The Conjunction Complexity Asymptotic of Self-Correcting Circuits for Monotone Symmetric Functions with Threshold 2

T.I. Krasnova

Moscow State University, Faculty of Mechanics and Mathematics,
Leninskie Gory, Moscow, 119991 Russia; e-mail: kotovati@ya.ru

Received April 13, 2012

Abstract—It is shown that the conjunction complexity $L_k^p(f^n)$ of monotone symmetric Boolean functions $f^n(x_1, \ldots, x_n) = \bigvee_{1 \leq i < j \leq n} x_i x_j$ realized by $k$-self-correcting circuits in the basis $B = \{k, -\}$ asymptotically equals to $(k+2)n$ for growing $n$ providing the price of a reliable conjunctor is $\geq k+2$.

DOI: 10.3103/S0027132214030061

In this paper we consider realization of Boolean functions $f^n(x_1, \ldots, x_n) = \bigvee_{1 \leq i < j \leq n} x_i x_j$ (i.e., monotone symmetric threshold functions with the threshold 2) by $k$-self-correcting circuits of functional elements in the basis $B = \{k, -\}$, see [1, 2]. A circuit is called $k$-self-correcting if under passing of at most $k$ of arbitrary unreliable elements to a faulty state the circuit realizes the same function as in the correct state of all its elements [3]. All inverters are supposed to be reliable, they always implement inversion and have zero weights. Every reliable conjunctor has a fixed weight $p$, where $p \geq k+2$, and always implements the conjunction. Every unreliable conjunctor has weight 1 and implements conjunction in its correct state and otherwise implements a Boolean constant $\delta$ which supposed to be fixed and a priori known. Thus, all faults of the circuit are supposed to be single-type constants at the outputs of faulty conjunctors. The conjunction complexity $L_k^p(f)$ is the least complexity of the $k$-self-correcting circuits realizing the Boolean function $f$ in the basis described above; here the complexity of a circuit is the sum of weights of all elements of the circuit.

The following theorem is the main result of the paper.

Theorem. For increasing $n$ the following relation is valid: $L_k^p(f^n) \sim (k+2)n$.

AUXILIARY STATEMENTS

Take an arbitrary circuit $S$ in the basis $B$. An element $E^-$ is called $x_i$-blocker (see [4]) if $E^-$ is a unique inverter in some path $Z$ from the input $x_i$ (i.e., the input of the circuit corresponding to the variable $x_i$) to $E^-$; all other elements from $Z$ (i.e., conjunctors) different from $E^-$ are called $x_i$-preblocking.

Lemma 1 [4]. If a function $f(x_1, \ldots, x_m)$ cannot be represented in the form

$$f(x_1, \ldots, x_m) = x_i g(x_1, \ldots, x_m),$$

(1)

then any path from the input $x_i$ to an output of the circuit contains an $x_i$-blocker.

Lemma 2. If a function $f(x_1, \ldots, x_m)$ cannot be represented in the form

$$f(x_1, \ldots, x_m) = x_i g(x_1, \ldots, x_m),$$

(2)

then no $x_i$-blocker can be an output element of the circuit.

Proof. Suppose an $x_i$-blocker $E^-$ is an output element of the circuit. Due to the definition, there exists a path from the input $x_i$ to $E^-$ not containing inverters except for $E^-$. Therefore, the function can be represented in form (2), but this is excluded by the hypothesis of the lemma. The lemma is proved.

We say that an element $E$ goes after an $x_i$-blocker if at least one of inputs of the element $E$ is fed by the output of this $x_i$-blocker.

Lemma 3. If a $k$-self-correcting circuit $S$ implements a function $f(x_1, \ldots, x_m)$ dependent essentially on the variable $x_i$ and not representable in forms (1) and (2), then the sum of all weights of the elements going after an $x_i$-blockers in $S$ is greater than or equal to $k+1$. 

121
Proof. Suppose the sum of the weights of the elements going after $x_i$-blockers is less than $k + 1$. Therefore, there is no reliable element among them and the number of unreliable ones is at most $k$. Suppose all these elements are faulty. In this case the function realized by the circuit must remain the same because the circuit is $k$-self-correcting. However, on the other hand, the function realized by the circuit does not depend on the variable $x_i$ under the fail described above. Indeed, due to Lemma 1, any path from $x_i$ to an output of the circuit contains an $x_i$-blocker and by Lemma 2 any $x_i$-blocker is not an output element, therefore, any path from $x_i$ to an output of the circuit contains a faulty element. We have got a contradiction to our assumption. The lemma is proved.

Note that $f_2^*$ essentially depends on all its variables and cannot be represented in forms (1) and (2).

LOWER ESTIMATE

We prove lower estimates under the assumption that inputs of circuits can be fed as by variables, so as by constants 0 and 1. It is clear that the estimates obtained here remain also valid in the case when inputs of a circuit are fed by variables only. Under this assumption, any circuit in the basis considered here possesses the following properties, see [5].

Property 1. If $S$ is a $k$-self-correcting circuit and constants are implemented in the outputs of some its reliable elements, then, removing those elements, we obtain a $k$-self-correcting circuit realizing the same function as $S$ does.

Property 2. If $S$ is a $k$-self-correcting circuit and some inputs of its reliable elements are fed by constants, then, removing those elements, we obtain a $k$-self-correcting circuit implementing the same function as $S$ does.

Note that the term “a constant is implemented” (or “fed by a constant”) means that it is implemented (fed, respectively) for all admissible faults of the circuit, admissible in the sense that there are at most $k$ faults and the elements themselves are correct. To prove the lower estimate, we need the following evident property generalizing the first two.

Property 3. If a $k$-self-correcting circuit $S$ contains a set $M$ of elements such that under correct state of all elements from $M$ some their outputs implement constants and inputs of the remaining ones are fed by constants, then, removing all the elements from $M$, we obtain a $k$-self-correcting circuit realizing the original function.

It is not difficult to notice that for any circuit $S$ there exists an equivalent circuit $S'$ containing the same conjunctors as $S$ does and not containing any chains of two and more inverters. Below we consider just such circuits without chains of two and more inverters.

Lemma 4. For $n \geq 3$ the inequality $L_k^c(f_2^n) \geq L_k^c(f_2^{n-1}) + k + 2$ is valid.

Proof. Let $S$ be an arbitrary minimal $k$-self-correcting circuit realizing $f_2^n$, $n \geq 3$. Show that one can remove some elements with the total weight $k + 2$ from $S$ and obtain a $k$-self-correcting circuit for $f_2^{n-1}$. Since the minimal circuits under consideration do not contain chains of two and more inverters, then all the elements going after $x_i$-blockers are conjunctors.

Suppose for some input $x_i$ of the circuit $S$ the conjunctors $K_1^i, \ldots, K_r^i$ whose total weight is at least $k + 2$ go after $x_i$-blockers. In this case, due to Property 3, for $x_i \equiv 0$ one can remove all those conjunctors and also the $x_i$-preblocking conjunctors and $x_i$-blockers and obtain a $k$-self-correcting circuit realizing $f_2^{n-1}$. Thus, the assertion of the lemma is valid.

Now suppose for any input $x_i$, $i = 1, \ldots, n$, the $x_i$-blockers are followed by some conjunctors $K_1^i, \ldots, K_r^i$ with the total weight less than $k + 2$. Note that in this case all those $r$ conjunctors are unreliable, therefore, the sum of their weights does not exceed $k + 1$. Due to Lemma 3, for any $i = 1, \ldots, n$ the total weight of all elements following the $x_i$-blockers is not less than $k + 1$. Thus, the number of unreliable conjunctors going after $x_i$-blockers is exactly $k + 1$ for any $i = 1, \ldots, n$.

Suppose the circuit $S$ contains an input $x_i$ connected with an input of at least one conjunctor. Define a monotone enumeration of vertices in the circuit $S$ so that for any arc the number of its beginning is less than the number of its end (see [2]) and choose among all such conjunctors the conjunctor $K_1^i$ with the least number. Due to the minimality of the circuit, in this case there exists a chain $K_1^i, K_2^i, \ldots, K_r^i, E^−, l \geq 1$ such that at least one input of conjunctors $K_j^i, j = 2, \ldots, l$, is connected with the output of conjunctors $K_{j-1}^i$, and the input of the inverter $E^−$ (that is an $x_i$-blocker in this case) is connected with the output of the conjunctor $K_r^i$.

If among the conjunctors $K_1^i, \ldots, K_r^i$ there exists at least one conjunctor $K_k^i$ not going after an $x_i$-blocker, then by Lemma 3 and Property 3 for $x_i \equiv 0$ one can remove $(k + 1)$ conjunctors going after...