A NEW HEURISTIC ALGORITHM FOR SEQUENTIAL TWO-BLOCK DECOMPOSITION OF BOOLEAN FUNCTIONS

Arkadij Zakrevskij

The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Surganov str. 6, 220012, Minsk, Belarus, zakr@newman.bas-net.by

Abstract: The task of simple decomposition of a Boolean function, generally non-disjunctive, is considered, its solution is reduced in main to search for appropriate weak partitions on the set of arguments. A special attention is paid to the case of presence of a good solution for the given Boolean function, in remaining random. To find it, a two-stage heuristic combinatorial algorithm is offered, optimized on speed. At the first stage the randomized search for "traces" of the decomposition is fulfilled. These traces are represented by some "triads" - the simplest weak partitions corresponding to non-trivial decompositions. At the second stage the whole sought-for partition is restored from the discovered trace. The results of computer experiments confirming practical efficiency of the algorithm are quoted.

Keywords: Boolean functions, decomposition methods, logic design.

1. SETTING THE PROBLEM

In modern technology of design of logic circuits implementing given Boolean functions, an important role is played by decomposition methods. Their essence consists in possible replacement of the considered Boolean function by an equivalent composition of several functions of smaller number of variables. Different sorts of decomposition were offered, among which the special notice was given to the *sequential two-block decomposition*, called also *simple* decomposition, *disjunctive* or *non-disjunctive*.

As a result of the disjunctive decomposition the initial Boolean function $f(\boldsymbol{x})$ is substituted by a composition $g(h(\boldsymbol{u}), \boldsymbol{v})$ at the partition $\boldsymbol{u}/\boldsymbol{v}$ on the set of arguments $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, where $\boldsymbol{u} \cup \boldsymbol{v} = \boldsymbol{x}$ and $\boldsymbol{u} \cap \boldsymbol{v} = \varnothing$ (such a partition $\boldsymbol{u}/\boldsymbol{v}$ is named strong) (Povarov, 1954; Ashenhurst, 1959). A more general case is represented by the non-disjunctive decomposition. In this case function $f(\boldsymbol{x})$ is substituted by the composition $g(h(\boldsymbol{u}, \boldsymbol{w}), \boldsymbol{w}, \boldsymbol{v})$ at weak partition $\boldsymbol{u}/\boldsymbol{v}$, where $\boldsymbol{x} = \boldsymbol{u} \cup \boldsymbol{w} \cup \boldsymbol{v}$, $\boldsymbol{u} \cap \boldsymbol{w} = \boldsymbol{u} \cap \boldsymbol{v} = \boldsymbol{w} \cap \boldsymbol{v} = \varnothing$ (Curtis, 1962; Zakrevskij, 1964). Both cases are illustrated by examples in Fig. 1: a) $\boldsymbol{u} = (x_1, x_2, x_3, x_4)$, $\boldsymbol{v} = (x_5, x_6, x_7)$; b) $\boldsymbol{u} = (x_1, x_2, x_3)$, $\boldsymbol{w} = (x_4, x_5)$, $\boldsymbol{v} = (x_6, x_7)$. Note, that in both cases of decomposition the condition $|\boldsymbol{u}| > 1$ and $|\boldsymbol{v}| > 0$ should be satisfied, otherwise the decomposition is trivial, because it exists always.

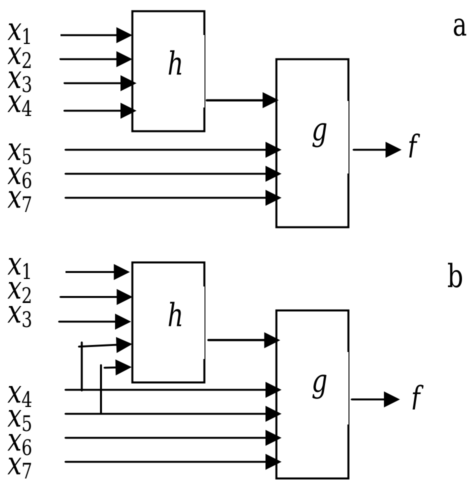

Fig. 1. Examples of simple decomposition of a Boolean function, disjunctive (a) and non-disjunctive (b).

Solving the following two tasks are laying in the basis of decomposition methods.

The task 1. For a given function $f(\boldsymbol{x})$ and partition $\boldsymbol{u}/\boldsymbol{v}$ (strong either weak) to find out, whether $f(\boldsymbol{x})$ is decomposable at $\boldsymbol{u}/\boldsymbol{v}$, i. e. whether there exists a composition $(g(h(\boldsymbol{u}), \boldsymbol{v})$ or $g(h(\boldsymbol{u}, \boldsymbol{w}), \boldsymbol{w}, \boldsymbol{v})$ equivalent to function f (and, maybe, to find functions g and h).

If such a composition does exist, we shall term partition $\boldsymbol{u}/\boldsymbol{v}$ as *appropriate*.

The task of checking a Boolean function $f(\boldsymbol{x})$ for decomposability at a given partition on the set of arguments was regarded in (Povarov, 1954; Ashenhurst, 1959; Curtis, 1962), where a necessary and sufficient condition for that was formulated as follows:

Let $f_i(\boldsymbol{u}, \boldsymbol{v})$ be the coefficients of the Shannon disjunctive decomposition of $f(\boldsymbol{x})$ by variables of set $\boldsymbol{w}$. Then the coefficients of the similar decomposition of each $f_i(\boldsymbol{u}, \boldsymbol{v})$ at variables from $\boldsymbol{u}$ must accept not more than two different values.

Checking Boolean functions for satisfying this condition was laid into the base of many known methods offered for solving task 1.

A new algorithm for solving the same problem was suggested in paper (Zakrevskij A.D. 2006), based on representation of considered functions by Boolean vectors and using efficient component-wise operations above them. It is checking a Boolean function for satisfying the condition formulated in the following assertion.

Assertion 1. A Boolean function $f(\boldsymbol{x})$ is decomposable at partition $\boldsymbol{u}/\boldsymbol{v}$, if and only if

$$(f^{+} \oplus S_{\boldsymbol{u}}^{\vee} f^{+}) \wedge S_{\boldsymbol{v}}^{\vee} f^{+} = 0,$$

where

$f^{+} = f(\boldsymbol{x}) \oplus f_{\boldsymbol{u}}^{0}$,

$f_{\boldsymbol{u}}^{0}$ is the initial coefficient f_0 of Shannon decomposition of function $f(\boldsymbol{x})$ at set $\boldsymbol{u}$,

$S_{\boldsymbol{v}}^{\vee}$ and $S_{\boldsymbol{u}}^{\vee}$ are operators of disjunctive symmetrization of Boolean function $f(\boldsymbol{x})$ over the given subset of $\boldsymbol{x}$ ($\boldsymbol{v}$ or $\boldsymbol{u}$), introduced in [4] and defined as follows: if $\boldsymbol{u} = (u_1, u_2, \ldots, u_k)$, then

$$S_{\boldsymbol{u}}^{\vee} f(\boldsymbol{x}) = S_{u1}^{\vee}(S_{u2}^{\vee} \ldots (S_{uk}^{\vee} f(\boldsymbol{x}))\ldots),$$

where

$$S_{xi}^{\vee} f(\boldsymbol{x}) = f(x_1, \ldots, x_i, \ldots, x_n) \vee f(x_1, \ldots, \neg x_i, \ldots, x_n).$$

In result of applying operator $S_{\boldsymbol{u}}^{\vee}$ to Boolean space of variables from set $\boldsymbol{x}$, where function $f(\boldsymbol{x})$ is defined, any interval with inner variables taken from set $\boldsymbol{u}$, which has if only one 1, is filled up with 1s completely. Operator $S_{\boldsymbol{v}}^{\vee}$ is defined similarly.

The task 2. For a given function $f(\boldsymbol{x})$ to find an appropriate partition.

The second task is more difficult. A heuristic combinatorial algorithm is offered below to solve it, optimized on speed.

2. RELATIONS ON THE SET OF PARTITIONS

Consider two partitions $\boldsymbol{u}/\boldsymbol{v}$ and $\boldsymbol{u}^*/\boldsymbol{v}^*$, such that $\boldsymbol{u}^* \subseteq \boldsymbol{u}$ and $\boldsymbol{v}^* \subseteq \boldsymbol{v}$. Let's speak, that partition $\boldsymbol{u}^*/\boldsymbol{v}^*$ submits to partition $\boldsymbol{u}/\boldsymbol{v}$. The following assertions are fair by that [4].

Assertion 2. If the function $f(\boldsymbol{x})$ is decomposable at partition $\boldsymbol{u}/\boldsymbol{v}$, it is decomposable as well at submitted partition $\boldsymbol{u}^*/\boldsymbol{v}^*$.

Assertion 3. If the function $f(\boldsymbol{x})$ is not decomposable at partition $\boldsymbol{u}^*/\boldsymbol{v}^*$, it is not decomposable also at partition $\boldsymbol{u}/\boldsymbol{v}$.

Let's assume $|\boldsymbol{u}| = k$ and $|\boldsymbol{v}| = m$. Partition with $k = 2$ and $m = 1$ we shall term as a *triad*. It is the simplest of partitions, at which a nontrivial decomposition can be defined.

Assertion 4. The number of triads is equal to

$$C_n^2 (n-2) = \frac{n(n-1)(n-2)}{2}.$$

Assertion 5. The Boolean function $f(\boldsymbol{x})$ is not decomposable, if it is not decomposable at any of triads.

It follows from here that the function is decomposable, if and only if it is decomposable if only at one of triads.

Let's estimate the probability of decomposability of a random Boolean function $f(\boldsymbol{x})$ of n variables.

Consider some triad $\boldsymbol{u}/\boldsymbol{v}$, having put for example $\boldsymbol{u} = (a, b)$, $\boldsymbol{v} = (c)$, and some coefficient $\varphi(a, b, c)$ of function $f(\boldsymbol{x})$ Shannon decomposition by variables of set $\boldsymbol{w} = \boldsymbol{x} \setminus (\boldsymbol{u} \cup \boldsymbol{v})$.

Assertion 6. The number of different values of the coefficients of the Shannon decomposition of an arbitrary Boolean function $\varphi(a, b, c)$ by variables a and b does not exceed two, if the coefficients φ_0 and φ_1 of the decomposition of function φ by c obey to the condition: $\varphi_0 = \neg\varphi_1$ or at any rate one of the coefficients φ_0 and φ_1 represents constant 0 or 1.

It follows from this condition

Assertion 7. Among 256 different Boolean functions $\varphi(a, b, c)$ there are 74 functions, for which the number of different values of coefficients of Shannon decomposition by variables a and b does not exceed two.

Let's designate through γ the share of such functions ($\gamma = 74/256$).

Considering the above assertions and taking into account, that in any triad $|\boldsymbol{w}| = n - 3$ and, therefore, the number of coefficients of the function $f(\boldsymbol{x})$ Shannon decomposition by $\boldsymbol{w}$ is equal to 2^{n-3}, we shall formulate

Assertion 8. At equiprobable sampling of function $f(\boldsymbol{x})$ from the set of all Boolean functions of n variables the