DIMACS Technical Report 97-79
December 1997

Equational Theories of Boolean Functions

by

Oya Ekin[1,2,3] Stephan Foldes [4,5,6] Peter L. Hammer[7,8,9]
Lisa Hellerstein[10,11]

[1]Affiliated Student Member
[2]Partially supported by ONR (grants N0001492J1375 and N0001492J4083) and DIMACS.
[3]Address: RUTCOR, Rutgers University, P.O. Box 5062, New Brunswick, NJ 08903, email: ekin@rutcor.rutgers.edu
[4]Visitor
[5]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.
[6]Address: RUTCOR, Rutgers University, P.O. Box 5062, New Brunswick, NJ 08903, email: sfoldes@mba1981.hbs.edu
[7]Permanent Member
[8]Partially supported by ONR (grants N0001492J1375 and N0001492J4083) and DIMACS.
[9]Address: RUTCOR, Rutgers University, P.O. Box 5062, New Brunswick, NJ 08903, email: hammer@rutcor.rutgers.edu
[10]Partially supported by NSF Grant CCR-9501660, RUTCOR, and DIMACS.
[11]Address: Dept. of Computer and Information Science, Polytechnic University, 5 Metrotech Center, Brooklyn, NY 11201, email: hstein@duke.poly.edu

---

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs and Bellcore.

DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

Several noteworthy classes of Boolean functions are characterized by algebraic identities. For a given DNF-specified class, such characteristic identities exist if and only if the class is closed under the operation of forming Boolean minors by variable identification. A single identity suffices to characterize a class if and only if the number of forbidden identification minors minimal in a specified sense is finite. If general first-order sentences are allowed instead of identities only, then essentially all classes can be described by an appropriate set of sentences.

1 Introduction

Classes of Boolean functions may be specified in different ways. For example, consider the class of positive functions. (Formal definitions will be given in a moment.) Positive functions can be described in at least the following ways:

(a) functions with a disjunctive normal form containing no negated variables,

(b) functions f such that

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

(c) functions f such that

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

Here our interest is principally in equational characterizations such as (c). In this characterization we have a universally quantified sentence without connectives in a certain first-order language with no other relation symbol than identity.

In this article we

- provide such characterizations for a number of Boolean function classes,
- show that for essentially every class there is a theory describing the class that consists of an appropriate set of first-order sentences (with identity as the only relation symbol, but not necessarily universally quantified),
- provide a necessary and sufficient condition for a class to have an equational theory with universal quantifiers only.

It is assumed that the reader is familiar with the basic terminology of Boolean lattices, universal algebras, and first-order predicate calculus. The familiarity needed is rather minimal and may be acquired by selectively consulting general expository texts such as [13] (Sections 30 and 10), [8] (first three chapters), [1] (first three chapters), [5] (Chapters VIII and XI). To appreciate the theoretical and application context of Boolean and pseudo-Boolean functions, [7], [10], [12] may be consulted. For the notions of variable, term, formula, atomic formula, universal closure, sentence, and sentence satisfied in a universal algebra, we adhere to the formal definitions of Johnstone ([8], pages 2 and 19-21). Thus the concepts of "variable" and "term" that we adopt are broader than their meaning in the context of disjunctive normal forms.

A Boolean lattice may be viewed as a universal algebra with two binary operations xy and $x \vee y$, two constant operations 0 and 1, and the unary operation of complementation, denoted $-x$ or $\bar{x}$. Recall that a Boolean lattice structure is completely determined by the order relation

$$x \leq y \Leftrightarrow x \vee y = y$$

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 $\forall i \;\; x_i \leq y_i$.

We define a *Boolean function* as a map f from a finite Boolean lattice $\{0,1\}^n = B^n$, $n \geq 1$, 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 simply write 0 and 1 for these extrema.

To every Boolean function f corresponds a universal algebra on the set B^n: this *Boolean function algebra* has two binary operations xy and $x \vee y$, two constant operations 0 and 1, and two unary operations, namely $-x$ (complementation, also denoted $\bar{x}$), and f. Two Boolean functions are called *isomorphic* if the corresponding function algebras are isomorphic as universal algebras.

We fix a first order predicate language with identity, to be called *equational language* (for Boolean functions), as follows. The operation symbols shall be those of Boolean lattices (binary meet and join, nullary 0 and 1, unary complementation denoted $-x$ or $\bar{x}$ plus the additional unary symbol f). There shall be no relation symbols other than =. Thus the atomic formulae are all of the form $E = G$ where both E and G are terms built up from variables and the six operation symbols of the language we have specified. For example,

$$f(x) \vee f(y) \vee f(x \vee y) = f(x \vee y)$$

denotes an atomic formula.

A *Boolean term* is a term without the symbol f. A *literal* is a Boolean term of the form x or $-x$, where x is a variable and is called a *positive* or *negative* literal accordingly. A variable occurrence is *negated* if it occurs within a negative literal. An *elementary conjunction* is a Boolean term that is either a product of literals or that is reduced to the symbol 1, subject to the condition that no variable occurs in it both negated and non-negated. A *disjunctive normal form (DNF)* is a Boolean term that is either a join of elementary conjunctions or that is reduced to the symbol 0.

Any term may be interpreted in any Boolean function algebra. If the variables occurring in the term are interpreted as certain 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.*

A Boolean term may be interpreted in any Boolean lattice. If the variables occurring in the term are interpreted as certain 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 a fixed n, the set $\mathcal{F}_n$ of Boolean functions on B^n is a Boolean lattice. The lattice order is given by

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

It is well known that every f in $\mathcal{F}_n$ 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 $f \in \mathcal{F}_n$ is a function $g \in \mathcal{F}_n$ having an elementary conjunction DNF and such that $g \leq f$ in $\mathcal{F}_n$. Moreover, g is a *prime implicant* if there are no other distinct implicants g' of f with $g \leq g'$. In the lattice $\mathcal{F}_n$, every Boolean function f is the join of its prime implicants. A DNF of f that is expressed as the join of elementary conjunction DNFs of its prime implicants can be obtained using the *consensus algorithm* (see Quine [11]). We assume that the reader is familiar with this algorithm, and with the operation of *adjunction of consensus* applied to elementary conjunctions or to the Boolean functions they represent (see [11]). A set S of Boolean functions in $\mathcal{F}_n$ represented by elementary conjunctions is the set of prime implicants of some $f \in \mathcal{F}_n$ if and only if

(i) distinct members of S are incomparable in $\mathcal{F}_n$,

(ii) S is closed under adjunction of consensus.

In one phrase, S is to be an antichain closed under adjunction of consensus.

Let $f \in \mathcal{F}_n$ and let r be any map from the set $\{1, \ldots, n\}$ to itself. Let D be a DNF of f. For each i, replace each occurrence of x_i (preceded by $-$ or not), by $x_{r(i)}$. (A literal $-x_i = \bar{x}_i$ will thus become $-x_{r(i)} = \bar{x}_{r(i)}$). In this manner a new DNF D' is obtained by *identification of variables*, and r is called the *identification map*. This operation is a restricted case of the variable contraction operation considered by Wang and Williams [14] and Wang [15]. If f' is the Boolean function on B^n 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. Note also that isomorphic Boolean functions are identification minors of each other, corresponding to permutations of $\{1, \ldots, n\}$ as identification maps. In this case we shall speak of *permutation of variables* rather than identification of variables.

Sometimes one is indifferent to which particular identification map r is used, and what matters is only the partition of $\{1, \ldots, n\}$ associated with r. (In which i and j are in the same class if and only if $r(i) = r(j)$.) In this case we speak simply of *variable identification with respect to a given partition.* If a non-singleton partition class is

$$\{i_1, \ldots, i_k\}$$

then we say that the *variables* $x_{i_1}, \ldots, x_{i_k}$ *are identified*, and we indicate this by writing $x_{i_1} = \ldots = x_{i_k}$.

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

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

Then f' is said to be obtained from f by *adding ineffective variables.* We also say that f and f' are *equivalent modulo ineffective variables.* This is the case if and only if f and f' have a common DNF representation. As usual, for any Boolean function $f \in \mathcal{F}_n$, we say that *a* *variable* $x_i, 1 \leq i \leq n$, *is ineffective* 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 *effective* if it is not ineffective.

2 Identities and Inequalities for Special Classes

In order to illustrate the basic idea of this section, recall that the *dual* of a Boolean function f, denoted by f^d, is defined on the same domain lattice B^n by

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

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

$$f(\boldsymbol{x}) \leq f^d(\boldsymbol{x})$$

It is called *dual-major* if

$$f(\boldsymbol{x}) \geq f^d(\boldsymbol{x})$$

and it is called *self-dual* if

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

Clearly, these last three properties can be expressed as

$$\forall \boldsymbol{x} \;\; f(\boldsymbol{x})f(\bar{\boldsymbol{x}}) = 0 \tag{1}$$

$$\forall \boldsymbol{x} \;\; f(\boldsymbol{x}) \vee f(\bar{\boldsymbol{x}}) = 1 \tag{2}$$

$$\forall \boldsymbol{x} \;\; f(\boldsymbol{x}) = \overline{f(\bar{\boldsymbol{x}})} \tag{3}$$

characterizing respectively dual-minor, dual-major and self-dual functions through equational sentences to be satisfied by f.

For any elementary conjunction, if we replace each non-negated variable occurrence x by the negative literal $-x$, and, simultaneously, each negative literal $-x$ 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 2.1 *A Boolean function is reflexive if and only if*

$$\forall \boldsymbol{x} \;\; f(\boldsymbol{x}) = f(\bar{\boldsymbol{x}}) \tag{4}$$

Proof. Necessity is obvious. For sufficiency, assume (4) and write f as join of its prime implicants,

$$f = p_1 \vee \ldots \vee p_m$$

Then for the function f' defined by $f'(\boldsymbol{x}) = f(\bar{\boldsymbol{x}})$ we have

$$f' = r_1 \vee \ldots \vee r_m$$

where each function r_i has a DNF that is the reflection of an elementary conjunction DNF of p_i. Observe that since

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

is an antichain closed under consensus, so is

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

□

Note that (1), ..., (4) are all universally quantified sentences in the equational language that we specified in the preceding section.

Consider now 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

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

or, more compactly,

$$\forall \boldsymbol{x}, \boldsymbol{y} \;\; f(\boldsymbol{x}) \leq f(\boldsymbol{x} \vee \boldsymbol{y}) \tag{5}$$

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

$$\forall \boldsymbol{x}, \boldsymbol{y} \;\; f(\boldsymbol{x}) f(\boldsymbol{x} \vee \boldsymbol{y}) = f(\boldsymbol{x}) \tag{6}$$

This is now a universally quantified sentence, characterizing the class of positive functions. In accordance with the usual practice of displaying algebraic identities, such as the distributive law

$$x(y + z) = xy + xz$$

which, when asserted to hold in a ring, is understood to be universally quantified, we shall simply say that the identity

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

characterizes the class of positive functions. An *identity* can thus be defined as an atomic formula in equational language, and it is said to be *validated* by a Boolean function f if its universal closure is satisfied in the function algebra of f.

Our principal concern is to find identities such as (7) that *characterize* specified classes of Boolean functions (in the sense that all members of the class, but no other functions, validate the given identities). Observe that if we have an inequality

$$T \leq Q$$

where T and Q are terms of our equational language, such as in (5), then this inequality can be converted to either of the following identities

$$T \cdot Q = T$$

$$T \vee Q = Q$$

Similarly to positive functions, *negative* functions are defined as those with a DNF in which all variable occurrences are within negative literals. The reader can convince himself that this class is characterized by

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

or, equivalently, by

$$f(\boldsymbol{x})f(\boldsymbol{x}\boldsymbol{y}) = f(\boldsymbol{x}) \tag{9}$$

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

A Boolean function that is constant 0 or has a DNF

$$C_1 \vee \ldots \vee C_m$$

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 [6]).

The following result is generally known in one form or another. References of interest include [9] and [2]. We present a proof for completeness' sake.

Proposition 2.2 *The class of Horn functions is characterized by*

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

or, equivalently, by the inequality

$$f(\boldsymbol{x}\boldsymbol{y}) \leq f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \tag{11}$$

Proof. The equivalence of (10) and (11) is easily verified, therefore we need only to show that (11) characterizes Horn functions.

If $\boldsymbol{x} = \boldsymbol{a}$ and $\boldsymbol{y} = \boldsymbol{b}$ violated (11) 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

$$g(\boldsymbol{a}\boldsymbol{b}) = 1 \;\; g(\boldsymbol{a}) = g(\boldsymbol{b}) = 0$$

Clearly g cannot be positive, and the ith component of the vector $\boldsymbol{a}\boldsymbol{b}$ 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

$$\bar{x}_i \bar{x}_j P$$

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

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

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 (11) 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:

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

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

$$T_1 = Q_1 \quad \ldots \quad T_n = Q_n \tag{12}$$

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

$$-(\overline{T}_i Q_i \vee T_i \overline{Q}_i) = 1$$

Denoting the term on the left side by L_i, the set (12) is equivalent to

$$L_1 \cdot L_2 \cdot \ldots \cdot L_n = 1$$

As for co-Horn functions, the characterization, obtained by a dual argument, is

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

and for definite co-Horn functions this same identity plus $f(0) = 0$.

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 [3]).

Proposition 2.3 *Polar functions are characterized by*

$$f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \leq f(\boldsymbol{xy}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}) \tag{13}$$

and therefore they can be characterized by an identity.

Proof. First verify that f is polar if and only if the set

$$N = \{\boldsymbol{x} \in B^n : f(\boldsymbol{x}) = 0\}$$

is order-convex in the domain lattice B^n of f. (Necessity of convexity is immediate. For sufficiency, consider maximal order ideals and dual ideals contained in $B^n \setminus N$.)

The convexity of N means that

$$\boldsymbol{x} \leq \boldsymbol{z} \leq \boldsymbol{y} \Rightarrow f(\boldsymbol{z}) \leq f(\boldsymbol{x}) \vee f(\boldsymbol{y})$$

This implies (13).

For the converse, consider the relative complement of $\boldsymbol{z}$ in the order interval $[\boldsymbol{x}, \boldsymbol{y}]$. □

Condition (13) may be referred to as *supermodularity.* As for the characteristic identity for supermodularity, we content ourselves with the knowledge that we can construct it: the inequality (13) is actually of a more compact form.

A Boolean function is called *bilinear* if it is both Horn and co-Horn (see [4] for more). Bilinear functions are obviously characterized by the two identities that characterize respectively Horn functions and co-Horn functions. Remarkably, they are also charaterized by the following inequality opposite to (13):

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

This inequality is referred to as *submodularity.* The proof is similar to that of Proposition 2.2 and it is left to the reader.

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 obviously possess the characterization by the identity

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

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

Proposition 2.4 *A Boolean function is linear if and only if it validates the identity*

$$f(\boldsymbol{x}) \vee f(\boldsymbol{y}) = f(\boldsymbol{x}\boldsymbol{y}) \vee f(\boldsymbol{x} \vee \boldsymbol{y}) \tag{14}$$

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 (14) 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 $f^-(\boldsymbol{x}\boldsymbol{y}) = 1$. In both cases the right side of (14) 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 (11) and (13), i.e. f is a polar Horn function, which means it is linear. □

Proposition 2.5 *Quadratic Boolean functions are characterized by the inequality*

$$f(\boldsymbol{xy} \vee \boldsymbol{xz} \vee \boldsymbol{yz}) \leq f(\boldsymbol{x}) \vee f(\boldsymbol{y}) \vee f(\boldsymbol{z}) \tag{15}$$

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

$$f(\boldsymbol{ab} \vee \boldsymbol{ac} \vee \boldsymbol{bc}) = 0 \tag{16}$$

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 in 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 (16), and completes the proof of inequality (15) 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

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

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 (15). □

In the next section we shall see that the characterization of quadratic functions by inequality (15) cannot be generalized to higher degree functions. However, the method used for quadratic functions can be extended to yield the following:

Proposition 2.6 *Let f be a positive Boolean function, and let $k \geq 2$. Then, f has degree at most k if and only if f satisfies the following inequality:*

$$f(\bigvee_{i=1}^{k+1} \prod_{j \neq i} \boldsymbol{v}_j) \leq f(\boldsymbol{v}_1) \vee \ldots \vee f(\boldsymbol{v}_{k+1}) \tag{17}$$

Proof. First we show that if f is of degree at most k, then (17) always holds. Suppose

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

for some vectors $\boldsymbol{a}_i, 1 \leq i \leq k{+}1$, 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 1st 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 (17) 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

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

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

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

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

These vectors violate (17). □

Using the fact that a Boolean function f is negative if and only if $\bar{f}$ (satisfying $\bar{f}(\boldsymbol{x}) = f(\overline{\boldsymbol{x}})$) is positive, one can obviously obtain, for each $k \geq 2$, 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 $E \cdot F = 1$.

3 General Criterion for Classes Definable by Identities

In the preceding section we have seen that a number of noteworthy classes of Boolean functions can be characterized by identities.

We have seen that whenever a class is characterized by a finite set of identities, it can also be characterized by a single identity.

We have seen that for every inequality there is an equivalent identity. The inequality, however, may sometimes be simpler to write, and for this reason, on occasion we left the characterization in the form of an inequality -conversion to an identity being trivial. Sometimes we omitted altogether to write the characteristic identities or inequalities explicitly, and contented ourselves with the knowledge that they exist and could be written. The question we address in this section is what classes can be described by identities.

Let g and g' be Boolean functions on B^n such that g' is an identification minor of g with respect to an identification map r whose range has m elements. Take any map b from $\{1, ..., n\}$ to itself that maps the range of r bijectively to $\{1, ..., m\}$. Consider the identification minor g_0 of g with respect to the composed map br. Then g_0 is isomorphic to g' and it has a DNF representation in which no variables other than $x_1, ..., x_m$ occur. Let g_1 be the Boolean function on B^m defined by any such DNF. Then any given identity $C = D$ is validated by g_1 if and only if the semantic values of the terms C and D are the same for each interpretation of the f-symbol by g in which the vector variables are interpreted by vectors $(a_1, \ldots, a_n) \in B^n$ such that $a_i = a_j$ for all i, j for which $r(i) = r(j)$. We then have the following:

Key Observation *Suppose that a certain identity is validated by a Boolean function g, and that g' is an identification minor of g. Then the identity is also validated by some Boolean function g_1 having the same DNF as a function g_0 isomorphic to g' .* □

By a *class* henceforward we mean a set $\mathcal{C}$ of Boolean functions such that if f and g are isomorphic or have a common DNF, then $f \in \mathcal{C}$ if and only if $g \in \mathcal{C}$. Assume that $\mathcal{C}$ has a *characterization by a set I of identities*, i.e. that $\mathcal{C}$ consists precisely of those Boolean functions f that validate every identity in I. Then $\mathcal{C}$ is closed under taking identification minors. The main result in this section will assert that any class closed for identification minors admits of a characterization by an appropriate set of identities.

In this section it will be convenient to call upon the notion of Boolean *matrices*, i.e. matrices whose entries are 0 or 1. Since no matrices of other kind will be used, we shall omit the adjective "Boolean". For a Boolean function on domain B^m the *domain matrix* is defined to be the $2^m \times m$ matrix whose rows are the 2^m possible distinct rows, ordered from top to bottom in lexicographic order. Clearly the domain matrix depends only on m, and not on the particular Boolean function.

Consider a Boolean function g on B^m. Let $t = 2^m$. Let A be the domain matrix of g. It is a $t \times m$ matrix. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$ be the row vectors of A. 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 $x_1, \ldots, x_t$ 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. subsets of $\mathcal{F}_t$) as follows:

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

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

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

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

M_1 is the disjunction of all $-f(D(h))$ for $h \in H_1$

$M(g)$ is the disjunction $M_0 \vee M_1$

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

Proposition 3.1 *For any class $\mathcal{K}$ of Boolean functions the following conditions are equivalent:*

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

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

Proof. We have already observed that (i) implies (ii).

Conversely, if (ii) holds, then let G be the set of Boolean functions not in $\mathcal{K}$. Let I consist of all identities of the form

$$M(g) = 1$$

where $M(g)$ is the negative decriptor of some g in G. We shall prove that I characterizes K.

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.

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

$$f(h_n(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_t)) \approx g(h_m(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t)) \tag{18}$$

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

Assume now that $f \in \mathcal{F}_n$ does not validate $M(g) = 1$, where $M(g)$ is the negative descriptor of some $g \in G$. We shall show that f cannot belong to K. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_t \in B^n$ be vectors such that for all $h \in \mathcal{F}_t$ (where $t = 2^m, g \in \mathcal{F}_m$) we have the relation (18). Let A be the domain matrix of g (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.

Let N_0 be the set of those i, $1 \leq i \leq n$, for which the ith column of W is also a column of A. Let N_1 be a subset of N_0 with the property that for every $i \in N_0$ there is exactly one $j \in N_1$ such that the ith and jth columns of W are the same.

Let N_2 be a subset of $\overline{N_0} = \{1, \ldots, n\} \setminus N_0$ with the property that for every $i \in \overline{N_0}$ there is exactly one $j \in N_2$ such that the ith and jth columns of W are the same.

There is then a (unique) map r from the set $\{1, \ldots, n\}$ to itself whose image set is $N_1 \cup N_2$ and such that for each i, the ith and $r(i)$th columns of W are the same. Let $f' \in \mathcal{F}_n$ be the identification minor of f obtained with r as identification map. Note that all variables x_i of f' with i outside $N_1 \cup N_2$ are ineffective.

We claim that each variable $x_i, i \in N_2$, is also ineffective in f'. It suffices to show that if $\boldsymbol{c} = (c_1, \ldots, c_n)$ and $\boldsymbol{d} = (d_1, \ldots, d_n)$ are vectors in B^n such that

for all $i \in N_1$, $c_i = d_i$

for all $i \notin N_1 \cup N_2$, $c_i = c_{r(i)}$ and $d_i = d_{r(i)}$,

then $f'(\boldsymbol{c}) = f'(\boldsymbol{d})$. To show this, let $h \in \mathcal{F}_t$ such that for each $i \in N_1 \cup N_2$, for the ith column vector $W(i)$ of W

$$h(W(i)) = (c_i, \ldots, c_i)$$

and whose value is $(0, \ldots, 0)$ on all other vectors in B^t. Similarly, let $k \in \mathcal{F}_t$ such that, for each $i \in N_1 \cup N_2$,

$$k(W(i)) = (d_i, \ldots, d_i)$$

and whose value is $(0, \ldots, 0)$ on all other vectors in B^t. Then

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

$$k_n(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_t) = \boldsymbol{d}$$

and therefore, from (18),

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

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

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 thus $f'(\boldsymbol{c}) = f'(\boldsymbol{d})$.

Similarly, we claim that if the jth column vector of A is not a column of W, then x_j is an ineffective variable of g. Let

$$\boldsymbol{a}_c = (a_{c1}, \ldots, a_{cm})$$

$$\boldsymbol{a}_d = (a_{d1}, \ldots, a_{dm})$$

be two rows of A such that $a_{ci} = a_{di}$ for all $1 \leq i \leq m$ except possibly for $i = j$. We need to show that $g(\boldsymbol{a}_c) = g(\boldsymbol{a}_d)$. Let h and k be Boolean functions on B^t such that, for each $1 \leq i \leq m$ for the ith column vector $A(i)$ of A

$$h(A(i)) = (a_{ci}, \ldots, a_{ci})$$

$$k(A(i)) = (a_{di}, \ldots, a_{di})$$

and whose values are $(0, \ldots, 0)$ on all other vectors in B^t. Then

$$h_m(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t) = \boldsymbol{a}_c$$

$$k_m(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t) = \boldsymbol{a}_d$$

and by (18)

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

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

But the right hand sides of the last two relations are equal, since the jth column of A is not a column of W. Therefore $g(\boldsymbol{a}_c) = g(\boldsymbol{a}_d)$.

It follows that g is equivalent modulo ineffective variables to an identification minor of f. Consequently, f cannot belong to K. □

Observe that if $\mathcal{K}$ is a recursive (decidable) set of Boolean functions, then the set I of identities defined in the proof above 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, polar, bilinear, constant, linear, quadratic, positive of degree $\leq k$, negative of degree $\leq k$. It is not difficult to verify that each of these classes is closed under taking identification minors. Thus Proposition 3.1 corroborates the fact, established in the previous section, that these classes can be characterized by identities.

The question still arises as to when the set I of identities can be made finite. To address this question, consider on the set of all Boolean functions, the relation $g \preceq f$ given by

$$g \preceq f \Leftrightarrow g \text{ is equivalent modulo ineffective variables to an identification minor of } f$$

This relation is a pre-order, i.e.

(i) $f \preceq f$,

(ii) $h \preceq g, g \preceq f$ together imply $h \preceq f$.

As usual we write $g < f$ if $g \preceq f$ but not $f \preceq g$.

If $g \leq f$ and also $f \leq g$, then f and g are called "equivalent" and we may write $f \sim g$. This is the case precisely when there is a bijective correspondence between the variables occurring in some DNF D_f of f and those occurring in some DNF D_g of g, such that substituting in D_f the corresponding variables yields D_g.

Let $f \sim f'$ be two equivalent Boolean functions. Let $M(g)$ be the negative descriptor of any Boolean function g. From condition (18) considered in the Proof of Proposition 3.1 it is clear that $M(g) = 1$ is validated by f if and only if it is validated by f'.

Proposition 3.1 asserts that a class $\mathcal{K}$ can be characterized by a set I of identities if and only if $\mathcal{K}$ is a lower section in this preorder (i.e. $g \preceq f, f \in \mathcal{K}$ together imply $g \in \mathcal{K}$). If this is the case, consider the set F_0 of Boolean functions g such that

(i) $g \notin \mathcal{K}$

(ii) for each $h < g$, $h \in \mathcal{K}$.

With every $g \in F_0$, the set F_0 also contains all equivalents of g. Choose a subset F of F_0 that for each $g \in F_0$ contains one and only one equivalent of g. Distinct members of F are incomparable by the relation $\preceq$. The set F is called a set of *minimal forbidden minors*, and it *characterizes* the class $\mathcal{K}$ in the sense that a function f belongs to $\mathcal{K}$ if and only if $g \preceq f$ for no member g of F. Such characterization by forbidden minors does not necessarily provide the simplest description, even for rather trivial classes. For example, if $\mathcal{K}$ is the class of constant functions with value 1, i.e. those that validate the identity $f(\boldsymbol{x}) = 1$, then a 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 3.2 *Let $\mathcal{K}$ be a class of Boolean functions characterized by some set of identities. The following conditions are equivalent.*

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

(ii) $\mathcal{K}$ is characterized by a single identity,

(iii) $\mathcal{K}$ is characterized by a finite set of minimal forbidden minors.

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

Assume (iii). Let $g_1, \ldots, g_n$ be the minimal forbidden minors. Then, referring to the proof of Proposition 3.1, $\mathcal{K}$ is characterized by the identities

$$M(g_1) = 1, \ldots, M(g_n) = 1$$

Conversely, assuming (ii), let $E = F$ be an identity characterizing $\mathcal{K}$. Let n be the number of variables occurring in this identity, i.e. in the term E or F. To show that there are only a finite number of minimal forbidden functions, it is enough to establish that every Boolean function f on B^m with $m > 2^n$ that does not validate $E = F$ has an identification minor g

with at most 2^n effective variables that also does not validate $E = F$. For such an f, consider a particular interpretation of the n variables occurring in $E = F$ by vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ in B^m that results in different semantic values for the terms E and F. These n vectors $\boldsymbol{v}_i$ generate in B^m a Boolean sublattice of dimension at most 2^n. The atoms of this sublattice define a partition of $\{1, \ldots m\}$ into at most 2^n classes. Any identification map that maps each partition class to a representative element will then do to complete the proof. □

There are classes that do indeed require an infinite set of identities. For $n \geq 2$, let g_n be the Boolean function on B^n represented by the DNF that is the join of all elementary conjunctions $x_i x_j, 1 \leq i < j \leq n$. Let $\mathcal{K}$ be the set of Boolean functions f such that $g_n \preceq f$ for no g_n. Then $\mathcal{K}$ is a class closed for identification minors, and

$$F = \{g_n : n \geq 2\}$$

is an infinite set of minimal forbidden minors.

4 First-order Theories with Existential Quantification

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

$$T = Q$$

Define the *renamable analogue class* $r(\mathcal{K})$ of $\mathcal{K}$ as follows: a Boolean function f on B^n shall belong to $r(\mathcal{K})$ 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 $\mathcal{K}$, where $\boldsymbol{x} + \boldsymbol{s}$ is the Boolean sum

$$\boldsymbol{x} + \boldsymbol{s} = \boldsymbol{x}\overline{\boldsymbol{s}} \vee \overline{\boldsymbol{x}}\boldsymbol{s}$$

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

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

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

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

if P is of the form $X \cdot Y$, then $P(+s) = X(+s) \cdot Y(+s)$;

if P is of the form $-X$, then $P(+s) = -X(+s)$.

We can form the first-order sentence

$$\exists s \;\; \forall v_1, \ldots, v_n \;\; T(+s) = Q(+s) \tag{19}$$

where $v_1, \ldots, v_n$ are the variables occurring in T or Q. A Boolean function f belongs to the renamable analogue class $r(\mathcal{K})$ if and only if sentence (19) is satisfied in the function algebra associated with f. In general, we say that a set S of first-order sentences in 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

$$\forall v_1, \ldots, v_n \;\; T = Q \tag{20}$$

where T and Q are terms (and $\forall v_1, \ldots, v_n$ is empty if no variables occur in $T = Q$). A sentence of the more complex form

$$\exists v \;\; \forall v_1, \ldots, v_n \;\; T = Q$$

is called a *simple existential sentence.* For every sentence A of the form (20) there is a simple existential sentence so that the two sentences are satisfied in precisely the same Boolean function algebras: just prefix A with $\exists v$, where v is any variable distinct from the $v_1, \ldots, v_n$ appearing in (20). Therefore, if a class is characterized by identities, it can also be characterized by simple existential sentences. And we have shown above the following:

Proposition 4.1 *If $\mathcal{K}$ is a class of Boolean functions that is characterized by an identity then the renamable analogue class $r(\mathcal{K})$ is characterized by a simple existential sentence.* □

The renamable analogues of Horn, polar, and bilinear functions are called *renamable Horn*, *renamable polar*, and *renamable bilinear*, respectively. The renamable analogues of positive functions are called *unate.* Finally, observe that functions of degree at most k are joins of renamable analogues of positive functions of degree at most k.

Proposition 4.2 *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 polar
(iv) renamable bilinear
(v) degree $\leq k$, for $k \geq 3$

Proof. The first statement is a corollary of Proposition 4.1. To prove the second statement, we invoke Proposition 3.1 and consider the following identifications:

(i) In $x_1\bar{x}_2 \vee x_3\bar{x}_4$, representing a unate function, identify x_2 and x_3.

(ii) In $x_1x_2x_3 \vee \bar{x}_4\bar{x}_5\bar{x}_6$ identify x_i and x_{i+3} for $i = 1, 2, 3$.

(iii) In $x_1x_2\bar{x}_3 \vee \bar{x}_4x_5x_6$ identify 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 $x_1 = x_3, x_2 = x_5, x_4 = x_6$.

(v) In $x_1x_2x_3 \ldots x_k \vee \bar{x}_{k+1} \ldots \bar{x}_{2k}$ let $x_1 = x_{k+1}$ and adjoin consensus. □

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 prescribed form. Ultimately, essentially all classes admit of a theory:

Proposition 4.3 *Let $\mathcal{K}$ be a set of Boolean functions. Then there is a set S of sentences in equational language that characterizes $\mathcal{K}$ if and only if $\mathcal{K}$ 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 $\mathcal{K}$ is finite, we can let S consist of a single sentence, namely the disjunction of the characteristic sentences of the functions in $\mathcal{K}$. If $\mathcal{K}$ is infinite, we let S consist of the negations of all characteristic sentences of functions not in $\mathcal{K}$.

The sentence we shall construct shall have $n + 1$ variables $v_1, \ldots, v_n$ and 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 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 $v_2 \vee v_4$.

Define now five formulas in 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 $1 \leq i < j \leq n$, of the formulas $\textbf{not}(v_i = v_j)$.

Z is the conjunction, for all i, of $\textbf{not}(v_i = 0)$.

A is the conjunction, for all i, of $\forall w \ \ (wv_i = 0 \ \ \textbf{or} \ \ wv_i = v_i)$

L is the formula $v_1 \vee \ldots \vee v_n = 1$.

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

$$\exists v_1, \ldots, v_n(D \textbf{ and } Z \textbf{ and } A \textbf{ and } L \textbf{ and } G)$$

□

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

References

[1] J.L. Bell, A.B. Slomson, *Models and Ultraproducts: An Introduction*, North Holland, 1969.

[2] R. Dechter, J. Pearl, “Structure identification in relational data”, *Artificial Intelligence*, **58**, (1992), 237–270.

[3] O. Ekin, *Special Classes of Boolean Functions*, Ph.D. Thesis, Rutgers University, 1997.

[4] O. Ekin, P.L Hammer and U.N. Peled, “Horn functions and submodular Boolean functions”, *Theoretical Computer Science*, **175**, (1997), 257–270.

[5] S. Foldes, *Fundamental Structures of Algebra and Discrete Mathematics*, Wiley, 1994.

[6] P.L. Hammer and A. Kogan, “ Horn functions and their DNFs”, *Information Processing Letters*, **44** (1992), 23–29.

[7] P.L. Hammer, S. Rudeanu, *Boolean Methods in Operations Research and Related Areas*, Springer-Verlag, 1968.

[8] P.T. Johnstone, *Notes on Logic and Set Theory*, Cambridge University Press, 1987.

[9] J.C.C. McKinsey, “The decision problem for some classes of sentences without quantifiers”, *J. Symbolic Logic* **8** (1943), 61–76.

[10] E.Mendelsohn, *Boolean Algebra and Switching Circuits*, McGraw-Hill, 1970.

[11] W.V. Quine, “A way to simplify truth functions”, *American Mathematical Monthly*, **62** (1955), 627–631.

[12] W.G. Schneeweiss, *Boolean Functions with Engineering Applications and Computer Programs*, Springer-Verlag, 1989.

[13] G. Szasz, *Introduction to Lattice Theory*, Academic Press, 1963.

[14] C. Wang, A.C. Williams, "The threshold order of a Boolean function", *Discrete Applied Mathematics*, **31** (1991), 51–69.

[15] C.Wang, "Boolean minors", *Discrete Mathematics*, **141** (1995), 237–258.