On a quasi-ordering on Boolean functions

Miguel Couceiro and Maurice Pouzet

Abstract. It was proved few years ago that classes of Boolean functions definable by means of functional equations [9], or equivalently, by means of relational constraints [16], coincide with initial segments of the quasi-ordered set \((\Omega, \leq)\) made of the set \(\Omega\) of Boolean functions, suitably quasi-ordered. Furthermore, the classes defined by finitely many equations [9] coincide with the initial segments of \((\Omega, \leq)\) which are definable by finitely many obstructions. The resulting ordered set \((\Omega/\equiv, \subseteq)\) embeds into \(([\omega]^{<\omega}, \subseteq)\), the set -ordered by inclusion- of finite subsets of the set \(\omega\) of integers. We prove that \((\Omega/\equiv, \subseteq)\) 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 classes of Boolean functions with a bounded number of essential variables are finitely definable. We provide a concrete equational characterization of the subclasses made of linear functions. We describe the classes of functions with bounded polynomial degree in terms of minimal obstructions.

1. Introduction

Two approaches of Boolean definability have been considered recently. One in terms of functional equations [9], an other in terms of relational constraints [16]. 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 \(\Omega\) 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 from \(f\) by identifying, permuting or adding variables. These classes coincide with initial segments for this quasi-ordering called identification minor in [9], minor in [16], subfunction in [20], and simple variable substitution in [4]. Since then, greater emphasis on this quasi-ordering has emerged. For an example, it was observed that \(\Omega\) 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 \(\Omega\) contains infinite antichains (see e.g. [11, 9, 16, 10]). 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.

Date: April, 2006.

Key words and phrases: Quasi-orders, qosets, partial-orders, posets, initial segments, antichains, order-embeddings. Boolean functions, minors, essential variables, functional equations, equational classes, relational constraints, linear functions.

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 named author was supported by INTAS.
Some properties are easier to express in terms of the poset \((\Omega/\equiv,\subseteq)\) associated with the quasi-ordered set \((\Omega,\leq)\) and made of the equivalence classes associated with the equivalence \(\equiv\) defined by \(f \equiv g\) if \(f \leq g\) and \(g \leq f\). As we will see (Corollary 1), for each \(x \in \Omega/\equiv\), the initial segment \(\downarrow x := \{y \in \Omega/\equiv: y \leq x\}\) is finite, hence \((\Omega/\equiv,\subseteq)\) decomposes into the levels \(\Omega/\equiv_0,\ldots,\Omega/\equiv_n,\ldots\), where \(\Omega/\equiv_n\) is the set of minimal elements of \(\Omega/\equiv \cup \{\Omega/\equiv_m: m < n\}\). Moreover, each level is finite; for an example \(\Omega/\equiv_0\) 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 \(\varphi_{\Omega/\equiv}\), which counts for every \(n\) the number \(\varphi_{\Omega/\equiv}(n)\) of elements of \(\Omega/\equiv_n\), behave?

From the fact that for each \(x \in \Omega/\equiv\), the initial segment \(\downarrow x\) is finite it follows that initial segments of \((\Omega/\equiv,\subseteq)\) correspond bijectively to antichains of \((\Omega/\equiv,\subseteq)\). Indeed, for each antichain \(A \subseteq (\Omega/\equiv,\subseteq)\), the set \(\text{Forbid}(A) := \{y \in \Omega/\equiv: x \in A \Rightarrow x \nsubseteq y\}\) is an initial segment of \((\Omega/\equiv,\subseteq)\). Conversely, each initial segment \(I\) of \((\Omega/\equiv,\subseteq)\) is of this form (if \(A\) is the set of minimal elements of \(\Omega/\equiv \setminus I\), then since for each \(x \in \Omega/\equiv\) the set \(\downarrow x\) is finite, \(I = \text{Forbid}(A)\)). 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 \(x, y \in (\Omega/\equiv)\), 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 \(\text{Forbid}(A)\) where \(A\) runs through the finite antichains of \((\Omega/\equiv\setminus I)\) 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 \((\Omega/\equiv,\subseteq)\) and, as in this case, can be written as \(\text{Forbid}(A)\) for some antichain \(A\) of \((\Omega,\leq)\) (the difference with an initial segment of \((\Omega/\equiv,\subseteq)\)) 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 [9], 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) \(I = \text{Forbid}(A)\) 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) \(\text{Forbid}(\{f\}) \in \mathcal{F}\) for every \(f \in \Omega:\)
(3) \( \downarrow f \in \mathcal{F} \) for every \( f \in \Omega \);

(4) the class of \( f \in \Omega \) with no more than \( k \) essential variables belongs to \( \mathcal{F} \) for every integer \( k \).

Most of the Boolean clones are finitely definable (in fact, there are only 8 clones which cannot be defined by finitely many equations, see [10]). In particular, the clone of linear operations (w.r.t. the 2-element field) belongs to \( \mathcal{F} \); we give an explicit equation defining the class of linear operations with at most \( k \) essential variables (see Theorem 8). Our proof makes use of basic linear algebra over the 2-element field.

We also consider the classes \( D^k \), \( 1 \leq k \), 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 [8] 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 \( \mathcal{P}(T) \). In our case, \( \mathcal{F} \) is dually isomorphic to the sublattice of \( \mathcal{P}(\Omega/\equiv) \) generated by the final segments of the form \( \uparrow x \) for \( x \in \Omega/\equiv \). This lattice is the tail-lattice of \( (\Omega/\equiv, \subseteq) \). From the fact that \( (\Omega/\equiv, \subseteq) \) is up-closed and has finitely many minimal elements, it follows that the Priestley space of the tail-lattice of \( (\Omega/\equiv, \subseteq) \) is the set \( \mathcal{J}(\Omega/\equiv, \subseteq) \) of ideals of \( (\Omega/\equiv, \subseteq) \) ordered by inclusion and equipped with the topology induced by the product topology on \( \mathcal{P}(\Omega/\equiv) \) (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 \( \mathcal{J}(\Omega/\equiv, \subseteq) \) of ideals of \( (\Omega/\equiv, \subseteq) \) ordered by inclusion and equipped with the topology induced by the product topology on \( \mathcal{P}(\Omega/\equiv) \).

This result ask for a description of \( \mathcal{J}(\Omega/\equiv, \subseteq) \). We prove that it embeds the poset \( (\mathcal{P}(\omega), \subseteq) \), the power set of \( \omega \), ordered by inclusion.

Our proof is a by-product of an attempt to locate \( (\Omega/\equiv, \subseteq) \) 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 \( (\Omega/\equiv, \subseteq) \), we cannot answer the first question. We answer the second.

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

**Theorem 3.** \( (\Omega/\equiv, \subseteq) \) 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 $(\Omega/ \equiv, \subseteq)$ enjoys this property, it embeds into $([\omega]^{<\omega}, \subseteq)$. The proof that $([\omega]^{<\omega}, \subseteq)$ embeds into $(\Omega/ \equiv, \subseteq)$ is based on a strengthening of a construction of an infinite antichain in $(\Omega, \leq)$ given in [16].

Since $J([\omega]^{<\omega}, \subseteq)$ is isomorphic to $(\mathcal{P}(\omega), \subseteq)$, $J(\Omega/ \equiv, \subseteq)$ embeds $(\mathcal{P}(\omega), \subseteq)$, 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.

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 $\equiv$ associated to $\leq$ is defined by $x \equiv y$ 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 $\equiv$ the equivalence class of $x$ and $Q/ \equiv$ the set of equivalence classes. The image of $\leq$ via the quotient map from $Q$ into $Q/ \equiv$ (which associates $x$ to $x/ \equiv$) is an order, denoted $\subseteq$. According to our notations, we have $x < y$ if and only if $x \equiv y$. 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 $\text{Forbid}(X)$ 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 $I(Q, \equiv) = (\mathcal{P}(Q), \subseteq)$. An ideal of $Q$ is a non-empty 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 $J(Q, \leq)$ 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 $J([\omega]^{<\omega}, \subseteq)$ is isomorphic to $(\mathcal{P}(\omega), \subseteq)$.
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 poset the quotient map from $Q$ onto $Q/\equiv$ induces an isomorphism from $I(Q, \leq)$ onto $I(Q/\equiv, \subseteq)$ and from $\mathcal{J}(Q, \leq)$ onto $\mathcal{J}(Q/\equiv, \subseteq)$.

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 $\text{Min}(P)$ the subset of $P$ made of minimal elements of $P$. Define inductively the sequence $(P_n)_{n \in \mathbb{N}}$ setting $P_0 := \text{Min}(P)$ and $P_n := \text{Min}(P \setminus \bigcup\{P_{n'} : n' < n\})$. For each integer $n$, the set $P_n$ is an antichain, called a level of $P$. If $P_n$ is non-empty, 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, set $\varphi(x) := \downarrow x$. This defines an embedding from $(P, \leq)$ into $([\omega]^{<\omega}, \subseteq)$.

### 2.2. Boolean functions

Let $\mathbb{B} := \{0, 1\}$. 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 $\Omega$ denotes the set $\bigcup_{n \geq 1} \mathbb{B}^n$ of all Boolean functions. For $i, n \in \mathbb{N}^*$ with $i \leq n$, define the $i$-th $n$-ary projection $e^n_i$ by setting $e^n_i(a_1, \ldots, a_n) := a_i$. Set $I := \{e^n_i : i, n \in \mathbb{N}^*\}$. 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 $a \in \mathbb{B}^m$ is $f(g_1(a), \ldots, g_n(a))$. 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 further extensions see e.g. [7, 4, 5, 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
In Corollary 1.

Proof. According to the above lemma, for every $p_1, \ldots, p_n \in I_c$ such that $g = f(p_1, \ldots, p_n)$. In other words,

$$g \leq f$$

if and only if $g \circ I_c \subseteq f \circ I_c$.

Thus $\leq$ constitutes a quasi-order on $\Omega$. If $g \leq f$ and $f \leq g$, then $g$ and $f$ are said to be equivalent, $g \equiv f$. Let $\Omega/ \equiv$ denote the set of all equivalent classes of Boolean functions and let $\sqsubseteq$ denote the partial-order induced by $\leq$. A class $K \sqsubseteq \Omega$ 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 $K/ \equiv$ is an initial segment of $\Omega/ \equiv$. (For an early reference on the quasi-order $\leq$ see e.g. [19] and for further background see [9, 16, 20, 4, 2, 3]. For variants and generalizations see e.g. [5, 6, 11, 12, 13].)

2.3. Definability of Boolean function classes by means of functional equations. A functional equation (for Boolean functions) is a formal expression

$$h_1(f(g_1(x_1, \ldots, x_p)), \ldots, f(g_m(x_1, \ldots, x_p))) = h_2(f(g'_1(x_1, \ldots, x_p)), \ldots, f(g'_m(x_1, \ldots, x_p)))$$

(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 $x_1, \ldots, x_p$ are $p$ distinct vector variable symbols, and $f$ is a distinct function symbol. Such equations were systematically studied in [9]. See e.g. [17, 10, 16] 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 the equation (1) if, for all $v_1, \ldots, v_p \in \mathbb{B}^n$, we have

$$h_1(f(g_1(v_1, \ldots, v_p)), \ldots, f(g_m(v_1, \ldots, v_p))) = h_2(f(g'_1(v_1, \ldots, v_p)), \ldots, f(g'_m(v_1, \ldots, v_p)))$$

Lemma 4.

(1) If $g < f$ then $\text{ess}(g) < \text{ess}(f)$;

(2) Saloama [18]: For every Boolean function $f$ we have

$$\max\{\text{ess}(g) : g < f\} \geq \text{ess}(f) - 2.$$

Corollary 1. In $(\Omega/ \equiv, \sqsubseteq)$ every principal initial segment is finite and each level is finite.

Proof. According to the above lemma, for every $n \geq 1$, and for each Boolean function $f$ in the $n$-th level, we have $n < \text{ess}(f) \leq 2n + 1$. The result follows. □
where $g_1(v_1, \ldots, v_p)$ is interpreted component-wise, that is,

$$g_1(v_1, \ldots, v_p) = (g_1(v_1(1), \ldots, v_p(1)), \ldots, g_1(v_1(n), \ldots, v_p(n))).$$

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.

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 [9]. For variants and extensions, see e.g. [10, 17, 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 $K/\equiv$ is an initial segment of $\Omega/\equiv$.

### 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

$$fR = \{f(v_1, \ldots, v_n) : v_1, \ldots, v_n \in R\}$$

where the $m$-vector $f(v_1, \ldots, v_n)$ 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 [16]. See also [2, 4, 5, 6, 11], for further variants and extensions.

The connection between definability by functional equations and by relational constraints was made explicit by Pippenger who established in [16] 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 proof of Theorem 1 in [6], and show that for each functional equational (1), there is a relational constraint satisfied by exactly the same Boolean functions satisfying (1) 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 functional equation (1), let \((R, S)\) be the relational constraint defined by

\[
R := \{(g_1(a), \ldots, g_m(a), g'_1(a), \ldots, g'_r(a)) : a \in \mathbb{B}^p\},
\]

\[
S := \{(b_1, \ldots, b_m, b'_1, \ldots, b'_r) \in \mathbb{B}^{m+r} : h_1(b_1, \ldots, b_m) = h_2(b'_1, \ldots, b'_r)\}.
\]

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 \(a_1, \ldots, a_n \in R\),

\[
h_1(f(a_1(1), \ldots, a_n(1)), \ldots, f(a_1(m), \ldots, a_n(m))) =
= h_2(f(a_1(m + 1), \ldots, a_n(m + 1)), \ldots, f(a_1(m + t), \ldots, a_n(m + t))).
\]

Since \(R\) is the range of \(g = (g_1, \ldots, g_m, g'_1, \ldots, g'_r)\), we have that \(f\) satisfies \((R, S)\) if and only if for every \(v_1, \ldots, v_p \in \mathbb{B}^n\)

\[
h_1(f(g_1(v_1, \ldots, v_p)), \ldots, f(g_m(v_1, \ldots, v_p))) =
= h_2(f(g'_1(v_1, \ldots, v_p)), \ldots, f(g'_r(v_1, \ldots, v_p))).
\]

In other words, \(f\) satisfies \((R, S)\) if and only if \(f\) satisfies (1).

Conversely, let \((R, S)\) be a relational constraint. We may suppose \(R\) non-empty, indeed, constraints with empty antecedent are satisfied by every Boolean function, and thus they can be discarded as irrelevant. With the help of the following two facts, we will construct a functional equation satisfied by exactly the same functions as those satisfying \((R, S)\).

**Fact 1.** For each non-empty Boolean relation \(R \subseteq \mathbb{B}^m\), there is a \(p \geq 1\) and a map \(g := (g_1, \ldots, g_m)\), where each \(g_i\) is a \(p\)-ary Boolean function \(g_i : \mathbb{B}^p \to \mathbb{B}\), such that the range of \(g\) is \(R\).

**Fact 2.** For each Boolean relation \(S \subseteq \mathbb{B}^m\), there exist maps \(h_1, h_2 : \mathbb{B}^m \to \mathbb{B}\), such that

\[
S = \{b \in B^m : h_1(b) = h_2(b)\}.
\]

Let \((R, S)\) be a relational constraint. Consider the functional equation

\[
h_1(f(g_1(x_1, \ldots, x_p)), \ldots, f(g_m(x_1, \ldots, x_p))) =
= h_2(f(g_1(x_1, \ldots, x_p)), \ldots, f(g_m(x_1, \ldots, x_p)))
\] (2)

where the \(g_i\)'s and \(h_j\)'s are the maps given in Fact 1 and Fact 2. Let \(f\) be an \(n\)-ary Boolean function. By construction, we have that \(f\) satisfies (2) if and only if for every \(v_1, \ldots, v_p \in \mathbb{B}^n\), \((f(g_1(v_1, \ldots, v_p)), \ldots, f(g_m(v_1, \ldots, v_p))) \in S\). From the fact that \(R\) is the range of \((g_1, \ldots, g_m)\), it follows that \(f\) satisfies (2) if and only if \(f\) satisfies \((R, S)\).

In the sequel, we will make use of the following result of Pippenger ([16], Theorem 2.1). For the reader’s convenience, we provide a proof.

**Lemma 5.** For each Boolean function \(f\), there is a relational constraint \((R, S)\) such that \(\Omega(R, S) = \text{Forbid}(\{f\})\).
Proof. Let $f$ be Boolean function, say of arity $n$. Let $v_1,\ldots,v_n$ be $2^n$-vectors such that $\mathbb{B}^n = \{(v_1(i),\ldots,v_n(i)) : 1 \leq i \leq 2^n\}$. Consider the $2^n$-ary relations $R_f$ and $S_f$ given by

$$R := \{v_1,\ldots,v_n\}, \quad S_f := \bigcup \{gR_f : g \in Forbid(\{f\})\}$$

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

$$f = g'(p_1,\ldots,p_m)$$

(3)

We claim that $g'(p_1(v_1,\ldots,v_n),\ldots,p_m(v_1,\ldots,v_n))$ does not belong to $S_f$. Otherwise, there would be $g \in Forbid(\{f\})$, and projections $p'_1,\ldots,p'_m$ such that

$$g'(p_1(v_1,\ldots,v_n),\ldots,p_m(v_1,\ldots,v_n)) = g(p'_1(v_1,\ldots,v_n),\ldots,p'_m(v_1,\ldots,v_n)).$$

By definition, this amounts to

$$g'(p_1(v_1,\ldots,v_n)(i),\ldots,p_m(v_1,\ldots,v_n)(i)) = g(p'_1(v_1,\ldots,v_n)(i),\ldots,p'_m(v_1,\ldots,v_n)(i))$$

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

$$g'(p_1(v_1(i),\ldots,v_n(i)),\ldots,p_m(v_1(i),\ldots,v_n(i))) = g(p'_1(v_1(i),\ldots,v_n(i)),\ldots,p'_m(v_1(i),\ldots,v_n(i))).$$

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

$$(v_1(i),\ldots,v_n(i)) = (x_1,\ldots,x_n)$$

we get

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

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

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

With equation (3) we get $f = g(p'_1,\ldots,p'_m)$ that is $f$ is obtained from $g$ by simple variable substitutions, contradicting our assumption $g \in Forbid(\{f\})$. \qed

Now we can present a proof of Theorem 1.

Proof of Theorem 1. We show that $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

$(i) \Rightarrow (ii)$ To see that each class $I \in \mathcal{F}$ can be defined by a single functional equation, note that

$$h_1(f(g_1(x_1,\ldots,x_p)),\ldots,f(g_m(x_1,\ldots,x_p))) = h_2(f(g'_1(x_1,\ldots,x_p)),\ldots,f(g'_m(x_1,\ldots,x_p)))$$

(1)

is satisfied by exactly the same functions satisfying

$$h_1(f(g_1(x_1,\ldots,x_p)),\ldots,f(g_m(x_1,\ldots,x_p))) + h_2(f(g'_1(x_1,\ldots,x_p)),\ldots,f(g'_m(x_1,\ldots,x_p))) = 0$$

where $+$ denotes the sum modulo 2. Thus, if $I$ is defined by the equations $H_1 = 0,\ldots,H_n = 0$, then it is also defined by $\bigvee_{1 \leq i \leq n} H_i = 0$. 


(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 $H = 0$.

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

**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 of Claim 1.** If $m \leq 2^n$ set $g' := g$. If not, let $v_1, \ldots, v_m \in R$ such that $g(v_1, \ldots, v_m) \not\in S$. Say that two indices $i, j$ with $1 \leq i, j \leq m$ are equivalent if $v_i = v_j$. Let $C_1, \ldots, C_m'$ be an enumeration of the equivalence classes. For each $i, 1 \leq i \leq m$, 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 $1 \leq j \leq m'$, let $w_j := v_{c(j)}$, 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 $(R, S)$.

Form 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 $I := \text{Forbid}(A)$ where $A$ is a finite antichain. Since $I$ is a finite intersection of sets of the form $\text{Forbid}([f])$, in order to get that $I \in \mathcal{F}$, it suffices to show that $\text{Forbid}([f]) \in \mathcal{F}$. By Lemma 5, $\text{Forbid}([f])$ is defined by a single constraint. As shown in the proof of Theorem 5, this is equivalent to say that $\text{Forbid}([f])$ is defined by a single equation, and thus $\text{Forbid}([f]) \in \mathcal{F}$. □

3. **Proof of Lemma 1**

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

$$H_1 = 0 \text{ and } H_2 = 0$$

respectively, then $K_1 \cup K_2$ and $K_1 \cap K_2$ are defined by

$$H_1 \land H_2 = 0 \text{ and } H_1 \lor H_2 = 0$$

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) ⇒ (iii) of Theorem 1. Note that from this equivalence and the fact that $\mathcal{F}$ is closed under finite unions, it follows that $\Omega/\equiv$ is up-closed.

Statement (2). Implication (iii) ⇒ (i) of Theorem 1.

Statement (3). Let $f \in \Omega$. Let $\overline{f}$ be its image in $P := (\Omega/\equiv, \subseteq)$ (i.e., the equivalence class containing $f$), and $m := h(\overline{f}, P)$. The initial segment $\downarrow f$ is of the form $\text{Forbid}(A)$ for some antichain $A$. This antichain $A$ is made of representative
of the minimal elements of $B := P \setminus \mathcal{F}$. If $y$ is minimal in $B$ then for every $x$ such that $x < y$, we have $x \leq \mathcal{F}$. It follows that $h(y, P) \leq h(\mathcal{F}, P) + 1 = m + 1$, 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.

Statement (4). Let $E^k$ be the set of operations with at most $k$ essential variables. Its image $E^k$ in $P := (\Omega/\equiv, \sqsubseteq)$ is in fact included into the union of all levels $P_n$ for $n \leq k$. Since by Corollary 1, all levels are finite, $E^k$ is a finite union of initial segments of the form $\downarrow f$. According to Statement (1) and Statement (3), $E^k \in \mathcal{F}$.

4. Proof of Theorem 3

Let $P := (\Omega/\equiv, \sqsubseteq)$.

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 [16].

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 $p_0, \ldots, p_n \in I$ such that $u_m = u_n(p_0, \ldots, p_n)$. Note that for every $m \geq 4$, $u_n(1, x_1, \ldots, x_m) = f_n(x_1, \ldots, x_m)$ 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 $1 \leq k \leq n$, $p_k(x_0, \ldots, x_m) \neq x_0$, then by taking $x_0 = 1$ we would conclude that $f_m \leq f_n$, contradicting Lemma 7. If there is $1 \leq k \leq n$ such that $p_k(x_0, \ldots, x_m) = x_0$, then by taking $x_i = 1$ if and only if $i = 0, 1$, we would have

$$u_m(x_0, \ldots, x_m) = 1 \neq 0 = u_n(x_0, p_1(x_0, \ldots, x_m), \ldots, p_n(x_0, \ldots, x_m))$$

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 \( 1 \leq j \leq m \). But then by taking \( x_i = 1 \) if and only if \( i = 0, k \), for some \( 1 \leq k \leq m \) such that \( k \neq j \), we would have
\[
\begin{align*}
   u_m(x_0, \ldots, x_i, \ldots, x_m) &= 1 \\
   0 &= u_n(x_1, p_1(x_0, \ldots, x_m), \ldots, p_n(x_0, \ldots, x_m)) = 0
\end{align*}
\]
which contradicts our assumption \( u_m \leq u_n \). \( \square \)

Let \( I \) be a non-empty finite set of integers greater or equal than 4, and let \( g_I \) be the \( \sum_{i \in I} i \)-ary function given by
\[
g_I = \sum_{i \in I} f_i(x_1^i, \ldots, x_i^i) \cdot \prod_{j \in I \setminus \{i\} : 1 \leq k \leq j} x_k^j
\]
Observe that
\begin{itemize}
   \item By identifying all \( x_i^j \) to \( x_0 \), for \( j \in I \setminus \{i\} \) and \( 1 \leq k \leq j \), we obtain \( x_0 \cdot f_i(x_1^i, \ldots, x_i^i) \), and
   \item \( g_I = 1 \) if and only if there exactly one \( i \in I \) such that
      \begin{enumerate}
         \item \( \prod_{j \in I \setminus \{i\} : 1 \leq k \leq j} x_k^j = 1 \)
      \end{enumerate}
\end{itemize}

**Proposition 1.** Let \( I \) be a non-empty finite set of integers greater or equal than 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 \( u_k \leq g_I \).

**Proof.** By the first observation above it follows that if \( n \in I \) then \( u_n \leq g_I \). To prove the converse, suppose that \( n \notin I \) and for a contradiction suppose that \( u_n \leq g_I \), i.e., there are projections \( p_k(x_0, x_1, \ldots, x_n), i \in I \) and \( 1 \leq k \leq i \), such that
\[
u_n = \sum_{i \in I} f_i(p_1^i, \ldots, p_i^i) \cdot \prod_{j \in I \setminus \{i\} : 1 \leq k \leq j} p_k^j
\]
(4)
Consider the vector \((a_0, a_1, \ldots, a_n)\) given by \( a_l = 1 \) iff \( l = 0, 1 \). Clearly, \( u_n(a_0, a_1, \ldots, a_n) = 1 \) and, in order to have (4) = 1, there must exist exactly one \( i \in I \) such that
\begin{itemize}
   \item \( \prod_{j \in I \setminus \{i\} : 1 \leq k \leq j} x_k^j = 1 \)
   \item \( \prod_{j \in I \setminus \{i\} : 1 \leq k \leq j} p_k^j \in \{x_0, x_1\} \)
\end{itemize}
Since \( x_2, \ldots, x_n \) are essential in \( u_n \), we also have that for each \( 2 \leq l \leq n \), there is \( 1 \leq k \leq i \) such that \( p_k^l = x_l \).

Now, if for all \( 1 \leq k \leq i \), \( p_k^l \neq x_1 \), then there are \( j \in I \setminus \{i\} \) and \( 1 \leq k \leq j \), such that \( p_k^l = x_1 \), because \( x_1 \) is essential in \( u_n \). Consider \((b_0, b_1, \ldots, b_n)\) given by \( b_l = 1 \) iff \( l = 0, 2 \). We have \( u_n(b_0, b_1, \ldots, b_n) = 1 \), but (4) = 0, which constitutes a contradiction.

Thus, there is \( 1 \leq k \leq i \), \( p_k^l = x_1 \). If there is \( 1 \leq t \leq i \) such that \( p_t^l = x_0 \), then for \((b_0, b_1, \ldots, b_n)\) given by \( b_l = 1 \) iff \( l = 0, 1 \), we have \( u_n(b_0, b_1, \ldots, b_n) = 1 \), but (4) = 0, because for each \( 2 \leq l \leq n \), there is \( 1 \leq r \leq i \) such that \( p_r^l = x_1 \) and \( n \geq 4 \). Hence, for every \( 1 \leq t \leq i \), \( p_t^l \neq x_0 \), and since for each \( 2 \leq l \leq n \), there is \( 1 \leq r \leq i \) such that \( p_r^l = x_1 \), we must have \( i \neq n \). Also, \( n \notin I \) and thus \( i > n \). But in this case, there must exist \( 1 \leq r_1 < r_2 \leq i \),
ON A QUASI-ORDERING ON BOOLEAN FUNCTIONS

\[ p_{r_1} = p_{r_2} = x_s. \] Now, if \( s = 1 \), then for \((b_0, b_1, \ldots, b_n)\) given by \( b_l = 1 \) if \( l = 0, 1 \), we have \( u_n(b_0, b_1, \ldots, b_n) = 1 \) and \((4) = 0\), once again by the fact that for each \( 2 \leq l \leq n \), there is \( 1 \leq r \leq i \) such that \( p_{r_l} = x_l \). If \( 1 < s \leq n \), then for \((b_0, b_1, \ldots, b_n)\) given by \( b_l = 1 \) if \( l \neq s \), we have \( u_n(b_0, b_1, \ldots, b_n) = 1 \) and \((4) = 0\).

Since in all possible cases we derive the same contradiction, the proof of the proposition is complete. \( \square \)

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

5. Boolean functions with bounded polynomial degree

A multilinear monomial is a term of the form

\[ \overrightarrow{x}_I = \prod_{i \in I} x_i, \]

for some finite set \( I \). The size \( |I| \) is called the degree of \( \overrightarrow{x}_I \). A multilinear polynomial is a sum of monomials and its degree is the largest degree of its monomials. We convention that 0 is a multilinear monomial, and that 1 is the empty monomial \( \overrightarrow{x}_\emptyset \).

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.

\[ f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1, \ldots, n\}} a_I \cdot \overrightarrow{x}_I \]

where each \( a_I \) belongs to \( \mathbb{B} \).

**Lemma 9.** If \( f \) is uniquely represented by the multilinear polynomial

\[ \sum_{I \subseteq \{1, \ldots, n\}} a_I \cdot \overrightarrow{x}_I \]

then for \( a_I \neq 0 \), the variables occurring in \( \overrightarrow{x}_I \) 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 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 \( \text{Critical}(K) \) the set of minimal elements of \( \Omega \setminus K/\equiv \). Observe that

\[ K/\equiv = \text{Forbid(Critical}(K)). \]

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

**Theorem 6.** For each \( k \geq 2 \), an equivalence class \( \overline{g} \), of a Boolean function \( g \), is in \( \text{Critical}(D^k) \) if and only if \( g \equiv r \), for \( r = p + q \) where
\[(1) \ p = x_1 \cdot \ldots \cdot x_k \text{ or} \]
\[p = \sum_{i \in I} \overrightarrow{A}_{f_n(i)}, \text{ where } I = \{1, \ldots, k + 1\} \]
\[\text{(2) } \deg(q) < k \text{ and all variables occurring in } q \text{ occur in } p.\]

The set \(\text{Critical}(D^k)\) consists of the equivalence classes of \(x_1 \cdot x_2 + x_1, x_1 + x_2, x_1 \text{ and } x_1 \cdot x_2 + x_1 + 1, x_1 + x_2 + 1, x_1 + 1\).

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

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

If \(p = x_1 \cdots x_k\) then this term becomes a term of degree \(k - 1\). If

\[p = \sum_{i \in I} \overrightarrow{A}_{f_n(i)}, \text{ where } I = \{1, \ldots, k + 1\} \]

then the polynomial \(p_{x_j = x_i}\), obtained from \(p\) by identifying \(x_j\) to \(x_i\), also becomes a term of degree \(k - 1\). Thus, if \(g \equiv r\), for \(r = p + q\), then \(\overrightarrow{g}\) is in \(\text{Critical}(D^k)\).

To show that the converse also holds, we shall make use of the following two claims.

Claim 2. For each \(k \geq 2\), \(D^k = \text{Forbid}(A)\) for some antichain \(A\) containing only functions with degree equal to \(k\).

Proof. It suffices to show that if \(f \not\in D^k\), 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 \(n - 1\). In view of Lemma 9, 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

\[C = \overrightarrow{A}_I, \text{ where } I = \{1, \ldots, n\} \]

Consider the monomials \(\overrightarrow{A}_{I \setminus \{1\}}, \overrightarrow{A}_{I \setminus \{2\}}, \overrightarrow{A}_{I \setminus \{3\}}\). If at least two appear in the polynomial representation of \(f\), say \(\overrightarrow{A}_{I \setminus \{1\}}\) and \(\overrightarrow{A}_{I \setminus \{2\}}\), then by choosing \(i = 1\) and \(j = 2\), it follows that \(\overrightarrow{A}_{I \setminus \{1\}}\), appears in the polynomial representation of \(f_{x_1 = x_2}\), and thus \(f_{x_1 = x_2}\) has degree at least \(n - 1\) as desired. Similarly, if \(\overrightarrow{A}_{I \setminus \{1\}}\) and \(\overrightarrow{A}_{I \setminus \{3\}}\), or \(\overrightarrow{A}_{I \setminus \{2\}}\) and \(\overrightarrow{A}_{I \setminus \{3\}}\), 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 appears in the polynomial representation of \(f\), say \(\overrightarrow{A}_{I \setminus \{1\}}\). In this case, \(\overrightarrow{A}_{I \setminus \{2\}}\) 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 \(\overrightarrow{A}_{I \setminus \{1\}}\) or \(\overrightarrow{A}_{I \setminus \{3\}}\), 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 3. Let $D^k = \text{Forbid}(A)$, for some antichain $A$. If $A$ is made of minimal functions, then each function in $A$ has at most $k + 1$ essential variables.

Proof. By the previous claim, $A$ contains only functions with degree equal to $k$. For a contradiction, suppose that there is $f \in A$ with more than $k + 1$ variables. 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. \hfill $\Box$

Suppose that $\overline{g} \in \text{Critical}(K)$. By Claims 2 and 3, we may assume that $g$ has degree $k$, and has either $k$ or $k + 1$ essential variables. Let $r \equiv g$ with essential variables $x_1, \ldots, x_k$ or $x_1, \ldots, x_{k+1}$. Let $p$ the sum of the monomials in $r$ 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 we can identify that variable of $q$ with a variable of $p$, and obtain a function $f < r \equiv g$ with degree $k$, and hence not in $D^k$, 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 $p = x_1 \cdots x_k$ or, for $I = \{1, \ldots, k+1\}$

$$p = \sum_{i \in I} \overline{x}_I \setminus \{i\}.$$ 

For a contradiction, suppose that $p$ does not have neither the former nor the latter expressions. Let $I' \subseteq I$ with $1 \not\in |I'| < k + 1$, such that for every $i \in I'$, $\overline{x}_{I' \setminus \{i\}}$ is a monomial of $p$, and let $j \in I$ such that $\overline{x}_{I \setminus \{j\}}$ 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 $t \in I' \setminus \{l\}$, $\overline{x}_{I' \setminus \{j\}}$ is a monomial of $p_{x_j = x_l}$ with degree $k - 1$. But the monomial $\overline{x}_{I \setminus \{j\}}$ 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 $f < r \equiv g$ 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 $x_1 \cdot x_2 + x_1, x_1 \cdot x_2 + x_1$, and $x_1 \cdot x_2 + x_1 + 1, x_1 + x_2 + 1$ are indeed $\text{Critical}(D^1)$. 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 $\overline{g} \in \text{Critical}(D^1)$ 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. Thus $g \in \Omega \setminus D^2$, and from Claim 2 it follows that $g' < g$, for some $\overline{g'} \in \text{Critical}(D^2)$. Since $g' \in \Omega \setminus D^2$, this contradicts the minimality of $g$, and the proof of Theorem 6 is complete. \hfill $\Box$

Remark 1. The procedure given in the proof of Claim 2, 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

$$\sum_{I \subseteq \{1, \ldots, k\}} f(\sum_{i \in I} x_i) = 0$$

6. Linear functions with a bounded number of essential variables

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

$$\prod_{1 \leq i \leq k+1} (f(x_i) + f(0)) \longrightarrow \bigvee_{1 \leq j < l \leq k+1} (f(x_j \cdot x_l)) + f(0) = 1$$

(5)

**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 (5). So suppose that $f$ is the sum of $n > k$ variables. Without loss of generality, assume that $f = x_1 + \ldots + x_{k+1} + c_{k+2}x_{k+2} + \ldots + c_nx_n + c$, where $c_{k+2}, \ldots, c_n, c \in \{0, 1\}$. For $1 \leq i \leq k+1$, let $a_i$ be the unit $n$-vector with all but the $i$-th component equal to 0. Clearly, for every $1 \leq j < l \leq k+1$, $a_j \cdot a_l$ is the zero-vector 0, and hence,

$$\bigvee_{1 \leq j < l \leq k+1} (f(a_j \cdot a_l)) + f(0) = 0$$

Furthermore, for every $1 \leq i \leq k+1$, $f(a_i) + f(0) = 1$. Thus $f$ does not satisfy (5).

Now we show that every linear function $f$ in $L_k$ satisfies (5). We make use of the following

**Claim 4.** Let $1 \leq n \leq k$ and let $a_1, \ldots, a_{k+1}$ be $k+1$ $n$-vectors of odd weight. Then there are $1 \leq i, j \leq k+1$, $i \neq j$, such that $a_j \cdot a_i$ has odd weight.

**Proof of Claim 4.** Let $a_1, \ldots, a_{k+1}$ be $k+1$ $n$-vectors of odd weight. Since there are at most $n$ linearly independent $n$-vectors, $a_1, \ldots, a_{k+1}$ must be linearly dependent, i.e., there is $I \subseteq \{1, \ldots, k+1\}$ and $j \in \{1, \ldots, k+1\} \setminus I$ such that $a_j = \sum_{i \in I} a_i$. We have

$$a_j = a_j \cdot a_j = a_j \cdot \sum_{i \in I} a_i = \sum_{i \in I} a_j \cdot a_i$$

Since the weight of $a_j$ 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 $a_j \cdot a_i$, $i \in I$, with odd weight. In particular, there are $1 \leq i, j \leq k+1$, $i \neq j$, such that $a_j \cdot a_i$ has odd weight. □
Let \( f \) be a linear function in \( L^k \), say \( f = x_1 + \ldots + x_n + c \), where \( c \in \{0, 1\} \) and \( 1 \leq n \leq k \). Observe that \( f(a) + f(0) = 1 \) if and only if \( a \) has odd weight. Now, if \( a_1, \ldots, a_{k+1} \) are \( k+1 \) \( n \)-vectors such that

\[
\prod_{1 \leq i \leq k+1} (f(a_i) + f(0)) = 1
\]

then each \( a_i, 1 \leq i \leq k+1 \), has odd weight and by Claim 4 it follows that there are \( 1 \leq i < j \leq k+1 \) such that \( a_i \cdot a_j \) has odd weight, and hence,

\[
\bigvee_{1 \leq j < i \leq k+1} (f(a_j \cdot a_i) + f(0)) = 1
\]

and the proof of Theorem 8 is complete. \( \Box \)

An equivalent form of Claim 4 in the proof of Theorem 8 is the following lemma of independent interest, which appears equivalently formulated in [14] as Problem 19 O (i), page 238.

**Lemma 10.** If \( k+1 \) subsets \( A_i, 1 \leq i \leq k+1 \) of a \( k \)-element set \( A \) have odd size, then there are \( 1 \leq i, j \leq k+1 \), \( i \neq j \), such that \( A_i \cap A_j \) has odd size.

**Remark 2.** 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 \( A_3 \cap A_5 \).

7. Acknowledgment

The authors would like to thank Arto Salomaa for sending a copy of the paper [18], which provided the optimal lower bound given in (2) of Lemma 4.

References


Department of Mathematics, Statistics and Philosophy, University of Tampere, Kanslerinrinne 1, 33014 TAMPERE, FINLAND

E-mail address: Miguel.Couceiro@uta.fi

PCS, Université Claude-Bernard Lyon1, Domaine de Gerland -bât. Recherche [B], 50 avenue Tony-Garnier, F69365 Lyon cedex 07, FRANCE

E-mail address: pouzet@univ-lyon1.fr