ELSEVIER

Discrete Mathematics 211 (2000) 27–51

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Equational characterizations of Boolean function classes

Oya Ekin[a,1] Stephan Foldes[b,2], Peter L. Hammer[b,3], Lisa Hellerstein[c,*,4]

[a] *Department of Industrial Engineering, Bilkent University, Ankara, Turkey*
[b] *RUTCOR, Rutgers University, 640 Bartholomew Rd., Piscataway, NJ 08854-8003, USA*
[c] *Department of Computer and Information Science, Polytechnic University, 5 Metrotech Center, Brooklyn, NY 11201, USA*

Received 10 February 1998; revised 23 February 1999; accepted 2 November 1999

Abstract

Several noteworthy classes of Boolean functions can be characterized by algebraic identities (e.g. the class of positive functions consists of all functions f satisfying the identity $f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x} \vee \boldsymbol{y})$). We give algebraic identities for several of the most frequently analyzed classes of Boolean functions (including Horn, quadratic, supermodular, and submodular functions) and proceed then to the general question of which classes of Boolean functions can be characterized by algebraic identities. We answer this question for function classes closed under addition of inessential (irrelevant) variables. Nearly all classes of interest have this property. We show that a class with this property has a characterization by algebraic identities if and only if the class is closed under the operation of variable identification. Moreover, a single identity suffices to characterize a class if and only if the number of minimal forbidden identification minors is finite. Finally, we consider characterizations by general first-order sentences, rather than just identities. We show that a class of Boolean functions can be described by an appropriate set of such first-order sentences if and only if it is closed under permutation of variables.

* Corresponding author.
E-mail addresses: karasan@bilkent.edu.tr (O. Ekin), sfoldes@mba1981.hbs.edu (S. Foldes), hammer@rutcor.rutgers.edu (P.L. Hammer), hstein@duke.poly.edu. (L. Hellerstein)

[1] Part of this author's work was done at the National Autonomous University of Mexico (UNAM) in August 1997. Partially supported by RUTCOR and DIMACS.
[2] Partially supported by ONR grants N0001492J1375 and N0001492J4083 and by DIMACS.
[3] Partially supported by NSF Grant CCR-9501660, RUTCOR, and DIMACS.
[4] Partially supported by ONR grants N0001492J1375 and N0001492J4083 and by DIMACS. Part of this author's work was done at RUTCOR.

0012-365X/00/$ - see front matter
PII: S0012-365X(99)00132-6

1. Introduction

Classes of Boolean functions may be specified in different ways. For example, consider the class of positive (i.e., monotone non-decreasing) functions. The following are among the many ways to describe positive functions:

(a) functions that can be expressed by a disjunctive normal form containing no negated variables

(b) functions f such that

$$\forall \boldsymbol{x}, \boldsymbol{y} \quad \boldsymbol{x} \leqslant \boldsymbol{y} \;\Rightarrow\; f(\boldsymbol{x}) \leqslant f(\boldsymbol{y})$$

(c) functions f such that

$$\forall \boldsymbol{x}, \boldsymbol{y} \quad f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x} \vee \boldsymbol{y})$$

Here our interest is principally in equational characterizations, such as (c). Characterization (c) has a particularly simple form; it is a universally quantified sentence without connectives in a certain first-order language with no relation symbol other than identity (=).

In this paper we

- provide equational characterizations for a number of Boolean function classes (Section 3),
- provide a necessary and sufficient condition for a class to have an equational characterization that uses universal quantifiers but no existential quantifiers, if the class is closed under addition of inessential (irrelevant) variables (Section 4),
- show that for every class closed under permutation of variables, there is a characterization of the class that consists of an appropriate set of first-order sentences (with identity as the only relation symbol, but not necessarily universally quantified) (Section 5).

We also give conditions for a class to have a *finite* equational characterization (Section 4.3), and consider characterizations of renamable analogues of common classes (Section 5).

A universal algebraic proof of the results of Section 4 (Propositions 4.1–4.3), establishing a connection with the Birkhoff-Tarski HSP Theorem, was given by one of the co-authors of this paper, Foldes [5].

This paper deals only with classes of Boolean functions. Recently, Pippenger extended results from Section 4 to apply to classes of functions of the form $f : \{0,\ldots,k-1\}^n \to \{0,\ldots,l-1\}$, for fixed $k, l \geqslant 2$ (Boolean functions are the special case $k = l = 2$) [13]. He also presented an alternative proof of Propositions 4.1–4.3 of this paper.

2. Preliminaries

This section reviews some standard terminology and introduces several terms particular to this paper. The standard terminology is taken from the theory of Boolean functions, and also from first-order logic, universal algebra, and the theory of lattices.

Additional background information can be found in Sections 30 and 10 of [16], the first three chapters of [1], the first three chapters of [10], and Chapters VIII and XI of [4]. The theory and application of Boolean and pseudo-Boolean functions is discussed in [8,11,12,15].

2.1. Boolean functions

For every positive integer n, the set $\{0,1\}^n = B^n$ is a Boolean lattice where a binary n-vector $\boldsymbol{x} = (x_1, \ldots, x_n)$ is less than or equal to $\boldsymbol{y} = (y_1, \ldots, y_n)$ if and only if $\forall i\ x_i \leqslant y_i$. For $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$, $\boldsymbol{x} \wedge \boldsymbol{y}$ denotes the binary meet (bitwise **and**) of $\boldsymbol{x}$ and $\boldsymbol{y}$, and $\boldsymbol{x} \vee \boldsymbol{y}$ denotes the binary join (bitwise **or**) of $\boldsymbol{x}$ and $\boldsymbol{y}$. Complementation of $\boldsymbol{x} \in \{0,1\}^n$ is denoted $\neg \boldsymbol{x}$ or $\bar{\boldsymbol{x}}$. Clearly,

$$\boldsymbol{x} \leqslant \boldsymbol{y} \ \Leftrightarrow\ \boldsymbol{x} \vee \boldsymbol{y} = \boldsymbol{y}$$

Under the standard definition, a Boolean function is a map f from a finite Boolean lattice B^n, $n \geqslant 1$, to the set $\{0,1\}$. To simplify the exposition of our results, we define a Boolean function to be a map from B^n to B^n as follows: A *Boolean function* is a map f from a finite Boolean lattice $\{0,1\}^n = B^n$, $n \geqslant 1$, into itself such that the possible values of f are confined to the minimum $[0, \ldots, 0]$ and the maximum $[1, \ldots, 1]$ of B^n. We write 0 and 1 for these extrema.

For any non-negative integer n and any set A, a map from A^n to A is called an n-ary operation on A (operation of arity n). A *universal algebra* on a set A is a couple $(A, (f_i : i \in I))$ where I is an arbitrary set and for each $i \in I$, f_i is an n-ary operation on A for some non-negative integer n.

To every Boolean function f on B^n there corresponds a universal algebra on the set B^n. This *Boolean function algebra* has two binary operations, $\boldsymbol{x} \wedge \boldsymbol{y}$ (abbreviated $\boldsymbol{xy}$) and $\boldsymbol{x} \vee \boldsymbol{y}$, two constant operations 0 and 1, and two unary operations, namely $\neg \boldsymbol{x}$ (complementation, also denoted $\bar{\boldsymbol{x}}$), and f.

Two Boolean functions are called *isomorphic* if the corresponding function algebras are isomorphic as universal algebras. Equivalently, two Boolean functions are isomorphic if they are equal under some *permutation of variables* (defined below). For example, $f(x_1, x_2) = x_1 \vee \bar{x}_2$ and $g(x_1, x_2) = x_2 \vee \bar{x}_1$ are isomorphic.

2.2. The equational language

We fix a first-order predicate language with identity, to be called the *equational language* (for Boolean functions). The *operation symbols* of this language are the unary function symbol f and the operation symbols of Boolean lattices: binary join and meet ($\vee$ and $\wedge$), nullary 0 and 1, and unary complementation denoted $\neg$ (or by an overbar). The symbol $=$ is the only *relation symbol*. There is a countable set V of vector variables that is disjoint from the set of operation and relation symbols.

A *term* of the equational language is defined as follows: Any variable $\boldsymbol{x} \in V$ is a term. The nullary symbols 0 and 1 are terms. If t is a term, then $f(t)$ is a term, and

so is $\neg t$ (or $\bar{t}$). If t_1 and t_2 are terms, then so are $t_1 \vee t_2$ and $t_1 \wedge t_2$. Note that $t_1 \wedge t_2$ is also written as $t_1 t_2$, and is described as the *product* of t_1 and t_2.

An *atomic formula* of the equational language is an expression of the form $t_1 = t_2$, where t_1 and t_2 are terms. For example,

$$f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x} \vee \boldsymbol{y})$$

is an atomic formula of the equational language.

A (*first-order*) *formula* in the equational language is defined as follows: Every atomic formula is a first-order formula. If ϕ and ψ are first-order formulas, then so are **not**(ϕ), $(\phi$ **or** $\psi)$ and $(\phi$ **and** $\psi)$. If ϕ is a first-order formula, and $\boldsymbol{x} \in V$ is any variable, then $\forall \boldsymbol{x} \phi$ is also a first-order formula. A *first-order sentence*, or *sentence* for short, is a first-order formula in which every variable occurrence is within the scope of some universal quantifier.

A *Boolean term* is a term without the symbol f. If $\boldsymbol{x}$ is a variable, then the terms $\boldsymbol{x}$ and $\bar{\boldsymbol{x}}$ are called *positive* and *negative* literals respectively. A variable occurrence is *negated* if it occurs within a negative literal. An *elementary conjunction* is a Boolean term that is a product of a set of literals not containing both a variable and its negation; if the set is empty, the elementary conjunction is reduced to the symbol 1.

A *disjunctive normal form* (*DNF*) is a Boolean term that is a join of a set of elementary conjunctions; if the set is empty, the DNF is reduced to the symbol 0.[1]

A Boolean term may be interpreted in any Boolean lattice. If the variables occurring in the term are interpreted as specific elements of the lattice, then the term will unequivocally represent an element of the lattice called the *semantic value of the term under the given interpretation of variables*. For example, the semantic value of $\boldsymbol{x} \wedge \boldsymbol{y}$ under the interpretation of $\boldsymbol{x}$ and $\boldsymbol{y}$ as $[0,1]$ and $[1,0]$ respectively is [0,0].

Any term in the equational language may be interpreted in any Boolean function algebra. If the variables occurring in the term are interpreted as specific elements of the underlying lattice B^n, then the term will unequivocally represent an element of the function algebra called the *semantic value of the term under the given interpretation of variables*. For example, let f defined on B^2 be given by $f(x_1,x_2)=1$ if at least one of x_1 and x_2 is equal to 1, and $f(x_1,x_2)=0$ otherwise. Then under the interpretation of the variables $\boldsymbol{x}$ and $\boldsymbol{y}$ as $[0,1]$ and $[1,0]$ respectively, the semantic value of $f(\boldsymbol{x})$ is [1,1] (also written as 1) and the sematic value of $f(\boldsymbol{x}) \wedge \boldsymbol{y}$ is $[1,0]$.

2.3. DNF representations of Boolean functions

For a fixed n, the set $\mathscr{F}_n$ of Boolean functions on B^n is a Boolean lattice. The lattice order is given by

$$f \leqslant g \;\Leftrightarrow\; \forall \boldsymbol{x} \in B^n (f(\boldsymbol{x}) \leqslant g(\boldsymbol{x})).$$

[1] It is common in the literature on DNF to refer to the 'terms' of a DNF. Since we use the word 'term' more generally, as it is used in logic, we refer instead to the 'elementary conjunctions' of the DNF.

It is well known that every f in $\mathscr{F}_n$ can be represented by a Boolean formula. More formally, every f in $\mathscr{F}_n$ is the semantic value of some DNF whose variables are among $x_1,\ldots,x_n$ and where x_i is interpreted as the function f_i given by

$$f_i(a_1,\ldots,a_n)=[a_i,\ldots,a_i]$$

for all $[a_1,\ldots,a_n]\in B^n$. Such a DNF is called a *DNF (representation) of* f.

An *implicant* of $f\in\mathscr{F}_n$ is a function $g\in\mathscr{F}_n$ having a DNF consisting of one elementary conjunction and such that $g\leqslant f$ in $\mathscr{F}_n$. Moreover, g is a *prime implicant* if there are no other distinct implicants g' of f with $g\leqslant g'$. In the lattice $\mathscr{F}_n$, every Boolean function f is the join of its prime implicants.

Two elementary conjunctions are said to 'conflict' in the variable x_i if x_i is a literal in one of them, and $\bar{x}_i$ is a literal in the other. If the two elementary conjunctions conflict in exactly one variable, i.e., they have the form x_iP and $\bar{x}_iQ$ and P and Q have no conflict, their *consensus* is defined to be the elementary conjunction PQ. The *consensus method* starts from an arbitrary DNF representation of a Boolean function f, and performs the following operations in any order, until neither applies:

- Adjunction of consensus: if T and T' are two elementary conjunctions in the DNF that conflict in exactly one variable, T'' is the consensus of T and T', and there is no elementary conjunction S in the DNF whose literals are a subset of the literals of T'', then adjoin T'' to the DNF.
- Absorption: if T and T' are distinct elementary conjunctions in the DNF such that the literals in T are a subset of the literals T', then delete T' from the DNF.

The consensus method is guaranteed to terminate with a DNF that is the join of all the elementary conjunctions representing the prime implicants of f (see [14]).

For example, the consensus method will transform the DNF

$$x_1\bar{x}_2\vee x_2x_3\vee x_1x_3x_4\vee x_4$$

into the DNF

$$x_1\bar{x}_2\vee x_1x_3\vee x_2x_3\vee x_4 \tag{1}$$

2.4. Operations on Boolean functions

Let $f\in\mathscr{F}_n$ and let r be any onto map from $\{1,\ldots,n\}$ to $\{1,\ldots,m\}$, for some $m\leqslant n$. Let D be a DNF of f. For each $I\in\{1,\ldots,n\}$, replace each occurrence of x_i in D, whether or not preceded by $\neg$, by $x_{r(i)}$. (A literal $\neg x_i=\bar{x}_i$ will thus become $\neg x_{r(i)}=\bar{x}_{r(i)}$.) The result is a join of products of literals. If any literal occurs more than once in a product, eliminate all but once occurrence of that literal in the product. If any product contains both a variable and its negation, then discard that product. If any product occurs more than once, then discard all but one occurrence of that product. In this manner a new DNF D' is obtained by *identification of variables*, and r is called the *identification map*. For example, if $f\in\mathscr{F}_4$ is represented by DNF (1), and if r is a map from $\{1,\ldots,4\}$ to $\{1,2\}$, such that $r(1)=r(2)=1$ and $r(3)=r(4)=2$, then

the DNF obtained from DNF (1) by this identification map is $x_1x_2 \vee x_2$, which by the consensus method would become the DNF x_2.

Identification of variables is a restricted case of the variable contraction operation considered by Wang and Williams [17] and Wang [18]. If f' is the Boolean function on B^m represented by D', then f' is a minor of f in the terminology of these authors, and accordingly we shall call f' an *identification minor* of f. To obtain f' from f, the choice of the DNF D is irrelevant. If r is a bijection, then we say that f' is obtained from f *by permutation of variables.*

Associated with an identification map r is a vector mapping s defined as follows. Let $J = \{[a_1,\ldots,a_n] \in B^n \mid \forall i,j, r(i) = r(j) \Rightarrow a_i = a_j\}$. Then s is defined to be the bijection from J to B^m such that $s(a_1,\ldots,a_n) = [b_1,\ldots,b_m]$ implies that $a_i = b_{r(i)}$ for all $i \in \{1,\ldots,n\}$.

A rather trivial operation on Boolean functions will be needed. Let $f \in \mathscr{F}_n$, $n \geqslant 1$, and let $m \geqslant n$. Define $f' \in \mathscr{F}_m$ by

$$f'(a_1,\ldots,a_n,\ldots,a_m) = 1 \text{ if and only } f(a_1,\ldots,a_n) = 1$$

Then we say that f' is obtained from f by *adding inessential variables*. As usual, for any Boolean function $f \in \mathscr{F}_n$, we say that a variable $x_i, 1 \leqslant i \leqslant n$, is *inessential* in f whenever for all $\boldsymbol{a} = [a_1,\ldots,a_{i-1},a_i,a_{i+1},\ldots,a_n]$ in B^n we have

$$f(\boldsymbol{a}) = f(a_1,\ldots,a_{i-1},b_i,a_{i+1},\ldots,a_n)$$

for both $b_i = 0$ and $b_i = 1$. This is the case precisely when f has a DNF in which x_i does not occur. We say that the variable x_i is *essential* if it is not inessential. In the literature, inessential variables are sometimes called *irrelevant* or *dummy* variables.

3. Identities and inequalities for special classes

3.1. A motivating example

Consider the class of *positive functions*, consisting of those Boolean functions that have at least one DNF without negative literals. Obviously these are the functions f for which it is true that

$$\forall \boldsymbol{x},\boldsymbol{y} \quad \boldsymbol{x} \leqslant \boldsymbol{y} \;\Rightarrow\; f(\boldsymbol{x}) \leqslant f(\boldsymbol{y})$$

or, more compactly,

$$\forall \boldsymbol{x},\boldsymbol{y} \quad f(\boldsymbol{x}) \leqslant f(\boldsymbol{x} \vee \boldsymbol{y}). \tag{2}$$

This is not a sentence in our equational language, but can be readily converted to the equivalent statement

$$\forall \boldsymbol{x},\boldsymbol{y} \quad f(\boldsymbol{x}) f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x}). \tag{3}$$

This is now a universally quantified sentence, characterizing the class of positive functions. In accordance with the usual practice of displaying algebraic identities, we shall

eliminate the universal quantifier and say that the identity

$$f(\boldsymbol{x})f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x}) \tag{4}$$

characterizes the class of positive functions. An *identity* can thus be defined as an atomic formula in the equational language. Formally, an identity is said to be *satisfied* by a Boolean function f if its universal closure is satisfied in the function algebra of f. Equivalently, this means that the equality holds for all interpretations of the variables as elements in the domain of f.

Our principal concern is to find identities such as (4) that *characterize* specified classes (i.e., sets) of Boolean functions. We say that a class $\mathscr{K}$ of Boolean functions has a *characterization by a set I of identities* if $\mathscr{K}$ consists precisely of those Boolean functions f that satisfy every identity in I. (The set I may be finite or infinite.)

Observe that if we have an inequality

$$T \leqslant Q$$

where T and Q are terms of our equational language, such as in (2), then this inequality can be converted to either of the identities

$$T \wedge Q = T,$$

$$T \vee Q = Q.$$

3.2. Further characterizations

Negative functions, which are analogous to positive functions, are defined as those with a DNF in which all variable occurrences are within negative literals. It is easy to show that this class is characterized by

$$f(\boldsymbol{x})f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x} \vee \boldsymbol{y}) \tag{5}$$

or, equivalently, by

$$f(\boldsymbol{x})f(\boldsymbol{xy}) = f(\boldsymbol{x}). \tag{6}$$

This illustrates the obvious fact that equational characterizations are not unique.

A Boolean function that is constant 0 or has a DNF

$$C_1 \vee \cdots \vee C_m$$

in which every elementary conjunction C_i has at most one negated variable occurrence is called a *Horn function*. Replace 'at most' in this definition by 'exactly one' and we have *definite Horn* functions. Replace 'negated' by 'non-negated' and we have the *co-Horn* and *definite co-Horn* classes. The reader can verify that every prime implicant of a function in any one of these classes also belongs to that class (see [7]).

The following result is implicit in work of Horn [9]. We present a proof for the sake of completeness.

Proposition 3.1. *The class of Horn functions is characterized by*

$$f(\boldsymbol{x})f(\boldsymbol{xy}) \vee f(\boldsymbol{y})f(\boldsymbol{xy}) = f(\boldsymbol{xy}) \tag{7}$$

or, equivalently, by the inequality

$$f(\boldsymbol{xy}) \leqslant f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \tag{8}$$

Proof. The equivalence of (7) and (8) is easily verified, therefore we need only to show that (8) characterizes Horn functions.

If $\boldsymbol{x} = \boldsymbol{a}$ and $\boldsymbol{y} = \boldsymbol{b}$ violated (8) for a Horn function, we would have, for some implicant g of f with at most one negative literal occurrence $\bar{x}_i$ in its elementary conjunction DNF

$$g(\boldsymbol{ab}) = 1 \quad \text{and} \quad g(\boldsymbol{a}) = g(\boldsymbol{b}) = 0.$$

Clearly g cannot be positive, and the ith component of the vector $\boldsymbol{ab}$ must be 0. Without loss of generality, this implies that the ith component of $\boldsymbol{a}$ is 0. But then $g(\boldsymbol{a}) = 0$ implies that for some j such that x_j occurs non-negated in the elementary conjunction DNF of g, the jth component of $\boldsymbol{a}$ is 0. This forces $g(\boldsymbol{ab}) = 0$, a contradiction.

Conversely, if f is not a Horn function, then some prime implicant g of f is not one either. Let $\bar{x}_i$ and $\bar{x}_j$ be two distinct negative literals in an elementary conjunction DNF of g, which is then without loss of generality of the form

$$\bar{x}_i\bar{x}_jP.$$

Since g is a prime implicant, neither the function g_i represented by $x_i\bar{x}_jP$ nor the function g_j represented by $\bar{x}_ix_jP$ can be an implicant of f. Choose vectors $\boldsymbol{a}$, $\boldsymbol{b}$ such that

$$g_i(\boldsymbol{a}) = g_j(\boldsymbol{b}) = 1 \quad \text{and} \quad f(\boldsymbol{a}) = f(\boldsymbol{b}) = 0.$$

Then both the ith and jth components of the vector $\boldsymbol{ab}$ must be 0 and $g(\boldsymbol{ab}) = 1$. Hence $f(\boldsymbol{ab}) = 1$ and (8) fails for $\boldsymbol{x} = \boldsymbol{a}$, $\boldsymbol{y} = \boldsymbol{b}$. □

It is now easy to see that definite Horn functions are characterized by the following two identities:

$$f(\boldsymbol{x})f(\boldsymbol{xy}) \vee f(\boldsymbol{y})f(\boldsymbol{xy}) = f(\boldsymbol{xy}) \quad \text{and} \quad f(1) = 0.$$

These, however, could be expressed as a single identity. In general, any finite set of identities

$$T_1 = Q_1 \ldots T_n = Q_n \tag{9}$$

can be expressed as a single identity. First, $T_i = Q_i$ is equivalent to

$$\neg(\bar{T}_iQ_i \vee T_i\bar{Q}_i) = 1.$$

Denoting the term on the left side by L_i, the set (9) is equivalent to

$$L_1 \wedge L_2 \wedge \cdots \wedge L_n = 1.$$

As for co-Horn functions, a dual argument shows they are characterized by the identity

$$f(\boldsymbol{x})f(\boldsymbol{x} \vee \boldsymbol{y}) \vee f(\boldsymbol{y})f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x} \vee \boldsymbol{y})$$

or, equivalently, by the inequality

$$f(\boldsymbol{x} \vee \boldsymbol{y}) \leqslant f(\boldsymbol{x}) \vee f(\boldsymbol{y}). \tag{10}$$

Definite co-Horn functions are characterized by the identity for co-Horn functions plus $f(0) = 0$.

The *dual* of a Boolean function f, denoted by f^{d}, is defined on the same domain lattice B^n by

$$f^{\mathrm{d}}(\boldsymbol{x}) = \overline{f(\bar{\boldsymbol{x}})}.$$

A function f is called *dual-minor* if for every $\boldsymbol{x}$ in the domain lattice

$$f(\boldsymbol{x}) \leqslant f^{\mathrm{d}}(\boldsymbol{x}).$$

It is called *dual-major* if

$$f(\boldsymbol{x}) \geqslant f^{\mathrm{d}}(\boldsymbol{x})$$

and it is called *self-dual* if

$$f(\boldsymbol{x}) = f^{\mathrm{d}}(\boldsymbol{x}).$$

Clearly, these last three properties can be expressed as

$$f(\boldsymbol{x})f(\bar{\boldsymbol{x}}) = 0, \tag{11}$$

$$f(\boldsymbol{x}) \vee f(\bar{\boldsymbol{x}}) = 1, \tag{12}$$

$$f(\boldsymbol{x}) = \overline{f(\bar{\boldsymbol{x}})}, \tag{13}$$

characterizing respectively dual-minor, dual-major and self-dual functions through identities satisfied by f.

For any elementary conjunction, if we replace each non-negated variable occurrence x by the negative literal $\neg x$, and, simultaneously, each negative literal $\neg x$ by the positive literal x, we obtain another elementary conjunction, called the *reflection* of the first one. A Boolean function is called *reflexive* if the set of elementary conjunctions representing its prime implicants is closed under reflection.

Proposition 3.2. *A Boolean function is reflexive if and only if it satisfies*

$$f(\boldsymbol{x}) = f(\bar{\boldsymbol{x}}). \tag{14}$$

Proof. Necessity is obvious. For sufficiency, assume (14) is satisfied and let

$$\{p_1, \ldots, p_m\}$$

be the elementary conjunctions representing the prime implicants of f. Then f is represented by the DNF

$$p_1 \vee \cdots \vee p_m.$$

The function f' defined by $f'(\boldsymbol{x}) = f(\bar{\boldsymbol{x}})$ is represented by the DNF

$$r_1 \vee \cdots \vee r_m$$

where each r_i is the reflection of p_i. Since neither consensus nor absorption can be performed on the DNF

$$p_1 \vee \cdots \vee p_m,$$

the same is true for

$$r_1 \vee \cdots \vee r_m.$$

It follows that

$$\{r_1, \ldots, r_m\}$$

represent the prime implicants of f'. □

A Boolean function is called *polar* if it has a DNF in which no elementary conjunction contains both negated and non-negated variable occurrences (see [2]). A Boolean function is called *supermodular* if it satisfies the inequality

$$f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \leqslant f(\boldsymbol{xy}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}). \tag{15}$$

The expression in (15) contains the symbol $\leqslant$, and thus is not an identity. However, the expression could clearly be converted into an equivalent identity, if desired. The equivalent identity is less compact, and we omit it.

Proposition 3.3. *A function is polar if and only if it is supermodular.*

Proof. We first show that a Boolean function f defined on B^n is polar if and only if the following property holds:

$$\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in B^n, \text{ if } \boldsymbol{x} \leqslant \boldsymbol{y} \leqslant \boldsymbol{z} \text{ and } f(\boldsymbol{y}) = 1, \text{ then } f(\boldsymbol{x}) = 1 \text{ or } f(\boldsymbol{z}) = 1 \text{ (or both)}. \tag{16}$$

Necessity of this property is immediate. To show sufficiency, we define the following sets:

- $S = \{\boldsymbol{x} \in B^n \mid f(\boldsymbol{x}) = 1 \text{ and for all } \boldsymbol{y} \in B^n,\ \boldsymbol{x} \leqslant \boldsymbol{y} \Rightarrow f(\boldsymbol{y}) = 1\}$,
- $T = \{\boldsymbol{x} \in B^n \mid f(\boldsymbol{x}) = 1 \text{ and for all } \boldsymbol{y} \in B^n,\ \boldsymbol{y} \leqslant \boldsymbol{x} \Rightarrow f(\boldsymbol{y}) = 1\}$.

Clearly, there is a positive function g_1 defined on B^n such that $g_1(\boldsymbol{x}) = 1$ precisely when $\boldsymbol{x} \in S$. Similarly, there is a negative function g_2 defined on B^n such that $g_2(\boldsymbol{x}) = 1$ precisely when $\boldsymbol{x} \in T$. For all $\boldsymbol{y} \in B^n$, if $\boldsymbol{y} \notin S \cup T$, then $f(\boldsymbol{y}) \neq 1$, lest there exist $\boldsymbol{x}, \boldsymbol{z} \in B^n$, such that $\boldsymbol{x} \leqslant \boldsymbol{y} \leqslant \boldsymbol{z}$ and $f(\boldsymbol{x}) = f(\boldsymbol{z}) = 0$. Thus $f = g_1 \vee g_2$. Since g_1 has a

DNF with no negated variables, and g_2 has a DNF with no non-negated variables, f has a DNF in which no elementary conjunction contains both negated and non-negated variables.

Property (16) immediately implies (15). For the converse, assume (15) holds and let $\boldsymbol{x} \leqslant \boldsymbol{y} \leqslant \boldsymbol{z}$. Define $\boldsymbol{q} = \boldsymbol{x} \vee (\boldsymbol{z} \wedge \bar{\boldsymbol{y}})$. By (15), $f(\boldsymbol{q}) \vee f(\boldsymbol{y}) \leqslant f(\boldsymbol{qy}) \vee f(\boldsymbol{q} \vee \boldsymbol{y})$. Since $\boldsymbol{qy} = \boldsymbol{x}$ and $\boldsymbol{q} \vee \boldsymbol{y} = \boldsymbol{z}$, (16) follows. □

A Boolean function is called *bilinear* if it is both Horn and co-Horn (see [3] for more). Bilinear functions are obviously characterized by the two identities that characterize, respectively, Horn functions and co-Horn functions. Remarkably, as shown in [3], they are also charaterized by the following inequality opposite to (15):

$$f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \geqslant f(\boldsymbol{xy}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}). \tag{17}$$

This follows directly from (10) and (8). Functions satisfying this inequality are called *submodular*.

The *degree* of an elementary conjunction is the number of distinct variables occurring in it. The *degree* of a Boolean function is the maximum degree of the elementary conjunction representation of its prime implicants. Degree 0 functions coincide with constant functions, and they are obviously characterized by the identity

$$f(\boldsymbol{x}) = f(\boldsymbol{y}).$$

A function of degree at most 1 (respectively 2) is called *linear* (respectively *quadratic*).

Proposition 3.4. *A Boolean function is linear if and only if it satisfies the identity*

$$f(\boldsymbol{x}) \vee f(\boldsymbol{y}) = f(\boldsymbol{xy}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}). \tag{18}$$

Proof. First, suppose f is linear. This means $f = f^+ \vee f^-$ where f^+ is positive linear and f^- is negative linear. Assume the left side of (18) is 1. Without loss of generality, this means that $f(\boldsymbol{x}) = 1$. If $f^+(\boldsymbol{x}) = 1$, then $f^+(\boldsymbol{x} \vee \boldsymbol{y}) = 1$, and if $f^-(\boldsymbol{x}) = 1$ then $f^-(\boldsymbol{xy}) = 1$. In both cases the right side of (18) is 1. Similarly one shows that if the left side is 0, so is the right side, proving the identity.

Conversely, suppose that the identity holds. This implies the inequalities (17) and (15), i.e., f is a polar bilinear function, which means it is linear. □

Proposition 3.5. *Quadratic Boolean functions are characterized by the inequality*

$$f(\boldsymbol{xy} \vee \boldsymbol{xz} \vee \boldsymbol{yz}) \leqslant f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \vee f(\boldsymbol{z}). \tag{19}$$

Proof. Suppose f is quadratic. Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ be vectors such that

$$f(\boldsymbol{a}) \vee f(\boldsymbol{b}) \vee f(\boldsymbol{c}) = 0$$

which means $f(\boldsymbol{a}) = f(\boldsymbol{b}) = f(\boldsymbol{c}) = 0$. We shall show that

$$f(\boldsymbol{ab} \vee \boldsymbol{ac} \vee \boldsymbol{bc}) = 0. \tag{20}$$

Let p be any prime implicant of f. At most two variables x_i and x_j occur in an elementary conjunction representation of p. Let $q_i = 1$ if x_i occurs negated, $q_i = 0$ otherwise, and define q_j similarly. Then the ith component of the vector $\boldsymbol{a}$ is q_i, or the jth component is q_j (or both). Let $t \in \{i, j\}$ such that the tth component of $\boldsymbol{a}$ is q_t. As t was defined as a function of $\boldsymbol{a}$, write $t(\boldsymbol{a})$ for t. Define $t(\boldsymbol{b})$ and $t(\boldsymbol{c})$ similarly. Since

$$\{t(\boldsymbol{a}), t(\boldsymbol{b}), t(\boldsymbol{c})\} \subseteq \{i, j\}$$

we may assume without loss of generality that $t(\boldsymbol{a}) = t(\boldsymbol{b}) = i$. Then the ith component of the vector

$$\boldsymbol{ab} \vee \boldsymbol{ac} \vee \boldsymbol{bc}$$

is q_i, and therefore the value of p on that vector is 0. This implies (20), and completes the proof of inequality (19) for quadratic functions.

Conversely, suppose that f is not quadratic, i.e., that some prime implicant p of f has degree at least three. Then p is represented by an elementary conjunction of the form

$$P_1 P_2 P_3$$

where each factor P_i is an elementary conjunction with at least one variable, but no two of the three factors P_1, P_2, P_3 have a common variable. Define elementary conjunctions

$$R_1 = P_1 P_3, \quad R_2 = P_2 P_3, \quad R_3 = P_1 P_2.$$

If R_i represents the function r_i, then none of these r_i is an implicant of f, i.e., there are vectors $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ such that

$$r_1(\boldsymbol{x}) = r_2(\boldsymbol{y}) = r_3(\boldsymbol{z}) = 1,$$

$$f(\boldsymbol{x}) = f(\boldsymbol{y}) = f(\boldsymbol{z}) = 0.$$

These vectors violate (19). □

In the next section we shall see (as an application of Proposition 4.1) that the characterization of quadratic functions by inequality (19) cannot be generalized to higher degree functions. However, the method used for quadratic functions can be extended to yield the following result for positive functions:

Proposition 3.6. *Let f be a positive Boolean function, and let $k \geqslant 2$. Then, f has degree at most k if and only if f satisfies the inequality*

$$f\left(\bigvee_{i=1}^{k+1} \prod_{j \neq i} \boldsymbol{v}_j\right) \leqslant f(\boldsymbol{v}_1) \vee \cdots \vee f(\boldsymbol{v}_{k+1}). \tag{21}$$

Proof. First we show that if f is of degree at most k, then (21) always holds. Suppose

$$f(\boldsymbol{a}_1) = \cdots = f(\boldsymbol{a}_{k+1}) = 0$$

for some vectors $\boldsymbol{a}_i, 1 \leqslant i \leqslant k+1$, in the domain lattice. Let p be a prime implicant of f. Then p must be positive and at most k variables occur in an elementary conjunction representation of p, without loss of generality $x_1, \ldots, x_k$. Then for each $\boldsymbol{a}_j$, there is a $t \in \{1, \ldots, k\}$ such that the tth component of $\boldsymbol{a}_j$ is 0. Write $t(\boldsymbol{a}_j)$ for t. Since

$$\{t(\boldsymbol{a}_1), \ldots, t(\boldsymbol{a}_{k+1})\} \subseteq \{1, \ldots, k\}$$

we may assume, without loss of generality, that $t(\boldsymbol{a}_1) = t(\boldsymbol{a}_2) = 1$. Then the first component of the vector

$$\bigvee_{i=1}^{k+1} \prod_{j \neq i} \boldsymbol{a}_j$$

is 0 and therefore the value of p on this vector is 0. It follows that the left-hand side of (21) is 0.

Conversely, suppose that some prime implicant p of f has degree at least $k+1$. Then p is represented by an elementary conjunction of the form

$$P_1 \cdots P_k P_{k+1}$$

where each factor P_i is an elementary conjunction with at least one variable, but no two factors have a common variable. For each i let

$$R_i = \prod_{j \neq i} P_i.$$

If r_i is the function represented by R_i, then none of the r_i's is an implicant of f, i.e., there are vectors, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k+1}$ such that

$$r_1(\boldsymbol{v}_1) = \cdots = r_{k+1}(\boldsymbol{v}_{k+1}) = 1,$$

$$f(\boldsymbol{v}_1) = \cdots = f(\boldsymbol{v}_{k+1}) = 0.$$

These vectors violate (21). □

Using the fact that a Boolean function f is negative if and only if f' (satisfying $f'(\boldsymbol{x}) = f(\bar{\boldsymbol{x}})$) is positive, one can obviously obtain, for each $k \geqslant 2$, an inequality and therefore an identity that characterizes, among negative functions, those that are of degree at most k. Further, since each of the positive and negative classes can be characterized by an appropriate identity, we can conclude that, for each k, each of the classes 'positive and of degree at most k' and 'negative and of degree at most k' is characterized by an appropriate identity. To see this, the key fact to recall is that a class defined by an identity $C = D$ can always be characterized by an identity of the form $E = 1$, and if another class is characterized by $F = 1$, then the intersection of the two classes is characterized by $E \wedge F = 1$.

4. General criterion for classes definable by identities

In the preceding section we showed that a number of specific classes of Boolean functions can be characterized by identities. The problem we address in this section is

to determine, in general, which classes can be described by identities. We solve this problem for classes closed under addition of inessential variables.

Some local notation will be convenient. For $\boldsymbol{a} \in B^m$, $\boldsymbol{b} \in B^n$, we shall write $\boldsymbol{a} \approx \boldsymbol{b}$ if either both $\boldsymbol{a}$ and $\boldsymbol{b}$ have all their components equal to 0, or both have all their components equal to 1.

4.1. A key lemma

Lemma 1. *Suppose that a certain identity is satisfied by a Boolean function g. Then the identity is also satisfied by every identification minor g' of g.*

Proof. Let g and g' be Boolean functions defined on B^n and B^m respectively, such that g' is an identification minor of g obtained from the identification map r.

Let $J = \{[a_1, \ldots, a_n] \in B^n \mid \text{if } r(i) = r(j), \text{ then } a_i = a_j\}$. The set J contains the vectors $[0, \ldots, 0]$ and $[1, \ldots, 1]$. It is closed under meet, join, and complementation. Let s be the vector mapping (from J to B^m) associated with r.

Suppose a given identity $C = D$ is satisfied by g. Interpret the f-symbol in C and D by g. Then for all interpretations of the vector variables in C and D by vectors $[a_1, \ldots, a_n] \in B^n$, the semantic values of C and D are the same. In particular, the semantic values of C and D are the same for all interpretations of the vector variables by vectors in J.

The following properties hold for s.

- for all $\boldsymbol{a} \in J$, $g(\boldsymbol{a}) \approx g'(s(\boldsymbol{a}))$.
- $s(1, 1, \ldots, 1) = [1, 1, \ldots, 1]$ and $s(0, 0, \ldots, 0) = [0, 0, \ldots, 0]$
- If $\boldsymbol{a}, \boldsymbol{b} \in J$ then

$$s(\boldsymbol{a} \wedge \boldsymbol{b}) = s(\boldsymbol{a}) \wedge s(\boldsymbol{b}),$$

$$s(\boldsymbol{a} \vee \boldsymbol{b}) = s(\boldsymbol{a}) \vee s(\boldsymbol{b}),$$

$$\overline{s(\boldsymbol{a})} = s(\bar{\boldsymbol{a}}).$$

We now show that $C = D$ is satisfied by g'. Consider an interpretation of C and D in which the f-symbol in C and D is interpreted by g', and each variable x is interpreted by an arbitrary vector $\boldsymbol{b}_{(x)} \in B^m$. We show that the semantic values of C and D are equal under this interpretation, and hence $C = D$ is satisfied by g'.

Since s is a bijection from J to B^m, for each $\boldsymbol{b}_{(x)}$ there exists a vector $\boldsymbol{a}_{(x)} \in J$ such that $s(\boldsymbol{a}_{(x)}) = \boldsymbol{b}_{(x)}$. Consider the interpretation of C and D that interprets the f-symbol in C and D by g and each vector variable $\boldsymbol{x}$ by the vector $\boldsymbol{a}_{(x)}$. Under this interpretation, the semantic values of C and D are some $[c_1, \ldots, c_n]$ and $[d_1, \ldots, d_n]$. Clearly $[c_1, \ldots, c_n]$ and $[d_1, \ldots, d_n]$ are in J. Since $C = D$ is satisfied by g, $[c_1, \ldots, c_n] = [d_1, \ldots, d_n]$.

Now, consider again the interpretation in which the f-symbol is interpreted by g', and each variable x in C and D is interpreted by $\boldsymbol{b}_{(x)}$. It follows from the above properties of s that the semantic values of C and D under these interpretations are $s(c_1, \ldots, c_n)$ and $s(d_1, \ldots, d_n)$. Since $[c_1, \ldots, c_n] = [d_1, \ldots, d_n]$, it is also true that $s(c_1, \ldots, c_n) = s(d_1, \ldots, d_n)$. □

4.2. Necessary and sufficient conditions for characterization by identities

The following proposition follows immediately from Lemma 1.

Proposition 4.1. *Let $\mathscr{K}$ be a class of Boolean functions. If $\mathscr{K}$ has a characterization by a set I of identities, then $\mathscr{K}$ is closed under identification minors.*

Application: As an application of Proposition 4.1, consider, for any $k \geqslant 3$, the class of Boolean functions of degree $\leqslant k$. This class is not closed under identification of variables: in $x_1x_2x_3 \ldots x_k \vee \bar{x}_{k+1} \ldots \bar{x}_{2k}$, let $x_1 = x_{k+1}$ and apply the consensus method. Thus the class cannot be characterized by a set of identities.

The converse of Proposition 4.1 does not hold for all classes $\mathscr{K}$. For example, the class consisting of the function $f(x_1, x_2) = x_1$ and all identification minors of f is clearly closed under identification minors. However, it can be shown that this class cannot be characterized by identities. (The proof is based on two observations: f has one inessential variable, and the function f^* obtained by adding a second inessential variable to f is not in the class. It can be shown that any identity satisfied by f would also be satisfied by f^*. We leave the details of this proof to the reader.)

Below, in Proposition 4.2, we show that the converse of Proposition 4.1 does hold for classes $\mathscr{K}$ closed under addition of inessential variables. That is, we show the following: Let $\mathscr{K}$ be a class of Boolean functions closed under addition of inessential variables. If $\mathscr{K}$ is closed under identification minors, then it has a characterization by a (possibly infinite) set of identities.

The proof of Proposition 4.2 is based on the following intuition. Consider the set $\mathscr{G}$ of functions not in $\mathscr{K}$. The idea is to construct, for each function $g \in \mathscr{G}$, an identity that is satisfied by all functions in $\mathscr{K}$, but not satisfied by g. The set of all such identities clearly characterizes $\mathscr{K}$.

How do we construct the identity for a given $g \in \mathscr{G}$? Suppose g is defined on B^m. Let $t = 2^m$, and let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$ be the t elements of B^m. Then the value of g on $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$ uniquely describes g. Without loss of generality, assume that $g(\boldsymbol{a}_1) = \cdots = g(\boldsymbol{a}_j) = 0$ and $g(\boldsymbol{a}_{j+1}) = \cdots = g(\boldsymbol{a}_t) = 1$.

Consider first the following identity in the equational language:

$$(f(\boldsymbol{x}_1) \vee \cdots \vee f(\boldsymbol{x}_j)) \vee (\neg f(\boldsymbol{x}_{j+1}) \vee \cdots \vee \neg f(\boldsymbol{x}_t)) = 1.$$

Clearly this identity is not satisfied by g; interpret $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t$ as $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$ respectively. Unfortunately, because $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t$ may be interpreted in other ways, this identity may also not be satisfied by functions $f \in \mathscr{K}$. In essence, the identity is comparing the value of f on $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t$ (however they are interpreted) to the value of g on $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$. Since $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t$ may have no relation to $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$, these comparisons are insufficient to distinguish g from many of the functions $f \in \mathscr{K}$.

To overcome this, it is possible to incorporate additional comparisons into the identity. For example, in addition to comparing the values of f and g on $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t$ and $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$, respectively, one could also compare the value of f and g on the DNFs $\boldsymbol{x}_1 \vee \boldsymbol{x}_2\bar{\boldsymbol{x}}_7$ and $\boldsymbol{a}_1 \vee \boldsymbol{a}_2\bar{\boldsymbol{a}}_7$, respectively. The resulting identity is still not satisfied by g,

but some of the functions in $\mathscr{K}$ that did not satisfy the previous identity may satisfy this identity.

More generally, it is possible to add a comparison between f and g on *any* two corresponding DNFs over the variables $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t$ and $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t$, respectively. There are 2^{2^t} distinct Boolean functions defined on B^t. For our construction, we fix a DNF representation for each of these functions. We then construct an identity for g that consists of 2^{2^t} comparisons, one for each of these 2^{2^t} DNF representations. We show that this set of comparisons is sufficient for our purposes; the constructed identity is not satisfied by g, but is satisfied by all functions $f \in \mathscr{K}$.

We now present the notation that will be used in our proof. The proof relies on *Boolean matrices*, i.e., matrices whose entries are 0 or 1. Since no matrices of any other kind will be used, we shall omit the adjective 'Boolean'. For every m, we define the *domain matrix of order m*, A_m, to be the $2^m \times m$ matrix with all 2^m rows distinct, such that the rows (viewed as binary strings) are in increasing lexicographic order. The rows of A_m correspond to the elements of the domain of any function g on B^m.

Consider a Boolean function g on B^m. Again, let $t = 2^m$. Let $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t$ be the row vectors of A_m, the domain matrix of order m. Let h be any Boolean function on B^t. Let us fix a DNF representation $D(h)$ of h. For any n, and vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t$ in B^n, let

$$h_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t)$$

denote the semantic value of the Boolean term $D(h)$ under the interpretation of the variables $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t$ of $D(h)$ as $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t$ in B^n. Note that this value is independent of the choice of the particular DNF representation $D(h)$ of h.

Define two complementary sets of functions on B^t (i.e. a partition of the 2^{2^t} functions in $\mathscr{F}_t$) as follows:

$$H_0 = \{h \in \mathscr{F}_t\colon g(h_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t)) = 0\},$$

$$H_1 = \{h \in \mathscr{F}_t\colon g(h_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t)) = 1\}.$$

Then define the following terms of the equational language, where f is the function symbol of the equational language:

M_0 is the join of all $f(D(h))$ for $h \in H_0$,

M_1 is the join of all $\neg f(D(h))$ for $h \in H_1$,

$M(g)$ is the join $M_0 \vee M_1$.

We shall call $M(g)$ the *negative descriptor* of g.

Example. Let the Boolean function g on B_2 be represented by the DNF

$$x_1 \vee x_2.$$

Then $m=2$ and $t=4$. The domain matrix A_2 is

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Thus, $\boldsymbol{a}_1=[0,0]$, $\boldsymbol{a}_2=[0,1]$, $\boldsymbol{a}_3=[1,0]$, and $\boldsymbol{a}_4=[1,1]$. Let h be represented by the DNF

$$D(h)=\boldsymbol{x}_1\boldsymbol{x}_2 \vee \boldsymbol{x}_3\boldsymbol{x}_4.$$

Let $n=2$, and $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_4$ equal $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_4$ respectively. Then

$$\begin{aligned} h_2(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_4) &= h_2([0,0],[0,1],[1,0],[1,1]) \\ &= [0,0][0,1] \vee [1,0][1,1] \\ &= [0,0] \vee [1,0] = [1,0]. \end{aligned}$$

The function h is in H_1 because $g(h_2(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_4))=g(1,0)=1\vee 0=1$. The term M_1 is the join of a number of terms, one of which is $\neg f(\boldsymbol{x}_1\boldsymbol{x}_2 \vee \boldsymbol{x}_3\boldsymbol{x}_4)$. $M(g)$ is also the join of a number of terms, one of which is $\neg f(\boldsymbol{x}_1\boldsymbol{x}_2 \vee \boldsymbol{x}_3\boldsymbol{x}_4)$. □

We now present Proposition 4.2 and its proof.

Proposition 4.2. *Let $\mathscr{K}$ be a class of Boolean functions that is closed under addition of inessential variables. If $\mathscr{K}$ is closed under identification minors, then $\mathscr{K}$ has a characterization by a (possibly infinite) set I of identities.*

Proof. Let $\mathscr{K}$ be a class of Boolean functions closed under addition of inessential variables. Suppose $\mathscr{K}$ is closed under identification minors. Let $\mathscr{G}$ be the set of Boolean functions not in $\mathscr{K}$. Let I consist of all identities of the form $M(g)=1$ where $M(g)$ is the negative descriptor of some g in $\mathscr{G}$. We will prove that I characterizes $\mathscr{K}$.

Let $g\in\mathscr{F}_m$, $t=2^m$. To say that $M(g)=1$ is not satisfied by a given $f\in\mathscr{F}_n$ means that there are vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t$ in B^n such that for all $h\in\mathscr{F}_t$

$$f(h_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t)) \approx g(h_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t)) \tag{22}$$

Obviously then $M(g)=1$ is not satisfied by g: take $\boldsymbol{b}_1=\boldsymbol{a}_1,\ldots,\boldsymbol{b}_t=\boldsymbol{a}_t$. Thus for all $g\in\mathscr{G}$, g does not satisfy every identity in I.

Let $f\in\mathscr{F}_n$ be such that f does not satisfy $M(g)=1$, where $M(g)$ is the negative descriptor of some $g\in\mathscr{G}$. We shall show that $f\notin\mathscr{K}$. Let $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t\in B^n$ be vectors such that for all $h\in\mathscr{F}_t$ (where $t=2^m, g\in\mathscr{F}_m$) we have relation (22). Let A be the domain matrix of order m (a $t\times m$ matrix), and consider the $t\times n$ matrix W whose rows are the vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t$, in this order. The columns of A are all distinct, but W may contain repeated columns.

Let n' be the number of distinct columns in W. Let $r : \{1,\ldots,n\} \to \{1,\ldots,n'\}$ be an identification map such that for all $i,j \in \{1,\ldots,n\}$, columns i and j of W are equal if and only if $r(i) = r(j)$. Let s be the vector mapping associated with r, and let f' be the identification minor of f associated with r. Clearly, for all $j \in \{1,\ldots,t\}, f(\boldsymbol{b}_j) = f'(s(\boldsymbol{b}_j))$.

Let W' be the $n' \times t$ matrix whose rows are $s(\boldsymbol{b}_1),\ldots,s(\boldsymbol{b}_t)$. All columns of W' are distinct. Let $Z = \{i |$ the ith column of W' is not equal to a column of $A\}$.

We first prove the following claim: For all $i \in Z$, variable x_i is inessential in f'. To prove the claim, it suffices to show that if $\boldsymbol{c}' = [c'_1,\ldots,c'_{n'}] \in B^{n'}$ and $\boldsymbol{d}' = [d'_1,\ldots,d'_{n'}] \in B^{n'}$ are such that $c'_i = d'_i$ for all $i \notin Z$, then $f'(\boldsymbol{c}') = f'(\boldsymbol{d}')$. Let $\boldsymbol{c} = [c_1,\ldots,c_n] = s^{-1}(\boldsymbol{c}')$ and let $\boldsymbol{d} = [d_1,\ldots,d_n] = s^{-1}(\boldsymbol{d}')$. Then $f(\boldsymbol{c}) = f'(\boldsymbol{c}')$ and $f(\boldsymbol{d}) = f'(\boldsymbol{d}')$. Let $h \in \mathscr{F}_t$ be such that for each $j \in \{1,\ldots,n\}$, for the jth column vector $W(j)$ of W, $h(W(j)) = c_j$ and whose value is 0 on all other vectors in B^t. Similarly, let $k \in \mathscr{F}_t$ be such that, for each $j \in \{1,\ldots,n\}$, $k(W(j)) = d_j$, and whose value is 0 on all other vectors in B^t. Then $h_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t) = \boldsymbol{c}$ and $k_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t) = \boldsymbol{d}$, and therefore, from (22),

$$f(\boldsymbol{c}) \approx g(h_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t)),$$

$$f(\boldsymbol{d}) \approx g(k_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t)).$$

But the values of h and k coincide on all column vectors of A, and therefore $g(h_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t)) = g(k_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t))$ implying $f(\boldsymbol{c}) = f(\boldsymbol{d})$ and hence $f'(\boldsymbol{c}') = f'(\boldsymbol{d}')$. This proves the claim.

We now prove a second claim: For $j \in \{1,\ldots,m\}$, if the jth column of A is not a column of W, then x_j is an inessential variable of g. The proof, which is similar to the proof of the previous claim, is as follows. Let $X = \{j |$ the jth column of A is not equal to a column of $W\}$. Let $\boldsymbol{c} = [c_1,\ldots,c_m] \in B^m$ and $\boldsymbol{d} = [d_1,\ldots,d_m] \in B^m$ such that $c_i = d_i$ for all $i \notin X$. Let $h \in \mathscr{F}_t$ be such that for each $j \in \{1,\ldots,m\}$, for the jth column vector $A(j)$ of A, $h(A(j)) = c_j$, and whose value is 0 on all other vectors in B^t. Similarly, let $k \in \mathscr{F}_t$ be such that, for each $j \in \{1,\ldots,m\}$, $k(A(j)) = d_j$, and whose value is 0 on all other vectors in B^t. Then $h_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t) = \boldsymbol{c}$ and $k_m(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_t) = \boldsymbol{d}$, and therefore, from (22),

$$f(h_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t)) \approx g(\boldsymbol{c}),$$

$$f(k_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t)) \approx g(\boldsymbol{d}).$$

But the values of h and k coincide on all column vectors of W, and therefore $f(h_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t)) = f(k_n(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t))$ implying $g(\boldsymbol{c}) = g(\boldsymbol{d})$. This proves the second claim.

Thus W' (respectively, A) is a matrix corresponding to f' (respectively, g), such that any column appearing in W' (respectively, A) but not in A (respectively, W'), corresponds to an inessential variable of f' (respectively, g).

Consider the submatrix A' of A produced by deleting all columns of A that do not appear as columns in W'. Let $P = \{i_1,\ldots,i_{m'}\}$ be the set of indices of the columns of A that are not deleted in producing A', such that $i_1 < i_2 < \cdots < i_{m'}$. For simplicity,

assume $m' \neq 0$ ($m' = 0$ is an easy special case). Corresponding to A' is a function g' produced from g by 'deleting' from g variables x_j where $j \notin P$, which are inessential. Formally, let g' be the minor of g produced by the identification map $r : \{1,\ldots,m\} \to \{1,\ldots,m'\}$, such that $r(i_j) = j$ for $j \in \{1,\ldots,m'\}$, and $r(k) = 1$ for $k \notin P$. Similarly, let W'' be the submatrix of W' produced by deleting columns of W' not appearing in A. Then there is an identification minor of f'' of f' produced by 'deleting' from f' those variables x_j whose corresponding columns were deleted from W' (all such variables are inessential to f').

Since A is a domain matrix of degree m, the rows of A' include all binary vectors of length m'. Thus the value of g' on the row vectors of A' uniquely determines the function g'. The matrix W'' is equal to A' under some permutation of columns. For any matrix M, let $M[i]$ denote the ith row of M. Let $j \in \{1,\ldots,t\}$. By (22), taking $h \in \mathscr{F}_t$ to be the function represented by the one-variable DNF x_j, we get $g(A[j]) \approx f(W[j])$. It follows that $g'(A'[j]) = f''(W''[j])$. Since the value of f'' and g' are equal on corresponding rows of W'' and A', it follows that f'' and g' are isomorphic.

It follows from the above that g can be produced from f by addition of inessential variables and identification of variables. Since $\mathscr{K}$ is closed under identification of variables and addition of inessential variables, if $f \in \mathscr{K}$ then $g \in \mathscr{K}$. But $g \notin \mathscr{K}$. Therefore, $f \notin \mathscr{K}$. □

Observe that if $\mathscr{K}$ is a recursive (decidable) set of Boolean functions, then I is a recursive set of identities.

Consider any of the following classes of Boolean functions: positive, negative, Horn, definite Horn, co-Horn, definite co-Horn, supermodular, submodular, constant, linear, quadratic, positive of degree $\leqslant k$, negative of degree $\leqslant k$. It is not difficult to verify that each of these classes is closed under taking identification minors. Thus Proposition 4.2 corroborates the fact, established in the previous section, that these classes can be characterized by identities.

Combining the above two propositions, we get the following:

Proposition 4.3. *Let $\mathscr{K}$ be a class of Boolean functions closed under addition of inessential variables. Then the following conditions are equivalent*:

(i) *there is a set I of identities such that $\mathscr{K}$ consists precisely of those Boolean functions that satisfy every identity in I,*

(ii) *$\mathscr{K}$ is closed under taking identification minors.*

Note that the above proposition applies only to classes closed under addition of inessential variables.

Define a *DNF identity* to be an identity of the form $T_1 \vee \cdots \vee T_m = 1$, where each T_i is either 0, 1, or a conjunction of terms of the form $f(D)$ or $\neg f(D)$, where D is a Boolean term. The semantic value of each $f(D)$ in a DNF identity (under any valid interpretation of the variables) is either 0 or 1. Thus a DNF identity is equivalent to an expression of the form $P(f(D_1),\ldots,f(D_p))$, where P is an arbitrary p-place Boolean

predicate, and $D_1,\ldots,D_p$ are Boolean terms. We note here that Pippenger, in his recent paper, in fact considered only DNF identities, rather than general identities [13].

Classes characterizable by a set of DNF identities are clearly closed under addition of inessential variables, and the identities constructed in the proof of Proposition 4.2 are DNF identities. Therefore, as observed by Pippenger, the following variant of Proposition 4.3 holds [13]:

Proposition 4.4. *A class of Boolean functions is characterizable by a set of DNF identities if and only if it is closed under identification of variables and addition of inessential variables.*

There are classes that can be characterized by identities but not by DNF identities. Consider for example the class characterized by the identity $f(\boldsymbol{x})=\boldsymbol{x}f(\boldsymbol{x})$. It contains the function $g(x_1)=x_1$, but not the function produced by adding an inessential variable to g. Thus it is not closed under addition of inessential variables, and hence cannot be characterized by DNF identities.

4.3. Finite characterizations

The question still arises as to which classes of functions can be characterized by a finite set of identities. To address this question, consider on the set of all Boolean functions the relation $g \preccurlyeq f$ given by $g \preccurlyeq f \Leftrightarrow g$ is an identification minor of f. This relation $\preccurlyeq$ is reflexive and transitive. As usual, we write $g \prec f$ if $g \preccurlyeq f$ but not $f \preccurlyeq g$. Functions f and g are isomorphic if and only if $g \preccurlyeq f$ and $f \preccurlyeq g$.

Proposition 4.3 asserts that a class $\mathscr{K}$ of functions closed under addition of inessential variables can be characterized by a set I of identities if and only if for all functions f and g, the relations $g \preccurlyeq f, f \in \mathscr{K}$ together imply $g \in \mathscr{K}$. If this is the case, consider the set F_0 of Boolean functions g such that (i) $g \notin \mathscr{K}$, and (ii) for each $h \prec g$, $h \in \mathscr{K}$.

For every $g \in F_0$, the set F_0 also contains all functions isomorphic to g. Choose a subset F of F_0 such that for each $g \in F_0$, F contains one and only one function isomorphic to g. Distinct members of F are incomparable by the relation $\preccurlyeq$. The set F is called a set of *minimal forbidden minors*, and it *characterizes* the class $\mathscr{K}$ in the sense that a function f belongs to $\mathscr{K}$ if and only if $g \preccurlyeq f$ for no member g of F. The set of minimal forbidden minors is unique up to isomorphism. A characterization by minimal forbidden minors may not provide the simplest description of a class, even for rather trivial classes. For example, if $\mathscr{K}$ is the class of constant functions with value 1, i.e., those that satisfy the identity $f(\boldsymbol{x})=1$, then the set of minimal forbidden minors contains five functions, with DNFs 0, x_1, $\bar{x}_1$, $x_1x_2 \vee \bar{x}_1\bar{x}_2$, $x_1 \vee \bar{x}_2$.

Proposition 4.5. *Let $\mathscr{K}$ be a class of Boolean functions closed under addition of inessential variables. If $\mathscr{K}$ is characterized by some set of identities, then the following conditions are equivalent.*

(i) *$\mathscr{K}$ is characterized by a finite set of identities,*

(ii) *$\mathscr{K}$ is characterized by a single identity*,
(iii) *$\mathscr{K}$ is characterized by a finite set of minimal forbidden minors.*

Proof. The equivalence of (i) and (ii) was already seen earlier.

Assume (iii). Let $g_1,\dots,g_n$ be the minimal forbidden minors. Referring to the proof of Proposition 4.2, consider the identities $M(g_1)=1,\dots,M(g_n)=1$. By Lemma 1, if f satisfies these identities, $f\in\mathscr{K}$. Conversely, by the proof of Proposition 4.2, if f belongs to $\mathscr{K}$ then f satisfies every $M(g_i)$. Therefore, the identities characterize $\mathscr{K}$.

Now assume (ii). Let $E=F$ be an identity characterizing $\mathscr{K}$. Let n be the number of variables occurring in this identity, i.e., in the terms E and F. Let f be a Boolean function on B^m with $m>2^n$ that does not satisfy $E=F$. Consider an interpretation of the n variables occurring in $E=F$ by vectors $\boldsymbol{v}_1,\dots,\boldsymbol{v}_n$ in B^m that results in different values for E and F. Consider the $n\times m$ matrix W with rows $\boldsymbol{v}_1,\dots,\boldsymbol{v}_n$, in that order. Let n' be the number of distinct columns of W. Clearly $n'\leqslant 2^n$. Consider an identification map $r:\{1,\dots,m\}\to\{1,\dots,n'\}$ such that $r(i)=r(j)$ if and only if columns i and j of W are equal. This map produces an identification minor f' defined on $B^{n'}$. Let s be the vector mapping corresponding to r. Interpreting the variables in E and F by $s(\boldsymbol{v}_1),\dots,s(\boldsymbol{v}_n)$ (with respect to f') also results in different values for the terms E and F. Hence f' does not satisfy $E=F$. Thus for every f defined on B^m, with $m\geqslant 2^n$ and $f\notin\mathscr{K}$, there exists f' defined on $B^{n'}$ with $n'\leqslant 2^n$, such that $f'\preccurlyeq f$ and $f'\notin\mathscr{K}$. This implies (iii). □

There are classes that do indeed require an infinite set of identities. For $n\geqslant 2$, let g_n be the Boolean function on B^n represented by the DNF that is the join of all elementary conjunctions $x_ix_j, 1\leqslant i<j\leqslant n$. Let $\mathscr{K}$ be the class of Boolean functions f such that $g_n\preccurlyeq f$ for no g_n. Then $\mathscr{K}$ is closed under addition of inessential variables and under identification minors, and

$$F=\{g_n\colon n\geqslant 2\}$$

is an infinite set of non-isomorphic minimal forbidden minors.

We note that in a recent paper, Hellerstein showed that the class of linear threshold functions cannot be characterized by a finite set of identities. Since it is closed under addition of inessential variables and under identification minors, it can be characterized by an infinite set of identities [6].

5. First-order characterizations with existential quantification

Let $\mathscr{K}$ be a class of Boolean functions characterized by an identity

$$T=Q.$$

Define the *renamable analogue class* $r(\mathscr{K})$ of $\mathscr{K}$ as follows: a Boolean function f on B^n shall belong to $r(\mathscr{K})$ if and only if for some $\boldsymbol{s}\in B^n$ the function f_s defined by

$$f_s(\boldsymbol{x})=f(\boldsymbol{x}+\boldsymbol{s})$$

belongs to $\mathscr{K}$, where $\boldsymbol{x}+\boldsymbol{s}$ is the Boolean sum

$$\boldsymbol{x}+\boldsymbol{s}=\boldsymbol{x}\bar{\boldsymbol{s}}\vee\bar{\boldsymbol{x}}\boldsymbol{s}.$$

Let $\boldsymbol{s}$ be a variable that does not occur in T or Q. For each term P in the equational language we define, by induction on the length of P, the term $P(+\boldsymbol{s})$ as follows:

(i) if P is reduced to a single symbol, then $P(+\boldsymbol{s})=P$

(ii) if P is of the form $f(X)$ where X is a term, then $P(+\boldsymbol{s})=f(X(+\boldsymbol{s})\bar{\boldsymbol{s}}\vee\overline{X(+\boldsymbol{s})}\boldsymbol{s})$;

if P is of the form $X\vee Y$, then $P(+\boldsymbol{s})=X(+\boldsymbol{s})\vee Y(+\boldsymbol{s})$;

if P is of the form $X\wedge Y$, then $P(+\boldsymbol{s})=X(+\boldsymbol{s})\wedge Y(+\boldsymbol{s})$;

if P is of the form $\neg X$, then $P(+\boldsymbol{s})=\neg X(+\boldsymbol{s})$.

The above definition of $P(+\boldsymbol{s})$ ensures the following: Let f be a Boolean function on B^n. Given an interpretation of the variables in P as elements of B^n, the semantic value of P in the function algebra associated with f_s (under that interpretation of the variables) is equal to the semantic value of $P(+\boldsymbol{s})$ in the function algebra associated with f (under the same interpretation of the variables).

We can form the first-order sentence

$$\exists\boldsymbol{s}\ \forall\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n\ T(+\boldsymbol{s})=Q(+\boldsymbol{s}) \tag{23}$$

where $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n$ are the variables occurring in T or Q. A Boolean function f belongs to the renamable analogue class $r(\mathscr{K})$ if and only if sentence (23) is satisfied in the function algebra associated with f. In general, we say that a set S of first-order sentences in the equational language *characterizes* a set F of Boolean functions if F consists precisely of those Boolean functions in whose associated algebras every sentence belonging to S is satisfied. Note that this generalizes the notion of characterization by identities, in the sense that a class of functions is characterized by a set of identities if and only if the universal closures of these identities (which are sentences) characterize the class. All universal closures of identities are sentences of the form

$$\forall\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n\ T=Q \tag{24}$$

where T and Q are terms (and $\forall\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n$ is empty if no variables occur in $T=Q$). A sentence of the more complex form

$$\exists\boldsymbol{v}\ \forall\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n\ T=Q$$

is called a *simple existential sentence*. We have shown the following:

Proposition 5.1. *If $\mathscr{K}$ is a class of Boolean functions that is characterized by an identity then the renamable analogue class $r(\mathscr{K})$ is characterized by a simple existential sentence.*

For every sentence A of the form (24) there is a simple existential sentence so that the two sentences are satisfied in precisely the same Boolean function algebras: just prefix A with $\exists\boldsymbol{v}$, where $\boldsymbol{v}$ is any variable distinct from the $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n$ appearing in

(24). Therefore, if a class is characterized by identities, it can also be characterized by simple existential sentences.

The renamable analogues of Horn, supermodular, and submodular functions are called *renamable Horn*, *renamable supermodular*, and *renamable submodular*, respectively. The renamable analogues of positive functions are called *unate*.

Proposition 5.2. *Each of the following classes of Boolean functions can be characterized by an appropriate simple existential sentence. None of these classes can be characterized by any set of identities.*

(i) unate,
(ii) renamable Horn,
(iii) renamable supermodular,
(iv) renamable submodular.

Proof. The first statement is a corollary of Proposition 5.1. To prove the second statement, we invoke Proposition 4.2 and consider the following identification maps r:

(i) In $x_1\bar{x}_2 \vee x_3\bar{x}_4$, representing a unate function, let r be such that $r(1) = 1$, $r(2) = r(3) = 2$ and $r(4) = 3$.

(ii) In $x_1x_2x_3 \vee \bar{x}_4\bar{x}_5\bar{x}_6$, let r be such that $r(i) = r(i+3) = i$ for $i = 1, 2, 3$.

(iii) In $x_1x_2\bar{x}_3 \vee \bar{x}_4x_5x_6$ use the same map as in (ii).

(iv) In $\bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4 \vee \bar{x}_5\bar{x}_6$ let $r(1) = r(3) = 1$, $r(2) = r(5) = 2$, and $r(4) = r(6) = 3$. □

We have noted above that classes characterized by sets of simple existential sentences include all classes characterized by identities. By relaxing syntactic constraints, we obtain more and more classes of Boolean functions that may be described by a theory consisting of sentences of a prescribed form. Ultimately, essentially all classes admit of a theory:

Proposition 5.3. *Let $\mathscr{K}$ be a class of Boolean functions. Then there is a set S of sentences in the equational language that characterizes $\mathscr{K}$ if and only if $\mathscr{K}$ is closed under permutation of variables.*

Proof. The condition is obviously necessary, as permuting the variables of a Boolean function f defines a function f' such that the corresponding function algebras are isomorphic, and any given sentence is satisfied in the algebra of f if and only if it is true in the algebra of f'.

To prove sufficiency, it is enough to show that for any given Boolean function g on B^n, there is a characteristic sentence satisfied only in the algebra of g and in isomorphic function algebras. If $\mathscr{K}$ is finite, we can let S consist of a single sentence, namely the join of the characteristic sentences of the functions in $\mathscr{K}$. If $\mathscr{K}$ is infinite, we let S consist of the negations of all characteristic sentences of functions not in $\mathscr{K}$.

The sentence we shall construct shall have $n+1$ variables: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ and $\boldsymbol{w}$.

For each vector $\boldsymbol{a} = [a_1, \ldots, a_n]$ in B^n, let $V(\boldsymbol{a})$ be the Boolean term that is the join of those variables $\boldsymbol{v}_i$ for which $a_i = 1$. If $a_i = 0$ for all i, then $V(\boldsymbol{a})$ is the term 0. To illustrate, for $n = 4$ and $\boldsymbol{a} = [0, 1, 0, 1]$, the term $V(\boldsymbol{a})$ is $\boldsymbol{v}_2 \vee \boldsymbol{v}_4$.

Define now five formulas in the equational language, to be denoted by

D (for 'distinct')

Z ('non-zero')

A ('atoms')

L ('generating a Boolean lattice')

G ('on which f is computed like g')

D is defined as the conjunction, for all $1 \leqslant i < j \leqslant n$, of the formulas $\mathbf{not}(\boldsymbol{v}_i = \boldsymbol{v}_j)$.

Z is the conjunction, for all i, of $\mathbf{not}(\boldsymbol{v}_i = 0)$.

A is the conjunction, for all i, of $\forall \boldsymbol{w}\ ((\boldsymbol{w}\boldsymbol{v}_i = 0) or (\boldsymbol{w}\boldsymbol{v}_i = \boldsymbol{v}_i))$.

L is the formula $\boldsymbol{v}_1 \vee \cdots \vee \boldsymbol{v}_n = 1$.

G is the conjunction, for all $\boldsymbol{a} \in B^n$, of the formulas

$$f(V(\boldsymbol{a})) = g(\boldsymbol{a})$$

where $g(\boldsymbol{a})$ stands for the symbol 0 or 1, according to the value of the function g on the vector $\boldsymbol{a}$.

The characteristic sentence for g is then

$$\exists \mathbf{v}_1, \ldots, \mathbf{v}_n (D \textbf{ and } Z \textbf{ and } A \textbf{ and } L \textbf{ and } G).$$

This sentence is clearly satisfied by g; for $1 \leqslant i \leqslant n$, take $\mathbf{v}_i$ to be the vector in B^n that is 1 in the ith component, and 0 elsewhere.

Suppose some function f satisfies the sentence. Consider the $\mathbf{v}_1, \ldots, \mathbf{v}_n$ satisfying D, Z, A, L, and G. Conditions D, Z, A, and L, together ensure that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are the n distinct Boolean vectors in B^n containing a 1 in exactly one component. Condition G then ensures that f is isomorphic to g. □

The proof above is constructive in a number of senses. If the set $\mathscr{K}$ is finite, or recursive, then so is the set S of characteristic sentences. Indeed, the converse also holds. The proof essentially provides an algorithm to match sets of Boolean functions with theories in the first-order equational language.

Acknowledgements

We thank Nicholas Pippenger for sending us the technical report containing his recent extensions to our work [13].

References

[1] J.L. Bell, A.B. Slomson, Models and Ultraproducts: An Introduction, North-Holland, Amsterdam, 1969.
[2] O. Ekin, Special classes of boolean functions, Ph.D. Thesis, Rutgers University, 1997.

[3] O. Ekin, P.L Hammer, U.N. Peled, Horn functions and submodular Boolean functions, Theoret. Comput. Sci. 175 (1997) 257–270.
[4] S. Foldes, Fundamental Structures of Algebra and Discrete Mathematics, Wiley, New York, 1994.
[5] S. Foldes, Equational varieties of Boolean functions via the HSP Theorem, Technical Report 18-98, Rutgers Center for Operations Research, July 1998, http://rutcor.rutgers.edu/~rrr.
[6] L. Hellerstein, On generalized constraints and certificates, Technical Report 26-98, Rutgers Center for Operations Research, September 1998, http://rutcor.rutgers.edu/~rrr.
[7] P.L. Hammer, A. Kogan, Horn functions and their DNFs, Inform. Process. Lett. 44 (1992) 23–29.
[8] P.L. Hammer, S. Rudeanu, Boolean Methods in Operations Research and Related Areas, Springer, Berlin, 1968.
[9] A. Horn, On sentences which are true of direct unions of algebras, J. Symbolic Logic 16 (1951) 14–21.
[10] P.T. Johnstone, Notes on Logic and Set Theory, Cambridge University Press, Cambridge, 1987.
[11] E. Mendelsohn, Boolean Algebra and Switching Circuits, McGraw-Hill, New York, 1970.
[12] N. Pippenger, Theories of Computability, Cambridge University Press, Cambridge, 1997.
[13] N. Pippenger, Galois theory for minors of finite functions, Technical Report 98-08, University of British Columbia, Computer Science Department, 1998.
[14] W.V. Quine, A way to simplify truth functions, Amer. Math. Mon. 62 (1955) 627–631.
[15] W.G. Schneeweiss, Boolean Functions with Engineering Applications and Computer Programs, Springer, Berlin, 1989.
[16] G. Szasz, Introduction to Lattice Theory, Academic Press, New York, 1963.
[17] C. Wang, A.C. Williams, The threshold order of a Boolean function, Discrete Appl. Math. 31 (1991) 51–69.
[18] C. Wang, Boolean minors, Discrete Math. 141 (1995) 237–258.