RUTCOR
RESEARCH
REPORT

On Generalized Constraints and Certificates

Lisa Hellerstein[a]

RRR 26-98, September, 1998

RUTCOR
Rutgers Center for
Operations Research
Rutgers University
640 Bartholomew Road
Piscataway, New Jersey
08854-8003
Telephone: 732-445-3804
Telefax: 732-445-5472
Email: rrr@rutcor.rutgers.edu
http://rutcor.rutgers.edu/~rrr

[a]Polytechnic University, 5 Metrotech Center, Brooklyn, NY, 11201, hstein@duke.poly.edu

RUTCOR RESEARCH REPORT
RRR 26-98, SEPTEMBER, 1998

ON GENERALIZED CONSTRAINTS AND CERTIFICATES

Lisa Hellerstein

Abstract. Ekin, Foldes, Hammer, and Hellerstein showed that a set of Boolean functions is characterizable by a (possibly infinite) set of Boolean equations iff it is closed under permutation of variables, addition of dummy variables, and identification of variables. Subsequently, Pippenger introduced constraint characterizations, which generalize previous characterizations of clones. He showed that a set of finite functions can be characterized by a set of constraints iff it is characterizable by Boolean equations. He also developed a Galois theory for sets of finite functions characterizable by constraints. In this paper we generalize Pippenger's results by considering sets of finite functions, such as the unate functions, that are closed under permutation of variables and addition of dummy variables but not necessarily under identification of variables. We introduce the notion of a generalized constraint, and consider the question of which sets of functions can be characterized by finite sets of generalized constraints. We show a relation between sets of finite functions with this property, and sets of finite functions that have constant-size certificates of non-membership. We show that the set of linear threshold functions cannot be characterized by a finite set of generalized or standard constraints. Finally, we extend Pippenger's Galois theory results to generalized constraints.

Acknowledgements: The author gratefully acknowledges the the partial support of NSF Grant CCR-9501660.

1 Introduction

Ekin, Foldes, Hammer, and Hellerstein considered the problem of characterizing sets of Boolean functions using Boolean equations [2]. They gave a number of examples of sets characterizable by such equations. For example, the set of positive (monotone increasing) Boolean functions is characterized by the single equation $f(\boldsymbol{a})f(\boldsymbol{a} \vee \boldsymbol{b}) = f(\boldsymbol{a})$, where $\boldsymbol{a}$ and $\boldsymbol{b}$ are interpreted as arbitrary elements in the domain of f, and $\vee$ is componentwise conjunction. Ekin et al. showed that a set of Boolean functions is characterizable by a (possibly infinite) set of equations iff it is closed under *identification minors*. By definition, a set is closed under identification minors if it is closed under addition of dummy variables, permutation of variables, and identification of variables (also called diagonalization).[1]

Subsequently, Pippenger introduced the notion of a constraint [19]. Let $B_k = \{0, \ldots, k-1\}$ and let a finite function be a map $f : B_k^n \to B_l$ where $n \geq 1$. Roughly speaking, a constraint restricts the behavior of a finite function on certain sets of its inputs. Thus a constraint may be satisfied by some Boolean functions and not by others. Constraints are generalizations of the "invariants" defined by Geiger and independently by Bodnarchuk, Kaluzhinin, Kotov, and Romov in their work on clones [1, 8]. Clones are sets of Boolean functions that are closed under identification minors and composition, and which contain the monadic identity function $f(x_1) = x_1$ (cf. [18]).

Pippenger showed that a set of Boolean functions is characterizable by a set of constraints iff it is characterizable by a set of Boolean equations. He also developed a Galois theory (in the sense of Everett [4], Ore [17], and Ward [21]) for sets of finite functions closed under identification minors. In this theory, the primal objects are finite functions and the dual objects are constraints. Pippenger showed that a set of finite functions is characterizable by a (possibly infinite) set of constraints iff it is closed under identification minors. Dually, he showed that a set of constraints is characterizable by a (possibly infinite) set of functions iff it is closed under certain operations on constraints. He also extended the Galois theory to functions closed under identification minors and under some additional operations (such as substitution of variables by constants and complementation of variables).

However, the above Galois theory results do not apply to sets of functions such as the unate functions, which are not closed under identification of variables. In this paper we consider sets of finite functions, such as the unate functions, that are closed under permutation of variables and addition of dummy variables but not necessarily under identification of variables. We say that such sets of functions are closed under *special minors*. We define the notion of a *generalized constraint* to deal with such functions.

We show a connection between sets that can be characterized by finite sets of generalized constraints, and sets closed under special minors that have constant-size *certificates of non-membership* (defined below). We show that if $\mathcal{F}$ is a set of finite functions closed under special

[1] Boolean equations were defined precisely by Pippenger [19]. In fact, Ekin et al. proved their results not for Boolean equations, but for a slightly more general class of expressions that they called identities. They also defined identification minors in a slightly different way than we define them here. Here we follow the definitions used by Pippenger [19], and state our results accordingly.

minors, then $\mathcal{F}$ has constant-size certificates of non-membership iff $\mathcal{F}$ can be characterized by a finite set of generalized constraints. The analogous statement holds for $\mathcal{F}$ if it is closed under identification minors and standard (not generalized) constraints.

Ekin et al. showed that there are sets of Boolean functions that can be characterized by an infinite set of Boolean equations but not by a finite set. Pippenger generalized this result. Because of the correspondence between Boolean equations and constraints, the sets constructed by Ekin et al. can be characterized by an infinite set of constraints, but not by a finite set. The sets constructed by Ekin et al. and by Pippenger are somewhat artificial. We show that a widely-studied set, the set of threshold functions, also has the property that it can be characterized by an infinite set of (generalized or standard) constraints, but not by a finite set. We also consider some sets of "renamable" functions which were proved by Ekin et al. not to be closed under identification minors, but which are closed under special minors. We explore whether these sets have constant-size certificates of non-membership, or equivalently, characterizations by a finite set of generalized constraints.

Finally, we generalize Pippenger's Galois theory. We define the sets of finite functions as the primal objects and generalized constraints as the dual objects. We extend his dual results on finite functions and constraints to apply to finite functions and generalized constraints.

2 Preliminaries

Let $k, l \geq 1$. An n-adic (k, l)-ean function is a map $f : B_k^n \rightarrow B_l$. A (k, k)-ean function is called simply a k-ean function.

Consider a set $\mathcal{F}$ of (k, l)-ean finite functions. Let g be a (k, l)-ean finite function that is not in $\mathcal{F}$. A subset D of the domain of g is called a *certificate of non-membership* of g in $\mathcal{F}$ if for every n-adic function in $\mathcal{F}$, there exists some $a \in D$ such that $f(a) \neq g(a)$. The *size* of the certificate D is defined to be the number of elements of D. Let $\mathcal{N} = \{0, 1, \ldots\}$ denote the natural numbers, and let $p : \mathcal{N} \rightarrow \mathcal{N}$. A set $\mathcal{F}$ of (k, l)-ean finite functions has *certificates of non-membership of size* $p(n)$ if for each function $g \notin \mathcal{F}$ on n variables, g has a certificate of non-membership in $\mathcal{F}$ of size at most $p(n)$. If $\mathcal{F}$ has certificates of non-membership of size c for some constant c, we say that $\mathcal{F}$ has constant-size certificates. The size of certificates of non-membership for a set of functions $\mathcal{F}$ can have implications for the learnability of functions in $\mathcal{F}$ [10, 9].

Let $a_1, a_2, ...$ be a sequence of natural numbers such that $a_1 \leq a_2 \leq ....$ If the sequence contains a maximum element, we define the limit of the sequence to be the value of that element. Otherwise, we define the limit of the sequence to be ∞. For all $a \in \mathcal{N}$, $a < \infty$. For all $a \in \mathcal{N} \bigcup \{\infty\}$, we define $a + \infty = \infty$.

Let $\mathcal{Q}$ be a set of functions $\phi : A \rightarrow \mathcal{N} \bigcup \{\infty\}$ for some fixed set A. We define a partial order $<$ on functions in $\mathcal{Q}$ as follows: for $\phi, \phi' \in \mathcal{Q}$, $\phi < \phi'$ iff $\phi \neq \phi'$ and for all $a \in A$, $\phi(a) \leq \phi(a')$. We say that ϕ is a maximal element of $\mathcal{Q}$ if there is no $\phi' \in \mathcal{Q}$ such that $\phi < \phi'$. Let $\phi_1, \phi_2, \ldots$ be a sequence of functions in $\mathcal{Q}$ such that $\phi_1 \leq \phi_2 \leq .....$ We define the limit of the sequence to be the function $\phi : A \rightarrow \mathcal{N} \bigcup \{\infty\}$ such that for all

$a \in A$, $\phi(a) = \lim_{i \to \infty} \phi_i(a)$. The set $\mathcal{Q}$ is *chain complete* if $\mathcal{Q}$ contains the limits of all such sequences.

We will use the following two lemmas.

Lemma 2.1 *Let A be a finite set. Let $\mathcal{Q}$ be a set of functions $\phi : A \to \mathcal{N} \bigcup \{\infty\}$. Then the number of maximal elments of $\mathcal{Q}$ is finite.*

Proof.

The lemma follows easily from properties of *well-quasi-ordered sets*. A set S with a relation $\leq$ is well-quasi-ordered if $\leq$ is reflexive and transitive, and for every infinite sequence $x_1, x_2, \ldots$ of elements in S, there exist $i < j$ with $x_i \leq x_j$. Well-quasi-ordered sets contain no infinite anti-chains (cf. [11]) and they are closed under finite products [16]. Since $\mathcal{N} \bigcup \{\infty\}$ is well-quasi-ordered, so is $(\mathcal{N} \bigcup \{\infty\})^{|A|}$, which is in one-to-one correspondence with the set of all functions $\phi : A \to \mathcal{N} \bigcup \{\infty\}$. The correspondence preserves the $\leq$ relation. Thus Q is well-quasi-ordered and contains no infinite anti-chains, and hence it contains only a finite number of maximal elements. □

Lemma 2.2 *Let A be a finite set. Let $\mathcal{Q}$ be a set of functions $\phi : A \to \mathcal{N} \bigcup \{\infty\}$. such that $\mathcal{Q}$ is chain complete. Then for each element $\phi \in \mathcal{Q}$, there exists a maximal element ϕ' of $\mathcal{Q}$ such that $\phi \leq \phi'$.*

Proof. Although this follows easily from Zorn's Lemma (which can be found in e.g. [14], pp. 504–510), we give a short direct proof.

Suppose for contradiction that there exists a $\phi \in \mathcal{Q}$ such that there is no maximal $\phi' \in \mathcal{Q}$ satisfying $\phi \leq \phi'$. Choose such a ϕ so that $|\{a \in A | \phi(a) \neq \infty\}|$ is minimized. Since ϕ itself cannot be maximal, there exists $\phi_1 \in \mathcal{Q}$ such that $\phi < \phi_1$. Since ϕ is not bounded above by a maximal element, ϕ_1 is not maximal, and hence there exists $\phi_2 \in \mathcal{Q}$ such that $\phi < \phi_1 < \phi_2$. Inductively, it follows that there is an infinite sequence of elements in $\mathcal{Q}$, $\phi < \phi_1 < \phi_2 < \ldots$. Let $X = \{a \in A | \phi(a) \neq \infty\}$. Since A is finite, so is X. Since $\mathcal{Q}$ is chain complete, $\mathcal{Q}$ contains the function $\phi^* = \lim_{i \to \infty} \phi_i$. Since $\phi_1 < \phi_2 \ldots$ is an infinite, strictly increasing sequence, there exists an $a^* \in X$ such that $\lim_{i \to \infty} \phi_i(a^*) = \infty$, and thus $\phi^*(a^*) = \infty$. Since $\phi < \phi^*$ and ϕ is not less than any maximal element of $\mathcal{Q}$, it follows that ϕ^*, like ϕ, is not a maximal element of $\mathcal{Q}$ nor is it less than a maximal element of $\mathcal{Q}$. But $|\{a \in A | \phi^*(a) = \infty\}| \leq |X| - 1$ which contradicts the choice of ϕ. □

An m-adic k-ean *repetition function* is a map $\phi : B_k^m \to \mathcal{N} \bigcup \{\infty\}$.

An m-ary (k,l)-ean *generalized constraint* is a pair (ϕ, S) where ϕ is an m-adic k-ean repetition function called the *antecedent*, and $S \subseteq B_l^m$ is called the consequent. We call m the *dimension* of the generalized constraint. A *constraint*, as defined by Pippenger, is equivalent to a generalized constraint in which $\phi(a) \in \{0, \infty\}$ for all $a \in B_k^m$. To avoid confusion, we will call such a constraint a *standard constraint*.

If $M \subseteq B_k^{m \times n}$ is an $m \times n$ matrix of elements from B_k and ϕ is an m-adic k-ean repetition function, we write $M \prec \phi$ to mean that for all $a \in B_k^m$, the number of columns of M that are equal to a is at most $\phi(a)$. If f is an n-adic (k,l)-ean function, we write $f(M)$ for the columns of elements from B_l obtained by applying f to each row of M. If f is an n-adic (k,l)-ean function and (ϕ, S) is an m-ary (k,l)-ean generalized constraints, we say that f *satisfies* (ϕ, S) if for every $m \times n$ matrix M such that $M \prec \phi$, we have that $f(M) \in S$. Note that if (ϕ, S) and (ϕ', S) are two (k,l)-ean generalized constraints such that $\phi < \phi'$, then any (k,l)-ean function f satisfying (ϕ', S) also satisfies (ϕ, S).

We say that a set $\mathcal{F}$ of (k,l)-ean functions is characterized by a set $\mathcal{T}$ of (k,l)-ean generalized constraints if $\mathcal{F}$ is precisely the set of functions satisfying all constraints in $\mathcal{T}$. Similarly, we say that $\mathcal{T}$ is characterized by $\mathcal{F}$ if $\mathcal{T}$ is precisely the set of generalized constraints satisfied by all functions in $\mathcal{F}$.

If $(\phi_1, S), (\phi_2, S), \ldots$ is an infinite sequence of generalized constraints such that $\phi_1 \leq \phi_2 \leq \ldots$, then we say that the generalized constraint $(\lim_{i \to \infty} \phi_i, S)$ is obtained from that sequence by taking the *limit of antecedents*.

In what follows, unless otherwise stated we assume that functions and constraints are finite and (k,l)-ean, for some fixed k and l.

3 Constant-size certificates of non-membership

Theorem 3.1 *Let $\mathcal{F}$ be a set of finite functions closed under special minors. The set $\mathcal{F}$ can be characterized by a finite set of generalized constraints iff it has constant-size certificates of non-membership.*

Proof. Suppose $\mathcal{F}$ is characterized by a finite set $\mathcal{T}$ of generalized constraints. Let m be the maximum dimension of any constraint in $\mathcal{T}$. We show that $\mathcal{F}$ has certificates of non-membership of size m. Let g be an n-adic finite function not in $\mathcal{F}$. Then there exists some generalized constraint (ϕ, S) in $\mathcal{T}$ such that g does not satisfy (ϕ, S). Let m' be the dimension of (ϕ, S). Clearly $m' \leq m$. Since g does not satisfy (ϕ, S), there exists some $m' \times n$ matrix $M \prec \phi$ such that $g(M) \notin S$. For all n-adic functions $f \in \mathcal{F}$, f satisfies (ϕ, S) and hence $f(M) \neq g(M)$. Thus the rows of M form a certificate of non-membership of g in $\mathcal{F}$, and the size of that certificate is at most m.

Conversely, suppose $\mathcal{F}$ has certificates of non-membership of size c, for some constant c. Let g be an n-adic function not in $\mathcal{F}$, and let D be a certificate of non-membership of g in $\mathcal{F}$ that has size $c' \leq c$. Form a $c' \times n$ matrix M whose rows consist of the elements of D in some fixed order. Define the m'-ary generalized constraint (ϕ, S) where $S = B_l^{m'} \backslash \{g(M)\}$, and for all $\mathbf{a} \in B_k^{m'}$, $\phi(\mathbf{a})$ is equal to the number of times that $\mathbf{a}$ appears as a column of M. Because $M \prec \phi$, g does not satisfy (ϕ, S),

We now show that (ϕ, S) is satisfied by every function in $\mathcal{F}$. Suppose not. Then there exists $f \in \mathcal{F}$ such that f does not satisfy (ϕ, S). Suppose f is n'-adic. Then there exists an $m' \times n'$ matrix M' such that $M' \prec \phi$ and $f(M') \notin S$, that is, $f(M') = g(M)$. Since $M' \prec \phi$, for every $\mathbf{a}' \in B_k^{m'}$, the number of times $\mathbf{a}'$ appears as a column of M' is at most the number of times it appears as a column of M. We may therefore define a 1-1 map $h : \{1, \ldots, n'\} \to \{1, \ldots, n\}$ such that column i of M' equals column $h(i)$ of M'. The n-adic function f' defined by $f'(x_1, \ldots, x_n) = f(x_{h(1)}, \ldots, x_{h(n')})$ can be obtained from f by permuation of variables and addition of dummy variables. Note that $f'(M) = f(M') = g(M)$. Since $\mathcal{F}$ is closed under special minors, f' is also in $\mathcal{F}$. But then g and f' have the same output on all elements of D, contradicting that D is a certificate of non-membership of g in $\mathcal{F}$.

Let $\mathcal{T}$ be the set of all (ϕ, S) constructed as above for each g not in $\mathcal{F}$. The generalized constraints in $\mathcal{T}$ characterize $\mathcal{F}$. Consider the closure $\tilde{\mathcal{T}}$ of $\mathcal{T}$ under the operation of taking limits of antecedents. It is easy to show that if a function satisfies an infinite sequence of constraints $(\phi_1, S), (\phi_2, S), \ldots$ such that $\phi_1 \leq \phi_2 \leq \ldots,$ then the function will also satisfy the constraint $(\lim_{i\to\infty} \phi_i, S)$. Therefore the set $\tilde{\mathcal{T}}$ of generalized constraints also characterizes $\mathcal{F}$.

Now consider the set $\mathcal{T}_{max} = \{(\phi, S) \in \tilde{\mathcal{T}} |$ for all $(\phi', S) \in \tilde{\mathcal{T}},\ \phi' \not> \phi\}$. Since each generalized constraint of $\mathcal{T}$ has dimension at most m, the number of different consequents appearing in generalized constraints of $\tilde{\mathcal{T}}$ is finite. Hence by Lemma 2.1, $\mathcal{T}_{max}$ is finite. We now show that $\mathcal{T}_{max}$ characterizes $\mathcal{F}$. The generalized constraints of $\mathcal{T}_{max}$ are satisfied by all functions in $\mathcal{F}$ because $\mathcal{T}_{max}$ is a subset of $\mathcal{T}$. Consider any g not in $\mathcal{F}$. Since $\tilde{\mathcal{T}}$ characterizes $\mathcal{F}$, there exists $(\phi, S) \in \tilde{\mathcal{T}}$ that is not satisfied by g. By Lemma 2.2, there exists a $(\phi', S) \in \mathcal{T}_{max}$ such that $\phi \leq \phi'$. Since g does not satisfy (ϕ, S), it does not satisfy (ϕ', S). It follows that the finite set $\mathcal{T}_{max}$ characterizes $\mathcal{F}$. $\square$

As stated in the introduction, standard constraints are essentially those (ϕ, S) for which the output of ϕ is 0 or ∞ on all inputs. We can prove the following corollary.

Corollary 3.1 *Let $\mathcal{F}$ be a set of finite functions closed under identification minors. The set $\mathcal{F}$ can be characterized by a finite set of standard constraints iff it has constant-size certificates of non-membership.*

Proof. If $\mathcal{F}$ is characterized by a finite set of standard constraints, then it is characterized by a finite set of generalized constraints, and hence by Theorem 3.1 it has constant-size certificates of non-membership.

To prove the converse, suppose $\mathcal{F}$ has constant-size certificates of non-membership. By Theorem 3.1 it can be characterized by a finite set $\mathcal{Q}$ of generalized constraints. We need to show it can be characterized by a finite set of standard constraints. Let $(\phi, S) \in \mathcal{Q}$ and let $Y = \{\boldsymbol{a} \in B_k^m | \phi(a) \neq 0\}$. Consider the constraint $\hat{\phi}$ whose value is ∞ on all elements of $\boldsymbol{a} \in Y$, and whose value is 0 on all $\boldsymbol{a} \notin Y$.

We show that $(\hat{\phi}, S)$ is satisfied by all elements of $\mathcal{F}$. Let $f \in \mathcal{F}$ be an n-adic function in $\mathcal{F}$. Consider an $m \times n$ matrix $M \prec \hat{\phi}$. Let n' be the number of distinct columns appearing in M. Let $I = \{i_1, \ldots, i_{n'}\}$ be the indices of the leftmost occurences of each distinct column in M, where $i_1 < i_2 < \ldots < i_n$. Let $h : \{1, \ldots, n\} \to \{1, \ldots, n'\}$ be such for $1 \leq j \leq n$, $h(j) = t$, where t is such that column j and column i_t of M are equal. Define the function $f'(x_1, \ldots, x_{n'}) = f(x_{h(1)}, x_{h(2)}, \ldots, x_{h(n)})$. The function f' can be obtained from f by identification and permutation of variables. Since $f \in \mathcal{F}$, $f' \in \mathcal{F}$. Let M' be the matrix obtained from M by deleting all but the leftmost occurence of each distinct column. Then $f'(M') = f(M)$. Clearly $M' \prec \phi$, and since $f' \in \mathcal{F}$ and satisfies (ϕ, S), $f'(M') \in S$. Therefore $f(M) \in S$, and f satisfies $(\hat{\phi}, S)$.

Since $\phi \leq \hat{\phi}$, every function satisfying $(\hat{\phi}, S)$ also satisfies (ϕ, S). We may therefore form a new finite set of constraints $\hat{\mathcal{Q}} = \{(\hat{\phi}, S) | (\phi, S) \in \mathcal{Q}\}$ that characterizes $\mathcal{F}$. Since all constraints in $\hat{\mathcal{Q}}$ are standard constraints, this proves the corollary. □

We also have the following complexity theoretic corollary for sets of Boolean functions (an analogous corollary holds for non-Boolean finite functions).

Corollary 3.2 *Let $\mathcal{F}$ be a set of Boolean functions closed under special minors such that $\mathcal{F}$ has constant-size certificates of non-membership. Then the following problem is in co-NP: Given a Boolean formula γ, determine whether γ represents a function in $\mathcal{F}$.*

Proof. By Theorem 3.1, $\mathcal{F}$ can be characterized by a finite set $\mathcal{T}$ of generalized constraints. Let m be the maximum dimension of any constraint in $\mathcal{T}$. Let γ be a Boolean formula representing an n-adic Boolean function g that is not in $\mathcal{F}$. Then there is a certificate D of non-membership of g in $\mathcal{T}$ of size at most m, corresponding to a generalized constraint in $\mathcal{T}$ that is violated by g. In non-deterministic polynomial time, one can guess the elements in the certificate D, evaluate the formula γ on those elements, and verify that g does violate a constraint in $\mathcal{T}$. □

We note that the above corollary does not hold if $\mathcal{F}$ has constant-size certificates of non-membership, but is not closed under special minors. Let S be any non-recursive subset of the natural numbers. Consider the set $\mathcal{F}$ of all n-adic Boolean functions f satisfying either (1) $n \in S$ or (2) $n \notin S$ and the value of f is 0 on all elements of its domain. The set $\mathcal{F}$ has certificates of non-membership of size 1, but determining whether a Boolean formula represents a function in $\mathcal{F}$ is an unsolvable problem, and hence clearly not in co-NP.

Similarly, the corollary does not hold if $\mathcal{F}$ is closed under special minors, but does not have constant-size certificates. Again, let S be any non-recursive subset of the natural numbers. Say that an n-adic Boolean function $f(x_1, \ldots, x_n)$ is an *exactly-one* function if its output is 1 precisely when exactly one of its n input variables x_i is set to 1. Let $\mathcal{C}$ be the set of n-adic Boolean functions f such that $n \in S$ and f is an exactly-one function. Let $\mathcal{F}$ be the closure of $\mathcal{C}$ under special minors (the argument also holds if we consider closure under identification minors). None of the functions in $\mathcal{F} - \mathcal{C}$ is an exactly-one function. Consider any function $g : B_2^n \to B_2$ such that g is an exactly-one function. Then $g \in \mathcal{F}$ iff $n \in S$. It follows that determining whether a formula γ represents a function in $\mathcal{F}$ is an unsolvable problem.

4 Particular sets of Boolean functions

Ekin et al. gave a number of examples of well-known sets of Boolean functions, such as positive and Horn functions, that can be characterized by a finite set of identities, and hence (by Pippenger's result) by a finite set of constraints. Here we give examples of particular sets of Boolean functions that can and cannot be characterized by finite sets of (standard or generalized) constraints.

Threshold functions

We show here that the well-known set of (Boolean) threshold funtions also has the property that it can be characterized by an infinite set of constraints, but not by a finite set. A threshold function is a Boolean function $f(x_1, \ldots, x_n)$ such that there exist real numbers $a_1, \ldots, a_n$ and θ for which $f(x_1, \ldots, x_n) = 1$ iff $\sum_{i=1}^n a_i x_i \geq \theta$. The equation $\sum_{i=1}^n a_i x_i = \theta$ defines a hyperplane that separates the points of B_2^n on which f has the value 1, from the points of B_2^n on which it has the value 0. See Winder [22] or Hu [12] for many early references to threshold functions.

Threshold functions are closed under many operations, including adding dummy variables, identifying variables, permuting variables, complementing variables, and substituting Boolean constants for variables. (These operations define the Boolean minors of Wang and Williams.) Thus, in particular, they are closed under identification minors. It follows directly from the results of Ekin et al. and Pippenger that they can be characterized by a possibly infinite set of constraints. Using early results on threshold functions, we prove that they cannot be characterized by a *finite* set of (standard or generalized) constraints.

We need the following definitions. For a Boolean function $f : B_2^n \rightarrow B_2$, define $f^+ = \{\boldsymbol{a} \in B_2^n | f(\boldsymbol{a}) = 1\}$ and $f^- = \{\boldsymbol{b} \in B_2^n | f(\boldsymbol{b}) = 0\}$. Let $c \geq 2$ be a positive integer. A Boolean function f is c-asummable if given any $\boldsymbol{a}_1, .., \boldsymbol{a}_c$ in f^+ (where $\boldsymbol{a}_1, .., \boldsymbol{a}_c$ not necessarily distinct), and $\boldsymbol{b}_1, ..., \boldsymbol{b}_c$ in f^- (also not necessarily distinct)

$$\boldsymbol{a}_1 + \boldsymbol{a}_2 + .. + \boldsymbol{a}_c \neq \boldsymbol{b}_1 + \boldsymbol{b}_2 + ... + \boldsymbol{b}_c$$

(Addition here is standard vector addition.)

We use the following two properties of k-asummability.

Property 1: If f is a threshold function, then f is k-asummable for every $k \geq 2$ [3] (or see [12], pp.77-79).

Property 2: For every integer $k \geq 2$, there exist k-asummable Boolean functions that are not threshold functions [23].

The following is a well-known fact.

Fact: Let V and W be disjoint sets of points in $\mathcal{R}^n$. There exists a hyperplane separating the elements of V from the elements in W iff the convex hulls of V and W do not intersect (cf. [12], p. 40).

We now present two technical lemmas. The proof of the first lemma is known (cf. [12], pp. 42, 77-79); we present the proof here for completeness.

Lemma 4.1 *Let $S = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$ and $T = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{m'}\}$ be two finite subsets in $\mathcal{R}^n$ such that the convex hulls of S and T intersect. Furthermore, assume that each $\boldsymbol{a}_i \in \{0,1\}^n$ and each $\boldsymbol{b}_i \in \{0,1\}^n$. Then for some non-negative integer z, there exist z points $\boldsymbol{u}_1, .., \boldsymbol{u}_z$ in S (not necessarily distinct), and z points $\boldsymbol{v}_1, ..., \boldsymbol{v}_z$ in T (not necessarily distinct) such that $\boldsymbol{u}_1 + ... + \boldsymbol{u}_z = \boldsymbol{v}_1 + ... + \boldsymbol{v}_z$.*

Proof. Since the convex hulls of S and T intersect, there exist non-negative real numbers $c_1, ..., c_m$ and $d_1, .., d_{m'}$ such that

$$c_1 + ... + c_m = 1$$

$$d_1 + ... + d_{m'} = 1$$

$$c_1\boldsymbol{b}_1 + ... + c_m\boldsymbol{b}_m = d_1\boldsymbol{b}_1 + ... + d_{m'}\boldsymbol{b}_{m'}.$$

Hence there exist non-negative real numbers, $c_1, ..., c_m$ and $d_1, .., d_{m-p}$, not all zero such that

$$a_1 + ... + a_m = d_1 + ... + d_{m'} \ (*)$$

$$a_1\boldsymbol{b}_1 + ... + a_m\boldsymbol{b}_m = d_1\boldsymbol{b}_{m+1} + ... + d_{m-p}\boldsymbol{b}_{m'}. \ (**)$$

Since the points in S and T have rational coordinates, there exist $a_1, .., a_m$ and $d_1, .., d_{m'}$ satisfying (*) and (**) that are also rational. Multiplying (*) and (**) by a common denominator of the fractions if necessary, we may assume that $a_1, ..., a_m$ and $d_1, ..., d_{m-p}$ are integers in those equations. Consider each c_i as indicating how many times $\boldsymbol{a}_i$ should be repeated, and d_i as indicating how many times $\boldsymbol{c}_i$ should be repeated. It follows that for some non-negative integer z, there exist z points $\boldsymbol{u}_1, .., \boldsymbol{u}_z$ in S (not necessarily distinct), and z points $\boldsymbol{v}_1, ..., \boldsymbol{v}_z$ in T (not necessarily distinct) such that $\boldsymbol{u}_1 + ... + \boldsymbol{u}_z = \boldsymbol{v}_1 + ... + \boldsymbol{v}_z$. □

Lemma 4.2 *Let c be a positive integer. Then there exists a positive integer $\tau(c)$ with the following property: If g is a Boolean function that is not a threshold function, and Q is a certificate of size at most c of non-membership of g in the set of threshold functions, then there exist elements $\boldsymbol{u}_1, ..., \boldsymbol{u}_z$ in $Q \bigcap g^+$ (not necessarily distinct), and $\boldsymbol{v}_1, ..., \boldsymbol{v}_z$ in $Q \bigcap g^-$ (not necessarily distinct) such that*

1. $z \leq \tau(c)$
2. $\boldsymbol{u}_1 + ... + \boldsymbol{u}_z = \boldsymbol{v}_1 + ... + \boldsymbol{v}_z$

Proof. Suppose that g is an n-adic Boolean function that is not a threshold function, and that Q is a certificate of non-membership of g in Q of size c. Let $S = Q \bigcap g^+$ and let $T = Q \bigcap g^-$.

We first prove that the convex hull of S intersects the convex hull of T. Suppose not. Then there exists a hyperplane in R^n separating S from T and thus there must exist a hyperplane P in R^n separating S from T that does not intersect any vertices in B_2^n. Consider an n-adic Boolean function f whose value is 1 on all points in B_2^n that are on the same side of P as S, and 0 on all other points in B_2^n. This function is clearly a threshold function. This contradicts that Q is a certificate of non-membership of g in the set of threshold functions, proving that the convex hulls of S and T must intersect.

We say that Q is a *reduced certificate* if for all $1 \leq i < j \leq n$, there exists $\boldsymbol{b}$ in Q such that $b[i] \neq b[j]$. That is, if we form a matrix M whose rows consist of all $\boldsymbol{b}$ such that $\boldsymbol{b} \in Q$, then all columns of M are distinct. Assume for now that the certificate Q is a *reduced certificate*. (We will remove this assumption later.)

Note that since M has at most c rows (because Q has size at most c) and there are only 2^c different binary vectors of length c, it follows that n is at most 2^c. Thus the number of possible reduced certificates of size c (corresponding to any g) is finite. Without loss of generality, let $Q = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_p\}$, and let $1 \leq m \leq p$ be such that $g(\boldsymbol{b}_i) = 1$ for $1 \leq i \leq m$ and $g(\boldsymbol{b}_i) = 0$ for $m+1 \leq i \leq p$. Let $S = \{\boldsymbol{b}_1, .., \boldsymbol{b}_m\}$ and $T = \{\boldsymbol{b}_{m+1}, ..., \boldsymbol{b}_p\}$. The convex hulls of S and T intersect. Thus by Lemma 4.1, for some non-negative z, there exist z points $\boldsymbol{u}_1, .., \boldsymbol{u}_z$ in S (not necessarily distinct), and z points $\boldsymbol{v}_1, ..., \boldsymbol{v}_z$ in T (not necessarily distinct) such that

$$\boldsymbol{u}_1 + ... + \boldsymbol{u}_z = \boldsymbol{v}_1 + ... + \boldsymbol{v}_z$$

.

Let z^* be the smallest such z.

Let Z be the maximum of z^* over all reduced certificates Q of size c, such that for some non-threshold function g, Q is a certificate of non-membership of g in the set of threshold functions. Since there are a finite number of possible reduced certificates Q, and a finite number of values a function g could take on the elements of Q, Z is well-defined and finite. Let $\tau(c) = Z$. We have thus proved the lemma in the case where Q is a reduced certificate.

Now consider an n-adic non-threshold function g, and a certificate Q that g is not a threshold function, where Q is not a reduced certificate. Form the matrix M whose rows consist of all $\boldsymbol{b} \in Q$. Let $I = \{i_1, \ldots, i_{n'}\}$ be the indices of the leftmost occurences of each distinct column in M, such that $i_1 < i_2 < \ldots < i_{n'}$. Form a new set Q' by replacing each $\boldsymbol{b} \in Q$ with $\boldsymbol{b}'$, such that $\boldsymbol{b}'$ is obtained from $\boldsymbol{b}$ by deleting from $\boldsymbol{b}$ every component j for which $j \notin I$. Let $S' = \{\boldsymbol{b}' \in Q' | g(\boldsymbol{b}) = 1\}$ and $T' = \{\boldsymbol{b}' \in Q' | g(\boldsymbol{b}') = 0\}$. Since the convex hulls of S and T intersect, it is easy to verify that the convex hulls of S' and T' also intersect. Now consider an n'-adic Boolean function g' such that $g'(\boldsymbol{b}') = 1$ for all $\boldsymbol{b}' \in S'$, and $g'(\boldsymbol{b}') = 0$ for all $\boldsymbol{b}' \in T'$. Since the convex hulls of S' and T' intersect, g' is not a threshold function, and Q' is a certificate of non-membership of g' in the set of threshold functions.

Since Q' is a reduced certificate, by the above there exists a positive integer $z \leq Z$ such that there exist z points $\boldsymbol{u}'_1, .., \boldsymbol{u}'_z \in S'$ (not necessarily distinct) and z points $\boldsymbol{v}'_1, ..., \boldsymbol{v}'_z$ in T' (not necessarily distinct) such that

$$\boldsymbol{u}'_1 + ... + \boldsymbol{u}'_z = \boldsymbol{v}'_1 + ... + \boldsymbol{v}'_z.$$

The above equation is also satisfied by the $\boldsymbol{u}_1, .., \boldsymbol{u}_z$ and $\boldsymbol{v}_1, .., \boldsymbol{v}_z$ in S and T respectively that correspond to the $\boldsymbol{u}_i$'s and $\boldsymbol{v}_i$'s. Since $\tau(c) = Z$, this completes the proof. $\Box$

We can now prove our result for threshold functions.

Theorem 4.1 *The set of threshold functions cannot be characterized by any finite set of standard or generalized constraints.*

Proof. By Theorem 3.1 and Corollary 3.1, it suffices to show that the set of threshold functions does not have constant-size certificates of non-membership.

Suppose for contradiction that the set of threshold functions has certificates of non-membership of size c. Let $\tau(c)$ be as defined in Lemma 4.2. By Property 2, there exists a function g that is $\tau(c)$-asummable, but that is not a threshold function. Since the set of threshold functions has certificates of non-membership of size c, g must have a certificate Q of size at most c of non-membership in the set of threshold functions.

Let $S = Q \bigcap g^+$ and let $T = Q \bigcap g^-$. By Lemma 4.2 for some $z \leq \tau(c)$, there exist elements $\boldsymbol{b}_1, ..., \boldsymbol{b}_z$ in S (not necessarily distinct), and $\boldsymbol{c}_1, ..., \boldsymbol{c}_z$ in T (not necessarily distinct) such that $\boldsymbol{b}_1 + ... + \boldsymbol{b}_z = \boldsymbol{c}_1 + ... + \boldsymbol{c}_z$. Thus g is not $\tau(c)$-asummable. Contradiction. □

We note that although the set of threshold functions does not have constant-size certificates of non-membership, it does have certificates of size $n + 2$. This follows from Kirschberger's theorem on separation in $\mathcal{R}^n$ which implies that a Boolean function $f : B_2^n \rightarrow B_2$ is a threshold function iff for each subset K of $n+2$ points of B_2^n, there exists a hyperplane separating the elements from $K \bigcap f^+$ from the elements of $K \bigcap f^-$ [13], [20].

A weaker, but still polynomial, bound on the size of certificates of non-membership for threshold functions follows from results in computational learning theory. Maass and Turan showed that threshold functions can be learned using $O(n^3)$ proper equivalence queries [15]. It follows by results of Hellerstein, Pillaipakkamnatt, Raghavan, and Wilkins, and independently Hegedüs that if a set of functions that can be learned using $O(p(n))$ proper equivalence queries, for some function p, then it has certificates of non-membership of size $O(p(n))$ [10, 9]. Thus threshold functions have certificates of non-membership of size $O(n^3)$.

4.1 Renamable functions

A Boolean function $f(x_1, \ldots, x_n)$ is *positive* in a variable x_i if

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

for all $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in B_2$. It is *negative* in x_i if it satisfies the reverse inequality. A Boolean function $f(x_1, \ldots, x_n)$ is positive (monotonically increasing) if it is positive in each of its variables x_i. It is unate if for each variable x_i, f is either positive or negative in x_i.

The unate functions are the *renamable analogue* of the positive Boolean functions. If $\mathcal{K}$ is a set of Boolean functions, then the renamable analogue $r(\mathcal{K})$ of $\mathcal{K}$ is the set of functions $f : B_2^n \rightarrow B_2$ such that for some $\boldsymbol{s} \in B_2^n$, the function f_s defined by $f_s(\boldsymbol{x}) = f(\boldsymbol{x} + \boldsymbol{s})$ is in $\mathcal{K}$ (where addition here is componentwise modulo 2). In other words, the renamable analogue of a set of Boolean functions is the closure of that set under the operation of complementation of variables.

Ekin et al. considered the problem of characterizing $r(\mathcal{K})$ when $\mathcal{K}$ can be characterized by a finite set of identities (and hence by a finite set of standard constraints) [2]. They showed that in this case $r(\mathcal{K})$ can be characterized by a finite set of "simple existential sentences". However, as shown by Ekin et al., $r(\mathcal{K})$ may not be characterizable by Boolean equations. They give examples of four sets $\mathcal{K}$ having a finite characterization by identities: postive functions, polar functions, Horn DNF functions, and bilinear functions (definitions below). They showed for each of these sets $\mathcal{K}$, the renamable analogue $r(\mathcal{K})$ is not closed under identification of variables, and hence is not characterizable by Boolean equations. Thus the renamable analogues cannot be characterized by standard constraints either. However, since each set $r(\mathcal{K})$ is closed under special minors, it can be characterized by a (possibly infinite) set of generalized constraints.

Each of the four sets $\mathcal{K}$ listed above have constant-size certificates of non-membership, and hence by Corollary 3.1 have a finite characterization by standard constraints. However, not all the renamable analogues of these sets have constant-size certificates of non-membership. We consider the four renamable analogues $r(\mathcal{K})$ in turn.

1. Unate functions

It is known that the set of unate functions, the renamable analogue of the positive functions, has certificates of non-membership of size 4 (cf. [6]). The proof is as follows: For any Boolean function $g(x_1, \ldots, x_n)$ that is non-unate, there exists a variable x_i, elements $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in B_2$ and $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n \in B_2$ such that

$$g(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) < g(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$$

and

$$g(b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_n) > g(b_1, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_n)$$

. The four elements of the domain of g appearing in these inequalities constitute a certificate that g is not unate.

An easy consequence of the above is that the following Boolean generalized constraint characterizes the set of unate functions: (ϕ, S) where $S = \{0,1\}^4 - \{(0,1,1,0)\}$ and $\phi : B_2^4 \rightarrow \mathcal{N} \bigcup \{\infty\}$ such that $\phi(0,1,0,1) = 1$, $\phi(a,a,b,b) = \infty$ for all $\{a,b\} \in B_2$, and $\phi(x_1,x_2,x_3,x_4) = 0$ otherwise.

2. Renamable polar functions

This set is the renamable analogue of the polar functions. A polar function is a Boolean function which can be expressed by a DNF formula in which each term contains only negated variables, or only non-negated variables. Feigelson and Hellerstein showed that the set of renamable polar functions does not have constant-size certificates of non-membership [7]. In fact, they showed something stronger— that there does not exist any polynomial $p(n)$ such that the set of renamable polar functions has certificates of non-membership of size $p(n)^2$. Their proof is constructive; they defined a set of functions based on BCH codes, proved that these functions are not renamable polar, and showed that for any polynomial $p(n)$, they do not have certificates of non-membership in the set of renamable polar functions of size $p(n)$.

3. Renamable Horn DNF functions

This set is the renamable analogue of the Horn DNF functions. A Boolean function is a Horn DNF function if it can be expressed as a DNF formula in which each term contains at most one negated variable. In Feigelson's thesis, he showed that there does not exist any polynomial $p(n)$ such that the set of renamable Horn DNF functions has certificates of non-membership of size $p(n)$ [5]. (The proof is similar to the proof for renamable polar functions.) Thus the set does not have constant-size certificates of non-membership.[3]

4. Renamable bilinear functions

This set is the renamable analogue of the bilinear functions. A Boolean function is bilinear if it can be written as a DNF formula in which each term contains at most one negated variable and at most one non-negated variable (and hence each term has at most two variables). We show here that the set of renamable bilinear functions does not have constant-size certificates of non-membership. Consider a function $f(x_1, \ldots, x_n) = x_1x_2 \vee x_2x_3 \vee \ldots x_{n-1}x_n \vee x_nx_1$ such that n is odd and greater than 1. We first show that f is not renamable bilinear. Suppose it is. Then there exists a bilinear function g such that for some $\boldsymbol{s} \in B_2^n$, $f(\boldsymbol{x}) = g(\boldsymbol{x} + \boldsymbol{s})$ (addition componentwise mod 2). Therefore, $g(x_1, \ldots, x_n) = \sigma(x_1)\sigma(x_2) \vee \sigma(x_2)\sigma(x_3) \vee \ldots \sigma(x_{n-1})\sigma(x_n) \vee \sigma(x_n)\sigma(x_1)$, where $\sigma(x_i) = x_i$ if $\boldsymbol{s}[i] = 0$, and $\sigma(x_i) = \neg x_i$ if $\boldsymbol{s}[i] = 0$. Since f is a positive function, g is a unate function. The DNF formula given for f is a monotone DNF formula, and it is easy to show that any reduced DNF formula for f must contain all terms in the given formula. (By reduced we mean that no term can be deleted, and no literal can be deleted from a term, without changing the value of the function represented by the formula.) Similarly, any reduced DNF formula for g must contain all terms appearing in the given DNF formula for g. Thus since g is bilinear, each term in the given DNF for g must contain one negated variable and one non-negated variable, implying $\boldsymbol{s}[i] \neq \boldsymbol{s}[i+1]$ for $1 \leq i \leq n$ (consider n+1 to be equal to 1). But this is impossible because n is odd. Therefore f is not renamable bilinear.

We now show that any certificate that f is not renamable bilinear must have size at least n. Consider any set $S = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$ of points in the domain of f, such that $m < n$. Let $S^+ = \{\boldsymbol{a}_{i_1}, \ldots, \boldsymbol{a}_{i_p}\}$ be the subset of S consisting of all $\boldsymbol{a}_i \in S$ such that $f(\boldsymbol{a}_i) = 1$. For each $\boldsymbol{a}_{i_j} \in S^+$, let $t(\boldsymbol{a}_{i_j})$ be one term x_rx_{r+1} that is satisfied by $\boldsymbol{a}_{i_j}$ (there may be others). Consider the function $f'(x_1, \ldots, x_n) = t(\boldsymbol{a}_{i_1}) \vee \ldots \vee t(\boldsymbol{a}_{i_p})$. Since $p \leq m < n$, the given DNF

[2]The result given by Feigelson and Hellerstein is actually for the dual of renamable polar functions, which is defined with respect to a CNF representation rather than a DNF representation, but the result immediately extends to the DNF representation

[3]Again, Feigelson's result is actually given in terms of renamable Horn CNF, rather than DNF.

for f' contains some but not all the terms in the DNF for f. It follows that there exists $\boldsymbol{s} \in B_2^n$ such that $s[i] \neq s[i+1]$ for all $1 \leq i \leq n$ such that $x_i x_{i+1}$ is a term in the given DNF for f'. Therefore f' is renamable bilinear. Furthermore, $f'(\boldsymbol{a}_i) = f(\boldsymbol{a}_i)$ for all $\boldsymbol{a}_i \in S$. Thus S is not a certificate that f is not renamable bilinear. It follows that any certificate that f is not renamable bilinear must have size at least n. Since n is any odd number greater than 1, the renamable bilinear functions do not have constant-size certificates of non-membership.

5 Closure conditions for generalized constraints

Here we extend the Galois theory of Pippenger from standard constraints to generalized constraints. For generalized constraints, the closure condition on sets of finite functions is closure under special minors, rather than closure under identification minors.

Our results and proofs closely follow Pippenger's (parts of which are closely related to Geiger's work on clones [8]). Our aim in this section is to show that, in fact, Pippenger's work can be extended to apply to generalized constraints. This requires modifying definitions appropriately and adapting proofs. We include many modified proofs for completeness, although in some cases in which the modifications to the proofs are minor, we omit the modified proofs.

Theorem 5.1 *A set of functions can be characterized by a set of generalized constraints iff it is closed under special minors.*

Proof. It is easy to show that if (ϕ, S) is a generalized constraint, then the set of functions satisfying (ϕ, S) is closed under permutation of variables and addition of dummy variables (i.e. closed under special minors). If $\mathcal{T}$ is any set of generalized constraints, the set of functions satisfying all the constraints in $\mathcal{T}$ is an intersection of sets closed under special minors and is therefore itself closed under special minors. Thus any set of functions characterized by generalized constraints is closed under special minors.

We now prove the converse. Let $\mathcal{F}$ be a set of functions closed under special minors. Let g be any function not in $\mathcal{F}$. We claim that there is a generalized constraint (ϕ, S) that is satisfied by every function in $\mathcal{F}$ but not by g. The set of all such (ϕ, S), for each g not in $\mathcal{F}$, characterizes $\mathcal{F}$.

To prove the claim, suppose g is n-adic. Let $\mathcal{F}_n$ be the set of n-adic functions in $\mathcal{F}$. Let M be a $k^n \times n$ matrix whose rows are all k^n elements of B_k^n, and let ϕ be an n-adic k-ean bounding function such that $\phi(x) = 1$ if x appears as a column of M, and $\phi(x) = 0$ otherwise. Let $S = \{f(M) | f \in \mathcal{F}_n\}$.

We first show that every function in $\mathcal{F}$ satisfies (ϕ, S). Let $f' \in \mathcal{F}$. Suppose f' is n'-adic. Let $M' \prec \phi$ be a $k^n \times n'$ matrix. The columns of M' are a subset of the columns of M. Define the map $h : \{1, \ldots, n'\} \to \{1, \ldots, n\}$ such that column i of M' equals column $h(i)$ of M. The n-adic function f defined by $f(x_1, \ldots, x_n) = f'(x_{h(1)}, \ldots, x_{h(n')})$ can be obtained from f' by permuation of variables and addition of dummy variables, and therefore belongs to $\mathcal{F}_n$. We have $f'(M') = f(M)$. Since $f(M) \in S$, f' satisfies the constraint (ϕ, S).

We now show that g does not satisfy (ϕ, S). Since $M \prec \phi$, if g satisfies (ϕ, S) then $g(M) \in S$ and hence there exists $f \in \mathcal{F}$ such that $f(M) = g(M)$. But $f(M) = g(M)$ implies that $f = g$ since M contains all elements in the domains of both functions. This contradicts that $g \notin F$. $\square$

We now give necessary and sufficient closure conditions for a set of generalized constraints to be characterizable by a set of functions. To do this, we introduce the following operations on generalized constraints. All of the operations listed, except the last, are generalizations of operations given for standard constraints. In the following, we consider an argument of a constraint (ϕ, S) to be an argument of the function ϕ together with the corresponding entries of the elements of S.

1. *Permuation of arguments.* Let (ϕ, S) and (ϕ', S) be an m-ary generalized constraint. Let π be a permuation of $\{1, \ldots, m\}$. If for all $(a_1, \ldots, a_m) \in B_k^m$, $\phi(a_1, \ldots, a_m) = \phi'(a_{\pi(1)}, \ldots, a_{\phi(m)})$ and for all $(b_1, \ldots, b_m) \in B_l^m$, $(b_1, \ldots, b_m) \in S$ iff $(b_{\pi(1)}, \ldots, b_{\pi(m)})$ then we say that ϕ' is obtained from (ϕ, S) by permutation of arguments.

2. *Projection.* Let (ϕ, S) and (ϕ', S') be generalized constraints such that the first is m-ary and the second $(m-1)$-ary. If ϕ' is such that for all $(a_1, \ldots, a_{m-1}) \in B_k^{m-1}$, $\phi'(a_1, \ldots, a_{m-1}) = \sum_{d \in B_k} \phi(a_1, \ldots, a_{m-1}, d)$, and $S = \{(b_1, \ldots, b_{m-1}) \in B_l^{m-1} |\ \exists b_m \in B_l$ such that $(b_1, \ldots, b_{m-1}, b_m) \in S\}$, then we say that (ϕ', S') is obtained from (ϕ, S) by projection.

3. *Diagonalization.* Let (ϕ, S) and (ϕ', S') be generalized constraints such that the first is m-ary and the second is $(m-1)$-ary. If ϕ' is such that for all $(a_1, \ldots, a_{m-1}) \in B_k^{m-1}$, $\phi'(a_1, \ldots, a_{m-1}) = \phi(a_1, \ldots, a_{m-1}, a_{m-1})$ and $S' = \{(b_1, \ldots, b_{m-1}) | (b_1, \ldots, b_{m-1}, b_{m-1}) \in S\}$, then we say (ϕ', S') is obtained from (ϕ, S) by diagonalization (or *identifying* arguments).

4. *Addition of an extra argument.* Let (ϕ, S) and (ϕ', S') be generalized constraints such that the first is $(m-1)$-ary and the second is m-ary.
   If $S' = \{(b_1, \ldots, b_m) \in B_l^m | (b_1, \ldots, b_{m-1}) \in S\}$ and for all $(a_1, \ldots, a_{m-1}) \in B_k^{m-1}$, $\phi(a_1, \ldots, a_{m-1}) = \sum_{d \in B_k} \phi'(a_1, \ldots, a_{m-1}, d)$ then we say that (ϕ', S) is obtained from (ϕ, S) by addition of an extra argument. Note that given (ϕ, S), there may be more than one possible (ϕ', S') that can be obtained from S by addition of an extra argument (although S' will be the same in all cases).

5. *Restricting the antecedent.* If (ϕ, S) and (ϕ', S) are such that $\phi' \leq \phi$, then we say that (ϕ', S) is obtained from (ϕ, S) by restricting the antecedent.

6. *Extending the consequent.* If (ϕ, S) and (ϕ, S') are such that $S \subseteq S'$, then we say that (ϕ, S') is obtained from (ϕ, S) by extending the consequent.

7. *Intersecting consequents.* The generalized constraint produced by intersecting the consequents of (ϕ, S) and (ϕ, S') is $(\phi, S \bigcap S')$.

8. *Taking the limit of antecedents* Defined in Section 2.

We define a *generalized equality constraint* to be a generalized constraint (ϕ, S) such that $\phi(a) = \infty$ if all arguments of a are equal and $\phi(a) = 0$ otherwise, and such that the elements of S are exactly those in which all arguments are equal.

We say that a set of generalized constraints is *minor-closed* if it contains the binary generalized equality constraint and is closed under all eight of the above operations.

We will show that a set of generalized constraints can be characterized by a set of functions iff the set of generalized constraints is minor-closed. The difficult direction is to show that every minor-closed set of generalized constraints can be characterized by a set of functions. To prove the analogous lemma for constraints, Pippenger followed a two-part strategy used by Geiger in his work on clones. We modify Pippenger's proof to apply to generalized constraints.

We need the following definitions. An n-adic (k,l)-ean partial function g consists of a subset $D \subseteq B_k^n$ called the domain of g and a map $g : D \to B_l$. If the domain D of a partial function is a subset of the domain of the partial function f and if $g(x) = f(x)$ for every $x \in D$, then g is a *restriction* of f and f is an *extension* of g. If g is an n-adic (k,l)-ean partial function and (ϕ, S) is an m-ary (k,l)-ean constraint, we say that g *satisfies* (ϕ, S) if for every $m \times n$ matrix M such that $M \prec R$, and such that every row of M belongs to the domain of g, we have that $g(M) \in S$.

We define a *generalized trivial constraint* to be an m-ary generalized constraint (ϕ, S) where $\phi(\boldsymbol{a}) = \infty$ for all $\boldsymbol{a} \in B_k^m$, and $S = B_l^m$

The proof of the following lemma is an easy modification of the proof of the analogous statement for standard constraints, so we omit it.

Lemma 5.1 *A minor-closed set of generalized constraints contains all trivial constraints and all equality constraints.*

We now extend a central lemma in Pippenger's proof to apply to generalized constraints.

Lemma 5.2 *Let $\mathcal{T}$ be a minor-closed set of generalized constraints and let (ϕ, S) be a generalized constraint not belonging to $\mathcal{T}$. Then there exists a partial function g that satisfies every constraint in $\mathcal{T}$ but that does not satisfy (ϕ, S).*

Proof. Suppose (ϕ, S) is m-ary. Then S cannot contain all elements of B_l^m, because then (ϕ, S) could be obtained from a trivial constraint by restricting the antecedent, and hence would be in $\mathcal{T}$. The minor-closed set $\mathcal{T}$ cannot contain $(\phi, B_l^m \backslash \{s\})$ for every $s \in B_l^m \backslash S$, because if it did, the generalized constraint obtained by intersection of their consequents, (ϕ, S), would also be in $\mathcal{T}$. Choose some $s \in B_l^m \backslash S$ such that $(\phi, B_l^m \backslash \{s\}) \notin \mathcal{T}$.

Let $X = \{(a_1, \ldots, a_m) \in B_l^m | \phi(a_1, \ldots, a_m) \neq \infty\}$. Consider the set Q consisting of all m-adic k-ean repetition functions ϕ' such that $(\phi', B_l^m \backslash \{s\})$ is in $\mathcal{T}$ and such that for all $(a_1, \ldots, a_m) \in X$, $\phi(a_1, \ldots, a_m) = \phi'(a_1, \ldots, a_m)$. By Lemmas 2.1 and 2.2, since $\mathcal{T}$ is closed under limits of antecedents, the set Q_{max} of maximal elements in Q is finite, and for all $\phi' \in Q$, there exists $\phi'' \in Q_{max}$ such that $\phi' \leq \phi''$. Define a repetition function β such that for all $\mathbf{a} \in B_m^k$,

- $\beta(\mathbf{a}) = \phi(\mathbf{a})$ if $\mathbf{a} \in X$
- $\beta(\mathbf{a}) = 0$ if $\boldsymbol{a} \notin X$ and $\phi''(\mathbf{a}) = \infty$ for all $\phi'' \in Q_{max}$
- $\beta(\mathbf{a}) = \max_{\phi'' \in Q_{max} s.t. \phi''(\mathbf{a}) \neq \infty}\{\phi''(\mathbf{a}) + 1\}$ otherwise.

Note that in the third case the value of β will be finite because Q_{max} is a finite set. We claim that for all $\phi'' \in Q_{max}$, β is not less than or equal to ϕ''. To prove the claim, consider $\phi'' \in Q_{max}$. For some $\mathbf{a} \in B_k^m \backslash X$, $\phi''(\mathbf{a}) \neq \infty$ (otherwise $\phi'' = \phi$, implying that $(\phi, B_l^m \backslash \{s\}) \in \mathcal{T}$, a contradiction). Therefore $\beta(\mathbf{a}) > \phi''(\mathbf{a})$, implying that β is not less than or equal to ϕ''. It follows that $\beta \notin Q$ and hence $(\beta, B_l^m \backslash \{s\})$ is not in $\mathcal{T}$.

Let $n = \Sigma_{\mathbf{a} \in B_k^m} \beta(\mathbf{a})$. Define an $m \times n$ matrix M whose columns consist of $\beta(\mathbf{a})$ copies of $\mathbf{a}$ for each $\mathbf{a} \in B_k^m$. Define a partial function g by taking the domain of g to be the set of rows of M, with the values of g given by $g(M) = s$.

First, we claim that g satisfies every generalized constraint in $\mathcal{T}$. Suppose, to obtain a contradiction, that (ϕ', S') is an m'-ary generalized constraint in $\mathcal{T}$ that is not satisfied by g. Let M' be an $m' \times n$ matrix such that $M' \prec \phi'$ and $g(M') = s'$ where $s' \notin S'$. Let θ be an m'-adic k-ary repetition function such that $\theta(\mathbf{a})$ equals the number of times that $\mathbf{a}$ appears as a column of M'. Clearly $\theta \leq \phi'$ and (θ, S') is also not satisfied by g. Since $\mathcal{T}$ is closed under restricting the antecedent, (θ, S') is also in $\mathcal{T}$.

Every row of M' must belong to the domain of g and must therefore be a row of M. Define the map $h : \{1, \ldots, m'\} \to \{1, \ldots, m\}$ such that row i of M' equals row $h(i)$ of M. We also use h to denote the maps $h : B_k^m \to B_k^{m'}$ and $h : B_l^m \to B_l^{m'}$ defined by

$$h\left(\begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ a_m \end{pmatrix}\right) = \begin{pmatrix} a_{h(1)} \\ \cdot \\ \cdot \\ a_{h(m')} \end{pmatrix}.$$

For $\mathbf{a}' \in B_k^{m'}$, we define $h^{-1}(\mathbf{a}') = \{\mathbf{a} \in B_k^m | h(\mathbf{a}) = \mathbf{a}'\}$. For $\mathbf{c}' \in B_l^{m'}$, we define $h^{-1}(\mathbf{c}')$ analogously. Note that for all $\mathbf{a}' \in B_k^{m'}$, $\theta(\mathbf{a}') = \sum_{\mathbf{a} \in h^{-1}(\mathbf{a}')} \beta(\mathbf{a})$.

Consider the generalized constraint $(\beta, h^{-1}(S'))$ where $h^{-1}(S') = \{h^{-1}(s') | s' \in S'\}$. The generalized constraint $(\beta, h^{-1}(S'))$ can be obtained from (θ, S') by identification of arguments (corresponding to rows i, j of M such that $h(i) = h(j)$), addition of extra arguments, and permutation of arguments. Hence $(\beta, h^{-1}(S')) \in \mathcal{T}$.

Since $h(s) = s'$ does not belong to S', s does not belong to $h^{-1}(S')$. Therefore $h^{-1}(S') \subseteq B_m^l \backslash \{s\}$ and $(\beta, B_l^m \backslash \{s\})$ can be obtained from $(\beta, h^{-1}(S'))$ by extending the consequent. Hence $(\beta, B_l^m \backslash \{s\}) \in \mathcal{T}$, which is a contradiction. This completes the proof that g satisfies every constraint in $\mathcal{T}$.

We now claim that g does not satisfy (ϕ, S). If it did, then since $M \prec \phi$, we would have that $s \in g(M)$ belonged to S, contradicting the choice of s. $\square$

The next lemma states that the partial function g whose existence is proved in the previous lemma, can be extended to a total function that also satisfies all generalized constraints in **a**. The proof is somewhat long and is an easy modification of Pippenger's proof of the analogous result for constraints, and we omit it.

Lemma 5.3 *Let $\mathcal{T}$ be a minor-closed set of generalized constraints. If g is a partial function statisfying all the generlized constraints in $\mathcal{T}$, then there is an extension of g to a total function that also satisfies all the generalized constraints in $\mathcal{T}$.*

The following theorem is dual to Theorem 5.1.

Theorem 5.2 *A set of generalized constraints can be characterized by a set of finite functions iff it is closed under minors.*

Proof. If a set of generalized constraints can be characterized by a set of finite functions, then it is clear that the set is closed under minors.

For the converse, let $\mathcal{T}$ be a minor-closed set of generalized constraints and let (ϕ, S) be a generalized constraint not in $\mathcal{T}$. By Lemma 5.2 there exists a partial function g that satisfies every constraint in $\mathcal{T}$ but does not satisfy (ϕ, S). By Lemma 5.3 there is an extension of g to a total function f that also satisfies every constraint in $\mathcal{T}$. Since g does not satisfy (ϕ, S), neither does f.

The set of such f, for every (ϕ, S) not in $\mathcal{T}$, characterizes $\mathcal{T}$. □

6 Extensions and open questions

If a set of functions is closed under special minors, and under substitution of constants for variables, then it has a characterization by a set of generalized constraints (ϕ, S) satisfying $\phi(\mathbf{1}) = \phi(\mathbf{0}) = \infty$ (where $\mathbf{1}$ and $\mathbf{0}$ represent the all 0 and all 1's vectors). Conversely, if a set of functions has a characterization by a set of generalized constraints satisfying this property, then it is closed under special minors and under substitution of constants for variables (these two observations follow directly from results of Pippenger [19]).

The set of unate functions is closed under special minors and under substitution of constants for variables. Feigelson and Hellerstein gave a characterization of the unate functions in terms of forbidden "projection" minors (where here projection means substitution of constants for variables) [6].

The unate functions have constant-size certificates of non-membership. We would like to have a good characterization of the sets which have constant-size certificates of non-membership, from among those sets that are closed under special minors minors and substitution of variables for constants. Of course the characterization in this paper applies, because it deals with sets closed under special minors, but there may be better characterizations for the sets closed both under special minors and under substitution of variables for constants.

We showed that there is no simple relationship between the size of certificates of non-membership for a set of functions $\mathcal{K}$ and the size of certificates of non-membership of the renamable analogue $r(\mathcal{K})$. An interesting question is to determine under which conditions on

$\mathcal{K}$ the existence of constant-size certificates of non-membership for $\mathcal{K}$ implies constant-size (or non constant-size) certificates of non-membership for $r(\mathcal{K})$.

The set of degree ≥ 3 functions was studied by Ekin et al. [2], who showed that this set is not closed under identification minors, and hence cannot be characterized by standard constraints. However, it can be characterized by generalized constraints. It is open whether it has finite certificates of non-membership. In general, there is a need for techniques that can be used for proving bounds on the size of certificates of non-membership.

7 Acknowledgments

Part of this work was done while the author was visiting the University of Calgary and the Universitat Politècnica de Catalunya. The author would like to thank Aaron Feigelson, Vijay Raghavan, David Guijarro, Simon Hellerstein, Stephan Foldes, and Peter Hammer for helpful discussions, and Peter Hammer for posing the question of the existence of a finite equational characterization of threshold functions. The author would also like to thank Nick Pippenger for sending his paper on standard constraints, and for very helpful comments and corrections to a draft of this paper.

References

[1] V. G. Bodnarchuk, L. A. Kaluzhinin, V. N. Kotov and B. A. Romov, "Galois theory for Post algebras. I, II", *Cybernetics*, **5** (1969) 243–252, 531–539.

[2] O. Ekin, S. Foldes, P. L. Hammer, and L. Hellerstein, "Equational theories of Boolean functions," DIMACS Technical Report 97-79, December 1997.

[3] C. C. Elgot, "Truth functions realizable by single threshold organs," AIEE Conference Paper 60-1311, Oct. 1960, Revised Nov. 1960.

[4] C. J. Everett, "Closure operations and galois theory in lattices", *Transactions of the AMS*, **55** (1944) 514–525.

[5] A. Feigelson, "On Boolean functions and their orientations: learning, monotone dimension, and certificates", PhD. Thesis, Department of Electrical and Computer Engineering, Northwestern University, 1998.

[6] A. Feigelson and L. Hellerstein, "The forbidden projections of unate functions", *Discrete Applied Mathematics*, **77** (1997) 221–236.

[7] A. Feigelson and L. Hellerstein, "Conjunctions of unate DNF formulas", *Information and Computation*, **140**(2) (1998) 203–228.

[8] D. Geiger, "Closed systems of functions and predicates", *Pacific J. Math.*, **27** (1968) 95–100.

[9] T. Hegedüs, "Generalized Teaching Dimensions and the Query Complexity of Learning", *Proceedings of the Eighth Annual Conference on Computational Learning Theory* (1995) 108–117.

[10] L. Hellerstein, K. Pillaipakkamnatt, V. Raghavan, D. Wilkins, "How many queries are needed to learn?", *Journal of the Association for Computing Machinery*, **43**(5) (1996) 840–862.

[11] G. Higman, "Ordering by divisibility in abstract algebras," *Proc. of the London Mathematical Society*, **2**(3) (1956) 326–36.

[12] S. T. Hu, Threshold Logic, Univ. of California Press, 1965.

[13] P. Kirschberger, "Über Tschebyecheffsche Annaherungsmethoden", *Math. Annalen*, **57** (1903) 509–540.

[14] S. Lang, *Algebra*, Addison Wesley, 1971.

[15] W. Maass and G. Turan, "On the complexity of learning from counterexamples (Extended Abstract)", in *Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, ACM Press, 1989, 262–267.

[16] C. St. J. A. Nash-Williams, "On well-quasi-ordering finite trees," *Proceedings of the Cambridge Philosophical Society*, **59** (1963) 833–35.

[17] Ø. Ore, "Galois Connexions", *Transactions of the AMS"*, **55** (1944) 493–513.

[18] N. Pippenger, *Theories of Computability*, Cambridge University Press, 1997.

[19] N. Pippenger, "Galois theory for minors of finite functions," UBC Computer Science Department Technical Report 98-08.

[20] H. Rademacher and I. J. Schoenberg, "Helly's theorems on convex domains and Tchebycheff's approximation problem". *Canadian J. Math.*, **2** (1950) 245–256.

[21] M. Ward, "The closure operators of a lattice", *Annals of Math.*, **43** (1942) 191–196.

[22] R. O. Winder, "Fundamentals of threshold logic", in: J. T. Tou (Ed.), *Applied Automata Theory*, Academic Press, New York, 1968, 235–318.

[23] R. O. Winder, "More about threshold logic", *Switching circuit theory and logical design*, (1961) 55–64.