Clones of Pivotally Decomposable Functions

Miguel Couceiro LORIA

(CNRS - Inria Nancy Grand Est - Université de Lorraine)

Equipe Orpailleur – Bâtiment B, Campus Scientifique B.P. 239

54506 Vandœuvre-lès-Nancy Cedex, France France

Email: miguel.couceiro[at]inria.fr

Bruno Teheux

Mathematics Research Unit, FSTC,
 University of Luxembourg
 6, rue Coudenhove-Kalergi
L-1359 Luxembourg, Luxembourg
 Email: bruno.teheux[at]uni.lu

Abstract—This paper is a contribution to the understanding of the relation between pivotal decompositions of operations on a set A and clones on the same set. In this preliminary study we establish sufficient conditions on a pivotal operation Π so that the corresponding class of Π -decomposable operations constitutes a clone, and discuss the normal form representations that such pivotal operations induce. We also outline several open questions, providing directions for further research.

I. 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 operations $f\colon\{0,1\}^n\to\{0,1\}$ 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 $\mathbf{x} = (x_1, \dots, x_n) \in \{0, 1\}^n$ 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*) [16], or *pivotal decomposition* [1]. Boolean operations 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 \land and \lor) that were shown in [11] to be decomposable into expressions of the form

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

where med is the ternary lattice polynomial given by

$$\operatorname{med}(x_1, x_2, x_3) = (x_1 \land x_2) \lor (x_1 \land x_3) \lor (x_2 \land x_3)$$
$$= (x_1 \lor x_2) \land (x_1 \lor x_3) \land (x_2 \lor x_3).$$

The latter decomposition scheme is referred to as *median decomposition* in [4] and [11]. We refer the reader to [3], [13], [17] for applications of the median decomposition formula to obtain median representations of Boolean operations.

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 $\Pi(x, y, z) = xy + (1 x)z$,
- in (2) we have $\Pi(x, y, z) = (x \wedge y) \vee (\overline{x} \wedge z)$, and
- in (3) we have $\Pi(x, y, z) = \text{med}(x, y, z)$.

These facts were observed in [12] where these decomposition schemes, called *pivotal decompositions*, were investigated. In particular, it was observed that not every ternary operation serves as a pivotal operation.

In this paper we are interested in classes of pivotally decomposable operations that constitute clones of operations over a set A. Our motivation is rooted in [2] where a study of normal form representations of Boolean operations was presented and based on compositions of Boolean clones. In particular, it was shown that normal form representations of Boolean operations that have the ternary operator med as the only logical connective, allow shorter representations than the classical DNF, CNF and polynomial representations.

As we will see, clones of pivotally decomposable operations provide nice normal form representations having a unique operation as logical connective, namely, the corresponding pivotal operation.

The paper is organised as follows. After recalling in Section II basic notions and terminology needed throughout the paper, we define the concept of pivotal operation and that of pivotally decomposable class in Section III and introduce the notion of normal form associated with a pivotal operation and mention some related properties. In Section IV we establish sufficient conditions on pivotal operations so that the corresponding pivotal decomposable classes constitute clones. As it turns out, such a clone can be generated by the corresponding pivotal operation together with constant operations. As a concrete example, we analyse the case of Boolean operations and conclude that only 4 of them can be used as pivotal operations, and we also provide the descriptions of the corresponding clones of pivotally decomposable operations.

We finish the paper with some concluding remarks as well as few unsettled questions that we present as open problems in Section V.

II. PRELIMINARIES: BASIC NOTIONS AND NOTATIONS

For any positive integer n, we denote by [n] the set $\{1,\ldots,n\}$. 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 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 way that it is inessential.

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

- contains all projections on A, i.e., operations $p_i^n \colon A^n \to A$ given by $p_i^n(x_1, \ldots, x_n) = x_i$ for $i \in [n]$, and
- is closed under 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

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

also belongs to C.

In the case when A is finite, the set of all clones on Aforms 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., [6], [8]. In the case when |A| = 2, the lattice of clones on A is countably infinite, and it was completely described by E. Post [15]. In particular, it follows that each Boolean clone can be generated by a finite set of Boolean operations. For instance,

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

For further background see, e.g., [6], [8].

III. PIVOTAL OPERATIONS AND INDUCED NORMAL FORMS

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 1 (Definition 2.1 in [12]). A pivotal operation on A is a ternary operation Π on A that satisfies the equation

$$\Pi(x, y, y) = y. (4)$$

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

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

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

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 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

- $\begin{array}{ll} 1) & N_{\Pi}^{0} = \mathcal{O}_{A}^{(0)}. \\ 2) & \text{For any } k \geq 0 \text{, the class } N_{\Pi}^{k+1} \text{ is defined by } N_{\Pi}^{k+1} = \\ & \{\Pi(x_{k+1},g,g') \mid g,g' \in N_{\Pi}^{k}\}. \end{array}$

We denote by N_{Π} the class $\bigcup_{k>0} N_{\Pi}^k$ 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 4. If Π is a pivotal operation, then $\Lambda_{\Pi} \subseteq N_{\Pi}$.

IV. CLONES OF PIVOTALLY DECOMPOSABLE OPERATIONS

We aim to give conditions on a pivotal operation Π for Λ_{Π} to be a clone. To this extent, we consider the following equations:

$$\Pi(x,1,0) = x,\tag{6}$$

$$\Pi(\Pi(x, y, z), t, u) = \Pi(x, \Pi(y, t, u), \Pi(z, t, u)).$$
 (7)

The relevance of property (7) is made apparent by the following lemma.

Lemma 5. Let Π be a pivotal operation that satisfies (7). If $f: A^n \to A \text{ and } g_1, \ldots, g_n: A^m \to A \text{ are } \Pi\text{-decomposable},$ then so is $f(g_1, \ldots, g_n)$.

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

$$\mathbf{c}_{\mathbf{x}}^{0} = f(0, g'_{2}(\mathbf{x}), \dots, g'_{n}(\mathbf{x})),$$

$$\mathbf{c}_{\mathbf{x}}^{1} = f(1, g'_{2}(\mathbf{x}), \dots, g'_{n}(\mathbf{x})),$$

$$\mathbf{a}_{\mathbf{x}}^{0} = g'_{1}(0, x_{2}, \dots, x_{nm}),$$

$$\mathbf{a}_{\mathbf{x}}^{1} = g'_{1}(1, x_{2}, \dots, x_{nm}).$$

We obtain by Π -decomposability of f that

$$f(g_1'(\mathbf{x}), \dots, g_n'(\mathbf{x})) = \Pi(g_1'(\mathbf{x}), \mathbf{c}_{\mathbf{x}}^1, \mathbf{c}_{\mathbf{x}}^0).$$

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

$$\begin{split} \Pi(g_{1}'(\mathbf{x}), &\mathbf{c}_{\mathbf{x}}^{1}, \mathbf{c}_{\mathbf{x}}^{0}) \\ &= \Pi(\Pi(x_{1}, \mathbf{a}_{\mathbf{x}}^{1}, \mathbf{a}_{\mathbf{x}}^{0}), \mathbf{c}_{\mathbf{x}}^{1}, \mathbf{c}_{\mathbf{x}}^{0}), \\ &= \Pi(x_{1}, \Pi(\mathbf{a}_{\mathbf{x}}^{1}, \mathbf{c}_{\mathbf{x}}^{1}, \mathbf{c}_{\mathbf{x}}^{0}), \Pi(\mathbf{a}_{\mathbf{x}}^{0}, \mathbf{c}_{\mathbf{x}}^{1}, \mathbf{c}_{\mathbf{x}}^{0})), \\ &= \Pi(x_{1}, f(g_{1}', \dots, g_{n}')(\mathbf{x}_{1}^{1}), f(g_{1}', \dots, g_{n}')(\mathbf{x}_{1}^{0})), \end{split}$$

where the first equality is obtained by Π -decomposability of g'_1 , the second one by equation (7) 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

$$f(g_1'(\mathbf{x}), \dots, g_n'(\mathbf{x})) = \Pi(x_\ell, f(g_1', \dots, g_n')(\mathbf{x}_\ell^1),$$
$$f(g_1', \dots, g_n')(\mathbf{x}_\ell^0)), \quad \ell \in [nm]. \quad (8)$$

The decomposability of $\Pi(g_1,\ldots,g_n)$ follows from (8) 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 (6), then Λ_Π must contain all projections.

Lemma 6. Let Π be a pivotal operation. The following conditions are equivalent.

- 1) Π satisfies equation (6).
- 2) Λ_{Π} contains all projections on A.
- 3) Λ_{Π} contains the unary projection p_1^1 .

Proof: 1) \implies 2): Let $n \ge 1$ and $k \in [n]$. For every $i \in [n]$ such that $i \ne k$ and for every $\mathbf{x} \in A^n$,

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

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

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

where the last equality is obtained by (6). We conclude that $p_k^n \in \Lambda_{\Pi}$.

- 2) \implies 3): Trivial.
- 3) \Longrightarrow 1): 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 (6), and the proof of the lemma is now complete.

By combining Lemmas 2, 5, and 6, we obtain the following result.

Proposition 7. Suppose that Π is a pivotal operation that satisfies equation (7). Then Λ_{Π} is a clone if and only if Π satisfies equation (6). In the latter case, Λ_{Π} is a clone that contains all constant operations.

In addition, if Λ_Π is a clone containing the pivotal operation $\Pi,$ then we have that the pivotal operation together with constant maps suffice to construct expressions representing each member of $\Lambda_\Pi.$

Proposition 8. 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. 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 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 example below, we analyse the particular case of Boolean operations, and we determine those operations that can be used as pivotal operations Π and identify the corresponding Boolean clones, i.e., those of the form Λ_{Π} .

Example 9. Let Π be a Boolean pivotal operation that satisfies (6). Then 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 (6):

$$\Pi(x,0,0) = 0, \qquad \Pi(x,1,1) = 1, \quad \Pi(x,1,0) = x.$$
 (9)

Moreover, it is not difficult to check that the four possibilities for the unary section $\Pi(x,0,1)$ give rise to operations Π that satisfy equation (7). Hence, there are four Boolean operations Π_0,\ldots,Π_3 that verify the conditions of Proposition 7. Each of these operations satisfies the equations given in (9) and are determined by

$$\begin{split} \Pi_0(x,0,1) &= x, \\ \Pi_1(x,0,1) &= \overline{x}, \\ \Pi_2(x,0,1) &= 0, \\ \Pi_3(x,0,1) &= 1. \end{split}$$

Simple computations then show that we must have

$$\begin{split} &\Pi_0(x,y,z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z), \\ &\Pi_1(x,y,z) = (x \wedge y) \vee (\overline{x} \wedge z), \\ &\Pi_2(x,y,z) = y \wedge (x \vee z), \\ &\Pi_3(x,y,z) = z \vee (x \wedge y). \end{split}$$

Note that each Π_i , $i \in \{0,1,2,3\}$, is Π_i -decomposable, and hence each verifies $\Pi_i \in \Lambda_{\Pi_i}$. By Proposition 8, for each $i \in \{0,1,2,3\}$, Λ_{Π_i} is generated by Π and constants. Thus:

- Λ_{Π_0} is the clone M of all monotone Boolean operations, since $\Pi_0 = \text{med}$,
- Λ_{Π_1} is the clone $\mathcal{O}_{\{0,1\}}$ of all Boolean operations, since Π_1 is the pivotal operation used in Shannon decomposition,
- Λ_{Π_2} is the clone M of all monotone Boolean operations, 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, and
- Λ_{Π_3} is the clone M of all monotone Boolean operations (by a similar argument to that used for Λ_{Π_2}).

Furthermore, it follows from Lemma 6 that if Λ is a Boolean clone for which there exits a pivotal operation Π such that $\Lambda = \Lambda_{\Pi}$, then Π has to satisfy equation (6). We thus conclude that Λ is either M or $\mathcal{O}_{\{0,1\}}$.

V. CONCLUDING REMARKS AND FURTHER RESEARCH DIRECTIONS

In this paper we explored decomposition schemes for operations of several variables based on ternary operations, called pivotal operations, that subsume classical decompositions of Boolean functions and lattice polynomial functions.

As observed, different pivotal operations give rise to different classes of pivotally decomposable operations. Among the latter, some constitute clones while others do not, and we showed that those that are clones and contain the pivotal operation share the feature that their members have normal form representations by expressions that use a single nontrivial connective, namely, the corresponding pivotal operation.

In this preliminary study we presented sufficient conditions on pivotal operations which ensure that the resulting class of pivotally decomposable operations is a clone. Moreover, such clones were shown to contain all constant operations. Furthermore, if a clone contains the pivotal operations, then this operation together with the constant ones suffice to generate the given clone.

However, the question of determining necessary conditions still elludes us. Going even further, we would like to describe the natural Galois connection between pivotal operations and clones of operations, and establish a unified theory of corresponding normal form representations.

To achieve this goal, the following three questions should be answered that we must, for the time being, leave as open problems:

- (I) Give necessary conditions to complete the description of the Galois correspondence between pivotal operations and clones.
- (II) Determine canonical expressions for the normal form representations induced by pivotal operations, and provide procedures to build them.
- (III) Present a comparative study of such normal forms based on complexity of such representations (e.g., in terms length of produced expressions or efficiency of methods to treat them).

ACKNOWLEDGMENT

This work was supported by the internal research project F1R-MTHPUL-12RDO2 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] M. Couceiro, S. Foldes, E. Lehtonen. Composition of Post classes and normal forms of Boolean functions, *Discrete Math.* 306 (2006) 3223– 3243.
- [3] 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.
- [4] M. Couceiro, J.-L. Marichal. Polynomial functions over bounded distributive lattices, J. Multiple-Valued Logic Soft Comput. 18 (2012) 247–256.
- [5] M. Couceiro, M. Pouzet. On a quasi-order on Boolean functions, *Theoret. Comput. Sci.* 396 (2008) 71–87.
- [6] K. Denecke, S. L. Wismath. Universal Algebra and Applications in Theoretical Computer Science, Chapman & Hall/CRC, Boca Raton, 2002.
- [7] L. Hellerstein. On generalized constraints and certificates, *Discrete Math.* 226 (2001) 211–232.
- [8] D. Lau. Function Algebras on Finite Sets, Springer-Verlag, Berlin, Heidelberg, 2006.
- [9] E. Lehtonen. Descending chains and antichains of the unary, linear, and monotone subfunction relations, *Order* 23 (2006) 129–142.
- [10] E. Lehtonen, Á. Szendrei. Equivalence of operations with respect to discriminator clones, *Discrete Math.* 309 (2009) 673–685.
- [11] J.-L. Marichal. Weighted lattice polynomials, *Discrete Math.* **309** (2009) 814–820.
- [12] J.-L. Marichal, B. Teheux. Pivotal decompositions of functions, *Discrete Appl. Math.*, 174:102–112, 2014.
- [13] F. Miyata. Realization of arbitrary logical functions using majority elements, *IEEE Trans. on Electronic Computers* EC-12 (1963) 183–191.
- [14] N. Pippenger. Galois theory for minors of finite functions, *Discrete Math.* 254 (2002) 405–419.
- [15] E. L. Post. The Two-Valued Iterative Systems of Mathematical Logic, Annals of Mathematical Studies, vol. 5, Princeton University Press, Princeton, 1941.
- [16] C.E. Shannon. A symbolic analysis of relay and switching circuits, Trans. Am. Inst. Electr. Eng. 57 (1938) 713–723.
- [17] Y. Tohma. Decompositions of logical functions using majority decision elements, *IEEE Trans. on Electronic Computers* EC-13 (1964) 698–705.