Products of all elements in a loop and a framework for non-associative analogues of the Hall-Paige conjecture

Kyle Pula
Department of Mathematics
University of Denver, Denver, CO, USA
jpula@math.du.edu

Submitted: Jul 11, 2008; Accepted: Apr 26, 2009; Published: May 11, 2009
Mathematics Subject Classification: 05B15, 20N05

Abstract

For a finite loop Q, let $P(Q)$ be the set of elements that can be represented as a product containing each element of Q precisely once. Motivated by the recent proof of the Hall-Paige conjecture, we prove several universal implications between the following conditions:

(A) Q has a complete mapping, i.e. the multiplication table of Q has a transversal,

(B) there is no $N \trianglelefteq Q$ such that $|N|$ is odd and $Q/N \cong \mathbb{Z}_{2^m}$ for $m \geqslant 1$, and

(C) $P(Q)$ intersects the associator subloop of Q.

We prove $(A) \implies (C)$ and $(B) \iff (C)$ and show that when Q is a group, these conditions reduce to familiar statements related to the Hall-Paige conjecture (which essentially says that in groups $(B) \implies (A)$). We also establish properties of $P(Q)$, prove a generalization of the Dénes-Hermann theorem, and present an elementary proof of a weak form of the Hall-Paige conjecture.

1 Background

As the present work is motivated by the search for non-associative analogues of the well-known Hall-Paige conjecture in group theory, we begin with a brief historical sketch of this topic. As the culmination of over 50 years of work by many mathematicians, the following theorem seems now to have been established.

Theorem 1.1. *If G is a finite group, then the following are equivalent:*

(1) *G has a complete mapping, i.e. the multiplication table of G has a transversal,*

(2) *Sylow 2-subgroups of G are trivial or non-cyclic, and*

(3) *there is an ordering of the elements of G such that $g_1 \cdots g_n = 1$.*

The history of Theorem 1.1 dates back at least to a result of Paige from 1951 in which he proves (1) $\implies$ (3) [15]. In 1955 Hall and Paige proved that for all finite groups (1) $\implies$ (2) and that for solvable, symmetric, and alternating groups the converse holds as well. They conjectured that the converse holds in all finite groups, and this claim came to be known as the Hall-Paige conjecture [13].

In 1989 Dènes and Keedwell noted that condition (2) holds in all non-solvable groups and proved that condition (3) does as well [8]. Combining the above results, they observed that the Hall-Paige conjecture was thus equivalent to the statement that non-solvable groups have complete mappings, and many authors have since contributed to the effort of demonstrating such complete mappings. Evans provides an excellent survey of this progress up to 1992 in [11] and of the more recent progress in [12]. Jumping ahead to the most recent developments (consult the previous references for complete details), Wilcox improved on earlier results to show that a minimal counterexample to the Hall-Paige conjecture must be simple and reduced the number of candidates to the Tits group or a sporadic simple group (some of which were already known to have complete mappings) [22]. The closing work on these efforts was completed by Bray and Evans who demonstrated complete mappings in J_4 and all remaining cases, respectively [1, 12].

We would like to consider the Hall-Paige conjecture in more general varieties of loops, and this paper takes on the modest goal of making sense of conditions (1), (2), and (3) of Theorem 1.1 in non-associative settings. While (1) translates directly, (2) and (3) present difficulties since it is not clear what a Sylow 2-subloop should be and any product in a non-associative loop requires the specification of some association.

The primary contribution of this paper is to propose natural generalizations of these conditions and establish several universal implications between them. As detailed in §2, we prove a number of related results including a generalization of the Dénes-Hermann theorem and provide an elementary proof of a weak form of the Hall-Paige conjecture.

We begin with a minimal background on the theories of latin squares and loops.

1.1 Latin squares

A *latin square of order* n is an $n \times n$ array whose entries consist of n distinct symbols such that no symbol appears as an entry twice in a row or column. More formally, a Latin square L on a finite set of symbols S is a subset of S^3 such that the projection along any pair of coordinates is a bijection. When the triple $(x, y, z) \in L$, we say that the symbol x appears as a row, y as a column, and z as an entry.

A *k-plex* is a subset of L in which each symbol appears as a row, column, and entry precisely k times. A 1-plex is called a *transversal* and a k-plex with k odd is called an odd-plex. For the theory and history of k-plexes, consult [4, 10, 20, 21].

We introduce the following generalizations of the concepts of transversals and k-plexes. A *row k-plex* of L is a collection of triples representing each row precisely k times. We call a subset $C = \{(x_i, y_i, z_i) : 1 \leqslant i \leqslant m\} \subseteq L$ *column-entry regular*, or just *regular* for short, if for each symbol s we have $|\{i : y_i = s\}| = |\{i : z_i = s\}|$. That is, s appears as an entry the same number of times it appears as a column. We denote by C_r the multiset of symbols appearing as rows in C. For example, if C is a k-plex, then C_r contains precisely k copies of each symbol. We will be primarily interested in regular row transversals, i.e. selections of a single triple from each row so that each symbol appears as a column the same number of times as an entry (Figure 1 depicts such a selection in the multiplication table of a loop).

1.2 Loops

A set with a binary operation, say $(Q, \cdot)$, is a *loop* if for each $x, z \in Q$, the equations $x \cdot y_1 = z$ and $y_2 \cdot x = z$ have unique solutions $y_1, y_2 \in Q$ and $(Q, \cdot)$ has a neutral element (which we always denote 1). A *group* is a loop in which the associativity law holds. We assume in all cases that Q is finite and typically write Q rather than $(Q, \cdot)$.

The *left*, *right*, and *middle inner mappings* of a loop are defined as $L(x, y) = L_{yx}^{-1} L_y L_x$, $R(x, y) = R_{xy}^{-1} R_y R_x$, and $T(x) = R_x^{-1} L_x$, respectively. A subloop S of a loop Q is said to be *normal*, written $S \trianglelefteq Q$, if S is invariant under all inner mappings of Q. A loop Q is *simple* if it has no normal subloops except for $\{1\}$ and Q. This definition of normality is equivalent to what one would expect from the standard universal algebraic definition. In fact, just as with groups, loops can be defined more formally as universal algebras though we have not elected to do so here.

We write $A(Q)$ for the associator subloop of Q, the smallest normal subloop of Q such that $Q/A(Q)$ is a group. Likewise, we write Q' for the derived subloop of Q, the smallest normal subloop of Q such that Q/Q' is an Abelian group. Note that $A(Q) \trianglelefteq Q'$ and thus cosets of Q' are partitioned by cosets of $A(Q)$. When Q is a group, $A(Q) = \{1\}$.

The *multiplication table* of a loop Q is the set of triples $\{(x, y, xy) : x, y \in Q\}$. Multiplication tables of loops are latin squares and, up to the reordering of rows and columns, every latin square is the multiplication table of some loop. It thus makes sense to say that a loop has a k-plex or more generally a regular row k-plex whenever its multiplication table does.

Most literature on the Hall-Paige conjecture focuses on the concept of a complete mapping of a group rather than a transversal of its multiplication table, though the two are completely equivalent [9, p. 7]. In the general loop setting, we prefer the latter concept as it emphasizes the combinatorial nature of the problem and generalizes more naturally to the concepts of k-plexes and regular k-plexes.

For $H \subseteq Q$ and $k \geqslant 1$, let $P^k(H)$ be the set of elements in Q that admit factorizations containing every element of H precisely k times. We call these elements *full k-products of H*. When $k = 1$, we write just $P(H)$ and refer to its elements as *full products of H*. We work primarily in the case $H = Q$ and simply refer to these elements as *full k-products*. While in the group case, the set $P(G)$ has been well-studied (see the commentary preceding Theorem 2.3 for some background), to the best of our knowledge, the present article contains the first investigation of the general loop case.

Although we assume a basic familiarity with both loops and latin squares, we provide references for any non-trivial results that we employ. For standard references on latin squares consult Dénes and Keedwell [7, 9] and for loops Bruck [2] and Pflugfelder [16].

2 Summary of Results

We propose the following conditions as fruitful interpretations of (1), (2), and (3) of Theorem 1.1 in varieties of loops in which associativity need not hold.

Definition 2.1 (HP-condition)**.** We say a class of loops $\mathcal{Q}$ satisfies the *HP-condition* if for each $Q \in \mathcal{Q}$ the following are equivalent:

(A) Q has a transversal,

(B) there is no $N \trianglelefteq Q$ such that $|N|$ is odd and $Q/N \cong \mathbb{Z}_{2^m}$ for $m \geqslant 1$, and

(C) $A(Q)$ intersects $P(Q)$.

When $\mathcal{Q}$ is the variety of groups, satisfaction of the HP-condition reduces to Theorem 1.1. The equivalence of (1) and (A) is clear; as is that of (3) and (C), given that when Q is a group, $A(Q) = \{1\}$. We take an indirect approach to showing (2) $\iff$ (B) by showing (B) $\iff$ (C), a corollary of Theorems 2.4 and 2.5. In 2003, Vaughan-Lee and Wanless gave the first elementary proof of (2) $\iff$ (3). Their paper also provides some background on this result (whose initial proof invoked the Feit-Thompson theorem) [18]. As corollaries of our main results, we show that in all loops (B) $\iff$ (C) and (A) $\implies$ (C).

The following easy observation sets the context for our main results. It is well-known in the group case and follows in the loop case for the same simple reasons. We include it as part of Lemma 3.1 for completeness.

Observation 2.2. *$P^k(Q)$ is contained in a single coset of Q'.*

At least as far back as 1951, authors have asked whether, in the group case, this observation can be extended to show that $P^k(Q)$ in fact coincides with this coset. For a history of this line of investigation, see [7, p. 35] and [9, p. 40]. This result now bears the names of Dénes and Hermann who first established the claim for all groups.

Theorem 2.3 (Dénes, Hermann [6] 1982)**.** *If G is a group, then $P(G)$ is a coset of G'. It follows that $P^k(G)$ is also a coset of G'.*

An admittedly cumbersome but more general way to read this statement is that $P(G)$ intersects every coset of $A(G)$ that is contained in the relevant coset of G'. Since $A(G) = \{1\}$ and these cosets partition cosets of G', this technical phrasing reduces to the theorem as stated. We extend the Dénes-Hermann theorem to show that this more general phrasing holds in all loops. Although the result is more general, our proof of Theorem 2.4 relies essentially upon the Dénes-Hermann theorem. In §7, we discuss prospects of a further generalization.

Theorem 2.4. *If $P(Q) \subseteq xQ'$, then $P(Q) \cap yA(Q) \neq \emptyset$ for all $y \in xQ'$. That is, $P(Q)$ intersects every coset of $A(Q)$ contained in xQ' and, in particular, if $P(Q) \subseteq Q'$, then $P(Q)$ intersects $A(Q)$. It follows that $P^k(Q)$ also intersects every coset of $A(Q)$ in the corresponding coset of Q'.*

Coupled with Theorem 2.4, our next result establishes (B) $\iff$ (C).

Theorem 2.5. *$P(Q) \subseteq Q'$ if and only if (B) holds.*

In 1951, Paige showed that if a group G has a transversal, then $1 \in P(G)$ [15]. We extend this result to a much wider class of structures.

Theorem 2.6. *If C is a regular subset of the multiplication table of Q, then $P(C_r)$ intersects $A(Q)$. In particular, if Q has a k-plex (or just a regular row k-plex), then $P^k(Q)$ intersects $A(Q)$.*

Applying these results, we establish that for all loops:

- (A) $\implies$ (C) by Theorem 2.6 and
- (B) $\iff$ (C) by Theorems 2.4 and 2.5.

By 1779, Euler had shown that a cyclic group of even order has no transversal and in 1894 Maillet extended his argument to show that all loops for which condition (B) fails lack transversals [7, p. 445]. In 2002, Wanless showed that such loops lack not just transversals, i.e. 1-plexes, but contain no odd-plexes at all [20]. While their arguments are quite nice, our proof of (A) $\implies$ (B) provides an alternative, more algebraic proof of these results.

Corollary 2.7. *If a loop fails to satisfy (B), then it has no regular row odd-plexes.*

It is not true in general that (B) $\wedge$ (C) $\implies$ (A) (for a smallest possible counter-example, see Figure 1). In a separate paper still in preparation, we show that this implication holds in several technical varieties of loops that include non-associative members and provide both computational and theoretical evidence suggesting that it may hold in the well-known variety of Moufang loops as well [17].

Q	1	2	3	4	5	6
1	[1]	2	3	4	5	6
2	2	1	4	[3]	6	5
3	3	5	[1]	6	2	4
4	[4]	6	2	5	1	3
5	5	3	6	2	4	[1]
6	[6]	4	5	1	3	2

Figure 1: Loop Q with no transversal and yet $P(Q) = Q' = Q$. Q contains 168 regular row transversals, one of which has been bracketed.

The equivalent statements in Theorem 1.1 are typically stated with the additional claim that G can be partitioned into n mutually disjoint transversals, i.e. G has an orthogonal mate. In the group case, it is easy to show that having an orthogonal mate is equivalent to having at least one transversal. While this equivalence may extend to other varieties of loops (this question for Moufang loops is addressed directly in [17]), the argument seems unrelated to the most difficult part of Theorem 1.1 (that (2) $\implies$ (1)).

We do however introduce a weakening of the orthogonal mate condition in the following theorem. While this result follows directly from a combination of Theorems 1.1 and 2.6, we provide an elementary proof (in particular, we avoid the classification of finite simple groups).

Theorem 2.8. *If G is a group of order n, then the following are equivalent:*

(i) *G has a regular row transversal,*

(ii) *G can be partitioned into n mutually disjoint regular row transversals,*

(iii) *Sylow 2-subgroups of G are trivial or non-cyclic, and*

(iv) $1 \in P(G)$.

Corollary 2.9. *Theorem 1.1 is equivalent to the claim that a group has a transversal if and only if it has a regular row transversal.*

We make the following two observations not to suggest that our methods may be useful in tackling these important problems but rather to indicate their theoretical context.

Observation 2.10. *When $\mathcal{Q}$ is the class of odd ordered loops, condition (B) always holds and thus the implication $(A) \implies (B)$ is equivalent to Ryser's conjecture, that every latin square of odd order has a transversal [5].*

A natural question might be whether Q has a 2-plex if and only if $A(Q)$ intersects $P^2(Q)$. Since this latter condition is satisfied in all loops, an affirmative answer to this question is equivalent to a conjecture attributed to Rodney, that every latin square has a 2-plex [5, p. 105].

3 Properties of the sets $P^k(Q)$

We begin with a sequence of easy observations about the sets $P^k(Q)$.

Lemma 3.1. *For $i, j, k \geqslant 1$,*

(i) $1 \in P^2(Q)$,

(ii) $P^i(Q)P^j(Q) \subseteq P^{i+j}(Q)$ *and* $|P^k(Q)| \leqslant |P^{k+1}(Q)|$,

(iii) $P^k(Q)$ *is contained in a coset of* Q',

(iv) $P^k(Q) \subseteq P^{k+2}(Q)$,

(v) $P^2(Q) \subseteq Q'$, *and*

(vi) $P(Q) \subseteq aQ'$ *where* $a^2 \in Q'$.

Proof. (i) Let q^ρ be the right inverse of q. Then $1 = \prod_{q \in Q} qq^\rho \in P^2(Q)$.

(ii) Observe that $P^i(Q)P^j(Q) = \{ab : a \in P^i(Q), b \in P^j(Q)\}$. Thus ab is a full $(i+j)$-product. It then follows that $|P^k(Q)| \leqslant |P^{k+1}(Q)|$ since for $q \in P(Q)$, $qP^k(Q) \subseteq P^{k+1}(Q)$ and $|P^k(Q)| = |qP^k(Q)|$.

(iii) Any two elements of $P^k(Q)$ have factors that differ only in their order and association. In other words, if $x, y \in P^k(Q)$, then $xQ' = yQ'$.

(iv) By (i), we have $1 \in P^2(Q)$; thus $P^k(Q) = P^k(Q) \cdot 1 \subseteq P^k(Q)P^2(Q)$. By (ii) we have $P^k(Q)P^2(Q) \subseteq P^{k+2}(Q)$. Thus $P^k(Q) \subseteq P^{k+2}(Q)$.

(v) The claim follows immediately from (i) and (iii).

(vi) By (iii), $P(Q) \subseteq aQ'$ for some $a \in Q$ and thus $P(Q)^2 \subseteq a^2Q'$. By (ii), $P(Q)^2 \subseteq P^2(Q)$ and by (v) $P^2(Q) \subseteq Q'$. It follows that $a^2Q' = Q'$ and thus $a \in Q'$. □

Our next lemma uses the idea that Q/N is a set of cosets of N and thus $P(Q/N)$ is a subset of these cosets.

Lemma 3.2. *If $N \trianglelefteq Q$, $|N| = k$, and $a_1N, \ldots, a_kN \in P(Q/N)$, then*

$$P(Q) \cap (a_1N \cdots a_kN) \neq \emptyset.$$

That is, $P(Q)$ intersects every member of $P(Q/N)^k$.

Proof. Let $|Q| = mk$. For any $aN \in P(Q/N)$, we may select a system of coset representatives of N in Q, say $\{x_1, \ldots, x_m\}$, and some association of the left hand side such that

$$x_1N \cdots x_mN = aN \tag{1}$$

and thus using the same association pattern $x_1 \cdots x_m \in aN$. Furthermore, since (1) depends only on the order and association of the cosets of N (rather than the specific representatives chosen), we may select k disjoint sets of coset representatives of N in Q, say $\{x_{(i,1)}, \ldots, x_{(i,m)} : 1 \leqslant i \leqslant k\}$, and corresponding association patterns such that

$$(x_{(1,1)} \cdots x_{(1,m)}) \cdots (x_{(k,1)} \cdots x_{(k,m)}) \in a_1N \cdots a_kN \in P(Q/N)^k$$

for any selection of $a_iN \in P(Q/N)$ for $1 \leqslant i \leqslant k$. Having selected each element of Q as a coset representative precisely once, the left-hand side falls in $P(Q)$ and we are done. □

4 Theorem 2.6

For $x \in Q$, we write L_x (R_x) for the left (right) translation of Q by x. Our notation for the left translation is not to be confused with the convention of using L for a latin square. The latter usage appears only in our introduction. In any case, the meaning is always made clear by the context.

The *multiplication group of* Q, written $\mathrm{Mlt}(Q)$, is the subgroup of the symmetric group S_Q generated by all left and right translations, i.e. $\langle L_x, R_x : x \in Q\rangle$, while the *left* *multiplication group of* Q, written $\mathrm{LMlt}(Q)$, is generated by all left translations. If $H \trianglelefteq Q$ and $\rho \in \mathrm{Mlt}(Q)$, we may define the map $\rho_H(xH) := \rho(x)H$, which is said to be induced by ρ. It is straightforward to verify that the map is well-defined and that $\rho_H \in \mathrm{Mlt}(Q/H)$.

To prove Theorem 2.6 in the group case one would like to use the fact that from an identity like

$$a_1(a_2(\cdots(a_kx)\cdots) = x$$

we may conclude that $a_1(a_2(\cdots(a_k)\cdots) = 1$, which is trivial in the presence of associativity but typically false otherwise. In the general loop case, the following lemma shows we can at least conclude that

$$a_1(a_2(\cdots(a_k)\cdots) \in A(Q).$$

Lemma 4.1.

(i) If $\rho \in LMlt(Q)$, then $\rho_{A(Q)} = L_{\rho(1)A(Q)}$.

(ii) If $\rho \in Mlt(Q)$, then $\rho_{Q'} = L_{\rho(1)Q'}$.

(iii) Since they are left translations, $\rho_{A(Q)}$ and $\rho_{Q'}$ are constant if and only if they have fixed points.

(iv) If $a_1(a_2(\cdots(a_kx)\cdots) = x$, then $a_1(a_2(\cdots(a_k)\cdots) \in A(Q)$.

Proof. Set $A := A(Q)$.

(i) Let $\rho = L_{a_1}\cdots L_{a_k}$. Then $\rho_A(qA) = a_1(a_2\cdots(a_kq)\cdots)A$. Since Q/A is a group, we may reassociate to get $\rho_A(qA) = a_1(a_2\cdots(a_k)\cdots)A \cdot qA = \rho(1)A\cdot qA$. Thus $\rho_A = L_{\rho(1)A}$.

(ii) Let $\rho = T^{\epsilon_1}_{a_1}\cdots T^{\epsilon_k}_{a_k}$ where $T^{\epsilon_i} \in \{L, R\}$. Since Q/Q' is an Abelian group, we may reassociate and commute to get $\rho_{Q'}(qQ') = a_1(a_2\cdots(a_k)\cdots)Q'\cdot qQ' = \rho(1)Q'\cdot qQ'$. Thus $\rho_{Q'} = L_{\rho(1)Q'}$.

(iii) Since $\rho_{A(Q)}$ is a left translation, if it has a fixed point, it is constant. Likewise for $\rho_{Q'}$.

(iv) Let $\rho(z) := a_1(a_2(\cdots(a_kz)\cdots)$. Since $\rho_A(xA) = \rho(x)A = xA$, it is constant by (iii). Thus $\rho_A(A) = A$ and in particular $\rho(1) = a_1(a_2(\cdots(a_k)\cdots) \in A$. □

Lemma 4.1 is stated somewhat more generally then we actually need. If the translation notation feels cumbersome, the idea is very basic. Given the product $a_1(a_2(\cdots(a_kx)\cdots) = x$, we may reduce both sides mod A to get

$$\begin{aligned} a_1Aa_2A\cdots a_kAxA &= xA \\ a_1Aa_2A\cdots a_kA &= 1A \\ a_1a_2\cdots a_k &\in A. \end{aligned}$$

Lemma 4.2. *If $C \neq \emptyset$ is regular, then there exists C' such that*

(i) $\emptyset \neq C' \subseteq C$,

(ii) $P(C'_r)$ *intersects* $A(Q)$*, and*

(iii) $C \setminus C'$ *is regular (and possibly empty).*

It follows that $P(C_r)$ *intersects* $A(Q)$*.*

Proof. Let $[k] := \{1, \ldots, k\}$. Suppose $C = \{(x_i, y_i, z_i) : i \in [k]\}$ is regular. Select $i_1 \in [k]$ at random. Having selected $i_1, \cdots, i_m \in [k]$, pick $i_{m+1} \in [k]$ such that $y_{i_m} = z_{i_{m+1}}$. Since C is regular, such a selection can always be made. If $i_{m+1} \notin \{i_1, \ldots, i_m\}$, continue.

Otherwise, stop and consider the set $\{i_j, \ldots, i_m\}$ where $i_j = i_{m+1}$. Reindex C such that $\langle i_j, \ldots, i_m \rangle = \langle 1, \cdots, s \rangle$ and set $C' := \{(x_i, y_i, z_i) : 1 \leqslant i \leqslant s\}$. Note that $y_s = z_1$. By construction, C' has the following form:

$$\begin{aligned} C' = \{&(x_1, y_1, y_s), \\ &(x_2, y_2, y_1), \\ &(x_3, y_3, y_2), \\ &\cdots \\ &(x_{s-1}, y_{s-1}, y_{s-2}), \\ &(x_s, y_s, y_{s-1})\}. \end{aligned}$$

C' is clearly regular and thus so too is $C \setminus C'$. Furthermore, by construction we have

$$x_1(x_2(\cdots(x_s z_1)\cdots)) = z_1.$$

By Lemma 4.1, $x_1(x_2(\cdots(x_s)\cdots)) \in A(Q)$. Since this product is in $P(C'_r)$ as well, $P(C'_r) \cap A(Q) \neq \emptyset$. Iterating this construction we have $P(C_r)$ intersects $A(Q)$. $\square$

Proof of Theorem 2.6. If C is a k-plex, then C_r consists of k copies of each element of Q and thus $P(C_r) = P^k(Q)$. By Lemma 4.2, $P^k(Q)$ intersects $A(Q)$. $\square$

5 Theorem 2.8

Lemma 5.1. *If* G *is a group and* $g_1, \ldots, g_k \in G$ *such that* $g_1 \cdots g_k = 1$ *and no proper contiguous subsequence evaluates to 1, then* G *admits a regular set* C *such that* $C_r = \{g_1, \ldots, g_k\}$ *and no column (and thus no entry) is selected more than once.*

Proof. Set $h_i := g_{i+1} \cdots g_k$ for $1 \leqslant i \leqslant k-1$ and $h_0 = h_k := 1$. Note that we have $g_i h_i = h_{i-1}$ for $1 \leqslant i \leqslant k$. We claim that $C := \{(g_i, h_i, h_{i-1}) : 1 \leqslant i \leqslant k\}$ is the desired regular set. It is clear that C is regular and that $C_r = \{g_1, \ldots, g_k\}$. To see that no column is selected more than once, suppose that $h_i = h_{i+j}$ for $j \geqslant 1$. That is, $g_{i+1} \cdots g_k = g_{i+j+1} \cdots g_k$. Canceling on the right, we have $g_{i+1} \cdots g_{i+j} = 1$, a contradiction. $\square$

Proof of Theorem 2.8.
(i) $\Longrightarrow$ (ii) Here we may use the standard argument from the group case showing that a single transversal extends to n disjoint transversals. Let $T = \{(x_i, y_i, z_i) : 1 \leqslant i \leqslant n\}$

be a regular row transversal of G. For each $g \in G$, form $T_g := \{(x, yg, zg) : (x, y, z) \in T\}$. It is easy to check that the family $\{T_g : g \in G\}$ partitions the multiplication table of G into regular row transversals.

(i) $\Longleftarrow$ (ii) If G admits a partition into regular row transversals, then it certainly has a regular row transversal.

(i) $\Longrightarrow$ (iv) Let T be a regular row transversal. By Theorem 2.6, $P(G) \cap A(G) \neq \emptyset$ and thus $1 \in P(G)$.

(i) $\Longleftarrow$ (iv) Let $g_1 \cdots g_n = 1$. We partition G as follows:

- If no proper contiguous subsequence of $g_1 \cdots g_n$ evaluates to 1, stop.
- Otherwise, extract the offending subsequence $g_i \cdots g_j = 1$ and note that

$$g_1 \cdots g_{i-1} g_{j+1} \cdots g_n = 1.$$

- Iterate this process with these shortened products.

Suppose we have thus partitioned G into k disjoint sequences $\{g_{(i,1)}, \ldots, g_{(i,n_i):1 \leqslant i \leqslant k}\}$ such that $g_{(i,1)} \cdots g_{(i,n_i)} = 1$ for $1 \leqslant i \leqslant k$ and no proper contiguous subsequence of $g_{(i,1)}, \ldots, g_{(i,n_i)}$ evaluates to 1. Now we apply Lemma 5.1 to each subsequence to get regular sets C_i for $1 \leqslant i \leqslant k$. Then $\bigcup_{i=1}^{k} C_i$ is a regular row transversal of G.

(iii) $\Longleftrightarrow$ (iv) As noted earlier, this is an established equivalence in the Hall-Paige conjecture. □

6 Theorem 2.5

Lemma 6.1. (2) $\Longleftrightarrow$ (3) *holds for Abelian groups.*

Proof. As mentioned above, Vaughan-Lee and Wanless give a direct, elementary proof of this result for all groups [18]. For an earlier though indirect proof, Paige showed that (1) $\Longleftrightarrow$ (2) holds in Abelian groups [14] and Hall and Paige showed that (1) $\Longleftrightarrow$ (3) in solvable groups [13]. □

Lemma 6.2. *If a group G has a cyclic Sylow 2-subgroup S, then there exists $N \trianglelefteq G$ such that $G/N \cong S$.*

Proof. This is a direct application of Burnside's Normal Complement theorem that can be found in most graduate level group theory texts (see [24] for example). □

Proof of Theorem 2.5. ($\Longleftarrow$) We show the contrapositive. Suppose $P(Q) \subseteq aQ' \neq Q'$. Since $G := Q/Q'$ is an Abelian group, $P(G) = \{bQ'\}$ such that $b^2 \in Q'$. By Lemma 3.2, $P(Q)$ intersects every element of $P(G)^{|Q'|} = \{b^{|Q'|}Q'\}$ and therefore $aQ' = b^{|Q'|}Q'$. Since $aQ' \neq Q'$ and $b^2 \in Q'$, it follows that $aQ' = bQ'$ and $|Q'|$ is odd.

Since $P(G) \neq \{1Q'\}$, by Lemmas 6.1 and 6.2 there is $N \trianglelefteq G$ such that $|N|$ is odd and $G/N \cong \mathbb{Z}_{2^m}$. N is a collection of coset of Q'. Letting H be their union, we have $Q/H \cong G/N \cong \mathbb{Z}_{2^m}$ and $|H| = |N||Q'|$ is odd.

($\Longrightarrow$) Again we argue the contrapositive. Suppose $N \trianglelefteq Q$ such that $|N| = q$ is odd and $Q/N \cong \mathbb{Z}_{2^m}$ for $m \geqslant 1$. Since $Q/N \cong \mathbb{Z}_{2^m}$, $P(Q/N) = \{aN\} \neq \{N\}$ such that $a^2 \in N$. By Lemma 3.2, $P(Q)$ intersects every element of $P(Q/N)^{|N|} = \{aN\}^{|N|} = \{aN\}$.

Given that Q/N is an Abelian group, $Q' \subseteq N$ but since $P(Q)$ intersects $aN \neq N$, it is therefore disjoint from Q'. □

7 Theorem 2.4

An *A-loop* is a loop in which all inner mappings are automorphisms. The variety of A-loops is larger than that of groups but is certainly not all loops. Bruck and Paige conducted the earliest extensive study of A-loops [3].

Before proving Theorem 2.4, we make several additional observations about the sets $P^k(Q)$. While none of these results will be used directly in our proof, we hope they are of some interest in that they may suggest an alternative proof of the Dénes-Hermann theorem.

Lemma 7.1. *Set* $P^\omega := \bigcup_{i=1}^{\infty} P^i(Q)$.

(i) $P^\omega \leqslant Q$,

(ii) $P^\omega = P^k(Q) \cup P^{k+1}(Q)$ *for sufficiently large* k,

(iii) If $P^\omega \trianglelefteq Q$, *then* $P^\omega = Q'$ *or* $P^\omega = Q' \cup aQ'$ *where* $a^2 \in Q'$, *and*

(iv) P^ω *is fixed by all automorphisms of* Q. *Thus, if* Q *is an* A*-loop, then* $P^\omega \trianglelefteq Q$.

Proof. (i) Since Q is finite, we need only verify that P^ω is closed under multiplication. If $x, y \in P^\omega$, then $x \in P^i(Q)$ and $y \in P^j(Q)$ for some $i, j \geqslant 1$. Thus $xy \in P^{i+j}(Q) \subseteq P^\omega$.

(ii) Again, since Q is finite, the nested sequence $(P^{2i}(Q) : 1 \leqslant i < \infty)$ must terminate at some step, say $P^{k_1}(Q)$. Likewise $(P^{2i+1}(Q) : 1 \leqslant i < \infty)$ must terminate at some step, say $P^{k_2}(Q)$. Thus letting $k = \max\{k_1, k_2\}$, we have $P^\omega = P^k(Q) \cup P^{k+1}(Q)$. (In fact, by Lemma 3.1 part (ii), the sequences terminate at the same time.)

(iii) Suppose $P^\omega \trianglelefteq Q$. We show that Q/P^ω is an Abelian group and thus $Q' \subseteq P^\omega$. To see that Q/P^ω is a group, note that $aP^\omega bP^\omega \cdot cP^\omega = (ab \cdot c)P^\omega$. We would like to show that $(ab \cdot c)P^\omega = (a \cdot bc)P^\omega$.

To that end, let $a' \in P(Q \setminus \{a\})$ and likewise for b' and c'. We translate both $(ab \cdot c)P^\omega$ and $(a \cdot bc)P^\omega$ by $(a'b' \cdot c')P^\omega$ on the left to get

$$(a \cdot bc)P^\omega \cdot (a'b' \cdot c')P^\omega = [(a \cdot bc) \cdot (a'b' \cdot c')]P^\omega$$
$$(ab \cdot c)P^\omega \cdot (a'b' \cdot c')P^\omega = [(ab \cdot c) \cdot (a'b' \cdot c')]P^\omega$$

Note that both $(a \cdot bc) \cdot (a'b' \cdot c')$ and $(ab \cdot c) \cdot (a'b' \cdot c')$ are elements of $P(Q)$ and thus both right-hand sides reduce to P^ω. Thus both $(ab \cdot c)P^\omega$ and $(a \cdot bc)P^\omega$ are left inverses of $(a'b' \cdot c')P^\omega$. Since left inverses are unique, we have $(ab \cdot c)P^\omega = (a \cdot bc)P^\omega$ and Q/P^ω is a group.

To see that Q/P^ω is Abelian, consider $aP^\omega bP^\omega$ and $bP^\omega aP^\omega$. Again let $a' \in P(Q \setminus \{a\})$ and $b' \in P(Q \setminus \{b\})$. We then have

$$abP^\omega \cdot a'b'P^\omega = (ab \cdot a'b')P^\omega$$
$$baP^\omega \cdot a'b'P^\omega = (ba \cdot a'b')P^\omega$$

Since $(ab \cdot a'b')$ and $(ba \cdot a'b')$ are both members of $P(Q)$, the right-hand sides reduce to P^ω. As above, it follows that $aP^\omega bP^\omega = bP^\omega aP^\omega$.

Since Q' is the smallest normal subloop of Q such that Q/Q' is an Abelian group, $Q' \subseteq P^\omega$.

(iv) First note that for $i \geqslant 1$, $P^i(Q)$ is always fixed by automorphisms of Q and thus so is P^ω. If Q is an A-loop, then P^ω is fixed by every inner-mapping. That is, $P^\omega \trianglelefteq Q$. $\square$

In the spirit of the observations made in Lemma 7.1, Yff showed that when G is a group, $P^3(G)$ coincides with a coset of G' [23, p. 269]. Although this fact is an easy application of the Dénes-Hermann theorem, his proof applies directly to all finite groups and avoids the use of the Feit-Thompson theorem.

To our knowledge, Theorem 2.4 is the first extension beyond groups of the Dénes-Hermann theorem. Although our generalization is rather modest, we suspect the result extends almost completely.

Question 7.2. *If $|Q|$ is sufficiently large, does it follow that $P(Q)$ is a coset of Q'?*

The Dénes-Hermann theorem is equivalent to the claim that for any finite group G

$$|\{g_1 \cdots g_n : \text{ ranging over all orderings }\}| = |G'|.$$

To answer Question 7.2 affirmatively, it would suffice to show the perhaps stronger claim that given any fixed ordering of the elements of Q, we have

$$|\{q_1 \cdots q_n : \text{ ranging over all associations }\}| = |A(Q)|.$$

The restriction on $|Q|$ in Question 7.2 is necessary as Vojtěchovský and Wanless have observed that for 3 of the 5 non-associative loops of order 5, $P(Q)$ has order 4 whereas $Q = Q'$ (see Figure 2 for one such example) [19]. At the time of this writing, we are unaware of any other loops with this property.

We recall the following special case of the correspondence and isomorphism theorems, proofs of which can be found in most standard universal algebra texts.

Lemma 7.3. *If $N \trianglelefteq Q$ and $N \leqslant H \leqslant Q$, then*

(i) $H \trianglelefteq Q$ if and only if $H/N \trianglelefteq Q/N$ and

(ii) when $H \trianglelefteq Q$, $Q/H \cong (Q/N)/(H/N)$.

We employ the following lemma in our proof of Theorem 2.4.

Q	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

Figure 2: Loop Q for which $Q = Q'$ but $P(Q) = Q \setminus \{1\}$. As such, Q demonstrates the necessity of the cardinality restriction in Question 7.2.

Lemma 7.4. $(Q/A(Q))' = Q'/A(Q)$.

Proof. Set $A := A(Q)$. By definition, $(Q/A)'$ is the smallest normal subloop of Q/A such that the factor loop is an Abelian group. Since $A \leqslant Q' \trianglelefteq Q$, by the correspondence theorem we have $(Q'/A) \trianglelefteq (Q/A)$ and $(Q/A)/(Q'/A) \cong Q/Q'$, an Abelian group. Thus $(Q/A)' \leqslant (Q'/A)$.

We now show that $(Q'/A) \leqslant (Q/A)'$. Fix $N/A \trianglelefteq Q/A$ such that $(Q/A)/(N/A)$ is an Abelian group. Again by the correspondence theorem, $N \trianglelefteq Q$ and $Q/N \cong (Q/A)/(N/A)$. Since Q/N is an Abelian group, $Q' \leqslant N$ and thus $Q'/A \leqslant N/A$. It follows that $(Q'/A) \leqslant (Q/A)'$ □

Proof of Theorem 2.4. Let $A := A(Q)$ and $k := |A|$. Since $P(Q)$ is contained in a single coset of Q', it suffices to show that $P(Q)$ intersects at least $[Q' : A]$ cosets of A (the maximum possible).

By Theorem 2.3, $P(Q/A) = \{xA(Q/A)'\}$ such that $x^2A \in (Q/A)'$. By Lemma 7.4, $xA(Q/A)' = xA(Q'/A) = (xQ')A$. Thus we have $P(Q/A) = \{(xQ')A\}$. By Lemma 3.2, $P(Q)$ intersects each of the $[Q' : A]$ elements of $P(Q/A)^k = \{(x^kQ')A\} = \{qA : q \in x^kQ'\}$. □

8 Concluding Remarks

We have proposed the HP-condition as a possible framework for extensions of Theorem 1.1 from groups into the larger world of non-associative loops. Having shown several universal implications between the points of the HP-condition, we leave open the difficult problem of identifying interesting varieties of loops in which conditions (B) and (C) imply (A).

It would also be of interest to identify classes of loops in which the existence of a regular row transversal implies the existence of a transversal. As noted in Corollary 2.9, this implication in groups is fully equivalent to Theorem 1.1.

I thank Michael Kinyon and Petr Vojtěchovský for their helpful conversations regarding this material and Anthony Evans and Ian Wanless for sharing several articles and preprints related to the Hall-Paige conjecture. Lastly I thank the anonymous referee whose feedback clarified the historical background and helped to focus the exposition.

References

[1] J. Bray. Unpublished notes. 2008.

[2] R. H. Bruck. *A survey of binary systems.* Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie. Springer Verlag, Berlin, 1958.

[3] R. H. Bruck and L. J. Paige. Loops whose inner mappings are automorphisms. *Ann. of Math. (2)*, 63:308–323, 1956.

[4] D. Bryant, J. Egan, B. Maenhaut, and I. M. Wanless. Indivisible plexes in latin squares. *Designs, Codes and Cryptography*, 52(1):93–105, 2009.

[5] C. J. Colbourn and J. H. Dinitz. *The CRC Handbook of Combinatorial Designs.* CRC Press, Boca Raton, FL, 1996.

[6] J. Dénes and P. Hermann. On the product of all elements in a finite group. In *Algebraic and geometric combinatorics*, volume 65 of *North-Holland Math. Stud.*, pages 105–109. North-Holland, Amsterdam, 1982.

[7] J. Dénes and A. D. Keedwell. *Latin squares and their applications.* Academic Press, New York, 1974.

[8] J. Dénes and A. D. Keedwell. A new conjecture concerning admissibility of groups. *European J. Combin.*, 10(2):171–174, 1989.

[9] J. Dénes and A. D. Keedwell. *Latin squares, New developments in the theory and applications*,volume 46 of *Annals of Discrete Mathematics.* North-Holland, Amsterdam, 1991.

[10] J. Egan and I. M. Wanless. Latin squares with no small odd plexes. *Journal of Combinatorial Designs*, 16(6):477–492, 2008.

[11] A. B. Evans. The existence of complete mappings of finite groups. In *Proceedings of the Twenty-third Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1992)*, volume 90, pages 65–75, 1992.

[12] A. B. Evans. The admissibility of sporadic simple groups. *J. Algebra*, 321:1407–1428, 2009.

[13] M. Hall and L. J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 5:541–549, 1955.

[14] L. J. Paige. A note on finite Abelian groups. *Bull. Amer. Math. Soc.*, 53:590–593, 1947.

[15] L. J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 1:111–116, 1951.

[16] H. O. Pflugfelder. *Quasigroups and loops: introduction*, volume 7 of *Sigma Series in Pure Mathematics.* Heldermann Verlag, Berlin, 1990.

[17] K. Pula. The Hall-Paige conjecture for finite Moufang loops. In preparation, 2009.

[18] M. Vaughan-Lee and I. M. Wanless. Latin squares and the Hall-Paige conjecture. *Bull. London Math. Soc.*, 35(2):191–195, 2003.

[19] P. Vojtěchovský and I. M. Wanless. Private correspondence. February 2009.

[20] I. M. Wanless. A generalisation of transversals for Latin squares. *Electron. J. Combin.*, 9(1):Research Paper 12, 15 pp. (electronic), 2002.

[21] I. M. Wanless. Transversals in Latin squares. *Quasigroups Related Systems*, 15(1):169–190, 2007.

[22] S. Wilcox. Reduction of the hall-paige conjecture to sporadic simple groups. *J. Algebra*, 321(5):1407–1428, 2009.

[23] P. Yff. On the Dénes-Hermann theorem: a different approach. *European J. Combin.*, 12(3):267–270, 1991.

[24] H. Zassenhaus. *The theory of groups.* Chelsea, New York, New York, 1949.