ISSN 0027-1322, Moscow University Mathematics Bulletin, 2015, Vol. 70, No. 5, pp. 226–229. © Allerton Press, Inc., 2015.
Original Russian Text © Yu.A. Kombarov, 2015, published in Vestnik Moskovskogo Universiteta, Matematika. Mekhanika, 2015, Vol. 70, No. 5, pp. 47–50.

BRIEF COMMUNICATIONS

# Upper Estimate of Realization Complexity of Linear Functions in a Basis Consisting of Multi-Input Elements

**Yu. A. Kombarov**

*Moscow State University, Faculty of Mechanics and Mathematics, Leninskie Gory, Moscow, 119991 Russia; e-mail: yuri.kombarov@gmail.com*

June 6, 2014

**Abstract**—The paper is focused on realization of parity functions by circuits in the basis $U_\infty$. This basis contains all functions of the form $(x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k})^\beta$. A method of construction of circuits for a parity function of $n$ variables with the complexity $\lfloor(7n-4)/3\rfloor$ is described. This improves the previously known upper bound of $U_\infty$-complexity of parity functions that was $\lceil(5n-1)/2\rceil$. The minimality of constructed circuits is verified for very small $n$ (for $n<7$).

**DOI:** 10.3103/S0027132215050083

**Introduction.** We study circuits of functional elements [1] realizing linear Boolean functions (the homogeneous linear function $l_n(x_1,\ldots,x_n)=x_1\oplus\ldots\oplus x_n$ and the inhomogeneous linear function $\overline{l_n}(x_1,\ldots,x_n)=x_1\oplus\ldots\oplus x_n\oplus 1$). The complexity of realization of linear functions by circuits (defined as the minimal number of functional elements sufficient to realize a function $f$ by a circuit in a given basis $B$ and denoted by $L_B(f)$) is known for many bases consisting of elements having not more than two inputs. For example, it was proved in [2] that $L_{\{x\&y,x\vee y,\overline{x}\}}(l_n)=L_{\{x\&y,x\vee y,\overline{x}\}}(\overline{l_n})=4n-4$, and the results of [3] and [4] imply $L_{\{x|y\}}(l_n)=4n-4$ and $L_{\{x|y\}}(\overline{l_n})=4n-3$ (here $x|y$ denotes the Sheffer stroke defined as $x|y=\overline{x\&y}$). The complexity of linear functions is also known for the basis $U_2$ consisting of all elements realizing nonlinear functions essentially dependent on two variables. The equality $L_{U_2}(l_n)=L_{U_2}(\overline{l_n})=3n-3$ was proved in [5].

The structure of minimal circuits is known for some bases. For example, it was shown in [6] that all minimal circuits realizing $l_n$ or $\overline{l_n}$ in the basis $\{x\&y,x\vee y,\overline{x}\}$ consist of $n-1$ four-element blocks each of which realizes a linear function of two variables. In [4], a similar fact was proved for circuits realizing homogeneous linear functions in the basis $\{x|y\}$.

The complexity of realization of linear functions is known for some bases containing multi-input elements. One of the first results in this direction was obtained in [7] where the minimal circuits realizing linear function in the basis $NOR$ were considered, this basis consists of all elements realizing functions of the form $\overline{x_1\vee\ldots\vee x_k}$ ($k\in\{2,3,\ldots\}$). It was shown that $L_{NOR}(l_2)=5$, $L_{NOR}(\overline{l_2})=4$ and $L_{NOR}(l_n)=L_{NOR}(\overline{l_n})=3n-2$ for $n\geq 3$. Due to duality reasons, this result can be extended to the basis $NAND$ consisting of all elements realizing functions of the form $\overline{x_1\&\ldots\&x_k}$ ($k\in\{2,3,\ldots\}$): $L_{NAND}(l_n)=L_{NAND}(\overline{l_n})=3n-2$ for $n\geq 3$.

Circuits realizing linear functions in various bases consisting of multi-input elements were studied in [8]. For the basis $T$ consisting of all elements realizing threshold Boolean functions, the equality $L_T(l_n)=L_T(\overline{l_n})=\lceil\log(n+1)\rceil$ was proved. Circuits realizing linear functions in the basis $U_\infty$ were also considered in [8]. The basis $U_\infty$ consists of all elements realizing functions of the form $(x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k})^\beta$, where $k\in\{2,3,\ldots\}$, and $\sigma_1,\ldots,\sigma_k,\beta\in\{0,1\}$. This basis is a natural generalization of the basis $U_2$. The inequalities $2n-1\leq L_{U_\infty}(l_n)\leq\lceil(5n-4)/2\rceil$ and $2n-1\leq L_{U_\infty}(\overline{l_n})\leq\lceil(5n-4)/2\rceil$ were proved in [8]. This paper is focused on improvement of two latter estimates.

**Definitions and auxiliary assertions.** Below we consider circuits in the basis $U_\infty$ consisting of elements realizing function of the form $x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k}$ or $x_1^{\sigma_1}\vee\ldots\vee x_k^{\sigma_k}$. We call the elements realizing functions of the form $x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k}$ conjunctors and the elements realizing functions of the form $x_1^{\sigma_1}\vee\ldots\vee x_k^{\sigma_k}$ disjunctors. If an element realizes a function of the form $x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k}$, we call its $i$th input ($i\in\{1,\ldots,k\}$) *positive* in the case $\sigma_i=1$ and *negative* in the case $\sigma_i=0$. Positive and negative inputs for disjunctors are defined similarly. The figure represents functional elements as triangles and inputs of elements are on the upper sides of triangles. Negative inputs are marked by circles. The *complexity of a circuit* $S$ in the basis $U_\infty$ is said to be the number of elements in the circuit $S$. We denote the complexityof

the circuit $S$ by $L(S)$. The *complexity of realization of a Boolean function* $f$ in the basis $U_\infty$ is said to be the value $L_{U_\infty}(f) = \min L(S)$, where the minimum is taken over all circuits $S$ realizing $f$.

The following result was proved in [8].

**Theorem 1.** *The following estimates are valid for* $n \geq 2$*:*

$$2n-1 \leq L_{U_\infty}(l_n) \leq \lceil (5n-4)/2 \rceil,$$

$$2n-1 \leq L_{U_\infty}(\overline{l_n}) \leq \lceil (5n-4)/2 \rceil.$$

In order to prove the upper estimate, paper [8] described a construction method for circuits realizing linear functions of $n$ variables with the complexity $\lceil (5n-4)/2 \rceil$. For odd $n$ those circuits consist of $\lfloor n/2 \rfloor$ five-element blocks realizing linear functions of three variables in accordance with the representations $l_3(x_1,x_2,x_3) = x_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3 \vee x_1x_2x_3$, and $\overline{l_3}(x_1,x_2,x_3) = \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2x_3 \vee x_1\bar{x}_2x_3 \vee x_1x_2\bar{x}_3$, and for even $n$ they consist of $n/2-1$ such blocks and one three-element block realizing a homogeneous linear function of two variables in accordance with the representation $l_2 = \bar{x}_1x_2 \vee x_1\bar{x}_2$. Figure 1 show a circuit of thirteen elements realizing $l_6$ and constructed according to the construction described above,

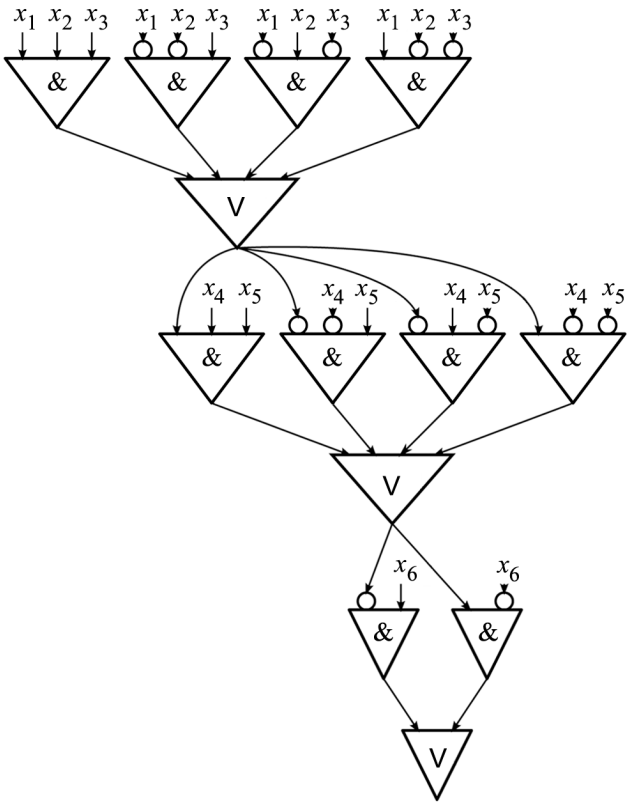


**Fig. 1.**

The following lemma allows us to construct circuits realizing linear functions of $n$ variables with the complexity less than $\lceil (5n-4)/2 \rceil$.

**Lemma 1.** *Let there exist circuits* $S_1$ *and* $S_2$ *in the basis* $U_\infty$ *such that* $S_1$ *realizes a linear function of* $n$ *variables,* $S_2$ *realizes a linear function of* $m$ *variables, and a certain input of the circuit* $S_2$ *is connected only with positive inputs of conjunctors. In this case there exists a circuit* $S_3$ *in the basis* $U_\infty$ *realizing a linear function of* $n+m-1$ *variables with the complexity* $L(S_1)+L(S_2)-1$.

*Proof.* Let the inputs of the circuit $S_1$ be supplies with the variables $x_1,\ldots,x_n$ and the inputs of the circuit $S_2$ be supplied with the variables $y_1,\ldots,y_n$. Let $E^*$ be an output element of the circuit $S_1$, $\{v_1^+,\ldots,v_p^+\}$ be the set of vertices of the circuit (i.e., output elements or inputs of the circuit) connected with the positive inputs of the element $E^*$, and $\{v_1^-,\ldots,v_q^-\}$ be the set of vertices of the circuit connected with negative inputs of the element $E^*$ (probably, $p=0$ or $q=0$). If $E^*$ is a disjunctor, we replace it by the conjunctor whose negative inputs are connected with the vertices $\{v_1^+,\ldots,v_p^+\}$ and positive inputs are connected with the vertices $\{v_1^-,\ldots,v_q^-\}$. Obviously, after this transformation the circuit realizes a linear function (being the negation of the function realized by the circuit $S_1$ originally). Below we assume that the element $E^*$ is a conjunctor.

By condition, one input of the circuit $S_2$ is connected only with positive inputs of conjunctors. Assume that this is the input corresponding to the variable $y_1$. Let $E_1,\ldots,E_k$ are conjunctors whose inputs connected to this input.

Join the circuits $S_1$ and $S_2$ connecting the output of the element $E^*$ of the circuit $S_1$ with the input of the circuit $S_2$ corresponding to the variable $y_1$. The obtained circuit $S$ realizes a linear function of the variables $x_1,\ldots,x_n,y_2,\ldots,y_m$ with the complexity $L(S_1)+L(S_2)$. The output of the element $E^*$ of the circuit $S$ is connected with positive inputs of the conjunctors $E_1,\ldots,E_k$, positive inputs of $E^*$ are connected with the vertices $\{v_1^+,\ldots,v_p^+\}$, and negative inputs are connected with the vertices $\{v_1^-,\ldots,v_q^-\}$.

Further, for each $i \in \{1,\ldots,k\}$ we remove the input of the element $E_i$ connected with the output of $E^*$ and add $p$ positive inputs connected with the vertices $\{v_1^+,\ldots,v_p^+\}$ and also add $q$ negative inputs connected with the vertices $\{v_1^-,\ldots,v_q^-\}$. It is easy to see that after this transformation the function realized by the element $E_i$ does not change and hence the function realized by the circuit $S$ does not change too. After applying all $k$ transformations, the circuit gets no elements whose inputs are connected to the output ofthe

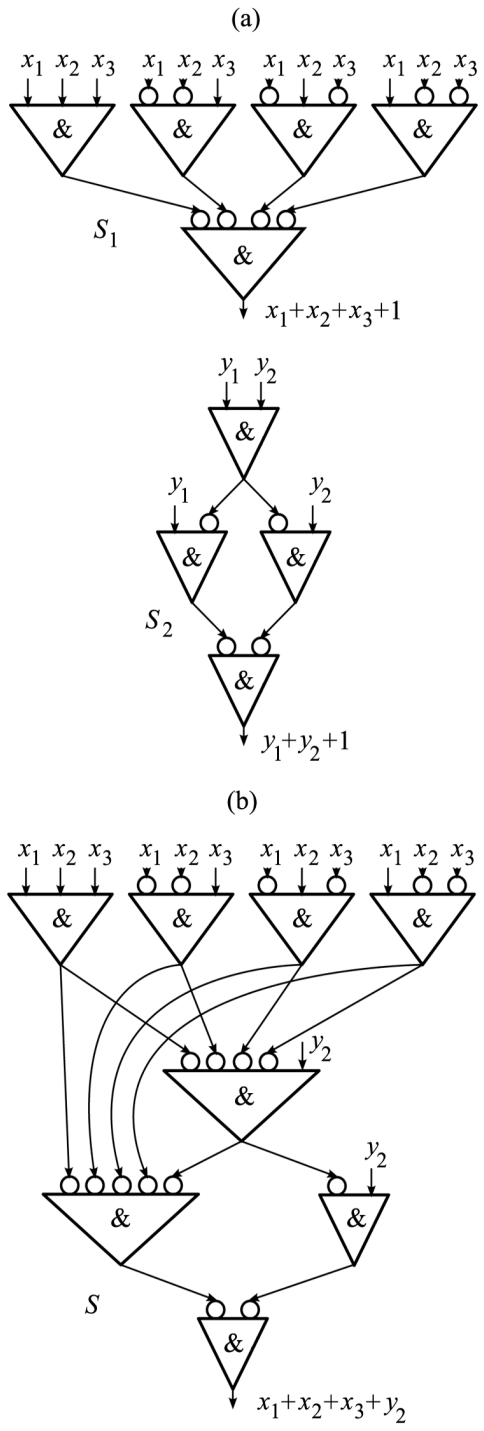


**Fig. 2.**

element $E^*$, therefore, the element $E^*$ can be removed from $S$ not changing the function realized by the circuit. Lemma 1 is proved.

Figure 2, *a* presents an example of a pair of circuits $S_1$ and $S_2$ for which Lemma 1 is applicable, Figure 2, *b* shows the result of application of the lemma to these circuits.

**Upper estimate of complexity of linear functions.** The following theorem improves the upper estimate of the complexity of linear functions in the basis $U_\infty$ previously obtained in [8].

**Theorem 2.** *The following estimates hold for* $n \geq 2$*:*

$$L_{U_\infty}(l_n) \leq \left\lfloor \frac{7n-4}{3} \right\rfloor, \; L_{U_\infty}(\overline{l_n}) \leq \left\lfloor \frac{7n-4}{3} \right\rfloor.$$

*Proof.* Show that for any $n \in \{2,3,\ldots\}$ and $\varepsilon \in \{0,1\}$ there exists a circuit realizing $l_n^\varepsilon$ with the complexity $\lfloor (7n-4)/3 \rfloor$. To do that, it is sufficient to prove that for any $n$ there exists a circuit realizing a linear function of $n$ variables (homogeneous or inhomogeneous) with the necessary complexity. This follows form the fact that, given a circuit realizing a linear function of $n$ variables, one can obtain a circuit realizing the negation of this function by taking one input of this circuit and replacing all positive inputs of elements connected with that taken input by negative ones and replacing negative inputs of elements connected with that taken input by positive ones.

We prove the required assertion by induction. The base of induction is formed by the cases $n = 2,3,4$. In order to construct a circuit of three elements realizing $l_2$ and a circuit of five elements realizing $l_3$, it is sufficient to use the representation of the required function in the perfect disjunctive normal form. A circuit of eight elements realizing $l_4$ is shown in Figure 2,*b*.

Let $n \geq 5$ and there exists a circuit $S_{n-3}$ realizing a linear function of $n-3$ variables with the complexity $\lfloor (7(n-3)-4)/3 \rfloor = \lfloor (7n-25)/3 \rfloor$. Prove that there exists a circuit realizing a linear function of $n$ variables with the complexity $\lfloor (7n-4)/3 \rfloor$. Let $S$ be the circuit shown in Figure 2,*b* (realizing a homogeneous linear function of four variables). Note that the input of the circuit $S$ corresponding to the variable $y_2$ is connected with positive inputs of conjunctors only. Therefore, Lemma 1 is applicable to the circuits $S_{n-3}$ and $S$ and hence there exists a circuit realizing a linear function of $n$ variables with the complexity $L(S_{n-3})+L(S)-1 = \lfloor (7n-25)/3 \rfloor + 8 - 1 = \lfloor (7n-4)/3 \rfloor$. Theorem 2 is proved.

**Remark.** The proof of Theorem 2 contains a description of the procedure allowing one to construct a circuit realizing $l_n^\varepsilon$ with the complexity $\lfloor (7n-4)/3 \rfloor$ for any $n$ and $\varepsilon$. The author expects that the circuits constructed here are minimal for any $n$. Show that they are minimal for small $n$. To do that, we use the following lemma proved in [8].

**Lemma 2.** *The relations* $L_{U_\infty}(l_n) = L_{U_\infty}(\overline{l_n})$ *and* $L_{U_\infty}(l_{n+1}) \geq L_{U_\infty}(l_n) + 2$ *are valid for* $n \geq 2$.

Lemma 2 is proved by the method of obstructive constants and forms the base of the proof of the lower estimate in Theorem 1.

For $n = 2,3,4,5,6$ the complexities of constructed circuits realizing linear functions of $n$ variables are equal to $3,5,8,10,12$, respectively. It is not difficult to check (see [8]) that a linear function of two variables cannot be realized by a circuit of two elements. Therefore, $L_{U_\infty}(l_2) = L_{U_\infty}(\overline{l_2}) = 3$. This fact and Lemma 2 imply $L_{U_\infty}(l_3) = L_{U_\infty}(\overline{l_3}) = 5$. Applying full computer search, we had checked that there are no circuits

of seven elements realizing $l_4$ or $\overline{l_4}$. Therefore, $L_{U_\infty}(l_4) = L_{U_\infty}(\overline{l_4}) = 8$. This fact and Lemma 2 imply $L_{U_\infty}(l_5) = L_{U_\infty}(\overline{l_5}) = 10$ and $L_{U_\infty}(l_6) = L_{U_\infty}(\overline{l_6}) = 12$.

## ACKNOWLEDGMENTS

The author is grateful to his scientific advisor, Prof. N. P. Red'kin for help in the work.

The work was supported by the Russian Foundation for Basic Research (project no. 14–01–00598, "Problems of synthesis, complexity, and checking of control systems").

## REFERENCES

1. O. B. Lupanov, *Asymptotic Complexity Estimates of Control Systems* (Moscow State Univ., Moscow, 1984) [in Russian].
2. N. P. Red'kin, "Proof of the Minimality of Some Circuits of Functional Elements," Problemy Kibern. **23**, 83 (1970).
3. N. P. Red'kin, "Minimal Realization of a Linear Function by a Circuit of Functional Elements," Kibernetika **6**, 31 (1971).
4. Yu. A. Kombarov, "Minimal Circuits in the Sheffer Basis for Linear Boolean Functions," Diskretn. Analiz Issled. Oper. **20** (4), 65 (2013).
5. C. P. Schnorr, "Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen," Computing **13**, 155 (1974).
6. Yu. A. Kombarov, "Minimal Realizations of Linear Boolean Functions," Diskret. Analiz Issled. Oper. **19** (3), 39 (2012).
7. H. Ch. and S. Muroga, "Logic Networks with a Minimum Number of NOR (NAND) Gates for Parity Functions of $n$ Variables," IEEE Trans. Comput. **C-36** (2), 157 (1987).
8. I. Wegner, "The Complexity of the Parity Function in Unbounded Fan-in, Unbounded Depth Circuits," Theor. Comput. Sci. **85**, 155 (1991).

*Translated by V. Valedinskii*