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 $\Pi$ so that the corresponding class of $\Pi$-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 $f: A^n \to A$ 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 $f: \{0, 1\}^n \to \{0, 1\}$ that can be decomposed into expressions of the form

$$f(x) = x_kf(x_k^1) + (1 - x_k)f(x_k^0),$$

(1)

for $x = (x_1, \ldots, x_n) \in \{0, 1\}^n$ and $k \in [n]$ and where $x_k^c$ denotes the $n$-tuple obtained from $x$ 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

$$f(x) = (x_k \land f(x_k^1)) \lor (\top_k \land f(x_k^0))$$

(2)

where $\top_k = 1 - x_k$.

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

$$f(x) = \text{med}(f(x_k^0), x_k, f(x_k^1)),$$

(3)

where med is the ternary lattice polynomial given by

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

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,

$$f(x) = \Pi(x_k, f(x_k^1), f(x_k^0)).$$

Indeed,

- in (1) we have $\Pi(x, y, z) = xy + (1 - x)z$,
- in (2) we have $\Pi(x, y, z) = (x \land y) \lor (\top \land z)$, 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 \( f: A^n \to A \) is called an \( n \)-ary operation on \( A \). We denote by \( \mathcal{O}(n) \) 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 \( a \in A^n \) we define the \( S \)-section \( f^S_a \) of \( f \) as the \(|S|\)-ary operation on \( A \) defined by \( f^S_a(x) = f(a_i) \), where \( a_i \) is the \( i \)-tuple whose \( i \)-th coordinate is \( x_i \), if \( i \in S \), and otherwise.

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

1) contains all projections on \( A \), i.e., operations \( p^i_n: A^n \to A \) given by \( p^i_n(x_1, \ldots, x_n) = x_i \) for \( i \in [n] \), and

2) 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 \( f(g_1, \ldots, g_n) \in \mathcal{O}_A^{mn} \) that is defined by

\[
 f(g_1, \ldots, g_n)(x) = f(g_1(x), \ldots, g_n(x)) \quad (x \in A^n)
\]

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 \( n \)-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 \( a \in A^n \) we define the \( S \)-section \( f^S_a \) of \( f \) as the \(|S|\)-ary operation on \( A \) defined by \( f^S_a(x) = f(a_i) \), where \( a_i \) is the \( i \)-tuple whose \( i \)-th coordinate is \( x_i \), if \( i \in S \), and otherwise.

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

\[
 f(x) = \Pi(x_i, f(x_i)), \quad x \in A^n, i \in [n].
\]

Also, we denote by \( \Lambda \) the class of \( \Pi \)-decomposable operations on \( A \).

Note that condition (4) ensures that \( \Pi \)-decomposability of an operation does not depend on its inessential arguments. Indeed, if the \( j \)-th argument of \( f \) is inessential, then \( f(x) = f(x_1) = f(x_0) \) for every \( x \in A^n \). It follows from (4) that \( f(x) = \Pi(x_i, f(x_i)), f(x_j) \) for any \( x \in A^n \). In particular, we can state the following result.

Lemma 2. If \( f \) is a pivotal operation, then every constant operation on \( A \) is \( \Pi \)-decomposable.

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

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

1) \( N^0_{\Pi} = \mathcal{O}_A^{(0)} \).

2) For any \( k \geq 0 \), the class \( N^k_{\Pi} \) is defined by \( N^{k+1}_{\Pi} = \{\Pi(x_{k+1}, g, g') \mid g, g' \in N^k_{\Pi}\} \).

We denote by \( N_{\Pi} \) the class \( \bigcup_{k \geq 0} N^k_{\Pi} \) of the \( \Pi \)-normal forms.

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

Proposition 4. If \( f \) is a pivotal operation, then \( f \in N_{\Pi} \).

IV. CLONES OF PIVOTALLY DECOMPOSABLE OPERATIONS

We aim to give conditions on a pivotal operation \( f \) for \( \Lambda \) to be a clone. To this extent, we consider the following equations:

\[
 \Pi(x, 1, 0) = x, \quad (6)
\]

\[
 \Pi(\Pi(x, y, z), t, u) = \Pi(\Pi(x, y, t, u), \Pi(z, t, u)). \quad (7)
\]

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

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

Proof: For every \( i \in [n] \) let \( g'_i: A^{nm} \to A \) be the operation defined by \( g'_i(x) = g_i(x_i) \) where \( x_i = \)
We prove that $f(g_1', \ldots, g_n')$ is II-decomposable. For $x \in A^{nm}$, set
\begin{align*}
  e_k^0 &= f(0, g_2(x), \ldots, g_n(x)), \\
  e_k^1 &= f(1, g_2(x), \ldots, g_n(x)), \\
  a_k^0 &= g_1(0, x_2, \ldots, x_{nm}), \\
  a_k^1 &= g_1(1, x_2, \ldots, x_{nm}).
\end{align*}
We obtain by II-decomposability of $f$ that
\[ f(g_1(x), \ldots, g_n(x)) = f(g_1, e_k, e_k^0). \]

By iterating the pivotal decomposition expression (to each argument), we get the following equalities
\begin{align*}
  \Pi(g_1', x_i, e_k^0) &= \Pi(\Pi(x_1, a_k^0, e_k^0), c_k, e_k^0), \\
  &= \Pi(x_1, \Pi(a_k^0, c_k^0, e_k^0)), \\
  &= \Pi(x_1, f(g_1', \ldots, g_n')(x_i^1), f(g_1', \ldots, g_n')(x_i^0)),
\end{align*}
where the first equality is obtained by II-decomposability of $g_i$, the second one by equation (7) and the last one by II-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
\[ f(g_1', \ldots, g_n')(x) = \Pi(x, f(g_1', \ldots, g_n')(x_i^1), f(g_1', \ldots, g_n')(x_i^0)), \]
\[ f(g_1', \ldots, g_n')(x^i), \quad i \in [nm]. \tag{8} \]
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 $\Lambda_{II}$ must contain all projections.

**Lemma 6.** Let $\Pi$ be a pivotal operation. The following conditions are equivalent.

1) $\Pi$ satisfies equation (6).
2) $\Lambda_{II}$ contains all projections on $A$.
3) $\Lambda_{II}$ contains the unary projection $p_1^1$.

**Proof:** 1) $\implies$ 2): Let $n \geq 1$ and $k \in [n]$. For every $i \in [n]$ such that $i \neq k$ and for every $x \in A^n$,
\[ \Pi(x, p_k^0(x_i^1), p_k^0(x_i^0)) = \Pi(x, x_k, x_k) = x_k \]
where the last equality is obtained by (4). If $i = k$, then
\[ \Pi(x, p_k^0(x_i^1), p_k^0(x_i^0)) = \Pi(x_k, 1, 0) = x_k \]
where the last equality is obtained by (6). We conclude that $p_k^0 \in \Lambda_{II}$.

2) $\implies$ 3): Trivial.

3) $\implies$ 1): If $\Lambda_{II}$ 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 II 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 $\Pi$ is a pivotal operation that satisfies equation (7). Then $\Lambda_{II}$ is a clone if and only if $\Pi$ satisfies equation (6). In the latter case, $\Lambda_{II}$ is a clone that contains all constant operations.

In addition, if $\Lambda_{II}$ 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 $\Lambda_{II}$.

**Proposition 8.** Let $\Pi$ be a pivotal operation such that $\Lambda_{II}$ is a clone that contains $\Pi$. Then $\Lambda_{II}$ is the clone generated by $\Pi$ and the constant maps. In particular, $\Lambda_{II} = N_{II}$.

**Proof:** Let $C$ be the clone generated by $\Pi$ and the constant operations. We have to prove that $\Lambda_{II} = C$. The right to left inclusion is trivial since $\Lambda_{II}$ 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,
\[ \Lambda_{II} \subseteq N_{II} \subseteq C \subseteq \Lambda_{II}, \]
where the first inclusion is obtained by Proposition 4, the second inclusion follows from the definitions of $N_{II}$ 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 $\Pi$ and identify the corresponding Boolean clones, i.e., those of the form $\Lambda_{II}$.

**Example 9.** Let $\Pi$ 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):
\[ \Pi(x, 0, 0) = 0, \quad \Pi(x, 1, 1) = 1, \quad \Pi(x, 1, 0) = x. \tag{9} \]

Moreover, it is not difficult to check that the four possibilities for the unary section $\Pi(x, 0, 1)$ give rise to operations $\Pi$ that satisfy equation (7). Hence, there are four Boolean operations $\Pi_0, \ldots, \Pi_3$ that verify the conditions of Proposition 7. Each of these operations satisfies the equations given in (9) and are determined by
\begin{align*}
  \Pi_0(x, 0, 1) &= x, \\
  \Pi_1(x, 0, 1) &= x, \\
  \Pi_2(x, 0, 1) &= 0, \\
  \Pi_3(x, 0, 1) &= 1.
\end{align*}
Simple computations then show that we must have

\[
\Pi_0(x, y, z) = (x \land y) \lor (x \land z) \lor (y \land z), \\
\Pi_1(x, y, z) = (x \land y) \lor (x \lor z), \\
\Pi_2(x, y, z) = y \land (x \lor z), \\
\Pi_3(x, y, z) = z \lor (x \lor y).
\]

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

- \(\Lambda_{\Pi_0}\) is the clone of all monotone Boolean operations, since \(\Pi_0 = \text{mod}\);
- \(\Lambda_{\Pi_1}\) is the clone \(O_{\{0,1\}}\) of all Boolean operations, since \(\Pi_1\) is the pivotal operation used in Shannon decomposition;
- \(\Lambda_{\Pi_2}\) is the clone of all monotone Boolean operations, since \(\Pi_2(x, y, 0) = y \land x\) and \(\Pi_2(x, 1, z) = x \lor z\), and every composition of \(\Pi_2\) with projections or constants is monotone, and
- \(\Lambda_{\Pi_3}\) is the clone of all monotone Boolean operations (by a similar argument to that used for \(\Lambda_{\Pi_2}\)).

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

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 eludes 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-MTPHUL-12RDO2 of the University of Luxembourg.

REFERENCES