Acta Cybernetica **18** (2007) 61–75.

Functional Equations, Constraints, Definability of Function Classes, and Functions of Boolean Variables*

Miguel Couceiro† and Stephan Foldes‡

Abstract

The paper deals with classes of functions of several variables defined on an arbitrary set A and taking values in a possibly different set B. Definability of function classes by functional equations is shown to be equivalent to definability by relational constraints, generalizing a fact established by Pippenger in the case $A = B = \{0, 1\}$.

Conditions for a class of functions to be definable by constraints of a particular type are given in terms of stability under certain functional compositions. This leads to a correspondence between functional equations with particular algebraic syntax and relational constraints with certain invariance properties with respect to clones of operations on a given set.

When $A = \{0, 1\}$ and B is a commutative ring, such B-valued functions of n variables are represented by multilinear polynomials in n indeterminates in $B[X_1, \ldots, X_n]$. Functional equations are given to describe classes of field-valued functions of a specified bounded degree. Classes of Boolean and pseudo-Boolean functions are covered as particular cases.

Keywords: Function classes, class composition, stability, functional equations, relational constraints, function class definability, ring-valued functions, multilinear polynomial representations, linear equations, field-valued functions of Boolean variables, Boolean functions, pseudo-Boolean functions.

1 Introduction and Basic Definitions

For arbitrary sets B and C, by a *C-valued function on B* we mean a map

$$f : B^n \to C$$

*The work of the first named author was partially supported by the Graduate School in Mathematical Logic MALJA. Supported in part by grant #28139 from the Academy of Finland

†Department of Mathematics, Statistics and Philosophy University of Tampere Kansleririnne 1, 33014 Tampere, Finland E-mail: Miguel.Couceiro@uta.fi

‡Institute of Mathematics, Tampere University of Technology PL553, 33101 Tampere, Finland, E-mail: stephan.foldes@tut.fi

where $n \geq 1$ is called the *arity* of f. The *essential arity* of an n-ary C-valued function $f : B^n \to C$ is defined as the cardinality of the set of indices

$$\begin{aligned} I \;=\; & \{1 \leq i \leq n : \text{ there are } a_1, \dots a_{i-1}, a_i, b_i, a_{i+1}, \dots, a_n \text{ with } a_i \neq b_i \text{ and} \\ & f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, b_i, a_{i+1}, \dots, a_n)\}. \end{aligned}$$

For each $i \in I$, we say that the ith *variable of f is essential*. Note that the essential arity of f is zero if and only if f is constant. If $B = C$, then a C-valued function on B is called an *operation on B*. Operations on the two-element set $B = \{0, 1\}$ are usually refered to as *Boolean functions*.

For any maps $g_1, \dots, g_n : D \to B$, where D is any set and $f : B^n \to C$, the *composition* $f(g_1, \dots, g_n)$ is defined as the map from D to C given by $f(g_1, \dots, g_n)(a) = f(g_1(a), \dots, g_n(a))$, for every $a \in D$.

Let A, B and C be arbitrary non-empty sets, $\mathcal{I}$ a class (i.e. set) of C-valued functions on B (of various arities), and $\mathcal{J}$ a class of B-valued functions on A (of various arities). The *class composition* $\mathcal{I}\mathcal{J}$ is defined as the set

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

If $\mathcal{I}$ is a singleton, $\mathcal{I} = \{f\}$, then we write $f\mathcal{J}$ for $\{f\}\mathcal{J}$. We note that this construction underlies the various notions of subfunction and minor appearing e.g. in [13, 12, 15, 3, 8, 4].

Consider arbitrary non-empty sets A, B, and C, and let $\mathcal{I}$ be a class of C-valued functions on B and $\mathcal{J}$ a class of B-valued functions on A. We say that $\mathcal{I}$ is *stable under right composition with $\mathcal{J}$* if $\mathcal{I}\mathcal{J} \subseteq \mathcal{I}$. Similarly, we say that $\mathcal{J}$ is *stable under left composition with $\mathcal{I}$* if $\mathcal{I}\mathcal{J} \subseteq \mathcal{J}$. Note that a clone on an arbitrary set A is simply a class $\mathcal{C}$ of A-valued functions on A that contains all projections, and is stable under (left or right) composition with itself, i.e. $\mathcal{C}\mathcal{C} \subseteq \mathcal{C}$ (or equivalently, $\mathcal{C}\mathcal{C} = \mathcal{C}$).

Consider arbitrary non-empty sets A and B. A *functional equation* (for B-valued function on A) is a formal expression

$$\begin{aligned} h_1(\mathbf{f}(g_1(\mathbf{v}_1, \dots, \mathbf{v}_p)), \dots, \mathbf{f}(g_m(\mathbf{v}_1, \dots, \mathbf{v}_p))) = \\ = h_2(\mathbf{f}({g'}_1(\mathbf{v}_1, \dots, \mathbf{v}_p)), \dots, \mathbf{f}({g'}_t(\mathbf{v}_1, \dots, \mathbf{v}_p))) \end{aligned} \quad (1)$$

where $m, t, p \geq 1$, $h_1 : B^m \to C$, $h_2 : B^t \to C$, each g_i and ${g'}_j$ is a map $A^p \to A$, the $\mathbf{v}_1, \dots, \mathbf{v}_p$ are p distinct symbols called *vector variables*, and $\mathbf{f}$ is a distinct symbol called *function symbol*.

For $n \geq 1$, we denote by $\mathbf{n}$ the set $\mathbf{n} = \{1, \dots, n\}$, so that an n-vector (n-tuple) v in A^n is a map $v : \mathbf{n} \to A$. In this way, if g is an p-ary operation on A and $v_1, \dots, v_p$ are n-vectors in A^n, then $g(v_1, \dots, v_p)$ denotes the n-vector

$$(g(v_1, \dots, v_p)(1), \dots, g(v_1, \dots, v_p)(n)) \in A^n.$$

For an n-ary B-valued function on A, $f : A^n \to B$, we say that f *satisfies* the

equation (1) if, for all $v_1, \ldots, v_p \in A^n$, we have

$$h_1(f(g_1(v_1, \ldots, v_p)), \ldots, f(g_m(v_1, \ldots, v_p))) = \\ = h_2(f(g'_1(v_1, \ldots, v_p)), \ldots, f(g'_t(v_1, \ldots, v_p))). \quad (2)$$

A class (i.e. set) $\mathcal{K}$ of B-valued functions on A is said to be *defined*, or *definable*, by a set $\mathcal{E}$ of functional equations, if $\mathcal{K}$ is the class of all those functions which satisfy every member of $\mathcal{E}$.

To illustrate, let $A = B = \{0, 1\}$, $m = 2$, $t = 1$, $p = 2$, and let g_1 be the projection function $(x, y) \mapsto x$, g_2 the conjunction $(x, y) \mapsto xy$, $h_1 = g_2$, and h_2 the identity $x \mapsto x$. The functional equation (1) so specified defines the clone (Post class) of monotone Boolean functions. In a more free style of notation, this equation can be displayed as

$$\mathbf{f}(\mathbf{v}_1)\mathbf{f}(\mathbf{v}_1\mathbf{v}_2) = \mathbf{f}(\mathbf{v}_1\mathbf{v}_2).$$

When the specific context is well understood, we shall present functional equations in such more informal manner.

Useful functional properties have often been advantangeously expressed by functional equations. Classical examples include the linearity of $\mathbb{F}$-valued functions on a field $\mathbb{F}$, as well as monotonicity and convexity properties traditionally expressed by functional inequalities which are obviously equivalent to functional equations in max-plus language. More contemporary examples include the submodular property of real-valued functions $\{0, 1\}^n \longrightarrow \mathbb{R}$, and Post classes (clones) of Boolean functions traditionally characterized by relations. Many strong consequences of submodularity, such as the Hall-Rado theorems, follow directly from the characterizing submodular inequality which is essentially a max-plus functional equation (see Welsh [14]). For Boolean functions, equations were systematically studied in [3] and, in a variant form, by Pogosyan [9]. Also, in [5] equations were shown to provide a measure of complexity, essentially in terms of the syntax of the functional equations used to define Post classes.

2 Definability of Function Classes by Functional Equations and Relational Constraints

An *m-ary relation on A* is a subset R of A^m, and thus the relation R can be viewed as a class (set) of unary maps from $\mathbf{m}$ to A. A function $f : A^n \to A$ is said to *preserve* R, and R is said to be *invariant under* f, if $fR \subseteq R$, where fR is the class composition $\{f\}R$ as explained above. An m-ary *A-to-B constraint* (or simply, m-ary *constraint*, when the underlying sets are understood from the context) is a couple (R, S) where $R \subseteq A^m$ and $S \subseteq B^m$. The relations R and S are called the *antecedent* and *consequent*, respectively, of the relational constraint (Pippenger [8]). A B-valued function on A, $f : A^n \longrightarrow B$, $n \geq 1$, is said to *satisfy* an m-ary A-to-B constraint (R, S) if $fR \subseteq S$. A class $\mathcal{K}$ of B-valued functions on A is said to be *defined*, or *definable*, by a set $\mathcal{T}$ of A-to-B constraints, if $\mathcal{K}$ is the class of all those functions which satisfy every constraint in $\mathcal{T}$.

As an example, the already mentioned clone of monotone Boolean functions can be equivalently defined by the single constraint $(\leq, \leq)$, where $\leq$ denotes the less-or-equal relation on $\{0, 1\}$.

In [8], Pippenger has shown that in the Boolean case, i.e. when $A = B = \{0, 1\}$, definability of a function class by functional equations is equivalent to definability by relational constraints. The following theorem is not restricted to the Boolean case, and not even contingent on the finiteness of the underlying sets.

Theorem 1. *Let A be an arbitrary non-empty set, and B any set with at least two elements. For any class $\mathcal{K}$ of B-valued functions on A, the following are equivalent:*

(i) $\mathcal{K}$ is definable by some set of functional equations;

(ii) $\mathcal{K}$ is definable by some set of relational constraints.

Proof. To prove that $(i) \Rightarrow (ii)$, it is enough to show that for every functional equation (1) there is a relational constraint (R, S), such that the B-valued functions on A satisfying the equation are exactly the same as those satisfying the constraint. Indeed, we can define the constraint (R, S) by

$$\begin{aligned} R &= \{(g_1(a), \ldots, g_m(a), {g'}_1(a), \ldots, {g'}_t(a)) : a \in A^p\}, \\ S &= \{(b_1, \ldots, b_m, {b'}_1, \ldots, {b'}_t) \in B^{m+t} : h_1(b_1, \ldots, b_m) = h_2({b'}_1, \ldots, {b'}_t)\}. \end{aligned}$$

Conversely, let us show that $(ii) \Rightarrow (i)$. Let $\mathcal{T}$ be a set of constraints, and let $\mathcal{K}$ be the class of B-valued functions on A defined by $\mathcal{T}$. Consider the set $\mathcal{T}'$ of constraints obtained from $\mathcal{T}$ by removing all those constraints with empty antecedent. Clearly, $\mathcal{T}$ and $\mathcal{T}'$ define the same class $\mathcal{K}$ of B-valued functions on A. Therefore, the proof will be complete if we can show that for every constraint (R, S) with $R \neq \emptyset$ there is a functional equation (1) satisfied by exactly the same functions as those satisfying (R, S).

Let m be the arity of (R, S). The construction of the equation (1) is based on the following facts.

Fact 1. *Given a non-empty relation $R \subseteq A^m$, there is a $p \geq 1$ and a map $g : A^p \to A^m$, such that the range of g is R.*

Fact 2. *Given a relation $S \subseteq B^m$, there exist maps $h_1, h_2 : B^m \to B$, such that*

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

Using these functions g, h_1 and h_2, the equation (1) can be defined as follows: the integer m is the arity of (R, S), $t = m$, and p is the arity of $g : A^p \to A^m$. For $1 \leq i \leq m = t$, let $g_i = {g'}_i$ be the ith component of g, i.e. we have

$$g(a) = (g_1(a), \ldots, g_m(a))$$

for all $a \in A^p$. The maps h_1, h_2 in (1) are given by Fact 2. □

It is not difficult to see that both Fact 2 and Theorem 1 itself would fail if we allowed B to be a singleton. However, the implication $(i) \Rightarrow (ii)$ in Theorem 1 would continue to hold.

3 Definability of Function Classes by Invariant Constraints

The question of definability of Boolean function classes by constraints (R, S), where $R, S \subseteq \{0,1\}^n$ are of a special algebraic kind, was considered in [1]. Specifically, the relations R and S were required to be affine subspaces of the vector space $\{0,1\}^n$ over the two-element field $\mathbf{GF}(2)$. A subset of $\{0,1\}^n$ is an affine subspace if and only if it is closed under the triple sum operation $u+v+w$, i.e. if and only if it is invariant under the clone $\mathcal{L}_{01}$ of constant-preserving linear Boolean functions - that is, functions which are the sum of an odd number of variables. (See e.g. Godement [6].) Also it is well known that the non-empty affine subspaces can be described as ranges of affine maps, and that affine hyperplanes can be described as kernels of affine forms, i.e. as sets on which a given form agrees with the null form. As shown in [1], this accounts for the definability of certain function classes by linear equations.

In this section we consider general notions of closure for the antecedent R and the consequent S of a constraint (R, S), and we address the question of definability of classes of B-valued functions on a set A by such invariant constraints, without any restriction on the underlying sets A and B.

Associativity Lemma. *Consider arbitrary non-empty sets A, B, C and E, and let $\mathcal{I}$ be a class of E-valued functions on C, $\mathcal{J}$ a class of C-valued functions on B, and $\mathcal{K}$ a class of B-valued functions on A. The following hold:*

(i) $(\mathcal{I}\mathcal{J})\mathcal{K} \subseteq \mathcal{I}(\mathcal{J}\mathcal{K})$*;*

(ii) If $\mathcal{J}$ is stable under right composition with the clone of projections on B, then $(\mathcal{I}\mathcal{J})\mathcal{K} = \mathcal{I}(\mathcal{J}\mathcal{K})$.

Proof. The inclusion (i) is a direct consequence of the definition of function class composition. Property (ii) asserts that the converse inclusion also holds if $\mathcal{J}$ is stable under right composition with projections. A typical function in $\mathcal{I}(\mathcal{J}\mathcal{K})$ is of the form

$$f(g_1(h_{11}, \ldots, h_{1m_1}), \ldots, g_n(h_{n1}, \ldots, h_{nm_n}))$$

where f is in $\mathcal{I}$, the g_i's are in $\mathcal{J}$, and the h_{ij}'s are in $\mathcal{K}$. By taking appropriate functions $g'_1, \ldots, g'_n$ obtained from $g_1, \ldots, g_n$ by addition of inessential variables and permutation of variables, the function above can be expressed as

$$f(g'_1(h_{11}, \ldots, h_{1m_1}, \ldots, h_{n1}, \ldots, h_{nm_n}), \ldots, g'_n(h_{11}, \ldots, h_{1m_1}, \ldots, h_{n1}, \ldots, h_{nm_n}))$$

which is easily seen to be in $(\mathcal{I}\mathcal{J})\mathcal{K}$. □

Note that statement (ii) of the Associativity Lemma applies, in particular, if $\mathcal{J}$ is any clone on $C = B$.

Let $\mathcal{F}$ be a set of B-valued functions on A. If $\mathcal{P}$ is the clone of all projections on A, then $\mathcal{F}\mathcal{P} = \mathcal{F}$ expresses closure under taking minors as in [8], or closure under simple variable substitutions in the terminology of [2].

For a class $\mathcal{F}$ of A-valued functions on A, an m-ary relation R on A is said to be $\mathcal{F}$-*invariant* if $\mathcal{F}R \subseteq R$. In other words, R is $\mathcal{F}$-invariant if every member of $\mathcal{F}$ preserves R. If two classes of functions $\mathcal{F}$ and $\mathcal{G}$ generate the same clone, then the $\mathcal{F}$-invariant relations are the same as the $\mathcal{G}$-invariant relations. (See Pöschel [10] and [11].) Observe that we always have $R \subseteq \mathcal{F}R$ if $\mathcal{F}$ contains the projections, but we can have $R \subseteq \mathcal{F}R$ even if $\mathcal{F}$ contains no projections. (Take the Boolean triple sum $x_1 + x_2 + x_3$ as the only member of $\mathcal{F}$.)

For a clone $\mathcal{C}$, the intersection of m-ary $\mathcal{C}$-invariant relations is always $\mathcal{C}$-invariant and it is easy to see that, for an m-ary relation R, the smallest $\mathcal{C}$-invariant relation containing R in A^m is $\mathcal{C}R$, and it is said to be *generated by* R. (See [10] and [11], where Pöschel denotes $\mathcal{C}R$ by $\Gamma_{\mathcal{C}}(R)$.)

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be clones on arbitrary non-empty sets A and B, respectively. If R is $\mathcal{C}_1$-invariant and S is $\mathcal{C}_2$-invariant, we say that (R, S) is a $(\mathcal{C}_1, \mathcal{C}_2)$-*constraint*. The following result generalizes Lemma 1 in [1]:

Lemma 2. *Consider arbitrary non-empty sets A and B. Let f be a B-valued function on A, and let $\mathcal{C}$ be a clone on A. If every function in $f\mathcal{C}$ satisfies an A-to-B constraint (R, S), then f satisfies $(\mathcal{C}R, S)$.*

Proof. The assumption means that $(f\mathcal{C})R \subseteq S$. By the Associativity Lemma, $(f\mathcal{C})R = f(\mathcal{C}R)$, and thus $f(\mathcal{C}R) \subseteq S$. □

A class $\mathcal{K}$ of B-valued functions on A is said to be *locally closed* if for every B-valued function f on A the following holds: if every finite restriction of f (i.e restriction to a finite subset) coincides with a finite restriction of some member of $\mathcal{K}$, then f belongs to $\mathcal{K}$.

Theorem 3. *Consider arbitrary non-empty sets A and B and let $\mathcal{C}_1$ and $\mathcal{C}_2$ be clones on A and B, respectively. For any class $\mathcal{K}$ of B-valued functions on A, the following conditions are equivalent:*

(i) $\mathcal{K}$ is locally closed and it is stable both under right composition with $\mathcal{C}_1$ and under left composition with $\mathcal{C}_2$;

(ii) $\mathcal{K}$ is definable by some set of $(\mathcal{C}_1, \mathcal{C}_2)$-constraints.

Proof. To show that $(ii) \Rightarrow (i)$, assume that $\mathcal{K}$ is definable by some set $\mathcal{T}$ of $(\mathcal{C}_1, \mathcal{C}_2)$-constraints. For every (R, S) in $\mathcal{T}$, we have $\mathcal{K}R \subseteq S$. Since R is $\mathcal{C}_1$-invariant, $\mathcal{K}R = \mathcal{K}(\mathcal{C}_1 R)$. By the Associativity Lemma, $\mathcal{K}(\mathcal{C}_1 R) = (\mathcal{K}\mathcal{C}_1)R$, and therefore $(\mathcal{K}\mathcal{C}_1)R = \mathcal{K}R \subseteq S$. Since this is true for every (R, S) in $\mathcal{T}$ we must have $\mathcal{K}\mathcal{C}_1 \subseteq \mathcal{K}$.

For every (R, S) in $\mathcal{T}$, we have $\mathcal{K}R \subseteq S$, and therefore $\mathcal{C}_2(\mathcal{K}R) \subseteq \mathcal{C}_2 S$. By the Associativity Lemma, $(\mathcal{C}_2\mathcal{K})R \subseteq \mathcal{C}_2(\mathcal{K}R) \subseteq \mathcal{C}_2 S$, and $\mathcal{C}_2 S = S$ because S is $\mathcal{C}_2$-invariant. Thus $(\mathcal{C}_2\mathcal{K})R \subseteq S$ for every (R, S) in $\mathcal{T}$, and we must have $\mathcal{C}_2\mathcal{K} \subseteq \mathcal{K}$.

To see that $\mathcal{K}$ is locally closed, consider $f \notin \mathcal{K}$, say of arity $n \geq 1$, and let (R, S) be an m-ary $(\mathcal{C}_1, \mathcal{C}_2)$-constraint that is satisfied by every function g in $\mathcal{K}$ but not satisfied by f. Hence for some $a^1, \ldots, a^n$ in R, $f(a^1, \ldots, a^n) \notin S$ but

$g(a^1, \ldots, a^n) \in S$, for every n-ary function g in $\mathcal{K}$. Thus the restriction of f to the finite set $\{(a^1(i), \ldots, a^n(i)) : i \in \mathbf{m}\}$ does not coincide with that of any member of $\mathcal{K}$.

To prove $(i) \Rightarrow (ii)$, we show that for every function g not in $\mathcal{K}$, there is a $(\mathcal{C}_1, \mathcal{C}_2)$-constraint (R, S) which is satisfied by every member of $\mathcal{K}$ but not satisfied by g. The class $\mathcal{K}$ will then be definable by the set $\mathcal{T}$ of those $(\mathcal{C}_1, \mathcal{C}_2)$-constraints that are satisfied by all members of $\mathcal{K}$.

Note that $\mathcal{K}$ is a fortiori stable under right composition with the clone containing all projections, that is, $\mathcal{K}$ is closed under simple variable substitutions. We may assume that $\mathcal{K}$ is non-empty. Suppose that g is an n-ary B-valued function on A which is not in $\mathcal{K}$. Since $\mathcal{K}$ is locally closed, there is a finite restriction g_F of g to a finite subset $F \subseteq A^n$ such that g_F disagrees with every function in $\mathcal{K}$ restricted to F. Suppose that F has size m, and let $a^1, \ldots, a^n$ be m-tuples in A^m, such that $F = \{(a^1(i), \ldots, a^n(i)) : i \in \mathbf{m}\}$. Define R_0 to be the set $\{a^1, \ldots, a^n\}$, and let $S = \{f(a^1, \ldots, a^n) : f \in \mathcal{K}, f \text{ } n\text{-ary}\}$. Clearly, (R_0, S) is not satisfied by g, and it is not difficult to see that every member of $\mathcal{K}$ satisfies (R_0, S). As $\mathcal{K}$ is stable under left composition with $\mathcal{C}_2$, it follows that S is $\mathcal{C}_2$-invariant. Let R be the $\mathcal{C}_1$-invariant relation generated by R_0, i.e. $R = \mathcal{C}_1 R_0$. By Lemma 2, the constraint (R, S) constitutes indeed the desired separating $(\mathcal{C}_1, \mathcal{C}_2)$-constraint. □

This generalizes the characterizations of closed classes of functions given by Pippenger in [8] as well as in [1] and [2] by considering arbitrary underlying sets, possible infinite, and more general closure conditions. In the finite case, we obtain as special cases of Theorem 3 the characterizations given in Theorem 2.1 and Theorem 3.2 in [8], by taking $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{P}$, and $\mathcal{C}_1 = \mathcal{U}$ and $\mathcal{C}_2 = \mathcal{P}$, respectively, where $\mathcal{U}$ is a clone containing only functions having at most one essential variable, and $\mathcal{P}$ is the clone of all projections. Taking $A = B = \{0, 1\}$ and $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{L}_{01}$, we obtain the characterization of classes of Boolean functions definable by sets of affine constraints given in [1]. For arbitrary non-empty underlying sets, Theorem 1 in [2] corresponds to the particular case $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{P}$. In this case, from Theorem 1 and Theorem 3 we conclude the following:

Corollary 4. *Consider arbitrary non-empty sets A and B. The equationally definable classes of B-valued functions on A are exactly those locally closed classes that are stable under right composition with the clone of projections on A.*

In certain cases, given a $(\mathcal{C}_1, \mathcal{C}_2)$-constraint (R, S), $R \subseteq A^m$, $S \subseteq B^m$, the construction of a functional equation given in the proof of Theorem 1 in the previous section can be refined to yield a functional equation with special algebraic syntax. To do this, one may seek to use, instead of arbitrary functions as given by Fact 1 and Fact 2 in the proof of Theorem 1, functions $g_1, \ldots, g_m, h_1, h_2$ of a particular kind still satisfying the conditions of these Facts. For example, in [1], the functions were chosen to be affine maps, based on the range-and-kernel theory of linear algebra. Another application of this strategy will be given in Section 4.

Also, in certain cases, given a functional equation (1) with a special algebraic syntax, if the functions $g_1, \ldots, g_m, {g'}_1, \ldots, {g'}_t, h_1, h_2$ appearing in the equation have

particular structure-preserving properties, then it may be possible to conclude that the construction of the constraint (R, S), as given in the first part of the proof of Theorem 1, yields relations R and S invariant under certain clones $\mathcal{C}_1$ and $\mathcal{C}_2$. Thus the affine functions appearing in the "linear" functional equations defined in [1] were used to construct affine constraints. The same principle, together with Theorem 3, will be used in Section 4 to show that certain natural function classes cannot be defined by a particular type of functional equations.

4 Functions of Boolean Variables Valued in a Ring

In this section we consider functions $\{0,1\}^n \to B$, where B is a commutative ring. We view $\{0,1\}$ as endowed with the two-element field structure, $\{0,1\} = \mathbf{GF}(2)$, as well as with the lattice structure where $0 < 1$. If B is also $\{0,1\} = \mathbf{GF}(2)$, then these B-valued functions are called Boolean functions. If B is the field $\mathbb{R}$ of real numbers, then the functions under consideration are called *pseudo-Boolean functions*, which provide an algebraic representation for set functions $\mathcal{P}(E) \to \mathbb{R}$ for finite E (see e.g. [4] for a recent reference).

Every Boolean function $\{0,1\}^n \to \{0,1\}$ is well known to be representable by a unique multilinear polynomial in n indeterminates over $\mathbf{GF}(2)$, i.e. a polynomial which is linear in each of its indeterminates, called its *Zhegalkin polynomial*, *Reed-Muller polynomial* or *ring-sum expansion*. Also, pseudo-Boolean functions can be uniquely represented by multilinear polynomials in n indeterminates over $\mathbb{R}$ (see Hammer and Rudeanu [7]).

Consider any commutative ring B with null and identity elements 0_B and 1_B, respectively. For a polynomial $p \in B[X_1, \ldots, X_n]$ in n indeterminates, and an n-tuple $(a_1, \ldots, a_n) \in \{0,1\}^n$, for each a_i let a_i^B denote 0_B or 1_B according to whether a_i is 0 or 1, and denote the evaluation $p(a_1^B, \ldots, a_n^B)$ simply by $p(a_1, \ldots, a_n)$. The B-valued function on $\{0,1\}$ given by

$$(a_1, \ldots, a_n) \mapsto p(a_1, \ldots, a_n)$$

is said to be *represented* by p. By a method similar to that used by Hammer and Rudeanu [7] in the case $B = \mathbb{R}$, we show in the next theorem the existence of a unique multilinear polynomial representation for any B-valued function on $\{0,1\}$, for any commutative ring B with identity. This unifies the Zhegalkin and pseudo-Boolean polynomial representations.

Theorem 5. *Consider any commutative ring B with identity. For any $n \geq 1$, every B-valued function f on $\{0,1\}$, $f : \{0,1\}^n \to B$, is represented by a unique multilinear polynomial $p \in B[X_1, \ldots, X_n]$.*

Proof. The existence of representation is proved by induction on essential arity. For essential arity 0, i.e. for constant functions, representation by constant polynomials is obvious. For a function $f : \{0,1\}^n \to B$ with essential arity $m > 0$, assuming the claim proved for lesser essential arities, and taking any index i such that the ith

variable of f is essential, let f_0 and f_1 be the n-ary B-valued functions given by

$$f_0(a_1,\ldots,a_n) = f(a_1,\ldots a_{i-1},0,a_{i+1},\ldots,a_n)$$
$$f_1(a_1,\ldots,a_n) = f(a_1,\ldots a_{i-1},1,a_{i+1},\ldots,a_n).$$

We have

$$f(a_1,\ldots,a_n) = (1-a_i^B)f_0(a_1,\ldots,a_n) + a_i^B f_1(a_1,\ldots,a_n)$$

and both f_0 and f_1 have essential arity less than m. By the induction hypothesis, f_0 and f_1 are represented by polynomials p_0 and p_1, respectively. Thus f is represented by the polynomial

$$p = (1-X_i)p_0 + X_i p_1$$

and if p had any powers of indeterminates X_j^k with $k>1$, by replacing each such occurrence by X_j we would obtain a multilinear polynomial representing f.

Uniqueness is proved by contradiction. Suppose that f had two distinct multilinear polynomial representations p and q. Then the multilinear polynomial $p-q$ would represent the constant zero function. Let J be a set of indices of smallest possible size, such that the monomial $c\prod_{j\in J} X_j$ occurs in $p-q$ with coefficient $c \neq 0_B$: such a J must exist if $p-q$ is not the zero polynomial. But then the evaluation of $p-q$ at $(a_1,\ldots,a_n)$, where $a_j = 1_B$ if $j\in J$ and $a_j = 0_B$ otherwise, would be $c \neq 0_B$, contradicting the fact that $p-q$ represents the constant zero function. Thus $p-q$ must be the null polynomial, i.e. $p=q$. □

Let f be a B-valued function on $\{0,1\}$, $f:\{0,1\}^n \to B$, where B is a commutative ring with identity. The *degree* of f is the smallest non-negative integer d such that for every $J\subseteq\{1,\ldots,n\}$ of size $\mid J \mid > d$ the coefficient of $\prod_{j\in J} X_j$ in the multilinear polynomial representation of f is zero. Thus the functions of degree 0 are precisely the constants (including the constant zero function).

Theorem 6. *If B is any field of characteristic 2, and $k\geq 1$, then the class of B-valued functions on $\{0,1\}$ having degree less than k is defined by the following functional equation (with vector variables $\mathbf{v}_1,\ldots,\mathbf{v}_k$):*

$$\sum_{I\subseteq\{1,\ldots,k\}} \mathbf{f}(\sum_{i\in I}\mathbf{v}_i) = 0 \qquad (3)$$

In (3) the inner summations refer to addition of vectors over the two-element field $\mathbf{GF}(2)=\{0,1\}$, while the outer summation refers to addition in the field B. For $I=\emptyset$, the empty sum $\sum_{i\in I}\mathbf{v}_i$ represents the constant zero.

Proof. First we prove that (3) is satisfied by every B-valued function on $\{0,1\}$ having degree less than k. From the form of the equation (3), it is easy to see that the class of functions satisfying (3) is closed under linear combinations with coefficients in B. Therefore, it is sufficient to prove that, for $n\geq 1$, every n-ary B-valued function f on $\{0,1\}$ represented by a product of less than k indeterminates, i.e. of the form $\prod_{j\in J} X_j$, $\mid J \mid < k$, $J\subseteq\{1,\ldots,n\}$, satisfies (3) .

Let $v_1, \ldots, v_k$ be any n-vectors in $\{0,1\}^n$. Let w^J be the characteristic vector of J in $\{0,1\}^n$, i.e. $w^J = (a_1, \ldots, a_n)$, where $a_j = 1$ if $j \in J$, and $a_j = 0$ otherwise. For every $I \subseteq \{1, \ldots, k\}$, consider the vector $w^J \cdot (\sum_{i \in I} v_i)$ in $\{0,1\}^n$, where the product $\cdot$ is defined componentwise. Observe that there are 2^k possible choices for I, yet due to the size of $\mid J \mid < k$, there at most 2^{k-1} distinct vectors of the form $w^J \cdot (\sum_{i \in I} v_i)$ in $\{0,1\}^n$. Therefore, there are distinct subsets I_1, I_2 of $\{1, \ldots, k\}$, such that

$$w^J \cdot (\sum_{i \in I_1} v_i) = w^J \cdot (\sum_{i \in I_2} v_i)$$

and for the symmetric difference D of I_1 and I_2, we have

$$w^J \cdot (\sum_{i \in D} v_i) = 0$$

The 2^k subsets of $\{1, \ldots, k\}$, are matched into pairs $\{I, I + D\}$, where $I + D$ is the symmetric difference of I and D, and because f is represented by $\prod_{j \in J} X_j$, by the definition of w^J it follows that for each such pair we have

$$f(\sum_{i \in I} v_i) = f(w^J \cdot (\sum_{i \in I} v_i)) = f(w^J \cdot (\sum_{i \in I+D} v_i)) = f(\sum_{i \in I+D} v_i)$$

Therefore, due to the fact that the underlying field B has characteristic 2, the terms in the equation cancel pairwise.

Conversely, suppose now that the n-ary function f is represented by a polynomial of degree greater than or equal to k. We show that f does not satisfy the equation (3).

Let g be the B-valued function on $\{0,1\}$ represented by the sum of those monomials in the polynomial representation of f which have degree less than k. By the first part of the proof, g satisfies (3). Working towards a contradiction, suppose that f satisfies (3). Given the form of equation (3), this is the case if and only if the n-ary function $h = f + g$, represented by the sum of all monomials in the polynomial representation of f having degree greater than or equal to k, satisfies (3).

Let J be an inclusionwise minimal subset of $\{1, \ldots, n\}$, such that the monomial $c \prod_{j \in J} X_j$ appears in the polynomial representation of h with coefficient $c \neq 0_B$. Note that $\mid J \mid \geq k$. We claim that if f (or equivalently, h) satisfies (3), then the function $h_{\mathbf{k}}$ represented by the monomial $c \prod_{j \in \mathbf{k}} X_j$ where $\mathbf{k} = \{1, \ldots, k\}$, also satisfies equation (3).

Observe that, by the construction in the proof of Theorem 1, equation (3) is equivalent to a constraint (R, S) whose antecedent R is the range of a linear map with codomain $\mathbf{GF}(2)^m$, i.e. R is a subspace of the vector space $\mathbf{GF}(2)^m$ over $\mathbf{GF}(2)$. Thus by Theorem 3 it follows that the class $\mathcal{K}$ of functions satisfying (3) is stable under right composition with the clone $\mathcal{L}_0$ of 0-preserving linear Boolean functions. In particular, $\mathcal{K}$ is closed under permutation and identification of variables, as well as under fixing variables to 0. It is not difficult to see that $h_{\mathbf{k}}$ can be

obtained from h by a combination of these operations. In other words, if h satisfies the equation (3), then $h_{\mathbf{k}}$ also satisfies the equation.

Now, let $v_1, \ldots, v_k$ be the unit n-vectors $e_1, \ldots, e_k$ in $\{0,1\}^n$. We have

$$\sum_{I \subseteq \mathbf{k}} h_{\mathbf{k}}(\sum_{i \in I} v_i) = h_{\mathbf{k}}(\sum_{i \in \mathbf{k}} v_i) = c \neq 0$$

which shows that $h_{\mathbf{k}}$ does not satisfy the equation (3), and yields the desired contradiction. □

In [1] it was shown that, for any positive integer k, the class of Boolean functions whose Zhegalkin polynomial has degree less than k, can be defined by "linear" equations. Theorem 6 above explicitly gives such an equation for every $k \geq 1$. For $k = 1$, the equation (3) can be rewritten as $\mathbf{f}(\mathbf{v}) = \mathbf{f}(0)$, and for $k = 2$, as $\mathbf{f}(\mathbf{v} + \mathbf{w}) = \mathbf{f}(\mathbf{v}) + \mathbf{f}(\mathbf{w}) + \mathbf{f}(0)$.

If B is a field and $A = \{0,1\} = \mathbf{GF}(2)$, then a functional equation (1) is called *linear* if the functions $g_1, \ldots, g_m, {g'}_1, \ldots, {g'}_t$ are all affine maps from the p-dimensional vector space $\mathbf{GF}(2)^p$ to $\mathbf{GF}(2)$, and h_1, h_2 are affine maps from the B-vector spaces B^m and B^t, respectively, to the scalar field B. (Recall that a function $F^n \to F$, where F is any field, is affine if and only if it is of the form $(a_1, \ldots, a_n) \mapsto c_1 a_1 + \ldots c_n a_n + c$, for fixed scalars $c_1, \ldots, c_n, c$ in F.) Obviously, the functional equation (3) in Theorem 6 is linear. Our next result shows that the requirement on the characteristic of the underlying field is indeed essential.

Theorem 7. *For any field B of characteristic different from 2, and any $k \geq 2$, the class of B-valued functions on $\{0,1\}$ having degree less than k is not definable by any set of linear functional equations.*

Proof. As in the proof Theorem 6, if there would be a $k \geq 2$ such that the class $\mathcal{K}$ of B-valued functions on $\{0,1\}$ having degree less than k is definable by some set of linear functional equations, then, using the construction given in the proof of Theorem 1, we would conclude that the class in question is definable by some set of constraints whose antecedents are affine subspaces of vector spaces over $\mathbf{GF}(2)$. These affine subspaces would be closed under the triple sum $u+v+w$, i.e. invariant under the clone $\mathcal{L}_{01}$ of constant-preserving linear Boolean functions. By Theorem 3, this would imply that $\mathcal{K}$ is stable under right composition with the clone $\mathcal{L}_{01}$. We show that this is not the case.

Consider the $(k-1)$-ary function f represented by the monomial $X_1 \ldots X_{k-1}$. Let τ be the $(k+1)$-ary Boolean function in $\mathcal{L}_{01}$ given by

$$(a_1, \ldots, a_{k+1}) \mapsto a_{k-1} + a_k + a_{k+1}$$

Note that the B-valued function τ_B defined on $\{0,1\}$ which is valued 1_B on exactly those vectors $(a_1, \ldots, a_{k+1})$ for which $\tau(a_1, \ldots, a_{k+1}) = 1$ and valued 0_B otherwise, is represented by the polynomial

$$X_{k-1} + X_k + X_{k+1} - 2X_{k-1}X_k - 2X_kX_{k+1} - 2X_{k-1}X_{k+1} + 4X_{k-1}X_kX_{k+1}$$

where + and − are to be interpreted in B. Thus, the composition $f(f_1, \ldots, f_{k-1})$, where $f_{k-1} = \tau$ and f_i is the $(k+1)$-ary ith projection function

$$(a_1, \ldots, a_{k+1}) \mapsto a_i$$

for $k = 1, \ldots, k-2$, is represented by the polynomial in $k+1$ indeterminates

$$X_1 \ldots X_{k-2}(X_{k-1} + X_k + X_{k+1} - \\ - 2X_{k-1}X_k - 2X_kX_{k+1} - 2X_{k-1}X_{k+1} + 4X_{k-1}X_kX_{k+1})$$

where + and − are to be interpreted in B. From the fact that B has characteristic different from 2, it follows that this polynomial has degree greater than k. □

Note that for $k = 1$, the class of functions of degree less that k, i.e. the class of constants, is defined by the linear expression $\mathbf{f}(\mathbf{v}) = \mathbf{f}(0)$. In fact, from Theorem 7 above it follows that, if B is any field of characteristic different from 2, then the set of constants is the only linearly definable class of B-valued functions on $\{0,1\}$ of bounded degree. However, Corollary 4 guarantees the existence of equational characterizations of these classes, because bounded degree classes are stable under right composition with the minimal clone $\mathcal{P}$ containing only projections. The following generalization of Corollary 3.3 in [4] provides an equation characterizing classes of bounded degree functions of Boolean variables, and whose codomain is any commutative ring with identity.

Theorem 8. *If B is any commutative ring with identity, and $k \geq 1$, then the class of B-valued functions on $\{0,1\}$ having degree less than k is defined by the following functional equation (with vector variables $\mathbf{v}_1, \ldots, \mathbf{v}_k$):*

$$\mathbf{f}(\bigwedge_{i \in \mathbf{k}} \mathbf{v}_i) + \sum_{\substack{I \subseteq \mathbf{k} \\ I \neq \emptyset}} (-1)^{|I|} \mathbf{f}(\bigvee_{j \in I} \bigwedge_{i \in \mathbf{k} \setminus \{j\}} \mathbf{v}_i) = 0 \qquad (4)$$

where $\mathbf{k} = \{1, \ldots, k\}$.

In (4) the summation refers to addition in the commutative ring B. Equation (4) was obtained in [4] as a combination of two opposite inequalities in the ordered real field $B = \mathbb{R}$. Inequalities are not available in general in a commutative ring, in particular in finite fields. However, the following direct proof, based on the principles used in establishing the functional inequality in Theorem 3.1 in [4], can still be used in the arbitrary commutative ring context.

Proof. First we show that every B-valued function on $\{0,1\}$ of degree less than k satisfies equation (4). As in the proof of Theorem 6, it is enough to show that every monomial of degree less than k satisfies equation (4), because every linear combination (with coefficients in B) of functions satisfying (4), also satisfies the equation.

Let f be an n-ary B-valued function on $\{0,1\}$ represented by $\prod_{j \in J} X_j$, $\mid J \mid < k$, $J \subseteq \{1, \ldots, n\}$. Let w^J be the characteristic vector of J in $\{0,1\}^n$. Let $v_1, \ldots, v_k$

be any n-vectors in $\{0,1\}^n$, and let u denote their conjunction $\bigwedge_{i\in\mathbf{k}} v_i$. For every $j \in \mathbf{k} = \{1,\ldots,k\}$, let

$$u_j = \bigwedge_{i\in\mathbf{k}\setminus\{j\}} v_i$$

and let the vector $z(I)$ be defined by

$$z(I) = w^J \cdot (\bigvee_{j\in I} u_j) \quad \text{for } \emptyset \neq I \subseteq \mathbf{k}, \text{ and } \quad z(\emptyset) = w^J \cdot u$$

where the product $\cdot$ is defined componentwise. From the fact that $k >\mid J \mid$, it follows that there is an $l \in \mathbf{k}$ such that

$$w^J \cdot u = w^J \cdot u_l$$

Fix such an index l. It is not difficult to see that, for every $I \subseteq \mathbf{k}$, we have

$$f(\bigvee_{j\in I} u_j) = f(z(I)) \quad \text{and} \quad z(I) = z(I + \{l\})$$

and thus the terms in the sum

$$f(\bigwedge_{i\in\mathbf{k}} v_i) + \sum_{\substack{I\subseteq\mathbf{k}\\ I\neq\emptyset}} (-1)^{|I|} f(\bigvee_{j\in I} u_j)$$

cancel pairwise, i.e. the sum is zero, which shows that f satisfies (4).

In order to complete the proof of Theorem 8, we need to show that if f is an n-ary function of degree greater than or equal to k, then equation (4) is not satisfied by f. Let g and h be the n-ary functions represented by the sum of monomials, in the polynomial representation of f, having degree less than k and greater than or equal to k, respectively. As in the proof of Theorem 6, f satisfies equation (4) if and only if h satisfies the equation. We prove that h does not satisfy (4).

Let J be an inclusionwise minimal subset of $\mathbf{n} = \{1,\ldots,n\}$, such that the monomial $c\prod_{j\in J} X_j$ appears in the polynomial representation of h, with coefficient $c \neq 0_B$. Note that $\mid J \mid \geq k$. Let J_0 be any subset of J of size k. For every $j \in J_0$, consider the n-vectors $y_j = (a_1,\ldots,a_n)$, where $a_j = 0$, $a_i = 0$ if $i \notin J$, and $a_i = 1$ if $i \in J \setminus \{j\}$. Let $v_1,\ldots,v_k$ be defined as the vectors y_j, $j \in J_0$, in any order. Let $u = \bigwedge_{i\in\mathbf{k}} v_i$, and for each $j \in \mathbf{k}$, let

$$u_j = \bigwedge_{i\in\mathbf{k}\setminus\{j\}} v_i$$

Observe that for $I \subseteq \mathbf{k}$, all monomials in the polynomial representation of h are evaluated to zero on

$$\bigvee_{j\in I} u_j$$

except in the case $I = \mathbf{k}$, where the only monomial which has non-zero value is $c\prod_{j\in J} X_j$, because the n-vector

$$\bigvee_{j\in\mathbf{k}} u_j = (a_1, \ldots, a_n)$$

is given by $a_t = 1$ if $t \in J$, and $a_t = 0$ otherwise. Therefore, we have

$$h(\bigwedge_{i\in\mathbf{k}} v_i) + \sum_{\substack{I\subseteq\mathbf{k}\\ I\neq\emptyset}} (-1)^{|I|} h(\bigvee_{j\in I} u_j) = (-1)^k h(\bigvee_{j\in\mathbf{k}} u_j) = (-1)^k c \neq 0$$

which shows that h, and thus f, does not satisfy equation (4). □

Theorem 8 provides in particular an alternative equational characterization of classes of Boolean functions whose Zhegalkin polynomials have degree bounded by a positive integer k.

References

[1] M. Couceiro, S. Foldes. "Definability of Boolean Function Classes by Linear Equations over GF(2)", *Discrete Applied Mathematics* 142 (2004) 29–34.

[2] M. Couceiro, S. Foldes. "On Closed Sets of Relational Constraints and Classes of Functions Closed under Variable Substitutions", *Algebra Universalis*, **54** (2005) 149–165.

[3] O. Ekin, S. Foldes, P.L. Hammer, L. Hellerstein. "Equational Characterizations of Boolean Functions Classes", *Discrete Mathematics* 211 (2000) 27–51.

[4] S. Foldes, P.L. Hammer. "Submodularity, Supermodularity and Higher Order Monotonicities of Pseudo-Boolean Functions", *Mathematics of Operations Research* **30** 2 (2005) 453-461.

[5] S. Foldes, G. R. Pogosyan. "Post classes characterized by functional terms", *Discrete Applied Mathematics* 142 (2004) 3551.

[6] R. Godement. *Algebra*, Kershaw Publishing Company, 1969.

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

[8] N. Pippenger. "Galois Theory for Minors of Finite Functions", *Discrete Mathematics* 254 (2002) 405–419.

[9] G. R. Pogosyan. "Classes of Boolean Functions Defined by Functional Terms", *Multiple -Valued Logic* **7** 5–6 (2001) 417–448.

[10] R. Pöschel. "Concrete Representation of Algebraic Structures and a General Galois Theory", *Contributions to General Algebra*, Proceedings Klagenfurt Conference, May 25-28 (1978) 249–272. Verlag J. Heyn, Klagenfurt, Austria 1979.

[11] R. Pöschel. "A General Galois Theory for Operations and Relations and Concrete Characterization of Related Algebraic Structures", Report R-01/80. *Zentralinstitut für Math. und Mech.*, Berlin 1980.

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

[13] C. Wang, A.C. Williams. "The Threshold Order of a Boolean Function", *Discrete Applied Mathematics* 31 (1991) 51–69.

[14] D. J. A. Welsh. *Matroid Theory*, Academic Press, 1976.

[15] I. E. Zverovich. "Characterization of Closed Classes of Boolean Functions in Terms of Forbidden Subfunctions and Post Classes", *Discrete Applied Mathematics* 149 (2005) 200-218.