Synthesis and complexity of asymptotically optimal circuits with unreliable gates

Marina An. Alekhina
Penza State University
Krasnaya st., 40, Penza, Russia
ama@sura.ru

Abstract. We consider the realization of Boolean functions by combinatorial circuits with unreliable gates computing the functions from a full final basis $B$. We assume that all gates of the basis can have inverse faults on the outputs independently with probability $\varepsilon$ ($\varepsilon \in (0, 1/2)$). We describe a set $M_k$ ($k \geq 3$) of Boolean functions, presence even by one of which in basis $B$ guarantees the computing of almost all Boolean functions by asymptotically optimal circuits with unreliability $\varepsilon$ at $\varepsilon \to 0$. We prove that, for almost all functions, the complexity of asymptotically circuits with unreliable gates exceeds the complexity of the minimal circuits constructed from absolutely reliable gates by a multiplicative factor of $3(1 + b)$.

Keywords: Boolean function, synthesis, complexity, reliability of combinatorial circuits

1. Introduction

J. von Neumann [1] was the first who tried to solve the problem of synthesis reliable combinatorial circuits of unreliable functional gates. He supposed that gates were exposed to inverse faults on the outputs, when functional gate with Boolean function $e(\tilde{x})$ in the faulty state realizes function $\bar{e}(\tilde{x})$. All gates of the circuit turned into the faulty states independently with the probability $\varepsilon$ ($\varepsilon \in (0, 1/2)$). With the use of the J. Neumann’s iterative method any Boolean function $f(x_1, ..., x_n)$ can be realized by a circuit for which the error’s probability on the output not greater than $c_1\varepsilon$ at any input binary vector of variable’s values (a number $c_1$ is the some absolute constant, $c_1$ dependents from a basis).

To increase the reliability of the circuits J. von Neumann used the circuit, realizing the function (the median) $g(x_1, x_2, x_3) = x_1x_2 \lor x_1x_3 \lor x_2x_3$ (in the sequel denote this function by $g$). Later the problem of realization of Boolean functions by reliable circuits at the single-type constant faults only on the inputs or only on the outputs of gates was being solved by the author. But to increase the reliability of the circuits were used the circuits, realizing both the median $g(x_1, x_2, x_3) = x_1x_2 \lor x_1x_3 \lor x_2x_3$ and the
functions \(g_1(x_1, x_2, x_3, x_4) = x_1x_2 \lor x_3x_4, g_2(x_1, x_2, x_3, x_4) = (x_1 \lor x_2)\overline{x}_3 \lor x_4\). S. I. Aksenov [2] expanded the set of functions with the specified property. He introduced the sets of the functions \(G_1 = \{x_1^a x_2^a \lor x_1^a x_3^a \lor x_2^a x_3^a\}, G_2 = \{(x_1^a x_2^a \lor x_3^a x_4^a)^{05}\}, a_i \in \{0, 1\}, i = 1, 5\) and showed that at inverse faults on outputs of gates the presence of any function of the set \(G = G_1 \cup G_2 (|G_1| = 8, |G_2| = 3 \cdot 16 \cdot 2 = 96)\) (S. I. Aksenov [2] write \(|G_2| = 32\), that is not correct) in a given full final basis \(B\) guarantees the realization of any Boolean function by a circuit, functioning with the errors’ probabilities not more then \(\varepsilon + c_2 \varepsilon^2\), where \(\varepsilon \in (0, d]\), constants \(c_2, d\) are some positive numbers. It turned out that presence of some other functions in the basis \(B\) gives the same result. Let’s describe these functions.

2. Properties of functions used for increase of reliability of circuits

Two binary vectors \(\bar{a} = (a_1, ..., a_k)\) and \(\bar{b} = (b_1, ..., b_k)\) are called next if

\[
\sum_{i=1}^{k} |a_i - b_i| = 1.
\]

Suppose Boolean function \(m(x_1, ..., x_k)\) depends essentially no less than from three variables (i.e. \(k \geq 3\)) and has a property: there exist a binary vector \((b_1, ..., b_k)\) such that the function \(m\) equals 0 on it and all next binary vectors and the function \(m\) equals 1 on the binary vector \((b_1, ..., b_k)\) and all next binary vectors. We shall call the binary vectors \((b_1, ..., b_k)\) and \((\bar{b}_1, ..., \bar{b}_k)\) by the characteristic binary vectors of function \(m(x_1, ..., x_k)\). By \(M_k\) denote the set of functions \(m(x_1, ..., x_k)\) with the called property. It is not difficult to check that \(2^{k} - 2^{k-2} \leq |M_k| \leq 2^{k-2} - 2\). Let’s notice also

1) \(M_3 = G_1, \ |M_3| = 8\),
2) \((G_1 \cup G_2) \subset M_4\) and \(|M_4| = 992\),
3) \(M_i \subset M_j, 3 \leq i < j\).

Let’s consider the realization of Boolean functions by the circuits of unreliable gates in a full final basis \(B\). The circuit of unreliable functional gates [3] realizes the Boolean function \(f(x_1, ..., x_n)\) if for any the binary vector \(\bar{a} = (a_1, ..., a_n)\) on the circuit inputs without any faults the value \(f(\bar{a})\) appears on the circuit output. It is supposed that all gates of the circuit independently pass in faulty states and while type of malfunctions (inverse, constant or others) has not value.

Let \(P(f(\bar{a}))(S, \bar{a})\) be a probability of the appearance of the value \(f(\bar{a})\) on the output of the circuit \(S\), realizing Boolean function \(f(\bar{x})\), when the input binary vector is \(\bar{a}\). Unreliability \(P(S)\) of the circuit \(S\) is defined as maximum out of values \(P(f(\bar{a}))(S, \bar{a})\) if \(\bar{a}\) is the input binary vector of the circuit \(S\). The reliability of the circuit \(S\) equals \(1 - P(S)\).

**Theorem 2.1.** Let arbitrary Boolean function can be realized by a circuit with unreliability at most \(p\) and let function \(f(x_1, ..., x_n)\) be realized by the circuit \(S\), \(P(S) \leq p\). Suppose a circuit \(S_m\) realizes the function \(m(x_1, ..., x_k) \in M_k\) and \(P(S_m) \leq p\). By \(v^1\) and \(v^0\) denote the errors’ probabilities of the circuit \(S_m\) on the characteristic binary vectors of the function \(m(x_1, ..., x_k)\). Then the function \(f\) can be realized a circuit \(D\) such that \(P(D) \leq \max\{v^0, v^1\} + (2^k - 1)p^2\).

**Proof:**
Let \((b_1, ..., b_k)\) be a characteristic binary vector of function \(m(x_1, ..., x_k)\) and \(m(b_1, ..., b_k) = 0\). Let the
components $b_{i_1}, ..., b_{i_t}$ of this vectors equal to zero, but all the others equal to 1. Take $t$ copies of the circuit $S$ and $k-t$ copies of the circuit $S'$, realizing function $f$ with unreliability $P(S') \leq p$. Connect $i_1,...,i_t$ inputs of the circuit $S_m$ with the circuits $S$ outputs, but the rest $k-t$ inputs with the circuits $S'$ outputs. By $D$ denote the constructed this way circuit. The circuit $D$ realizes the function $f$. Compute the probabilities of errors on the circuit $D$ output.

Let $a$ be an input binary vector of the circuit $D$ such that $f(a) = 0$. Then the error’s probability $P_1(D, a)$ on the circuit’s $D$ output satisfies the inequality $P_1(D, a) \leq v^0 + kpP(S_m) + (2^k - k - 1)p^2$. But $P(S_m) \leq p$ so $P_1(D, a) \leq v^1 + (2^k - 1)p^2 = v^1 + (2^k - 1)p^2$.

Let $a$ be an input binary vector of the circuit $D$ such that $f(a) = 1$. Then the error’s probability $P_0(D, a)$ on the circuit’s $D$ output satisfies the inequality $P_0(D, a) \leq v^0 + kpP(S_m) + (2^k - k - 1)p^2$. But $P(S_m) \leq p$ so $P_0(D, a) \leq v^0 + (2^k - 1)p^2$.

Hence $P(D) \leq \max\{v^0, v^1\} + (2^k - 1)p^2$. Theorem is proved. □

**Theorem 2.2.** Let a full final basis $B$ contains the function $m(x_1, ..., x_k) \in M_k$ and all functional gates with the probability $\varepsilon \in (0, d]$ are subject to inverse faults on outputs (a number $d$ is some positive constant). Let $f$ be any Boolean function and let $S$ be a circuit, realizing $f$ with unreliability $P(S) \leq s\varepsilon$ (a positive constant $s$ depends only from the basis $B$). Then the function $f$ can be realized a circuit $D$ such that $P(D) \leq \varepsilon + (2^k - 1)s^2\varepsilon^2$.

Proof of Theorem 2.2 follows from the equality $v^1 = v^0 = \varepsilon$ and Theorem 2.1.

**Remark 2.1.** It is easy to check that at $\varepsilon \in (0, 1/2)$ the unreliability of any circuit containing at least one gate no less than $\varepsilon$.

From the Theorem 2.2 and Remarks 2.1 follows that if the basis $B$ contains function from the set $M_k$ then any Boolean function, expect functions $x_1, x_2, ..., x_n,$ can be realized by asymptotically optimal on the reliability circuits with unreliability, which equals $\varepsilon$ at $\varepsilon \to 0$. It is obvious, that functions $x_1, x_2, ..., x_n$ can be realized absolutely reliably, not using functional gates.

Obviously to increase the reliability of the circuits with the use of functions $m \in M_k$ we duplicate many times the circuits realizing functions $f$ and $\tilde{f}$. Naturally there is a question on the complexity the constructed circuits.

3. On complexity of circuits at inverse faults on outputs of gates

Consider the realization of Boolean functions by circuits of unreliable gates in any full final basis $B = \{e_1, ..., e_t\}$. In this section (except Lemma 2.2) suppose that all gates of the circuit are subject to inverse faults on the outputs of gates independently with a probability $\varepsilon \in (0, 1/2)$. It is ascribe a positive number $v(E_i)$ to each gate $E_i$ of the basis $B$. This number $v(E_i)$ is called a cost (a weight) of the gate $E_i$. A complexity $L(S)$ of a circuit $S$ is defined as

$$L(S) = \sum_{E_i \in S} v(E_i).$$

Let $\rho = \min v(E_i)/(n(E_i) - 1)$, where $n(E_i)$ is a number essential variables of function $e_i$ and $n(E_i) > 1$. Unreliability and reliability of the circuit $S$ are defined also as in the previous section.

Inverse faults on outputs of gates were investigated in von J. Neumann’s [1], S.I. Ortyukov’s [4], D. Uhlig’s [5] and some other authors’ papers. J. von Neumann offered an iterative method to rise the
reliability of circuits, however the complexity of the circuit repeatedly increases with a extension of the iterations number. The complexity of the circuits is devoted the S.I. Ortyukov’s [4] and D.Uhlig’s [5] papers.

Introduce Shannon’s function

\[
L_{p,\varepsilon}(n) = \max_f \min_S L(S),
\]

where \(S\) is a circuit of the unreliable gates and \(S\) realizes the function \(f(x_1, \ldots, x_n)\) with the unreliability \(P(S) \leq p\).

O. B. Lupanov [6] has shown

\[
L_{0,0}(n) \sim \rho \cdot 2^n / n
\]

for the circuits realizing Boolean functions and consisting only of the reliable gates (i.e. \(\varepsilon = 0, \ p = 0\)).

By \(N_g\) denote the minimal number of the reliable gates which is necessary for the realization of the function \(g(x_1, x_2, x_3) = x_1 x_2 \lor x_1 x_3 \lor x_2 x_3\) in the basis \(B\).

Formulate S. I. Ortyukov’s result [4]: if \(\varepsilon < \varepsilon_0, \ p > q(\varepsilon) N_g\), where \(q(\varepsilon) = \varepsilon + 3\varepsilon^2 + o(\varepsilon^2)\) at \(\varepsilon \rightarrow 0\) there is a function \(\rho(\varepsilon) \rightarrow \rho\) at \(\varepsilon \rightarrow 0\) such that \(L_{p,\varepsilon}(n) \lesssim \rho(\varepsilon) \cdot 2^n / n\). D. Uhlig [5] has received the following result.

**Theorem 3.1.** ([5]) For any arbitrarily small positive numbers \(c, \ b \ (c, b > 0)\) there exists a number \(\varepsilon_1 (\varepsilon_1 \in (0, 1/2))\) with the property that if \(\varepsilon \in (0, \varepsilon_1)\), if each gate of the given basis \(B\) has an error probability not greater than \(\varepsilon\) and if \(p \geq (1 + c)\varepsilon N_g\) (more precisely if \(p \geq q(\varepsilon) N_g\), the function \(q(\varepsilon)\) is defined above) then \(L_{p,\varepsilon}(n) \lesssim (1 + b) \rho \cdot 2^n / n\).

Thus S. I. Ortyukov and D. Uhlig have found the methods of the synthesis of the asymptotically optimal on the complexity circuits functioning with some level of the reliability \(1 - p\) for the inverse faults on the outputs of the gates.

Denote \(P_\varepsilon(f) = \inf P(S)\), where \(S\) is the circuit of the unreliable gates and \(S\) realizes Boolean function \(f(\bar{x})\).

The circuit of unreliable gates \(A\) realizing Boolean function \(f(\bar{x})\) is called asymptotically optimum on reliability if \(P(A) \sim P_\varepsilon(f)\) at \(\varepsilon \rightarrow 0\), i.e.

\[
\lim_{\varepsilon \rightarrow 0} \frac{P(A)}{P_\varepsilon(f)} = 1.
\]

If the basis \(B\) contains the function \(g(x_1, x_2, x_3) = x_1 x_2 \lor x_1 x_3 \lor x_2 x_3\) (and hence \(N_g = 1\)) at \(p \sim \varepsilon (\varepsilon \rightarrow 0)\) then the circuits constructed by S. I. Ortyukov and D. Uhlig are not only optimum on the complexity but also asymptotically optimal on the reliability (see Remark 2.1). These circuits function with unreliability, which asymptotically equals \(\varepsilon\) at \(\varepsilon \rightarrow 0\). If the basis \(B\) does not contain the median \(g\) (for example \(B = \{\bar{x} \lor \bar{y}\}\)) then circuits constructed by S.I. Ortyukov and D. Uhlig are not asymptotically optimal on the reliability.

Let \(B = \{x|y\} \ (x|y = \bar{x} \lor \bar{y})\), and the costs (the weights) of all basic gates are equal to 1, then \(\rho = 1\). Remember that all basic gates are subject to inverse faults on outputs. Theorems 3.2 and 3.3 are correct.

**Theorem 3.2.** ([7]) In basis \(\{x|y\}\) at \(\varepsilon \in (0, 1/160]\) any Boolean function can be realized by a circuit \(S\) such that \(P(S) \leq 3\varepsilon + 48\varepsilon^2\).
Let $h(x_1, ..., x_n)$ be any Boolean function. By $K(n)$ denote the set of Boolean functions $f(x_1, ..., x_n) = \left(\bar{x}_i \lor h(x_1, ..., x_n)\right)^a$, where $i = 1, n, a \in \{0, 1\}$.

**Theorem 3.3.** ([17]) If $\varepsilon \in (0, 1/8]$, Boolean function $f(\bar{x}) \notin K(n)$, and $S$ is any circuit, realizing $f$, then $P(S) \geq 3\varepsilon - 6\varepsilon^2 + 4\varepsilon^3$.

From Theorems 3.2 and 3.3 it follows that at inverse faults on the outputs of the gates any Boolean function $f \not\in K(n)$ can be realized by the circuit $S$ with the unreliability $P(S) \sim 3\varepsilon$ as $\varepsilon \to 0$. Therefore any circuit $A$, satisfying conditions of Theorem 3.2 and realizing function $f \notin K(n)$, is asymptotically optimal on the reliability.

Obviously $|K(n)| \leq 2n2^{2n-1}$ that it is little since the number of all Boolean functions of $n$ variables, which equals $2^{2n}$. Therefore at inverse faults on outputs gates $x/y$ almost all Boolean functions can be realized by asymptotically optimal on the reliability circuits.

It is necessary to know a value $N_g$ in basis $\{x/y\}$ for comparison of these results with S. I. Ortyukov’s and D. Uhlig’s results. It is easily proved that

$$g(x_1, x_2, x_3) = (x_1x_2)[((x_1|x_3)(x_2|x_3))|(x_1|x_3)(x_2|x_3))].$$

From the formula (2) it follows that $N_g \leq 6$, i.e. it is enough six gates for the realization of the function $g$. But undifficult to check up that it is not enough four gates for the realization of the function $g$, i.e. $N_g \geq 5$. Hence the circuits constructed by S. I. Ortyukov and D. Uhlig function with the unreliability it is no more $p$ and $p \geq g(\varepsilon)N_g > 5\varepsilon$. However from Theorem 3.2 it follows that any Boolean function can be realized by the circuit $S$ with unreliability $P(S) \leq 3\varepsilon$ at $\varepsilon \to 0$. Thus one cannot consider that the circuits constructed by S. I. Ortyukov and D. Uhlig are asymptotically optimal on the reliability.

It is proved [7] also that any Boolean function of $n$ variables can be realized by circuit $S$ such that $P(S) \leq 3\varepsilon + 126\varepsilon^2$, $L(S) \leq 224 \cdot 2^n/n$ in basis $\{x/y\}$ at $\varepsilon \leq 1/600$. The estimation of complexity can be improved (see Theorem 3.4).

**Lemma 3.1.** ([7]) In basis $\{x/y\}$ at $\varepsilon \leq 1/600$ the function $g(x_1, x_2, x_3) = x_1x_2 \lor x_1x_3 \lor x_2x_3$ can be realized by a circuit $A$ such that $P(A) \leq 3\varepsilon + 33\varepsilon^2$ and $L(A) = 111$.

**Lemma 3.2.** ([8]) Let $B$ be any full final basis. Let a circuit $S_1$ realizes Boolean function $f$ with unreliability $P(S_1)$. Let a circuit $G$ realizes function $g$ with unreliability $P(G)$. Then $f$ can be realized by a circuit $S_2$ such that $P(S_2) \leq P(G) + 3P^2(S_1)$, $L(S_2) = 3L(S_1) + L(G)$.

We remark that Lemma 3.2 is true at any faults of the basic gates.

**Theorem 3.4.** In basis $\{x/y\}$ for any $b (b > 0)$ there is a constant $\varepsilon_2$ ($\varepsilon_2 \in (0, 1/2)$) such that at any $\varepsilon \in (0, \varepsilon_2)$ Any Boolean function $f(x_1, x_2, ..., x_n)$ can be realized by a circuit $S$ such that $P(S) \leq 3\varepsilon + 144\varepsilon^2$, $L(S) \leq 3(1+b)2^n/n$.

**Proof:**

Let $f(x_1, x_2, ..., x_n)$ be any Boolean function. Using Theorem 3.1 and believing $c = 1/100$ we get that there is constant $\varepsilon_1$ such that at anyone $\varepsilon \in (0, \varepsilon_1)$ and $p = 1.01\varepsilon N_g$ the function $f$ can be realized by a circuit $S_1$ such that $P(S_1) \leq 1.01\varepsilon N_g \leq 6.06\varepsilon$ and $L(S_1) \leq (1+b)2^n/n$. From Lemma 3.1 at $\varepsilon \in (0, 1/600)$ it follows that the function $g(x_1, x_2, x_3)$ can be realized by a circuit $G$ such that
\[ P(G) \leq 3\varepsilon + 33\varepsilon^2. \] Take three copies of the circuit \( S_1 \) and unite their outputs with the inputs of the circuit \( G \). By \( S \) denote the constructed circuit. From Lemma 3.2 we have \( P(S) \leq P(G) + 3P^2(S_1) \leq 3\varepsilon + 33\varepsilon^2 + 3(6,06\varepsilon)^2 \leq 3\varepsilon + 144\varepsilon^2, \) if \( \varepsilon \in (0,\varepsilon_2) \) \( (\varepsilon_2 = \min\{\varepsilon_1, 1/600\}) \) It is evident that \( L(S) = 3L(S_1) + L(A) \lesssim 3L(S_1) \lesssim 3(1 + b)2^n/n. \) Theorem is proved. \( \square \)

The circuits constructed at the proof of Theorem 3.4 for almost all functions are asymptotically optimal on the reliability, and its complexity differs from the complexity of the minimal circuits constructed only from the reliable gates \( 3(1 + b) \) times more (see (1)), where the constant \( b \) is any arbitrarily small positive number.

Received in the basis \( \{\overline{x} \lor \overline{y}\} \) at inverse faults on the outputs of the gates results are true [8] for dual functions in the basis \( \{\overline{x} \land \overline{y}\} \) at the inverse faults on the outputs of the gates.

**Remark 3.2.** It is obvious that the suggested in Theorem 3.4 method of synthesis of asymptotically optimal on the reliability circuits \( S \) can be realized in any full final basis \( B \) at inverse faults on the outputs of the gates, and the complexity of these circuits satisfies to an inequality \( L(S) \lesssim 3(1 + b)\rho \cdot 2^n/n. \) And, if the basis \( B \) contains function from the set \( M_k \) then unreliability of asymptotically optimal circuits for almost all Boolean function equals \( \varepsilon \) at \( \varepsilon \to 0. \)

**References**


