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*

A R T I C L E I N F O

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

A B S T R A C T

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

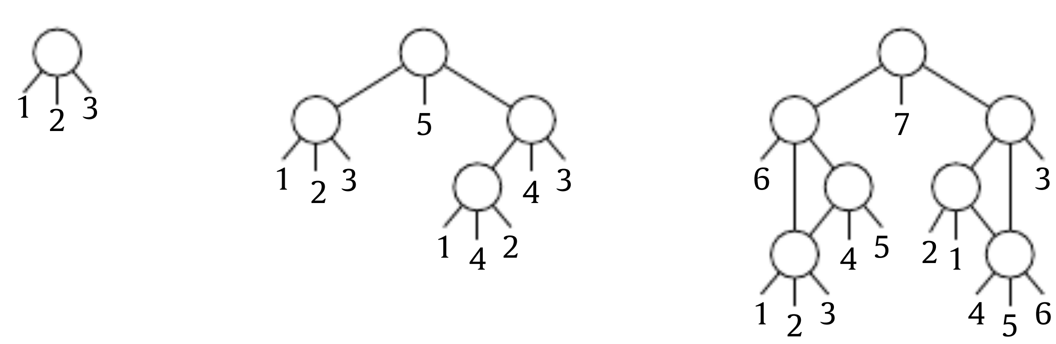
In this paper, we are considering Boolean functions over the domain of truth values $\{0, 1\}$. We are concerning ourselves with the decomposition of the majority-n function

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

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).

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

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 if at least k of the arguments $x_1, \dots, x_{2k}$ 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

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

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.

Example 2. We use Theorem 3 to find a decomposition for majority-3. Then, $f_1^1 = S_{>0}(x_1) = x_1$ and $f_2^1 = S_{>1}(x_1) \vee x_2 S_{>-1}(x_1) = x_2$. Hence $\langle x_1x_2x_3\rangle = \langle x_3x_1x_2\rangle$.

The optimum network for majority-5 can be directly derived from this decomposition as illustrated by the following example.

Example 3. For $k = 2$, we have $f_1^2 = \langle x_1x_2x_3\rangle$, corresponding to the subnetwork on the left-hand side in (2), and

$$\begin{aligned} f_2^2 &= S_{>2}(x_1, x_2, x_3) \vee x_4 S_{>0}(x_1, x_2, x_3) \\ &= x_1x_2x_3 \vee x_4(x_1 \vee x_2 \vee x_3). \end{aligned}$$

One can readily verify that $f_2^2 = \langle x_1 x_4 \langle x_2 x_4 x_3\rangle\rangle$, which corresponds to the subnetwork on the right-hand side in the optimum network for majority-5.

It is worth noting that in [5], the authors also show how to describe f_2^k in terms of k majority-3 operations and $k+1$ majority-5 operations.

6. Parity-splitting decomposition

In this section, we introduce a new decomposition, which we will use to explain the optimum majority network for majority-7. Let $n = 2k + 1$, as in the previous sections. The decomposition is not applicable to all odd n, but only when k is odd, e.g., $n = 3$, $n = 7$, $n = 11$, and so on. We first define a function

$$\begin{aligned} &g_k(x_1, \dots, x_k, x_{k+1}, \dots, x_{2k}) = \\ &\quad S_{>k}(x_1, \dots, x_{2k}) \oplus S_{=k}(x_1, \dots, x_{2k})(x_1 \oplus \cdots \oplus x_k), \quad (7) \end{aligned}$$

which is true, if (i) either more than k arguments are true, or if (ii) exactly k arguments are true while an odd number of these k arguments must be from the first arguments $x_1, \dots, x_k$. We can use this function to describe a pair of majority-decomposing functions.

Theorem 4. *Let $k \geq 1$, and k be odd. Then $f_1^k = g_k(x_1, \dots, x_k, x_{k+1}, \dots, x_{2k})$ and $f_2^k = g_k(x_{k+1}, \dots, x_{2k}, x_1, \dots, x_k)$ are a pair of majority-decomposing functions.*

Proof. It is easy to see that case (a) and (c) of Theorem 1 are true from the definition of g_k.

In the case of (b), the functions simplify to $f_1^k = x_1 \oplus \cdots \oplus x_k$ and $f_2^k = x_{k+1} \oplus \cdots \oplus x_{2k}$. Since k is odd, we have $f_1^k \oplus f_2^k = x_1 \oplus \cdots \oplus x_{2k} = 1$. □

Example 4. Let $k = 3$, i.e., $n = 7$. Then one can verify that

$$\begin{aligned} f_1^3 &= S_{>3}(x_1, x_2, x_3, x_4, x_5, x_6) \\ &\quad \oplus (x_1 \oplus x_2 \oplus x_3) S_{=3}(x_1, x_2, x_3, x_4, x_5, x_6) \end{aligned}$$

which corresponds to the subnetwork on the right-hand side in the optimum network for majority-7 in (2). Similarly, f_2^3 corresponds to the subnetwork on the left-hand side, as it is obtained by simply swapping x_1, x_2, x_3 with x_4, x_5, x_6. In fact, it is quite surprising that in the optimum network for majority-7, there is no sharing between the networks for f_1^3 and f_2^3, although their expressions are very similar.

Also the optimum network for $k = 1$, i.e., majority-3, can be derived from the parity-splitting decomposition.

Example 5. Let $k = 1$. Then we have

$$\begin{aligned} f_1^1 &= S_{>1}(x_1, x_2) \oplus x_1 S_{=1}(x_1, x_2) \\ &= x_1x_2 \oplus x_1(x_1 \oplus x_2) = x_1. \end{aligned}$$

Analogously, we find $f_2^1 = x_2$.

7. Application to finding optimum majority networks

Having found that the reviewed and proposed decompositions can in fact explain the optimum results for $n \leq 7$, we investigate whether they help to find optimum networks for larger n.

Theorem 1 describes a large set of pairs of majority-decomposing functions. Case (a) and (c) fix the output for f_1^k and f_2^k for all input patterns with less or more than k ones. But for the $\binom{2k}{k} = \frac{(2k)!}{k!^2}$ input patterns that have exactly k ones, one can decide whether to assign f_1^k to 1 or 0. This leads to $2^{\frac{(2k)!}{k!^2}}$ different pairs of decomposing functions. Concretely, these are 4, 64, 2^{20}, 2^{70}, and 2^{252} for $k = 1, 2, 3, 4$, and 5.

We first show that Conjecture 1 and Conjecture 2 cannot both hold for $n = 9$, i.e., $k = 4$. In other words, there exists no majority network for majority-9 with 10 gates in which each gate points to a primary input and only the top-most gate points to x_9. Instead of finding a majority network for majority-9, we tried to find a majority network for a pair of functions (f_1^4, f_2^4) with 8 inputs and 9 gates. We leave f_1^4 and f_2^4 unspecified, but only constrain them to adhere to the conditions from Theorem 1. This allows to explore the full space of all $2^{\frac{8!}{4!^2}} = 2^{70}$ possible decompositions. We expressed this problem using a SAT solver similar to the encoding proposed in [9,10]. On a MacBook computer using a 2.7 GHz Intel Core i5 processor with 8 GB memory, we are able to show that the problem is unsatisfiable within about 5 minutes. Since no network with 9 gates exists to compute any pair (f_1^4, f_2^4), there cannot be a majority network to compute majority-9 with 10 gates that follows the structure described in Conjecture 2. However, there still may exist a majority network for majority-9 with 10 gates, but if so, it cannot have a decomposition structure similar to those found for $n = 3, 5$ and 7. Or, the optimum network requires more than 10 gates but can still have a structure as described by Conjecture 2.

$(x_1 \oplus \cdots \oplus x_5) S_{=5}(x_1, \ldots, x_{10})$ from the parity-splitting decomposition using 6 gates. We can show with exhaustive search that this is not possible. This implies that the structure for majority-7 in (2) cannot trivially be extended for majority-11, with two disjoint subnetworks for f_1^5 and f_2^5. However, this result does not imply that there is no 13-operation majority network for majority-11 that used the parity-splitting decomposition, since there may be shared nodes for f_1^5 and f_2^5.

8. Conclusions

We have derived the necessary properties for two functions $f_1(x_1, \ldots, x_{n-1})$ and $f_2(x_1, \ldots, x_{n-1})$, called pair of majority-decomposing functions, such that $f = \langle x_n f_1 f_2 \rangle$, where $n = 2k + 1$. Our result generalizes previously proposed decompositions. We derive a new decomposition for the special case in which k is odd. The interest in such decompositions is motivated by the problem of finding optimum majority-3 networks that realize majority-n. This problem was first posed more than 50 years ago [5]. Yet, until today the optimum solution for $n = 9$ is still unknown. Optimum solutions for $n = 3, 5$ and 7 can be explained using pairs of majority-decomposing functions. Consequently, the study of pairs of majority-decomposing functions can help in the surprisingly daunting task of finding optimum majority networks for $n = 9$ and beyond.

Acknowledgement

The authors wish to thank Luca Amaru for insightful discussions. This research was supported by the Swiss National Science Foundation (200021-169084 MAJesty) and by the European Research Council in the project H2020-ERC-2014-ADG 669354 CyberCare.

References

[1] R.L. Wigington, A new concept in computing, Proc. IRE 47 (4) (1959) 516–523.

[2] M. Cohn, R. Lindaman, Axiomatic majority-decision logic, IEEE Trans. Electron. Comput. 10 (1) (1961) 17–21.

[3] S.B. Akers Jr., Synthesis of combinational logic using three-input majority gates, in: Symp. on Switching Circuit Theory and Logical Design, 1962, pp. 149–157.

[4] L.G. Amarù, P.-E. Gaillardon, G. De Micheli, Majority-inverter graph: a new paradigm for logic optimization, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 35 (5) (2016) 806–819.

[5] S. Amarel, G.E. Cooke, R.O. Winder, Majority gate networks, IEEE Trans. Electron. Comput. 13 (1) (1964) 4–13.

[6] D.E. Knuth, The Art of Computer Programming, vol. 4A, Addison-Wesley, 2011.

[7] D. Dor, U. Zwick, Selecting the median, SIAM J. Comput. 28 (5) (1999) 1722–1758.

[8] S.B. Akers Jr., A truth table method for the synthesis of combinational logic, IEEE Trans. Electron. Comput. 10 (4) (1961) 604–615.

[9] A. Kojevnikov, A.S. Kulikov, G. Yaroslavtsev, Finding efficient circuits using SAT-solvers, in: Int'l Conf. on Theory and Applications of Satisfiability Testing, 2009, pp. 32–44.

[10] M. Soeken, L.G. Amarù, P.-E. Gaillardon, G. De Micheli, Exact synthesis of majority-inverter graphs and its applications, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 36 (11) (2017) 1842–1855.