HAL open science

Pivotal decomposition schemes inducing clones of operations

Miguel Couceiro, Bruno Teheux

To cite this version:

Miguel Couceiro, Bruno Teheux. Pivotal decomposition schemes inducing clones of operations. Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry, 2018, 59 (1), pp.25-40. 10.1007/s13366-017-0354-6 . hal-01450835

HAL Id: hal-01450835

https://inria.hal.science/hal-01450835v1

Submitted on 31 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

PIVOTAL DECOMPOSITION SCHEMES INDUCING CLONES OF OPERATIONS

MIGUEL COUCEIRO AND BRUNO TEHEUX

Abstract. We study pivotal decomposition schemes and investigate classes of pivotally decomposable operations. We provide sufficient conditions on pivotal operations that guarantee that the corresponding classes of pivotally decomposable operations are clones, and show that under certain assumptions these conditions are also necessary. In the latter case, the pivotal operation together with the constant operations generate the corresponding clone.

1. Introduction and Motivation

Several classes of operations have the remarkable feature that each member $f\colon A^n \to A$ is decomposable into simpler operations that are then combined by a single operation, in order to retrieve the values of the original operation f. A noteworthy example is the class of Boolean functions $f\colon \{0,1\}^n \to \{0,1\}$ that can be decomposed into expressions of the form

$$f(\mathbf{x}) = x_k f(\mathbf{x}_k^1) + (1 - x_k) f(\mathbf{x}_k^0), \tag{1}$$

for $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ and $k \in [n]$, and where $\mathbf{x}_k^c$ denotes the n-tuple obtained from $\mathbf{x}$ by substituting its k-th component by $c \in \{0,1\}$. Such decomposition scheme is referred to as *Shannon decomposition* (or *Shannon expansion*) [18], or *pivotal decomposition* [1]. Boolean functions are similarly decomposable into expressions in the language of Boolean lattices

$$f(\mathbf{x}) = (x_k \wedge f(\mathbf{x}_k^1)) \vee (\overline{x}_k \wedge f(\mathbf{x}_k^0)) \tag{2}$$

where $\overline{x}_k = 1 - x_k$.

More recent examples include the class of polynomial operations over a distributive lattice (essentially, combinations of variables and constants using the lattice operations $\wedge$ and $\vee$) that were shown in [13] to be decomposable into expressions of the form

$$f(\mathbf{x}) = \mathrm{med}(f(\mathbf{x}_k^0), x_k, f(\mathbf{x}_k^1)), \tag{3}$$

where med is the ternary lattice polynomial given by

$$\begin{aligned}\mathrm{med}(x_1, x_2, x_3) &= (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)\\ &= (x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge (x_2 \vee x_3).\end{aligned}$$

The latter decomposition scheme is referred to as *median decomposition* in [5] and [13]. We refer the reader to [15, 19, 4] for applications of the median decomposition formula to obtain median representations of Boolean functions.

Note that decomposition schemes (1), (2) and (3) share the same general form, namely,

$$f(\mathbf{x}) = \Pi(x_k, f(\mathbf{x}_k^1), f(\mathbf{x}_k^0)).$$

Indeed,

- in (1) we have $\Pi(x, y, z) = xy + (1 - x)z$,

Date: Thursday 12th January, 2017,22:41.

- in (2) we have $\Pi(x,y,z) = (x \wedge y) \vee (\overline{x} \wedge z)$, and
- in (3) we have $\Pi(x,y,z) = \mathrm{med}(x,y,z)$.

These facts were observed in [14] where such pivotal decomposition schemes were investigated. These preliminary efforts were then further pursued under the observation that certain classes of pivotal operations fulfill certain closure requirements, notably, closure under functional composition. This led to the study [6] of those classes of pivotally decomposable operations that constitute clones. In particular, we presented conditions on pivotal operations to ensure that the corresponding classes of pivotally decomposable operations constitute clones. However, several questions were stated without being answered. In this paper we settle many of these questions and provide new insights in this line of research.

The paper is organised as follows. In Section 2 we recall basic notions and terminology that will be used throughout the paper (Subsection 2.1). We also introduce the concepts of pivotal operation and that of pivotally decomposable class (Subsection 2.2) and discuss normal form representations that arise from such pivotal decompositions (Subsection 2.3). Moreover, we investigate certain symmetry properties that are common to pivotal operations (Subsection 2.4). In Section 3 we consider the problem of describing classes of pivotally decomposable operations that are clones. A general solution to this problem still eludes us, but we provide several sufficient conditions on pivotal operations that ensure the latter (Subsection 3.1). In fact, we show that under certain assumptions many of these conditions are also necessary (Subsection 3.2). The question of determining sets of generators for clones of pivotally decomposable operations is also addressed and partially answered. Taking this framework further into the realm of clone theory, many natural questions emerge. For instance, we construct an example of a pivotal operation Π for which the class of Π-decomposable operations is a clone that does not contain Π (Subsection 3.3); such an example is shown not to exist in the case of Boolean functions. Further questions that remain open are then discussed in Section 4.

2. Basic notions and notation

In this section we recall basic terminology used throughout the paper. In particular, we introduce the concepts of pivotal operation and of pivotally decomposable class, and we observe that, under certain conditions, pivotal decompositions lead to normal form representations that use a unique non trivial connective, namely, the pivotal operation. In the last subsection we investigate symmetric properties of pivotal operations and present some characterizations.

2.1. **Preliminaries: Clones of operations.** For any positive integer n, we denote by $[n]$ the set $\{1,\dots,n\}$. For a nonempty set A, a function $f\colon A^n \to A$ is called an *n-ary operation* on A. We denote by $\mathcal{O}_A^{(n)}$ the set of n-ary operations on A and by $\mathcal{O}_A = \bigcup_{n\geq 1} \mathcal{O}_A^{(n)}$ the set of *operations* on A. For any $f \in \mathcal{O}_A^{(n)}$, $S \subseteq [n]$ and $\mathbf{a} \in A^n$ we define the *S-section $f_S^{\mathbf{a}}$ of f* as the $|S|$-ary operation on A defined by $f_S^{\mathbf{a}}(\mathbf{x}) = f(\mathbf{a}_S^{\mathbf{x}})$, where $\mathbf{a}_S^{\mathbf{x}}$ is the n-tuple whose i-th coordinate is x_i, if $i \in S$, and a_i, otherwise. For $k \in [n]$, we say that the k-th argument of $f \in \mathcal{O}_A^{(n)}$ is *essential* if there is a tuple $\mathbf{b} \in A^n$ such that $f_k^{\mathbf{b}}$ is non-constant. Otherwise, we way that it is *inessential*.

A *clone* on A is a set $\mathcal{C} \subseteq \mathcal{O}_A$ of operations on A that

(1) contains all projections on A, i.e., operations $p_i^n\colon A^n \to A$ given by

$$p_i^n(x_1,\dots,x_n) = x_i, \text{ for } i \in [n], \text{ and}$$

(2) is closed under taking functional compositions, i.e., if $f \in C \cap \mathcal{O}_A^{(n)}$ and $g_1, \ldots, g_n \in C \cap \mathcal{O}_A^{(m)}$, then their *composition* $f(g_1, \ldots, g_n) \in \mathcal{O}_A^{(m)}$ that is defined by

$$f(g_1, \ldots, g_n)(\mathbf{x}) = f(g_1(\mathbf{x}), \ldots, g_n(\mathbf{x})) \quad (\mathbf{x} \in A^m)$$

also belongs to C.

In the case when A is finite, the set of all clones on A forms an algebraic lattice, where the lattice operations are the following: meet is the intersection, join is the smallest clone that contains the union. The greatest element is the clone $\mathcal{O}_A$ of all operations on A; the least element is the clone $\mathcal{J}_A$ of all projections on A. For sets A of cardinality at least 3, this lattice is uncountable, and its structure remains a topic of current research; see, e.g., [8, 10]. In the case when $|A| = 2$, the lattice of clones on A is countably infinite, and it was completely described by E. Post [17]. In particular, it follows that each Boolean clone can be generated by a finite set of Boolean functions. For instance,

- the clone $\mathcal{O}_{\{0,1\}}$ of all Boolean functions can be generated by $\{\neg, \wedge\}$ or, equivalently, by $\{0, \neg, \mathrm{med}\}$;
- the clone M of all monotone Boolean functions, i.e., verifying $\mathbf{x} \leq \mathbf{y} \implies f(\mathbf{x}) \leq f(\mathbf{y})$, can be generated by $\{0, 1, \wedge, \vee\}$ or, equivalently, by $\{0, 1, \mathrm{med}\}$;
- the clone SM of all self-dual monotone Boolean functions, i.e., monotone operations verifying $f(\neg\mathbf{x}) = \neg f(\mathbf{x})$, is generated by $\{\mathrm{med}\}$.

For further background see, e.g., [8, 10].

2.2. **Pivotal operations and pivotally decomposable classes.** In what follows, A denotes an arbitrary fixed nonempty set, and 0 and 1 are two fixed elements of A. In the setting of operations, the notion of pivotal operation Π and that of Π-decomposable operation can be defined as follows.

Definition 2.1 (Definition 2.1 in [14])**.** A *pivotal operation* on A is a ternary operation Π on A that satisfies the equation

$$\Pi(x, y, y) \;=\; y. \tag{4}$$

If Π is a pivotal operation, then $f \in \mathcal{O}_A^{(n)}$ is Π-*decomposable* if

$$f(\mathbf{x}) \;=\; \Pi(x_i, f(\mathbf{x}_i^1), f(\mathbf{x}_i^0)), \qquad \mathbf{x} \in A^n, i \in [n]. \tag{5}$$

Also, we denote by Λ_Π the class of Π-decomposable operations on A.

Note that condition (4) ensures that Π-decomposability of an operation does not depend on its inessential arguments. Indeed, if the ith argument of f is inessential, then $f(\mathbf{x}) = f(\mathbf{x}_i^1) = f(\mathbf{x}_i^0)$ for every $\mathbf{x} \in A^n$. It follows from (4) that $f(\mathbf{x}) = \Pi(x_i, f(\mathbf{x}_i^1), f(\mathbf{x}_i^0))$ for any $\mathbf{x} \in A^n$. In particular, we can state the following result.

Lemma 2.2. *If Π is a pivotal operation, then every constant operation on A is Π-decomposable.*

2.3. **Normal form representations induced by pivotal decompositions.** Note that if an operation f is Π-decomposable, then we arrive at a representation of f by an expression built from the pivotal operation Π and applied to variables and constants, by iterating its Π-decomposition expression (5). This fact motivates the following notion of Π-normal form.

Definition 2.3. Let $\Pi \in \mathcal{O}_A^{(3)}$. We define the classes of k-*ary* Π-*normal forms* N_Π^k inductively on $k \geq 0$ by the following rules.

(1) $N_\Pi^0 = \mathcal{O}_A^{(0)}$.

(2) For any $k \geq 0$, the class N_Π^{k+1} is defined by

$$N_\Pi^{k+1} = \{\Pi(x_{k+1}, g, g') \mid g, g' \in N_\Pi^k\}.$$

We denote by N_Π the class $\bigcup_{k\geq 0} N_\Pi^k$ of the Π-*normal forms*.

Observe that $N_\Pi^k \subseteq \mathcal{O}_A^{(k)}$ for every $k \geq 0$. By repeated applications of (5), we get the following result.

Proposition 2.4. *If Π is a pivotal operation, then $\Lambda_\Pi \subseteq N_\Pi$.*

2.4. **Symmetric pivotal operations.** As we will see later in the paper, a pivotal operation Π is not necessarily Π-decomposable. However, when it is, then it verifies certain symmetry properties. Consider the following equations:

$$\Pi(x, y, z) = \Pi(z, x, y), \tag{6}$$

$$\Pi(x, y, z) = \Pi(z, y, x), \tag{7}$$

$$\Pi(x, 1, 0) = x, \tag{8}$$

Clearly, Π is symmetric if and only if it satisfies (6) and (7). The following result states that if $\Pi \in \Lambda_\Pi$ and satisfies (6) and (8), then it is symmetric.

Proposition 2.5. *If Π is a Π-decomposable pivotal operation that satisfies* (8) *and* (6)*, then it satisfies* (7)*. In particular, Π is a symmetric operation.*

Proof. We obtain successively

$$\begin{aligned}
\Pi(x, y, z) &= \Pi(x, \Pi(1, y, z), \Pi(0, y, z)) && (9)\\
&= \Pi(x, \Pi(y, \Pi(1, 1, z), \Pi(1, 0, z)), \Pi(z, \Pi(0, y, 1), \Pi(0, y, 0))) && (10)\\
&= \Pi(x, \Pi(y, 1, z), \Pi(z, y, 0)) && (11)\\
&= \Pi(x, \Pi(z, y, 1), \Pi(z, y, 0)) && (12)\\
&= \Pi(z, y, x). && (13)
\end{aligned}$$

where (9), (10) and (13) were obtained by Π-decomposability of Π, and where (11) and (12) were obtained by (4), (8) and (7). □

Under the assumption of Π-decomposability of Π and (8), symmetry of a pivotal operation Π can be characterized in the following way.

Theorem 2.6. *Le Π be a Π-decomposable pivotal operation that satisfies* (8) *. The following conditions are equivalent.*

(*i*) *Π is symmetric.*
(*ii*) *Π satisfies the equations*

$$\Pi(0, 1, 0) = \Pi(0, 0, 1) \quad \textit{and} \quad \Pi(1, 1, 0) = \Pi(1, 0, 1).$$

Proof. It is clear that (i) implies (ii). Let us prove that (ii) implies (i). It suffices to prove that Π satisfies

$$\Pi(x, y, z) = \Pi(x, z, y), \tag{14}$$

$$\Pi(x, y, z) = \Pi(y, x, z). \tag{15}$$

First, note that for every $x \in A$ we obtain successively

$$\begin{aligned}
\Pi(x, 1, 0) &= \Pi(x, \Pi(1, 1, 0), \Pi(0, 1, 0)) = \Pi(x, \Pi(1, 0, 1), \Pi(0, 0, 1))\\
&= \Pi(x, 0, 1), && (16)
\end{aligned}$$

where the first identity is obtained by (7), the second by contition (ii) and the last one by Π-decomposability of Π. Then, for every $y \in A$ we have

$$\begin{aligned}
\Pi(x, y, 0) &= \Pi(y, \Pi(x, 1, 0), \Pi(x, 0, 0)) = \Pi(y, \Pi(x, 0, 1), \Pi(x, 0, 0))\\
&= \Pi(x, 0, y), && (18)
\end{aligned}$$

where the first and last identities are obtained by decomposability of Π, and the second by (16). Using a similar argument, we obtain

$$\Pi(x,y,1) \;=\; \Pi(x,1,y). \tag{19}$$

Finally, we obtain for any $z \in A$

$$\begin{aligned}\Pi(x,y,z) &= \Pi(z,\Pi(x,y,1),\Pi(x,y,0)) \;=\; \Pi(z,\Pi(x,1,y),\Pi(x,0,y))\\ &= \Pi(x,z,y),\end{aligned} \tag{20}$$

where the first and last identities are obtained by decomposability (5) of Π, and the second by (18) and (19). This proves that (14) holds. Now, using (8) and (4) in the first identity in (17) we obtain that

$$\Pi(x,y,0) \;=\; \Pi(y,x,0). \tag{21}$$

Similarly, we have

$$\begin{aligned}\Pi(x,y,1) &= \Pi(y,\Pi(x,1,1),\Pi(x,0,1)) \;=\; \Pi(y,1,x),\\ &= \Pi(y,x,1),\end{aligned} \tag{22}$$

where the first identity is obtained by decomposability of Π, the second by (4), (16) and (8), and the last one by (19). Using (21) and (22) in the first identity of (20), we obtain (15) by Π-decomposability of Π. □

3. Clones of pivotally decomposable operations

In Subsection 3.1, we provide sufficient conditions on a pivotal operation Π for Λ_Π to be a clone, and in Subsection 3.2, we prove that these conditions are also necessary under the assumption that Π belongs to Λ_Π, and satisfies two additional equations (30) and (31) that involves only Π, and the elements 0 and 1. Certain natural questions are also discussed and answered negatively by counter-examples that are constructed in Subsection 3.3.

3.1. Sufficient conditions for Λ_Π to be a clone.

Let us consider the following equations:

$$\Pi(\Pi(x,y,z),t,u) = \Pi(x,\Pi(y,t,u),\Pi(z,t,u)). \tag{23}$$

The relevance of property (23) is made apparent by the following lemma.

Lemma 3.1. *Let Π be a pivotal operation that satisfies* (23)*. If $f\colon A^n \to A$ and $g_1,\dots,g_n\colon A^m \to A$ are Π-decomposable, then so is $f(g_1,\dots,g_n)$.*

Proof. For every $i \in [n]$ let $g'_i\colon A^{nm} \to A$ be the operation defined by $g'_i(\mathbf{x}) = g_i(\mathbf{x}_i)$ where $\mathbf{x}_i = (x_{(i-1)m+1},\dots,x_{im})$. We prove that $f(g'_1,\dots,g'_n)$ is Π-decomposable. For $\mathbf{x} \in A^{nm}$, set

$$\mathbf{c}^0_{\mathbf{x}} = f(0,g'_2(\mathbf{x}),\dots,g'_n(\mathbf{x})), \qquad \mathbf{c}^1_{\mathbf{x}} = f(1,g'_2(\mathbf{x}),\dots,g'_n(\mathbf{x})),$$
$$\mathbf{a}^0_{\mathbf{x}} = g'_1(0,x_2,\dots,x_{nm}), \qquad \mathbf{a}^1_{\mathbf{x}} = g'_1(1,x_2,\dots,x_{nm}).$$

We obtain by Π-decomposability of f that

$$f(g'_1(\mathbf{x}),\dots,g'_n(\mathbf{x})) = \Pi(g'_1(\mathbf{x}),\mathbf{c}^1_{\mathbf{x}},\mathbf{c}^0_{\mathbf{x}}).$$

By iterating the pivotal decomposition expression (to each argument), we get the following equalities

$$\begin{aligned}\Pi(g'_1(\mathbf{x}),\mathbf{c}^1_{\mathbf{x}},\mathbf{c}^0_{\mathbf{x}}) &= \Pi(\Pi(x_1,\mathbf{a}^1_{\mathbf{x}},\mathbf{a}^0_{\mathbf{x}}),\mathbf{c}^1_{\mathbf{x}},\mathbf{c}^0_{\mathbf{x}}),\\ &= \Pi(x_1,\Pi(\mathbf{a}^1_{\mathbf{x}},\mathbf{c}^1_{\mathbf{x}},\mathbf{c}^0_{\mathbf{x}}),\Pi(\mathbf{a}^0_{\mathbf{x}},\mathbf{c}^1_{\mathbf{x}},\mathbf{c}^0_{\mathbf{x}})),\\ &= \Pi(x_1,f(g'_1,\dots,g'_n)(\mathbf{x}^1_1),f(g'_1,\dots,g'_n)(\mathbf{x}^0_1)),\end{aligned}$$

where the first equality is obtained by Π-decomposability of g'_1, the second one by equation (23) and the last one by Π-decomposability of f. Thus, we have proved that condition (5) holds for $f(g'_1, \ldots, g'_n)$ and $i = 1$. We can proceed in a similar way to obtain

$$f(g'_1(\mathbf{x}), \ldots, g'_n(\mathbf{x})) = \Pi(x_\ell, f(g'_1, \ldots, g'_n)(\mathbf{x}^1_\ell), f(g'_1, \ldots, g'_n)(\mathbf{x}^0_\ell)), \tag{24}$$

for every $\ell \in [nm]$. The decomposability of $\Pi(g_1, \ldots, g_n)$ follows from (24) by identifying all arguments in $\{x_i, x_{m+i}, \ldots, x_{(n-1)m+i}\}$ for every $i \in [m]$. □

Similarly, if the pivotal operation satisfies equation (8), then Λ_Π must contain all projections.

Lemma 3.2. *Let Π be a pivotal operation. The following conditions are equivalent.*

(i) Π satisfies equation (8).
(ii) Λ_Π contains all projections on A.
(iii) Λ_Π contains the unary projection p^1_1.

Proof. (i) $\implies$ (ii): Let $n \geq 1$ and $k \in [n]$. For every $i \in [n]$ such that $i \neq k$ and for every $\mathbf{x} \in A^n$,

$$\Pi(x_i, p^n_k(\mathbf{x}^1_i), p^n_k(\mathbf{x}^0_i)) = \Pi(x_i, x_k, x_k) = x_k$$

where the last equality is obtained by (4). If $i = k$, then

$$\Pi(x_i, p^n_k(\mathbf{x}^1_i), p^n_k(\mathbf{x}^0_i)) = \Pi(x_k, 1, 0) = x_k$$

where the last equality is obtained by (8). We conclude that $p^n_k \in \Lambda_\Pi$.

(ii) $\implies$ (iii): Trivial.

(iii) $\implies$ (i): If Λ_Π contains the unary projection p^1_1, then for every $x \in A$ we have

$$x = p^1_1(x) = \Pi(x, 1, 0).$$

Thus Π satisfies equation (8), and the proof of the lemma is now complete. □

By combining Lemmas 2.2, 3.1, and 3.2, we obtain the following result.

Proposition 3.3. *Suppose that Π is a pivotal operation that satisfies equation (23). Then Λ_Π is a clone if and only if Π satisfies equation (8). In the latter case, Λ_Π is a clone that contains all constant operations.*

We illustrate the previous results by analyzing the particular case of Boolean functions.

Example 3.4. Let Π be a Boolean pivotal operation such that Λ_Π is a clone. According to Proposition 3.2, the operation Π satisfies equation (8). Hence, the unary sections $\Pi(x, 0, 0)$ and $\Pi(x, 1, 1)$ are determined by (4) while the value of the section $\Pi(x, 1, 0)$ is determined by (8):

$$\Pi(x, 0, 0) = 0, \qquad \Pi(x, 1, 1) = 1, \quad \Pi(x, 1, 0) = x. \tag{25}$$

Moreover, it is not difficult to check that the four possibilities for the unary section $\Pi(x, 0, 1)$, namely,

$$\Pi_0(x, 0, 1) = x, \qquad \Pi_1(x, 0, 1) = \overline{x},$$
$$\Pi_2(x, 0, 1) = 0, \qquad \Pi_3(x, 0, 1) = 1,$$

give rise to operations $\Pi_0, \ldots, \Pi_3$ that satisfy equation (23). Simple computations then show that we must have

$$\Pi_0(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z), \qquad \Pi_1(x, y, z) = (x \wedge y) \vee (\overline{x} \wedge z),$$
$$\Pi_2(x, y, z) = y \wedge (x \vee z), \qquad \Pi_3(x, y, z) = z \vee (x \wedge y).$$

Hence, the clones $\Lambda_{\Pi_0}, \ldots, \Lambda_{\Pi_3}$ are as follows:

(a) Λ_{Π_0} is the clone M of all monotone Boolean functions, since $\Pi_0 = \text{med}$;
(b) Λ_{Π_1} is the clone $\mathcal{O}_{\{0,1\}}$ of all Boolean functions, since Π_1 is the pivotal operation used in Shannon decomposition;
(c) Λ_{Π_2} is the clone M of all monotone Boolean functions, since $\Pi_2(x, y, 0) = y \wedge x$ and $\Pi_2(x, 1, z) = x \vee z$, and every composition of Π_2 with projections or constants is monotone;
(d) Λ_{Π_3} is the clone M of all monotone Boolean functions (by a similar argument to that used for Λ_{Π_2}).

The situation can be summarized by the following result.

Proposition 3.5. *If $\mathcal{C}$ is Boolean clone, then there is a Boolean pivotal operation Π such that $\mathcal{C} = \Lambda_\Pi$ if and only if $\mathcal{C}$ is the clone of all monotone Boolean functions or the clone of all Boolean functions.*

3.2. **The case of a pivotally decomposable Π.** In the section, we derive results about clones of Π-decomposable operations under the additional assumption that the operation Π itself is Π-decomposable, i.e., that $\Pi \in \Lambda_\Pi$.

The next result states that under this assumption, the pivotal operation together with constant maps suffice to construct expressions representing each member of Λ_Π.

Proposition 3.6. *Let Π be a pivotal operation such that Λ_Π is a clone that contains Π. Then Λ_Π is the clone generated by Π and the constant maps. In particular, $\Lambda_\Pi = N_\Pi$.*

Proof. Let C be the clone generated by Π and the constant operations. We have to prove that $\Lambda_\Pi = C$. The right to left inclusion is trivial since Λ_Π is a clone and contains each of the mentioned generators of C by assumption and Lemma 2.2. We derive the converse inclusion and the last part of the statement from the following sequence of inclusions,

$$\Lambda_\Pi \subseteq N_\Pi \subseteq C \subseteq \Lambda_\Pi,$$

where the first inclusion is obtained by Proposition 2.4, the second inclusion follows from the definitions of N_Π and C, and the third inclusion is a consequence of the first part of this proof. □

In the presence of a Π-decomposable operation Π, equation (8) has interesting consequences on the equational theory of the the algebra $\langle A, \Pi, 0, 1\rangle$, where Π is a pivotal operation.

Lemma 3.7. *If Π is a pivotal operation on A that satisfies* (8)*, then it satisfies the following equations:*

$$\Pi(0, 1, z) = z, \tag{26}$$

$$\Pi(1, 1, z) = 1, \tag{27}$$

$$\Pi(0, y, 0) = 0, \tag{28}$$

$$\Pi(1, y, 0) = y. \tag{29}$$

Proof. The proof follows from straightforward applications of equations (5) and (8). For instance, we obtain successively

$$\Pi(0, 1, z) = \Pi(z, \Pi(0, 1, 1), \Pi(0, 1, 0)) = \Pi(z, 1, 0) = z,$$

where the first equality is obtained by (5) and the two last ones by (8). □

According to Proposition 3.3, if Π is a pivotal operation that satisfies equations (8) and (23), then Λ_Π is a clone. In the next theorem, we prove that the converse

statement also holds, under the assumption that $\Pi \in \Lambda_\Pi$ and that

$$\Pi(\Pi(1,0,1),0,1) = \Pi(1,\Pi(0,0,1),\Pi(1,0,1)), \tag{30}$$

$$\Pi(\Pi(0,0,1),0,1) = \Pi(0,\Pi(0,0,1),\Pi(1,0,1)). \tag{31}$$

Theorem 3.8. *Let Π be a Π-decomposable pivotal operation that satisfies* (30) *and* (31)*. The following conditions are equivalent:*

(i) Λ_Π *is a clone,*
(ii) Π *satisfies equations* (8) *and* (23)*.*

In this case, Λ_Π *is the clone generated by* Π *and the constant maps.*

Proof. Proposition 3.3 states that (ii) $\implies$ (i). Conversely, assume that Π is a pivotal operation such that Λ_Π is a clone that contains Π. By Lemma 3.2, it follows that Π satisfies equation (8).

We prove that (23) also holds. In what follows, we use without further warning the fact that Λ_Π is a clone that contains Π and every constant operation to apply (5) to operations which are compositions of Π and constant ones.

Hence, if $L(x,y,z)$ and $R(x,y,z)$ denote the operations given by the left-hand side and right-hand side of equation (23), respectively, we have

$$L(x,y,z) = \Pi\big(x,\Pi\big(\Pi(1,y,z),t,u\big),\Pi\big(\Pi(0,y,z),t,u\big)\big),$$
$$R(x,y,z) = \Pi\big(x,\Pi\big(1,\Pi(y,t,u),\Pi(z,t,u)\big),\Pi\big(0,\Pi(y,t,u),\Pi(z,t,u)\big)\big).$$

To prove that $L(x,y,z) = R(x,y,z)$ it suffices to prove that the two following equations hold:

$$\Pi\big(\Pi(1,y,z),t,u\big) = \Pi\big(1,\Pi(y,t,u),\Pi(z,t,u)\big), \tag{32}$$

$$\Pi\big(\Pi(0,y,z),t,u\big) = \Pi\big(0,\Pi(y,t,u),\Pi(z,t,u)\big). \tag{33}$$

We prove that (32) holds (with the help of (30)). Equation (33) can be obtained in a similar way (with the help of (31)).

By decomposing with respect to y, we obtain that the right-hand side of (32) is equal to

$$\Pi\big(y,\Pi\big(\Pi(1,1,z),t,u\big),\Pi\big(\Pi(1,0,z),t,u\big)\big),$$

while the left-hand side of (32) is equal to

$$\Pi\big(y,\Pi\big(1,\Pi(1,t,u),\Pi(z,t,u)\big),\Pi\big(1,\Pi(0,t,u),\Pi(z,t,u)\big)\big).$$

Hence, to prove that equation (32) holds, we first observe that

$$\begin{aligned}
\Pi\big(\Pi(1,1,z),t,u\big) &= \Pi(1,t,u) && \text{by (27)},\\
&= \Pi\big(z,\Pi(1,t,u),\Pi(1,t,u)\big) && \text{by (4)},\\
&= \Pi\big(z,\Pi\big(1,\Pi(1,t,u),\Pi(1,t,u)\big),\Pi\big(1,\Pi(0,t,u),\Pi(1,t,u)\big)\big), && \text{by (5), (4)},\\
&= \Pi\big(1,\Pi(1,t,u),\Pi(z,t,u)\big) && \text{by (5)}.
\end{aligned}$$

It remains to prove that

$$\Pi\big(\Pi(1,0,z),t,u\big) = \Pi\big(1,\Pi(0,t,u),\Pi(z,t,u)\big). \tag{34}$$

By decomposing with regard to z we obtain

$$\Pi\big(\Pi(1,0,z),t,u\big) = \Pi\big(z,\Pi\big(\Pi(1,0,1),t,u\big),\Pi(0,t,u)\big),$$
$$\Pi\big(1,\Pi(0,t,u),\Pi(z,t,u)\big) = \Pi\big(z,\Pi\big(1,\Pi(0,t,u),\Pi(1,t,u)\big),\Pi(0,t,u)\big),$$

and it suffices to prove that

$$\Pi\big(\Pi(1,0,1),t,u\big) = \Pi\big(1,\Pi(0,t,u),\Pi(1,t,u)\big). \tag{35}$$

Observe that by decomposing with respect to u,

$$\Pi\big(\Pi(1,0,1),t,u\big) = \Pi\big(u,\Pi\big(\Pi(1,0,1),t,1\big),\Pi\big(\Pi(1,0,1),t,0\big)\big),$$
$$\Pi\big(1,\Pi(0,t,u),\Pi(1,t,u)\big) = \Pi\big(u,\Pi\big(1,\Pi(0,t,1),\Pi(1,t,1)\big),\Pi\big(1,0,\Pi(1,t,0)\big)\big),$$

where we have applied (28) to obtain the second identity. Hence, to prove (35) it suffices to prove that

$$\Pi\big(\Pi(1,0,1),t,1\big) = \Pi\big(1,\Pi(0,t,1),\Pi(1,t,1)\big), \tag{36}$$
$$\Pi\big(\Pi(1,0,1),t,0\big) = \Pi\big(1,0,\Pi(1,t,0)\big). \tag{37}$$

By (5) we obtain

$$\Pi\big(\Pi(1,0,1),t,0\big) = \Pi\big(t,\Pi(1,0,1),0\big) = \Pi\big(1,0,\Pi(1,t,0)\big),$$

which proves (37). Next, we observe that

$$\Pi\big(\Pi(1,0,1),t,1\big) = \Pi\big(t,1,\Pi\big(\Pi(1,0,1),0,1\big)\big)$$
$$\Pi\big(1,\Pi(0,t,1),\Pi(1,t,1)\big) = \Pi\big(t,1,\Pi\big(1,\Pi(0,0,1),\Pi(1,0,1)\big)\big).$$

We conclude that (36) is satisfied by applying (31), which holds by assumption. □

Since (30) and (31) are instances of (23), Theorem 3.8 can be restated as follows.

Corollary 3.9. *Let Π be a Π-decomposable pivotal operation. The following conditions are equivalent:*

(i) Λ_Π *is a clone and* Π *satisfies* (30) *and* (31)*,*
(ii) Π *satisfies* (8) *and* (23)*.*

By noting that equations (30) and (31) are satisfied by a symmetric pivotal operation that satisfies (8), we obtain the following corollary.

Corollary 3.10. *Let Π be a symmetric Π-decomposable pivotal operation that satisfies* (8)*. The following conditions are equivalent:*

(i) Λ_Π *is a clone,*
(ii) Π *satisfies* (23)*.*

3.3. **Further issues and counter-examples.** In view of Theorem 3.8 and Corollary 3.9, a natural question arises: can the Π-decomposability of Π be deduced from equations (8) and (23)? Example 3.4 shows that the answer is positive if Π is a Boolean pivotal operation. Now, we prove that it is not true in general. We set $A_\Delta = \{(x,y) \in A^2 \mid x \neq y \ \&\ (x,y) \neq (1,0)\}$.

Proposition 3.11. *Let Π be a pivotal operation that satisfies* (8)*. If there exits a function $f\colon A_\Delta \to A$ such that $\Pi(x,y,z) = f(y,z)$ for every $(y,z) \in A_\Delta$, then Π also satisfies* (23)*.*

Proof. Note first that Π is well defined by the conditions in the statement. Moreover, equations (4) and (8) ensure that (23) is satisfied when $t = u$ or $(t,u) = (1,0)$, respectively. Now, if $(t,u) \in A_\Delta$, then

$$\Pi(\Pi(x,y,z),t,u) = f(t,u) = \Pi(x,f(t,u),f(t,u)) = \Pi(x,\Pi(y,t,u),\Pi(z,t,u)).$$

This shows that (23) does indeed hold for such a Π. □

Example 3.12. Assume that A has at least three elements $0,1,2$. Let $f\colon A_\Delta \to A$ be any mapping that satisfies $f(2,0) = f(2,1) \neq f(2,2)$. Then the pivotal operation Π defined as in Proposition 3.11 is not Π-decomposable since $\Pi(1,2,2) = f(2,2)$ while $\Pi(2,\Pi(1,2,1),\Pi(1,2,0)) = f(2,0)$.

Theorem 3.8 gives a characterization of pivotal operations Π such that Λ_Π is a clone, under the assumption that $\Pi \in \Lambda_\Pi$. We now give an example of a pivotal operation Π such that Λ_Π is a clone that does not contain Π. Note however that Example 3.4 shows that such a Π does not exist in the case of Boolean functions.

Example 3.13. Let $A = \{0, a, 1\}$ and $N\colon A \to A$ be the map defined by $N(0) = 1$, $N(a) = a$, and $N(1) = 0$. Define $\Pi\colon A^3 \to A$ as the map that satisfies (8), (4) and

$$\Pi(x, 0, 1) = N(x) \tag{38}$$

$$\Pi(x, 1, a) = 1 \tag{39}$$

$$\Pi(x, 0, a) = 1 \tag{40}$$

$$\Pi(x, a, 1) = 0 \tag{41}$$

$$\Pi(x, a, 0) = 0. \tag{42}$$

First, observe that $\Pi \notin \Lambda_\Pi$. Indeed, for any $x \in A$ we have on the one hand $\Pi(x, a, a) = a$ while $\Pi(a, \Pi(a, \Pi(x, 1, a), \Pi(x, 0, a)) = \Pi(a, 1, 1) = 1$. According to Proposition 3.3, it suffices to prove that Π satisfies equation (23). If $t = u$ or $(t, u) \in \{(a, 0), (a, 1), (1, a), (0, a)\}$ then $\Pi(x, t, u)$ is constant and (23) holds trivially. If $(t, u) = (1, 0)$ then $\Pi(x, t, u)$ is the first projection and (23) holds as well. It remains to consider the case $(t, u) = (0, 1)$. We have to prove

$$\Pi(x, N(y), N(z)) \;=\; N(\Pi(x, y, z)). \tag{43}$$

If $y = z$ then or $(y, z) \in \{(a, 0), (a, 1), (1, a), (0, a)\}$ then(43) clearly holds by (39) - (42). If $(y, z) \in \{(0, 1), (1, 0)\}$ then (43) holds by (38).

4. Conclusions and Further Research

In this paper, we studied pivotal decompositions of operations from a clone theory perspective, and presented a characterization of classes of Π-decomposable operations that are clones in the case when the pivotal operation Π is itself Π-decomposable and satisfies (30) and (31). However in Example 3.13 we showed that there exists a clone of Π-decomposable operations that does not contain Π, i.e., Π is not Π-decomposable. This leaves open a complete description of classes of pivotally decomposable operations that are clones. Moreover, once such a description is obtained, a structural analysis of the set of all pivotally decomposable clones is to be expected.

Another topic that will deserve our attention is motivated by Theorem 2.6 that states that if a pivotal operation Π is a Π-decomposable and satisfies $\Pi(x, 1, 0) = x$, $\Pi(0, 0, 1) = 0$, and $\Pi(1, 0, 1) = 1$, then Π is symmetric and hence is a majority operation. Furthermore, if Π satisfies (23), then Π is a median operation (see [2] and the bibliography therein). These observations establish noteworthy connections between pivotally decomposable classes and median algebras, and should deserve a deeper study in future research.

As a third line of research that emerges from this paper deals with normal form representations of operations arising from pivotal decomposition schemes. Proposition 2.4 provides normal form representations for the elements of a pivotally decomposable class. Here, determining canonical expressions for these representations based on the pivotal operation, as well as studying the complexity of such representations (e.g., with respect to classical normal form representations) constitute an interesting topic of research which is under current investigation. We envision a similar study to that of [3] where, in particular, it was shown that normal form representations of Boolean functions that use the ternary median as the only logical connective, produce asymptotically shorter representations than the classical DNF, CNF and polynomial representations.

Acknowledgment

This work was supported by the internal research project F1R-MTH-PUL-15MRO3 of the University of Luxembourg.

References

[1] R.E. Barlow, F. Proschan. Importance of system components and fault tree events, *Stochastic Process. Appl.* **3** (1975) 153–172.

[2] H. J. Bandelt and J. Hedlíková. Median algebras. *Discrete mathematics*, 45:1–30, 1983.

[3] M. Couceiro, S. Foldes, E. Lehtonen. Composition of Post classes and normal forms of Boolean functions, *Discrete Math.* **306** (2006) 3223–3243.

[4] M. Couceiro, E. Lehtonen, J.-L. Marichal, T. Waldhauser. An algorithm for producing median normal form representations for Boolean functions, in the proceedings of the *Reed–Muller Workshop 2011*, 49–54, 2011.

[5] M. Couceiro, and J.-L. Marichal. Polynomial functions over bounded distributive lattices, *J. Multiple-Valued Logic Soft Comput.* **18** (2012) 247–256.

[6] M. Couceiro, B. Teheux. Clones of pivotally decomposable functions. *45th IEEE International Symposium on Multiple-Valued Logic* (ISMVL 2015), IEEE Computer Society, 195–198.

[7] M. Couceiro, M. Pouzet. On a quasi-order on Boolean functions, *Theoret. Comput. Sci.* **396** (2008) 71–87.

[8] K. Denecke, S. L. Wismath. *Universal Algebra and Applications in Theoretical Computer Science,* Chapman & Hall/CRC, Boca Raton, 2002.

[9] L. Hellerstein. On generalized constraints and certificates, *Discrete Math.* **226** (2001) 211–232.

[10] D. Lau. *Function Algebras on Finite Sets,* Springer-Verlag, Berlin, Heidelberg, 2006.

[11] E. Lehtonen. Descending chains and antichains of the unary, linear, and monotone subfunction relations, *Order* **23** (2006) 129–142.

[12] E. Lehtonen, Á. Szendrei. Equivalence of operations with respect to discriminator clones, *Discrete Math.* **309** (2009) 673–685.

[13] J.-L. Marichal. Weighted lattice polynomials, *Discrete Math.* **309** (2009) 814–820.

[14] J.-L. Marichal, B. Teheux. Pivotal decompositions of functions, *Discrete Appl. Math.*, 174:102–112, 2014.

[15] F. Miyata. Realization of arbitrary logical functions using majority elements, *IEEE Trans. on Electronic Computers* **EC-12** (1963) 183–191.

[16] N. Pippenger. Galois theory for minors of finite functions, *Discrete Math.* **254** (2002) 405–419.

[17] E. L. Post. *The Two-Valued Iterative Systems of Mathematical Logic,* Annals of Mathematical Studies, vol. 5, Princeton University Press, Princeton, 1941.

[18] C.E. Shannon. A symbolic analysis of relay and switching circuits, *Trans. Am. Inst. Electr. Eng.* **57** (1938) 713–723.

[19] Y. Tohma. Decompositions of logical functions using majority decision elements, *IEEE Trans. on Electronic Computers* **EC-13** (1964) 698–705.

LORIA, (CNRS - Inria Nancy Grand Est - Université de Lorraine), BP239 - 54506 Vandoeuvre les Nancy, France

E-mail address: `miguel.couceiro@{loria,inria}.fr`

Mathematics Research Unit, FSTC, University of Luxembourg, 6, rue Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: `bruno.teheux@uni.lu`