Polyabelian loops and Boolean completeness

François Lemieux, Cristopher Moore, Denis Thérien

Abstract. We consider the question of which loops are capable of expressing arbitrary Boolean functions through expressions of constants and variables. We call this property *Boolean completeness*. It is a generalization of functional completeness, and is intimately connected to the computational complexity of various questions about expressions, circuits, and equations defined over the loop. We say that a loop is *polyabelian* if it is an iterated affine quasidirect product of Abelian groups; polyabelianness coincides with solvability for groups, and lies properly between nilpotence and solvability for loops. Our main result is that a loop is Boolean-complete if and only if it is not polyabelian. Since groups are Boolean-complete if and only if they are not solvable, this shows that polyabelianness, for these purposes, is the appropriate generalization of solvability to loops.

Keywords: loops, quasigroups, functional closure, solvability, quasidirect products, computational complexity

Classification: 17A01, 17-08, 68Q15, 68W30, 03G05

1. Introduction

In the preface of his book, *The theory of groups* ([10]), H. Zassenhaus enumerates the main elements used to understand the algebraic structure of finite groups: *We are referring to the consistent application of the concept of homomorphic mapping. With such mapping one view the objects, so to speak, through the wrong end of a telescope. These mappings, applied to finite groups, give rise to the concepts of normal subgroup and of factor group. Repeated application of the process of diminution yields the composition series, whose factor groups are the finite simple groups. These are, accordingly, the bricks of which every finite group is built. How to build is indicated — in principle at least — by Schreier extension theory. The Jordan-Hölder-Schreier theorem tells us that the type and the number of bricks is independent of the diminution process. The determination of all finite simple groups is still the main unsolved problem.*

While most of the elements described above apply in the non-associative case as well, the theory we have now is far from being as consistent for loops as it is for groups. For example, there are at least two distinct ways of extending the concept of solvability to loops: one can apply homomorphic mapping to the loop itself or to its multiplication group. We say a loop is $\mathcal{M}$-*solvable* if its multiplication

Work supported by FCAR (Québec) and CRSNG (Canada).

group is solvable. For groups $\mathcal{M}$-solvability and solvability coincide, but in the non-associative case the $\mathcal{M}$-solvable loops are a proper subclass of the solvable ones. The same situation arises with central nilpotence and $\mathcal{M}$-nilpotence ([4], [23]).

For reasons rooted in computer science and physics, we have become interested in how various classes of groupoids can express Boolean functions. Say that a groupoid G is *Boolean-complete* if any Boolean function can be represented as an expression in G built from variables, constants and products in G. Two disjoint sets are chosen to represent true and false values, respectively. In the associative case, we have the following theorem ([12], [19]):

Theorem 1.1. *A group is Boolean-complete if and only if it is non-solvable.*

It is natural to try to generalize this to the non-associative case, and ask which loops and quasigroups are Boolean-complete. It turns out that neither the traditional notion of solvability, nor solvability of the multiplication group, is the right criterion. To give the right characterization we need to define a new kind of product that we call *affine quasidirect*. Iterated affine quasidirect products of Abelian groups define what we call *polyabelian* loops. For groups, polyabelianness coincides with solvability, but in the non-associative case polyabelianness is a proper subclass of solvability and incomparable with $\mathcal{M}$-solvability. Our main result is the following:

Theorem 1.2. *A finite loop is Boolean-complete if and only if it is non-polyabelian.*

Our motivation for this comes from the fact that if a groupoid can express arbitrary Boolean functions, then various natural questions about it have a high computational complexity. Evaluating circuits and expressions in such a groupoid are **P**-complete and $\mathbf{NC}^1$-complete respectively ([15]), and solving equations of constants and variables in non-solvable groups is **NP**-complete ([9]).

On the other hand, if a groupoid lacks this expressive power, all these problems may be significantly easier. Languages recognized by solvable groups have simple combinatorial descriptions ([18], [21]), and circuits over them can be evaluated quickly in parallel ([2], [3]). Similarly, cellular automata defined with polyabelian operations can be predicted much more quickly than by explicit simulation ([14]). Thus the algebraic properties of a groupoid are intimately linked to its computational complexity.

This paper is organized as follows. Section 2 gives an introduction to the algebraic terms and concepts we will use. In Section 3 we define the functional closure of a groupoid, and show that simple non-Abelian loops are functionally complete. In Section 4 we define Boolean-completeness and show that the set of non-Boolean-complete groupoids forms a pseudovariety. In Section 5 we define the affine quasidirect product and polyabelian loops, and compare polyabelianness to solvability and nilpotence. Sections 6 and 7 are devoted to the proof that polyabelianness corresponds precisely to non-Boolean-completeness for loops.

More details, and an analysis of how these properties and others affect the computational complexity of various problems on quasigroups and loops, are given in [15]. We recommend [16] for an introduction to computation theory, including **P**, $\mathbf{NC}^1$, and **NP**-completeness.

2. Definitions

For the theory of quasigroups and loops, we refer the reader to [1], [4], [5], [8], [17]. We will use the following standard terms.

A *groupoid* $(G, \cdot)$ is a binary operation $f : G \times G \to G$, written $f(a, b) = a \cdot b$ or simply ab. The *order* of a groupoid is the number of elements in G, written $|G|$. Throughout the paper, we will assume that our groupoids are finite.

A *quasigroup* is a groupoid whose multiplication table is a *Latin square*, in which each symbol occurs once in each row and each column. Equivalently, for every a, b there are unique elements a/b and $a\backslash b$ such that $(a/b) \cdot b = a$ and $a \cdot (a\backslash b) = b$; thus the left (right) *cancellation property* holds, that $bc = bd$ (resp. $cd = bd$) implies $c = d$.

An *identity* is an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all a. A *loop* is a quasigroup with an identity.

In a loop, the *left* (*right*) *inverse* of an element a is $a^\lambda = 1/a$ (resp. $a^\rho = a\backslash 1$) so that $a^\lambda \cdot a = 1$ (resp. $a \cdot a^\rho = 1$). A loop has the left (right) *inverse property* if $a\backslash b = a^\lambda \cdot b$ (resp. $b/a = b \cdot a^\rho$). If a loop has both the left and right inverse property, it has the *inverse property* and $a^\lambda = a^\rho$, in which case we will refer to them both as a^{-1}.

A groupoid is *associative* if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c. A *semigroup* is an associative groupoid, and a *monoid* is a semigroup with identity. A *group* is an associative quasigroup; groups have inverses and an identity.

Two elements a, b *commute* if $a \cdot b = b \cdot a$. A groupoid is *commutative* if all pairs of elements commute. Commutative groups are also called *Abelian*. We will use $+$ instead of $\cdot$ for products in an Abelian group, and call the identity 0 instead of 1.

In a group, the *order* of an element a is the smallest $p > 0$ such that $a^p = 1$ (or $pa = 0$ in an Abelian group).

A *homomorphism* is a function ϕ from one groupoid $(A, \cdot)$ to another $(B, \star)$ such that $\phi(a \cdot b) = \phi(a) \star \phi(b)$. An *isomorphism* is a one-to-one and onto homomorphism; we will write $A \cong B$ if A and B are isomorphic. Homomorphisms and isomorphisms from a groupoid into itself are called *endomorphisms* and *automorphisms* respectively; the automorphisms of a groupoid A form a group $\mathrm{Aut}(A)$.

A *subgroupoid* (*subquasigroup, subloop*, etc.) of G is a subset $H \subseteq G$ which is closed under multiplication, i.e. $b_1 \cdot b_2 \in H$ for all $b_1, b_2 \in H$. The subgroupoid generated by a set S is written $\langle S \rangle$.

The *left* (*right*) *cosets* of a subloop $H \subseteq G$ are the sets $aH = \{ah \,|\, h \in H\}$ and $Ha = \{ha \,|\, h \in H\}$ for each $a \in G$. A subloop H is *normal* if the following hold for all $a, b \in G$:

$$aH = Ha, \quad a(bH) = (ab)H, \quad \text{and} \quad (aH)b = a(Hb)$$

Then the set of cosets of H is the *quotient loop* or *factor* G/H; it has identity $1H = H$, and is the image of G under the homomorphism $\phi(a) = aH$. Conversely, any homomorphic image $\phi(G)$ of a loop is a quotient $G/(\ker\phi)$ where the *kernel* $\ker\phi = \{g \in G \mid \phi(g) = 1\}$ is a normal subloop of G.

A subloop of G is *proper* if it is neither $\{1\}$ nor all of G. A *minimal* normal subloop of G is one which does not properly contain any proper normal subloops of G, and which is not $\{1\}$. A *simple* loop is one with no proper normal subloops.

The *commutator* of two elements in a loop is $[a, b] = ab \,/\, ba$, i.e. the unique element such that $ab = [a, b](ba)$. The *associator* of three elements is $[a, b, c] = (ab)c \,/\, a(bc)$, i.e. the unique element such that $(ab)c = [a, b, c](a(bc))$. The subloop generated by all possible commutators and associators in a loop G is called the *commutator-associator subloop* or *derived subloop* G'. It is normal, and it is the smallest subloop such that the quotient G/G' is an Abelian group.

A loop G is *solvable* if its *derived series* $G = G_0 \supset G_1 \supset \cdots$, where $G_{i+1} = G'_i$ for all i, ends in $G_k = \{1\}$ after a finite number of steps. A groupoid is solvable if it has no subsets which are non-solvable loops under the groupoid operation.

A *divisor* of a groupoid is a factor of a subgroupoid. Any non-solvable loop has a simple non-Abelian divisor. A divisor is not necessarily a subgroupoid, even for groups.

The *center* of a loop is the set of elements that associate and commute with everything, $Z(G) = \{c \mid cx = xc,\ c(xy) = (xc)y = x(yc) \text{ for all } x, y \in G\}$. It is a normal subloop of G, and is always an Abelian group.

The *upper central series* of a loop is $\{1\} = Z_0 \subset Z_1 \subset \cdots$ where Z_{i+1}/Z_i is the center of G/Z_i. A loop is *nilpotent* (of class k) if $Z_k = G$ for some k. Inductively, G is nilpotent if it has a nontrivial center $Z(G)$, and $G \,/\, Z(G)$ has a non-trivial center, and so on until we get an Abelian group H for which $Z(H) = H$. The nilpotent loops are a proper subclass of the solvable ones.

A *pseudovariety* is a class of groupoids V such that subgroupoids, factors, and finite direct products of groupoids in V are also in V. Solvable and nilpotent loops both form pseudovarieties.

In a quasigroup Q, we can define left and right multiplication as functions $L_a(b) = a \cdot b$ and $R_a(b) = b \cdot a$. These are permutations on Q (the rows and columns of the multiplication table), and the *multiplication group* $\mathcal{M}(Q)$ is the group of permutations they generate. More generally, any groupoid has a *multiplication semigroup* generated by the L_a and R_a, which are not necessarily one-to-one functions on Q. If we have more than one operation we will refer to $L_a^{\odot}$, $\mathcal{M}(Q, \odot)$, and so on. The elements of $\mathcal{M}(Q)$ that fix the identity are called *inner mappings*, and they form a subgroup $\mathcal{J}(Q) \subseteq \mathcal{M}(Q)$.

Finally, we refer to the identity function $\mathbf{1}(x) = x$, the *cyclic group* $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ with addition mod p, and the groups S_n and A_n of permutations and even permutations respectively on n elements.

3. The functional closure of a groupoid

Definition 3.1. *The* functional closure *of a groupoid G is the smallest set $\mathcal{P}(G)$ of functions $\phi : G^k \to G$ on an arbitrary number of variables $x_1, \dots, x_k$ containing the following:*

- (*constants*) *a for all $a \in G$;*
- (*projections*) *x_i for all i;*
- (*products*) *$\phi_1 \cdot \phi_2$ for all $\phi_1, \phi_2 \in \mathcal{P}(G)$.*

A function in $\mathcal{P}(G)$ is said to be *expressible in G* or simply *expressible* when G is implicit. We will refer to the set of expressible functions on k variables as $\mathcal{P}^k(G)$: for instance, $\mathcal{P}^1(G)$ contains the multiplication semigroup $\mathcal{M}(G)$, as well as functions like $\phi(x) = x^2$. The functional closure is also an example of a *clone* ([22]).

We generalize the definition of the inner mapping group of a loop G as follows. Let U be the set of functions ϕ in $\mathcal{P}^1(G)$ such that $\phi(1) = 1$. Hence, for an element $x \in G$, $U(x) = \{\phi(x) \mid \phi \in U\}$ is the set of y's that we can send x to, while fixing 1. This set has the following property.

Lemma 3.2. *Let G be a loop and let $x \in G$, and let N be a subloop of G. Then N is normal if and only if $U(N) = N$, and $U(x)$ is the smallest normal subloop of G that contains x.*

Proof: To show that $U(N) = N$ for any normal subloop N, note that for any $\phi \in \mathcal{P}^1(G)$ and any $n \in N$, $\phi(n)/\phi(1) \in N$, and if $\phi \in U$ then $\phi(1) = 1$ so $\phi(n) \in N$. Thus $U(N) \subseteq N$, and clearly $N \subseteq U(N)$ since U includes the identity function.

To prove the second statement, it is shown in [5, p. 63] that $K = \langle \mathcal{J}(x) \rangle$ is the smallest normal subloop that contains x. Since U contains the inner mappings, $K \subseteq U(x)$, and since $x \in K$, $U(x) \subseteq U(K) = K$. □

Given a loop G, it is natural to ask if $\mathcal{P}(G)$ contains all functions $G^n \to G$ ($n \geq 0$). This property is called *functional completeness*, and obviously includes Boolean-completeness as a consequence. We can show that if G is a simple loop then G is functionally complete if and only if it is not an Abelian group; if it is Abelian, it can only express affine functions, as we show below. Before giving the proof of the other direction, we need some lemmas.

Lemma 3.3. *If G is a simple loop, then for any $x, y \in G$ ($x \neq 1$), there is a function $\pi_{x \to y}$ in $\mathcal{P}^1(G)$ that sends x to y and keeps the identity fixed.*

Proof: If G is simple and $x \neq 1$, then $U(x) = G$ by Lemma 3.2. The result then follows from the definition of U. □

Lemma 3.4. *If Q is a finite quasigroup, the divisions a/b and $a \backslash b$ are in $\mathcal{P}^2(Q)$ as functions of a and b. Therefore, when Q is a loop, functions that yield the commutator, associator, and left and right inverses are in $\mathcal{P}$ as well.*

Proof: Recall the definition of L_a and R_a above. If Q is a quasigroup of order n, L_a and R_a are permutations on its elements, and $L_a^{n!}$ and $R_a^{n!}$ are the identity $\mathbf{1}$. Then $aL_a^{n!-1}(b) = L_a^{n!}(b) = b$, so

$$a\backslash b = L_a^{n!-1}(b) = \underbrace{a(a(\cdots(a}_{n!-1\,\text{times}} \cdot b)))$$

is in $\mathcal{P}(Q)$. Similarly for a/b; then by composition we can define $[a,b] = ab\,/\,ba$, $[a,b,c] = (ab)c\,/\,a(bc)$, $a^\lambda = 1/a$ and $a^\rho = a\backslash 1$. □

Then we have the following ([6], [11]):

Theorem 3.5. *If G is a finite simple loop that is not an Abelian group then G is functionally complete.*

Proof: Let $g_1, g_2 \in G$ and $g_1 \neq 1$. By Lemma 3.3, there exists a function $\pi_{g_1\to g_2}(x)$ that fixes the identity and maps g_1 to g_2 and that is expressible in G.

Because it is simple and not an Abelian group, G is equal to its commutator-associator subloop. Thus, each element $h \in G$ can be written (assuming an implicit parenthesization) as $h = \prod_{i=1}^r \delta_i$, where each δ_i is a commutator $[g_i, h_i]$ or an associator $[f_i, g_i, h_i]$. By Lemma 3.4, the function

$$\Delta_i(x,y) = \begin{cases} [x,y] & \text{if } \delta_i \text{ is a commutator} \\ [f_i, x, y] & \text{if } \delta_i \text{ is an associator} \end{cases}$$

can be expressed in G, for all $1 \leq i \leq r$, and by Lemma 3.3 so can

$$w_{2,h} = \prod_{i=1}^r \Delta_i(\pi_{h\to g_i}(x), \pi_{h\to h_i}(y)).$$

Note that $w_{2,h}(h,h) = h$ and $w_{2,h}(g,1) = w_{2,h}(1,g) = 1$ for all $g \in G$.

By nesting these, we can express the function

$$w_{m+1,h} = w_{2,h}(w_{m,h}, x_{m+1})$$

for all $m \geq 2$, such that $w_{m,h}(h,\ldots,h) = h$ and $w_{m,h}(g_1,\ldots,g_m) = 1$ if $g_i = 1$ for any i.

Then let $h,k \in G$, with $h \neq 1$. We can express

$$z_{k,h} = w_{m,h}(\pi_{g_1k\to h}(g_1x), \ldots, \pi_{g_mk\to h}(g_mx))$$

where $m = |G|-1$ and $g_1,\ldots,g_m$ range over all the elements of G except for k's left inverse k^λ. Then $z_{k,h}(k) = h$ and $z_{k,h}(g) = 1$, for $g \neq k$.

Finally, let $\alpha = (c_1,\ldots,c_n) \in G^n$ and let

$$v_{\alpha,h} = w_{n,h}(z_{c_1,h}(x_1), \ldots, z_{c_n,h}(x_n)).$$

Then, $v_{\alpha,h}(\alpha) = h$ and $v_{\alpha,h}(\beta) = 1$ for any $\beta \neq \alpha$. Hence, we can express any function $f : G^n \to G$ using the expression

$$f(\alpha) = \prod_{f(\alpha)\neq 1} v_{\alpha,f(\alpha)}.$$

Note that any parenthesization can be used since at most one term in the product is different from the identity. □

We note that functional completeness was shown for non-Abelian simple groups by Maurer and Rhodes [12] and, more generally, for non-affine simple quasigroups by McKenzie [13].

4. Boolean-complete groupoids

We have shown that simple non-Abelian loops are characterized by their ability to express arbitrary functions. The rest of the paper will be devoted to characterizing those loops that can express all Boolean functions. We must first define what we mean by *expressing* a Boolean function.

Definition 4.1. *Let G be a groupoid, and let $T, F \subset G$ be two disjoint non-empty subsets of G. Define the mapping $\beta : T \cup F \to \{\text{TRUE}, \text{FALSE}\}$ with $\beta(g) = \text{TRUE}$ if $g \in T$ and $\beta(g) = \text{FALSE}$ is $g \in F$. We say that a Boolean function $f(x_1, \dots, x_n)$ is* expressed *by an expression $\phi \in \mathcal{P}^n(G)$, if for any $g_1, \dots, g_n \in T \cup F$, we have $f(\beta(g_1), \dots, \beta(g_n)) = \beta(\phi(g_1, \dots, g_n))$.*

Note that we only ask that the expression work on 'Boolean inputs,' and make no demands on it if some g_i is not in $T \cup F$.

Definition 4.2. *A groupoid G is Boolean-complete if there exist two disjoint subsets $T, F \subset G$ such that any Boolean function can be expressed by some $\phi \in \mathcal{P}(G)$ using elements in T to express* TRUE *and elements in F to express* FALSE*. If moreover F and T are singletons, then we say that G is* strongly *Boolean-complete.*

Lemma 4.3. *The set of non-Boolean-complete finite groupoids forms a pseudovariety. Therefore, if a divisor of a groupoid G is Boolean-complete, then G is also.*

Proof: If a subgroupoid $H \subset G$ is Boolean-complete, then G is also since $\mathcal{P}(H) \subset \mathcal{P}(G)$. If a factor $\phi(G)$ is Boolean-complete with subsets T and F, simply let T' and F' in G be the inverse images $\phi^{-1}(T)$ and $\phi^{-1}(F)$. This shows that non-Boolean-complete groupoids are closed under division. It remains to prove that finite direct products of non-Boolean-complete groupoids are non-Boolean-complete.

Let G and H be two non-Boolean-complete groupoids and suppose that $G \times H$ is Boolean-complete. Let T and F be two subsets of $G \times H$ containing true and false values. Since $G \times H$ is Boolean-complete but G and H are not, there must exist elements $a, b \in G$ and $c, d \in H$ such that either $(a, c) \in T$ and $(a, d) \in F$ or $(a, c) \in T$ and $(b, c) \in F$. Assume the first case, the other one being symmetric.

Let $f(x, y) \in \mathcal{P}^2(G \times H)$ express the function that computes NAND (x, y). By fixing the first component of x and y to a, we get that the first component of $f(x, y)$ is fixed to some $a_0 \in G$. Hence, we only have to look at the second component to determine if f evaluates to TRUE or FALSE. Observe that we do not have a contradiction yet since we can have a situation where $(a, c) \in T$ and $(a_0, c) \in F$.

Let $g_1(x, y) = f(x, y)$ and, for any $k \geq 1$, define

$$g_{k+1}(x, y) = g_k(f(f(x, x), f(x, x)), f(f(y, y), f(y, y))).$$

Then, for any $k \geq 1$, $g_k(x, y)$ computes NAND (x, y), since $f(f(x, x), f(x, x))$ has the same truth value as x.

If the first component of x and y is a_0, then we can define a_i as the first component of $g_i(x, y)$. Since G is finite, there must exist two integers $0 \leq i < j$ such that $a_i = a_j$. Hence, if we use only true and false values whose first component is a_i, then the first component of g_{j-i} is also a_i. Let $S = \{a_i\} \times H$. We have that the sets $T' = S \cap T$ and $F' = S \cap F$ are disjoint, and so H is Boolean-complete, a contradiction. □

The main motivation for our work comes from the following result due to Straubing [19], which also follows from the result of Maurer and Rhodes [12].

Theorem 4.4. *A finite group is Boolean-complete if and only if it is non-solvable.*

In one way, this theorem can be extended to loops.

Lemma 4.5. *A non-solvable finite loop is Boolean-complete.*

Proof: This is a direct consequence of Theorem 3.5 and the fact that any non-solvable loop is divided by a simple loop that is not Abelian.

□

However, a loop can be solvable and still be Boolean-complete.

Let $(G, \cdot)$ be

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	6	7	8	5
3	3	4	1	2	7	8	5	6
4	4	1	2	3	8	5	6	7
5	5	6	7	8	1	3	2	4
6	6	7	8	5	3	2	4	1
7	7	8	5	6	2	4	1	3
8	8	5	6	7	4	1	3	2

Here G' is the normal subloop $\{1,2,3,4\} \cong Z_4$. The lower right-hand block is the multiplication table of a Boolean-complete quasigroup $Q = (\{1,2,3,4\}, \star)$. To see this, let FALSE $= 1$ and TRUE $= 2$ and write $a \wedge b = (a \star b)^2$ and $\neg a = 3 \star (1 \star a)$. Since the product in Q can be expressed in $\mathcal{P}(G)$ as $a \star b = (5 \cdot a) \cdot (5 \cdot b)$, it follows that G is Boolean-complete. We note that this loop has a solvable multiplication group, and slightly larger examples exist with the inverse property ([15]).

As can be seen in this example, solvability does not constrain the lower right-hand block in any way. Thus a stricter property is needed to draw the line between Boolean-completeness and -incompleteness.

5. Polyabelian groupoids

The *direct product* of two groupoids $A \times B$ is the set of pairs (a,b) with pairwise multiplication, $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2, b_1b_2)$. Consider the following generalization:

Definition 5.1. *A quasidirect product* ([7]) *of two groupoids A and B is the set of pairs (a,b), under an operation of the form*

$$(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2,\ b_1 \odot_{a_1,a_2} b_2)$$

where each a_1, a_2 defines a local operation $\odot_{a_1,a_2}$ on B. We will denote such a product $A \otimes B$.

Observe that the quasidirect product, as defined above, makes no use of the product in B and so, it makes sense to talk of the quasidirect product of A and S even when S is a set with no underlying operation. In order to take into account the algebraic structure of B, we have to restrict the local operations.

If the local operations are of the form

$$b_1 \odot_{a_1,a_2} b_2 = f_{a_1,a_2}(b_1) \cdot g_{a_1,a_2}(b_2)$$

where f and g are functions from B to B, we will call them separable. *Furthermore, if B is an Abelian group and the $\odot$'s are of the form*

$$b_1 \odot_{a_1,a_2} b_2 = f_{a_1,a_2}(b_1) + g_{a_1,a_2}(b_2) + h_{a_1,a_2}$$

where f and g are endomorphisms on B and h is an element of B, depending arbitrarily on a_1 and a_2, then we will call them affine. *We will call a quasidirect product $A \otimes B$ separable or affine on B if all its local operations are.*

Lemma 5.2. 1. *If a groupoid G is a quasidirect product $A \otimes B$, then $A \cong G/B$ is a factor of G.*

2. *If G is a quasigroup, then A and B are quasigroups and all the $\odot$'s are quasigroup operations on B.*
3. *If G is a quasigroup and is affine on B, then all the f's and g's are automorphisms on B.*

4. *If G is a loop, then A is a loop and $B \cong \{1\} \times B$ is a normal subloop (where 1 is the identity of A).*
5. *If G is a loop affine on $(B, +)$, then for all $a \in A$ we have $f_{a,1} = g_{1,a} = \mathbf{1}$ and $h_{a,1} = h_{1,a} = 0$ (where 1 and 0 are the identities of A and B respectively). Thus $b_1 \odot_{1,1} b_2 = b_1 + b_2$ for $b_1, b_2 \in B$, and $+$ and $\cdot$ coincide in B.*

Proof: For the most part, we leave this to the reader. For (5), the identity of G must be $(1, b)$ where 1 is the identity of A and b is some element of B. Without loss of generality, we can assume that $b = 0$, since otherwise we can redefine the operation $+$ by adding a constant. Then $(a, b) \cdot (1, 0) = (a, f_{a,1}(b) + h_{a,1})$ and $(1, 0) \cdot (a, b) = (a, g_{1,a}(b) + h_{1,a})$. Setting the B component of both of these equal to b and using the fact that f and g are endomorphisms yields $f_{a,1} = g_{1,a} = \mathbf{1}$ and $h_{a,1} = h_{1,a} = 0$. □

The quasidirect product is a rather general way of extending to a loop from a normal subloop:

Lemma 5.3. *If a loop G has a normal subloop N, then G is isomorphic to a quasidirect product $(G/N) \otimes N$. Furthermore, all the local operations are expressible in $\mathcal{P}(G)$; if the local operations are separable, then the f's and g's are expressible; and if N is Abelian and G is affine on N, the f's, g's and h's are expressible.*

Proof: The first statement is standard and is proved in [1]. For the rest, choose a set T with one element in each coset of N (such a set is often called a *transversal*), and define an operation $\bullet$ on T where $t_1 \bullet t_2$ is the element of T in the same coset as $t_1 \cdot t_2$. Then clearly $T \cong G/N$.

Every element can be uniquely written $g = tn$ where $t \in T$ and $n \in N$. Then

$$(t_1 n_1) \cdot (t_2 n_2) = (t_1 \bullet t_2) \cdot (n_1 \odot_{t_1,t_2} n_2)$$

where

$$n_1 \odot_{t_1,t_2} n_2 = (t_1 \bullet t_2) \setminus ((t_1 n_1) \cdot (t_2 n_2))$$

which is in N since N is normal. Thus G is a quasidirect product $T \otimes N$, and all the local operations $\odot$ are in $\mathcal{P}(G)$.

If the $\odot$'s are separable, then

$$f_{t_1,t_2}(n) = n \odot_{t_1,t_2} g^{-1}_{t_1,t_2}(1)$$

where 1 is the identity of N. Thus f_{t_1,t_2} is expressible for each t_1 and t_2, and similarly for g_{t_1,t_2}.

If N is an Abelian group and G is affine on N, then

$$\begin{aligned} f_{a_1,a_2}(n) &= (n \odot_{a_1,a_2} 0) - (0 \odot_{a_1,a_2} 0) \\ g_{a_1,a_2}(n) &= (0 \odot_{a_1,a_2} n) - (0 \odot_{a_1,a_2} 0) \\ h_{a_1,a_2} &= (0 \odot_{a_1,a_2} 0) \end{aligned}$$

where we abuse notation by writing $+$ and 0, instead of $\cdot$ and 1, for products in N. Finally, $(N,+)$ is in $\mathcal{P}(G)$ since $a \odot_{0,0} b = a + b$ by Lemma 5.2. $\square$

Then define the following class of loops:

Definition 5.4. *A loop is* polyabelian *if it is an iterated quasidirect product of Abelian groups A_i:*

$$((A_0 \otimes A_1) \otimes A_2) \otimes \cdots \otimes A_k$$

where all the products are affine.

It is easy to show that subloops, factors, and finite direct products of polyabelian loops are polyabelian, so this class forms a pseudovariety. The next few lemmas show inclusions between the polyabelian loops and some common classes of groups and loops.

Lemma 5.5. *Polyabelian loops are solvable.*

Proof: Let $H_i = (A_i \otimes A_{i+1}) \otimes \cdots \otimes A_k$ with $H_0 = G$. Then the reader can show that all the H_i are normal subloops of G, and $H_i/H_{i+1} = A_i$ is Abelian. Therefore, $H_i' \subseteq H_{i+1}$ and the derived series ends after at most k steps. $\square$

The converse is not true for loops in general (for instance, the solvable Boolean-complete loops above, since the local operations in their lower right-hand blocks are not affine) but it is true for groups:

Lemma 5.6. *Solvable groups are polyabelian.*

Proof: Any solvable group G has a normal subgroup N which is Abelian, namely the last non-trivial group in its derived series such that $N' = \{1\}$. Since factors of solvable groups are solvable, G/N is solvable if G is, so we can assume by induction on smaller groups that G/N is polyabelian. Now express G as a quasidirect product of G/N and N using Lemma 5.3, with the local operation

$$\begin{aligned} n_1 \odot_{t_1,t_2} n_2 &= (t_1 \bullet t_2)^{-1} t_1 n_1 t_2 n_2 \\ &= ((t_1 \bullet t_2)^{-1} t_1 t_2) + (t_2^{-1} n_1 t_2) + n_2 \end{aligned}$$

where we use $+$ for products within N. Thus G is affine on N where

$$\begin{aligned} f_{t_1,t_2}(n) &= t_2^{-1} n t_2 \\ g_{t_1,t_2}(n) &= n \\ h_{t_1,t_2} &= (t_1 \bullet t_2)^{-1} t_1 t_2. \end{aligned}$$

Then G/N has an Abelian normal subgroup, and so on; by induction G is polyabelian.

(If $t_1 \bullet t_2 = t_1 t_2$ so that $h = 0$, then T is a subgroup of G isomorphic to G/N, the quasidirect product reduces to the *semidirect product* on groups, and G is a *split extension* of N by T ([20]). In [14] we defined polyabelianness with semidirect products only, in which case any solvable group is a subgroup of a polyabelian group by iterating wreath products.) $\square$

Lemma 5.7. *Nilpotent loops are polyabelian.*

PROOF: Let G be a nilpotent loop with center $Z(G)$. Then the local operation in $G/Z(G) \otimes Z(G)$ is

$$n_1 \odot_{t_1,t_2} n_2 = ((t_1 \bullet t_2)\backslash t_1 t_2) + n_1 + n_2$$

since n_1 and n_2 associate and commute with everything. So G is affine on $Z(G)$ with $f = g = \mathbf{1}$ and $h = (t_1 \bullet t_2)\backslash t_1 t_2$. Then $G/Z(G)$ has a non-trivial center, and so on; by induction G is polyabelian. □

Thus polyabelianness coincides with solvability for groups, and lies properly between nilpotence and solvability for loops. In [15] we also show that polyabelianness and $\mathcal{M}$-solvability are incomparable. In the final two sections, we will show that, for purposes of Boolean-completeness, polyabelianness is the correct generalization of solvability in the non-associative case: that is, a loop is Boolean-complete if and only if it is not polyabelian.

6. Polyabelian groupoids are not Boolean-complete

In one direction, we can prove this for all groupoids. We show that polyabelian groupoids cannot express the AND function. First, two lemmas from [22]:

Definition 6.1. *Let A be an Abelian group. A function $\phi : A^n \to A$ is* affine *if there exist endomorphisms $f_1, \ldots, f_n$ and an element h such that $\phi(x_1, \ldots, x_n) = \sum_i f_i(x_i) + h$.*

Recall the definition of the closure $\mathcal{P}(A)$ from Section 3. The closure of an Abelian group consists only of affine functions:

Lemma 6.2. *If A is an Abelian group, then any function in $\mathcal{P}(A)$ is affine, and the affine functions are closed under composition.*

PROOF: This is obvious: $\phi(a, b) = a + b$ is affine, and if ϕ_1 and ϕ_2 are both affine, then so are $\phi_1 + \phi_2$ and $\phi_1 \circ \phi_2$. □

Lemma 6.3. *If $\phi(a, b)$ is an affine function, then $\phi(a_1, b_1) = \phi(a_1, b_2)$ if and only if $\phi(a_2, b_1) = \phi(a_2, b_2)$ for any four elements a_1, a_2, b_1, b_2.*

PROOF: We can write $\phi(a, b) = f(a) + g(b) + h$ where f and g are endomorphisms. Then $\phi(a_1, b_1) = \phi(a_1, b_2)$ implies that $g(b_1) = g(b_2)$, which in turn implies that $\phi(a_2, b_1) = \phi(a_2, b_2)$ for any a_2. □

Theorem 6.4. *Polyabelian finite groupoids cannot express the* AND *function, and so are not Boolean-complete.*

PROOF: If G is Boolean-complete, then it can express an n-ary AND function for any n, i.e. $\phi(a_1, a_2, \ldots, a_n) \in T$ if and only if $a_i \in T$ for all i (assuming that $a_i \in T \cup F$ for all i). We will show that this is impossible for n sufficiently large.

If $G = (A_0 \otimes A_1) \otimes \cdots \otimes A_k$, then any $x \in G$ has a unique vector of components $(x_0, x_1, \ldots, x_k)$ where $x_i \in A_i$ for all i. Call x_i the *A_i-component* of x. We will proceed through the A_i by induction, showing that there are elements of T and F matching on all their components, and therefore equal; then T and F are not disjoint, a contradiction.

Since A is finite, it has a finite number $k \leq |A|^{|A|}$ of endomorphisms[1]. Therefore, if $\psi(a_1, \ldots, a_n) = \sum_i g_i(a_i) + h$ is an n-ary affine function on an Abelian group A of order p, and if n is greater than $(p-1)k$, then at least p of the variables have the same $g_i = g$. Then if these p variables are all equal, they contribute nothing to ψ since pg=0. In particular, if the $n-p$ other variables are true, ψ has the same value whether these p variables are true or false. As shorthand for this, we write $\psi(f^p t^{n-p}) = \psi(t^n)$. Thus ψ cannot be an AND function.

So assume that there is an n-ary AND function ϕ in $\mathcal{P}(G)$. To start the induction, since A_0 is a factor of G by Lemma 5.2, ϕ's A_0-component ϕ_0 is a function of the A_0-components of the a_i, expressible in $\mathcal{P}(A_0)$ and therefore affine by Lemma 6.2. Choose $t \in T$ and $f \in F$; then for n sufficiently large $\phi_0(f^p t^{n-p}) = \phi_0(t^n)$. Let $f_0 = \phi(f^p t^{n-p})$ and $t_0 = \phi(t^n)$; then $t_0 \in T$ and $f_0 \in F$ by hypothesis, and they have the same A_0-component.

Now suppose that $t_m \in T$ and $f_m \in F$ agree on their A_j-components for all $j \leq m$. Think of ϕ as a tree where each node corresponds to a subexpression equal to the product of its daughters according to some local operation. Then the A_j-components at each node depend only on the $A_{j'}$-components of its two subexpressions for $j' \leq j$ (since $A_0 \otimes \cdots \otimes A_j$ is a factor of G for all j) and t_m and f_m have the same A_j-component for all $j \leq m$, so inductively ϕ and each of its subexpressions have constant A_j-components for $j \leq m$ when restricted to inputs in $\{t_m, f_m\}$.

Furthermore, each node applies an affine local operation on A_{m+1}, and which one it applies depends only on its subexpressions' A_j-components for $j \leq m$. Since these are constant in this restriction, each node always applies the same local operation; the composition of all of these make ϕ_{m+1} an affine function on the A_{m+1}-components of its inputs.

Then if we let $f_{m+1} = \phi(f_m^p t_m^{n-p}) \in F$ and $t_{m+1} = \phi(t_m^n) \in T$, we see that f_{m+1} and t_{m+1} agree on their A_j-components for all $j \leq m+1$. After k steps of this induction, t_k and f_k agree on all their components, and so are equal; so T and F are not disjoint.

Thus, by contradiction, G cannot express an n-ary AND and is not Boolean-complete.

□

[1] If $A = \mathbb{Z}_p^m$, for instance, $k = p^{m^2}$ since the endomorphisms of A are $m \times m$ matrices with entries in $\mathbb{Z}_p$.

7. Non-polyabelian loops are Boolean-complete

Theorem 4.4 and Lemma 5.6 show that non-polyabelianness implies Boolean-completeness in the case of groups; we will now show this for loops.

Theorem 7.1. *Non-polyabelian loops are Boolean-complete.*

PROOF: Let H be the smallest non-polyabelian divisor of G. We will show that H (which is also a loop) is strongly Boolean-complete.

Assume without loss of generality that H is solvable, since we have already treated the non-solvable case with Lemma 4.5. Then H has a normal subloop K which is an Abelian group, namely the last non-trivial subloop in its derived series with $K' = \{1\}$. Let N be a minimal normal subloop of H contained in K; then N is also Abelian. Note that N can be smaller than K. We know that H is not affine on N; otherwise H/N would be a smaller non-polyabelian divisor of G.

Recall the definition of $U(x)$ from Section 3. Since N is minimal, $U(n) \supset N$ for any $n \in N$; otherwise $U(n) \cap N$ would be a smaller normal subloop since the intersection of normal subloops is normal. So for any $n_1, n_2 \in N$, there exists a function $\pi_{n_1 \to n_2} \in \mathcal{P}(H)$ that sends n_1 to n_2 and preserves the identity.

Since H is not affine on N, some local operation $\odot$ is either not separable or not affine. Define the *separator*

$$K_\odot(n_1, n_2) = (n_1 \odot n_2) - (n_1 \odot 0) - (0 \odot n_2) + (0 \odot 0)$$

where we use $+$ and $-$ for products in N. If $K_\odot = 0$, then $n_1 \odot n_2 = f(n_1) + g(n_2)$ where $f(n_1) = (n_1 \odot 0)$ and $g(n_2) = (0 \odot n_2) - (0 \odot 0)$, so $\odot$ is separable. Conversely, if $\odot$ is separable, then all the terms cancel and $K_\odot = 0$. Therefore, if $\odot$ is not separable, then $K_\odot(n_1, n_2) = k \neq 0$ for some n_1, n_2; however, $K_\odot(0, n) = K_\odot(n, 0) = 0$ for any n. But this gives us our AND gate: let FALSE $= 0$ and choose TRUE $= t \in N$, and let

$$a \wedge b = \pi_{k \to t}\big(K_\odot(\pi_{t \to n_1}(a), \pi_{t \to n_2}(b))\big).$$

If all the local operations are separable, then one must not be affine: that is, some f or g is not a endomorphism of N. Let $f(n) = (n \odot 0) - (0 \odot 0)$ as in Lemma 5.3, and define the *affinator*

$$L_f(n_1, n_2) = f(n_1 + n_2) - f(n_1) - f(n_2)$$

If f is not a endomorphism, then $L_f(n_1, n_2) = k \neq 0$ for some n_1, n_2; but $L_f(n, 0) = L_f(0, n) = 0$ for all n, so

$$a \wedge b = \pi_{k \to t}\big(L_f(\pi_{t \to n_1}(a), \pi_{t \to n_2}(b))\big)$$

is an AND gate. Similarly if some g is not a endomorphism.

Thus, any nonlinearity in the local operations can be used to construct an AND gate. Since we can express negation $\neg a = t/a$ as in Lemma 3.4, H is strongly Boolean-complete, and so G is Boolean-complete by Lemma 4.3. $\square$

The above result can be generalized to quasigroups with a slightly different technique. Without the cancellation property, however, a groupoid can be non-polyabelian without being Boolean-complete. Presumably, some yet subtler property is required to generalize this result to all groupoids. We refer the reader to [15] for more details.

References

[1] Albert A.A., *Quasigroups I*, Trans. Amer. Math. Soc. **54** (1943), 507–519 and *Quasigroup II*, Trans. Amer. Math. Soc. **55** (1944), 401–419.

[2] Barrington D.A., Straubing H., Thérien D., *Non-uniform automata over groups*, Information and Computation **89** (1990), 109–132.

[3] Barrington D., Thérien D., *Finite monoids and the fine structure of NC^1*, Journal of the ACM **35** (1988), 941–952.

[4] Bruck R.H., *Contributions to the theory of loops*, Trans. Amer. Math. Soc **60** (1946), 245–354.

[5] Bruck R.H., *A Survey of Binary Systems*, Springer-Verlag, 1966.

[6] Caussinus H., Lemieux F., *The complexity of computing over quasigroups*, in Proc. 14th annual FST&TCS, 1994, pp. 36–47.

[7] Chein O., Pflugfelder H.O., Smith J.D.H. (eds.), *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, 1990.

[8] Dénes J., Keedwell A.D., *Latin Squares and their Applications*, English University Press, 1974.

[9] Goldmann M., Russell A., Proc. 14th Annual IEEE Conference on Computational Complexity, 1999, The complexity of solving equations over finite groups.

[10] Hall P., *The Theory of Groups*, Macmillan, 1959.

[11] Lemieux F., *Finite Groupoids and their Applications to Computational Complexity*, Ph.D. Thesis, School of Computer Science, McGill University, Montréal, 1996.

[12] Maurer W.D., Rhodes J., *A property of finite simple non-Abelian groups*, Proc. Amer. Math. Soc. **16** (1965), 552–554.

[13] McKenzie R., *On minimal, locally finite varieties with permuting congruence relations*, preprint, 1976.

[14] Moore C., *Predicting non-linear cellular automata quickly by decomposing them into linear ones*, Physica D **111** (1998), 27–41.

[15] Moore C., Thérien D., Lemieux F., Berman J., Drisko A., *Circuits and expressions with non-associative gates*, to appear in J. Comput. System Sci.

[16] Papadimitriou C.H., *Computational Complexity*, Addison-Wesley, 1994.

[17] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Heldermann Verlag, 1990.

[18] Straubing H., *Families of recognizable sets corresponding to certain families of finite monoids*, J. Pure Appl. Algebra **15** (1979), 305–318.

[19] Straubing H., *Representing functions by words over finite semigroups*, Université de Montréal, Technical Report #838, 1992.

[20] Suzuki M., *Group Theory I.*, Springer-Verlag, 1982.

[21] Thérien D., *Classification of finite monoids: the language approach*, Theor. Comp. Sci. **14** (1981), 195–208.

[22] Szendrei A., *Clones in Universal Algebra*, Les Presses de L'Université de Montréal, 1986.
[23] Vesanen A., *Solvable groups and loops*, J. Algebra **180** (1996), 862–876.

Université du Québec à Chicoutimi, Chicoutimi, Québec, Canada
E-mail: flemieux@uqac.uquebec.ca

University of New Mexico, Albuquerque, New Mexico and the Santa Fe Institute, Santa Fe, New Mexico, USA
E-mail: moore@santafe.edu

McGill University, Montréal, Québec, Canada
E-mail: denis@cs.mcgill.ca

(*Received* September 15, 1999, *revised* March 9, 2000)