Information Processing Letters 139 (2018) 35–38

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Pairs of majority-decomposing functions

Mathias Soeken [a,*], Eleonora Testa [a], Alan Mishchenko [b], Giovanni De Micheli [a]

[a] Integrated Systems Laboratory, École Polytechnique Fédérale de Lausanne, Switzerland
[b] Department of EECS, UC Berkeley, CA, USA

ARTICLE INFO

Article history:
Received 27 December 2017
Received in revised form 27 June 2018
Accepted 7 July 2018
Available online 10 July 2018
Communicated by Kun-Mao Chao

Keywords:
Boolean functions
Majority functions
Decomposition
Logic synthesis
Combinatorial problems

ABSTRACT

We are interested in decompositions $\langle x_n f_1 f_2 \rangle$ of the majority function over n odd arguments $x_1, \dots, x_n$ such that f_1 and f_2 do not depend on x_n. In this paper, we derive the conditions for f_1 and f_2 that satisfy the decomposition. Such decompositions play a central role in finding optimum majority-3 networks for the majority-n function.

1. Introduction

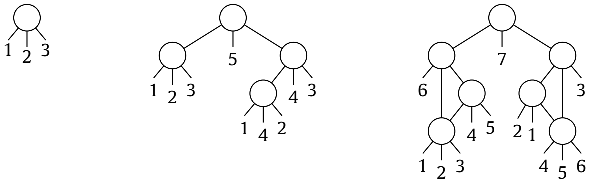
In this paper, we are considering Boolean functions over the domain of truth values $\{0, 1\}$. We are concerning ourselves with the decomposition of the majority-n function

$$\langle x_1 \dots x_n \rangle = [x_1 + \dots + x_n > \tfrac{n-1}{2}], \qquad (n \text{ odd}) \tag{1}$$

in terms of majority-3 operations without inversions, called majority networks. This is an important task in majority-based logic synthesis [1–4]. Ultimately, we are driven by the question of how many majority-3 operations are sufficient to realize the majority-n function. We will refer to the minimum number of operations as C_n in the remainder, and call majority networks *optimum* if they realize the majority-n function using C_n majority operations. Until today, it is only known that $C_3 = 1$, $C_5 = 4$, and $C_7 = 7$ [5,6]. The asymptotic complexity of C_n is linear, since finding the median element in an unsorted set has linear complexity [7]. This has led to the following conjecture.

Conjecture 1. $C_n = \frac{3(n-3)}{2} + 1$, *for odd* $n \geq 3$.

In particular, $C_9 = 10$, however, neither a witness nor a proof excluding the existence of a network with 10 majority operations has been found. Optimum majority networks for $n = 3$, 5, and 7 are for example:



(2)

Each circle corresponds to a majority node and a primary input x_i is represented by a leaf i. The structure of these known optimum majority networks has led to another conjecture, which does not predict the number of minimum operations, but predicts a common structure.

---

[*] Corresponding author.
E-mail address: mathias.soeken@epfl.ch (M. Soeken).

https://doi.org/10.1016/j.ipl.2018.07.004
0020-0190/© 2018 Elsevier B.V. All rights reserved.

Conjecture 2. *There always exists an optimum network in which (i) each node is connected to at least one primary input and (ii) the root node is the only node that is connected to x_n.*

For example, variables x_3, x_5, and x_7 only appear at the root nodes of the optimum majority networks for $n = 3, 5,$ and 7 in (2). In order to derive further knowledge from the optimum majority networks for $n = 3, 5,$ and 7, and motivated by Conjecture 2, in this paper, we investigate decompositions of the majority-n function $\langle x_1 \dots x_n \rangle$ into the majority-3 expression $\langle x_n f_1 f_2 \rangle$, such that f_1 and f_2 are Boolean functions over $n - 1$ variables that do not depend on x_n.

The main result of this paper is the following.

Theorem 1. *For $k \geq 1$, let $n = 2k + 1$, and f_1 and f_2 two $(n-1)$-variable Boolean functions. Then*

$$\langle x_1 \dots x_n \rangle = \langle x_n f_1 f_2 \rangle,$$

if, and only if

(a) $f_1(x_1, \dots, x_{2k}) = f_2(x_1, \dots, x_{2k}) = 1$, *if* $x_1 + \dots + x_{2k} > k$,
(b) $f_1(x_1, \dots, x_{2k}) \oplus f_2(x_1, \dots, x_{2k}) = 1$, *if* $x_1 + \dots + x_{2k} = k$, *and*
(c) $f_1(x_1, \dots, x_{2k}) = f_2(x_1, \dots, x_{2k}) = 0$, *if* $x_1 + \dots + x_{2k} < k$.

In other words, if the number of ones in the input pattern is less than k, then both functions must evaluate to 0, and if the number of ones is larger than k, then both functions must evaluate to 1. Only in the case where the number of ones equals k, one has the freedom to select the output of one function to be 1, if the other function outputs 0.

We made use of our findings in an exhaustive search algorithm and were able to find experimentally that Conjecture 1 and Conjecture 2 cannot *both* be true. More precisely, there cannot be a majority network for majority-9 with 10 majority operations (as predicted by Conjecture 1) adhering to a structure as described by Conjecture 2.

The next section will give the proof for Theorem 1. After introducing threshold functions in Section 3, Sections 4 and 5 review two results from the literature as special case of Theorem 1. The latter can be used as an explanation for the optimum majority networks for $n = 3$, and $n = 5$. Section 6 introduces a new decomposition, which is also a special case of Theorem 1 and can be used as an explanation for the optimum majority network for $n = 7$. Section 7 discusses consequences of the observations for finding optimum majority networks for $n \geq 9$. Section 8 concludes the paper.

2. Proof of the main theorem

Proof of Theorem 1. We prove by case distinction on x_n. If $x_n = 0$, then the result of the majority-n must be true only if more than k of the arguments $x_1, \dots, x_{2k}$ are true. Case (a) yields $\langle 011 \rangle = 1$; case (b) yields $\langle 001 \rangle = \langle 010 \rangle = 0$; case (c) yields $\langle 000 \rangle = 0$.

If $x_n = 1$, then the result of the majority-n must be true only if at least k of the arguments are true. Case (a) yields $\langle 111 \rangle = 1$; case (b) yields $\langle 101 \rangle = \langle 110 \rangle = 1$; case (c) yields $\langle 100 \rangle = 0$. □

3. Threshold functions

We introduce some important symmetric Boolean functions called *threshold functions*, which are a generalization of majority functions. Let

$$S_{>k}(x_1, \dots, x_n) = [x_1 + \dots + x_n > k] \tag{3}$$

be the function that is true, if *more than* k of the input arguments are true. Also, for $k > 0$ let

$$S_{=k}(x_1, \dots, x_n) = S_{>k-1}(x_1, \dots, x_n) \wedge \overline{S_{>k}(x_1, \dots, x_n)} \tag{4}$$

be the function that is true, if *exactly* k of the input arguments are true.

Let $n = 2k+1$ for some $k \geq 1$. Then the majority-n function can also be written as

$$\langle x_1 \dots x_n \rangle = S_{>k}(x_1, \dots, x_n). \tag{5}$$

4. Co-factor decomposition

We start with a simple decomposition in which f_1 and f_2 are the positive and negative co-factor of the majority-n function, respectively. One obtains the positive or negative co-factor of a function f with respect to a variable x_i, by fixing x_i to 1 or 0, respectively:

$$\langle x_1 \dots x_n \rangle = \langle x_n \langle x_1 \dots x_{n-1} 1 \rangle \langle x_1 \dots x_{n-1} 0 \rangle \rangle \tag{6}$$

Akers discovered this decomposition in the early 1960s [8].

Theorem 2. *For $k \geq 1$ and $n = 2k + 1$, the functions $f_1^k = \langle x_1 \dots x_{n-1} 0 \rangle$ and $f_2^k = \langle x_1 \dots x_{n-1} 1 \rangle$ are a pair of majority-decomposing functions.*

Proof. It follows easily from noting that $f_1^k = S_{>k}(x_1, \dots, x_{2k})$ and $f_2^k = S_{\geq k}(x_1, \dots, x_{2k})$. □

Example 1. We use the co-factor decomposition to derive an expression for majority-3. In this case, we get $n = 3$, $f_1^1 = \langle x_1 x_2 0 \rangle = x_1 \wedge x_2$, and $f_2^1 = \langle x_1 x_2 1 \rangle = x_1 \vee x_2$. Hence, the decomposition leads to the expression $\langle x_3 (x_1 \wedge x_2)(x_1 \vee x_2) \rangle$ with 3 majority-3 operations to express a single majority-3 operation.

5. Majority-reducing decomposition

In this section, we review a decomposition from Amarel, Cooke, and Winder [5] that sets $f_1^k = \langle x_1 \dots x_{2k-1} \rangle$. In other words, the majority-n function is decomposed in terms of the smaller majority-$(n-2)$ function.

Theorem 3 *([5]). For $k \geq 1$ and $n = 2k + 1$, the functions $f_1^k = \langle x_1 \dots x_{2k-1} \rangle$ and $f_2^k = S_{>k}(x_1, \dots, x_{2k-1}) \vee x_{2k} S_{>k-2}(x_1, \dots, x_{2k-1})$ are a pair of majority-decomposing functions.*