Enumeration of reversible functions and its application to circuit complexity

Mathias Soeken[1], Nabila Abdessaied[2], and Giovanni De Micheli[1]

[1] Integrated Systems Laboratory, EPFL, Switzerland
[2] Cyber-Physical Systems, DFKI GmbH, Bremen, Germany
mathias.soeken@epfl.ch

Abstract. We review combinational results to enumerate and classify reversible functions and investigate the application to circuit complexity. In particularly, we consider the effect of negating and permuting input and output variables and the effect of applying linear and affine transformations to inputs and outputs. We apply the results to reversible circuits and prove that minimum circuit realizations of functions in the same equivalence class differ at most in a linear number of gates in presence of negation and permutation and at most in a quadratic number of gates in presence of linear and affine transformations.

Keywords: Reversible function, equivalence class, permutation group, reversible circuit complexity

1 Introduction

In 1959, Nicolaas Govert de Bruijn has generalized George Pólya's theorem [14] for counting the number of equivalence classes that result from partitioning the set of all functions $f : D \to R$ under the consideration of permutation groups G and H acting on domain D and range R, respectively [4]. Two functions f_1 and f_2 are considered equivalent if there exists permutations $\pi \in G$ and $\sigma \in H$ such that $f_1(x) = \sigma f_2(\pi x)$ for all $x \in D$. The computation involves the groups' cycle index polynomials. Driven by the work of C.S. Lorens [12], Michael A. Harrison has investigated the effect of negation and permutation (using cycle indices derived by Ashenhurst [2] and Slepian [16]) and the effect of linear and affine transformations for Boolean functions [11]. As special cases he also considered the application of all these groups to reversible functions [8, 11]. Primenko [15] applied an alternative method to count the number of equivalence classes, but considered different permutation groups in his work.

In this paper, we review the above mentioned work. Afterwards, we and compute and apply the combinational results to reversible circuits and circuit complexity. We relate the investigated permutation groups to classes of reversible gates. Furthermore, we show that the size difference of reversible circuits composed of mixed-polarity multiple-controlled Toffoli (MPMCT) gates for functions of the same equivalence class is (i) linearly bounded when applying negations

and permutation of inputs and outputs and (ii) quadratically bounded when applying linear and affine transformations to inputs and outputs.

For reversible functions with 2 and 3 variables, we explicitly enumerate all equivalence classes and their circuit realizations which allows us to derive correlations and find conjectures. It is unclear whether the classification helps to find a class of *difficult* reversible functions, i.e., functions which have reversible circuits of worst-case or almost worst-case size. Thomas G. Draper [5] has conducted a similar study. He uses complementary techniques to classify Boolean functions into the same classes and uses his results to introduce a new notion of complexity. This notion allows to measure a circuit's complexity in terms of "rounds of nonlinearity" instead of counting gates.

The paper is organized as follows. Section 2 introduces necessary notation and definitions. Section 3 reviews how to compute the number of equivalence classes in reversible functions when applying permutation groups to inputs and outputs. Section 4 applies the results to circuit complexity of reversible circuits and Sect. 5 to Boolean functions. Section 6 concludes the paper.

2 Preliminaries

This section introduces background on permutation groups and reversible functions and circuits.

2.1 Permutation groups

We assume that the reader is familiar with the basics of permutation groups, i.e., subgroups of the symmetric group S_n over the elements $\{0, \ldots, n-1\}$. Including 0 in the set is unconventional but simplifies forthcoming computations. In the following, we introduce integer partitions and borrow the notation of [1].

Definition 1 (Integer partition). *An* integer partition *of a natural number n is a sequence of natural numbers $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ such that*

$$\lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_k \qquad \text{and} \qquad \lambda_1 + \lambda_2 + \cdots + \lambda_k = n. \tag{1}$$

We call the λ_i the parts of λ and write $\lambda \vdash n$ to say that λ is an integer partition of n. Sometimes it is useful to directly refer to the counts of a part. If $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \vdash n$, we write

$$\lambda = (1^{f_1} 2^{f_2} \ldots n^{f_n}), \tag{2}$$

where

$$f_i = |\{1 \leqslant j \leqslant k \mid \lambda_j = i\}| \qquad \text{for } 1 \leqslant i \leqslant n, \tag{3}$$

i.e., exactly f_i of the λ_j are equal to i. Also, we define

$$z_\lambda = \prod_{i=1}^{n} i^{f_i} f_i!. \tag{4}$$

Example 1. All integer partitions of $n = 4$ are

$$(1,1,1,1) \qquad (1,1,2) \qquad (1,3) \qquad (2,2) \qquad (4).$$

For $\lambda = (1,1,2)$ we have $f_1 = 2, f_2 = 1, f_3 = 0$, and $f_4 = 0$. Note that $\sum_{i=1}^{n} i f_i = n$.

Definition 2 (Permutation type). *Let $\pi \in S_n$ be a permutation. Then its* type $\text{type}(\pi) \vdash n$ *is an integer partition where each element corresponds to the length of one cycle in the cyclic representation of π.*

Example 2. Let $\pi = (0,1)(2)(3,7,4)(5,6) \in S_8$. Then $\text{type}(\pi) = (1,2,2,3)$.

Theorem 1 (e.g., [1]). *For each $\lambda \vdash n$, the number of permutations $\pi \in S_n$ with $\text{type}(\pi) = \lambda$ is $\frac{n!}{z_\lambda}$.* □

Definition 3 (Cycle index polynomial). *Let $G \subseteq S_n$ be a permutation group and*

$$g(\lambda) = |\{\pi \in G \mid \text{type}(\pi) = \lambda\}| \tag{5}$$

be the number of permutations in G that have type $\lambda \vdash n$. The cycle index polynomial *of G is*

$$Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{\lambda \vdash n} g(\lambda) x_1^{f_1} x_2^{f_2} \cdots x_n^{f_n}. \tag{6}$$

For each $\lambda \vdash n$ we implicitly assume that $\lambda = (1^{f_1} 2^{f_2} \ldots n^{f_n})$ as introduced in (2). We use the f_i in the same manner in the remainder of this paper.

Example 3. Let $G_1 = \{\pi_e\} \subset S_n$ where π_e is the identity permutation. Then

$$Z_{G_1} = x_1^n,$$

since G contains a single permutation of type $\lambda = (1, 1, \ldots, 1)$ and $f_1 = n$.

Let $G_2 = \{(0)(1)(2)(3), (0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$. Then

$$Z_{G_2} = \tfrac{1}{4}\left(x_1^4 + 3x_2^2\right),$$

since G contains four permutations, one of type $\lambda = (1,1,1,1)$ with $f_1 = 4$ and three of type $\lambda = (2,2)$ with $f_2 = 2$.

Let $G_3 = S_n$. Then

$$Z_{G_3} = \frac{1}{n!} \sum_{\lambda \vdash n} \frac{n!}{z_\lambda} x_1^{f_1} x_2^{f_2} \cdots x_n^{f_n},$$

because there are $n!$ permutations out of which $\frac{n!}{z_\lambda}$ have type λ (see Thm. 1).

Harrison reformulated De Bruijn's enumeration theorem [4] for the special case of reversible functions, and it is restated here.

Theorem 2 (De Bruijn [4], Harrison [8]). *The number of classes of reversible functions of n variables with a group G acting on the domain and a group H acting on the range is*

$$Z_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \cdots, \frac{\partial}{\partial z_k}\right) Z_H(1+z_1, 1+2z_2, \cdots, 1+sz_s) \tag{7}$$

evaluated at $z_1 = z_2 = \cdots = z_s = 0$ where $s \leqslant 2^n$.

Harrison introduces the notation of a *product of variables* to ease writing the complex cycle index polynomials (see also Sect. 3.2).

Definition 4 (Product of variables [10]). *Let $x_1^{i_1} \cdots x_r^{i_r}$ and $x_1^{j_1} \cdots x_s^{j_s}$ be two products of variables. The product of these terms, written '$\times$', is defined as*

$$\prod_{p,q} (x_p^{i_p} \times x_q^{j_q}) \tag{8}$$

where

$$x_p^{i_p} \times x_q^{i_q} = x_{\operatorname{lcm}(p,q)}^{i_p j_q \gcd(p,q)}$$

and gcd *and* lcm *are the greatest common divisor and least common multiple, respectively.*

2.2 Reversible functions and circuits

Let $\mathbb{B} = \{0, 1\}$ denote the *Boolean values*. We refer to functions $f\colon \mathbb{B}^n \to \mathbb{B}^m$ as *Boolean multiple-output functions* with n inputs and m outputs. We define $x^0 = \bar{x}$ and $x^1 = x$.

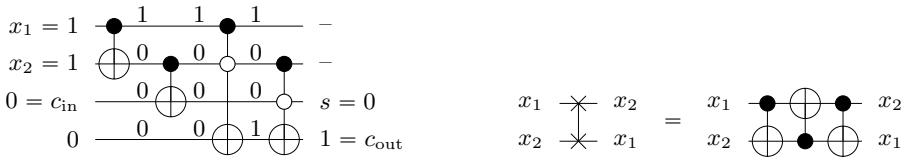
Definition 5 (Reversible function). *A function $f\colon \mathbb{B}^n \to \mathbb{B}^n$ is called* reversible *if f is bijective, i.e., if each input pattern uniquely maps to an output pattern, and vice versa. Otherwise, it is called* irreversible.

Each reversible function $f\colon \mathbb{B}^n \to \mathbb{B}^n$ corresponds to a permutation $\pi_f \in S_{2^n}$ by letting

$$f(x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1}) \quad \text{if and only if} \quad \pi(x) = y, \tag{9}$$

where $x = (x_0 x_1 \ldots x_{n-1})_2$ and $y = (y_0 y_1 \ldots y_{n-1})_2$ are the binary expansions of x and y. Reversible functions over n variables are realized by reversible circuits consisting of least n lines with gates from library of reversible gates. In this work, we consider the library of mixed-polarity multiple control Toffoli gates [18].

Definition 6 (MPMCT gate). *Let $X = \{x_1, \ldots, x_n\}$ be a set of variables. A* mixed-polarity multiple-control Toffoli (MPMCT) *gate* $\mathrm{T}(C, t)$ *has* control lines $C = \{x_{j_1}^{p_1}, x_{j_2}^{p_2}, \ldots, x_{j_k}^{p_k}\}$ *and a* target line $t \in X$ *with* $\{t, \bar{t}\} \notin C$. *The gate maps* $t \mapsto t \oplus (x_{j_1}^{p_1} \wedge x_{j_2}^{p_2} \wedge \cdots \wedge x_{j_k}^{p_k})$. *Values on remaining lines are passed through unaltered. A positive literal in C is referred to as* positive control line *and a negative literal as* negative control line. *A gate* $\mathrm{T}(\{x_i\}, t)$ *is called a* CNOT *gate, and a gate* $\mathrm{T}(\{\}, t)$ *is called a* NOT *gate.*



(a) Full adder (b) SWAP gate

Fig. 1. Reversible circuits.

Table 1. The permutation groups that are considered in this paper to act on the inputs and outputs of reversible functions over n variables. The table shows its notation, order, corresponding gate library, as well as the reference in which the cycle index polynomial has been derived.

Group	Notation	Order	Gates	Cycle index
Complementations	$\mathcal{C}_n$	2^n	NOT	[2]
Permutations	$\mathcal{S}_n$	$n!$	SWAP	[10]
Compl. and perm.	$\mathcal{G}_n$	$n!2^n$	SWAP, NOT	[10]
Linear transf.	$\mathcal{L}_n$	$2^{n(n-1)/2} \prod_{i=1}^{n} (2^i - 1)$	CNOT	[11]
Affine transf.	$\mathcal{A}_n$	$2^{n(n+1)/2} \prod_{i=1}^{n} (2^i - 1)$	CNOT, NOT	[11]

Example 4. Figure 1a shows a reversible circuit that realizes a full adder. The annotated values demonstrate the intermediate values of the gates for a given input assignment. The control lines are either denoted by solid black circles to indicate positive controls, or white circles to indicate negative controls. The target line is denoted by '$\oplus$'. Figure 1b depicts a SWAP gate for two variables and its realization using CNOT gates. In total three gates are required. The SWAP gate is not part of the MPMCT gate library.

3 Reversible function classification

In this section we review the main results from [8] and [11]. These works derive the number of classes after applying different permutation groups, which are subgroups of S_{2^n}, to the domain and range of reversible Boolean functions over n variables. The considered permutation groups are the group of *complementations* $\mathcal{C}_n$, the group of *permutations* $\mathcal{S}_n$, the group of *complementations and permutations* $\mathcal{G}_n$, the group of *linear transformations* $\mathcal{L}_n$, and the group of *affine transformations* $\mathcal{A}_n$. We slightly simplified the notation of the groups compared to the original papers for the sake of readability. We provide detailed definitions of all groups in the remainder of this section; a summary of the groups is given in Table 1.

3.1 Permutation groups

The aim of the following definitions is to describe a constructive approach on how to derive the permutations that are contained in the considered groups.

This is orthogonal to the algebraic approach used in [8] and [11] in which the groups are expressed in terms of other algebraic structures.

Definition 7. *The group of all 2^n complementations of n variables is*

$$\mathcal{C}_n = \bigcup_{0 \leqslant b < 2^n} \pi_b, \tag{10}$$

where $\pi_b \in S_{2^n}$ is a permutation such that $\pi_b(j) = j \oplus b$ for all $0 \leqslant j < 2^n$ and $j \oplus b$ refers to the bit-wise exclusive OR (addition modulo 2) on the binary expansions of j and b.

Example 5. The group $G_2 = \{(0)(1)(2)(3), (0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$ in Example 3 is $\mathcal{C}_2$.

The group $\mathcal{C}_n$ contains all permutations that are described by all reversible circuits on n lines that only contain NOT gates.

Definition 8. *The group of all $n!$ permutations of n variables is*

$$\mathcal{S}_n = \bigcup_{\sigma \in S_n} \pi_\sigma, \tag{11}$$

where $\pi_\sigma \in S_{2^n}$ is a permutation such that $\pi_\sigma(j) = (j_{\sigma 0} j_{\sigma 1} \dots j_{\sigma(n-1)})_2$ and $j = (j_0 j_1 \dots j_{n-1})_2$ is the binary expansion of j.

Example 6. We have $\mathcal{S}_2 = \{\pi_e, (1,2)\}$ and

$$\mathcal{S}_3 = \{\pi_3, (1,2)(5,6), (2,4)(3,5), (1,2,4)(3,6,5), (1,4)(3,6), (1,4,2)(3,5,6)\}.$$

The group $\mathcal{S}_n$ contains all permutations that are described by all reversible circuits on n lines that only contain SWAP gates.

Definition 9. *The group of all complementations and permutations is the combination of $\mathcal{C}_n$ and $\mathcal{S}_n$ and is denoted*

$$\mathcal{G}_n = \mathcal{C}_n \rtimes \mathcal{S}_n, \tag{12}$$

where '$\rtimes$' is the semi-direct product.

Example 7. We have

$$\mathcal{G}_2 = \{\pi_e, (0,3), (1,2), (0,1)(2,3), (0,2)(1,3), (0,3)(1,2), (0,1,3,2), (0,2,3,1)\}.$$

The notion of the semi-direct product is transferred to the circuit analogy of the group: The group $\mathcal{G}_n$ contains all permutations that are described by all reversible circuits on n lines that only contain SWAP and NOT gates.

Definition 10. *The group of all* linear transformations *on n variables is*

$$\mathcal{L}_n = \bigcup_{\substack{A \in \mathbb{B}^{n \times n} \\ \det(A) \neq 0}} \pi_A \tag{13}$$

where $\pi_A \in S_{2^n}$ is a permutation such that

$$\pi_A(j) = k \quad \textit{if, and only if} \quad A(j_0, j_1, \ldots, j_{n-1})^T = (k_0, k_1, \ldots, k_{n-1})^T,$$

where $j = (j_0 j_1 \ldots j_{n-1})_2$ and $k = (k_0 k_1 \ldots k_{n-1})_2$ are the binary expansions of j and k. Note that all arithmetic operations in $\det(A)$ are modulo 2.

Example 8. We have

$$\mathcal{L}_2 = \{\pi_e, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}.$$

The group $\mathcal{L}_n$ contains all permutations that are described by all reversible circuits on n lines that only contain CNOT gates that have a positive control line.

Definition 11. *The group of all* affine transformations *on n variables is*

$$\mathcal{A}_n = \mathcal{C}_n \rtimes \mathcal{L}_n. \tag{14}$$

Example 9. We have $\mathcal{A}_1 = S_2$ and $\mathcal{A}_2 = S_4$. However, note that $\mathcal{A}_3 \neq S_8$, as for example permutation $(6,7) \in S_8$ which corresponds to the Toffoli gate $\mathrm{T}(\{x_1, x_2\}, x_3)$ is not contained in $\mathcal{A}_3$.

The group $\mathcal{L}_n$ contains all permutations that are described by all reversible circuits on n lines that only contain CNOT gates and NOT gates.

3.2 Cycle index polynomials

In order to derive the number of equivalence classes using Theorem 2, one must derive the cycle index polynomial of the considered group. These are not simple to derive and we only give the general idea on how to derive them. References to detailed proofs are listed in the last column of Table 1. The simplest one is $Z_{\mathcal{C}_n}$:

$$Z_{\mathcal{C}_n} = \frac{1}{2^n}\left(x_1^{2^n} + (2^n - 1)x_2^{2^{n-1}}\right) \tag{15}$$

The group $\mathcal{C}_n$ contains of the identity (corresponds to no NOT gate on any line) and $2^n - 1$ permutations that consists of 2^{n-1} transpositions, i.e., cycles of size 2 [2] (corresponds to all configuration where there is at least one NOT gate on a line).

Example 10. We give an example on how Theorem 2 can be applied to

$$\mathcal{Z}_{\mathcal{C}_2} = \frac{1}{4}\left(x_1^4 + 3x_2^2\right)$$

in order to derive the number of equivalence classes of reversible functions over 2 variables with complementation acting on inputs and outputs. We need to compute

$$Z_{\mathcal{C}_2}\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}\right) Z_{\mathcal{C}_2}(1+z_1, 1+2z_2)$$

evaluated at $z_1 = z_2 = 0$. The first factor in the product evaluates to

$$Z_{\mathcal{C}_2}\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}\right) = \frac{1}{4}\left(\frac{\partial^4}{\partial z_1^4} + 3\frac{\partial^2}{\partial z_2^2}\right)$$

and the second product evaluates to

$$Z_{\mathcal{C}_2}(1+z_1, 1+2z_2) = \frac{1}{4}((1+z_1)^4 + 3(1+2z_2)^2).$$

The first factor is a sum containing partial derivatives and the second factor is a sum containing polynomials. The effect of the distributive law when multiplying the two factors is to combine all partial derivatives with all polynomials:

$$\frac{1}{16}\left(\frac{\partial^4}{\partial z_1^4}(1+z_1)^4 + \frac{\partial^4}{\partial z_1^4}3(1+2z_2)^2 + 3\frac{\partial^2}{\partial z_2^2}(1+z_1)^4 + 3\frac{\partial^2}{\partial z_2^2}3(1+2z_2)^2\right)$$

The second and the third term vanish and one gets $\frac{1}{16} \cdot 24 \cdot 3 \cdot 24 = 6$.

In [8], a lemma describes the effect of applying the resulting partial derivatives to the resulting polynomials in general. This allows to obtain a closed form solution for some cycle index polynomials. For example, applying Theorem 2 to $Z_{\mathcal{C}_n}$ simplifies to

$$\frac{1}{2^{2n}}\left(2^n! + (2^n-1)^2(2^{n-1})!2^{2^{n-1}}\right). \tag{16}$$

Key to derive the cycle index polynomial for $\mathcal{S}_n$ is to notice that π_σ in (11) is a homomorphism from S_n to S_{2^n} [10]. From this, one can derive that for two permutations $\sigma_1, \sigma_2 \in S_n$ with $\text{type}(\sigma_1) = \text{type}(\sigma_2)$ one also has $\text{type}(\pi_{\sigma_1}) = \text{type}(\pi_{\sigma_2})$. Investigating in detail how a k-cycle in σ translates to π_σ yields

$$Z_{\mathcal{S}_n} = \frac{1}{n!}\sum_{\lambda \vdash n}\frac{n!}{z_\lambda}\prod_{i_1|1}\cdots\prod_{i_n|n} x_{\text{lcm}(i_1,\ldots,i_n)}^{g(f_1,i_1)\cdots g(f_n,i_n)\,\gcd(i_1,\ldots,i_n)} \tag{17}$$

where

$$g(f_k, i_k) = \frac{1}{i_k}\sum_{d|i_k} 2^{f_k d}\mu\left(\frac{i_k}{d}\right) \tag{18}$$

where μ is the Möbius function.

A technique in [7] shows how to derive the cycle index polynomial for a permutation group $G = G_1 \rtimes G_2$ from its constituent groups. Applied to $\mathcal{G}_n = \mathcal{C}_n \rtimes \mathcal{S}_n$, this yields [8]:

$$Z_{\mathcal{G}_n} = \frac{1}{n!2^n}\sum_{\lambda \vdash n}\frac{n!2^n}{\prod_{i=1}^n f_i!(2i)^{f_i}}\bigtimes_{i=1}^{n}\left(\prod_{d|i} x_d^{e(d)} + \prod_{\substack{d|2i \\ d\nmid i}} x_d^{g(d)}\right)^{\times f_i} \tag{19}$$

Table 2. Number of equivalence classes when applying a permutation group to the inputs and outputs of all reversible functions over n variables.

n	$\mathcal{C}_n$ (NN)	$\mathcal{S}_n$ (PP)	$\mathcal{G}_n$ (NPNP)	$\mathcal{L}_n$ (LL)	$\mathcal{A}_n$ (AA)
1	1	2	1	2	1
2	6	7	2	2	1
3	924	1 172	52	10	4
4	81 738 720 000	36 325 278 240	142 090 700	52 246	302

with

$$e(k) = \frac{1}{k} \sum_{d|k} 2^d \mu\left(\frac{k}{d}\right) \quad \text{and} \quad g(2k) = \frac{1}{2k} \sum_{\substack{d|2k \\ d\nmid k}} 2^{d/2} \mu\left(\frac{2k}{d}\right). \tag{20}$$

Based on the properties of irreducible polynomials of $\mathbb{Z}_2[x]$ and the technique described in [7], in [11] the cycle index polynomials for $\mathcal{L}_n$ and $\mathcal{A}_n$ are derived. Since their description is quite involved and requires a lot of additional definitions, the reader is referred to [11] for all details.

The number of equivalence classes that result from applying the described five permutation groups both to the inputs and outputs of n-variable reversible functions is given in Table 2 for $n \leqslant 4$. In the remainder, we refer to two reversible functions f and g as NN-equivalent, if they are in the same equivalence class when the group $\mathcal{C}_n$ acts on both inputs and outputs. We use the abbreviations PP-, NPNP-, LL-, and AA-equivalent for the groups $\mathcal{S}_n$, $\mathcal{G}_n$, $\mathcal{L}_n$, and $\mathcal{A}_n$, respectively.

4 Application to reversible circuits

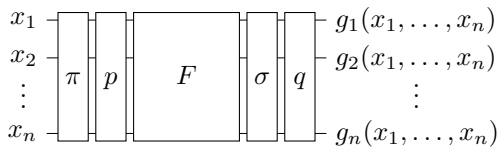
In this section we discuss how to apply the above introduced classification to reversible circuits. We study the relation of optimal circuit realizations for functions in the same equivalence class. Optimality refers to the minimal number of required Toffoli gates in an MPMCT circuit.

Theorem 3. *Let f and g be two NPNP-equivalent reversible functions over n variables. Then the size difference of two optimal circuits for f and g is at most $3(n-1)$ gates.*

Proof. Let F be an optimal circuit for f. Since f and g are NPNP-equivalent, there exists two permutations $\pi, \sigma \in S_n$ and two bit-vectors $p, q \in \mathbb{B}^n$ such that

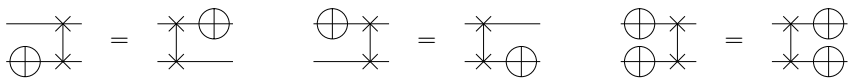
$$g_j(x_1, \ldots, x_n) = f_{\sigma j}^{q_j}\left(x_{\pi 1}^{p_1}, \ldots, x_{\pi_n}^{p_n}\right)$$

for all $1 \leqslant j \leqslant n$. A circuit for g can therefore be obtained from F by extending it with circuits for the permutations and negations:

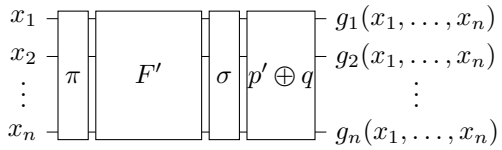


Since each permutation in S_n can be decomposed into $n-1$ transpositions, the circuits for π and σ consist each of at most $n-1$ SWAP gates. The circuits for p and q consist each of at most n NOT gates.

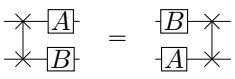
First, we move the circuit for p to the right of F by switching the polarities of the controls on lines i if $p_i = 1$ [17], leading to an updated circuit F' of the same size. Using the identities


(21)

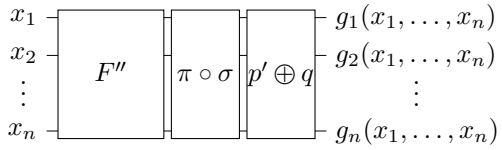
we can then pass the NOT gates to the back of the circuit, which changes p into p':



The circuit that realizes $p' \oplus q$ requires at most n NOT gates. A generalization of the identities in (21) is

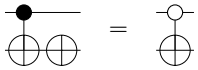


in which A and B are either an empty line, a control line, or a target line. This identity allows to move all SWAP gates in π over F' by updating the gates accordingly, resulting in a circuit F'' still of the same size as F:



The permutation $\pi \circ \sigma$ is still an element of S_n and hence can be realized using $(n-1)$ SWAP gates which are $3(n-1)$ CNOT gates.

The identity



allows to absorb NOT gates from $p \oplus q$ into CNOT gates from $\pi \circ \sigma$. The worst case requires all $(n-1)$ SWAP gates, since a SWAP gate need at least 3 CNOT gates [19]. In other words, in the worst case, there cannot be a line that is not part of a CNOT gate but contains a NOT gate. □

Conjecture 1. Let $\sigma \in S_n$. Any circuit that realizes π_σ requires at least $3(n-1)$ gates.

A proof to Conjecture 1 would make the upper bound of Theorem 3 a tight bound. We leave the proof to this conjecture for future work, but show experimental evidences for the validity later in this section and show that the conjecture is valid for $n = 2$ and $n = 3$.

Theorem 4. *Let f and g be two LL-equivalent reversible functions over n variables. Then the size difference of two optimal circuits for f and g is at most $2n^2$ gates.*

Proof. We apply the same technique as in Theorem 3 and construct a circuit for g from a minimal circuit for f by extending it with two circuits in the front and in the back that realize linear reversible functions. The result follows from the property that any linear reversible function over n variables can be realized with at most n^2 CNOT gates [3]. Since CNOT gates cannot easily be moved through a circuit without changing the size of the circuit, improving the bound as in the proof for Theorem 3 is not obvious. □

Corollary 1. *Let f and g be two AA-equivalent reversible functions over n variables. Then the size difference of two optimal circuits for f and g is at most $2n^2$ gates.*

Proof. This follows from applying the NOT absorption argument used in the proof to Theorem 3 to the result of Theorem 4. □

Evaluation. We computed all optimal reversible circuits for reversible functions of 2 and 3 variables and classified them with respect to NPNP-, LL-, and AA-equivalence. Tables 3 and 4 list the results of the evaluation. Each row refers to one equivalence class identified by its representative, which is chosen to be the lexicographically smallest permutation. For each class, the tables mention the size of the equivalence class (*Size*), the size of the smallest optimal reversible circuit in the class (*Min*), and the size of the largest optimal reversible circuit in the class (*Max*). Equivalence classes are sorted first by the size of the smallest circuit and in case of a tie by the size of the largest circuit. The bottom row lists the number of classes and the number of reversible functions.

The experimental results give evidence for the validity of Conjecture 1. The equivalence class π_e for NPNP-classification has Min = 0 and Max = 3 for $n = 2$ and Min = 0 and Max = 6 for $n = 3$, i.e., the difference is $3(n-1)$. Among the largest circuits in the equivalence class are the permutations $\pi_{(0,1)} \in \mathcal{S}_2$ and

Table 3. Equivalence classes for all 2-variable reversible functions in NPNP-, LL-, and AA-classification.

Representative	Size	Min	Max
$[0, 1, 2, 3]$	8	0	3
$[0, 3, 2, 1]$	16	1	2
2	24		

(a) NPNP-equivalence

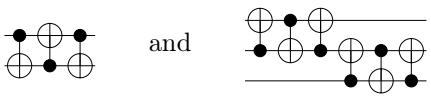
Representative	Size	Min	Max
$[0, 1, 2, 3]$	6	0	3
$[2, 3, 0, 1]$	18	1	3
2	24		

(b) LL-equivalence

Representative	Size	Min	Max
$[0, 1, 2, 3]$	24	0	3
1	24		

(c) AA-equivalence

$\pi_{(0,1)(1,2)} \in \mathcal{S}_3$, which are those permutations with the maximum number of transpositions:



It is hard to derive from the results a class of *difficult* functions, i.e., where almost each function requires the maximum number of gates in its optimal circuit realization. For NPNP-equivalence of 3-variable functions, there are 4, 30, and 18 classes for which Max is 4, 5, and 6. For LL- and AA-equivalence each equivalence class contains at least one difficult function (however, a regular pattern of the values for Min can be observed). As a result, without results for reversible functions with more than 3 variables, it is not possible to derive any conclusions.

Already Lorens [13] listed all equivalence classes of 3-variable reversible functions under these permutation groups. He devised a further classification based on properties of the inverse permutations of the equivalence classes' representatives. However, no correspondence to reversible circuits is given.

We provide the details of this evaluation including one minimal MPMCT circuit for each function in each equivalence class (for each considered permutation group) on `msoeken.github.io/revclass.html`. We expect that several interesting correlations and conjectures can be found in this data set. The web page also contains the programs that produced the enumeration results. By integrating them with the techniques described by Golubitsky [6], one may be able to obtain the classification results for 4-variable reversible functions.

Table 4. Equivalence classes for all 3-variable reversible functions in NPNP-, LL-, and AA-classification.

Representative	Size	Min	Max
[0, 1, 2, 3, 4, 5, 6, 7]	48	0	6
[0, 1, 6, 7, 4, 5, 2, 3]	288	1	5
[0, 1, 2, 7, 4, 5, 6, 3]	576	1	5
[0, 1, 7, 6, 5, 4, 2, 3]	288	2	5
[0, 5, 6, 3, 4, 1, 2, 7]	144	2	4
[0, 3, 6, 5, 4, 7, 2, 1]	288	2	5
[0, 1, 7, 6, 4, 5, 3, 2]	144	2	5
[0, 1, 6, 5, 4, 7, 2, 3]	576	2	5
[0, 1, 7, 6, 4, 5, 2, 3]	1152	2	5
[0, 1, 2, 5, 6, 7, 4, 3]	576	2	5
[0, 1, 2, 5, 4, 7, 6, 3]	2304	2	6
[0, 1, 2, 7, 6, 5, 4, 3]	1152	2	5
[0, 3, 5, 6, 7, 4, 2, 1]	144	3	4
[0, 1, 3, 6, 5, 4, 2, 7]	576	3	5
[0, 1, 5, 6, 7, 4, 2, 3]	576	3	4
[0, 3, 7, 5, 4, 6, 2, 1]	576	3	5
[0, 1, 2, 5, 4, 3, 6, 7]	288	3	5
[0, 1, 7, 5, 4, 6, 3, 2]	288	3	6
[0, 1, 7, 5, 4, 6, 2, 3]	1152	3	5
[0, 1, 6, 5, 4, 7, 3, 2]	1152	3	5
[0, 5, 3, 6, 4, 1, 2, 7]	576	3	5
[0, 3, 5, 6, 4, 7, 2, 1]	576	3	4
[0, 1, 5, 6, 4, 7, 2, 3]	1152	3	5
[0, 1, 2, 4, 7, 6, 5, 3]	576	3	5
[0, 1, 2, 5, 7, 6, 4, 3]	1152	3	5
[0, 1, 3, 5, 6, 7, 4, 2]	1152	3	5
[0, 1, 3, 5, 4, 6, 7, 2]	1152	3	5
[0, 1, 2, 5, 4, 6, 7, 3]	2304	3	6
[0, 5, 2, 1, 4, 7, 6, 3]	288	3	5
[0, 1, 3, 5, 4, 7, 6, 2]	1152	3	6
[0, 1, 2, 4, 5, 7, 6, 3]	2304	3	6
[1, 0, 2, 5, 4, 7, 6, 3]	2304	3	6
[0, 1, 2, 6, 7, 5, 4, 3]	1152	3	6
[1, 0, 2, 7, 6, 5, 4, 3]	384	3	6
[0, 1, 3, 4, 7, 6, 2, 5]	288	4	5
[0, 1, 3, 6, 7, 4, 2, 5]	1152	4	5
[0, 1, 5, 2, 3, 4, 6, 7]	288	4	5
[0, 1, 5, 7, 6, 4, 3, 2]	288	4	5
[0, 7, 3, 1, 4, 6, 2, 5]	576	4	5
[0, 1, 2, 4, 5, 3, 7, 6]	576	4	5
[0, 1, 2, 5, 4, 3, 7, 6]	576	4	6
[0, 1, 3, 5, 4, 2, 6, 7]	576	4	6
[0, 5, 3, 1, 4, 6, 2, 7]	576	4	6
[0, 1, 3, 5, 4, 6, 2, 7]	1152	4	6
[0, 5, 6, 1, 4, 3, 7, 2]	576	4	5
[0, 5, 1, 6, 4, 3, 2, 7]	576	4	5
[0, 1, 5, 2, 4, 3, 6, 7]	576	4	6
[0, 5, 2, 1, 3, 6, 4, 7]	1152	4	5
[0, 1, 2, 5, 4, 6, 3, 7]	384	4	6
[0, 5, 2, 1, 4, 6, 7, 3]	1152	4	6
[0, 1, 2, 5, 6, 4, 7, 3]	1152	4	6
[0, 5, 3, 1, 6, 4, 2, 7]	192	5	6
52	40320		

(a) NPNP-equivalence

Representative	Size	Min	Max
[0, 1, 2, 3, 4, 5, 6, 7]	168	0	6
[4, 5, 6, 7, 0, 1, 2, 3]	1176	1	6
[0, 1, 2, 7, 4, 5, 6, 3]	1176	1	6
[4, 1, 2, 3, 0, 5, 6, 7]	1176	1	6
[4, 7, 6, 5, 0, 1, 2, 3]	7056	2	6
[0, 1, 2, 5, 4, 7, 6, 3]	2352	2	6
[2, 1, 0, 7, 4, 5, 6, 3]	7056	2	6
[4, 6, 7, 5, 0, 1, 2, 3]	9408	3	6
[0, 1, 2, 5, 4, 6, 7, 3]	1344	3	6
[1, 0, 2, 5, 4, 7, 6, 3]	9408	3	6
10	40320		

(b) LL-equivalence

Representative	Size	Min	Max
[0, 1, 2, 3, 4, 5, 6, 7]	1344	0	6
[0, 1, 2, 7, 4, 5, 6, 3]	9408	1	6
[0, 1, 2, 5, 4, 7, 6, 3]	18816	2	6
[0, 1, 2, 5, 4, 6, 7, 3]	10752	3	6
4	40320		

(c) AA-equivalence

5 Application to Boolean functions

Harrison has also investigated the effect of the groups $\mathcal{C}_n$, $\mathcal{S}_n$, $\mathcal{G}_n$, $\mathcal{L}_n$, and $\mathcal{A}_n$ when being applied to the domain of Boolean functions $f : \mathbb{B}^n \to \mathbb{B}$. The results

Table 5. Number of equivalence classes of Boolean functions when applying a permutation group to the domain.

n	$\mathcal{C}_n$ [10]	$\mathcal{S}_n$ [10]	$\mathcal{G}_n$ [10]	$\mathcal{L}_n$ [11]	$\mathcal{A}_n$ [11]	S_{2^n}
1	3	4	3	4	3	3
2	7	12	6	8	5	5
3	46	80	22	20	10	9
4	4 336	3 984	402	92	32	17
5	134 281 216	37 333 248	1 228 158	2 744	382	33
6	288 230 380 379 570 176	25 626 412 338 274 304	400 507 806 843 728	950 998 216	15 768 919	65

Table 6. Number of equivalence classes of Boolean functions when applying a permutation group to the domain and output complementation.

n	$\mathcal{C}_n$ [9]	$\mathcal{S}_n$ [9]	$\mathcal{G}_n$ [9]	$\mathcal{L}_n$ [11]	$\mathcal{A}_n$ [11]	S_{2^n}
1	2	2	2	2	2	2
2	5	6	4	4	3	3
3	30	40	14	10	6	5
4	2 288	1 992	222	46	18	9
5	67 172 352	18 666 624	616 126	1 372	206	17
6	144 115 192 303 714 304	12 813 206 169 137 152	200 253 952 527 184	475 999 108	7 888 299	33

can be found in [10] and [11]. All these groups are subgroups of S_{2^n} which is isomorphic to the set of all reversible functions over n variables (see Eq. (9)). In this section, we investigate the effect of the group S_{2^n} when applied to the domain of Boolean functions. This corresponds to a reversible transformation of the input variables, which can, e.g., be realized using a reversible circuit.

We apply Pólya's theorem [14] to compute the number of equivalence classes with respect to S_{2^n} by assigning 2 to all variables in the cycle index polynomial:

$$Z_{S_{2^n}}(2,\ldots,2) = \sum_{\lambda \vdash 2^n} \frac{1}{z_\lambda} 2^{f_1+\cdots+f_{2^n}} \tag{22}$$

(cf. Example 3). The number of equivalence classes when additionally considering output negation is [9]

$$\frac{1}{2}\left(Z_{S_{2^n}}(2,\ldots,2) + Z_{S_{2^n}}(0,2,0,2,\ldots,0,2)\right). \tag{23}$$

Tables 5 and 6 show all numbers for n up to 6.

Conjecture 2. Let us denote the results of Eqs. (22) and (23) with a_n and b_n. Then the numbers in the tables lead us to conjecture that $a_n = 2^n + 1$ and $b_n = a_{n-1}$. We have not found these equations nor their derivations in the literature, but assume that such identities have already been proven.

6 Conclusions

We have reviewed the research on classification of reversible Boolean functions and applied the results to reversible circuit complexity. Our main result is that

the size difference of optimal circuit realizations for two NPNP-equivalent functions is at most linear and that the size difference of optimal circuit realizations for two LL- or AA-equivalent functions is at most quadratic. We have exhaustively classified all reversible functions with 2 and 3 variables. The results can help to discover further properties of reversible functions and circuits. In future work we further investigate the two conjectures in this paper.

Acknowledgments. This research was supported by H2020-ERC-2014-ADG 669354 CyberCare and by the European COST Action IC 1405 'Reversible Computation'.

References

1. Andrews, G.E.: The Theory of Partitions. Cambridge University Press, Cambridge, UK (1984)
2. Ashenhurst, R.L.: The application of counting techniques. Proc. ACM Nat. Mtg. pp. 293–305 (1952)
3. Beth, T., Rötteler, M.: Quantum algorithms: Applicable algebra and Quantum physics. Springer Tracts in Modern Physics 173, 96–150 (2001)
4. De Bruijn, N.G.: Generalization of Pólya's fundamental theorem in enumerative combinational analysis. Konikl. Nederl. Akademie Van Wetenschappen A 52(2), 59–69 (1959)
5. Draper, T.G.: Nonlinear complexity of Boolean permutations. Ph.D. thesis, University of Maryland (2009)
6. Golubitsky, O., Maslov, D.: A study of optimal 4-bit reversible toffoli circuits and their synthesis. IEEE Trans. Computers 61(9), 1341–1353 (2012)
7. Harrison, M.A.: Combinational problems in Boolean algebras and applications to the theory of switching. Ph.D. thesis, University of Michigan (1963)
8. Harrison, M.A.: The number of classes of invertible Boolean functions. J. ACM 10(1), 25–28 (1963)
9. Harrison, M.A.: The number of equivalence classes of Boolean functions under groups containing negation. IEEE Trans. on Electronic Computers 12, 559–561 (1963)
10. Harrison, M.A.: The number of transitivity sets of Boolean functions. J. Soc. Appl. Ind. Math. 11, 806–828 (1963)
11. Harrison, M.A.: On the classification of Boolean functions by the general linear and affine groups. J. Soc. Appl. Ind. Math. 12, 285–299 (1964)
12. Lorens, C.S.: Invertible Boolean functions. Tech. Rep. 21, Space-General Corp., El Monte, Calif., Research Memorandum (1962)
13. Lorens, C.S.: Invertible Boolean functions. IEEE Trans. on Electronic Computers 13, 529–541 (1964)
14. Pólya, G.: Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen. Acta Math. 68, 145–253 (1937)
15. Primenko, É.A.: Equivalence classes of invertible Boolean functions. Cybernetics 20(6), 771–776 (1984)
16. Slepian, D.: On the number of symmetry types of Boolean functions of n variables. Canadian J. Math. 5, 185–193 (1953)

17. Soeken, M., Thomsen, M.K.: White dots *do* matter: Rewriting reversible logic circuits. In: Int'l Conf. on Reversible Computation. pp. 196–208 (2013)
18. Toffoli, T.: Reversible computing. In: Colloquium on Automata, Languages and Programming. pp. 632–644 (1980)
19. Vatan, F., Williams, C.: Optimal quantum circuits for general two-qubit gates. Phys. Rev. A 69, 032315–1–032315–5 (2004)