Certificates of Non-Membership for Classes of Read-Once Functions

Dmitry Chistikov[1⋆], Valentina Fedorova[2], and Andrey Voronenko[2]

[1] Max Planck Institute for Software Systems (MPI-SWS), Germany
dch@mpi-sws.org
[2] Moscow State University, Russia
{fedorovavs,dm6}@cs.msu.ru

Abstract. A certificate of non-membership for a Boolean function f with respect to a class $\mathcal{C}$, $f \notin \mathcal{C}$, is a set S of input strings such that the values of f on strings from S are inconsistent with any function $h \in \mathcal{C}$. We study certificates of non-membership with respect to several classes of read-once functions, generated by their bases. For the basis $\{\&, \vee, \neg\}$, we determine the optimal certificate size for every function outside the class and deduce that 6 strings always suffice. For the same basis augmented with a function $x_1 \dots x_s \vee \overline{x}_1 \dots \overline{x}_s$, we show that there exist n-variable functions requiring $\Omega(n^{s-1})$ strings in a certificate as $n \to \infty$. For $s = 2$, we show that this bound is tight by constructing certificates of size $O(n)$ for all functions outside the class.

Keywords: certificate of non-membership, read-once function.

1 Introduction

Let Alice and Bob share the truth table of some Boolean function $f\colon \{0,1\}^n \to \{0,1\}$. Suppose that Alice learns that f does not belong to some fixed class of functions $\mathcal{C}$. Now she wants to prove this fact to Bob, who does not trust her word and is willing to carry out all needed computation by himself. If the class $\mathcal{C}$ is known to both Alice and Bob beforehand, then Alice may want just to point Bob to some of the values in the truth table of f. If the combination of these values is inconsistent with all possible functions $h \in \mathcal{C}$, then Bob will be convinced that $f \notin \mathcal{C}$. Suppose that Alice only cares to point Bob to as few values of f as possible, that is, all computational issues are ignored and the problem is combinatorial. How many values are sufficient to prove that $f \notin \mathcal{C}$?

To capture this setting, we construct sets of input strings called *certificates of non-membership*. Basically, such a certificate for a function f with respect to a class $\mathcal{C}$ can be used to prove that $f \notin \mathcal{C}$. In this paper, we study this concept for several classes of read-once functions, obtaining bounds on the smallest possible certificate size.

⋆ Part of this research was done while Dmitry Chistikov was affiliated with Moscow State University.

While we delay most formal definitions until later, some background on read-once functions is needed in the introduction. A function h is said to be *read-once* over a finite set of functions B, called a *basis*, if it can be expressed by a formula over B where no input variable appears more than once. All other functions will be called *read-many* over B. Read-once functions have been studied from various points of view for more than half a century. Classes of read-once functions emerge in different areas of discrete mathematics and computer science, from formula (circuit) complexity [17] and positional games [7,6] to computational learning theory [19,2,3] and probabilistic databases [15].

Related work. The idea of certifying non-membership in concept classes has been studied in computational learning theory for more than a decade. Perhaps the most well-known is the work of Hellerstein et al. [11], who defined so-called polynomial certificates to characterize polynomial-query learnable *representation classes* in Angluin's learning model (a standard model for exact learning; a representation class basically provides some language for expressing functions). Following this line of research, Arias, Khardon, and Servedio [1] studied certificate size, in the sense of [11], for classes of Boolean functions representable by monotone CNF (conjunctive normal forms), unate CNF, Horn CNF, and so-called renamable Horn CNF.

Since classes of read-once functions over all finite bases are known to be polynomial-time learnable in Angluin's model as proved by Bshouty, Hancock, and Hellerstein [3], it follows that appropriate representation classes have polynomial certificates. We shall see that with our definition of certificates of non-membership this conclusion can, in a sense, be strengthened (although our current paper does not deal with arbitrary finite bases).

We wish to emphasize that our definition of certificates is different from, although not unrelated to that in [11]: our certificates show that a certain object cannot be represented within a class, while certificates in [11,1] also show (not necessarily infinite) lower bounds on the representation size.

However, a different characterization of polynomial-query learnable classes, involving almost literally (under the name of *unique specification dimension*) the (worst-case) size of certificates of non-membership as used in the present paper, was obtained by Hegedűs [8]. We discuss this characterization and its implications for our results in sections 2 and 5. The same characteristic (worst-case size of a certificate of non-membership) was also studied by Hellerstein [10], who characterized and studied classes of functions admitting constant-size certificates.

Another related area of research is the development of certifying algorithms for various computational tasks such as decision problems (see, e. g., a general survey by McConnell et al. [12]). This area is motivated by software engineering and builds upon the idea that a kind of certificate should be provided as a part of an algorithm's output. The entire output can afterwards be verified (authenticated) by a separate algorithm, which in certain cases can be expected to run faster than the main (original) algorithm. When certifying algorithms are used to decide membership in some fixed class of discrete objects, they augment each

yes-answer and no-answer with a certificate of membership and non-membership, respectively.

As an example of the implementation of this approach we refer the reader to a series of linear-time certifying algorithms for deciding membership in (or, put differently, recognition of) various classes of graphs, developed by Heggernes and Kratsch [9]. Non-membership certificates output by these algorithms are based on characterizations in terms of forbidden induced subgraphs. For an overview of a related subject of characterizing graph classes with sets of forbidden minors, we refer the reader to a paper by Thomas [18].

For various classes of Boolean functions, certificates of non-membership can take the form of forbidden projections (a *projection* is obtained from a given function by substituting some constants for input variables). For the class of unate functions, a characterization in these terms was given by Feigelson and Hellerstein, who thus captured the family of all *minimal* non-unate functions [5]. Stetsenko obtained the list of all minimal forbidden projections of read-once functions over the standard basis $B_0 = \{\&, \vee, \neg\}$ in [16]. This result was subsequently extended to larger bases; most of the papers in this subarea are only available in Russian (in the current paper, for instance, we use a theorem by Peryazev [13]; see section 4).

Our contribution. We obtain several bounds on the size of certificates of non-membership for classes of read-once functions. For the standard basis $B_0 = \{\&, \vee, \neg\}$ we show in section 3 that all read-many functions over B_0 have constant-sized certificates of non-membership. In other words, the number of strings in a (shortest possible) certificate does not grow with the number of input variables. For each read-many function f we construct a certificate and prove its optimality, that is, show that no shorter certificate exists.

We next turn to generalizing these results to larger bases B. In section 4 we consider a family of bases of the form $B^{(s)} = B_0 \cup \{h_{\mathsf{t}}^{(s)}\}$, where s-variable functions $h_{\mathsf{t}}^{(s)}$ are taken from Stetsenko's list of all minimal read-many functions over B_0. For every fixed s, we construct a sequence of n-variable read-many functions that require $\Omega(n^{s-1})$-long certificates as $n \to \infty$.

Next, for $s = 2$ we complement this result by proving that each read-many function over the basis $B^{(2)}$ has a certificate of non-membership of size at most $O(n)$, so our lower bound turns out to be tight in this special case. This basis $B^{(2)}$ is especially interesting, because it is equivalent to the (standard in some areas) basis of all two-variable functions, in the sense that an arbitrary Boolean function is read-once over the former if and only if it is read-once over the latter.

Last but not least, using the aforementioned characterization of polynomial-query learning algorithms due to Hegedűs [8], we improve existing upper bounds by Angluin, Hellerstein, and Karpinski [2] and Bshouty, Hancock, and Hellerstein [3] on the query complexity of learning read-once functions over bases B_0 and $B^{(2)}$, respectively, in Angluin's learning model, i. e., with membership and equivalence queries. We discuss these conclusions along with open problems in section 5.

Some of the results obtained in this paper improve upon our previous work. More specifically, the upper bound for the basis B_0 can be thought of as a result of [23], although a direct proof was not given there (see discussion in section 3 on why such a proof is interesting on its own in this case; the lower bound presented here is new). The results on the bases $B^{(s)}$ in general and $B^{(2)}$ in particular generalize and improve over previously known ones for the basis $B^{(2)}$: a lower bound of the form $\Omega(n)$ with a rather involved proof, together with a weaker upper bound, appeared in [22], which is only available in Russian.

2 Definitions and Notation

In this section, we give basic definitions, including that of a certificate of non-membership, and fix some notation. We first define terms related to certificates, and then review other, mostly standard, concepts.

All mappings of the form $g\colon \{0,1\}^n \to \{0,1,*\}$ will be called *partial Boolean functions*. The *domain* of such a function f is the inverse image $g^{-1}(\{0,1\})$, and g is said to be undefined on all input strings outside its domain. A *total function* is a partial function whose domain is $\{0,1\}^n$. A total function $f\colon \{0,1\}^n \to \{0,1\}$ is called an *extension* of g if f and g agree on all strings from the domain of g. Unless explicitly stated otherwise, the term "function" will only be used to refer to total functions.

Now let $\mathcal{C}$ be an arbitrary class of functions, and consider some function f not contained in $\mathcal{C}$. Call a set $S \subseteq \{0,1\}^n$ a *certificate of non-membership* for the function f with respect to the class $\mathcal{C}$ if for any n-variable function $h \in \mathcal{C}$ there exists a string $x \in S$ such that $f(x) \neq h(x)$. Alternatively, consider a (unique) partial function g with domain S whose extension is f. Then S is a certificate of non-membership for f with respect to $\mathcal{C}$ if and only if g has no extensions inside $\mathcal{C}$. The *size* of a certificate S is its cardinality $|S|$; a certificate is *optimal* if no certificate of smaller size exists.

Recall the setting sketched in the introduction, where Alice wants to convince Bob that the function f is not contained in the class $\mathcal{C}$. The smallest possible number of input strings Alice needs to point Bob to is exactly the smallest cardinality of a certificate of non-membership for the function f. Indeed, let S be a certificate of the smallest possible size. Then the values of f on strings from S prove that $f \notin \mathcal{C}$, and for any set S' of input strings such that $|S'| < |S|$ there exists a function $h' \in \mathcal{C}$ which agrees with f on all strings from S'.

Now let B be a finite set of Boolean functions. A function f is called *read-once* over B if it is either 0, 1, or some variable x_i or if it can be expressed as $h(f_1, \ldots, f_s)$, where, firstly, $h \in B$ and, secondly, all f_i depend on disjoint sets of variables and are read-once over B. All other functions will be called *read-many* over B. The set B is usually referred to as the *basis*.

Let $\mathrm{ROF}[B]$ be the set of all read-once functions over B, and suppose that f is a read-many function over B. Denote by $M_B(f)$ the smallest possible size of a certificate of non-membership for f with respect to $\mathrm{ROF}[B]$. By $M_B(n)$ we denote the maximum of $M_B(f)$ over all read-many functions $f\colon \{0,1\}^n \to \{0,1\}$.

The value $M_B(f)$ captures the size of an optimal certificate for a specific function f, and the value $M_B(n)$ provides a tight upper bound on the optimal certificate size for all n-variable (read-many) functions. In this paper, we are primarily interested in obtaining lower and upper bounds on $M_B(f)$ and $M_B(n)$.

Remark. Hellerstein et al. [11] introduced the following definition to characterize polynomial-query learnable classes. A representation class for a Boolean concept class $\mathcal{C}$ is said to have polynomial certificates if there exist two-variable polynomials p and q with the following property: for all m, n and for all n-variable functions f of (minimal representation) size greater than $p(m,n)$ there exists a set Q of input strings such that, first, $|Q| \leq q(m,n)$ and, second, for any n-variable function h from $\mathcal{C}$ of size m or less there exists a string $x \in Q$ such that $f(x) \neq h(x)$. It is implied that non-representable functions have infinite size; for a more thorough treatment of this topic we refer the reader to [11].

One can formally check that any class $\mathcal{C}$ (or, more precisely, a representation class for $\mathcal{C}$) has polynomial certificates, as defined by Hellerstein et al., with $p(m,n)$ set, for all m, to the largest possible (representation) size of an n-variable function in $\mathcal{C}$ and with some polynomial $q(m,n)$ if and only if every function $f \notin \mathcal{C}$ has a certificate of non-membership of size $q(p(m,n),n)$ with respect to $\mathcal{C}$. Therefore, the fact that (certain representation) classes of read-once functions have polynomial certificates implies that the values $M_B(n)$ are bounded from above by polynomials in n. In this paper, we strengthen this conclusion and strive to obtain tight bounds on $M_B(n)$.

As mentioned in the introduction, a different characterization of polynomial-time learnable classes, which turns out to be more closely connected to our work, was independently obtained by Hegedűs [8]. It follows from his results that for an arbitrary basis B, the query complexity $L_B(n)$ of learning the class $\mathrm{ROF}[B]$ with membership and equivalence queries satisfies $M'_B(n) \leq L_B(n) \leq 2M'_B(n)\log_2|\mathrm{ROF}[B]|/\log_2 M'_B(n)$, where the value $M'_B(n)$ is called the unique specification dimension and satisfies $|M'_B(n) - M_B(n)| \leq 1$. We discuss the implications in more detail in the concluding section 5.

We shall sometimes appeal to rooted *trees* representing read-once functions. Leaves of these trees are labeled with variables (we shall not use 0 and 1 here) without repetitions, and non-leaf nodes with functions from B. Basically, any such tree is a Boolean formula with function symbols (gate operations) from B.

We call functions $f(x_1,\ldots,x_n)$ and $g(x_1,\ldots,x_n)$ *similar* if there exist constant values $\sigma,\sigma_1,\ldots,\sigma_n$ from $\{0,1\}$ and a permutation π on $\{1,\ldots,n\}$ such that $f(x_1,\ldots,x_n) = g^{\sigma}\left(x_{\pi(1)}^{\sigma_1},\ldots,x_{\pi(n)}^{\sigma_n}\right)$, where z^{τ} stands for z if $\tau = 1$ and for $\overline{z}$ if $\tau = 0$. We shall sometimes use this concept for partial functions, in which case it is understood that $\overline{*} = *$.

As usual, a function $f(x_1,\ldots,x_n)$ is called *monotone* if the inequalities $\alpha_i \leq \beta_i$, $i = 1,\ldots,n$, imply that $f(\alpha) \leq f(\beta)$ (here α_i and β_i are ith bits of α and β, respectively). A function is called *unate* if it is similar to some monotone function.

A function h is a *projection* of another function f if h can be obtained from f by substituting constants for some $k \geq 0$ input variables. The projection

obtained from f by substituting σ for x_i is denoted $f_\sigma^{x_i}$. A variable x_i is called *relevant* to f if $f_0^{x_i} \not\equiv f_1^{x_i}$, that is, if these two projections disagree on at least one input string. The function f is then said to *depend* on the variable x_i.

We shall usually write input strings as $\alpha = (\alpha_1 \dots \alpha_n)$, where $\alpha_i \in \{0,1\}$, but sometimes use comma to denote concatenation, as in $f(x_1, \dots, x_n)$ and $g(x_1, \beta)$, where $x_i \in \{0,1\}$ and $\beta \in \{0,1\}^{n-1}$. We write $\mathbf{0}$ and $\mathbf{1}$ to denote strings $(0 \dots 0)$ and $(1 \dots 1)$, respectively, and $\mathbf{e}_i$ to denote the string with all 0s and a unique 1 in the ith position. The length of the string is in these cases understood from the context.

The sign $\oplus$ denotes the binary sum modulo two function (parity, XOR). When applied to strings, the sum is calculated componentwise. Boolean conjunction is denoted by the & sign and by juxtaposition.

3 Certificates for the standard basis

In this section we consider read-many functions over the standard basis $B_0 = \{\&, \vee, \neg\}$. Our goal is to prove the following theorem.

Theorem 1. *Suppose that f is a read-many function over B_0. Then it holds that*

$$M_{B_0}(f) = \begin{cases} 6 & \text{if } f \text{ is unate, and} \\ 4 & \text{if } f \text{ is not unate.} \end{cases}$$

Corollary. *$M_{B_0}(2) = 4$, and $M_{B_0}(n) = 6$ for $n \geq 3$.*

Proof (of Corollary). All one-variable functions are read-once, and neither of the two two-variable read-many functions is unate. □

Notice that the statement of Theorem 1 provides both upper and lower bounds on $M_{B_0}(f)$. We first turn our attention to the upper bounds. We shall indicate two possible ways to prove them. First, one can use Stetsenko's theorem [16], which gives the list of all *minimal* read-many functions over B_0. More precisely, by this theorem, every read-many function over B_0 has a projection similar to one of the following functions (we shall use this list further in the text):

$$\begin{aligned}
h_{\mathsf{t}}^{(s)} &= x_1 \dots x_s \vee \overline{x}_1 \dots \overline{x}_s, && s \geq 2, \\
h_{\mathsf{d}}^{(s)} &= x_1(x_2 \vee x_3 \dots x_s) \vee x_2\overline{x}_3 \dots \overline{x}_s, && s \geq 3, \\
h_{\mathsf{m}}^{(s)} &= x_1(x_2 \vee \dots \vee x_s) \vee x_2 \dots x_s, && s \geq 3, \\
h_4 &= x_1(x_2 \vee x_3) \vee x_3x_4, \\
h_5 &= x_1(x_3x_4 \vee x_5) \vee x_2(x_3 \vee x_4x_5).
\end{aligned}$$

As a result, once this fact is known, one only needs to check that all listed functions have certificates of the specified length.

However, it is worth remarking that the second way to prove the upper bounds of our Theorem 1 seems more rewarding. We shall prove two lemmas

providing us with the general form of certificates of non-membership for read-many functions over B_0. It turns out that the proof of Stetsenko's theorem itself can be based on these constructions, since in fact they give an alternative characterization of read-once functions over B_0. This new proof appears to be significantly shorter than the original proof from [16]; so far this topic has only been sketched in print [23] (the statement equivalent to Lemma 1 also appeared there without proof), but its full discussion is beyond the scope of this paper as well.

Lemma 1 (see also [10,5]). *Every non-unate function $f(x_1, \ldots, x_n)$ is similar to an extension of some partial function g defined by*

$$\begin{aligned} g(x_1, \alpha) &= x_1, \qquad x_1 \in \{0, 1\}, \\ g(x_1, \beta) &= \overline{x}_1, \qquad x_1 \in \{0, 1\}, \end{aligned}$$

where α, β are some fixed $(n-1)$-bit strings.

Proof. We shall prove the contrapositive. Assume that for each variable x_i, the function f either does not have a projection equal to x_i, or does not have a projection equal to $\overline{x}_i$. Then by inverting some of the input variables one can transform the function f into a function without projections of the form $\overline{x}_i$ for all $i = 1, \ldots, n$. Since all such functions are monotone, it follows that f is unate. □

Lemma 2. *Every unate read-many function $f(x_1, \ldots, x_n)$ over B_0 is similar to an extension of some partial function g defined by*

$$\begin{aligned} g(x_1, x_2, \alpha) &= x_1 \,\&\, x_2, \qquad (x_1, x_2) \neq (0, 0), \\ g(x_1, x_2, \beta) &= x_1 \vee x_2, \qquad (x_1, x_2) \neq (1, 1), \end{aligned}$$

where α, β are some fixed $(n-2)$-bit strings.

Proof. Assume without loss of generality that f is monotone. By Subbotovskaya's theorem [17], a Boolean function is read-many over B_0 if and only if it has a projection h with a *special* variable x_i. A variable x_i relevant to h is called special if, first, h depends on at least one other variable and, second, both projections $h_0^{x_i}$ and $h_1^{x_i}$ depend on all variables relevant to h except for x_i. Take this pair of projections $h_0^{x_i}$, $h_1^{x_i}$ and note that they can be assumed read-once over B_0. (In other words, h can be assumed to be *minimal*: if either of $h_0^{x_i}$ and $h_1^{x_i}$ is read-many, then Subbotovskaya's theorem can be used to find another projection with fewer relevant variables.)

Now observe that $h_0^{x_i} \not\equiv h_1^{x_i}$, i. e., these two projections cannot agree on all input strings, otherwise the variable x_i would not be relevant to h. Both $h_0^{x_i}$ and $h_1^{x_i}$ are non-constant (by the definition of a special variable) and monotone (since f is assumed to be monotone), so they can be represented by trees T_0 and T_1 with layers of arbitrary-fan-in non-leaf nodes labeled by alternating & and $\vee$. Leaves of each tree are labeled with (the same set of) input variables without repetitions.

It has long been known (see, e. g., the paper of Corneil, Lerchs and Stewart Burlingham [4]) that there exists a one-to-one correspondence between the set of all trees with these properties (*cotrees*, with 0 and 1 replaced by & and $\vee$) and the set of undirected graphs without induced simple paths on four vertices (*cographs*). The vertices of these graphs correspond to leaves of the trees; x_j and x_k are adjacent in the graph if and only if their least common ancestor in the tree is labeled by $\vee$.

Since $h_0^{x_i} \not\equiv h_1^{x_i}$, these two trees are different, and so are their graphs. It follows that there exists a pair of variables x_j, x_k relevant to both projections such that the least common ancestors of x_j and x_k in these two trees are labeled by different symbols. It follows that one of these projections, $h_0^{x_i}$ or $h_1^{x_i}$, has a subprojection $x_j \& x_k$, and the other one a subprojection $x_j \vee x_k$ (a *subprojection* is, naturally, a projection of a projection). It remains to recall that h itself is a projection of f and permute the variables appropriately to obtain the statement of the lemma. □

Now observe that an arbitrary function f is read-once if and only if it has no certificate of size 4 or 6 that constitutes the domain of some partial function g satisfying the conditions of Lemma 1 or 2, respectively. Indeed, by De Morgan's laws all read-once functions over B_0 are unate, and the certificate of size 4 guarantees that the function is non-unate. Similary, one can use the tree representation of read-once functions to demonstrate that none of them can have both projections $x_1 \& x_2$ and $x_1 \vee x_2$, nor a projection of the form $x_1 \oplus x_2 \oplus c$, for $c \in \{0, 1\}$, which is exactly what a certificate of size 6 provides. Thus the upper bounds of Theorem 1 have been proved.

Let us now turn to the proof of the lower bounds. Again, we distinguish between two cases here.

Lemma 3. *Any partial function g with fewer than 4 strings in its domain has a read-once extension over B_0.*

Proof. Let the domain of g contain exactly 3 strings. Assume without loss of generality that g takes on the value 0 more often than the value 1. If g does not take on the value 1 at all, then the constant function 0 is a read-once extension of g. Otherwise g takes on the value 1 on a single string $\alpha = (\alpha_1 \dots \alpha_n)$, and in this case the function $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ is a read-once extension of g. □

Lemma 4. *If a partial function g with fewer than 6 strings in its domain has a unate extension, then it has a read-once extension over B_0.*

Proof. Let the domain of g contain exactly 5 strings, and assume without loss of generality that g takes on the value 0 more often than the value 1. Now suppose that g has a monotone extension. (If it does not, then it is similar to some function which does, and these two functions either both have or both do not have read-once extensions.) If g does not take on the value 1 at all, then it has a read-once extension 0. If it takes on the value 1 on a single string $\alpha = (\alpha_1 \dots \alpha_n)$, then one of its extensions is the read-once function $f = x_{i_1} \dots x_{i_k}$,

where $\{i_1, \ldots, i_k\} = \{i \mid \alpha_i = 1\}$. Indeed, if for some $\gamma \in \{0,1\}^n$ it holds that $g(\gamma) = 0$ and $f(\gamma) = 1$, then $\alpha \leq \gamma$ (i. e., $\alpha_i \leq \gamma_i$ for all $i = 1, \ldots, n$) and $1 = g(\alpha) > g(\gamma) = 0$. This means that g has no monotone extensions, which contradicts our initial assumption. Finally, if the function g takes on the value 1 on two input strings α and β, then it can be similarly shown to have the extension $x_{i_1} \ldots x_{i_k} \vee x_{j_1} \ldots x_{j_m}$, where $\{i_1, \ldots, i_k\} = \{i \mid \alpha_i = 1\}$ and $\{j_1, \ldots, j_m\} = \{j \mid \beta_j = 1\}$. This function is read-once by the distributivity of conjunction over disjunction. □

Now the lower bounds of Theorem 1 follow from Lemmas 3 and 4. This concludes the proof of Theorem 1.

4 Certificates for extended bases

In this section we consider bases $B^{(s)} = B_0 \cup \{h_{\mathrm{t}}^{(s)}\}$, $s \geq 2$, with $h_{\mathrm{t}}^{(s)} = x_1 \ldots x_s \vee \overline{x}_1 \ldots \overline{x}_s$ as defined in the previous section. We first show that the values $M_{B^{(s)}}(n)$ grow as $n \to \infty$, in contrast to the fact that $M_{B_0}(n) = \Theta(1)$.

Theorem 2. *Suppose that $s \geq 2$ is fixed. Assume that $n = ms$, where $m \geq 2$, and let $n \to \infty$ (thus $m \to \infty$). Then the following inequality holds:*

$$M_{B^{(s)}}\left(h_{\mathrm{t}}^{(n)}\right) \geq \binom{n-1}{s-1} = \Omega(n^{s-1}).$$

Proof. Consider the family of read-once functions obtained by permuting the variables of the function $\bigwedge_{i=1}^{m} h_{\mathrm{t}}^{(s)}(x_{(i-1)s+1}, \ldots, x_{is})$. Any certificate of non-membership for $h_{\mathrm{t}}^{(n)}$ with respect to the class $\mathrm{ROF}[B^{(s)}]$ must contain enough strings to distinguish $h_{\mathrm{t}}^{(n)}$ from all functions in this family. Note that these functions agree with $h_{\mathrm{t}}^{(n)}$ on all-zero and all-one strings $\mathbf{0}$ and $\mathbf{1}$, and also on strings containing k ones if s does not divide k. So take any string α with $k = ls$ ones, $0 < l < m$.

Since $h_{\mathrm{t}}^{(n)}(\alpha) = 0$, this α, when included in a certificate, can be thought of as eliminating all read-once alternatives g with $g(\alpha) = 1$. How many such alternatives are there in the family defined above? This number is equal to the number of partitions of the set of k positions with 1s into l subsets of size s, multiplied by the number of partitions of the set of $(n-k)$ positions with 0s into $(m-l)$ subsets of size s. In other words, this number is equal to

$$N_l = \frac{(ls)!}{(s!)^l \cdot l!} \cdot \frac{((m-l)s)!}{(s!)^{m-l} \cdot (m-l)!} = \frac{(ls)! \cdot ((m-l)s)!}{(s!)^m \cdot m!} \cdot \binom{m}{l}.$$

Consider the fraction

$$\frac{N_l}{N_{l-1}} = \frac{(ls)_s \cdot (m-l+1)}{((m-l+1)s)_s \cdot l} = \frac{(ls-1)_{s-1}}{((m-l+1)s-1)_{s-1}},$$

where parentheses with subscript denote falling factorials: $(a)_b = a(a-1)\ldots(a-b+1)$. Observe that this fraction is greater than 1 if and only if $l > m - l + 1$,

that is, if $l > (m+1)/2$. It follows that N_l is largest when $l = 1$ or $l = m-1$. In other words, every string in a certificate eliminates at most

$$N_1 = \frac{s! \cdot ((m-1)s)!}{(s!)^m \cdot m!} \cdot \binom{m}{1} = \frac{n!}{\binom{n}{s} \cdot (s!)^m \cdot (m-1)!}$$

alternatives from the family above.

Now let us count the cardinality of the family itself. This cardinality is equal to the number of partitions of an n-sized set into subsets of size s, i. e., to $F = n!/((s!)^m m!)$. It follows that the size of a certificate cannot be less than $F/N_1 = \binom{n}{s}/m = \binom{n-1}{s-1}$. □

Corollary. *$M_{B^{(s)}}(n) = \Omega(n^{s-1})$ for every fixed $s \geq 2$ as $n \to \infty$.*

We shall now prove the upper bound on $M_{B^{(2)}}(n)$, that is, for the special case $s = 2$. Note that the basis $B^{(2)}$ is sometimes called *binary* because all two-variable functions are read-once over this basis and vice versa, all functions from this basis have fan-in two. (The term "full binary basis" is usually used to refer to the entire set of all two-variable functions.)

Theorem 3. *For all $n \geq 3$ and all n-variable read-many functions f_n over $B^{(2)}$, the following inequality holds:*

$$M_{B^{(2)}}(f_n) \leq 2n + 3.$$

Corollary. *$n - 1 \leq M_{B^{(2)}}(n) \leq 2n + 3$ for $n \geq 3$.*

Note that all two-variable functions are read-once over $B^{(2)}$, hence the inequality $n \geq 3$.

We shall rely on Peryazev's theorem [13], which gives the list of forbidden projections for the class $\mathrm{ROF}[B^{(2)}]$. It says that every read-many function over $B^{(2)}$ has a projection similar to one of the functions from Stetsenko's list (excepting $h_{\mathrm{t}}^{(2)}$) or to one of the following functions:

$$\begin{aligned}
p_1 &= x_1x_2x_3 \oplus \overline{x}_2\overline{x}_3, \\
p_2 &= x_1(x_2 \vee x_3) \oplus x_2x_3, \\
p_3 &= x_1x_2x_3x_4 \oplus (x_1 \oplus \overline{x}_2)\overline{x}_3\overline{x}_4, \\
p_4 &= x_1(x_2 \vee x_3x_4) \oplus (x_3 \vee x_2x_4).
\end{aligned}$$

Remark. Since this result of Peryazev is only available in Russian, we take a short detour and briefly outline the proof from [13]. Consider any function f satisfying the following three properties: first, f is read-many over $B^{(2)}$; second, all projections of f, except for f itself, are read-once over $B^{(2)}$; third, f is not similar to any function from Stetsenko's list. The final goal is to show that any such function f is similar to one of the functions p_i, $1 \leq i \leq 4$.

The proof proceeds as follows. First of all, it follows from the second property above that for all variables x relevant to f it holds that both projections f_0^x and

f_1^x are read-once over $B^{(2)}$. If all these projections are also read-once over B_0, then, by Stetsenko's theorem, f is included in Stetsenko's list. This contradicts the third property above, so it must be the case that for some x and σ the projection f_σ^x is read-many over B_0, but read-once over $B^{(2)}$.

Further reasoning goes along the following lines. It is first shown that for the variable x chosen as above, both projections f_0^x and f_1^x depend on all variables relevant to f, except x. Second, it is deduced that exactly one of these projections is read-many over B_0, i. e., that the projection $f_{\overline{\sigma}}^x$ is necessarily read-once over B_0. At the same time it is shown that the formula expressing f_σ^x over $B^{(2)}$ can only contain exactly one occurrence of $\oplus$, i. e., of the (binary) sum modulo two. Finally, it is concluded that f can have at most 4 relevant variables. After this, it only remains to enumerate finitely many possible functions, split them into equivalence classes with respect to similarity, and choose the classes whose members satisfy the initial conditions. □

Let us return to the proof of Theorem 3, that is, to the construction of certificates of non-membership with respect to $\mathrm{ROF}[B^{(2)}]$. We take the following natural approach: for all *minimal* read-many projections (that is, functions from Peryazev and Stetsenko's lists) we explicitly construct a certificate of appropriate length. To this end, we employ several properties of read-once functions over this basis.

Let us give several auxiliary definitions. A projection of a function with exactly two relevant variables will be called a *binary projection*. We call a binary projection $h(x, y)$ *linear* if it is equal to $x \oplus y \oplus c$ for some $c \in \{0, 1\}$. All functions similar to $x \,\&\, y$ are called *nonlinear*.

Tree representations of read-once functions over $B^{(2)}$ reveal that for every such function g and every pair of its relevant variables x_i, x_j, all its binary projections of the form $h(x_i, x_j)$ are either all linear or all nonlinear, depending on the label of their least common ancestor in the tree. It follows that if a function f has binary linear and nonlinear projections for the same pair of variables, then f is read-many. We shall use this property to deal with functions from Peryazev's list.

Lemma 5. *For any function p_i from Peryazev's list there exists a certificate of non-membership with respect to $\mathrm{ROF}[B^{(2)}]$ of size at most $2n+3$, where n is the number of variables relevant to p_i.*

Proof. Functions p_1 and p_2 depend on three variables each, and the entire set $\{0, 1\}^3$ can be taken as a certificate, since $8 \leq 2 \cdot 3 + 3$. Functions p_3 and p_4 satisfy the equalities

$$p_3(x_1, x_2, 0, 0) = x_1 \oplus x_2 \oplus 1, \qquad p_4(1, x_2, x_3, 0) = x_2 \oplus x_3,$$
$$p_3(x_1, x_2, 1, 1) = x_1 x_2, \qquad p_4(0, x_2, x_3, 1) = x_2 \vee x_3,$$

which prove that each of them is read-many using $8 \leq 2 \cdot 4 + 3$ input strings. □

For infinite sequences of functions from Stetsenko's list (that is, for functions $h_{\mathsf{t}}^{(s)}$, $h_{\mathsf{d}}^{(s)}$, $h_{\mathsf{m}}^{(s)}$, $m \geq 3$), we develop a more refined technique. Let us call a variable

x_i of a function g *ambivalent* if for some x_j, $j \neq i$, the function g has two nonlinear binary projections $g'(x_i, x_j)$ and $g''(x_i, x_j)$ such that $g'(0, x_j) = \text{const}$ and $g''(1, x_j) = \text{const}$.

Lemma 6. *For every ambivalent variable x_i of a read-once function g there exists a* witness*—some variable x_k, $k \neq i$, such that g has a linear binary projection $x_i \oplus x_k \oplus c$.*

Proof. Let the variable x_i of g satisfy the definition of ambivalence with x_j. Consider some tree of g and let the least common ancestor w of x_i and x_j be labeled by a function h. Since g has binary nonlinear projections that depend on x_i, x_j, this h must belong to the set $\{\&, \vee\}$. Assume, for instance, that h is binary disjunction. Then all binary projections that depend on these two variables have the form $(x_i^\sigma \vee x_j^\tau)^\delta$, where $\sigma, \tau, \delta \in \{0, 1\}$.

Observe that if there exist projections $g'(x_i, x_j)$ and $g''(x_i, x_j)$ such that $g'(0, x_j) = \text{const}$ and $g''(1, x_j) = \text{const}$, then the values of σ for these projections should be different (indeed, it is exactly the value of σ that determines the unique $c \in \{0, 1\}$ that, when substituted for x_i, turns the projection into a constant function). This means that the largest subtree containing x_i but not x_j represents a read-once function that has both projections x_i and $\overline{x}_i$.

It remains to remark that this is only possible when there exists a variable x_k in this subtree such that the least common ancestor of x_i and x_k is labeled by $\oplus$. If this is not the case, then all nodes on the path from x_i to w are labeled with symbols from $\{\&, \vee, \neg\}$. It is then readily seen that every function represented by a subtree of this form can only have one of the projections x_i and $\overline{x}_i$, but not both. □

Now we can use Lemma 6 to find short certificates for functions from Stetsenko's list.

Lemma 7. *For each of the functions $h_{\mathsf{t}}^{(s)}$, $h_{\mathsf{d}}^{(s)}$, $h_{\mathsf{m}}^{(s)}$, $s \geq 3$, from Stetsenko's list, there exists a certificate of non-membership with respect to* $\mathrm{ROF}[B^{(2)}]$ *of size at most $2s + 3$.*

Proof. As earlier, if $s = 3$, then the entire set $\{0, 1\}^3$ can be taken as a certificate, because $8 \leq 2 \cdot 3 + 3$. So assume that $s \geq 4$.

First consider some function $h_{\mathsf{t}}^{(s)}$. We claim that the set

$$\{\mathbf{1},\ \mathbf{1} \oplus \mathbf{e}_1,\ \mathbf{1} \oplus \mathbf{e}_2\} \cup \{\mathbf{e}_i \mid i = 1, \ldots, s\} \cup \{\mathbf{e}_1 \oplus \mathbf{e}_i \mid i = 1, \ldots, s\}$$

containing exactly $2s + 3$ strings is a certificate of non-membership with respect to $\mathrm{ROF}[B^{(2)}]$. Indeed, strings from this set with at most two ones reveal (that the function has) projections $h_{\mathsf{t}}^{(s)}(x_1, \mathbf{0}, x_i, \mathbf{0}) = \overline{x}_1 \,\&\, \overline{x}_i$ for $i = 2, \ldots, n$. In a similar fashion, strings (from this set) with at most two zeros reveal that the projection $h_{\mathsf{t}}^{(s)}(x_1, x_2, \mathbf{1})$ is equal to either $x_1 \,\&\, x_2$ or $x_1 \oplus x_2 \oplus 1$, depending on the value on the string $\mathbf{1} \oplus \mathbf{e}_1 \oplus \mathbf{e}_2$. In the latter case there are both linear and nonlinear projections for x_1 and x_2, and in the former case the variable x_1 is

ambivalent. Lemma 6 then requires the existence of another variable x_k with a linear projection $x_1 \oplus x_k$, but this is also impossible, since for all pairs x_1, x_i, $i \geq 2$, nonlinear projections exist.

Now consider a function $h_{\mathsf{d}}^{(s)}$. Here we claim that the set

$$\{\mathbf{e}_2,\ \mathbf{e}_2{\oplus}\mathbf{e}_3,\ \mathbf{e}_2{\oplus}\mathbf{e}_4\} \cup \{\mathbf{1}{\oplus}\mathbf{e}_2{\oplus}\mathbf{e}_i \mid i = 1,\ldots,s\} \cup \{\mathbf{1}{\oplus}\mathbf{e}_2{\oplus}\mathbf{e}_3{\oplus}\mathbf{e}_i \mid i = 1,\ldots,s\}$$

containing exactly $2s+3$ strings is a desired certificate. Indeed, the values of $h_{\mathsf{d}}^{(s)}$ on the strings with at most three zeros reveal the projections $h_{\mathsf{d}}^{(s)}(1,0,x_3,\mathbf{1},x_i,\mathbf{1}) = x_3 \,\&\, x_i$ for $4 \leq i \leq s$, $h_{\mathsf{d}}^{(s)}(1,x_2,x_3,\mathbf{1}) = x_2 \vee x_3$, and $h_{\mathsf{d}}^{(s)}(x_1,0,x_3,\mathbf{1}) = x_1 \,\&\, x_3$. If the value on the string $\mathbf{e}_2 \oplus \mathbf{e}_3 \oplus \mathbf{e}_4$ is equal to 1, then the projection $h_{\mathsf{d}}^{(s)}(0,1,x_3,x_4,\mathbf{0})$ is equal to $x_3 \oplus x_4 \oplus 1$ and is thus linear, which contradicts the existence of a nonlinear projection on the same variables. If the value is equal to 0, then the projection is equal to $\overline{x}_3 \,\&\, \overline{x}_4$. In this case the variable x_3 is ambivalent but does not have a appropriate witness required by Lemma 6, which is also a contradiction.

Finally, consider a function $h_{\mathsf{m}}^{(s)}$. Here the certificate we construct is

$$\{\mathbf{1}{\oplus}\mathbf{e}_1,\ \mathbf{1}{\oplus}\mathbf{e}_1{\oplus}\mathbf{e}_2,\ \mathbf{1}{\oplus}\mathbf{e}_1{\oplus}\mathbf{e}_3\} \cup \{\mathbf{e}_1{\oplus}\mathbf{e}_i \mid i = 1,\ldots,s\} \cup \{\mathbf{e}_1{\oplus}\mathbf{e}_2{\oplus}\mathbf{e}_i \mid i = 1,\ldots,s\}.$$

Here the values on the strings from the second and the third subsets reveal the projections $h_{\mathsf{m}}^{(s)}(1,x_2,\mathbf{0},x_i,\mathbf{0}) = x_2 \vee x_i$ for $3 \leq i \leq s$ and $h_{\mathsf{m}}^{(s)}(x_1,x_2,\mathbf{0}) = x_1 \& x_2$. If the value on the string $\mathbf{1}{\oplus}\mathbf{e}_1{\oplus}\mathbf{e}_2{\oplus}\mathbf{e}_3$ is equal to 1, then the projection $h_{\mathsf{m}}^{(s)}(0,x_2,x_3,\mathbf{1})$ is equal to $x_2{\oplus}x_3{\oplus}1$ and is thus linear, which is a contradiction. If the value is equal to 0, then the projection is equal to $x_2 \& x_3$ and the variable x_2 is ambivalent. Here we arrive at a contradiction with Lemma 6, because, as earlier, no witness for x_2 is possible. This completes the proof of Lemma 7. □

For the two remaining functions we employ a different argument, although one strongly related to that of Lemma 6.

Lemma 8. *Suppose that a read-once function g over $B^{(2)}$ has projections $x_i \& x_j$ and $x_i \vee x_j$. Then every tree of g has at least three nodes labeled with $\oplus$: two on the paths from the corresponding leaves to their least common ancestor w, and one on the path from w to the root of the tree.*

Proof. The statement of Lemma 6 reveals that two nodes labeled with $\oplus$ must be present in the tree of g, and the argument employed in the proof confirms that they lie on the paths from x_i and x_j to w. However, an even stronger statement can be deduced. Indeed, in terms of the proof of Lemma 6, obtaining projections of the form $x_i \& x_j$ and $x_i \vee x_j$ can be thought of as finding appropriate Boolean constants to substitute for σ, τ and δ in $(x_i^\sigma \vee x_j^\tau)^\delta$ (again, nothing changes if w is labeled with &). One can see that the only appropriate substitutions are $\sigma = \tau = \delta = 1$ and $\sigma = \tau = \delta = 0$.

Now replace the subtree rooted at w with a single leaf x_0 and observe that the function represented by the obtained tree should have both projections x_0 and $\overline{x}_0$. Similarly to the proof of Lemma 6, one of the nodes on the path from x_0 to the root should be labeled with $\oplus$. □

Remark. The statement of Lemma 8 remains true if $x_i \,\&\, x_j$ and $x_i \vee x_j$ are replaced with any pair of nonlinear functions h' and h'' that depend only on x_i, x_j and are *dual* in the sense that $\overline{h}'(\overline{x}_i, \overline{x}_j) = h''(x_i, x_j)$.

Lemma 9. *For each of the functions h_4 and h_5 from Stetsenko's list there exists a certificate of non-membership with respect to* $\mathrm{ROF}[B^{(2)}]$ *of size at most $2n+3$, where n is the number of variables relevant to h_i.*

Proof. We construct a certificate for either function using the following trick. We give a proof (by contradiction) that the function is read-many, keeping track of input strings we use in our argument. It will then follow that the set of all used strings is a certificate of non-membership with respect to $\mathrm{ROF}[B^{(2)}]$, because the values of the function on the strings from this set are sufficient to prove that the function is outside $\mathrm{ROF}[B^{(2)}]$.

First consider the function h_4 and suppose for the sake of contradiction that it is read-once. Observe that it has projections $h_4(x_1, 0, x_3, 0) = x_1 \,\&\, x_3$ and $h_4(x_1, 1, x_3, 1) = x_1 \vee x_3$. Lemma 8 reveals that at least three nodes labeled with $\oplus$ should be present in the tree, apart from the least common ancestor of x_1 and x_3 labeled with a nonlinear function. However, this is impossible, since the number of leaves of such a tree should be at least 5, whereas they are all labeled with variables from $\{x_1, x_2, x_3, x_4\}$ without repetitions. This contradiction gives a certificate of size $8 \leq 2 \cdot 4 + 3$.

Now consider the function h_5, which has projections $h_5(x_1, 0, x_3, 1, 0) = x_1 \,\&\, x_3$ and $h_5(x_1, 1, x_3, 0, 1) = x_1 \vee x_3$. If it were read-once, then by Lemma 8, it would be expressed by $((x_1 \oplus x_i^\sigma) \vee (x_3 \oplus x_j^\tau)) \oplus x_k^\delta$ with $\{i, j, k\} = \{2, 4, 5\}$. Therefore, all binary projections that depend on pairs of variables x_i, x_k and x_j, x_k are linear. However, $h_5(0, x_2, 0, x_4, 1) = x_2 \,\&\, x_4$ and $h_5(1, 0, 1, x_4, x_5) = x_4 \vee x_5$, which is a contradiction.

If we now count the number of strings we have used to certify this contradiction, we find out that it is equal to 14, while $2 \cdot 5 + 3 = 13$. We argue that the string (11101) is not really needed. Indeed, we have only used it once to reveal the projection $x_1 \vee x_3$. However, if the value on (11101) is not known, then there are two options. If this value is 1, then our original argument holds. Otherwise, if the value is 0, then our function would have a projection $x_1 \oplus x_3$, which is also impossible, because then both linear and nonlinear projections exist for x_1 and x_3. This concludes the proof of Lemma 9. □

Theorem 3 follows from Lemmas 5, 7 and 9.

5 Conclusions and open problems

We have studied the size of optimal certificates of non-membership with respect to several classes of read-once functions. For the standard basis $B_0 = \{\&, \vee, \neg\}$, we have determined the exact value of $M_{B_0}(f)$ for all read-many functions f and deduced that $M_{B_0}(n) = \Theta(1)$. For the bases $B^{(s)} = B_0 \cup \{h_{\mathrm{t}}^{(s)}\}$, we have shown

that $M_{B^{(s)}}(n) = \Omega(n^{s-1})$. For the special case $s = 2$ (i. e., for the binary basis) we obtained a matching upper bound, thus establishing that $M_{B^{(2)}}(n) = \Theta(n)$.

Combined with the theorem of Hegedűs [8] stated in section 2, our results imply the following upper bounds on the complexity of learning read-once functions with membership and equivalence queries (the goal of learning is exact identification of an unknown read-once function of n variables). For the basis B_0 there exists a learning algorithm performing $O(n \log n)$ queries, and for the basis $B^{(2)}$ a learning algorithm performing $O(n^2)$ queries. This is an improvement upon the previously known results: the algorithm of Angluin, Hellerstein, and Karpinski [2] for the basis B_0 makes $O(n)$ equivalence and $O(n^3)$ membership queries, and the algorithm of Bshouty, Hancock, and Hellerstein [3] for the basis $B^{(2)}$ makes $O(n)$ equivalence and $O(n^4)$ membership queries.

We want to make two remarks here concerning the algorithms given by Hegedűs's theorem. First, it is important to note that these algorithms only achieve polynomial-query learnability and do not necessarily terminate in polynomial time. In fact, they build upon the majority vote (halving) approach and compute the pointwise majority of all "alive" hypotheses multiple times, which, in principle, may require superpolynomial and even superexponential time, in terms of n. Second, to deduce the upper bounds on the query complexity of these algorithms, one uses the inequality given in section 2 above. The needed values are, for these bases B, the worst-case size of a certificate of non-membership, which we denoted $M_B(n)$, and the number of read-once functions over B. For the latter, asymptotic formulas of the form $c\,\alpha^n\, n^{n-O(1)}$ are known for some constants c and α (the formula for the basis B_0 can be found in [14] and the formula for the basis $B^{(2)}$ in [20]), so both for the basis B_0 and for the basis $B^{(2)}$ the logarithm of the number of read-onde functions is $O(n \log n)$.

Returning to certificates of non-membership, we are interested in resolving the following open problem: does it hold that $M_B(n) \to \infty$ as $n \to \infty$ for all bases of the form $B_0 \cup \{h\}$, where h is a function from Stetsenko's list? Recent findings [21] show that this is true at least for the non-unate functions h: more precisely, $M_B(n) = \Theta(n)$ for $B = B_0 \cup \{h_{\mathsf{d}}^{(s)}\}$. Natural candidates for $M_B(n) = O(1)$ correspond to the "separate" functions h_4 and h_5. Similar questions also arise if all functions in B are monotone (for instance, if $B = \{\&, \vee, h_{\mathsf{m}}^{(3)}\}$, where $h_{\mathsf{m}}^{(3)}$ is the majority function on three inputs).

Acknowledgements. We are grateful to Dmitry Konstantinov for useful discussions on an early draft of this paper. This research was supported by Russian Presidential grant MD–757.2011.9.

References

1. M. Arias, R. Khardon, R. A. Servedio. Polynomial certificates for propositional classes. *Information and Computation* 204(5), 816–834 (2006)
2. D. Angluin, L. Hellerstein, M. Karpinski. Learning read-once formulas with queries. *Journal of the ACM* 40, 185–210 (1993)

3. N. H. Bshouty, T. R. Hancock, L. Hellerstein. Learning Boolean read-once formulas over generalized bases. *Journal of Computer and System Sciences* 50(3), 521–542 (1995)
4. D. G. Corneil, H. Lerchs, L. Stewart Burlingham. Complement reducible graphs. *Discrete Applied Mathematics* 3(3), 163–174 (1981)
5. A. Feigelson, L. Hellerstein. The forbidden projections of unate functions. *Discrete Applied Mathematics* 77(3), 221–236 (1997)
6. M. C. Golumbic, V. Gurvich. Read-once functions (book chapter). In: Y. Crama, P. L. Hammer, Boolean Functions: Theory, Algorithms and Applications. Encyclopedia of Mathematics and Its Applications, vol. 142. Cambridge University Press (2011)
7. V. Gurvich. On the normal form of positional games. *Soviet Mathematics Doklady* 25(3), 572–575 (1982)
8. T. Hegedűs. Generalized teaching dimensions and the query complexity of learning. In: Proceedings of COLT 1995, pp. 108–117 (1995)
9. P. Heggernes, D. Kratsch. Linear-time certifying recognition algorithms and forbidden induced subgraphs. *Nordic Journal of Computing* 14, 87–108 (2007)
10. L. Hellerstein. On generalized constraints and certificates. *Discrete Mathematics* 226, 211–232 (2001)
11. L. Hellerstein, K. Pillaipakkamnatt, V. Raghavan, D. Wilkins. How many queries are needed to learn? *Journal of the ACM* 43(5), 840–862 (1996)
12. R. M. McConnell, K. Mehlhorn, S. Näher, P. Schweitzer. Certifying algorithms. *Computer Science Review* 5(2), 119–161 (2011)
13. N. A. Peryazev. Weakly read-many functions over the binary basis. Diskretnaya Matematika i Informatika, vol. 4. Izdatel'stvo Irkutskogo universiteta (1998) (in Russian)
14. P. Savický, A. R. Woods. The number of Boolean functions computed by formulas of a given size. *Random Structures and Algorithms* 13(3–4), 349–382 (1998)
15. P. Sen, A. Deshpande, L. Getoor. Read-once functions and query evaluation in probabilistic databases. *Proceedings of the VLDB Endowment* 3(1–2), 1068–1079 (2010)
16. V. A. Stetsenko. On almost bad Boolean bases. *Theoretical Computer Science* 136(2), 419–469 (1994)
17. B. A. Subbotovskaya. Comparison of bases in the realization by formulas of functions of the algebra of logic. *Soviet Mathematics Doklady* 4, 478–481 (1963)
18. R. Thomas. Recent excluded minor theorems for graphs. In: Surveys in combinatorics, London Mathematical Society Lecture Note Series 267, pp. 201–222 (1999)
19. L. G. Valiant. A theory of the learnable. *Communications of the ACM* 27, 1134–1142 (1984)
20. V. A. Voblyi. The asymptotics of the number of repetition-free Boolean functions in the basis B_1. *Discrete Mathematics and Applications* 20(5–6), 707–708 (2011)
21. A. A. Voronenko. On the Shannon function for read-many certificate length in one base family. *Moscow University Computational Mathematics and Cybernetics*, **37**(4), 2013, 202–204.
22. A. A. Voronenko. On the complexity of proving that a Boolean function is not binary read-once. *Prikladnaya Diskretnaya Matematika* 13, 12–16 (2011) (in Russian)
23. A. A. Voronenko, V. S. Fedorova, D. V. Chistikov. Iterated Boolean functions in the elementary basis. *Russian Mathematics* (*Iz. VUZ*) 55(11), 61–65 (2011)