contains 9 gates. There are 512 possible sub libraries of the main NP library with 333 universal sub libraries as shown in Table 2. The smallest universal sub library contains 3 gates better than NCT and NCF libraries and there are 18 universal sub libraries with 3 gates, for example, the gate libraries $\{N_2^3, P_{32}^3, P_{31}^3\}$ and $\{N_3^3, P_{13}^3, P_{12}^3\}$ are universal for 3-in/out reversible circuits as shown in Table 3. The NP library gets an average size of the 40320 synthesized circuits of 5.516 better than the NCT and the NCF libraries as shown in Table 4.

Many combinations of the above gates have been used to propose different universal reversible libraries, for example, NCP, NCTF, NCPT and NCPF. The main aim of proposing a new universal reversible library is to synthesize circuits with smaller size. It can be easily shown that the higher the number of gates used in the library, the smaller the size of the synthesized circuits. Using many types of gates in a library will produce smaller circuits but will make the synthesis of circuits a hard problem.

The NCP library is a universal library with 15 gates as shown in Table 1. The average size of the 40320 synthesized circuits is 4.838 as shown in Table 4. There are 32768 possible sub libraries of the main NCP library with 26064 universal sub libraries as shown in Table 2. The smallest universal sub library contains 3 gates. There are 30 universal sub libraries with 3 gates, for example, the library $\{N_3^3, C_{13}^3, P_{21}^3\}$ is universal for 3-in/out reversible circuits as shown in Table 3.

The NCTF library is a universal library with 15 gates as shown in Table 1. The average size of the 40320 synthesized circuits of 5.33 as shown in Table 4. There are 32768 possible sub libraries of the main NCTF library with 23132 universal sub libraries as shown in Table 2. The smallest universal sub library contains 4 gates. There are 105 universal sub libraries with 4 gates, for example, the library $\{N_1^3, C_{12}^3, T3_{123}^3, F_{321}^3\}$ is universal for 3-in/out reversible circuits as shown in Table 3.

The NCPT library is a universal library with 18 gates as shown in Table 1. The average size of the 40320 synthesized circuits of 4.73 as shown in Table 4. There are 262144 possible sub libraries of the main NCPT library with 217384 universal sub libraries as shown in Table 2. The smallest universal sub library contains 3 gates. There are 36 universal sub libraries with 3 gates, for example, the library $\{N_3^3, P_{21}^3, T3_{123}^3\}$ is universal for 3-in/out reversible circuits as shown in Table 3.

The NCPF library is a universal library with 18 gates as shown in Table 1. The average size of the 40320 synthesized circuits of 4.597 as shown in Table 4. There are 262144 possible sub libraries of the main NCPF library with 220188 universal sub libraries as shown in Table 2. The smallest universal sub library contains 3 gates. There are 42 universal sub libraries with 3 gates, for example, the library $\{N_2^3, P_{31}^3, F_{123}^3\}$ is universal for 3-in/out reversible circuits as shown in Table 3.

3.4 n-bit Reversible Circuits

A little work has been done on the construction of universal libraries for *n*-bit reversible circuits due to the complexity of the problem [16]. The GT (Generalized Toffoli) library has been proposed. The GT library contains an extended version of *T*3 gate in addition to the gates in the NCT library, for example, the *T*4 is a 4-bit gate with 3 control bits and single target bit. The *T*4 gate flips the target bit if all control bits are set to 1, the *T*5 is a 5-bit with 4 control bits and single target bit. The *T*5 gate flips the target bit if all control bits are set to 1, and so on.

The GT4 library is the GT library for 4 bits with 32 basic gates. It contains 4 N^4 gates, 12 C^4 gates, 12 $T3^4$ gates and 4 $T4^4$ gates. The GT5 library is the GT library for 5 bits with 80 basic gates. It contains 5 N^5 gates, 20 C^5 gates, 30 $T3^5$ gates, 20 $T4^5$ gates and 5 $T5^5$ gates. The distribution of gates for the *GTn* library follows the reciprocal of Leibniz Harmonic triangle as shown in (7).

```
n
1 :                                 1
2 :                        2        2
3 :                3       6        3
4 :        4      12      12        4
5 :    5  20      30      20        5
6 :  6  30       60      60        30      6
7 : 7 42       105     140       105      42      7
```

Fig. 7: The reciprocal of Leibniz Harmonic Triangle.

The total number of gates for the *GTn* library can be calculated as follows,

$$num\_gates(GTn) = n \sum_{r=0}^{n-1} \binom{n-1}{r}, \quad (10)$$

where n is the number of bits and $r \geq 0$ is the number of controls per gate type, for example, $r = 0$ for N gate and $r = 1$ for C gate. The $GT4$ library is a universal library with 32 gates. The smallest universal sub library contains 5 gates, for example, the library $\{N_3^4, C_{31}^4, T4_{132}^4, T4_{1243}^4, T4_{1234}^4\}$ is universal for 4-in/out reversible circuits. The $GT5$ library is a universal library with 80 gates. The smallest universal sub library contains 6 gates, for example, the library $\{N_2^5, C_{21}^5, T5_{123}^5, T5_{1234}^5, T5_{13452}^5, T5_{12345}^5\}$ is universal for 5-in/out reversible circuits. The $GT6$ library is a universal library with 192 gates. The smallest universal sub library contains 7 gates, for example, the library $\{N_1^6, C_{12}^6, T6_{125}^6, T6_{1234}^6, T6_{1253}^6, T6_{123456}^6, T6_{234561}^6\}$ is universal for 6-in/out reversible circuits.

4 Universal Reversible Gate

This section proposes a novel universal *n*-bit reversible gate for *n*-in/out reversible circuits for $n \geq 2$. For $n = 1$, N gate is sufficient. The proposed gate is extendable according to the value of *n*, i.e. an extended *n*-bit version of the gate is universal for *n*-in/out reversible circuits.

4.1 2-bit Gate

The $G2$ gate is a 2-bit gate as shown in (8). It combines the action of N and C in a single gate, i.e. one bit is flipped if the other bit is set to 1 then the second bit is flipped unconditionally. For 2-in/out reversible circuits, there are 2 possible $G2$ gates as follows,

$$G2_{12} : (x_1, x_2) \to (x_1 \oplus 1, x_2 \oplus x_1) \equiv (1,3,2,4),$$
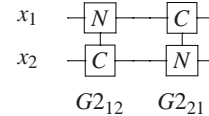$$G2_{21} : (x_1, x_2) \to (x_1 \oplus x_2, x_2 \oplus 1) \equiv (1,2,3,4). \quad (11)$$

Fig. 8: The 2 possible *G2* gates for 2-bit reversible circuits.

The $G2$ gate introduces a new type of mapping over the hypercube of 4 nodes. It performs a full path mapping over all the vertices of the hypercube through the diagonal to visit every vertex and return to the starting vertex. It can be shown using GAP that a permutation group with the 2 generators $G2_{12}$ and $G2_{21}$ is of size 24, i.e. a cascade of these two gates are sufficient to implement any of the 24 2-in/out reversible circuits.

4.2 3-bit Gate

The $G3$ gate is a 3-bit gate as shown in (9). It combines the action of N, C and $T3$ in a single gate, i.e. one bit is flipped if the other two bits are set to 1 then second bit is flipped if one of the remaining bits is set to 1. The last bit is flipped unconditionally. For 3-in/out reversible circuits, there are 6 possible $G3$ gates as shown in equation (12).
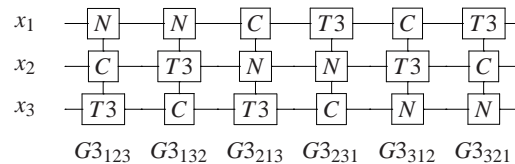
Fig. 9: The 6 possible *G3* gates for a 3-bit reversible circuit.

The $G3$ gate introduces a new mapping over the hypercube of 8 nodes shown in (1-(c)). It performs a full mapping path over all the vertices of the hypercube through the edges and the diagonals of different faces to visit every vertex and return to the starting vertex, for example, $G3_{123}$ starts from vertex-1, traverses BF as follows: $1 \mapsto 5 \mapsto 3 \mapsto 7$, then go to FF by the mapping $7 \mapsto 2$, then traverses FF as follows: $2 \mapsto 6 \mapsto 4 \mapsto 8$, then returns to vertex-1 by the mapping $8 \mapsto 1$. It can be seen that every $G3$ traverses the hypercube using 2 opposite faces, for example, $G3_{123}$ and $G3_{213}$ traverse the hypercube using BF and FF through different paths, $G3_{132}$ and $G3_{312}$ traverse the hypercube using UF and DF, while $G3_{231}$ and $G3_{312}$ traverses the hypercube using LF and RF.

It can be shown using GAP that a permutation group with the 6 generators of $G3$ is of size 40320, i.e. a cascade

$$
\begin{aligned}
G3_{123} &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1, x_3 \oplus x_1 x_2) \equiv (1,5,3,7,2,6,4,8), \\
G3_{132} &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1 x_3, x_3 \oplus x_1) \equiv (1,5,2,6,3,7,4,8), \\
G3_{213} &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus x_2, x_2 \oplus 1, x_3 \oplus x_1 x_2) \equiv (1,3,5,7,2,4,6,8), \\
G3_{231} &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus x_2 x_3, x_2 \oplus 1, x_3 \oplus x_2) \equiv (1,3,2,4,5,7,6,8), \\
G3_{312} &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus x_3, x_2 \oplus x_1 x_3, x_3 \oplus 1) \equiv (1,2,5,6,3,4,7,8), \\
G3_{321} &: (x_1, x_2, x_3) \rightarrow (x_1 \oplus x_2 x_3, x_2 \oplus x_3, x_3 \oplus 1) \equiv (1,2,3,4,5,6,7,8).
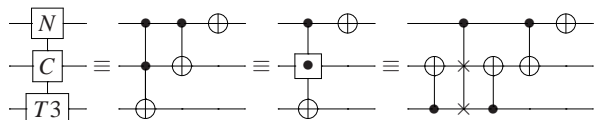\end{aligned}
\tag{12}
$$

of these 6 gates are sufficient to implement any 3-in/out reversible circuits as shown in Table 1. The main $G3$ gate library consists of 6 gates. There are 64 possible sub libraries of gates from the main $G3$ library, not every sub library is universal. There are 51 sub libraries that are universal for 3-in/out reversible circuits as shown in Table 2. The smallest sub library contains 2 gates. There are 9 universal sub libraries with 2 gates as shown in Table 3, these sub libraries contain any two $G3$ gates not starting with the same mapping, for example, a library with $G3_{123}$ and $G3_{132}$ is not universal since they start by the same mapping $1 \mapsto 5$, while a library with $G3_{123}$ and $G3_{213}$ is universal. It can be verified using GAP that a group with generators $\{G3_{123}, G3_{213}\}$ is of size 40320. The average size of the 40320 circuits synthesized with the $G3$ library is 6.402 as shown in Table 4. This average is better than a comparable library with 6 gates which is NT. The maximum number of gates to realize any 3-in/out reversible circuits is 8 similar to NCT and NCF and the size of the gate library is smaller than other gate libraries such as NCP, $NCTF$, $NCPT$ and $NCPF$. The $G3$ gate library is a pure gate library with only one type of gates. Realization of $G3$ gates using different gates is shown in (10). $G3_{123}$ and $G3_{321}$ have special importance since they realize the 3-bit cyclic-shift circuit [31] in a circuit with a single gate instead of a three gates circuit.

Fig. 10: Realization of $G3$ gate using different gates.

4.3 n-bit Reversible Gate

The $G4$ gate is a 4-bit gate. It combines the action of N, C, $T3$ and $T4$ in a single gate, i.e. one bit is flipped if the other three bits are set to 1, then the second bit is flipped if two of the remaining bits are set to 1, then the third bit is flipped if the remaining bit is set to 1. The last bit is flipped unconditionally. For 4-in/out reversible circuits,

Table 1: The universality of different libraries for 3-in/out reversible circuits.

Lib	LibSize	#specs
N	3	8
C	6	168
T	3	24
F	3	6
P	6	5040
NF	6	1152
NT	6	40320
NP	9	40320
NCT	12	40320
NCF	12	40320
NCP	15	40320
NCTF	15	40320
NCPT	18	40320
NCPF	18	40320
G3	6	40320

Table 2: Utilization of gates in universal sub libraries.

Lib	Lib Size	Num of Sub Libs	Num of Uni Sub Libs	Utilization
NT	6	64	4	6.25%
NP	9	512	333	65%
NCT	12	4096	1960	47.85%
NCF	12	4096	2460	60.00%
NCP	15	32768	26064	79.54%
NCTF	15	32768	23132	70.59%
NCPT	18	262144	217384	82.92%
NCPF	18	262144	220188	83.99%
G3	6	64	51	79.68%

there are 24 possible $G4$ gates as shown in equation (13) and equation (14).

Extending the G gate for n-bits is trivial as shown in (11). It can be shown using GAP that a permutation group with the $n!$ generators of Gn is of size $2^{n!}$, i.e. a cascade of these $n!$ gates are sufficient to implement any n-in/out reversible circuits.

The main Gn gate library consists of $n!$ gates. There are $2^{n!}$ possible sub libraries from the main Gn library. The smallest universal sub library always contains only 2 gates, for example, the sub library $\{G4_{2341}, G4_{1234}\}$ is

Table 4: Minimum size of 3-bit reversible circuits using different libraries.

Min Len	NT	NP	NCT	NCF	NCP	NCTF	NCPT	NCPF	G3
0	1	1	1	1	1	1	1	1	0
1	6	9	12	12	15	15	18	18	6
2	24	69	102	101	174	143	228	248	36
3	88	502	625	676	1528	1006	1993	2356	207
4	296	3060	2780	3413	8968	5021	10503	12797	1097
5	870	13432	8921	11378	23534	15083	23204	22794	4946
6	2262	21360	17049	17970	6100	17261	4373	2106	13819
7	5097	1887	10253	6739	0	1790	0	0	14824
8	9339	0	577	30	0	0	0	0	5208
9	12237	0	0	0	0	0	0	0	0
10	8363	0	0	0	0	0	0	0	0
11	1690	0	0	0	0	0	0	0	0
12	47	0	0	0	0	0	0	0	0
Avg	8.5	5.516	5.865	5.655	4.838	5.33	4.73	4.597	6.402
LibSize	6	9	12	12	15	15	18	18	6

$$
\begin{aligned}
G_{1234} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1, x_3 \oplus x_1 x_2, x_4 \oplus x_1 x_2 x_3), \\
G_{1243} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1, x_3 \oplus x_1 x_2 x_4, x_4 \oplus x_1 x_2), \\
G_{1324} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1 x_3, x_3 \oplus x_1, x_4 \oplus x_1 x_3 x_2), \\
G_{1342} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1 x_4, x_3 \oplus x_1 x_4 x_2, x_4 \oplus x_1), \\
G_{1423} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1 x_3 x_4, x_3 \oplus x_1, x_4 \oplus x_1 x_3), \\
G_{1432} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus 1, x_2 \oplus x_1 x_4 x_3, x_3 \oplus x_1 x_4, x_4 \oplus x_1), \\
G_{2134} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_2, x_2 \oplus 1, x_3 \oplus x_2 x_1, x_4 \oplus x_2 x_1 x_3), \\
G_{2143} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_2, x_2 \oplus 1, x_3 \oplus x_2 x_1 x_4, x_4 \oplus x_2 x_1), \\
G_{2314} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_3, x_2 \oplus x_3 x_1, x_3 \oplus 1, x_4 \oplus x_3 x_1 x_2), \\
G_{2341} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_4, x_2 \oplus x_4 x_1, x_3 \oplus x_4 x_1 x_2, x_4 \oplus 1), \\
G_{2413} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_3, x_2 \oplus x_3 x_1 x_4, x_3 \oplus 1, x_4 \oplus x_3 x_1), \\
G_{2431} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_4, x_2 \oplus x_4 x_1 x_3, x_3 \oplus x_4 x_1, x_4 \oplus 1), \\
G_{3124} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_2 x_3, x_2 \oplus 1, x_3 \oplus x_2, x_4 \oplus x_2 x_3 x_1), \\
G_{3142} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_2 x_4, x_2 \oplus 1, x_3 \oplus x_2 x_4 x_1, x_4 \oplus x_2), \\
G_{3214} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_3 x_2, x_2 \oplus x_3, x_3 \oplus 1, x_4 \oplus x_3 x_2 x_1), \\
G_{3241} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_4 x_2, x_2 \oplus x_4, x_3 \oplus x_4 x_2 x_1, x_4 \oplus 1), \\
G_{3412} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_3 x_4, x_2 \oplus x_3 x_4 x_1, x_3 \oplus 1, x_4 \oplus x_3), \\
G_{3421} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_4 x_3, x_2 \oplus x_4 x_3 x_1, x_3 \oplus x_4, x_4 \oplus 1), \\
G_{4123} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_2 x_3 x_4, x_2 \oplus 1, x_3 \oplus x_2, x_4 \oplus x_2 x_3), \\
G_{4132} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_2 x_4 x_3, x_2 \oplus 1, x_3 \oplus x_2 x_4, x_4 \oplus x_2), \\
G_{4213} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_3 x_2 x_4, x_2 \oplus x_3, x_3 \oplus 1, x_4 \oplus x_3 x_2), \\
G_{4231} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_4 x_2 x_3, x_2 \oplus x_4, x_3 \oplus x_4 x_2, x_4 \oplus 1), \\
G_{4312} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_3 x_4 x_2, x_2 \oplus x_3 x_4, x_3 \oplus 1, x_4 \oplus x_3), \\
G_{4321} &: (x_1,x_2,x_3,x_4) \rightarrow (x_1 \oplus x_4 x_3 x_2, x_2 \oplus x_4 x_3, x_3 \oplus x_4, x_4 \oplus 1).
\end{aligned}
\tag{13}
$$

universal for 4-in/out reversible circuits. The sub library $\{G5_{12345}, G5_{23451}\}$ is universal for 5-in/out reversible circuits and the sub library $\{G6_{234561}, G6_{514326}\}$ is universal for 6-in/out reversible circuits. It has been verified for $n \leq 10$ using a random gate generator on GAP that a sub library with 2 gates of size n is universal for n-in/out reversible circuits and this can be easily verified by symmetry for an arbitrary n. $Gn_{12...n}$ and $Gn_{n(n-1)...21}$ have special importance since they realize the n-bit cyclic-shift circuit [32] that acts on the states of a quantum register as $x \mapsto x + 1 \bmod 2^n$ in a single gate instead of a polylogarithmic number of operations.

5 Conclusion

In general, circuit synthesis using a single type of gates is more practical than using a gate library with more than

$$
\begin{aligned}
G_{1234} &: (1,9,5,13,3,11,7,15,2,10,6,14,4,12,8,16), \\
G_{1243} &: (1,9,5,13,2,10,6,14,3,11,7,15,4,12,8,16), \\
G_{1324} &: (1,9,3,11,5,13,7,15,2,10,4,12,6,14,8,16), \\
G_{1342} &: (1,9,2,10,5,13,6,14,3,11,4,12,7,15,8,16), \\
G_{1423} &: (1,9,3,11,2,10,4,12,5,13,7,15,6,14,8,16), \\
G_{1432} &: (1,9,2,10,3,11,4,12,5,13,6,14,7,15,8,16), \\
G_{2134} &: (1,5,9,13,3,7,11,15,2,6,10,14,4,8,12,16), \\
G_{2143} &: (1,5,9,13,2,6,10,14,3,7,11,15,4,8,12,16), \\
G_{2314} &: (1,3,9,11,5,7,13,15,2,4,10,12,6,8,14,16), \\
G_{2341} &: (1,2,9,10,5,6,13,14,3,4,11,12,7,8,15,16), \\
G_{2413} &: (1,3,9,11,2,4,10,12,5,7,13,15,6,8,14,16), \\
G_{2431} &: (1,2,9,10,3,4,11,12,5,6,13,14,7,8,15,16), \\
G_{3124} &: (1,5,3,7,9,13,11,15,2,6,4,8,10,14,12,16), \\
G_{3142} &: (1,5,2,6,9,13,10,14,3,7,4,8,11,15,12,16), \\
G_{3214} &: (1,3,5,7,9,11,13,15,2,4,6,8,10,12,14,16), \\
G_{3241} &: (1,2,5,6,9,10,13,14,3,4,7,8,11,12,15,16), \\
G_{3412} &: (1,3,2,4,9,11,10,12,5,7,6,8,13,15,14,16), \\
G_{3421} &: (1,2,3,4,9,10,11,12,5,6,7,8,13,14,15,16), \\
G_{4123} &: (1,5,3,7,2,6,4,8,9,13,11,15,10,14,12,16), \\
G_{4132} &: (1,5,2,6,3,7,4,8,9,13,10,14,11,15,12,16), \\
G_{4213} &: (1,3,5,7,2,4,6,8,9,11,13,15,10,12,14,16), \\
G_{4231} &: (1,2,5,6,3,4,7,8,9,10,13,14,11,12,15,16), \\
G_{4312} &: (1,3,2,4,5,7,6,8,9,11,10,12,13,15,14,16), \\
G_{4321} &: (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16).
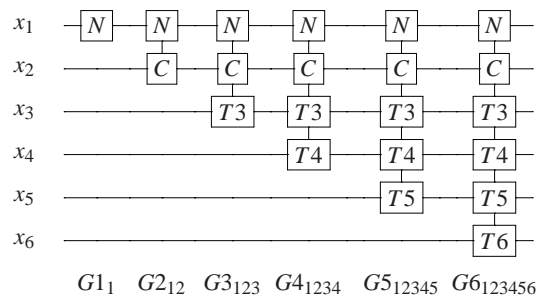\end{aligned}
\tag{14}
$$

Table 3: Utilization of gates in smallest universal sub libraries for 3-in/out reversible circuits.

Lib	Size of min Uni Sub Lib	Num of Sub Libs with min size	Num of Uni Sub Libs with min size	Utilization
NT	5	6	3	50%
NP	3	84	18	21.42%
NCT	4	495	21	4.24%
NCF	4	495	60	12.12%
NCP	3	455	30	6.59%
NCTF	4	1365	105	7.69%
NCPT	3	816	36	4.41%
NCPF	3	816	42	5.14%
G3	2	15	9	60%

Fig. 11: Extensions of *Gn* gate.

one gate type. The paper showed that common universal libraries must contain more than one gate type. This paper proposed a new gate type that is universal for *n*-in/out reversible circuits.

There is no systematic method to extend existing universal libraries to work over higher order circuits. The proposed gate is extendable in a trivial way to work over *n*-bit reversible circuits.

There is a trade-off between the number of gates used in a universal library and the size of the synthesized circuit. The paper showed that only 2 combinations of size *n* of the proposed gate can be used to synthesize any

arbitrary *n*-in/out reversible circuits. Using only 2 gates in the library might not produce a short circuit, i.e. the cascading of gates might be to long. The analysis of universal sub libraries for the proposed gate and the existing hybrid universal sub libraries to find the best sub library with minimum number of gates that produce an efficient circuit is an extension to this work.

References

[1] C. Bennett, Logical reversibility of computation. *IBM J. Res. Dev.*, *17* (6):525–532 (1997).

[2] E. Fredkin and T. Toffoli, Conservative logic. *Int. J. Theor. Phys.*, *21* : 219–253 (1982).

[3] J. Gruska, *Quantum computing*. McGraw-Hill, London (1999).

[4] M. Nielsen and I. Chuang, *Quantum computation and quantum information*. Cambridge University Press, Cambridge, United Kingdom (2000).

[5] A. De Vos, B. Desoete, F. Janiak, and A. Nogawski, Control gates as building blocks for reversible computers. In *Proc. of the 11th International Workshop on Power and Timing Modeling, Optimization and Simulation*, 9201–9210 (2001).

[6] A. De Vos, B. Desoete, A. Adamski, P. Pietrzak, M. Sibinski, and T. Widerski, Design of reversible logic circuits by means of control gates. In *Proceedings of the 10th International Workshop on Integrated Circuit Design, Power and Timing Modeling, Optimization and Simulation*, 255–264 (2000).

[7] T. Toffoli, Reversible computing. In W. de Bakker and J. van Leeuwen, editors, *Automata, Languages and Programming*, page 632. Springer, New York. *Technical Memo MIT/LCS/TM-151, MIT Lab for Computer Science*(unpublished) (1980).

[8] G. W. Dueck and D. Maslov, Reversible function synthesis with minimum garbage outputs. In *Proc. of the 6th International Symposium on Representations and Methodology of Future Computing Technologies*, 154–161 (2003).

[9] D. Maslov, G. W. Dueck, D. M. Miller, Fredkin/Toffoli templates for reversible logic synthesis. In *Proc. of the ACM/IEEE International Conference on Computer-Aided Design*, 256 (2003).

[10] D. M. Miller and G. W. Dueck, Spectral techniques for reversible logic synthesis. In *Proc. of the 6th International Symposium on Representations and Methodology of Future Computing Technologies*, 56–62 (2003).

[11] D. M. Miller, D. Maslov, and G. W. Dueck, A Transformation based algorithm for reversible logic synthesis. In *Proceedings of the 40th Conference on Design Automation*, 318–323 (2003).

[12] K. Iwama, Y. Kambayashi, and S. Yamashita, Transformation rules for designing CNOT–based quantum circuits. In *Proc. of the 39th Conference on Design Automation*, 419–424 (2002).

[13] D. Maslov, G. W. Dueck, and D. M. Miller, Simplification of Toffoli networks via templates. In *Proc. of the 16th Symposium on Integrated Circuits and Systems Design*, 53 (2003).

[14] D. Maslov, C. Young, D. M. Miller, and G. W.Dueck, Quantum circuit simplification using templates. *Design, Automation and Test in Europe*, 1208-1213 (2005).

[15] A. K. Prasad, V. V. Shende, K. N. Patel, I. L. Markov, and J. P. Hayes, Data structures and algorithms for simplifying reversible circuits. *J. Emerg. Technol. Comput. Syst.*, *2* (4): 277-293 (2006).

[16] O. Golubitsky, S. M. Falconer, and D. Maslov, Synthesis of the optimal 4-bit reversible circuits. In *Proc. of the 47th Design Automation Conference*, 653-656 (2010).

[17] D. Maslov (2011). Reversible logic synthesis benchmarks. *http://webhome.cs.uvic.ca/ dmaslov/* .

[18] A. Younes and J. Miller, Representation of Boolean quantum circuits as Reed-Muller expansions. *Int. J. Electron.*, *91* (7) 431–444 (2004).

[19] L. Storme, A. De Vos, and G. Jacobs, Group theoretical aspects of reversible logic gates. *J. Univers. Comput. Sci.*, *5* (5) 307–321 (1999).

[20] A. De Vos, B. Raa, and L. Storme, Generating the group of reversible logic gates. *J. Phys. A-Math. Theor.*, *35* (33) 7063–7078 (2002).

[21] A. De Vos and Y. Van Rentergem, From group theory to reversible computers. *Int. J. Unconv. Comput.*, *4* (1) 79–88 (2008).

[22] N. Abdessaieda, M. Soekena, M. K. Thomsena, and R. Drechslera, Upper bounds for reversible circuits based on Young subgroups *Inf. Process. Lett.*, *114* (6) 282-286 (2014).

[23] A. De Vos and A. De Baerdemacker, Symmetry groups for the decomposition of reversible computers, quantum computers, and computers in between. *Symm.*, *3* (2) 305-324 (2011).

[24] G. Yang, X. Song, W. N. N.Hung, M. A. Perkowski, and C.-J. Seo, Synthesis of reversible circuits with minimal costs. *Calcolo*, *45* 193–206 (2008).

[25] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.6.3; 2013. *http://www.gap-system.org*

[26] V. V. Shende, A. K. Prasad, I. L. Markov, and J. P. Hayes, Synthesis of reversible logic circuits. *IEEE Trans. on CAD*, *22* (6)pp. 710722 (2003).

[27] A. Younes, Tight Bounds on the Synthesis of 3-bit Reversible Circuits: NFFr Library. *J. Circuits Syst. Comput.*, *23* (3) 1450040 (2014).

[28] A. Younes, Tight bounds on the synthesis of 3-bit reversible circuits: NFT library *arXiv:1304.5804 [quant-ph]* (2014).

[29] M.I. Kargapolov and J.I. Merzljakov, *Fundamentals of the theory of groups*. Berlin: Springer (1979).

[30] J.D. Dixon and B. Mortimer, *Permutation groups*. New York: Springer (1996).

[31] A. De Vos, *Reversible computing*. Wiley-VCH, Weinhiem, pp. 49 (2010).

[32] T. Beth and M. Roetteler, *Quantum algorithms: applicable algebra and quantum physics*. In *Quant. Inf.*, 96–150 (2001).

Ahmed Younes is a Computer Science Associate Professor at Alexandria University and Honorary Research Fellow at School of Computer Science, University of Birmingham. He obtained his PhD from University of Birmingham, United Kingdom. He introduced a new technique, now called as 'Partial Diffusion Operator' in the field of amplitude amplification. He published papers in Quantum Algorithms, Quantum cryptography and Reversible Circuits.