Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 396 (2008) 71–87
Theoretical Computer Science
www.elsevier.com/locate/tcs

On a quasi-ordering on Boolean functions

Miguel Couceiro[a,b,*], Maurice Pouzet[c]

[a] *Department of Mathematics and Statistics, University of Tampere, Kanslerinrinne 1, 33014 Tampere, Finland*
[b] *Department of Philosophy, University of Tampere, Kanslerinrinne 1, 33014 Tampere, Finland*
[c] *ICJ, Department of Mathematics, Université Claude-Bernard Lyon1, 43 Bd 11 Novembre 1918, 68622 Villeurbanne Cedex, France*

Received 28 April 2006; received in revised form 16 October 2007; accepted 25 January 2008

Communicated by A.K. Salomaa

Abstract

It was proved few years ago that classes of Boolean functions definable by means of functional equations [O. Ekin, S. Foldes, P.L. Hammer, L. Hellerstein, Equational characterizations of boolean functions classes, Discrete Mathematics 211 (2000) 27–51], or equivalently, by means of relational constraints [N. Pippenger. Galois theory for minors of finite functions, Discrete Mathematics 254 (2002) 405–419], coincide with initial segments of the quasi-ordered set $(\Omega, \leq)$ made of the set Ω of Boolean functions, suitably quasi-ordered. Furthermore, the classes defined by finitely many equations [O. Ekin, S. Foldes, P.L. Hammer, L. Hellerstein, Equational characterizations of boolean functions classes, Discrete Mathematics 211 (2000) 27–51] coincide with the initial segments of $(\Omega, \leq)$ which are definable by finitely many obstructions. The resulting ordered set $(\tilde{\Omega}, \sqsubseteq)$ embeds into $([\omega]^{<\omega}, \subseteq)$, the set – ordered by inclusion – of finite subsets of the set ω of integers. We prove that $(\tilde{\Omega}, \sqsubseteq)$ also embeds $([\omega]^{<\omega}, \subseteq)$. From this result, we deduce that the dual space of the distributive lattice made of finitely definable classes is uncountable. Looking at examples of finitely definable classes, we show that the classes of Boolean functions with a bounded number of essential variables are finitely definable. We provide a concrete equational characterization for each of these classes, and for the subclasses made of linear functions. We describe the classes of functions with bounded polynomial degree in terms of minimal obstructions.

Keywords: Quasi-orders; Qosets; Partial-orders; Posets; Initial segments; Antichains; Order-embeddings; Boolean functions; Minors; Essential variables; Functional equations; Equational classes; Relational constraints; Linear functions

1. Introduction

Two approaches of Boolean definability have been considered recently. One in terms of functional equations [10], and the other in terms of relational constraints [17]. It turns out that these two approaches define the same classes of Boolean functions. These classes have been completely described by means of a quasi-order on the set Ω of all Boolean functions. The quasi-order is the following: for two functions $f, g \in \Omega$ set $g \leq f$ if g can be obtained

* Corresponding address: Department of Mathematics, University of Luxembourg, 162a, avenue de la Faïencerie, L-1511 Luxembourg, Luxembourg. Tel.: +352 691791966.
E-mail addresses: Miguel.Couceiro@uta.fi, miguel.couceiro@uni.lu (M. Couceiro), pouzet@univ-lyon1.fr (M. Pouzet).

0304-3975/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2008.01.025

from f by identifying or permuting variables, or adding dummy variables. These classes coincide with the initial segments for this quasi-ordering called *identification minor* in [10], *minor* in [17], *subfunction* in [21], and *simple variable substitution* in [4]. Since then, greater emphasis on this quasi-ordering has emerged. For an example, it was observed that Ω is the union of four blocks with no comparabilities in between, each block made of the elements above a minimal element. It is well known that Ω contains infinite antichains (see e.g. [12,10,17,11]). A complete classification of pairs C_1, C_2 of particular initial segments ("clones") for which $C_2 \setminus C_1$ contains no infinite antichains was given in [3]. Our paper is a contribution to the understanding of this quasi-ordering.

Some properties are easier to express in terms of the poset $(\tilde{\Omega}, \sqsubseteq)$ associated with the quasi-ordered set $(\Omega, \leq)$ and made of the equivalence classes associated with the equivalence $\simeq$ defined by $f \simeq g$ if $f \leq g$ and $g \leq f$. As we will see (Corollary 1), for each $x \in \tilde{\Omega}$, the initial segment $\downarrow x := \{y \in \tilde{\Omega} : y \sqsubseteq x\}$ is finite, hence, $(\tilde{\Omega}, \sqsubseteq)$ decomposes into the levels $\tilde{\Omega}_0, \ldots, \tilde{\Omega}_n, \ldots$, where $\tilde{\Omega}_n$ is the set of minimal elements of $\tilde{\Omega} \setminus \bigcup\{\tilde{\Omega}_m : m < n\}$. Moreover, each level is finite; for an example $\tilde{\Omega}_0$ is made of four elements (the equivalence classes of the two constants functions, of the identity and of the negation of the identity). This fact leads to the following:

Problem 1. How does the map $\varphi_{\tilde{\Omega}}$, which counts for every n the number $\varphi_{\tilde{\Omega}}(n)$ of elements of $\tilde{\Omega}_n$, behave?

From the fact that for each $x \in \tilde{\Omega}$, the initial segment $\downarrow x$ is finite it follows that initial segments of $(\tilde{\Omega}, \sqsubseteq)$ correspond bijectively to antichains of $(\tilde{\Omega}, \sqsubseteq)$. Indeed, for each antichain $A \subseteq \tilde{\Omega}$, the set $Forbid(A) := \{y \in \tilde{\Omega} : x \in A \Rightarrow x \not\sqsubseteq y\}$ is an initial segment of $(\tilde{\Omega}, \sqsubseteq)$. Conversely, each initial segment I of $(\tilde{\Omega}, \sqsubseteq)$ is of this form (if A is the set of minimal elements of $\tilde{\Omega} \setminus I$, then since for each $x \in \tilde{\Omega}$ the set $\downarrow x$ is finite, $I = Forbid(A)$). Viewing the elements of A as obstructions, this amounts to say that *every initial segment can be defined by a minimal set of obstructions*.

Another feature of this poset, similar in importance, is the fact that it is *up-closed*, that is for every pair $x, y \in \tilde{\Omega}$, the final segment $\uparrow x \cap \uparrow y$ is a finite union (possibly empty) of final segments of the form $\uparrow z$. This means that the collection of initial segments of the form $Forbid(A)$ where A runs through the finite antichains of $\tilde{\Omega}$ which is closed under finite intersections is also closed under finite unions.

Such initial segments have a natural interpretation in terms of Boolean functions. Indeed, as we have said, initial segments of $(\Omega, \leq)$ coincide with equational classes. Each of these initial segments identifies to an initial segment of $(\tilde{\Omega}, \sqsubseteq)$ and, as in this case, can be written as $Forbid(A)$ for some antichain A of $(\Omega, \leq)$ (the difference with an initial segment of $(\tilde{\Omega}, \sqsubseteq)$ is that the antichain A is not unique). Let us consider the set $\mathcal{F}$ of classes which can be defined by finitely many equations. They are characterized by the following theorem which appeared in [10], Proposition 4.5. For the sake of self-containment, we provide its proof at the end of Section 2.

Theorem 1. *For an initial segment I of $(\Omega, \leq)$, the following properties are equivalent:*

(i) $I \in \mathcal{F}$;
(ii) *I is definable by a single equation;*
(iii) $I = Forbid(A)$ *for some finite antichain.*

The following lemma reassembles the main properties of $\mathcal{F}$.

Lemma 1. (1) *$\mathcal{F}$ is closed under finite unions and finite intersections;*
(2) $Forbid(\{f\}) \in \mathcal{F}$ *for every* $f \in \Omega$;
(3) $\downarrow f \in \mathcal{F}$ *for every* $f \in \Omega$.

As an application of Lemma 1, and Corollary 1 mentioned above, one can easily verify that, for each positive integer k, *the class E^k of functions $f \in \Omega$ with no more than k essential variables is definable by finitely many equations*. Indeed, let $\tilde{E^k}$ be its image in $(\tilde{\Omega}, \sqsubseteq)$. As it will become clear from the proof of Corollary 1, if $ess(f) \leq k$, then $\tilde{f} \in \bigcup_{n<k} \tilde{\Omega}_n$ and hence, $\tilde{E^k} \subseteq \bigcup_{n<k} \tilde{\Omega}_n$. As mentioned, each level $\tilde{\Omega}_m$ of $(\tilde{\Omega}, \sqsubseteq)$ is finite, and thus $\tilde{E^k}$ is also finite. Since $E^k = \{\downarrow f : \tilde{f} \in \tilde{E^k}\}$, we conclude that E^k is a finite union of initial segments of the form $\downarrow f$. From Statement (1) and Statement (3) of Lemma 1, it follows that E^k is a member of $\mathcal{F}$, i.e., E^k is definable by finitely many equations. Using the basic facts from linear algebra over the 2-element field, we obtain an explicit equation defining the class E^k, for each positive integer k (see Theorem 8).

Most of the Boolean clones are finitely definable (in fact, there are only 8 clones which cannot be defined by finitely many equations, see [11]). In particular, the clone L of linear functions (w.r.t the 2-element field) belongs to $\mathcal{F}$, and

thus, for each positive integer k, the class $L^k = L \cap E^k$ of linear functions with no more than k essential variables also belongs to $\mathcal{F}$. For each positive integer k, we present an equational characterization of the class L^k of linear functions with at most k essential variables, alternative to that of E^k (see Theorem 9).

We also consider the classes D^k, $k \geq 1$, of functions which are represented by multilinear polynomials with degree less than k. We prove that each class D^k is in $\mathcal{F}$ by providing finite sets of minimal obstructions for each class D^k (see Theorem 6). Equivalent characterizations but in terms of functional equations were given in [6].

The set $\mathcal{F}$ ordered by inclusion is a bounded distributive lattice. As it is well known [9] a bounded distributive lattice T is characterized by its *Priestley space*, that is the collection of prime filters of T, the *spectrum of* T, ordered by inclusion and equipped with the topology induced by the product topology on $\mathfrak{P}(T)$. In our case, $\mathcal{F}$ is dually isomorphic to the sublattice of $\mathfrak{P}(\tilde{\Omega})$ generated by the final segments of the form $\uparrow x$ for $x \in \tilde{\Omega}$. This lattice is the *tail-lattice of* $(\tilde{\Omega}, \sqsubseteq)$. From the fact that $(\tilde{\Omega}, \sqsubseteq)$ is up-closed and has finitely many minimal elements, it follows that the Priestley space of the tail-lattice of $(\tilde{\Omega}, \sqsubseteq)$ is the set $\mathcal{J}(\tilde{\Omega}, \sqsubseteq)$ of ideals of $(\tilde{\Omega}, \sqsubseteq)$ ordered by inclusion and equipped with the topology induced by the product topology on $\mathfrak{P}(\tilde{\Omega})$ (see [1], Theorem 2.1 and Corollary 2.7). Hence we have:

Theorem 2. *The Priestley space of the lattice $\mathcal{F}$ ordered by reverse inclusion is the set $\mathcal{J}(\tilde{\Omega}, \sqsubseteq)$ of ideals of $(\tilde{\Omega}, \sqsubseteq)$ ordered by inclusion and equipped with the topology induced by the product topology on $\mathfrak{P}(\tilde{\Omega})$.*

This result asks for a description of $\mathcal{J}(\tilde{\Omega}, \sqsubseteq)$. We prove that it embeds the poset $(\mathfrak{P}(\omega), \subseteq)$, the power set of ω, ordered by inclusion.

Our proof is a by-product of an attempt to locate $(\tilde{\Omega}, \sqsubseteq)$ among posets, that we now describe. There are two well-known ways of classifying posets. One with respect to isomorphism, two posets P and Q being *isomorphic* if there is some order-isomorphism from P onto Q. The other w.r.t. equimorphism, P and Q being *equimorphic* if P is isomorphic to a subset of Q, and Q is isomorphic to a subset of P. Given a poset P, one may ask to which well-known poset P is isomorphic or, if this is too difficult, to which P is equimorphic. If P is the poset $(\tilde{\Omega}, \sqsubseteq)$, we cannot answer the first question. We answer the second.

Let $[\omega]^{<\omega}$ be the set of finite subsets of the set ω of integers. Once ordered by inclusion, this yields the poset $([\omega]^{<\omega}, \subseteq)$. This poset decomposes into levels, the nth level being made of the n-element subsets of ω. Since all its levels (but one) are infinite, it is not isomorphic to $(\tilde{\Omega}, \sqsubseteq)$. But:

Theorem 3. *$(\tilde{\Omega}, \sqsubseteq)$ is equimorphic to $([\omega]^{<\omega}, \subseteq)$.*

As it is well known and easy to see, the poset $([\omega]^{<\omega}, \subseteq)$ contains an isomorphic copy of every countable poset P such that the initial segment $\downarrow x$ is finite for every $x \in P$. Since $(\tilde{\Omega}, \sqsubseteq)$ enjoys this property, it embeds into $([\omega]^{<\omega}, \subseteq)$. The proof that $([\omega]^{<\omega}, \subseteq)$ embeds into $(\tilde{\Omega}, \sqsubseteq)$ is based on a strengthening of a construction of an infinite antichain in $(\Omega, \leq)$ given in [17].

Since $\mathcal{J}([\omega]^{<\omega}, \subseteq)$ is isomorphic to $(\mathfrak{P}(\omega), \subseteq)$, $\mathcal{J}(\tilde{\Omega}, \sqsubseteq)$ embeds $(\mathfrak{P}(\omega), \subseteq)$, proving our claim above.

This work was done while the first named author visited the Probabilities-Combinatoric-Statistic group at the Claude-Bernard University in Gerland during the fall of 2005. Some results appearing in this paper have been announced in [8].

2. Basic notions and basic results

2.1. Partially ordered sets and initial segments

A *quasi-ordered set* (qoset) is a pair $(Q, \leq)$ where Q is an arbitrary set and $\leq$ is a *quasi-order* on Q, that is, a reflexive and transitive binary relation on Q. If the quasi-order is a *partial-order*, i.e., if it is in addition antisymmetric, then this qoset is said to be a *partially-ordered set* (poset). *The equivalence $\simeq$ associated to $\leq$* is defined by $x \simeq y$ if $x \leq y$ and $y \leq x$. We denote $x < y$ the fact that $x \leq y$ and $y \not\leq x$. We denote $\tilde{x}$ the equivalence class of x and $\tilde{Q}$ the set of equivalence classes. The image of $\leq$ via the quotient map from Q into $\tilde{Q}$ (which associates $\tilde{x}$ to x) is an order, denoted $\sqsubseteq$. According to our notations, we have $x < y$ if and only if $\tilde{x} \sqsubset \tilde{y}$. Through this map, properties of qosets translate into properties of posets. The consideration of a poset rather than a qoset is then matter of convenience. Let

$(Q, \leq)$ be a qoset. A subset I of Q is an *initial segment* if it contains every $q' \in Q$ whenever $q' \leq q$ for some $q \in I$. We denote by $\downarrow X$ the initial segment *generated by* $X \subseteq Q$, that is,

$$\downarrow X = \{q' \in Q : q' \leq q \text{ for some } q \in X\}.$$

If $X := \{x\}$, we use the notation $\downarrow x$ instead of $\downarrow\{x\}$. An initial segment of the form $\downarrow x$ is *principal*. A *final segment* of $(Q, \leq)$ is an initial segment for the dual quasi-order. We denote $\uparrow X$ the final segment generated by X and use $\uparrow x$ if $X := \{x\}$. Given a subset X of Q, the set $Q \setminus \uparrow X$ is an initial segment of Q; we will rather denote it $Forbid(X)$ and refer to the members of X as *obstructions*. We denote by $I(Q, \leq)$ the poset made of the initial segments of $(Q, \leq)$ ordered by inclusion. For an example $I(Q, =) = (\mathfrak{P}(Q), \subseteq)$. An *ideal* of Q is a nonempty initial segment I of Q which is *up-directed*, this condition meaning that for every $x, y \in I$ there is some $z \in I$ such that $x, y \leq z$. We denote by $\mathcal{J}(Q, \leq)$ the poset made of the ideals of $(Q, \leq)$ ordered by inclusion.

Let $(Q, \leq)$ and $(P, \leq)$ be two posets. A map $e : Q \to P$ is an *embedding* of $(Q, \leq)$ into $(P, \leq)$ if satisfies the condition

$$q' \leq q \text{ if and only if } e(q') \leq e(q).$$

Such a map is necessarily one-to-one. If it is surjective, this is an *isomorphism* of Q onto P. For an example $\mathcal{J}([\omega]^{<\omega}, \subseteq)$ is isomorphic to $(\mathfrak{P}(\omega), \subseteq)$.

Hence an embedding of Q into P is an isomorphism of Q onto its image. The relation *Q is embeddable into P* if there is some embedding from Q into P is a quasi-order on the class of posets. Two posets which are equivalent with respect to this quasi-order, that is which embed in each other are said *equimorphic*. We note that if $(Q, \leq)$ is a qoset the quotient map from Q onto $\tilde{Q}$ induces an isomorphism from $I(Q, \leq)$ onto $I(\tilde{Q}, \sqsubseteq)$ and from $\mathcal{J}(Q, \leq)$ onto $\mathcal{J}(\tilde{Q}, \sqsubseteq)$.

A *chain*, or a *linearly ordered set*, is a poset in which all elements are pairwise comparable with respect to an order $\leq$. By an *antichain* we simply mean a set of pairwise incomparable elements.

Let $(P, \leq)$ be a poset. Denote by $Min(P)$ the subset of P made of minimal elements of P. Define inductively the sequence $(P_n)_{n\in\mathbb{N}}$ setting $P_0 := Min(P)$ and $P_n := Min(P \setminus \cup\{P_{n'} : n' < n\})$. For each integer n, the set P_n is an antichain, called a *level* of P. If P_n is nonempty, this is the *n-th level* of P. For $x \in P$, we write $h(x, P) = n$ if $x \in P_n$. Trivially, we have:

Lemma 2. *P is the union of the P_n's whenever for every $x \in P$, the initial segment $\downarrow x$ is finite.*

We will need the following result. It belongs to the folklore of the theory of ordered sets. For sake of completeness we give a proof.

Lemma 3. *A poset $(P, \leq)$ embeds into $([\omega]^{<\omega}, \subseteq)$ if and only if P is countable and for every $x \in P$, the initial segment $\downarrow x$ is finite.*

Proof. The two conditions are trivially necessary. To prove that they suffice, let $\{p_n : 1 \leq n\}$ be the set of (distinct) elements of P. Define $\varphi(x) := \{n : p_n \in \downarrow x\}$. Since each initial segment $\downarrow x$ is finite, this defines an embedding from $(P, \leq)$ into $([\omega]^{<\omega}, \subseteq)$. □

2.2. Boolean functions

Let $\mathbb{B} := \{0, 1\}$ and, for each positive integer n, let $\mathbf{n} = \{1, \ldots, n\}$. A *Boolean function* is a map $f : \mathbb{B}^n \to \mathbb{B}$, for some positive integer n called the *arity* of f. By a *class* of Boolean functions, we simply mean a set $K \subseteq \Omega$, where Ω denotes the set $\bigcup_{n\geq 1} \mathbb{B}^{\mathbb{B}^n}$ of all Boolean functions. For positive integers i and n with $i \leq n$, define the *i-th n-ary projection* e_i^n by setting $e_i^n(a_1, \ldots, a_n) := a_i$. Set $I_c := \{e_i^n : i \in \mathbf{n}\}$. These n-ary projection maps are also called *variables*, and denoted $x_1, \ldots, x_n$, where the arity is clear from the context. If f is an n-ary Boolean function and $g_1, \ldots, g_n$ are m-ary Boolean functions, then their *composition* is the m-ary Boolean function $f(g_1, \ldots, g_n)$, whose value on every $\mathbf{a} \in \mathbb{B}^m$ is $f(g_1(\mathbf{a}), \ldots, g_n(\mathbf{a}))$. This notion is naturally extended to classes $I, J \subseteq \Omega$, by defining their *composition* $I \circ J$ as the set of all composites of functions in I with functions in J, i.e.

$$I \circ J = \{f(g_1, \ldots, g_n) \mid n, m \geq 1,\ f \text{ n-ary in } I,\ g_1, \ldots, g_n \text{ m-ary in } J\}.$$

When $I = \{f\}$, we write $f \circ J$ instead of $\{f\} \circ J$. Using this terminology, a *clone* of Boolean functions is defined as a class C containing all projections and idempotent with respect to class composition, i.e., $C \circ C = C$. As an example, the class I_c made of all projections is a clone. For general background on clones see e.g. [16] and for further extensions see e.g. [7,4–6].

An m-ary Boolean function g is said to be obtained from an n-ary Boolean function f by *simple variable substitution*, denoted $g \leq f$, if there are m-ary projections $p_1, \ldots, p_n \in I_c$ such that $g = f(p_1, \ldots, p_n)$. In other words,

$$g \leq f \quad \text{if and only if} \quad g \circ I_c \subseteq f \circ I_c.$$

Thus $\leq$ constitutes a quasi-order on Ω. If $g \leq f$ and $f \leq g$, then g and f are said to be *equivalent*, $g \simeq f$. Let $\tilde{\Omega}$ denote the set of all equivalent classes of Boolean functions and let $\sqsubseteq$ denote the partial-order induced by $\leq$. A class $K \subseteq \Omega$ is said to be *closed under simple variable substitutions* if each function obtained from a function f in K by simple variable substitution is also in K. In other words, the class K is closed under simple variable substitutions if and only if $\tilde{K}$ is an initial segment of $\tilde{\Omega}$. (For an early reference on the quasi-order $\leq$ see e.g. [20] and for further background see [10,17,21,4,2,3]. For variants and generalizations see e.g. [5,6,12–14].)

2.2.1. Essential variables and minors

Let $f : \mathbb{B}^n \to \mathbb{B}$ be an n-ary Boolean function. For each $i \in \mathbf{n}$, x_i is said to be an *essential variable of* f if there are $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ in $\mathbb{B}$ such that

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Otherwise, x_i is called *a dummy variable of* f. The *essential arity of* f, denoted $ess(f)$, is the number of its essential variables.

As it is easy to prove, we have $f(a_1, \ldots, a_n) = f(a'_1, \ldots, a'_n)$ whenever $a_i = a'_i$ for each essential variable x_i. From this observation, we get first that f is constant if and only if its variables are all dummy. Next, if f is not constant, and $x_{i_1}, \ldots, x_{i_m}$ are its essential variables, then there is a unique m-ary f' such that $f(a_1, \ldots, a_n) = f'(a_{i_1}, \ldots, a_{i_m})$ for all $(a_1, \ldots, a_n) \in \mathbb{B}^n$. Furthermore, $ess(f') = m$. If a function g is obtained from f by addition of dummy variables or by permutation of variables then, obviously, $ess(g) = ess(f)$; whereas if g is obtained by identifying variables, $ess(g) < ess(f)$. With respect to our quasi-order on Ω, this implies that if $g \leq f$ then $ess(g) \leq ess(f)$. Hence, the number of essential variables is the same for the all functions belonging to an equivalence class associated with the quasi-order. Clearly, if f' is the function defined above, we have $f' \simeq f$. Thus, for $f, g \in \Omega$, we have $f \simeq g$ if and only if $f' = g'$ up to a permutation of their variables. Concerning the order on $\tilde{\Omega}$ we have:

Lemma 4. *Let* $f \in \Omega$.

(1) *If* $g < f$ *then* $ess(g) < ess(f)$*;*

(2) *Salomaa [19]: If there is some* g *such that* $g < f$ *then there is some* g *such that* $g < f$ *and* $ess(f) \leq ess(g) + 2$.

Corollary 1. *In* $(\tilde{\Omega}, \sqsubseteq)$ *every principal initial segment is finite and each level is finite.*

Proof. Let $f \in \Omega$. The fact that the principal initial segment $\downarrow \tilde{f}$ of $(\tilde{\Omega}, \sqsubseteq)$ is finite follows trivially from (1) of Lemma 4. The fact that each level is finite follows immediately from the fact that the number of essential variables of functions belonging to the nth level is bounded above by a function of n. As observed, we have $\tilde{f} \in \tilde{\Omega}_0$ if and only if f is constant or $ess(f) = 1$. We show that for every $n \geq 1$ and every function f, if $\tilde{f} \in \tilde{\Omega}_n$, then $n < ess(f) \leq 2n + 1$. These inequalities follow from a straightforward induction. Using the fact $\tilde{f} \in \tilde{\Omega}_0$ if and only if f is constant or $ess(f) = 1$ and (2) of Lemma 4, it is easy to verify that the inequalities hold for the case $n = 1$. So assume that the inequalities hold for $1 \leq k < n$. Let $\tilde{f} \in \tilde{\Omega}_n$. According to (2) of Lemma 4, there is some $\tilde{g} \in \tilde{\Omega}_{n-1}$ such that $g < f$ and $ess(f) \leq ess(g) + 2$. By induction hypothesis, we have $ess(g) \leq 2(n-1) + 1$ and hence, $ess(f) \leq 2n + 1$. Furthermore, $n - 1 < ess(g)$ and, by (1) of Lemma 4, $ess(g) < ess(f)$. Thus $n < ess(f)$, and the proof of Corollary 1 is complete. □

2.3. Definability of Boolean function classes by means of functional equations

A *functional equation* (for Boolean functions) is a formal expression

$$h_1(\mathbf{f}(g_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g_m(\mathbf{x}_1,\ldots,\mathbf{x}_p))) = h_2(\mathbf{f}(g'_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g'_t(\mathbf{x}_1,\ldots,\mathbf{x}_p))) \tag{1}$$

where $m, t, p \geq 1$, $h_1 : \mathbb{B}^m \to \mathbb{B}$, $h_2 : \mathbb{B}^t \to \mathbb{B}$, each g_i and g'_j is a map $\mathbb{B}^p \to \mathbb{B}$, the $\mathbf{x}_1,\ldots,\mathbf{x}_p$ are p distinct *vector variable symbols*, and $\mathbf{f}$ is a distinct *function symbol*. Such equations were systematically studied in [10]. See e.g. [18,11,17] for variants, and [5] for extensions and more stringent notions of functional equations.

An n-ary Boolean function $f : \mathbb{B}^n \to \mathbb{B}$, *satisfies* (1) if, for all $\mathbf{v}_1,\ldots,\mathbf{v}_p \in \mathbb{B}^n$, we have

$$h_1(f(g_1(\mathbf{v}_1,\ldots,\mathbf{v}_p)),\ldots,f(g_m(\mathbf{v}_1,\ldots,\mathbf{v}_p))) = h_2(f(g'_1(\mathbf{v}_1,\ldots,\mathbf{v}_p)),\ldots,f(g'_t(\mathbf{v}_1,\ldots,\mathbf{v}_p)))$$

where $g_1(\mathbf{v}_1,\ldots,\mathbf{v}_p)$ is interpreted component-wise, that is,

$$g_1(\mathbf{v}_1,\ldots,\mathbf{v}_p) = (g_1(\mathbf{v}_1(1),\ldots,\mathbf{v}_p(1)),\ldots,g_1(\mathbf{v}_1(n),\ldots,\mathbf{v}_p(n))).$$

A class K of Boolean functions is said to be *defined* by a set $\mathcal{E}$ of functional equations, if K is the class of all those Boolean functions which satisfy every member of $\mathcal{E}$. It is not difficult to see that if a class K is defined by a set $\mathcal{E}$ of functional equations, then it is also defined by a set $\mathcal{E}'$ whose members are functional equations in which the indices m and t are the same. Moreover, it is easy to verify that the functional equation

$$h_1(\mathbf{f}(g_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g_m(\mathbf{x}_1,\ldots,\mathbf{x}_p))) = h_2(\mathbf{f}(g'_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g'_t(\mathbf{x}_1,\ldots,\mathbf{x}_p)))$$

is satisfied by exactly the same functions satisfying

$$h_1(\mathbf{f}(g_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g_m(\mathbf{x}_1,\ldots,\mathbf{x}_p))) + h_2(\mathbf{f}(g'_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g'_t(\mathbf{x}_1,\ldots,\mathbf{x}_p))) = 0$$

where $+$ denotes the sum modulo 2. In the following, we consider equations of the form:

$$h(\mathbf{f}(g_1(\mathbf{x}_1,\ldots,\mathbf{x}_p)),\ldots,\mathbf{f}(g_l(\mathbf{x}_1,\ldots,\mathbf{x}_p))) = 0. \tag{2}$$

By an *equational class* we simply mean a class of Boolean functions definable by a set of functional equations. The following characterization of equational classes was first obtained by Ekin, Foldes, Hammer and Hellerstein [10]. For variants and extensions, see e.g. [11,18,5].

Theorem 4. *The equational classes of Boolean functions are exactly those classes that are closed under simple variable substitutions.*

In other words, a class K is equational if and only if $\tilde{K}$ is an initial segment of $\tilde{\Omega}$.

2.4. Definability of Boolean function classes by means of relational constraints

An *m-ary Boolean relation* is a subset R of $\mathbb{B}^m$. Let f be an n-ary Boolean function. We denote by fR the m-ary relation given by

$$fR = \{f(\mathbf{v}_1,\ldots,\mathbf{v}_n) : \mathbf{v}_1,\ldots,\mathbf{v}_n \in R\}$$

where the m-vector $f(\mathbf{v}_1,\ldots,\mathbf{v}_n)$ is defined component-wise as in the previous subsection.

An m-ary *Boolean constraint*, or simply an m-ary *constraint*, is a pair (R, S) where R and S are m-ary relations called the *antecedent* and *consequent*, respectively, of the relational constraint. A Boolean function is said to *satisfy* an m-ary constraint (R, S) if $fR \subseteq S$. Within this framework, a class K of Boolean functions is said to be *defined* by a set $\mathcal{T}$ of relational constraints, if K is the class of all those Boolean functions which satisfy every member of $\mathcal{T}$. For further background, see [17]. See also [2,4–6,12], for further variants and extensions.

The connection between definability by functional equations and by relational constraints was made explicit by Pippenger who established in [17] a complete correspondence between functional equations and relational constraints. This result was further extended and strengthened in [6].

Theorem 5. *The equational classes of Boolean functions are exactly those classes definable by relational constraints.*

Proof. We follow the same steps as in the Appendix of [17], and show that for each Eq. (2), there is a relational constraint satisfied by exactly the same Boolean functions satisfying (2) and, conversely, for each relational constraint (R, S) there is a functional equation satisfied by exactly the same Boolean functions satisfying (R, S).

For each Eq. (2), let (R, S) be the relational constraint defined by

$$R := \{(g_1(\mathbf{a}), \ldots, g_l(\mathbf{a})) : \mathbf{a} \in \mathbb{B}^p\},$$
$$S := \{(b_1, \ldots, b_l) \in \mathbb{B}^l : h(b_1, \ldots, b_l) = 0\}.$$

Let f be an n-ary Boolean function. From the definition of S, it follows that f satisfies (R, S) if and only if for every $\mathbf{a}_1, \ldots, \mathbf{a}_n \in R$,

$$h(f(\mathbf{a}_1(1), \ldots, \mathbf{a}_n(1)), \ldots, f(\mathbf{a}_1(l), \ldots, \mathbf{a}_n(l))) = 0.$$

Since R is the range of $g = (g_1, \ldots, g_l)$, we have that f satisfies (R, S) if and only if for every $\mathbf{v}_1, \ldots, \mathbf{v}_p \in \mathbb{B}^n$

$$h_1(f(g_1(\mathbf{v}_1, \ldots, \mathbf{v}_p)), \ldots, f(g_l(\mathbf{v}_1, \ldots, \mathbf{v}_p))) = 0.$$

In other words, f satisfies (R, S) if and only if f satisfies (2).

Conversely, let (R, S) be an m-ary relational constraint. We may suppose R nonempty, indeed, constraints with empty antecedent are satisfied by every Boolean function, and thus they can be discarded as irrelevant.

We will construct a functional equation satisfied by exactly the same functions as those satisfying (R, S). Let $\mathbf{c} = (c_1, \ldots, c_m)$ be a member of R and consider the characteristic function χ_R of R, that is, the map $\chi_R : \mathbb{B}^m \to \mathbb{B}$ such that $\chi_R(\mathbf{a}) = 1$ if and only if $\mathbf{a} \in R$. Consider the map $g := (g_1, \ldots, g_m)$, where each g_i is the m-ary Boolean function $g_i : \mathbb{B}^m \to \mathbb{B}$ given by $g_i(\mathbf{a}) = (a_i \cdot \chi_R(a)) \vee (c_i \cdot \overline{\chi_R(a)})$ for every $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{B}^m$. It is easy to verify that R is the range of g.

Now consider the characteristic function χ_S of S. Let $h : \mathbb{B}^m \to \mathbb{B}$ be the map given by $h(\mathbf{a}) = \chi_S(\mathbf{a}) + 1$ for every $\mathbf{a} \in \mathbb{B}^m$ and where $+$ denotes the sum modulo 2.

Consider the functional equation

$$h(\mathbf{f}(g_1(\mathbf{x}_1, \ldots, \mathbf{x}_m)), \ldots, \mathbf{f}(g_m(\mathbf{x}_1, \ldots, \mathbf{x}_m))) = 0 \tag{3}$$

where the g_i's and h are the maps given above. Let f be an n-ary Boolean function. By construction, we have that f satisfies (3) if and only if for every $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{B}^n$, $(f(g_1(\mathbf{v}_1, \ldots, \mathbf{v}_m)), \ldots, f(g_m(\mathbf{v}_1, \ldots, \mathbf{v}_m))) \in S$. From the fact that R is the range of $(g_1, \ldots, g_m)$, it follows that f satisfies (3) if and only if f satisfies (R, S). □

In the following, we will make use of the following result of Pippenger ([17], Theorem 2.1). For the reader's convenience, we provide a proof. For each relational constraint (R, S), let $\Omega(R, S)$ denote the set of all those Boolean functions which satisfy (R, S).

Lemma 5. *For each Boolean function f, there is a relational constraint (R, S) such that $\Omega(R, S) = Forbid(\{f\})$.*

Proof. Let f be a Boolean function, say of arity n. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be 2^n-vectors such that $\mathbb{B}^n = \{(\mathbf{v}_1(i), \ldots, \mathbf{v}_n(i)) : 1 \leq i \leq 2^n\}$. Consider the 2^n-ary relations R_f and S_f given by

$$R_f := \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}, \text{ and } S_f := \bigcup\{gR_f : g \in Forbid(\{f\})\}$$

respectively. Clearly, if $g \in Forbid(\{f\})$, then g satisfies (R_f, S_f). If g', say m-ary, is a member of $\uparrow f$, then there are n-ary projections $p_1, \ldots, p_m \in I_c$ such that

$$f = g'(p_1, \ldots, p_m). \tag{4}$$

We claim that $g'(p_1(\mathbf{v}_1, \ldots, \mathbf{v}_n), \ldots, p_m(\mathbf{v}_1, \ldots, \mathbf{v}_n))$ does not belong to S_f. Otherwise, there would be $g \in Forbid(\{f\})$, and projections $p'_1, \ldots, p'_t$ such that

$$g'(p_1(\mathbf{v}_1, \ldots, \mathbf{v}_n), \ldots, p_m(\mathbf{v}_1, \ldots, \mathbf{v}_n)) = g(p'_1(\mathbf{v}_1, \ldots, \mathbf{v}_n), \ldots, p'_t(\mathbf{v}_1, \ldots, \mathbf{v}_n)).$$

By definition, this amounts to

$$g'(p_1(\mathbf{v}_1, \ldots, \mathbf{v}_n)(i), \ldots, p_m(\mathbf{v}_1, \ldots, \mathbf{v}_n)(i)) = g(p'_1(\mathbf{v}_1, \ldots, \mathbf{v}_n)(i), \ldots, p'_t(\mathbf{v}_1, \ldots, \mathbf{v}_n)(i))$$

for all i, $1 \leq i \leq 2^n$. Which, in turn, amounts to

$$g'(p_1(\mathbf{v}_1(i), \ldots, \mathbf{v}_n(i)), \ldots, p_m(\mathbf{v}_1(i), \ldots, \mathbf{v}_n(i))) = g(p'_1(\mathbf{v}_1(i), \ldots, \mathbf{v}_n(i)), \ldots, p'_t(\mathbf{v}_1(i), \ldots, \mathbf{v}_n(i))).$$

Since for every $(x_1, \ldots, x_n) \in \mathbb{B}^n$ there is some i such that

$$(\mathbf{v}_1(i), \ldots, \mathbf{v}_n(i)) = (x_1, \ldots, x_n)$$

we get

$$g'(p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)) = g(p'_1(x_1, \ldots, x_n), \ldots, p'_t(x_1, \ldots, x_n))$$

for all $(x_1, \ldots, x_n) \in \mathbb{B}^n$, that is

$$g'(p_1, \ldots, p_m) = g(p'_1, \ldots, p'_t).$$

With (4) we get $f = g(p'_1, \ldots, p'_t)$ that is f is obtained from g by simple variable substitutions, contradicting our assumption $g \in \mathit{Forbid}(\{f\})$. □

Now we can present a proof of Theorem 1.

Proof of Theorem 1. We show that (i) ⇒ (ii) ⇒ (iii) ⇒ (i).

(i) ⇒ (ii) To see that each class $I \in \mathcal{F}$ can be defined by a single functional equation, note that if I is defined by the equations $H_1 = 0, \ldots, H_n = 0$, then it is also defined by $\bigvee_{i \in \mathbf{n}} H_i = 0$.

(ii) ⇒ (iii) Let $H = 0$ be a functional equation. According to the proof of Theorem 5, there is a relational constraint (R, S) such that the operations satisfying $\Omega(R, S)$ are those satisfying $H = 0$. In view of Theorem 5, to show that (ii) ⇒ (iii) it is enough to prove the following lemma.

Lemma 6. *The set $\Omega(R, S)$ of Boolean functions which satisfy a n-ary constraint (R, S) is of the form $\mathit{Forbid}(A)$ for some finite antichain A of Ω.*

Proof.

Claim 1. *If an m-ary Boolean function g does not satisfy (R, S), then there is some m'-ary g', where $m' \leq 2^n$, such that $g' \leq g$ and such that g' does not satisfy (R, S).*

Proof (*Proof of Claim 1*). If $m \leq 2^n$ set $g' := g$. If not, let $v_1, \ldots, v_m \in R$ such that $g(v_1, \ldots, v_m) \notin S$. Say that two indices $i, j \in \mathbf{m}$ are equivalent if $v_i = v_j$. Let $C_1, \ldots, C_{m'}$ be an enumeration of the equivalence classes. For each $i \in \mathbf{m}$, let $c(i)$ be the index for which $i \in C_{c(i)}$. Let g' be the m'-ary operation defined by $g' := g(p_1, \ldots, p_m)$, where $p_j(x_1, \ldots, x_{m'}) = x_{c(j)}$. Clearly, $m' \leq 2^n$ and, by definition, $g' \leq g$. For each $j \in \mathbf{m}'$, let $w_j := v_i$, whenever $c(i) = j$. We have $g(v_1, \ldots, v_m) = g(w_{c(1)}, \ldots, w_{c(m)})$ and since $g'(x_1, \ldots, x_{m'}) = g(x_{c(1)}, \ldots, x_{c(m)})$ it follows that $g'(w_1, \ldots, w_m) = g(v_1, \ldots, v_m)$ and hence, g' does not satisfy (R, S). This completes the proof of the lemma. □

From Claim 1, the minimal members of $\Omega \setminus \Omega(R, S)$ have arity at most 2^n and hence, there are only finitely many of such minimal members (w.r.t. the equivalence associated with the quasi-order). □

(iii) ⇒ (i) Let $I := \mathit{Forbid}(A)$ where A is a finite antichain. Since I is a finite intersection of sets of the form $\mathit{Forbid}(\{f\})$, in order to get that $I \in \mathcal{F}$, it suffices to show that $\mathit{Forbid}(\{f\}) \in \mathcal{F}$. By Lemma 5, $\mathit{Forbid}(\{f\})$ is defined by a single constraint. As shown in the proof of Theorem 5, this is equivalent to saying that $\mathit{Forbid}(\{f\})$ is defined by a single equation, and thus $\mathit{Forbid}(\{f\}) \in \mathcal{F}$, which completes the proof of Theorem 1.

3. Proof of Lemma 1

Statement (1). If K_1 and K_2 are classes in $\mathcal{F}$, say defined, respectively, by the expressions

$$h_1(\mathbf{f}(g_1(\mathbf{x}_1, \ldots, \mathbf{x}_p)), \ldots, \mathbf{f}(g_m(\mathbf{x}_1, \ldots, \mathbf{x}_p))) = 0$$

and

$$h_2(\mathbf{f}(g'_1(\mathbf{y}_1,\ldots,\mathbf{y}_l)),\ldots,\mathbf{f}(g'_t(\mathbf{y}_1,\ldots,\mathbf{y}_l)))=0$$

then, by taking disjoint sets $\{\mathbf{z}_1,\ldots,\mathbf{z}_p\}$ and $\{\mathbf{w}_1,\ldots,\mathbf{w}_l\}$ of vector variable symbols, we have that $K_1\cup K_2$ and $K_1\cap K_2$ are defined by

$$h_1(\mathbf{f}(g_1(\mathbf{z}_1,\ldots,\mathbf{z}_p)),\ldots,\mathbf{f}(g_m(\mathbf{z}_1,\ldots,\mathbf{z}_p))\cdot$$
$$h_2(\mathbf{f}(g'_1(\mathbf{w}_1,\ldots,\mathbf{w}_l)),\ldots,\mathbf{f}(g'_t(\mathbf{w}_1,\ldots,\mathbf{w}_l)))=0$$

and

$$h_1(\mathbf{f}(g_1(\mathbf{z}_1,\ldots,\mathbf{z}_p)),\ldots,\mathbf{f}(g_m(\mathbf{z}_1,\ldots,\mathbf{z}_p))\vee$$
$$h_2(\mathbf{f}(g'_1(\mathbf{w}_1,\ldots,\mathbf{w}_l)),\ldots,\mathbf{f}(g'_t(\mathbf{w}_1,\ldots,\mathbf{w}_l)))=0,$$

respectively. This proves that statement (1) of Lemma 1 holds. The fact that $\mathcal{F}$ is closed under finite intersections follows also from the equivalence (i) $\Leftrightarrow$ (iii) of Theorem 1. Note that from this equivalence and the fact that $\mathcal{F}$ is closed under finite unions, it follows that $\tilde{\Omega}$ is up-closed.

Statement (2). Implication (iii) $\Rightarrow$ (i) of Theorem 1.

Statement (3). Let $f\in\Omega$. Let $\tilde{f}$ be its image in $P:=(\tilde{\Omega},\sqsubseteq)$ (i.e., the equivalence class containing f), and $m:=h(\tilde{f},P)$. The initial segment $\downarrow f$ is of the form $Forbid(A)$ for some antichain A. This antichain A is made of representative of the minimal elements of $B:=P\setminus\downarrow\tilde{f}$. If y is minimal in B then for every x such that $x<y$, we have $x\leq\tilde{f}$. It follows that $h(y,P)\leq h(\tilde{f},P)+1=m+1$, that is the minimal elements of B belong to the union of levels P_n for $n\leq m+1$. From Corollary 1, all levels of P are finite. Hence A is finite.

4. Proof of Theorem 3

Let $P:=(\tilde{\Omega},\sqsubseteq)$.

Part 1. P embeds into $([\omega]^{<\omega},\subseteq)$.

We apply Lemma 3. The poset P is trivially countable, and by Corollary 1, for every $x\in P$, the initial segment $\downarrow x$ is finite. Thus, by Lemma 3, P embeds into $([\omega]^{<\omega},\subseteq)$.

Part 2. $([\omega]^{<\omega},\subseteq)$ embeds into P. The following is a particular case of Proposition 3.4 in [17].

Lemma 7. *The family $(f_n)_{n\geq 4}$ of Boolean functions, given by*

$$f_n(x_1,\ldots,x_n)=\begin{cases}1 & \text{if } \#\{i:x_i=1\}\in\{1,n-1\}\\ 0 & \text{otherwise}\end{cases}$$

constitutes an infinite antichain of Boolean functions.

Note that $f_n(a,\ldots,a)=0$ for $a\in\{0,1\}$. The following lemma was presented in [3].

Lemma 8. *Let $(f_n)_{n\geq 4}$ be the family of Boolean functions given above, and consider the family $(u_n)_{n\geq 4}$ defined by*

$$u_n(x_0,x_1,\ldots,x_n)=x_0\cdot f_n(x_1,\ldots,x_n).$$

The family $(u_n)_{n\geq 4}$ constitutes an infinite antichain of Boolean functions.

Proof. We follow the same steps as in [3]. We show that if $m\neq n$, then $u_m\not\leq u_n$. By definition, u_m and u_n cannot have dummy variables. Therefore, $u_m\not\leq u_n$, whenever $m>n$.

So assume that $m<n$, and for a contradiction, suppose that $u_m\leq u_n$, i.e. there are $(m+1)$-ary projections $p_0,\ldots,p_n\in I_c$ such that $u_m=u_n(p_0,\ldots,p_n)$. Note that for every $m\geq 4$, $u_m(1,x_1\ldots,x_m)=f_m(x_1\ldots,x_m)$ and $u_m(0,x_1\ldots,x_m)$ is the constant 0.

Now, suppose that $p_0(x_0,\ldots,x_m)=x_0$. If for all $k\in\mathbf{n}$, $p_k(x_0,\ldots,x_m)\neq x_0$, then by taking $x_0=1$ we would conclude that $f_m\leq f_n$, contradicting Lemma 7. Suppose that there is $k\in\mathbf{n}$ such that $p_k(x_0,\ldots,x_m)=x_0$. From the fact that each variable of u_m is essential, it follows that for each $j\in\mathbf{m}$ there is $l\in\mathbf{n}$ such that $p_l(x_0,\ldots,x_m)=x_j$.

Hence, by taking $x_i = 1$ if and only if $i = 0, 1$, we have that the vector $(p_1(x_0, \ldots, x_m), \ldots, p_n(x_0, \ldots, x_m))$ has at least 2 and at most $n - 2$ components equal to 1 and thus

$$\begin{aligned} u_m(x_0, \ldots, x_m) &= u_m(1, 1, 0, \ldots, 0) \\ &= f_m(1, 0, \ldots, 0) = 1 \neq 0 = f_n(p_1(1, 1, 0, \ldots, 0), \ldots, p_n(1, 1, 0, \ldots, 0)) \\ &= u_n(1, p_1(1, 1, 0, \ldots, 0), \ldots, p_n(1, 1, 0, \ldots, 0)) = u_n(x_0, p_1(x_0, \ldots, x_m), \ldots, p_n(x_0, \ldots, x_m)) \end{aligned}$$

which is also a contradiction.

Hence, $p_0(x_0, \ldots, x_m) \neq x_0$, say $p_0(x_0, \ldots, x_m) = x_j$ for $j \in \mathbf{m}$. But then by taking $x_i = 1$ if and only if $i = 0, k$, for some $k \in \mathbf{m}$ such that $k \neq j$, we would have

$$\begin{aligned} u_m(x_0, x_1, \ldots x_{k-1}, x_k, x_{k+1}, \ldots, x_m) &= u_m(1, 0, \ldots, 0, 1, 0, \ldots, 0) \\ &= f_m(0, \ldots, 0, 1, 0, \ldots, 0) = 1 \neq 0 \\ &= u_n(0, p_1(1, 0, \ldots, 0, 1, 0, \ldots, 0), \ldots, p_n(1, 0, \ldots, 0, 1, 0, \ldots, 0)) \\ &= u_n(x_j, p_1(x_0, \ldots, x_m), \ldots, p_n(x_0, \ldots, x_m)) \end{aligned}$$

which contradicts our assumption $u_m \leq u_n$. □

Let I be a nonempty finite set of integers greater than or equal to 4, and let g_I be the $\sum_{i \in I} i$-ary Boolean function (where $\sum_{i \in I} i$ denotes the sum of the positive integers in I) given by

$$g_I(x_l^t : t \in I, l \in \mathbf{t}) = \sum_{i \in I} f_i(x_1^i, \ldots, x_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} x_k^j$$

where the sum in the definition of g_I is taken modulo 2.

Lemma 9. *Let I be a nonempty finite set of integers greater than or equal to 4, and let g_I be the function defined above. If $n \in I$, then $u_n \leq g_I$.*

Proof. To prove Lemma 9 we have to show that, for every $n \in I$, there are $(n + 1)$-ary projections $p_1^i, \ldots, p_i^i$, for each $i \in I$, such that

$$u_n = \sum_{i \in I} f_i(p_1^i, \ldots, p_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} p_k^j.$$

For $j \in I \setminus \{n\}$ and $k \in \mathbf{j}$, let $p_k^j(x_0, x_1, \ldots, x_n) = x_0$, and for $k \in \mathbf{n}$, let $p_k^n(x_0, x_1, \ldots, x_n) = x_k$. Note that for each $i \in I \setminus \{n\}$, we have $f_i(p_1^i, \ldots, p_i^i) = 0$ and thus

$$f_i(p_1^i, \ldots, p_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} p_k^j = 0$$

whereas for $i = n$, we have

$$f_i(p_1^i, \ldots, p_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} p_k^j = f_n(x_1, \ldots, x_n) \cdot x_0.$$

Hence, we conclude that indeed

$$u_n = \sum_{i \in I} f_i(p_1^i, \ldots, p_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} p_k^j. \quad \square$$

Lemma 10. *Let I and g_I be as in Lemma 9. Then $g_I(x_l^t : t \in I, l \in \mathbf{t}) = 1$ if and only if there is exactly one $i \in I$ such that*

(i) *for all $j \in I \setminus \{i\}$ and $k \in \mathbf{j}$, $x_k^j = 1$, and*
(ii) $\#\{1 \leq k \leq i : x_k^i = 1\} \in \{1, i - 1\}$.

If $n \in I$, then $u_n \leq g_I$.

Proof. It is not difficult to verify that if there is exactly one $i \in I$ such that

(i) for all $j \in I \setminus \{i\}$ and $k \in \mathbf{j}$, $x_k^j = 1$, and
(ii) $\#\{1 \leq k \leq i : x_k^i = 1\} \in \{1, i-1\}$,

then $g_I(x_l^t : t \in I, l \in \mathbf{t}) = 1$.

Now, suppose that $g_I(x_l^t : t \in I, l \in \mathbf{t}) = 1$. Note that if an index $i \in I$ satisfying conditions (i) and (ii) exists, then conditions (i) and (ii) imply that it is unique.

So for a contradiction, suppose that there is no index $i \in I$ satisfying conditions (i) and (ii), that is, for each $i \in I$, there is $j \in I \setminus \{i\}$ and $k \in \mathbf{j}$, such that $x_k^j = 0$, or $\#\{1 \leq k \leq i : x_k^i = 1\} \notin \{1, i-1\}$. This means that for each $i \in I$, we have $\prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} x_k^j = 0$ or $f_i(x_1^i, \ldots, x_i^i) = 0$. Thus

$$\sum_{i \in I} f_i(x_1^i, \ldots, x_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} x_k^j = 0$$

which constitutes the desired contradiction. □

Proposition 1. *Let I be a nonempty finite set of integers greater than or equal to 4, and let g_I be the $\sum_{i \in I} i$-ary function given above. Then for every $n \geq 4$, $n \in I$ if and only if $u_n \leq g_I$.*

Proof. By Lemma 9, we only have to show that if $n \notin I$, then $u_n \not\leq g_I$. So assume that $n \notin I$ and for a contradiction suppose that $u_n \leq g_I$, i.e., there are projections $p_k^i(x_0, x_1, \ldots, x_n)$, $i \in I$ and $k \in \mathbf{i}$, such that

$$u_n = \sum_{i \in I} f_i(p_1^i, \ldots, p_i^i) \cdot \prod_{j \in I \setminus \{i\}} \prod_{k \in \mathbf{j}} p_k^j. \tag{5}$$

Consider the vector $(a_0, a_1, \ldots, a_n)$ given by $a_l = 1$ iff $l = 0, 1$. Clearly,

$$u_n(a_0, a_1, \ldots, a_n) = 1.$$

It follows from Lemma 10 that, in order to have (5) $= 1$, there must exist exactly one $i \in I$ such that

(i) for all $j \in I \setminus \{i\}$ and $k \in \mathbf{j}$, $p_k^j \in \{x_0, x_1\}$, and
(ii) $\#\{k \in \mathbf{i} : p_k^i \in \{x_0, x_1\}\} \in \{1, i-1\}$.

Fix such a unique $i \in I$.

Remark 1. Since $x_2, \ldots, x_n$ are essential in u_n, we have that for each $l \in \mathbf{n} \setminus \{1\}$, there is $k \in \mathbf{i}$ such that $p_k^i = x_l$.

Remark 2. Since $4 \leq n$, we have $i - (n-2) \leq i - 2$.

In the following, we will also make use of the following claims.

Claim 2. *There is $k \in \mathbf{i}$, such that $p_k^i = x_1$.*

Proof. For a contradiction, suppose that for all $k \in \mathbf{i}$, $p_k^i \neq x_1$. Since x_1 is essential in u_n, there are $j_1 \in I \setminus \{i\}$ and $k_1 \in \mathbf{j_1}$, such that $p_{k_1}^{j_1} = x_1$. Consider $\mathbf{b} = (b_0, b_1, \ldots, b_n)$ given by $b_l = 1$ iff $l = 0, 2$. We have $u_n(\mathbf{b}) = 1$. Since $p_{k_1}^{j_1}(\mathbf{b}) = 0$, we have that for every $j \in I \setminus \{j_1\}$,

$$f_j(p_1^j(\mathbf{b}), \ldots, p_j^j(\mathbf{b})) \cdot \prod_{t \in I \setminus \{j\}} \prod_{k \in \mathbf{t}} p_k^t(\mathbf{b}) = 0.$$

Moreover, the value of

$$f_{j_1}(p_1^{j_1}(\mathbf{b}), \ldots, p_{j_1}^{j_1}(\mathbf{b})) \cdot \prod_{t \in I \setminus \{j_1\}} \prod_{k \in \mathbf{t}} p_k^t(\mathbf{b})$$

is also equal to 0 because for each $l \in \mathbf{n} \setminus \{1, 2\}$, where $4 \leq n$, there is $k \in \mathbf{i}$ such that $p_k^i(\mathbf{b}) = 0$. Hence, the right-hand side of (5) is 0, which constitutes a contradiction. □

Claim 3. *For every* $t \in \mathbf{i}$, $p^i_t \neq x_0$.

Proof. For a contradiction, suppose that there is $t \in \mathbf{i}$ such that $p^i_t = x_0$. Consider $\mathbf{b} = (b_0, b_1, \ldots, b_n)$ given by $b_l = 1$ iff $l = 0, 1$. We have $u_n(\mathbf{b}) = 1$. From Remarks 1 and 2, it follows that $2 \leq \#\{k \in \mathbf{i} : p^i_k(\mathbf{b}) = 1\} \leq i - 2$, and hence, the right-hand side of (5) is 0. This constitutes the desired contradiction. □

From Claim 2 and Remark 1, it follows that $i \not\prec n$. Since $n \notin I$, we must have $i > n$. Thus there exists $s \in \mathbf{n}$ such that, for some $r_1, r_2 \in \mathbf{i}$ with $r_1 < r_2$, we have $p^i_{r_1} = p^i_{r_2} = x_s$. Note that by Claim 3, s cannot be equal to 0.

Now, if $s = 1$, then for $\mathbf{b} = (b_0, b_1, \ldots, b_n)$ given by $b_l = 1$ iff $l = 0, 1$, we have $u_n(\mathbf{b}) = 1$. From Remarks 1 and 2, it follows that $2 \leq \#\{k \in \mathbf{i} : p^i_k(\mathbf{b}) = 1\} \leq i - 2$ and hence, the right-hand side of (5) is 0.

If $s \in \mathbf{n} \setminus \{1\}$, then for $\mathbf{b} = (b_0, b_1, \ldots, b_n)$ given by $b_l = 1$ iff $l \neq s$, we have $u_n(\mathbf{b}) = 1$ and the right-hand side of (5) is 0.

Since in all the possible cases we derive the same contradiction, the proof of the proposition is complete. □

By making use of Proposition 1, it is not difficult to verify that the mapping $I \mapsto g_{I'}$, where $I' = \{i + 4 : i \in I\}$, is an embedding from $([\omega]^{<\omega}, \subseteq)$ into $(\tilde{\Omega}, \sqsubseteq)$.

5. Boolean functions with bounded polynomial degree

A *multilinear monomial* is a term of the form

$$\vec{x}_I = \prod_{i \in I} x_i,$$

for some finite set I. The size $\#I$ is called the *degree* of $\vec{x}_I$. A *multilinear polynomial* is a sum modulo 2 of monomials and its *degree* is the largest degree of its monomials. We convey that 0 is a multilinear monomial, and that 1 is the empty monomial $\vec{x}_\emptyset$. Note that the only monomials with degree zero are the multilinear monomials 0 and 1.

It is well known that each Boolean function $f : \mathbb{B}^n \to \mathbb{B}$ is uniquely represented by multilinear polynomial in $\mathbb{B}[x_1, \ldots, x_n]$, i.e.

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \mathbf{n}} a_I \cdot \vec{x}_I$$

where each a_I belongs to $\mathbb{B}$.

Lemma 11. *If* f *is uniquely represented by the multilinear polynomial*

$$\sum_{I \subseteq \mathbf{n}} a_I \cdot \vec{x}_I$$

then for $a_I \neq 0$, *the variables occurring in* $\vec{x}_I$ *are essential in* f.

The *degree* of a Boolean function $f : \mathbb{B} \to \mathbb{B}$, denoted $deg(f)$ is thus defined as the degree of the multilinear polynomial $p \in \mathbb{B}[x_1, \ldots, x_n]$ representing f. For each $1 \leq k$, let D^k be the class of Boolean functions with degree strictly less than k. For example, D^1 contains only constant functions, and thus it is the union of the two equivalence classes containing the constant-zero and constant-one functions.

Let K be an equational class of Boolean functions. We denote by $Critical(K)$ the set of minimal elements of $\tilde{\Omega} \setminus \tilde{K}$. In other words, $Critical(K)$ comprises the equivalence classes of those functions $f \in \Omega \setminus K$ which satisfy the condition: if $g < f$, then $g \in K$. From this fact it follows that

$$\tilde{K} = Forbid(Critical(K)).$$

The following theorem provides a characterization of each set $Critical(D^k)$. The case $k = 1$ appears to be different from the case $k \geq 2$.

Theorem 6. *For each* $k \geq 2$, *an equivalence class* $\tilde{g}$, *of a Boolean function* g, *is in* $Critical(D^k)$ *if and only if* $g \simeq r$, *for* $r = p + q$ *where*

(1) $p = \vec{x}_{\mathbf{k}} = \prod_{i \in \mathbf{k}} x_i$ *or*

$$p = \sum_{i \in I} \vec{x}_{I \setminus \{i\}}, \text{ where } I = \mathbf{k} + \mathbf{1} = \{1, \ldots, k+1\}$$

(2) $deg(q) < k$ *and all variables occurring in* q *occur in* p.

The set $Critical(D^1)$ *consists of the equivalence classes of* $x_1 \cdot x_2 + x_1$, $x_1 + x_2$, x_1 *and* $x_1 \cdot x_2 + x_1 + 1$, $x_1 + x_2 + 1$, $x_1 + 1$.

Corollary 2. *For each* $k \geq 1$, $Critical(D^k)$ *is finite. Thus* D^k *is finitely definable.*

Proof (*Proof of Theorem 6*). Let $k \geq 2$. First, we show that if g has the form given above, then $\tilde{g}$ is in $Critical(D^k)$. Suppose that $g \simeq r$, for some $r = p + q$ with p and q as given in (1) and (2). Let x_i and x_j be any two variables occurring in r and let $r_{x_j = x_i}$ be obtained from r by identifying x_i and x_j.

If $p = \vec{x}_{\mathbf{k}}$ then this term becomes a term of degree $k - 1$. If

$$p = \sum_{i \in I} \vec{x}_{I \setminus \{i\}}, \text{ where } I = \mathbf{k} + \mathbf{1}$$

then the polynomial $p_{x_j = x_i}$ obtained from p by identifying x_j to x_i, also becomes a term of degree $k - 1$. Indeed, all monomials containing both x_j and x_i become monomials of degree $k-1$, and the monomials $\vec{x}_{I \setminus \{j\}}$ and $\vec{x}_{I \setminus \{i\}}$ become the same monomial and thus their sum modulo 2 is 0. Thus, if $g \simeq r$, for $r = p + q$, then $\tilde{g}$ is in $Critical(D^k)$.

To prove that the converse also holds, we first show that every function g, such that $\tilde{g} \in Critical(D^k)$, has degree equal to k and has at most $k + 1$ essential variables. With these restrictions on the representatives of the members of $Critical(D^k)$, we show that if $\tilde{g} \in Critical(D^k)$, then $g \simeq p + q$, where p and q have the form given in (1) and (2) of Theorem 6.

Claim 4. *For each* $k \geq 2$, *if* $\tilde{g} \in Critical(D^k)$, *then* g *has degree equal to* k.

Proof. It suffices to prove that the functions which are representatives of equivalence classes in $Critical(D^k)$ have degree equal to k. We show that if $f \notin D^k$, say with degree $n > k$, then there are indices i, j such that x_i and x_j are essential variables of f, and the function $f_{x_i = x_j} < f$ obtained from f by identifying x_i and x_j, has degree at least $n - 1$. Thus $ess(f_{x_i = x_j}) \geq k$, which means that $f_{x_i = x_j} \notin D^k$, and which implies that $\tilde{f} \notin Critical(D^k)$.

In view of Lemma 11, we only need to consider variables x_i and x_j in the polynomial representation of f. So let C be a monomial in the polynomial representation of f, with degree n. By permuting the variables of f, if necessary, we may assume that

$$C = \vec{x}_I, \text{ where } I = \mathbf{n}.$$

Consider the monomials $\vec{x}_{I \setminus \{1\}}, \vec{x}_{I \setminus \{2\}}, \vec{x}_{I \setminus \{3\}}$. If at least two appear in the polynomial representation of f, say $\vec{x}_{I \setminus \{1\}}$ and $\vec{x}_{I \setminus \{2\}}$, then by choosing $i = 1$ and $j = 2$, it follows that $\vec{x}_{I \setminus \{1\}}$ appears in the polynomial representation of $f_{x_1 = x_2}$. Indeed, by identifying x_1 to x_2, the monomials C, $\vec{x}_{I \setminus \{1\}}$ and $\vec{x}_{I \setminus \{2\}}$ become the same monomial $\vec{x}_{I \setminus \{1\}}$ and hence, the sum of the three monomials is $\vec{x}_{I \setminus \{1\}}$. Thus $f_{x_1 = x_2}$ has degree at least $n - 1$ as desired. Similarly, if $\vec{x}_{I \setminus \{1\}}$ and $\vec{x}_{I \setminus \{3\}}$, or $\vec{x}_{I \setminus \{2\}}$ and $\vec{x}_{I \setminus \{3\}}$, appear in the polynomial representation of f, then $f_{x_1 = x_3}$, or $f_{x_2 = x_3}$, have degree at least $n - 1$.

Suppose that at most one of the above monomials appears in the polynomial representation of f, say $\vec{x}_{I \setminus \{1\}}$. In this case, by identifying x_2 to x_3, C becomes $\vec{x}_{I \setminus \{2\}}$, a monomial of degree $n - 1$, and $\vec{x}_{I \setminus \{1\}}$ becomes $\vec{x}_{I \setminus \{1,2\}}$, a monomials of degree $n - 2$. Thus $\vec{x}_{I \setminus \{2\}}$ appears in the polynomial representation of $f_{x_2 = x_3}$, and thus $f_{x_2 = x_3}$ has degree at least $n - 1$. Similarly, if $\vec{x}_{I \setminus \{2\}}$ or $\vec{x}_{I \setminus \{3\}}$, appear in the polynomial representation of f, then $f_{x_1 = x_3}$ or $f_{x_1 = x_2}$, have degree at least $n - 1$. □

Claim 5. *For each* $k \geq 2$, *if* $\tilde{g} \in Critical(D^k)$, *then* g *has at most* $k + 1$ *essential variables.*

Proof. By the previous claim, $Critical(D^k)$ contains only equivalence classes represented by functions with degree equal to k. For a contradiction, suppose that there is $f \in \Omega$ with more than $k + 1$ essential variables such that $\tilde{f} \in Critical(D^k)$. Let C be a monomial in the polynomial representation of f, with degree k. Let g be the function obtained from f by identifying all variables of f, not appearing in C. Clearly, $g < f$ and, since C is appears in the polynomial representation of g, g has degree k, which constitutes the desired contradiction. □

Suppose that $\tilde{g} \in \mathit{Critical}(D^k)$. By Claims 4 and 5, we may assume that g has degree k, and has either k or $k+1$ essential variables. Let $r \simeq g$ with essential variables $x_1, \ldots, x_k$ or $x_1, \ldots, x_{k+1}$. Let p be the sum of the monomials in the polynomial representation of r with degree k, and let q be the sum of the monomials in r with degree less than k. Clearly, $r = p + q$.

If an essential variable of q is not an essential variable of p, then by identifying that variable of q with any variable of p, we obtain a function f with degree k and with fewer essential variables than r. Hence, $f \notin D^k$ and $f < r \simeq g$, contradicting the minimality of g. Thus every essential variable of q is an essential variable of p.

We show that p is either of the form $p = \vec{x}_{\mathbf{k}}$ or, for $I = \mathbf{k}+\mathbf{1}$

$$p = \sum_{i \in I} \vec{x}_{I \setminus \{i\}}.$$

For a contradiction, suppose that p has neither the former nor the latter expressions. Let $I' \subseteq I$ with $1 < \#I' < k+1$, such that for every $i \in I'$, $\vec{x}_{I\setminus\{i\}}$ is a monomial of p, and let $j \in I$ such that $\vec{x}_{I\setminus\{j\}}$ is not a monomial of p. Consider $l \in I'$, and let $p_{x_j = x_l}$ be the polynomial obtained from p by identifying x_j to x_l. Then we have that for every $t \in I' \setminus \{l\}$, $\vec{x}_{I\setminus\{j,t\}}$ is a monomial of $p_{x_j=x_l}$ with degree $k-1$. But the monomial $\vec{x}_{I\setminus\{j\}}$ is a monomial of $p_{x_j=x_l}$ with degree k. Thus, by identifying x_j to x_l, we can obtain a function $f < r \simeq g$ with degree k, and hence not in D^k, which contradicts the minimality of g.

Now, let $k = 1$. It is not difficult to see that the equivalence classes of $x_1 \cdot x_2 + x_1$, $x_1 + x_2$, x_1 and $x_1 \cdot x_2 + x_1 + 1$, $x_1 + x_2 + 1$, $x_1 + 1$ are indeed in $\mathit{Critical}(D^1)$. Note that every polynomial of degree 1 is equivalent to one of the latter polynomials, and the only polynomials of degree 2 which are not equivalent to any of the latter polynomials are $x_1 \cdot x_2$ and $x_1 \cdot x_2 + 1$.

For a contradiction, suppose that there is $\tilde{g} \in \mathit{Critical}(D^1)$ such that g is not equivalent to any polynomial mentioned above. Since $x_1 + a < x_1 \cdot x_2 + a$, for $a \in \mathbb{B}$, g cannot be equivalent to $x_1 \cdot x_2$ nor to $x_1 \cdot x_2 + 1$. As observed, this means that g has degree greater than 2. As in the proof of Claim 4, we can find $g' < g$ with degree at least 2. Since $g' \in \Omega \setminus D^1$, this contradicts the minimality of g, and the proof of Theorem 6 is complete. □

Remark 3. The procedure given in the proof of Claim 4, applied repeatedly to monomials of maximum degree n in the polynomial representation of some function f, gives a function $g < f$ with degree $n-1$.

Several equational characterizations of the classes D^k (also, in domains more general than the Boolean case), were given in [6]. We present those characterizations which are given in terms of linear equations. For the proof, we refer the reader to [6].

Theorem 7 (*In [6]*). *Let $k \geq 1$. The class D^k of Boolean functions having degree less than k, is defined by*

$$\sum_{I \subseteq \mathbf{k}} \mathbf{f}\Big(\sum_{i \in I} \mathbf{x}_i\Big) = 0.$$

6. Boolean functions with a bounded number of essential variables

Theorem 8. *The class E^k of Boolean functions with at most $k \geq 1$ essential variables is defined by*

$$\prod_{i \in \mathbf{k}+\mathbf{1}} (\mathbf{f}(\mathbf{x}_i) + \mathbf{f}(\mathbf{x}_i + \mathbf{y}_i)) \longrightarrow \bigvee_{i \in \mathbf{k}+\mathbf{1}} \bigvee_{\substack{J \subseteq \mathbf{k}+\mathbf{1}\setminus\{i\} \\ \emptyset \neq J}} \mathbf{f}(\mathbf{x}_i) + \mathbf{f}\Big(\mathbf{x}_i + \Big(\sum_{j \in J} \mathbf{y}_j\Big) \cdot \mathbf{y}_i\Big) = 1. \tag{6}$$

Proof. First, we show that (6) is not satisfied by Boolean functions not in E^k. So let f be an n-ary Boolean function with more than k essential variables, say with the first $k+1$ variables essential. This means that there are $\mathbf{b}_i = (b_{i1}, \ldots, b_{in}) \in \mathbb{B}^n$, $i \in \mathbf{k}+\mathbf{1}$, such that

$$f(b_{i1}, \ldots, b_{ii}, \ldots, b_{in}) \neq f(b_{i1}, \ldots, b_{ii}+1, \ldots, b_{in}).$$

For each $i \in \mathbf{k}+\mathbf{1}$, let $\mathbf{a}_i$ be the unit n-vector with all but the ith component equal to 0. Clearly, for every $i \in \mathbf{k}+\mathbf{1}$ and every nonempty subset J of $\mathbf{k}+\mathbf{1} \setminus \{i\}$, we have $(\sum_{j \in J} \mathbf{a}_j) \cdot \mathbf{a}_i = 0$ and hence,

$$\bigvee_{i \in \mathbf{k}+\mathbf{1}} \bigvee_{\substack{J \subseteq \mathbf{k}+\mathbf{1}\setminus\{i\} \\ \emptyset \neq J}} f(\mathbf{b}_i) + f\Big(\mathbf{b}_i + \Big(\sum_{j \in J} \mathbf{a}_j\Big) \cdot \mathbf{a}_i\Big) = 0.$$

By assumption, $\prod_{i\in\mathbf{k+1}}(f(\mathbf{b}_i)+f(\mathbf{b}_i+\mathbf{a}_i))=1$, for every $i\in\mathbf{k}+\mathbf{1}$, which implies that f does not satisfy (6).

Now, we show that (6) is satisfied by every Boolean function in E^k. So suppose that f is an n-ary Boolean function in E^k. By Theorem 4, we may assume that all variables of f are essential. Note that if $\mathbf{c}_1,\ldots,\mathbf{c}_{k+1},\mathbf{d}_1,\ldots,\mathbf{d}_{k+1}$ are vectors in $\mathbb{B}^n$ for which

$$\prod_{i\in\mathbf{k+1}}(f(\mathbf{c}_i)+f(\mathbf{c}_i+\mathbf{d}_i))=0,$$

then

$$\prod_{i\in\mathbf{k+1}}(f(\mathbf{c}_i)+f(\mathbf{c}_i+\mathbf{d}_i))\longrightarrow\bigvee_{i\in\mathbf{k+1}}\ \bigvee_{\substack{J\subseteq\mathbf{k+1}\setminus\{i\}\\ \emptyset\neq J}} f(\mathbf{c}_i)+f(\mathbf{c}_i+(\sum_{j\in J}\mathbf{d}_j)\cdot\mathbf{d}_i)=1.$$

Let $\mathbf{c}_1,\ldots,\mathbf{c}_{k+1},\mathbf{d}_1,\ldots,\mathbf{d}_{k+1}\in\mathbb{B}^n$ such that

$$\prod_{i\in\mathbf{k+1}}(f(\mathbf{c}_i)+f(\mathbf{c}_i+\mathbf{d}_i))=1.$$

Note that $n\leq k$ and for each $i\in\mathbf{k}+\mathbf{1}$, $\mathbf{d}_i$ cannot be the all-zero vector. Thus the n-vectors $\mathbf{d}_1,\ldots,\mathbf{d}_{k+1}$ must be linearly dependent, that is, there is $i\in\mathbf{k}+\mathbf{1}$ and a nonempty subset J of $\mathbf{k}+\mathbf{1}\setminus\{i\}$, such that

$$\mathbf{d}_i=\sum_{j\in J}\mathbf{d}_j.$$

From the fact that $\mathbf{d}_i\cdot\mathbf{d}_i=\mathbf{d}_i$ and the assumption $f(\mathbf{c}_i)+f(\mathbf{c}_i+\mathbf{d}_i)=1$, it follows that

$$\bigvee_{i\in\mathbf{k+1}}\ \bigvee_{\substack{J\subseteq\mathbf{k+1}\setminus\{i\}\\ \emptyset\neq J}} f(\mathbf{c}_i)+f(\mathbf{c}_i+(\sum_{j\in J}\mathbf{d}_j)\cdot\mathbf{d}_i)=1.$$

Since the above holds for every $\mathbf{c}_1,\ldots,\mathbf{c}_{k+1},\mathbf{d}_1,\ldots,\mathbf{d}_{k+1}$ in $\mathbb{B}^n$ such that

$$\prod_{i\in\mathbf{k+1}}(f(\mathbf{c}_i)+f(\mathbf{c}_i+\mathbf{d}_i))=1$$

we conclude that f satisfies (6) and the proof of Theorem 8 is complete. □

Eq. (6) together with the equation

$$\mathbf{f}(\mathbf{z}_1+\mathbf{z}_2)=\mathbf{f}(\mathbf{z}_1)+\mathbf{f}(\mathbf{z}_2)+\mathbf{f}(\mathbf{0})$$

defining the clone L of linear functions (called affine in the terminology of linear algebra) provide an equational characterization for the class L^k of linear functions with at most $k\geq 1$ essential variables, since $L^k=L\cap E^k$. (For a recent reference to equational characterizations of Boolean clones, in particular, of clones comprising linear functions, see [11].) Theorem 9 below, provides an equation, alternative to (6), defining the subclass L^k of L and E^k.

Theorem 9. *The class L^k of linear functions with at most $k\geq 1$ essential variables is defined by*

$$\prod_{i\in\mathbf{k+1}}(\mathbf{f}(\mathbf{x}_i)+\mathbf{f}(\mathbf{0}))\longrightarrow\bigvee_{\substack{j,l\in\mathbf{k+1}\\ j<l}}(\mathbf{f}(\mathbf{x}_j\cdot\mathbf{x}_l))+\mathbf{f}(\mathbf{0}))=1. \tag{7}$$

Proof. Note that L^k is the class of linear functions which are the sum of at most $k\geq 0$ variables. First we show that if $f\in L\setminus L^k$, then f does not satisfy (7). So suppose that f is the sum of $n>k$ variables, i.e. $f=\sum_{i\in I}x_i+c$, where $c\in\{0,1\}$ and $\#I>k$. Without loss of generality, assume that $\mathbf{k}+\mathbf{1}\subseteq I$. For $i\in\mathbf{k}+\mathbf{1}$, let $\mathbf{a}_i$ be the unit n-vector with all but the ith component equal to 0. Clearly, for every $j,l\in\mathbf{k}+\mathbf{1}$ such that $j<l$, $\mathbf{a}_j\cdot\mathbf{a}_l$ is the zero-vector $\mathbf{0}$, and hence,

$$\bigvee_{\substack{j,l\in\mathbf{k+1}\\ j<l}}(f(\mathbf{a}_j\cdot\mathbf{a}_l))+f(\mathbf{0}))=0.$$

Furthermore, for every $i \in \mathbf{k}+\mathbf{1}$, $f(\mathbf{a}_i) + f(\mathbf{0}) = 1$. Thus f does not satisfy (7).

Now we show that every linear function f in L^k satisfies (7). We make use of the following

Claim 6. *Let $n \in \mathbf{k}$ and let $\mathbf{a}_1, \ldots, \mathbf{a}_{k+1}$ be $k+1$ n-vectors of odd weight. Then there are $i, j \in \mathbf{k}+\mathbf{1}$, $i \neq j$, such that $\mathbf{a}_j \cdot \mathbf{a}_i$ has odd weight.*

Proof (*Proof of Claim 6*). Let $\mathbf{a}_1, \ldots, \mathbf{a}_{k+1}$ be $k+1$ n-vectors of odd weight. Since there are at most n linearly independent n-vectors, $\mathbf{a}_1, \ldots, \mathbf{a}_{k+1}$ must be linearly dependent, i.e., there is $I \subseteq \mathbf{k}+\mathbf{1}$ and $j \in \mathbf{k}+\mathbf{1} \setminus I$ such that $\mathbf{a}_j = \sum_{i \in I} \mathbf{a}_i$. We have

$$\mathbf{a}_j = \mathbf{a}_j \cdot \mathbf{a}_j = \mathbf{a}_j \cdot \sum_{i \in I} \mathbf{a}_i = \sum_{i \in I} \mathbf{a}_j \cdot \mathbf{a}_i.$$

Since the weight of $\mathbf{a}_j$ is odd, and the weight function modulo 2 (i.e. the parity function) distributes over the component-wise sum of vectors, it follows that there is an odd number of products $\mathbf{a}_j \cdot \mathbf{a}_i$, $i \in I$, with odd weight. In particular, there are $i, j \in \mathbf{k}+\mathbf{1}$, $i \neq j$, such that $\mathbf{a}_j \cdot \mathbf{a}_i$ has odd weight. □

Let f be a linear function in L^k, say $f = \sum_{i \in \mathbf{n}} x_i + c$, where $c \in \{0, 1\}$ and $n \leq k$. Observe that $f(\mathbf{a}) + f(\mathbf{0}) = 1$ if and only if $\mathbf{a}$ has odd weight. Now, if $\mathbf{a}_1, \ldots, \mathbf{a}_{k+1}$ are $k+1$ n-vectors such that

$$\prod_{i \in \mathbf{k}+\mathbf{1}} (f(\mathbf{a}_i) + f(\mathbf{0})) = 1$$

then each $\mathbf{a}_i$, $i \in \mathbf{k}+\mathbf{1}$, has odd weight and by Claim 6 it follows that there are $i, j \in \mathbf{k}+\mathbf{1}$, $i < j$, such that $\mathbf{a}_i \cdot \mathbf{a}_j$ has odd weight, and hence,

$$\bigvee_{\substack{j,l \in \mathbf{k}+\mathbf{1} \\ j<l}} (f(\mathbf{a}_j \cdot \mathbf{a}_l) + f(\mathbf{0})) = 1$$

and the proof of Theorem 9 is complete. □

An equivalent form of Claim 6 in the proof of Theorem 9 is the following lemma of independent interest, which appears equivalently formulated in [15] as Problem 19 O (i), page 238.

Lemma 12. *If $k+1$ subsets A_i, $i \in \mathbf{k}+\mathbf{1}$ of a k-element set A have odd size, then there are $i, j \in \mathbf{k}+\mathbf{1}$, $i \neq j$, such that $A_i \cap A_j$ has odd size.*

Remark 4. The number of such pairs can be even. For an example, let $k = 4$, $A := \{0, 1, 2, 3\}$ and $A_1, \ldots, A_5$ whose corresponding vectors are $a_1 := 1110$, $a_2 := 1101$, $a_3 := 0111$, $a_4 = 1000$, $a_5 = 0001$. There are only four odd intersections, namely $A_1 \cap A_4$, $A_2 \cap A_4$, $A_2 \cap A_5$ and $A_3 \cap A_5$.

Acknowledgments

The authors would like to thank Arto Salomaa for sending a copy of the paper [19], which provided the optimal lower bound given in (2) of Lemma 4. The authors would also like to express their gratitude to the referee for his many comments and valuable suggestions to improve this manuscript.

The work of the first author was partially supported by the Graduate School in Mathematical Logic MALJA, and by grant #28139 from the Academy of Finland. The work of the second author was supported by INTAS program "Universal algebra and lattice theory".

References

[1] M. Bekkali, M. Pouzet, D. Zhani, Incidence structures and Stone–Priestley duality, Annals of Mathematics and Artificial Intelligence 49 (2007) 27–38.

[2] M. Couceiro, Galois connections for generalized functions and relational constraints, in: Proceedings of the Dresden 68th Workshop on General Algebra, Contributions to General Algebra 16 (2004) 35–54. Verlag J. Heyn, Klagenfurt, 2005.

[3] M. Couceiro, On the lattice of equational classes of Boolean functions and its closed intervals, Journal of Multiple-Valued Logic and Soft Computing 18 (2008) 81–104.

[4] M. Couceiro, S. Foldes, On closed sets of relational constraints and classes of functions closed under variable substitutions, Algebra Universalis 54 (2005) 149–165.
[5] M. Couceiro, S. Foldes, Function class composition, relational constraints and stability under compositions with clones, Rutcor Research Report 22–2004, Rutgers University. http://rutcor.rutgers.edu/˜rrr/.
[6] M. Couceiro, S. Foldes, Functional equations, constraints, definability of function classes, and functions of Boolean variables, Acta Cybernetica 18 (2007) 61–75.
[7] M. Couceiro, S. Foldes, E. Lehtonen, Composition of post classes and normal forms of Boolean functions, Discrete Mathematics 306 (2006) 3223–3243.
[8] M. Couceiro, M. Pouzet, Equational definability and a quasi-order on Boolean functions, in: The Proceedings of Second International Workshop on Boolean Functions: Cryptography and Applications BFCA' 06, Publications des Universités de Rouen et du Havre, 2006, pp. 157–174.
[9] B. Davey, H. Priestley, Introduction to Lattice and Order, Cambridge University Press, 1990.
[10] O. Ekin, S. Foldes, P.L. Hammer, L. Hellerstein, Equational characterizations of Boolean functions classes, Discrete Mathematics 211 (2000) 27–51.
[11] S. Foldes, G. Pogosyan, Post classes characterized by functional terms, Discrete Applied Mathematics 142 (2004) 35–51.
[12] L. Hellerstein, On generalized constraints and certificates, Discrete Mathematics 226 (2001) 211–232.
[13] E. Lehtonen, Order-theoretical analysis of subfunction relations between Boolean functions, Preprint, April, 2005. http://www.math.tut.fi/algebra/.
[14] E. Lehtonen, An infinite descending chain of Boolean subfunctions consisting of threshold functions, in: Contributions to General Algebra (Proceedings of AAA70, Vienna Workshop), vol. 17, 2006, pp. 145–148.
[15] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, second edition, Cambridge University Press, 2001.
[16] N. Pippenger, Theories of Computability, Cambridge University Press, Cambridge, 1997.
[17] N. Pippenger, Galois theory for minors of finite functions, Discrete Mathematics 254 (2002) 405–419.
[18] G. Pogosyan, Classes of Boolean functions defined by functional, Multiple Valued Logic 7 (2002) 417–448.
[19] A. Salomaa, On essential variables of functions, especially in the algebra of logic, Ann. Acad. Scient. Fennicae, Series A I 339, p. 11.
[20] C. Wang, Boolean minors, Discrete Mathematics 141 (1995) 237–258.
[21] I.E. Zverovich, Characterizations of closed classes of Boolean functions in terms of forbidden subfunctions and post classes, Discrete Applied Mathematics 149 (2005) 200–218.