Subdirect products and propagating equations with an application to the Moufang Theorem

Aleš Drápal *

Department of Mathematics, Charles University, Sokolovská 83, 186 75, Praha 8, Czech Republic

Petr Vojtěchovský †

Department of Mathematics, University of Denver, 2390 S. York St, Denver, Colorado, 80208, USA

Received dd mmmm yyyy, accepted dd mmmmm yyyy, published online dd mmmmm yyyy

Abstract

We introduce the concept of propagating equations and focus on the case of associativity propagating in varieties of loops.

An equation \(\varepsilon\) propagates in an algebra \(X\) if \(\varepsilon(\overrightarrow{y})\) holds whenever \(\varepsilon(\overrightarrow{x})\) holds and the elements of \(\overrightarrow{y}\) are contained in the subalgebra of \(X\) generated by \(\overrightarrow{x}\). If \(\varepsilon\) propagates in \(X\) then it propagates in all subalgebras and products of \(X\) but not necessarily in all homomorphic images of \(X\). If \(V\) is a variety, the propagating core \(V[\varepsilon] = \{X \in V : \varepsilon\) propagates in \(X\}\) is a quasivariety but not necessarily a variety.

We prove by elementary means Goursat’s Lemma for loops and describe all subdirect products of \(X^k\) and all finitely generated loops in \(HSP(X)\) for a nonabelian simple loop \(X\). If \(V\) is a variety of loops in which associativity propagates, \(X\) is a finite loop in which associativity propagates and every subloop of \(X\) is either nonabelian simple or contained in \(V\), then associativity propagates in \(HSP(X) \lor V\).

We study the propagating core \(S[x(yz) = (xy)z]\) of Steiner loops with respect to associativity. While this is not a variety, we exhibit many varieties contained in \(S[x(yz) = (xy)z]\), each providing a solution to Rajah’s problem, i.e., a variety of loops not contained in Moufang loops in which the Moufang Theorem holds.

Keywords: Propagation of equations, quasi-variety, Moufang Theorem, subdirect product, Moufang loop, Steiner loop, oriented Steiner loop.


---

*Partially supported by INTER-EXCELLENCE project LTAUSA19070 MŠMT Czech Republic.
†Partially supported by the 2019 PROF grant of the University of Denver.

E-mail addresses: drapal@karlin.mff.cuni.cz (Aleš Drápal), petr@math.du.edu (Petr Vojtěchovský)
1 Introduction

It is natural to ask whether an equation holds in a given algebra $X$ if it is satisfied on a given generating subset of $X$. The following definition formalizes this idea under the restriction that the equation involves all elements of the generating subset and it is satisfied for at least one ordering of the generators.

**Definition 1.1.** Let $X$ be an algebra and $\varepsilon$ an equation with $n$ variables in the signature of $X$. Then $\varepsilon$ propagates in $X$ if the implication

$$
\varepsilon(x_1, \ldots, x_n) \implies (\varepsilon(y_1, \ldots, y_n) \text{ for all } y_1, \ldots, y_n \in \langle x_1, \ldots, x_n \rangle)
$$

(1.1)

holds for all $x_1, \ldots, x_n \in X$. Here, $\langle x_1, \ldots, x_n \rangle$ denotes the subalgebra of $X$ generated by $x_1, \ldots, x_n$. An equation $\varepsilon$ propagates in a class $\mathcal{X}$ of algebras if it propagates in every $X \in \mathcal{X}$.

It is not difficult to come up with examples of propagating equations. For instance, idempotence propagates in magmas since if $xx = x$ for some element $x$ of a magma, then $\langle x \rangle = \{x\}$ and therefore $yy = y$ holds for every $y \in \langle x \rangle$. For any integer $m$, the equation $x^m = 1$ propagates in groups. Of course, any equation that cannot be satisfied in a given algebra propagates therein, e.g., the equation $2x = 1$ propagates in the ring of integers.

More importantly, some standard results from abstract algebra can be restated in the language of propagating equations. For instance, commutativity propagates in the variety of semigroups, i.e., if $xy = yx$ for some elements $x, y$ of a semigroup, then the subsemigroup generated by $x$ and $y$ is commutative. The celebrated Moufang Theorem [14] (see [7] for a shorter proof) says that associativity propagates in the variety $\mathcal{M}$ of Moufang loops, i.e., if $x(yz) = (xy)z$ for some elements $x, y, z$ of a Moufang loop, then the subloop generated by $x, y, z$ is associative.

In our recent paper [8] we answered in affirmative a question of Rajah by exhibiting a variety of loops not contained in $\mathcal{M}$ in which associativity propagates, namely the variety of Steiner loops satisfying the identity $(xz)((xy)z)(yz) = ((xz)((xy)z))(yz)$.

Our solution to Rajah’s problem was intentionally elementary, however, our understanding of propagation of associativity in loops remains limited, not to mention propagation of general equations in universal algebras. Typical questions that come to mind are:

- If an equation $\varepsilon$ propagates in an algebra $X$, under which assumptions does $\varepsilon$ propagate in the variety $\text{HSP}(X)$ generated by $X$?
- If $\varepsilon$ propagates in the varieties $\mathcal{V}_1$ and $\mathcal{V}_2$, under which assumptions does $\varepsilon$ propagate in the join $\mathcal{V}_1 \vee \mathcal{V}_2$?
- Given a variety $\mathcal{V}$ and an equation $\varepsilon$, what is the largest variety $\mathcal{W}$ contained in $\mathcal{V}$ in which $\varepsilon$ propagates, if it exists?

In this paper we make a few initial observations about propagation of equations and then focus heavily on the special case of associativity in loops, particularly on propagation in $\text{HSP}(X)$ for a given loop $X$. After introducing notation and terminology, we show that the class of algebras in which a given equation propagates is a quasivariety but not always a variety; it is therefore closed under subalgebras and products but not always under homomorphic images. In Section 2 we derive basic properties of subdirect products of loops. In Section 3 we prove Goursat’s Lemma for loops, showing that subdirect products of $X \times Y$
are precisely lifted graphs of isomorphisms. We also characterize normal subloops and normal subdirect products of \(X \times Y\) and we describe a class of subdirect products of \(X^k\).

In the short Section 4 we show that the above class accounts for all subdirect products of \(X^k\) as long as \(X\) is a nonabelian simple loop and we describe all normal subloops of \(X^k \times Y\) for an arbitrary loop \(Y\). In Section 5 we focus on the variety \(\text{HSP}(X)\) generated by a single nonabelian simple loop \(X\) and we describe all finitely generated algebras of \(\text{HSP}(X)\). Returning to propagation of equations, we prove our main result:

Suppose that an equation \(\varepsilon\) propagates in a variety of loops \(V\) and in finite loops \(X_1, \ldots, X_n\). If every subloop \(Y \leq X_i\) is either in \(V\) or is nonabelian and simple, then \(\varepsilon\) propagates in \(\text{HSP}(X_1, \ldots, X_n) \cup V\).

Finally, in Section 6 we study the class \(S_{[x(yz)=(xy)z]}\) of Steiner loops in which associativity propagates. We show that \(S_{[x(yz)=(xy)z]}\) is not a variety and we construct several varieties contained in \(S_{[x(yz)=(xy)z]}\) but not in the variety of abelian groups, cf. Corollary 6.4. Generalizing a result of Stuhl [17], we show that an oriented anti-Pasch Steiner loop is in \(S_{[x(yz)=(xy)z]}\) if and only if it has exponent 4.

The approach in Sections 2–4 is elementary and written in the language of loop theory and the exposition parallels that of group theory. Some of our results are known to hold more generally and some of our arguments could be simplified by using general results of universal algebra, such as the Fleischer Lemma [3, Lemma 10.1] and the Foster-Pixley Lemma [3, Corollary 10.2]. For instance, Goursat’s Lemma [11] holds in any Mal’cev variety [4, 12], Proposition 4.2 can be seen as a refinement of the Foster-Pixley Lemma for loops, and the step in the proof of Proposition 5.3 that relies on Proposition 4.2 goes through by applying the standard version of the Foster-Pixley Lemma.

Nevertheless, we record these results in the language of loop theory to make them accessible in their concrete form, in anticipation of future refinements concerned with particular classes of loops. Efforts to generalize Goursat’s Lemma from groups to more general varieties are long-standing. We thank the referee for pointing out the paper [12], where Goursat’s Lemma was first proved for loops.

1.1 Notation and terminology


A class of algebras with the same signature is a \textit{variety} if it is equationally defined. Given a class \(\mathcal{X}\) of algebras, let \(H(\mathcal{X})\) (resp. \(S(\mathcal{X}), P(\mathcal{X})\)) be the class of all homomorphic images (resp. subalgebras, products) of algebras from \(\mathcal{X}\). By the Birkhoff Theorem, the smallest variety containing \(\mathcal{X}\) is equal to \(\text{HSP}(\mathcal{X})\).

In a magma \((X, \cdot)\), let \(L_x: X \to X, L_x(y) = xy\) and \(R_x: X \to X, R_x(y) = yx\) denote the left and right translation by \(x \in X\), respectively. An algebra \((X, \cdot, \backslash, /)\) is a \textit{quasigroup} if the identities \(x(x\backslash y) = y = x(x/y), (x/y)y = x = (xy)/y\) hold [9]. A quasigroup \(X\) is a \textit{loop} if there is \(e \in X\) such that \(ex = xe = x\) holds for all \(x \in X\). Equivalently (but not from a universal-algebraic point of view, cf. [1]), \((X, \cdot, e)\) is a loop if all translations \(L_x, R_x\) are permutations of \(X\) and \(ex = xe = e\) holds for all \(x \in X\). Note that then \(x\backslash y = L_x^{-1}(y)\) and \(x/y = R_y^{-1}(x)\).

For a nonempty subset \(A\) of a loop \(X\) we write \(A \leq X\) if \(A\) is a subloop of \(X\) and \(A \leq X\) if \(A\) is a normal subloop of \(X\). A subloop \(A\) of \(X\) is \textit{proper} if \(A \neq X\) and \textit{trivial} if \(A = \{e\}\) or \(A = X\). A nontrivial loop is \textit{simple} if it has no nontrivial normal subloops.
A loop \(X\) is abelian if it is an abelian group. In particular, if we say that \(X\) is a nonabelian simple loop then \(X\) is a simple loop that is either not commutative or not associative.

The inner mapping group of a loop \(X\) is the permutation group \(\text{Inn}(X)\) generated by \(L_{x,y} = L_x^{-1}L_yL_x\), \(R_{x,y} = R_y^{-1}R_xR_y\) and \(T_x = R_x^{-1}L_x\), where \(x, y \in X\). The permutations \(L_{x,y}\), \(R_{x,y}\) and \(T_x\) are known as the standard generators of \(\text{Inn}(X)\). For each of the standard generators \(\psi\) of \(\text{Inn}(X)\) there exists a loop term \(t(x, y, z)\) such that \(\psi(z) = t(x, y, z)\), where for \(T_x\) we use \(y\) as a dummy variable. Each such term will be called an inner generating term.

Note that a subloop \(A\) of \(X\) is normal in \(X\) if and only if \(t(x, y, z) \in A\) for every inner generating term \(t\), every \(x, y \in X\) and every \(z \in A\).

An element \(z \in X\) is central if \(t(x, y, z) = z\) for every inner generating term \(t\) and every \(x, y \in X\). The center \(Z(X)\) of \(X\) consists of all central elements of \(X\). A subloop \(A \leq X\) is central if \(A \leq Z(X)\).

Given an abelian group \((Z, +, 0)\), a loop \((F, \cdot, e)\) and a loop cocycle \(f : F \times F \to Z\) (so \(f\) satisfies \(f(e, x) = f(x, e) = 0\) for all \(x \in F\)), the central extension \(X = \text{Ext}(Z, F, f)\) of \(Z\) by \(F\) is the loop \((Z \times F, *, (0, e))\) defined by \((a, x) * (b, y) = (a + b + f(x, y), xy)\). Note that \(Z \times \{e\} \leq Z(X)\) and \((Z \times \{e\})\) is isomorphic to \(F\).

A Steiner triple system of order \(n\), denoted by \(STS(n)\), is a decomposition of the \(n(n-1)/2\) edges of the complete graph \(K_n\) into disjoint triangles, called blocks. There is a unique \(STS(9)\) up to isomorphism. A Hall triple system is a Steiner triple system in which any three elements that do not form a block generate a subsystem isomorphic to \(STS(9)\). A Pasch configuration consists of blocks \(\{a, b, c\}, \{a, y, z\}, \{x, b, z\}, \{x, y, c\}\) for distinct points \(a, b, c, x, y, z\). A Steiner triple system is anti-Pasch if it contains no Pasch configurations. Note that every Hall triple system is anti-Pasch.

A Steiner quasigroup is a commutative quasigroup satisfying the identities \(xx = x\) and \(x(xy) = y\). There is a one-to-one correspondence between Steiner triple systems and Steiner quasigroups defined on a set \(X\): if \(x \neq y\) then \(x * y = z\) if and only if \(\{x, y, z\}\) is a block, and \(x * x = x\). A Steiner loop is a commutative loop satisfying the identity \(x(xy) = y\). There is a one-to-one correspondence between Steiner quasigroups and Steiner loops. If \((X, \cdot)\) is a Steiner quasigroup then \((X \cup \{e\}, *)\) is a Steiner loop, where \(x * e = e * x = x\) and \(x * x = e\) for \(x \in X \cup \{e\}\), and \(x * y = xy\) if \(x \neq y\) are elements of \(X\). Conversely, if \((X \cup \{e\}, *)\) is a Steiner loop then \((X, \cdot)\) is a Steiner quasigroup, where \(xx = x\) and \(xy = x * y\) whenever \(x \neq y\).

A mapping \(\varphi : X \rightarrow Y\) between loops is a homomorphism if \(\varphi(xy) = \varphi(x)\varphi(y)\) for every \(x, y \in X\). If \(\varphi : X \rightarrow Y\) is a homomorphism then \(\varphi(x/y) = \varphi(x)\varphi(y)\) and \(\varphi(x/y) = \varphi(x)/\varphi(y)\) for every \(x, y \in X\). We let \(\text{Im}(\varphi)\) denote the image of \(\varphi\) and \(\text{Ker}(\varphi) = \{x \in X : \varphi(x) = e\}\) the kernel of \(\varphi\). Note that if \(\varphi : X \rightarrow Y\) is a surjective loop homomorphism and \(A \subseteq X\) then \(f(A) \subseteq Y\) and \(Y/f(A)\) is a homomorphic image of \(X/A\).

### 1.2 Basic properties of equation propagation

For an equation \(\varepsilon\) and a class of algebras \(\mathcal{X}\) we call

\[\mathcal{X}[\varepsilon] = \{X \in \mathcal{X} : \varepsilon \text{ propagates in } X\}\]

the propagating core of \(\mathcal{X}\) with respect to \(\varepsilon\).
Theorem 1.2. Let \( \varepsilon \) be an equation and \( \mathcal{X} \) the class of all algebras in a signature \( \Sigma \). Then the propagating core \( \mathcal{X}[\varepsilon] \) is a quasivariety.

Proof. Let \( T \) be the class of all terms in \( \Sigma \) and note that \( y \in \langle x_1, \ldots, x_n \rangle \) if and only if \( y = u(x_1, \ldots, x_n) \) for some \( u \in T \). The implication (1.1) is therefore equivalent to the collection of implications

\[
\varepsilon(x_1, \ldots, x_n) \implies \varepsilon(u_1(x_1, \ldots, x_n), \ldots, u_n(x_1, \ldots, x_n)),
\]

where \( u_1, \ldots, u_n \) range over \( T \).

\[\square\]

Corollary 1.3. Let \( \varepsilon \) be an equation that propagates in the class \( \mathcal{X} \) of algebras. Then \( \varepsilon \) propagates in \( S(\mathcal{X}) \) and in \( P(\mathcal{X}) \).

Proof. This follows from Theorem 1.2 and from the fact that quasivarieties are closed under subalgebras and products, cf. [3, Theorem V.2.25].

As an immediate consequence of Corollary 1.3 we obtain:

Lemma 1.4. An equation \( \varepsilon \) propagates in an algebra \( X \) if and only if it propagates in every finitely generated subalgebra of \( X \).

Proposition 1.5. Let \( \varepsilon \) be an equation and \( \mathcal{V} \) a variety. Then the propagating core \( \mathcal{V}[\varepsilon] \) is a variety if and only if \( H(\mathcal{V}[\varepsilon]) \subseteq \mathcal{V}[\varepsilon] \).

The following example exhibits an algebra \( X \) and an equation \( \varepsilon \) that propagates in \( X \) but not in \( H(X) \).

Example 1.6. Consider the loop equation

\[(xx)x = e \] (1.2)

and the loop \((F, \cdot, e)\) with multiplication table

<table>
<thead>
<tr>
<th>(F)</th>
<th>(e)</th>
<th>(a)</th>
<th>(b)</th>
<th>(c)</th>
<th>(d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e)</td>
<td>(e)</td>
<td>(a)</td>
<td>(b)</td>
<td>(c)</td>
<td>(d)</td>
</tr>
<tr>
<td>(a)</td>
<td>(a)</td>
<td>(b)</td>
<td>(d)</td>
<td>(e)</td>
<td>(c)</td>
</tr>
<tr>
<td>(b)</td>
<td>(b)</td>
<td>(e)</td>
<td>(c)</td>
<td>(d)</td>
<td>(a)</td>
</tr>
<tr>
<td>(c)</td>
<td>(c)</td>
<td>(d)</td>
<td>(a)</td>
<td>(b)</td>
<td>(e)</td>
</tr>
<tr>
<td>(d)</td>
<td>(d)</td>
<td>(c)</td>
<td>(e)</td>
<td>(a)</td>
<td>(b)</td>
</tr>
</tbody>
</table>

Then (1.2) does not propagate in \( F \) because \((aa)a = ba = e, b = aa \in \langle a \rangle\), but \((bb)b = cb = a \neq e\).

Let \( X = \text{Ext}(\mathbb{Z}_3, F, f) = (\mathbb{Z}_3 \times F, *, (0, e)) \), where

\[f(x, y) = \begin{cases} 
0, & \text{if } x = e \text{ or } y = e \text{ or } x \neq y, \\
1, & \text{if } x = y \neq e.
\end{cases}\]

Let \( Z = \mathbb{Z}_3 \times \{e\} \leq X \) and note that \( X/Z \) is isomorphic to \( F \). We claim that (1.2) propagates in \( X \). Consider \((r, x) \in X\). If \( x \neq e \) then \((r, x) * (r, x) * (r, x) = (2r + 1, x^2) * (r, x) = (1, x^2) \neq (0, e)\), where we have used \( x^2 \neq x \). If \( x = e \) then \((r, x) = (r, e)\) generates a subgroup of \( Z \cong \mathbb{Z}_3 \) in which (1.2) certainly holds.
Example 6.2 will furnish a finite Steiner loop $X$ such that associativity propagates in $X$ but not in $H(X)$.

**Example 1.7.** Let $\mathcal{R}$ be the variety of unital rings. We claim that $R \in \mathcal{R}_{[x^2=x]}$ if and only if $\text{char}(R) = 2$. Indeed, if idempotence propagates in $R$ then, since $1^2 = 1$, we must have $(1 + 1)^2 = 1 + 1$ and thus $\text{char}(R) = 2$. Conversely, suppose that $R \in \mathcal{R}$, $\text{char}(R) = 2$ and $r \in R$ satisfies $r^2 = r$. Note that $\langle r \rangle = \{ f(r) : f \in \mathbb{Z}[x] \} \subseteq \{ 0, 1, r, 1 + r \}$. Then $u^2 = u$ for every $u \in \langle r \rangle$.

Note that $\mathcal{R}_{[x^2=x]}$ properly contains the variety $\{ R \in \mathcal{R} : x^2 = x \text{ holds in } R \}$ of unital boolean rings.

Summarizing, the propagating core $\mathcal{V}_{[e]}$ of a variety $\mathcal{V}$ is a quasivariety but it need not be a variety, cf. Example 1.6. When $\mathcal{V}_{[e]}$ is a variety, it might be properly contained between the varieties $\mathcal{V}$ and $\{ X \in \mathcal{V} : \varepsilon \text{ holds in } X \}$, cf. Example 1.7.

## 2 Basic properties of subdirect products in loops

Let $I$ be an index set, $X_i$ a loop for every $i \in I$ and $X = \prod_{i \in I} X_i$. The identity element of every $X_i$ will be denoted by $e$ rather than by $e_i$; it will be always clear from the context to which loop the identity element $e$ belongs. Given $x = (x_i) = (x_i)_{i \in I} \in X$, we denote by $\text{supp}(x) = \{ i \in I : x_i \neq e \}$ the support of $x$. For $J \subseteq I$, let $p_J : X \to \prod_{i \in J} X_i$ be the canonical projection defined by $p_J((x_i)_{i \in I}) = (x_i)_{i \in J}$ and let $e_J : \prod_{i \in J} X_i \to X$ be the canonical embedding defined by $e_J((y_i)_{i \in J}) = (y_i)_{i \in I}$, where $y_i = x_i$ if $i \in J$ and $y_i = e$ otherwise. For $A \subseteq X$ and $J \subseteq I$, let

$$A_J = p_J(A) \quad \text{and} \quad A[J] = \{ x \in A : \text{supp}(x) \subseteq J \}.$$


A subloop $A \leq \prod_{i \in I} X_i$ is a subdirect product of $\prod_{i \in I} X_i$ if $A_i = X_i$ for every $i \in I$, in which case we write $A \leq_{sd} \prod_{i \in I} X_i$. (Note that the factorization of $X = \prod_{i \in I} X_i$ matters in the definition of subdirect product. For instance, $A = \{ (x,x,x) : x \in \mathbb{R} \}$ is a subdirect product of $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ but not a subdirect product of $(\mathbb{R} \times \mathbb{R})$.

**Lemma 2.1.** Let $A \leq_{sd} \prod_{i \in I} X_i$ and let $\{ I_k : k \in K \}$ be a partition of $I$. Then $A \leq_{sd} \prod_{k \in K} A_{I_k}$ and $A_{I_k} \leq_{sd} \prod_{i \in I_k} X_i$ for every $k \in K$.

**Proof.** Let $k \in K$. If $a_{I_k} \in A_{I_k}$ then there is $a \in A$ such that $p_{I_k}(a) = a_{I_k}$. This shows that $A \leq_{sd} \prod_{k \in K} A_{I_k}$. If $i \in I_k$ and $x_i \in X_i$ then there is $a \in A$ such that $p_i(a) = x_i$. But then also $p_i(p_{I_k}(a)) = x_i$ and thus $A_{I_k} \leq_{sd} \prod_{i \in I_k} X_i$. \qed

**Lemma 2.2.** Let $I$ be a finite index set and $A \leq \prod_{i \in I} X_i = X$. Then $\prod_{i \in I} A[i],i \leq A$.

**Proof.** We have $A[i],i \leq A_i \leq X_i$ and thus $\prod_{i \in I} A[i],i \leq X$. Let $x = (x_i) \in \prod_{i \in I} A[i],i$. Then $x_i \in A[i],i$ and $e_i(x_i) \in A[i],i \leq A$. If $I = \{ 1, \ldots, n \}$, we conclude that $x = e_1(x_1) \cdots e_n(x_n) \in A[1] \cdots A[n] \leq A$. \qed

**Lemma 2.3.** Let $X = \prod_{i \in I} X_i$ and $J \subseteq I$. If $A \leq X$ then $A[J],J \leq A$ and $A[J],J \leq A_J$. If $A \leq X$ then $A[J],J \leq X$ and $A[J],J \leq X_J$. 

Proof. Let \( t \) be an inner generating term. For \( x, y \in X \) and \( i \in I \) we have \( t(x_i, y_i, e) = e \), which implies \( t(x, y, X[J]) \subseteq X[J] \). If \( A \leq X \) then \( t(A, A, A[J]) \subseteq A \cap X[J] = A[J] \), proving \( A[J] \triangleleft A \). Since epimorphisms preserve normality, \( A[J] \triangleleft A \) follows. If \( A \leq X \) then \( t(X, X, A[J]) \subseteq A \cap X[J] = A[J] \), so \( A[J] \triangleleft A \) and \( A[J]J \triangleleft X_J \).

Lemma 2.4. Let \( X = \prod_{i \in I} X_i \) and let \( J, K \) be subsets of \( I \) such that all of the following conditions are satisfied:

- \( J, K \) are finite,
- \( X_i \) is finite for every \( j \in J \),
- for every \( i \in I \setminus K \) there is \( j \in J \) such that \( X_i \) is isomorphic to \( X_j \).

Then every finitely generated subloop of \( X \) is isomorphic to a subloop of \( X_L \) for some finite subset \( L \) of \( I \).

Proof. Without loss of generality, we can assume that \( X_i = X_j \) whenever \( X_i \) is isomorphic to \( X_j \). Let \( A = \langle a_\ell = (a_\ell,i) : 1 \leq \ell \leq n \rangle \) be a finitely generated subloop of \( X \). Define an equivalence relation \( \sim \) on \( I \) by setting \( i \sim j \) if and only if \( X_i = X_j \) and \( a_i = a_j \) for every \( 1 \leq \ell \leq n \). Since \( J, K \) are finite and every \( X_j \) with \( j \in J \) is finite, \( \sim \) has only finitely many equivalence classes. Let \( L \) be a complete set of representatives of the equivalence classes of \( \sim \). Then \( p_L(A) \) is isomorphic to \( A \).

For \( K \triangleleft X \), denote by \( \pi_{X/K} \) the canonical projection \( X \to X/K \). A straightforward application of the Correspondence Theorem for loops yields:

Proposition 2.5. Let \( X = \prod_{i \in I} X_i \) and \( K = \prod_{i \in I} K_i \), where \( K_i \triangleleft X_i \) for every \( i \in I \). The mapping \( \pi : X \to \prod_{i \in I} X_i/K_i \) defined by \( \pi((x_i)) = (x_iK_i) \) induces a lattice isomorphism between all subloops \( A \leq X \) containing \( K \) and all subloops \( B \leq \prod_{i \in I} X_i/K_i \). Moreover, when \( A, B \) are such subloops, then:

(i) \( \pi^{-1}(B) = \{ (x_i) : (x_iK_i) \in B \} \);
(ii) \( A \leq X \) if and only if \( \pi(A) \leq \prod_{i \in I} X_i/K_i \);
(iii) \( A \leq_{sd} X \) if and only if \( \pi(A) \leq_{sd} \prod_{i \in I} X_i/K_i \);
(iv) \( \pi(A)[J] = \pi(A[J]) \) and \( K_J \leq A[J]_J \);
(v) \( (\pi(A)[J])_J \) is isomorphic to \( A[J]_J / K_J \) for every \( J \subseteq I \), and if \( J \) is a singleton then the two sets are equal.

Proof. Let \( A \leq X \) and \( B = \pi(A) \). We can write \( \pi = \prod_{i \in I} \pi_{X_i/K_i} \), where \( \gamma : X/K \to \prod X_i/K_i \) is the isomorphism given by \( (x_i)K \mapsto (x_iK_i) \). Parts (i) and (ii) then follow from the Correspondence Theorem applied to \( \pi_{X/K} \).

(iii) Suppose that \( A \leq_{sd} X \). Fix \( j \in I \) and \( a_jK_j \in X_j/K_j \). There is \( (x_i) \in A \) such that \( x_j = a_j \) and thus \( (x_iK_i) \in B \) and \( a_jK_j \in B_j \). Conversely, suppose that \( B \leq_{sd} \prod X_i/K_i \). Fix \( j \in I \) and \( a_j \in X_j \). There is \( (x_i) \in A \) such that \( x_j = a_j \) and \( (x_iK_i) \in B \) such that \( x_jK_j = a_jK_j \). Since \( K \leq A \), we can assume without loss of generality that \( x_j = a_j \). Then \( a_j \in A_j \).

(iv) Let \( (x_iK_i) \in \pi(A)[J] \). Then there is \( a = (a_i) \in A \) such that \( (a_iK_i) = (x_iK_i) \) and \( a_iK_i = K_i \) for \( i \not\in J \). Let \( k = (k_i) \) be defined by \( k_i = 1 \) if \( i \in J \), else \( k_i = a_i \). Note that \( k \in K \). Then \( c = a/k \in A \cap X[J] = A[J] \) since \( K \leq A \) and \( \pi(c) = \pi(a) = (x_iK_i) \). Conversely, if \( (x_iK_i) \in \pi(A)[J] \) then there is \( (a_i) \in A[J] \) such that \( (x_iK_i) = (a_iK_i) \), so certainly \( a_iK_i = K_i \) for \( i \not\in J \) and \( (x_iK_i) \in \pi(A)[J] \).
If \( x \in K \) then \( x = k_j \) for some \( k \in K \). Let \( \ell = e_j(k_j) \in K[J] \leq A[J] \). Then \( \ell_j = k_j = x \) and \( x \in A[J] \) follows.

(v) \( (\pi(A[J])_j = \pi(A[J])_j \) is isomorphic to \( ((A[J]K)/K)_J = (A[J]K)/K_J = (A[J]J)/K_J = A[J]/K_J \) via the restriction of \( \gamma \) to \( X_J/K_J \). If \( J = \{i\} \) then both \( (\pi(A[J])_j \) and \( A[J]/K_J \) are subsets of \( B_i/K_i \) and the above isomorphism is the identity map.

In the situation of Proposition 2.5, if \( K \leq A \) then we certainly have \( K_i \leq A[i]_i \) for every \( i \in I \), since \( K_i \) embeds into \( A[i] \). Conversely, if \( I \) is finite, \( A \leq X \) and \( K_i \leq A[i]_i \) for every \( i \), then \( K \leq A \) by Lemma 2.2.

We say that \( A \subseteq \prod_{i \in I} X_i \) is flat if \( A[i] = \{e\} \) for every \( i \in I \).

\[ \text{Lemma 2.6.} \quad \text{Let} \quad I \text{ be a finite index set,} \quad A \leq X = \prod_{i \in I} X_i \text{ and } N_i = A[i]_i \text{ for every } i \in I. \quad \text{Then } N_i \leq X_i \text{ and we can define } \pi = \prod_{i \in I} \pi_{X_i/N_i}, B = \pi(A) \text{ and } Y = \pi(X) = \prod_{i \in I} X_i/N_i. \quad \text{Then:} \]

(i) \( B \leq Y \).

(ii) \( B \) is a flat subloop of \( Y = \prod_{i \in I} X_i/N_i \).

(iii) \( A \leq_{sd} X \) if and only if \( B \leq_{sd} Y \).

(iv) \( X/A \) is isomorphic to \( Y/B \).

\[ \text{Proof.} \quad \text{Let } K_i = N_i = A[i]_i \text{ and } K = \prod_{i \in I} K_i. \quad \text{By Lemma 2.2, } K \leq A \text{ since } I \text{ is finite. By Lemma 2.3, } K_i \leq X_i \text{ and thus } K \leq X. \quad \text{By Proposition 2.5, } B \leq Y, B[i] = A[i]_i/K_i = K_i/K_i = K_i \text{ and, also, } A \leq_{sd} X \text{ if and only if } B \leq_{sd} Y. \quad \text{Write } \pi = \gamma \pi_{X/K} \text{ as in the proof of Proposition 2.5. Using the Third Isomorphism Theorem, we then have } X/A \cong (X/K)/(A/K) = \pi_{X/K}(X)/\pi_{X/K}(A) \cong \gamma \pi_{X/K}(X)/\gamma \pi_{X/K}(A) = Y/B. \quad \square \]

3 Lifted isomorphism graphs and subdirect products

Let \( \varphi: X_1 \rightarrow X_2 \) be a mapping between loops. The graph of \( \varphi \) is the set

\[ \mathcal{G}(\varphi) = \{(x, \varphi(x)) : x \in X_1\}. \]

\[ \text{Lemma 3.1.} \quad \text{Let } X_1, X_2 \text{ be loops and } \varphi: X_1 \rightarrow X_2 \text{ a mapping. Then } \varphi \text{ is a homomorphism if and only if } \mathcal{G}(\varphi) \leq X_1 \times X_2. \]

\[ \text{Proof.} \quad \text{Indeed, if } x, y \in X_1, \text{ then } (x, \varphi(x))(y, \varphi(y)) = (xy, \varphi(x)\varphi(y)) \text{ belongs to } \mathcal{G}(\varphi) \text{ if and only if } \varphi(x)\varphi(y) = \varphi(xy). \quad \square \]

\[ \text{Lemma 3.2.} \quad \text{Let } \varphi: X_1 \rightarrow X_2 \text{ be an injective loop homomorphism. Then the following conditions are equivalent:} \]

(i) \( \mathcal{G}(\varphi) \leq X_1 \times X_2 \),

(ii) \( X_1 \text{ is abelian and } \text{Im}(\varphi) \leq Z(X_2) \),

(iii) \( \mathcal{G}(\varphi) \leq Z(X_1 \times X_2) \).

\[ \text{Proof.} \quad \text{Working in the direct product } X_1 \times X_2, \text{ we have} \]

\[ t((x, u), (y, v), (z, \varphi(z))) = (t(x, y, z), t(u, v, \varphi(z))) \quad (3.1) \]
for every \( x, y, z \in X_1, u, v \in X_2 \) and every inner generating term \( t \).

Suppose that (i) holds. Then (3.1) is an element of \( G(\varphi) \) and substituting \( u = v = e \), we obtain \( (t(x, y, z), \varphi(z)) \in G(\varphi) \). Since \( (z, \varphi(z)) \in G(\varphi) \) and \( \varphi \) is injective, it follows that \( t(x, y, z) = z \) and \( X_1 \) is abelian. With \( x = y = e \) in (3.1), we obtain \( (z, t(u, v, \varphi(z))) \in G(\varphi) \), which means that \( t(u, v, \varphi(z)) = \varphi(z) \) and \( \text{Im}(\varphi) \leq Z(X_2) \).

Now suppose that (ii) holds. Then \( (t(x, y, z), t(u, v, \varphi(z))) = (z, \varphi(z)) \) and hence (3.1) shows \( G(\varphi) \leq Z(X_1 \times X_2) \). Clearly, (iii) implies (i). \( \square \)

Lemma 3.3. Let \( \varphi: K_1 \to K_2 \) be an isomorphism of loops and let \( K_i \leq X_i \) for \( i = 1, 2 \). Then \( G(\varphi) \leq X_1 \times X_2 \) if and only if \( K_i \leq Z(X_i) \) for \( i = 1, 2 \).

In particular, if \( \varphi: X_1 \to X_2 \) is an isomorphism of loops, then \( G(\varphi) \leq X_1 \times X_2 \) if and only if \( X_1 \) is abelian.

Proof. If \( K_i \leq Z(X_i) \) then \( G(\varphi) \leq K_i \leq K_2 \leq Z(X_1) \times Z(X_2) = Z(X_1 \times X_2) \) and hence \( G(\varphi) \leq X_1 \times X_2 \). Conversely, suppose that \( G(\varphi) \leq X_1 \times X_2 \). Then

\[
(t(x, y, z), \varphi(z)) = (t(x, y, z), t(e, e, \varphi(z))) = t((x, e), (y, e), (z, \varphi(z))) \in G(\varphi)
\]

for every \( x, y \in X_1 \) and \( z \in K_1 \). But then \( t(x, y, z) = z \) follows and we have \( K_1 \leq Z(X_1) \). Since \( \varphi \) is an isomorphism, \( K_2 \leq Z(X_2) \), too.

If \( \varphi: X_1 \to X_2 \) is an isomorphism, we deduce that \( G(\varphi) \leq X_1 \times X_2 \) if and only if \( X_i \leq Z(X_i) \) for \( i = 1, 2 \), which says that \( X_1, X_2 \) are abelian. Since \( X_1 \) is isomorphic to \( X_2 \), it suffices to check that \( X_1 \) is abelian. \( \square \)

For \( N_1 \leq X_1, N_2 \leq X_2 \) and a mapping \( \varphi: X_1/N_1 \to X_2/N_2 \), let

\[
G_{X_1/N_1, X_2/N_2}(\varphi) = (\pi_{X_1/N_1} \times \pi_{X_2/N_2})^{-1}(G(\varphi))
= \{(x_1, x_2) \in X_1 \times X_2 : \varphi(x_1N_1) = x_2N_2\}.
\]

If \( \varphi \) is a homomorphism then \( G_{X_1/N_1, X_2/N_2}(\varphi) \) is a subloop of \( X_1 \times X_2 \), being the preimage of \( G(\varphi) \) under the homomorphism \( \pi_{X_1/N_1} \times \pi_{X_2/N_2} \).

We call a subset \( A \) of \( X_1 \times X_2 \) a lifted isomorphism graph in \( X_1 \times X_2 \) if there exist \( N_1 \leq X_1, N_2 \leq X_2 \) and an isomorphism \( \varphi: X_1/N_1 \to X_2/N_2 \) such that \( A = G_{X_1/N_1, X_2/N_2}(\varphi) \).

Given a lifted isomorphism graph \( A \) in \( X_1 \times X_2 \), it is clear that \( N_1, N_2 \) and \( \varphi \) are uniquely determined. In particular, \( N_i = A[i]_i \) for \( i = 1, 2 \).

Proposition 3.4. Let \( X_1 \) and \( X_2 \) be loops. Then:

(i) [Goursat’s Lemma for loops] The subdirect products of \( X_1 \times X_2 \) are precisely the lifted isomorphism graphs in \( X_1 \times X_2 \).

(ii) If \( A = G_{X_1/N_1, X_2/N_2}(\varphi) \) is a lifted isomorphism graph in \( X_1 \times X_2 \) then \( A \leq X_1 \times X_2 \) if and only if \( X_1/N_1 \) is abelian.

Proof. Every lifted isomorphism graph in \( X_1 \times X_2 \) is clearly a subdirect product of \( X_1 \times X_2 \). Conversely, let \( A \leq_{sd} X_1 \times X_2 \), let \( N_i = A[i]_i \) and note that \( N_i \leq A_i = X_i \) by Lemma 2.3.

Suppose first that \( N_1 = \{e\} \) and \( N_2 = \{e\} \). If \( (x_1, x_2), (x_1, y_2) \in A \) then \( (e, x_2/y_2) = (x_1/x_1, x_2/y_2) \in A \) and hence \( x_2 = y_2 \) since \( N_2 = \{e\} \). Therefore, for each \( x_1 \in X_1 \) there exists exactly one \( x_2 \in X_2 \) such that \( (x_1, x_2) \in A \). Similarly, for each \( x_2 \in X_2 \) there
Lemma 3.3 implies \( M \). By Lemma 3.3, let

\[
M \subseteq X_1 \times X_2 \text{ such that } A \subseteq M_1 \times M_2, A[i]_i = N_i \leq X_i \text{ and } M_i/N_i \leq Z(X_i/N_i) \text{ for } i = 1, 2.
\]

If the equivalent conditions are satisfied then \((X_1 \times X_2)/A \cong (X_1/N_1 \times X_2/N_2)/G(\varphi)\) for some isomorphism \( \varphi : M_1/N_1 \to M_2/N_2 \).

**Proof.** Suppose that \( A \subseteq X_1 \times X_2 \) and set \( M_i = A_i = p_i(A) \subseteq X_i \). Then \( A \subseteq M_1 \times M_2 \). We have \( N_i = A[i]_i \subseteq X_i \) by Lemma 2.3 and obviously \( N_i \leq A_i = M_i \). By Goursat’s Lemma, \( \pi(A) = G(\varphi) \), where \( \varphi : M_1/N_1 \to M_2/N_2 \) is some isomorphism and \( \pi = \pi_{M_1/N_1} \times \pi_{M_2/N_2} \). Consider \( \rho = \pi_{X_1/N_1} \times \pi_{X_2/N_2} \). By the Correspondence Theorem (or see Proposition 2.5), \( A \subseteq X_1 \times X_2 \) implies \( \rho(A) = \pi(A) = G(\varphi) \subseteq X_1/N_1 \times X_2/N_2 \). By Lemma 3.3, \( A_i/N_i \leq Z(X_i/N_i) \) for \( i = 1, 2 \).

Conversely, suppose that (ii) holds and let \( \varphi \) be the uniquely determined isomorphism \( M_1/N_1 \to M_2/N_2 \) such that \( \pi(A) = G(\varphi) \). Since \( A_i/N_i \leq Z(X_i/N_i) \) for \( i = 1, 2 \), Lemma 3.3 implies \( G(\varphi) \subseteq X_1/N_1 \times X_2/N_2 \). Then, with \( \rho \) as above, we have \( A = \pi^{-1}(G(\varphi)) = \rho^{-1}(G(\varphi)) \subseteq X_1 \times X_2 \) by the Correspondence Theorem.

**Lemma 3.6.** Let \( \varphi : X_1 \to X_2 \) and \( \psi : X_1/N_1 \to X_2/N_2 \) be isomorphisms of loops and let \( A = G_{X_1/N_1, X_2/N_2}(\psi) \). Then:

(i) \( G(\varphi) \leq A \) if and only if \( \psi \pi_{X_1/N_1} = \pi_{X_2/N_2} \varphi \).

(ii) If \( G(\varphi) \leq A \) then \( A = \{(x_n, \varphi(x)) : x \in X_1, n \in N_1\} \).

(iii) If \( G(\varphi) \leq A \) then \( G(\varphi) \subseteq A \) if and only if \( N_1 \leq Z(X_1) \).

(iv) If \( G(\varphi) \leq A \) then \( A/G(\varphi) \cong N_1 \equiv N_2 \).

**Proof.** (i) The following conditions are equivalent: \( G(\varphi) \leq A \), \( \varphi(x)N_2 = \psi(x)N_1 \) for every \( x \in X_1 \), \( \pi_{X_2/N_2} \varphi = \psi \pi_{X_1/N_1} \). For the rest of the proof assume that \( G(\varphi) \leq A \).

(ii) If \( x \in X_1 \) and \( n \in N_1 \) then \( \psi(xnN_1) = \psi(xN_1) = \varphi(x)N_2 \) by (i) and thus \( (xn, \varphi(x)) \in A \). Conversely, let \( (x_1, x_2) \in A \) and \( x = \varphi^{-1}(x_2) \). Since \( (x_1, \varphi(x)) = (x_1, x_2) \in A \) and \( (x, \varphi(x)) \in G(\varphi) \leq A \), we have \( (x_1/x, e) \in A \), hence \( \psi((x_1/x)N_1) = N_2 \), \( x_1/x \in N_1 \) and \( x_1 = xN_1 \) for some \( n \in N_1 \).

(iii) Suppose that \( G(\varphi) \leq A \). In general, if \( U \subseteq V \), \( u_1, u_2 \in U \), \( v \in V \) and \( t \) is an inner generating term, then \( t(u_1, u_2, v)U = vU \). Hence \( (t(x, y, n), e)\mathbf{G}(\varphi) = t((x, \varphi(x)), (y, \varphi(y)), (n, e))\mathbf{G}(\varphi) = (n, e)\mathbf{G}(\varphi) \) for all \( x, y \in X_1 \) and \( n \in N_1 \). Since \( N_1 \leq X_1 \), we have \( m = t(x, y, n) \in N_1 \). We showed \( (m, e) \in (n, e)\mathbf{G}(\varphi) \), so \( (n, e) = (n, e)(z, \varphi(z)) = (nz, \varphi(z)) \) for some \( z \in X_1 \). But then \( z = e \), \( n = m = t(x, y, n) \) and \( N_1 \leq Z(X_1) \) follows.
Conversely, suppose that \( N_1 \leq Z(X_1) \). For any \( x, y, z \in X_1 \) and \( n, m \in N_1 \) we have \( t((xn, \varphi(x)), (ym, \varphi(y)), (z, \varphi(z))) = (t(xn, ym, z), t(\varphi(x), \varphi(y), \varphi(z))) = (t(x, y, z), \varphi(t(x, y, z))) \in G(\varphi) \), where we have used \( n, m \in Z(X_1) \). It follows from (ii) that \( G(\varphi) \cong A \).

(iv) Suppose again that \( G(\varphi) \cong A \). Then \( N_1 \leq Z(X_1) \) by (iii). Consider \( f: A \to N_1 \) defined by \( f(x, y) = x/\varphi^{-1}(y) \). For \( x \in X_1 \), \( n \in N_1 \) we have \( f(xn, \varphi(x)) = (xn)/x = n \) thanks to \( n \in Z(X_1) \). Then for every \( x, y \in X_1 \), \( n, m \in N_1 \), we have \( f(xn, \varphi(x))f(ym, \varphi(y)) = nmn = f((xn)(ym), \varphi(xy)) = f((xn)(ym), \varphi(x)\varphi(y)) = f((xn, \varphi(x))(ym, \varphi(y))) \), so \( f \) is a surjective homomorphism with kernel \( G(\varphi) \), establishing \( A/G(\varphi) \cong N_1 \). Similarly, \( A/G(\varphi) \cong N_2 \).

\[ \square \]

Lemma 3.7. Let \( A \) be a simple loop that is a homomorphic image of a subdirect product of \( X_1 \times X_2 \). Then \( A \) is abelian or a homomorphic image of \( X_1 \) or a homomorphic image of \( X_2 \).

\[ \text{Proof.} \] Let \( A \cong B/C \), where \( B \leq_{sd} X = X_1 \times X_2 \) and \( C \leq B \). Since \( p_1: B \to X_1 \) is a surjective homomorphism and \( C \leq B \), it follows that \( X_1/C_1 \) is a homomorphic image of \( B/C \cong A \). Since \( A \) is simple, we have either \( X_1/C_1 \cong A \) (and we are done) or \( C_1 = X_1 \). Similarly for the second coordinate.

We can therefore assume that \( C_1 = X_1 \) and \( C_2 = X_2 \), i.e., \( C \leq_{sd} X_1 \times X_2 \). By Lemmas 2.2 and 2.3, \( K_i = C[i] \leq C \), \( K = K_1 \times K_2 \leq X \) and \( K \leq C \). Let \( \gamma: X/K \cong (X_1/K_1) \times (X_2/K_2) \) be as in the proof of Proposition 2.5 so that \( \pi = \pi_{X_1/K_1} \times \pi_{X_2/K_2} = \gamma \pi_{X/K} \). Then, by the Third Isomorphism Theorem, we have \( B/C \cong (B/K)/C \cong \pi_{X/K}(B)/\pi_{X/K}(C) \cong \gamma(\pi_{X/K}(B))/\gamma(\pi_{X/K}(C)) = \pi(B)/\pi(C) \). By Proposition 2.5, \( \pi(B) \leq_{sd} X_1/K_1 \times X_2/K_2 \), \( \pi(C) \leq \pi(B) \) and \( \pi(C)[i] \mid C[i] \), so \( C[i]/K = K_1/K_2 = K_i \) for \( i = 1, 2 \).

We can therefore assume without loss of generality that \( C = \text{flat} \). By Goursat’s Lemma, \( C = G(\varphi) \) for some isomorphism \( \varphi: X_1 \to X_2 \) and \( B \) is a lifted isomorphism graph in \( X_1 \times X_2 \) such that \( C \leq B \). By Lemma 3.6, \( A \cong B/C \) is isomorphic to \( B[1], 1 \leq Z(X_1) \) and hence it is abelian.

\[ \square \]

Lemma 3.8. Let \( X \) be a loop, \( \sim \) an equivalence relation on \( \{1, \ldots, k\} \) with \( \ell \) equivalence classes and \( \varphi_i \in \text{Aut}(X) \) for every \( 1 \leq i \leq k \). Then

\[ S_X(\varphi_1, \ldots, \varphi_k) = \{ (x_1, \ldots, x_k) \in X^k : \varphi_i(x_i) = \varphi_j(x_j) \text{ whenever } i \sim j \} \]

is a subdirect product of \( X^k \) and it is isomorphic to \( X^\ell \).

\[ \text{Proof.} \] Let \( A = S_X(\varphi_1, \ldots, \varphi_k) \). Suppose that \( i \sim j \). If \( (x_1, \ldots, x_k), (y_1, \ldots, y_k) \in A \) then \( \varphi_i(x_i) = \varphi_j(x_j) \) and \( \varphi_i(y_i) = \varphi_j(y_j) \) imply \( \varphi_i(x_iy_i) = \varphi_j(x_jy_j) \), so \( A \) is closed under multiplication. Similarly, \( A \) is closed under divisions and hence it is a subloop of \( X^k \).

Let \( S \) be a complete set of representatives of the equivalence classes of \( \sim \) on \( X \). For every \( i \in S \), choose \( x_i \in X \) arbitrarily. Then \( (x_1, \ldots, x_k) \) belongs to \( A \) if and only if for every \( j \sim i \in S \) we have \( x_j = \varphi_j^{-1}(x_i) \). Hence the freely chosen tuple \( (x_i)_{i \in S} \) uniquely determines an element \( (x_1, \ldots, x_k) \) of \( A \) and \( A \cong X^{|S|} \) follows. We can certainly arrange for any \( 1 \leq i \leq k \) to be in \( S \). Thus \( A \) is a subdirect product of \( X^k \).

\[ \square \]

When \( \sim \) is the equality relation, Lemma 3.8 implies that \( S_X(\varphi_1, \ldots, \varphi_k) \cong X^k \).
Given $S_X^\sim(\varphi_1, \ldots, \varphi_k)$, let us define new automorphisms $\psi_i$ of $X$ as follows. In every equivalence class of $\sim$ choose a representative $i$ and let $\psi_j = \varphi_i^{-1} \varphi_j$ for all $j \sim i$. Then $S_X^\sim(\varphi_1, \ldots, \varphi_k) = S_X^\sim(\psi_1, \ldots, \psi_k)$. In particular, if $k = 2$, we see that the subdirect products $S_X^\sim(\varphi_1, \varphi_2)$ of $X \times X$ are precisely the graphs of automorphisms of $X$.

4 Subdirect products and normal subloops in $X^k$ for $X$ nonabelian simple

Lemma 4.1. Let $X$ be a nonabelian simple loop, $k \geq 0$ and $Y$ a loop. The normal subloops of $X^k \times Y$ are precisely the loops $M_1 \times \cdots \times M_k \times N$, where $M_i \in \{\{e\}, X\}$ for each $i \in \{1, \ldots, k\}$ and $N \leq Y$.

Proof. Let $A \trianglelefteq X^k \times Y$. We proceed by induction on $k$. The case $k = 0$ is clear. Suppose that $k \geq 1$, let $X_1 = X$, $X_2 = X^{k-1} \times Y$ so that $A \trianglelefteq X_1 \times X_2$. We have $p_1(A) \trianglelefteq X_1$ and $p_2(A) \trianglelefteq X_2$. By induction, $p_2(A) = M_2 \times \cdots \times M_k \times N$ for some $M_i \in \{\{e\}, X\}$ and $N \trianglelefteq Y$. Since $X$ is simple, $p_1(A) \in \{\{e\}, X\}$.

If $p_1(A) = \{e\}$ then $A = \{e\} \times p_2(A)$ and we are done. Suppose that $p_1(A) = X$ so that $A \trianglelefteq_{sd} X \times p_2(A)$. Note that $A \trianglelefteq X \times p_2(A)$ because $A \trianglelefteq X \times X_2$. By Goursat’s Lemma, there are $N_1 \trianglelefteq X$ and $N_2 \trianglelefteq p_2(A)$ such that $\phi: X/N_1 \cong p_2(A)/N_2$, $X/N_1$ is abelian and $A$ is isomorphic to $G_{X_1/N_1\times p_2(A)/N_2}(\phi)$. Since $N_1 \in \{\{e\}, X\}$ and $X$ is not abelian, we must have $N_1 = X$. But then $A = X \times p_2(A)$, finishing the proof. □

Proposition 4.2. Let $X$ be a nonabelian simple loop and let $k$ be a positive integer. Then the subdirect products of $X^k$ are precisely the subloops $S_X^\sim(\varphi_1, \ldots, \varphi_k)$ of $\bar{\text{Lemma}}$ 3.8.

Proof. We proceed by induction on $k$. The case $k = 1$ is trivial. By $\text{Proposition}$ 3.4, a subdirect product of $X \times X$ is equal to either $X \times X$ or to $G(\varphi)$ for some $\varphi \in \text{Aut}(X)$. By the remark following $\text{Lemma}$ 3.8, these are precisely the subloops $S_X^\sim(\varphi_1, \varphi_2)$. This gives the case $k = 2$ and we can assume that $k \geq 3$.

By $\text{Lemma}$ 3.8, every $S_X^\sim(\varphi_1, \ldots, \varphi_k)$ is a subdirect product of $X^k$.

Conversely, suppose that $A \trianglelefteq_{sd} X^k$. For $1 \leq i \leq k$ let $\delta_i$ be the homomorphism $X^k \to X^{k-1}$ that removes the $i$th coordinate. Let $B_i = \delta_i(A)$. Note that every $B_i$ is a subdirect product of $X^{k-1}$. In particular, by the induction assumption, $B_1 = S_X^\sim(\varphi_2, \ldots, \varphi_k)$ for some equivalence relation $\sim$ on $\{2, \ldots, k\}$ and some automorphisms $\varphi_i$ of $X$.

Suppose first that $\sim$ is not the equality relation and let $2 \leq r < s \leq k$ be such that $r \sim s$. By the induction assumption, $B_s = S_X^\sim(\psi_1, \ldots, \psi_{s-1}, \psi_s, \ldots, \psi_k)$ for some equivalence relation $\sim$ on $\{1, \ldots, k\} \setminus \{s\}$ and some automorphisms $\psi_i$ of $X$. Define a new equivalence relation $\equiv$ on $\{1, \ldots, k\}$ by adjoining $s$ to the equivalence class $[r]_\sim$, let $\theta_s = \varphi_s \varphi_r^{-1} \varphi_s$ and $\theta_i = \psi_i$ for $i \neq s$. We claim that $A = S_X^\equiv(\theta_1, \ldots, \theta_k)$. For $\subseteq$ inclusion, suppose that $(x_1, \ldots, x_k) \in A$ and consider $i \equiv j$ with $i \neq j$. We need to show that $\theta_i(x_i) = \theta_j(x_j)$. If $s \notin \{i, j\}$ then we have $i \approx j$, but then $(x_1, \ldots, x_{s-1}, x_{s+1}, \ldots, x_k) \in B_s$ shows that $\theta_i(x_i) = \psi_i(x_i) = \psi_j(x_j) = \theta_j(x_j)$. If $s \in \{i, j\}$, we can assume without loss of generality that $i \neq s = j$. Since $(x_2, \ldots, x_k) \in B_1$ and $r \sim s$, we have $\varphi_r(x_r) = \varphi_s(x_s)$ and thus $\theta_s(x_s) = \varphi_s \varphi_r^{-1} \varphi_s(x_s) = \psi_s(x_r)$. Now, $i \equiv s \equiv r$ implies $i \approx r$. As $(x_1, \ldots, x_{s-1}, x_{s+1}, \ldots, x_k) \in B_s$, we therefore have $\psi_i(x_i) = \psi_r(x_r)$. Combining, $\theta_i(x_i) = \psi_i(x_i) = \psi_r(x_r) = \theta_s(x_s)$ and we are through. For the other inclusion, suppose that $(x_1, \ldots, x_k) \in S_X^\equiv(\theta_1, \ldots, \theta_k)$. We have $\psi_i(x_i) = \theta_i(x_i) = \theta_j(x_j) = \psi_j(x_j)$ whenever $i \equiv j$ and $s \notin \{i, j\}$. Hence $(x_1, \ldots, x_{s-1}, x_{s+1}, \ldots, x_k) \in B_s$ and there is some $y \in X$ such that $(x_1, \ldots, x_{s-1}, y, x_{s+1}, \ldots, x_k) \in A$. Then $(x_2, \ldots, x_{s-1}, y, x_{s+1}, \ldots, x_k) \in S_X^\equiv(\theta_1, \ldots, \theta_k)$.
Proposition 3.4, \(A = X\) of \(\equiv\) \(B\).

Let \(X\) be a class of algebras in the same signature. Then, by definition, every \(A \in \text{HSP}(X)\) is a homomorphic image of some \(S \leq \prod_{i \in I} X_i\) for some \(X_i \in X\). If \(A\) is finitely generated then it is a homomorphic image of a finitely generated subalgebra \(S \leq \prod_{i \in I} X_i\).

If \(S(X) = X\), we can consider \(p_i(S) \in X\) instead of \(X_i\) and write \(S \leq \prod_{i \in I} X_i\) for some \(X_i \in X\). Therefore, by Lemma 2.4, if \(S(X) = X\) and every element of \(X\) is finite, then a finitely generated \(A \in \text{HSP}(X)\) is a homomorphic image of a subdirect product of finitely many \(X_i \in X\).

Let \(V_1, V_2\) be two varieties in the same signature. Then \(A \in \bigvee_{i \in I} V_i\) is a homomorphic image of some \(S \leq \prod_{i \in I} X_i\), where \(X_i \in V_j\) if and only if \(i \in I_j\). Using the equivalence relation on \(I_1 \cup I_2\) with equivalence classes \(I_1\) and \(I_2\), Lemma 2.1 then shows that we can write \(S \leq X_1 \times X_2\) for some \(X_i \in V_i\). We will use similar ideas below.

**Lemma 5.1.** Suppose that \(V_1, V_2\) are varieties of loops and let \(A\) a nonabelian simple loop. If \(A \not\in V_1 \cup V_2\) then \(A \not\in \bigvee_{i \in I} V_i\).

**Proof.** Suppose that \(A \not\in V_1 \cup V_2\). By Lemma 2.1, \(A\) is a homomorphic image of a subdirect product of \(X_1 \times X_2\), where \(X_i \in V_i\). By Lemma 3.7, \(A \in \bigvee_{i \in I} V_i\). \( \square \)

Not that for any algebra \(A\), the class \(X\) of all (proper) subalgebras of \(A\) satisfies \(S(X) = X\).

**Theorem 5.2.** Let \(A\) be a nontrivial finite simple loop and let \(V\) be the variety generated by all proper subloops of \(A\). Then \(A \not\in V\).

**Proof.** If \(A\) is abelian then \(V\) is the variety of trivial loops and \(A \not\in V\). Suppose that \(A\) is not abelian and \(A \in V\). Let \(X\) be the set of all proper subloops of \(A\). Since \(A\) is finite, we can assume that \(A \in \text{H}(B)\) for a finitely generated \(B \in \text{SP}(X)\). Any element of \(B(X)\) is of the form \(\prod_{i \in I} X_i\), where each \(X_i\) belongs to \(X\). Since \(X\) is finite, Lemma 2.4 applies and we can assume without loss of generality that \(I\) is finite. Hence \(B \leq \prod_{i \in I} X_i\) for suitable \(X_i \in X\). Let \(k\) be as small as possible. Then \(k \geq 2\) since \(|B| \geq |A| > |X_1|\).

By Lemma 2.1, \(A\) is a homomorphic image of \(X \times Y\), where \(X\) is a subdirect product of \(X_1 \times \cdots \times X_{k-1}\) and \(Y = X_k\). By the definition of \(k\), \(A\) is not a homomorphic image of \(X\). By Lemma 3.7, \(A\) must be a homomorphic image of \(Y\), a contradiction with \(|A| > |X_k|\). \( \square \)
Proposition 5.3. Let $X$ be a nonabelian simple loop, $k$ a positive integer and $\mathcal{V}$ a variety such that $X \notin \mathcal{V}$. Suppose that $Y \in \mathcal{V}$. Then each subdirect product of $\prod_{i=1}^{k+1} X_i$ is isomorphic to $X^{\ell} \times Y$ for some $1 \leq \ell \leq k$.

Proof. Let $X_i = X$ for $1 \leq i \leq k$, $X_{k+1} = Y$ and $A \leq_{sd} \prod_{i=1}^{k+1} X_i$. With $I_1 = \{1, \ldots, k\}$ and $I_2 = \{k+1\}$, Lemma 2.1 implies that $A \leq_{sd} A_{I_1} \times A_{I_2}$ and $A_{I_1} \leq_{sd} X^k$. By Lemma 3.8 and Proposition 4.2, every subdirect product of $X^k$ is isomorphic to $X^{\ell}$. Thus $A$ is (isomorphic to) a subdirect product of $X^{\ell} \times Y$. By Goursat’s Lemma, there are $M \leq X^{\ell}$ and $N \leq Y$ such that $X^{\ell}/M \cong Y/N$. By Lemma 4.1, $M = M_1 \times \cdots \times M_\ell$, where each $M_i \in \{\{e\}, X\}$. Thus $Y/N \cong X^{\ell}/M \cong X^r$ for some $0 \leq r$. If $r > 0$ then $X^r = Y/N \in HSP(Y) \subseteq \mathcal{V}$ and thus $X \in \mathcal{V}$ (using a projection), a contradiction. Hence $r = 0$, $M = X^h$, $N = Y$ and $A$ is isomorphic to $X^{\ell} \times Y$. □

Theorem 5.4. Let $X$ be a finite nonabelian simple loop and let $\mathcal{V}$ be the variety generated by all proper subloops of $X$. Then $X \notin \mathcal{V}$ and each finitely generated loop in $HSP(X)$ is isomorphic to $X^k \times Y$ for some $k \geq 0$ and some finite $Y \in \mathcal{V}$.

Proof. By Theorem 5.2, $X \notin \mathcal{V}$. Let $A$ be a finitely generated loop in $HSP(X)$. By Lemma 2.4, $A$ is a homomorphic image of a subdirect product of $Y_1 \times \cdots \times Y_n$, where each $Y_i$ is a subgroup of $X$. Hence $A$ is a homomorphic image of a subdirect product of $X \times \cdots \times X \times Y = X^k \times Y$, where $k \geq 0$ and $Y$ is a finite loop in $\mathcal{V}$. By Proposition 5.3, $A$ is a homomorphic image of $X^\ell \times Y$, $\ell \leq k$. By Lemma 4.1, $A$ is isomorphic to $X^h \times (Y/N)$, where $h \leq \ell$ and $N \subseteq Y$. □

Theorem 5.5. Let $X$ be a finite nonabelian simple loop. Let $\mathcal{V}_1$ be the variety generated by all proper subloops of $X$ and let $\mathcal{V}_2$ be a variety of loops not containing $X$. Let $A$ be a finitely generated loop contained in $HSP(X) \vee \mathcal{V}_2$. Then there are $k \geq 0$ and a finitely generated loop $Y \in \mathcal{V}_1 \vee \mathcal{V}_2$ such that $A \cong X^k \times Y$.

Proof. By Theorem 5.2, $X \notin \mathcal{V}_1$. Hence $X \notin \mathcal{V}_1 \cup \mathcal{V}_2$, and $X \notin \mathcal{V}_1 \vee \mathcal{V}_2$ by Lemma 5.1. By the assumption, $A$ is a homomorphic image of a subdirect product of $U \times V$, where $U$ is a finitely generated loop in $HSP(X)$ and $V \in \mathcal{V}_2$ is also finitely generated. By Theorem 5.4, $U = X^k \times Y$, where $Y \in \mathcal{V}_1$ is finite. Hence $A$ is a homomorphic image of $B \leq_{sd} Z \times W$, where $Z = X^k$ and $W \in \mathcal{V}_1 \vee \mathcal{V}_2$ is finitely generated. By Goursat’s Lemma, $B$ is a lifted isomorphism graph of some $\varphi: Z/N \rightarrow W/M$. By Lemma 4.1, $Z/N \cong X^r$ for some $r \geq 0$. If $r > 0$ then $X^r = W/M \in \mathcal{V}_1 \vee \mathcal{V}_2$ implies that $X \in \mathcal{V}_1 \vee \mathcal{V}_2$, a contradiction. Hence $r = 0$, $\varphi$ is trivial and $B = X^k \times W$. We are done by Lemma 4.1. □

We now return to propagation of equation in loops.

Theorem 5.6. Let $\mathcal{V}$ be a variety of loops. Let $X$ be a finite loop such that each $Y \leq X$ either belongs to $\mathcal{V}$ or is nonabelian and simple. If an equation $\varepsilon$ propagates in both $X$ and $\mathcal{V}$, then it also propagates in the variety $HSP(X) \vee \mathcal{V}$.

Proof. Let $Y_1, \ldots, Y_m$ be the subloops of $X$ ordered linearly by any extension of the inclusion partial order. For $1 \leq j \leq m$ let $\mathcal{W}_j = HSP(Y_1, \ldots, Y_j) \vee \mathcal{V}$. Note that $\mathcal{W}_1 = \mathcal{V}$ and $\mathcal{W}_m = HSP(X) \vee \mathcal{V}$. We will prove by induction on $1 \leq j \leq m$ that $\varepsilon$ propagates in $\mathcal{W}_j$. Since $\varepsilon$ propagates in $\mathcal{V}$, we can suppose that $j > 1$ and the claim holds for $\mathcal{W}_{j-1}$.

By Lemma 1.4, it suffices to show that $\varepsilon$ propagates in every finitely generated subloop
A of \( \mathcal{W}_j = \text{HSP}(Y_j) \lor \mathcal{W}_{j-1} \). If \( Y_j \in \mathcal{W}_{j-1} \) then \( \mathcal{W}_j = \mathcal{W}_{j-1} \), so we can suppose that \( Y_j \not\in \mathcal{W}_{j-1} \). In particular, \( Y_j \not\in \mathcal{V} \) and \( Y_j \) is therefore nonabelian and simple. Let us apply Theorem 5.5 to \( Y_j \) (in place of \( X \)), the variety \( \mathcal{V}_1 \) generated by all proper subloops of \( Y_j \) and \( \mathcal{V}_2 = \mathcal{W}_{j-1} \). We see that \( \mathcal{A} \cong Y_j^k \times Y \) for some \( k \) and some \( Y \in \mathcal{V}_1 \lor \mathcal{V}_2 \). Now, \( \mathcal{V}_1 \lor \mathcal{V}_2 = \mathcal{W}_{j-1} \) thanks to our ordering of the subloops of \( X \). By Corollary 1.3, \( \varepsilon \) propagates in \( \mathcal{A} \).

**Corollary 5.7.** Let \( \mathcal{V} \) be a variety of loops. Let \( X_1, \ldots, X_n \) be finite loops such that every \( Y \leq X_i \) either belongs to \( \mathcal{V} \) or is nonabelian and simple. If an equation \( \varepsilon \) propagates in \( X_1, \ldots, X_n \) and in \( \mathcal{V} \), then it also propagates in the variety \( \text{HSP}(X_1, \ldots, X_n) \lor \mathcal{V} \).

**Proof.** Let \( \mathcal{V}_i = \text{HSP}(X_1, \ldots, X_i) \lor \mathcal{V} \). By Theorem 5.6, \( \varepsilon \) propagates in \( \mathcal{V}_i \). If \( \varepsilon \) propagates in \( \mathcal{V}_i \), then Theorem 5.6 with \( X = X_{i+1} \) and \( \mathcal{V}_i \) implies that \( \varepsilon \) propagates in \( \mathcal{V}_{i+1} \).

Finally, we consider propagation of associativity in loops.

**Lemma 5.8.** Every loop in which associativity propagates is diassociative.

**Proof.** Let \( X \) be a loop in which associativity propagates and let \( x, y \in X \). Since \( x(ye) = (xy)e \), the subloop \( \langle x, y, e \rangle = \langle x, y \rangle \) is associative. \( \square \)

Let \( \mathcal{A} \) be the variety of abelian groups. As an immediate consequence of Corollary 5.7 we have:

**Corollary 5.9.** Let \( X_1, \ldots, X_n \) be finite loops in which associativity propagates and every \( Y \leq X_i \) is either an abelian group or a nonabelian simple loop. Then associativity propagates in \( \mathcal{V} = \text{HSP}(X_1, \ldots, X_n) \lor \mathcal{A} \). In other words, the Moufang Theorem holds in \( \mathcal{V} \).

### 6 Steiner loops in which associativity propagates

Besides Moufang loops, there are not many classes of diassociative loops that have been investigated. In fact, the only class that comes to mind is that of Steiner loops. In this section we investigate the quasivariety \( S_{[x(yz) = (xy)z]} \) of Steiner loops in which associativity propagates. We start with an easy observation from [5, 8].

**Lemma 6.1.** Associativity propagates in every anti-Pasch Steiner loop.

The following example was found by Michael Kinyon using a guided finite-model builder search. It shows that \( S_{[x(yz) = (xy)z]} \) is not a variety.

**Example 6.2.** Let \( S \) be the Steiner triple system on 13 points \( \{0, \ldots, 9, a, b, c\} \) with blocks given by the columns of

\[
\begin{align*}
000000111122222334445566 \\
1357893469a3457879a568787b \\
246cba578bc6acb98cbb9c9aac \\
\end{align*}
\]

Let \( F \) be the Steiner loop corresponding to \( S \), with identity element \( e \). Let \( f : F \times F \to \mathbb{Z}_2 \) be the loop cocycle with nonzero entries only in positions

\[
\begin{align*}
0011113344589aa \\
569abcab8c6cbbc \\
\end{align*}
\]
where a column with entries $x, y$ indicates that $f(x, y) = f(y, x) = 1$. Finally, let $X = \text{Ext}(\mathbb{Z}_2, F, f)$. Then it can be checked that $X$ is a Steiner loop, $Z(X) = \mathbb{Z}_2 \times \{e\}$, associativity propagates in $X$ (even though $X$ is not anti-Pasch), but associativity does not propagate in $X/Z(X)$.

Corollary 5.9 is a rich source of varieties of loops in which associativity propagates. For instance, both the Steiner loop of order 10 and the unique anti-Pasch Steiner loop of order 16 are nonabelian simple loops whose every proper subloop is abelian. More generally:

Call a Steiner triple system minimal if it has at least four points and each of its proper subsystems consists of at most one block.

**Proposition 6.3.** Let $S$ be a minimal anti-Pasch Steiner triple system. Then the associated Steiner loop $X$ is a nonabelian simple loop whose every proper subloop is abelian.

**Proof.** Let $N$ be a nontrivial normal subloop of $X$. Suppose first that $N = \{e, x\}$ so that $x \in Z(X)$. Let $y, z \in X$ be any nonidentity elements such that $\{x, y, z\}$ is not a block of $S$. Then $x(yz) \neq (xy)z$ because $S$ is anti-Pasch, a contradiction with $x \in Z(X)$. Now suppose that $|N| > 2$. Since $S$ is minimal, we must have $|N| = 4$ and $|X/N| = 4$ as well. By the remarks in the introduction of [13], $S$ is then isomorphic to the unique anti-Pasch Steiner triple system of order 15. An explicit calculation in the GAP [10] package LOOPS [15] shows that $X$ is a nonabelian simple loop whose every proper subloop is abelian. 

**Corollary 6.4.** Let $X_1, \ldots, X_n$ be Steiner loops associated with minimal anti-Pasch Steiner triple systems. Then associativity propagates in $\text{HSP}(X_1, \ldots, X_n) \vee A$.

**Proof.** Combine Corollary 5.9, Lemma 6.1 and Proposition 6.3. 

We conclude the paper with a generalization of a result of Stuhl from [17], where the following definitions can also be found.

Let $S = (X, B)$ denote a Steiner triple system with point set $X$ and blocks $B$. A Steiner triple system $(X, B)$ is oriented if each of its blocks $\{x, y, z\}$ is cyclically ordered, denoted by $(x, y, z)$. We can identify the orientation of an oriented Steiner triple system $(X, B)$ with a function $d : (X \times X) \setminus \{(x, x) : x \in X\} \rightarrow \mathbb{Z}_2 = \{0, 1\}$, where $d(x, y) = 0$ if $(x, y, z)$ is an oriented block and $d(x, y) = 1$ otherwise. In more detail, if $(x, y, z)$ is an oriented block, then $d(x, y) = d(y, z) = d(z, x) = 0$ and $d(y, x) = d(z, y) = d(x, z) = 1$. Note that a Steiner triple system of order $n$ gives rise to $2^{n(n-1)/6}$ oriented Steiner triple systems.

An oriented Steiner quasigroup is a central extension $\text{Ext}(\mathbb{Z}_2, S, f)$, where $S = (X, \cdot)$ is a Steiner quasigroup with orientation function $d$ and $f : X \times X \rightarrow \mathbb{Z}_2$ is any cocycle such that $f(x, y) = d(x, y)$ if $x \neq y$ and $f(x, x) = f(y, y)$ for all $x, y \in X$. Thus an oriented Steiner triple system gives rise to two oriented Steiner quasigroups, depending on the value of $f(x, x) \in \mathbb{Z}_2$. Note that an oriented Steiner quasigroup is not a Steiner quasigroup. Indeed, we have $(a, x) \ast (a, x) = (a + a + f(x, x), xx) = (f(x, x), x)$, so either $(0, x) \ast (0, x) \neq (0, x)$ or $(1, x) \ast (1, x) \neq (1, x)$.

If $\text{Ext}(\mathbb{Z}_2, S, f)$ is an oriented Steiner quasigroup and $L$ is the Steiner loop associated with $S$, then $X = \text{Ext}(\mathbb{Z}_2, L, f)$ will be called an oriented Steiner loop, where we extend the domain of the cocycle $f : S \times S \rightarrow \mathbb{Z}_2$ to $L \times L$ by setting $f(x, e) = f(e, x) = 0$ for every $x \in L$. If $f(x, x) = 0$ for every $x \in S$ then $(a, x) \ast (a, x) = (a + a + f(x, x), xx) = (0, e)$ and $X$ has exponent 2. If $f(x, x) = 1$ for every $x \in S$ then $(a, x)^4 = (0, e)$ no matter how $(a, x)$ is parenthesized and thus $X$ has exponent 4.
Stuhl proved in [17, Theorem 1 and Corollary 2] that an oriented Hall loop satisfies the Moufang Theorem if and only if it is of exponent 4. We generalize her result in Proposition 6.6.

**Lemma 6.5.** Let \( X = \text{Ext}(\mathbb{Z}_2, L, f) \) be an oriented anti-Pasch Steiner loop and let \( d = f(x, x) \) for some (and hence all) \( x \in L \setminus \{e\} \). Then

\[
(a, x) * ((b, y) * (c, z)) = (a, x) * ((b, y) * (c, z))
\]

if and only if one of the following conditions is satisfied:

- \( e \in \{x, y, z\} \),
- \( e \neq x = y \) and \( d = 1 \),
- \( e \neq y = z \) and \( d = 1 \),
- \( x = z \),
- \( \{x, y, z\} \) is a block.

**Proof.** We have \( (a, x) * ((b, y) * (c, z)) = (a, x) * ((b, y) * (c, z)) \) if and only if both

\[
xy \cdot z = x \cdot yz, \tag{6.1}
\]

\[
f(x, y) + f(xy, z) = f(x, yz) + f(y, z) \tag{6.2}
\]

hold. If \( e \in \{x, y, z\} \) then both conditions hold, so we can assume from now on that \( e \notin \{x, y, z\} \).

If \( x = y \) or \( y = z \) or \( x = z \) then (6.1) holds. Note that if \( x = y = z \) then (6.2) reduces to \( f(x, x) + f(e, z) = f(x, xz) + f(x, z) \). Whether \( (x, z, xz) \) is a block or \( (x, xz, z) \) is a block, the right hand side reduces to 1, so the three elements associate if and only if \( d = 1 \). Similarly, if \( y = z \) then (6.2) becomes \( f(x, y) + f(xy, y) = f(x, e) + f(y, y) = d \) and the left hand side is equal to 1 whether \( (x, y, xy) \) is a block or \( (x, xy, y) \) is a block. Finally, if \( x = z \) then (6.2) becomes \( f(x, y) + f(xy, x) = f(x, yx) + f(y, x) \), which holds whether \( (x, y, xy) \) is a block or \( (x, xy, y) \) is a block.

We can therefore assume that \( \{x, y, z\} \setminus \{e\} = 3 \). If \( \{x, y, z\} \) is a block then we can take \( z = xy \), (6.1) holds and (6.2) becomes \( f(x, y) + f(xy, xy) = f(x, x) + f(y, xy) \), which holds whether \( (x, y, xy) \) is a block or \( (x, xy, y) \) is a block. If \( \{x, y, z\} \) is not a block then \( xy \cdot z \neq x \cdot yz \) because \( L \) is anti-Pasch. \( \square \)

**Proposition 6.6.** Let \( X \) be an oriented anti-Pasch Steiner loop. Then associativity propagates in \( X \) if and only if \( X \) has exponent 4.

**Proof.** Let \( X = \text{Ext}(\mathbb{Z}_2, L, f) \) for some anti-Pasch Steiner loop \( L \) and let \( d = f(x, x) \) for some \( x \in L \setminus \{e\} \). Note that if \( x \neq y \) are nonidentity elements of \( L \), then \( \mathbb{Z}_2 \times \{e, x, y, xy\} \) is a group if and only if \( d = 1 \), by Lemma 6.5.

Suppose now that \( ((a, x) * (b, y)) * (c, z) = (a, x) * ((b, y) * (c, z)) \) for some elements of \( X \). In all five cases of Lemma 6.5, we can choose \( u, v \in L \) so that \( ((a, x), (b, y), (c, z)) \leq \mathbb{Z}_2 \times \{e, u, v, uv\} \). Hence, if \( d = 1 \) then associativity propagates in \( X \). If \( d = 0 \), consider any nonidentity elements \( x \neq y \in L \). By Lemma 6.5, \( (0, x) * ((0, x) * (0, y)) \neq ((0, x) * (0, x)) * (0, y) \) and \( X \) is not diassociative. We are done by Lemma 5.8. \( \square \)
7 Open problems

We start with concrete problems concerning propagation of associativity in Steiner loops.

**Problem 7.1.** Let $X$ be an oriented anti-Pasch Steiner loop as in Proposition 6.6. Does associativity propagate in the variety generated by $X$ if $X$ has exponent 4?

We conjecture that the answer to Problem 7.1 is positive if the underlying anti-Pasch Steiner triple system is minimal. To prove this, the theory built in this paper might have to be generalized to cover loops with an abelian Frattini subloop $F$ such that the factor modulo $F$ is finite and simple.

By Example 6.2, there exists a Steiner loop $X$ of order 28 such that associativity propagates in $X$ but not in $H(X)$.

**Problem 7.2.** What is the smallest order of a Steiner loop $X$ such that associativity propagates in $X$ but not in $H(X)$?

The same example shows that a Steiner loop in which associativity does not propagate might be a factor of a Steiner loop in which associativity propagates.

**Problem 7.3.** Is it true that for every Steiner loop $F$ (in which associativity does not propagate) there exists a Steiner loop $X$ in which associativity propagates and $F \in H(X)$?

By Corollary 5.9, if associativity propagates in a Steiner loop $X$ and all subloops of $X$ are either abelian or nonabelian simple, then it propagates in $HSP(X)$, too.

**Problem 7.4.** Characterize the class of Steiner loops $X$ for which associativity propagates in $HSP(X)$.

We now turn to more general questions concerning propagation of equations. These can be seen as suggestions for research programs. Recall that

$$V_{[\varepsilon]} = \{ X \in V : \varepsilon \text{ propagates in } X \}.$$ 

**Question 7.5.** Given an equation $\varepsilon$ and a variety $V$, when is the propagating core $V_{[\varepsilon]}$ a variety? If $V_{[\varepsilon]}$ is a variety, is it finitely based relative to $V$?

**Question 7.6.** If $\varepsilon$ propagates in $X$, under which conditions does $\varepsilon$ propagate in $HSP(X)$?

**Question 7.7.** Let $V_i$, $i \in I$, be varieties in which $\varepsilon$ propagates. Under which conditions does $\varepsilon$ propagate in the join $\bigvee_{i \in I} V_i$?

**Question 7.8.** Given an equation $\varepsilon$ and a variety $V$, under which conditions is $V \subseteq H(V_{[\varepsilon]})$?

**Question 7.9.** Given an equation $\varepsilon$ and a variety $V$, is there an algebra $X \in V$ such that $H(X) \subseteq V_{[\varepsilon]}$ but $HSP(X) \not\subseteq V_{[\varepsilon]}$?

Answering Question 7.9 for a given $\varepsilon$ and $V$ might not be difficult but it might be technically complicated. A possible strategy is to first find $Y, Z$ such that $Y \in V_{[\varepsilon]}$, $Z \in H(Y)$ but $Z \not\in V_{[\varepsilon]}$, then embed $Y$ into a simple algebra $X \in V_{[\varepsilon]}$. Then $H(X) \subseteq V_{[\varepsilon]}$ by simplicity but $Z \in HS(X) \not\subseteq V_{[\varepsilon]}$. 
References


