Science of Computer Programming ••• (••••) •••–•••

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

A finite alternation result for reversible boolean circuits

Peter Selinger

Department of Mathematics and Statistics, Dalhousie University, Halifax, Canada

ARTICLE INFO

Article history:
Received 2 February 2017
Accepted 22 August 2017
Available online xxxx

Keywords:
Reversible boolean circuits
Alternation depth
Permutations
Circuit synthesis

ABSTRACT

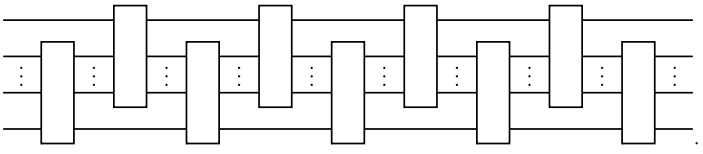
We say that a reversible boolean function on n bits has *alternation depth* d if it can be written as the sequential composition of d reversible boolean functions, each of which acts only on the top $n-1$ bits or on the bottom $n-1$ bits. Moreover, if the functions on $n-1$ bits are even, we speak of *even alternation depth*. We show that every even reversible boolean function of $n \geqslant 4$ bits has alternation depth at most 9 and even alternation depth at most 13.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

A reversible boolean function on n bits is a permutation of $\{0,1\}^n$. It is well-known that the NOT, controlled NOT, and Toffoli gates form a universal gate set for reversible boolean functions [5,2,1]. More precisely, these gates generate (via the operations of composition and cartesian product, and together with the identity functions) all reversible boolean functions on n bits, when $n \leqslant 3$, and all even reversible boolean functions on n bits, when $n \geqslant 4$. A particular representation of a reversible boolean function in terms of these generators is called a *reversible circuit*. The problem of finding a (preferably short) circuit to implement a given reversible function is called the *synthesis problem* [3].

When working with reversible boolean functions and circuits, it is not typically possible to reason inductively; we cannot usually reduce a problem about circuits on n bits to a problem about circuits on $n-1$ bits. In this paper, we prove a theorem that may, in some cases, make such inductive reasoning possible: we prove that when $n \geqslant 4$, every even reversible function on n bits can be decomposed into at most 9 reversible functions on $n-1$ bits:



(1)

If, moreover, each of the functions on $n-1$ bits is also required to be even, we prove that a decomposition into 13 such functions is possible. It is of course not remarkable that n-bit circuits can be decomposed into $(n-1)$-bit circuits: after all, we already know that they can be decomposed into 3-bit circuits, namely gates. What is perhaps remarkable is that the bound 9 (respectively, 13) on the depth is independent of n.

There are some potential applications of such a result — although admittedly, they may not be very practical. As a first application, one may obtain an alternative proof of universality, by turning any universal gate set on n bits into a universal

E-mail address: selinger@mathstat.dal.ca.

http://dx.doi.org/10.1016/j.scico.2017.08.011
0167-6423/© 2017 Elsevier B.V. All rights reserved.

Please cite this article in press as: P. Selinger, A finite alternation result for reversible boolean circuits, Sci. Comput. Program. (2017), http://dx.doi.org/10.1016/j.scico.2017.08.011

gate set on $n+1$ bits, provided that $n \geqslant 3$. This also yields a new method for circuit synthesis: given a good procedure for synthesizing even n-bit circuits, we obtain a procedure for synthesizing even $(n+1)$-bit circuits that is at most 13 times worse. By applying this idea recursively, we obtain circuits of size $O(13^n)$ for any reversible function on n bits. This is worse than what can be obtained by other methods. However, it may be possible to improve this procedure further, for example by noting that the 13 subcircuits need not be completely general; they can be chosen to be of particular forms, which may be easier to synthesize recursively.

Another potential application is the presentation of (even) reversible boolean functions by generators and relations. While the NOT, CNOT, and Toffoli gates are a well-known set of generators, to the author's knowledge, no complete set of relations for these generators is known. For any given n, the group of n-bit reversible functions is a finite group, so finding a complete set of relations for any fixed n is a finite (although very large) problem. However, it is not trivial to find a set of relations that works for all n; at present, it is not even known whether the theory is finitely axiomatizable. If we had a procedure for rewriting every circuit into one of the form (1), then we could obtain a complete set of relations for n-bit circuits by considering (a) a complete set of relations for $(n-1)$-bit circuits, (b) the relations required to do the rewriting, and (c) any relations required to prove equalities between circuits of the form (1). In particular, if it could be shown that a finite set of relations is sufficient for (b) and (c), a finite equational presentation of reversible boolean functions could be derived.

Finally, the task of realizing a given permutation with low alternation depth can also make for an entertaining puzzle. Such a puzzle has been implemented and is available from [4].

2. Statement of the main result

We write $S(X)$ for the group of permutations of a finite set X. For $f \in S(X)$ and $g \in S(Y)$, let $f \times g \in S(X \times Y)$ be the permutation defined componentwise by $(f \times g)(x, y) = (f(x), g(y))$. We also write $\mathrm{id}_X \in S(X)$ for the identity permutation on X. Recall that a permutation is *even* if it can be written as a product of an even number of 2-cycles.

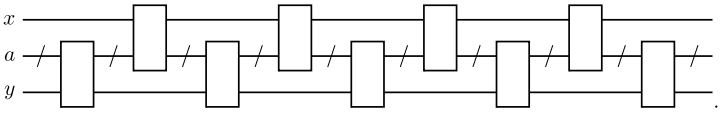
Let $2 = \{0, 1\}$ be the set of booleans, which we identify with the binary digits 0 and 1. By abuse of notation, we also write $2 = \mathrm{id}_2$ for the identity permutation on the set 2.

Definition. Let A be a finite set, and let $\sigma \in S(2 \times A \times 2)$ be a permutation. We say that σ has *alternation depth* d if it can be written as a product of d factors $\sigma = \sigma_1\sigma_2 \cdots \sigma_d$, where each factor σ_i is either of the form $f \times 2$ for some $f \in S(2 \times A)$ or of the form $2 \times g$ for some $g \in S(A \times 2)$.

The purpose of this paper is to prove the following theorem:

Theorem 2.1. *Let A be a finite set of 3 or more elements. Then every even permutation $\sigma \in S(2 \times A \times 2)$ has alternation depth 9.*

In circuit notation, Theorem 2.1 can be understood as stating that every reversible boolean function on the set $2 \times A \times 2$ can be expressed as a circuit in the following form:



(2)

Here, the lines labeled x and y each represent a bit, and the line labeled a represents an element of the set A. The case of boolean circuits arises as the special case where the cardinality of A is a power of 2.

Remark 2.2. The evenness of σ is a necessary condition for Theorem 2.1, because all permutations of the forms $f \times 2$ and $2 \times g$ are even, and therefore only even permutations can have an alternation depth.

Remark 2.3. Our definition of alternation depth does not require that the permutations $f \in S(2 \times A)$ and $g \in S(A \times 2)$ are themselves even. However, if Theorem 2.1 is to be applied recursively (as required, for example, by the potential applications mentioned in the introduction), we need each f and g to be even. Since the proof of Theorem 2.1 is already complicated enough without this restriction, we do not consider the case of even f and g until Section 6, where we prove that the alternation depth is at most 13 in that case.

Our proof of Theorem 2.1 is in two parts. In Section 3, we will show that every even permutation of a certain form $g+h$ has alternation depth 5. In Section 4, we will show that every even permutation can be decomposed into a permutation of alternation depth 4 and a permutation of the form $g+h$. Together, these results imply Theorem 2.1.

Please cite this article in press as: P. Selinger, A finite alternation result for reversible boolean circuits, Sci. Comput. Program. (2017), http://dx.doi.org/10.1016/j.scico.2017.08.011

Download English Version:

https://daneshyari.com/en/article/6875307

Download Persian Version:

https://daneshyari.com/article/6875307

Daneshyari.com