ISSN 0027-1322, Moscow University Mathematics Bulletin, 2010, Vol. 65, No. 2, pp. 88–91 . © Allerton Press, Inc., 2010.
Original Russian Text © D.A. Dagaev, 2010, published in Vestnik Moskovskogo Universiteta, Matematika. Mekhanika, 2010, Vol. 65, No. 2, pp. 53–56.

BRIEF COMMUNICATIONS

The Complexity of Pseudo-Linear Functions

D. A. Dagaev

Moscow State University, Faculty of Mechanics and Mathematics,
Leninskie Gory, Moscow, 119899, Russia

Received September 18, 2009

Abstract—Upper and lower estimates for the complexity of functions of the 3-valued logic taking values from the set $\{0,1\}$ with linear Boolean restrictions are derived.

DOI: 10.3103/S0027132210020099

We consider the problem of implementation of functions of the three-valued logic by formulas over finite systems. Lupanov [1] obtained an asymptotically exact estimate of the Shannon function for any complete system of Boolean functions. It was shown in [2] that for an arbitrary finite system Ψ of Boolean functions each function from $[\Psi]$ can be implemented by a formula with the complexity having at most exponential growth with respect to the number of variables. An example of a sequence of functions of the four-valued logic whose complexity in the class of formulas over some finite incomplete system has the double-exponential order of growth with respect to the number of variables was given in [3]. For some closed classes of the three-valued logic upper bounds of the corresponding Shannon functions were obtained in [4, 5]. In this paper we study the complexity of functions of the three-valued logic which take values from the set $\{0,1\}$ and whose restrictions to the set of collections of zeros and ones are linear Boolean functions. All necessary definitions can be found in [1–3, 6–9].

Let $E_k = \{0,1,\dots,k-1\}$, $k \geq 2$. By E_k^n we denote the set of all collections $\widetilde{\alpha} = (\alpha_1,\dots,\alpha_n)$ such that $\alpha_1,\dots,\alpha_n \in E_k$. By P_k we denote the set of all functions of the k-valued logic and by $P_{3,2}$ the set of all functions from P_3 taking values from the set E_2 only. Let $F \subseteq P_k$. By $[F]$ we denote the closure of the set F with respect to superpositions and the operation of introducing inessential variable (see [6]), and by $F(n)$ we denote the set of all functions from F depending on the variables $x_1,\dots,x_n$, $n \geq 1$.

Define the following sets of Boolean functions: L is the set of all linear functions, S is the set of all self-dual functions, T_i is the set of all functions preserving the constant i, $i = 0,1$. Assume $L_i = L \cap T_i$ for $i = 0,1$, $L_{01} = L_0 \cap L_1$, and $SL = S \cap L$. The disjunction of x_1 and x_2, conjunction of x_1 and x_2, sum modulo two of x_1 and x_2 are denoted by $x_1 \vee x_2$, $x_1 \& x_2$, $x_1 \oplus x_2$, respectively.

Let Ψ be a finite system of functions from P_k and let $f(x_1,\dots,x_n) \in [\Psi]$. Consider a formula Φ over Ψ implementing the function f and a set $F \subseteq [\Psi]$. By $L(\Phi)$ we denote the number of symbols of variables and constants occurring in the formula Φ (the complexity of the formula Φ), by $L_\Psi(f)$ we denote the complexity of the function f, and by $L_\Psi(F(n))$ — the Shannon function for the set F.

Let $f(x_1,\dots,x_n) \in P_{3,2}$. The projection of the function $f(x_1,\dots,x_n)$ is defined as the Boolean function $(\operatorname{pr} f)(x_1,\dots,x_n)$ whose value on an arbitrary collection $\widetilde{\alpha} \in E_2^n$ is given by the equality $(\operatorname{pr} f)(\widetilde{\alpha}) = f(\widetilde{\alpha})$. In what follows, the function $(\operatorname{pr} f)(x_1,\dots,x_n)$ is denoted by $\operatorname{pr} f(x_1,\dots,x_n)$. The projection $\operatorname{pr} F$ of a set of functions $F \subseteq P_{3,2}$ is defined as the set $\bigcup\{\operatorname{pr} f\}$, where the union is taken over all functions $f \in F$. It is not difficult to check that for any closed class $F \subseteq P_{3,2}$ the set $\operatorname{pr} F$ is a closed class of Boolean functions. Assume $\mathcal{L} = \{f \in P_{3,2} \mid \operatorname{pr} f \in L\}$. A function $f(x_1,\dots,x_n) \in P_{3,2}$ is called pseudo-linear if $f \in \mathcal{L}$.

Let $f(x_1,\dots,x_n) \in P_{3,2}$ and $H \subseteq E_3^n$. Define the restriction of the function f to the set H as the function from $P_{3,2}$ whose value on an arbitrary collection $\widetilde{\alpha} \in E_3^n$ is equal to $f(\widetilde{\alpha})$ for $\widetilde{\alpha} \in H$ and to 0 for $\widetilde{\alpha} \notin H$ (the notation is $f|_H$).

By $j_i(x)$ we denote the function from $P_{3,2}$ which is equal to 1 for $x = i$ and to 0 for the other cases, $i \in E_3$. By $x + y$ and $x \cdot y$ we denote the functions from $P_{3,2}$ such that for any $\alpha, \beta \in E_3$ the equalities $\alpha + \beta = j_1(\alpha) \oplus j_1(\beta)$ and $\alpha \cdot \beta = j_1(\alpha) \& j_1(\beta)$ hold, respectively.

Give a description of closed classes $H \subseteq P_{3,2}$ such that $\operatorname{pr} H = L$. Given an arbitrary pseudo-linear function $f(x_1,\dots,x_n)$, it is not difficult to see that the following equality holds:

$$f(x_1,\dots,x_n) = \sum j_{\sigma_1}(x_1)\dots j_{\sigma_n}(x_n),$$

where the sum is taken over all collections $\widetilde{\sigma} = (\sigma_1,\dots,\sigma_n) \in E_3^n$ such that $f(\widetilde{\sigma}) = 1$. Replacing each occurrence of the function $j_0(y)$ in the right-hand side of this equality by the function $1 + j_1(y) + j_2(y)$,

which is equal to it, and opening the brackets, we obtain a representation of the function $f(x_1,\dots,x_n)$ in the following form:

$$f(x_1,\dots,x_n)=\eta_f(x_1,\dots,x_n)+\delta_f(x_1,\dots,x_n), \tag{1}$$

where

$$\eta_f(x_1,\dots,x_n)=a+\sum_{i=1}^{n}a_ij_1(x_i),\qquad \delta_f(x_1,\dots,x_n)=\sum_{I,J}a_{I,J}\varkappa_{I,J}(x_1,\dots,x_n),$$

$$\varkappa_{I,J}(x_1,\dots,x_n)=\left(\prod_{i\in I}j_1(x_i)\right)\left(\prod_{j\in J}j_2(x_j)\right),$$

$a,a_i,a_{I,J}\in\{0,1\}$, and the sum in the definition of the function δ_f is taken over all sets I,J such that $I\cup J\subseteq\{1,\dots,n\}$, $I\cap J=\varnothing$, $J\neq\varnothing$. If $a_{I,J}=1$, then the function $\varkappa_{I,J}(x_1,\dots,x_n)$ is called a component of the function f. By K_f we denote the set of all components of the function f. Assume $K=\bigcup K_f$, where the union is taken over all pseudo-linear functions f. It is easy to see that the representation of a function $f\in\mathcal{L}$ in form (1) is unique (up to a permutation of summands and the order of factors in the summands). By J_f we denote the set of all functions $j_1(x_i)$, $1\le i\le n$, such that $a_i=1$ for the representation of the function f in form (1). Define a set H_f as follows: if $a=1$ in the representation of the function f in form (1), then $H_f=\{1\}$; otherwise $H_f=\varnothing$. Assume $Y_f=K_f\cup J_f\cup H_f$.

Let $a\in E_2$. Define a subset $Z_{2,a}$ of the set $P_{3,2}$, $a=0,1$, as follows. A function $f(x_1,\dots,x_n)\in P_{3,2}$ belongs to the set $Z_{2,a}$ if and only if it satisfies the following condition: if $\widetilde{\alpha}\in E_2^n$, $\widetilde{\beta}\in E_3^n$, and the collection $\widetilde{\alpha}$ is obtained from the collection $\widetilde{\beta}$ by replacing all twos by a, then $f(\widetilde{\alpha})=f(\widetilde{\beta})$, $n\ge 1$.

Define the following subsets of the set $\mathcal{L}$. Assume

$$L_2=\{f\in\mathcal{L}\mid K_f\subseteq\{\varkappa_{I,J}\in K\mid |I|\le 1\}\},$$

$$L_{2,r}=\{f\in\mathcal{L}\mid K_f\subseteq\{\varkappa_{I,J}\in K\mid I=\varnothing,|J|\le r\}\},\quad 1\le r<\infty,$$

$$L_{2,\infty}=\{f\in\mathcal{L}\mid K_f\subseteq\{\varkappa_{I,J}\in K\mid I=\varnothing\}\}.$$

It was shown in [7] that the set of all closed classes $F\subseteq\mathcal{L}$ such that $\operatorname{pr}F=L$ consists of the following classes: $\mathcal{L}$, L_2, $L_{2,\infty}$, $Z_{2,0}\cap\mathcal{L}$, $Z_{2,1}\cap\mathcal{L}$, $L_{2,r}$, where $1\le r<\infty$. And each of these closed classes, except for the class $L_{2,\infty}$, has a finite basis.

Assume $\lambda(x,y)=j_1(x)+j_1(y)$, $\mu(x,y)=j_1(x)j_2(y)$, $\nu_r(x_1,\dots,x_r)=j_2(x_1)j_2(x_2)\dots j_2(x_r)$, $r\ge 1$. Define the following systems of functions from $\mathcal{L}$. Assume

$$\mathfrak{A}=\{1,\lambda(x,y)\},\qquad \mathfrak{B}=\mathfrak{A}\cup\{j_1(x)j_1(y)j_2(z),j_0(x),j_1(x),j_2(x)\},\qquad \mathfrak{C}=\mathfrak{A}\cup\{\mu(x,y)\},$$

$$\mathfrak{D}_r=\mathfrak{A}\cup\{\nu_r(x_1,\dots,x_r)\},\qquad \mathfrak{E}=\{1,j_0(x)+j_0(y)\}.$$

It is known [7] that $[\mathfrak{A}]=Z_{2,0}\cap\mathcal{L}$, $[\mathfrak{B}]=\mathcal{L}$, $[\mathfrak{C}]=L_2$, $[\mathfrak{D}_r]=L_{2,r}$, $[\mathfrak{E}]=Z_{2,1}\cap\mathcal{L}$.

Below we obtain estimates of the Shannon functions for all finitely-generated closed classes $F\subseteq P_{3,2}$ such that $\operatorname{pr}F=L$.

Theorem 1. *Let $Q=Z_{2,0}\cap\mathcal{L}$, $U=Z_{2,1}\cap\mathcal{L}$, $W=L_2$, $V_r=L_{2,r}$, where $1\le r<\infty$. Then the following relations hold:*

$$L_{\mathfrak{A}}(Q(n))=L_{\mathfrak{C}}(U(n))=n+1,\quad n\ge 2; \tag{2}$$

$$L_{\mathfrak{D}_r}(V_r(n))=1+n+r(C_n^1+C_n^2+\dots+C_n^r),\quad n\ge r; \tag{3}$$

$$L_{\mathfrak{C}}(W(n))=n2^{n-1}+2^{n+1}-1,\quad n\ge 2. \tag{4}$$

Theorem 2. *The following relation holds:*

$$L_{\mathfrak{B}}(\mathcal{L}(n))\sim\frac{3^n}{\log_2 n}. \tag{5}$$

In order to prove Theorem 1, we need the following lemma.

Lemma. *Let $f(x_1,\dots,x_n)$ be a function from $L_{2,r}$ essentially depending on n variables, $n\ge 2$. Then $L_{\mathfrak{D}_r}(f)=|J_f|+|H_f|+r|K_f|$.*

The proof of Theorem 1 is the following. The equality $L_{\mathfrak{A}}(Q(n)) = n + 1$ in (2) follows from the fact that for any function $f(x_1, \ldots, x_n) \in Q$ essentially depending on n variables, $n \geq 2$, the relation $L_{\mathfrak{A}}(f) = L_{\{1,x+y\}}(\mathrm{pr}\, f) = n + 1$ holds. The equality $L_{\mathfrak{C}}(U(n)) = n + 1$ is valid due to the duality considerations.

Prove equality (3). If $n = r = 1$, then the statement is evident. Let $n \geq 2$, $n \geq r \geq 1$. It is easy to see that for any function $f(x_1, \ldots, x_n) \in V_r(n)$ the inequalities $|J_f| + |H_f| \leq 1 + n$ and $|K_f| \leq C_n^1 + \ldots + C_n^r$ hold. Therefore, by the Lemma, $L_{\mathfrak{D}_r}(V_r(n)) \leq 1 + n + r(C_n^1 + C_n^2 + \ldots + C_n^r)$, which implies the upper bound.

Prove the lower bound. By θ_n we denote the function from the set $V_r(n)$ for which all coefficients in the representation (1) are equal to 1. It is evident that $|J_{\theta_n}| + |H_{\theta_n}| = 1 + n$ and $|K_{\theta_n}| = C_n^1 + \ldots + C_n^r$. The lemma implies $L_{\mathfrak{D}_r}(\theta_n) = |J_{\theta_n}| + |H_{\theta_n}| + r|K_{\theta_n}| = 1 + n + r(C_n^1 + \ldots + C_n^r)$. Therefore, $L_{\mathfrak{D}_r}(V_r(n)) \geq L_{\mathfrak{D}_r}(\theta_n) = 1 + n + r(C_n^1 + C_n^2 + \ldots + C_n^r)$.

We prove equality (4) in the following way. First, for any function $f \in L_2$ essentially depending on n variables, $n \geq 2$, we obtain the inequality $L_{\mathfrak{C}}(f) \leq |Y_f| + B(f)$, where $B(f)$ is some quantity uniquely determined by the function f. Then we show that $|Y_f| \leq n2^{n-1} + 2^n$ and $B(f) \leq 2^n - 1$. This implies the inequality $L_{\mathfrak{C}}(f) \leq n2^{n-1} + 2^{n+1} - 1$. Finally, we consider the function $\tau_n(x_1, \ldots, x_n)$ from L_2 whose all the coefficients in representation (1) are equal to 1 and show that its complexity satisfies the inequality $L_{\mathfrak{C}}(\tau_n) \geq n2^{n-1} + 2^{n+1} - 1$.

Present the sketch of the proof of Theorem 2. The upper bound in relation (5) can be obtained with the help of a modification of the asymptotically optimal method for synthesis of formulas over the basis $\{\&, \vee, \bar{}\}$ [8] (other generalizations see in [10, 11]). The proof is based on the existence of a special partition $\mathfrak{Y}$ of the set E_3^n, $n \geq 1$, into disjoint subsets $\Gamma_0, \Gamma_1, \ldots, \Gamma_t$ (where t is a parameter depending on n). Such a partition can be obtained by using the method for constructing perfect Hamming codes [9] of length m, $m < n$, over the field $GF(3)$, where m is a parameter of the form $m = (3^r - 1)/2$, $r \in \mathbb{N}$. The partition $\mathfrak{Y}$ possesses the following properties: the number of collections contained in the set Γ_0 is "sufficiently small," and for each set Γ_i, $i = 1, \ldots, t$, there exists a number $j_i \leq m$ such that for any collection $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \Gamma_i$ the equality $\alpha_{j_i} = 2$ holds.

Let $f(x_1, \ldots, x_n) \in \mathcal{L}$, $n \geq 3$. By $f|_{\Gamma_i}$ we denote the restriction of the function f to the set Γ_i, $i = 0, \ldots, t$, and assume $A = \Gamma_1 \cup \ldots \cup \Gamma_t$. Describe the main stages in the construction of a formula Φ over $\mathfrak{B}$ implementing the function f. First, we construct formulas $\Phi_1, \ldots, \Phi_t$ implementing the functions $f|_{\Gamma_1}, \ldots, f|_{\Gamma_t}$, respectively, by a method similar to the method for synthesis of formulas from [8]. Here we use the functions $j_1(x) + j_1(y)$ and $j_1(x)j_1(y)j_2(x_{j_i})$ instead of the functions $x \vee y$ and $x\&y$, respectively (see the properties of the partition $\mathfrak{Y}$). Further, we construct a formula Φ_A implementing the function $f|_A$ and having the complexity not exceeding the lower cardinality bound for the function $L_{\mathfrak{B}}(\mathcal{L}(n))$. Then, for the formula Φ_0 corresponding to the function $f|_{\Gamma_0}$ we take a formula "similar" to the perfect disjunctive normal form of this function. Finally, we consider the formula $\Phi = j_1(\Phi_0) + j_1(\Phi_A)$ implementing the function f, and its complexity (by virtue of the properties of the partition $\mathfrak{Y}$) is asymptotically equal to the complexity of the formula Φ_A.

The lower bound in relation (5) follows from cardinality considerations [8] and the equality

$$|\mathcal{L}(n)| = 2^{n+1} \cdot 2^{3^n - 2^n}.$$

Remark. For closed classes $F \subseteq P_{3,2}$ such that $\mathrm{pr}\, F \in \{L_0, L_1, LS, L_{01}\}$, similar relations can be established.

ACKNOWLEDGMENTS

The authors are grateful to Prof. A. B. Ugol'nikov for attention to the work.

The work was supported by the Russian Foundation for Basic Research (project no. 08–01–00863), by the program "Leading Scientific Schools" (project no. NSh-4470.2008.1), and by the program of fundamental researches of OMN RAN "Algebraic and combinatorial methods of mathematical cybernetics" (project "Problems of optimal synthesis of control systems").

REFERENCES

1. O. B. Lupanov, "Complexity of Formula Realization of Functions of Logical Algebra," Probl. Kibernet. **3**, 61 (1960).
2. A. B. Ugol'nikov, "Depth of Formulas in Incomplete Bases," Matem. Voprosy Kibernet. **1**, 242 (1988).
3. A. B. Ugol'nikov, "Complexity of Realization for a Certain Sequence of Functions of 4-Valued Logic by Formulas," Vestn. Mosk. Univ., Matem. Mekhan., No. 3, 52 (2004).
4. D. A. Dagaev, "Depth and Complexity of Formula Implementation of Functions from Some Classes of the Three-

Valued Logic," in *Proc. XV Int. Conf. "Problems in Theoretical Cybernetics," Kazan', June 2–7, 2008* (Otechestvo, Kazan', 2008) [in Russian], p. 24.

5. D. A. Dagaev, "Depth of Formulas Implementing Functions from Some Classes of the Three-Valued Logic," in *Proc. IX Int. Seminar "Discrete Mathematics and its Applications," Moscow, June 18–23, 2007* (Center of Applied Researches, Department of Mechanics and Mathematics, Moscow State University, Moscow, 2007) [in Russian], pp. 84–87.
6. S. V. Yablonskii, *Introduction to Discrete Mathematics* (Vysshaya Shkola, Moscow, 2008) [in Russian].
7. D. Lau, *Function Algebras on Finite Sets* (Springer-Verlag, Berlin, 2006).
8. O. B. Lupanov, "On Synthesis of Some Classes of Control Systems," Probl. Kibernet. **10**, 63 (1963).
9. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, 1977).
10. S. B. Gashkov, "Parallel Computation of Some Classes of Polynomials with Increasing Number of Variables," Vestn. Mosk. Univ., Matem. Mekhan., No. 2, 88 (1990).
11. E. Yu. Zakharova, "Implementation of Functions from P_k by Formulas," Matem. Zametki **11** (1), 99 (1972).

Translated by A. Oshemkov