Quasigroups and Related Systems **10** (2003), 115 – 134

Quasigroup permutation representations

Jonathan D. H. Smith

Abstract

The paper surveys the current state of the theory of permutation representations of finite quasigroups. A permutation representation of a quasigroup includes a Markov chain for each element of the quasigroup, and yields an iterated function system in the sense of fractal geometry. If the quasigroup is associative, the concept specializes to the usual notion of a permutation representation of a group, the transition matrices of the Markov chains becoming permutation matrices in this case. The class of all permutation representations of a given fixed quasigroup forms a covariety of coalgebras. Burnside's Lemma extends to quasigroup permutation representations. The theory leads to a new approach to the study of Lagrangean properties of loops.

1. Introduction

One of the major programs in the study of quasigroups and loops has been the extension to them of various aspects of the representation theory of groups. For summaries of character theory, see [11], [19]. For a summary of module theory, see [18]. The purpose of the present paper is to survey the current state of the theory of permutation representations of finite quasigroups. The theory began with the papers [20], [21] introducing a concept of homogeneous space for finite quasigroups. Given a subquasigroup P of a finite quasigroup Q, the elements of the corresponding homogeneous space $P\backslash Q$ are the orbits on Q of the group of permutations generated by the left multiplications by elements of P. Each element of Q yields a Markov chain action on the homogeneous space $P\backslash Q$ as a set of states. The full structure is an instance of an iterated function system (IFS) in the sense of fractal geometry [1]. If P is a subgroup of a group Q, then the concept just specializes

2000 Mathematics Subject Classification: 20N05
Keywords: loop, quasigroup, permutation representation, coalgebra, Burnside lemma, Lagrange property, iterated function system, IFS

to the usual concept of a homogeneous space or transitive permutation representation for groups, the transition matrices of the Markov chain actions becoming deterministic permutation matrices in this case. Now arbitrary Q-sets for a group Q are just built up by taking disjoint unions of homogeneous spaces. Moreover, the class of (finite) Q-sets is closed under direct products. The class of all Q-sets admits a syntactical characterization as a variety of universal algebras, the axioms essentially characterizing a Q-set (X, Q) as a set X with a group homomorphism from Q to the group $X!$ of permutations of the set X.

For a quasigroup Q, the situation is not so simple. The first step is to establish a general framework, the concrete category $\mathbf{IFS}_Q$ of iterated function systems over the quasigroup Q. An object of this category, a so-called Q-IFS, is just a set X that is the state space of a family of Markov chain actions indexed by the underlying set of the quasigroup Q. Each homogeneous space $P\backslash Q$ is certainly a Q-IFS in this sense. The category $\mathbf{IFS}_Q$ has sums or coproducts given by disjoint unions, and products given by direct products. The transition matrices in the disjoint union are the direct sums of the transition matrices of the summands, while the transition matrices in the direct product are the tensor or Kronecker products of the transition matrices of the factors. If Q is a group, then the category of Q-sets is a full subcategory of $\mathbf{IFS}_Q$, and one may readily recognize when a Q-IFS is a Q-set (Proposition 5.3). For a finite quasigroup Q, each Q-IFS is equivalent to a certain coalgebra (Theorem 7.4). The class of Q-sets or permutation representations for Q is then defined to be the covariety of coalgebras generated by the homomorphic images of homogeneous spaces. Each Q-set is a sum of orbits or images of homogeneous spaces (Theorem 10.2), the number of orbits being counted by Burnside's Lemma (Theorem 11.2). The paper concludes with an application of the theory of quasigroup permutation representations to the study of Lagrangean properties of loops. For concepts and conventions of quasigroup theory and universal algebra that are not otherwise explained here, readers are referred to [23].

2. Relative multiplication groups

Quasigroups are construed as sets $(Q, \cdot, /, \backslash)$ equipped with three binary operations of multiplication, *right division* $/$ and *left division* $\backslash$, satisfying the identities:

$$\begin{array}{llll} \text{(IL)} & y \backslash (y \cdot x) = x; & \text{(SL)} & y \cdot (y \backslash x) = x; \\ \text{(IR)} & x = (x \cdot y)/y; & \text{(SR)} & x = (x/y) \cdot y. \end{array}$$

A subset P of a quasigroup Q is a *subquasigroup* of Q if it is closed under the three binary operations. More generally, the equational definition of quasigroups means that they form a variety in the sense of universal algebra, and are thus susceptible to study by the concepts and methods of universal algebra [23].

For each element q of a quasigroup Q, the *right multiplication*

$$R(q) : Q \to Q; x \mapsto x \cdot q$$

and *left multiplication*

$$L(q) : Q \to Q; x \mapsto q \cdot x$$

are elements of the group $Q!$ of bijections from the set Q to itself. For a subquasigroup P of a quasigroup Q, the *relative left multiplication group* of P in Q is the subgroup $\mathrm{LMlt}_Q(P)$ of $Q!$ generated by

$$L(P) = \{L(p) : Q \to Q \mid p \in P\}. \tag{2.1}$$

Relative right multiplication groups are defined similarly. A *loop* is a (non-empty) quasigroup Q with an *identity* element, an element e such that $R(e) = L(e) = 1$ in $Q!$. Loops form the non-empty members of the variety of quasigroups satisfying the identity $x/x = y \backslash y$. They may also be construed as algebras $(Q, \cdot, /, \backslash, e)$ such that $(Q, \cdot, /, \backslash)$ is a quasigroup and e is a nullary operation satisfying the identities $e \cdot x = x = x \cdot e$.

3. Quasigroup homogeneous spaces

The construction of a quasigroup homogeneous space for a finite quasigroup [20] [21] is analogous to the permutation representation of a group Q (with subgroup P) on the homogeneous space

$$P \setminus Q = \{Px \mid x \in Q\} \tag{3.1}$$

by the actions

$$R_{P\setminus Q}(q) : P \setminus Q \to P \setminus Q\,;\, Px \mapsto Pxq \tag{3.2}$$

for elements q of Q. Let P be a subquasigroup of a finite quasigroup Q. Let L be the relative left multiplication group of P in Q. Let $P \setminus Q$ be the set of orbits of the permutation group L on the set Q. If Q is a group, and P is nonempty, then this notation is consistent with (3.1). Let A be the

incidence matrix of the membership relation between the set Q and the set $P \setminus Q$ of subsets of Q. Let A^+ be the pseudoinverse of the matrix A, i.e. the unique matrix A^+ satisfying:

$$\begin{aligned} &(a) \qquad AA^+A = A \\ &(b) \qquad A^+AA^+ = A^+ \\ &(c) \qquad (A^+A)^* = A^+A \\ &(d) \qquad (AA^+)^* = AA^+ \end{aligned}$$

[13]. For each element q of Q, right multiplication in Q by q yields a permutation of Q. Let $R_Q(q)$ be the corresponding permutation matrix. Define a new matrix

$$R_{P\setminus Q}(q) = A^+ R_Q(q) A\,. \tag{3.3}$$

[In the group case, the matrix (3.3) is just the permutation matrix given by the permutation (3.2).] Then in the homogeneous space of the quasigroup Q, each quasigroup element q yields a Markov chain on the state space $P \setminus Q$ with transition matrix $R_{P\setminus Q}(q)$ given by (3.3). For the intuition behind (3.3), see the discussion of the example in the following section.

Remark 3.1. The set of convex combinations of the states from $P\setminus Q$ forms a complete metric space, and the actions (3.3) of the quasigroup elements form an iterated function system or IFS in the sense of fractal geometry [1]. For present purposes, this remark is relevant only as motivation for the nomenclature of Section 5 below.

4. An example

Consider the quasigroup Q whose multiplication table is the following Latin square:

1	3	2	5	6	4
3	2	1	6	4	5
2	1	3	4	5	6
4	5	6	1	2	3
5	6	4	2	3	1
6	4	5	3	1	2

.

Let P be the singleton subquasigroup $\{1\}$. Note that $\mathrm{LMlt}_Q P$ is the cyclic subgroup of $Q!$ generated by $(23)(456)$. Thus

$$P \setminus Q = \{\{1\}, \{2,3\}, \{4,5,6\}\},$$

yielding

$$A_P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad A_P^+ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} ,$$

whence (3.3) gives

$$R_{P\backslash Q}(5) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} . \tag{4.1}$$

The bottom row of (4.1), determining the image of the orbit $\{4,5,6\}$ under the action of the quasigroup element 5, may be understood as follows. From the multiplication table, one has $4 \cdot 5 = 2$, $5 \cdot 5 = 3$, and $6 \cdot 5 = 1$. Thus a uniformly chosen random element of $\{4,5,6\}$ is multiplied by the quasigroup element 5 to an element of the orbit $\{1\}$ with probability $1/3$, and to an element of the orbit $\{2,3\}$ with probability $2/3$.

5. The IFS category

Let Q be a finite quasigroup. Define a Q-IFS (X,Q) as a finite set X together with an *action map*

$$R : Q \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}X); q \mapsto R_X(q) \tag{5.1}$$

from Q to the set of endomorphisms of the complex vector space with basis X (identified with their matrices with respect to the basis X), such that each *action matrix* $R_X(q)$ is stochastic. (Recall that a square complex matrix is said to be *stochastic* if its entries are non-negative real numbers, and if each row sum is 1.)

Definition 5.2. Let (X,Q) be a Q-IFS. Then for Q non-empty, the *Markov matrix* of (X,Q) is the arithmetic mean

$$M_{(X,Q)} = \frac{1}{|Q|} \sum_{q \in Q} R_X(q) \tag{5.2}$$

of the action matrices of the elements of Q.

Note that the Markov matrix of a Q-IFS is stochastic. If P is a subquasigroup of a finite non-empty quasigroup Q, then the homogeneous space $P \setminus Q$ is a Q-IFS with the action map specified by (3.3). Each row of the Markov matrix of the Q-IFS $P \setminus Q$ takes the form

$$(|P_1|/|Q|, \ldots, |P_r|/|Q|), \tag{5.3}$$

where $P_1, \ldots, P_r$ are the orbits of the relative left multiplication group of P in Q. (Compare [22, Prop. 8.1], where this result was formulated for a loop Q. The proof given there applies to an arbitrary non-empty quasigroup Q.)

A *morphism*

$$\phi : (X, Q) \to (Y, Q) \tag{5.4}$$

from a Q-IFS (X, Q) to a Q-IFS (Y, Q) is a function $\phi : X \to Y$, whose graph has incidence matrix F, such that

$$R_X(q)F = FR_Y(q) \tag{5.5}$$

for each element q of Q. It is readily checked that the class of morphisms (5.4), for a fixed quasigroup Q, forms a concrete category $\mathbf{IFS}_Q$.

Proposition 5.3. *Let Q be a finite group.*

(*a*) *The category of finite Q-sets forms the full subcategory of $\mathbf{IFS}_Q$ consisting of those objects for which the action map* (5.1) *is a monoid homomorphism.*

(*b*) *A Q-IFS (X, Q) is a Q-set if and only if it is isomorphic to a Q-set (Y, Q) in $\mathbf{IFS}_Q$.*

Proof. For (a), suppose that the action map (5.1) of a Q-IFS (X, Q) is a monoid homomorphism. Let A be in the image of (5.1). Then A is a stochastic matrix with $A^r = I$ for some positive integer r. It follows that A is a permutation matrix (cf. §XV.7 of [4]). Part (b) follows from part (a): if the morphism $\phi : (X, Q) \to (Y, Q)$ is an isomorphism whose graph has incidence matrix F, then the action map of (X, Q) is the composite of the action map of (Y, Q) with the monoid isomorphism $R_Y(q) \mapsto FR_Y(q)F^{-1}$ given by (5.5). □

For a fixed finite quasigroup Q, the category $\mathbf{IFS}_Q$ has finite products and coproducts. Consider objects (X, Q) and (Y, Q) of $\mathbf{IFS}_Q$. Their *sum* or *disjoint union* $(X + Y, Q)$ consists of the disjoint union $X + Y$ of the sets X and Y together with the action map

$$q \mapsto R_X(q) \oplus R_Y(q) \tag{5.6}$$

sending each element q of Q to the direct sum of the matrices $R_X(q)$ and $R_Y(q)$. One obtains an object of $\mathbf{IFS}_Q$, since the direct sum of stochastic matrices is stochastic. The *direct product* $(X \times Y, Q)$ of (X, Q) and (Y, Q) is the direct product $X \times Y$ of the sets X and Y together with the action map

$$q \mapsto R_X(q) \otimes R_Y(q)$$

sending each element q of Q to the tensor (or Kronecker) product of the matrices $R_X(q)$ and $R_Y(q)$. Again, one obtains an object of $\mathbf{IFS}_Q$, since the tensor product of stochastic matrices is stochastic. It is straightforward to check that the disjoint union, equipped with the appropriate insertions, yields a coproduct in $\mathbf{IFS}_Q$, and that the direct product, equipped with the appropriate projections, yields a product in $\mathbf{IFS}_Q$.

6. Coalgebras and covarieties

For a given finite quasigroup Q, the permutation representations of Q are axiomatized as a certain covariety of coalgebras. This section thus summarises the basic coalgebraic concepts required. For more details, readers may consult [7], [8] or [17]. Crudely speaking, coalgebras are just the duals of algebras: coalgebras in a category $\mathcal{C}$ are algebras in the dual category $\mathcal{C}^{\mathrm{op}}$.

Let $F : \mathbf{Set} \to \mathbf{Set}$ be an endofunctor on the category of sets and functions. Then an *F-coalgebra*, or simply a *coalgebra* if the endofunctor is implicit in the context, is a set X equipped with a function α_X or $\alpha : X \to XF$. This function is known as the *structure map* of the coalgebra X. (Of course, for complete precision, one may always denote a coalgebra by its structure map.) A function $f : X \to Y$ between coalgebras is a *homomorphism* if $f\alpha_Y = \alpha_X f^F$. A subset S of a coalgebra X is a *subcoalgebra* if it is itself a coalgebra such that the embedding of S in X is a homomorphism. A coalgebra Y is a *homomorphic image* of a coalgebra X if there is a surjective homomorphism $f : X \to Y$.

Let $(X_i \mid i \in I)$ be a family of coalgebras. Then the *sum* of this family is the disjoint union of the sets of the family, equipped with a coalgebra structure map α given as follows. Let $\iota_i : X_i \to X$ insert X_i as a summand in the disjoint union X of the family. For each i in I, let α_i be the structure map of X_i. Then the restriction of α to the subset X_i of X is given by $\alpha_i \iota_i^F$. (More generally, the forgetful functor from coalgebras to sets creates colimits — cf. Proposition 1.1 of [2].)

A *covariety* of coalgebras is a class of coalgebras closed under the operations H of taking homomorphic images, S of taking subalgebras, and Σ of taking sums. (Note that homomorphic images are dual to subalgebras, while sums are dual to products.) If $\mathcal{K}$ is a class of F-coalgebras, then the smallest covariety containing $\mathcal{K}$ is given by $\mathrm{SH}\Sigma(\mathcal{K})$ (cf. [7, Th. 7.5] or [8, Th. 3.3]). This result is dual to the well-known characterization of the variety generated by a class of algebras (cf. e.g. Exercise 2.3A of [23, Ch. IV] or [16, Prop. 1.5.12]).

7. Actions as coalgebras

For a finite set Q, the Q-IFS are realised as coalgebras for the Q-th power of the endofunctor B sending a set to (the underlying set of) the free barycentric algebra it generates. Thus it is first necessary to recall some basic facts about barycentric algebras. For more details, readers may consult [15] or [16]. Let I° denote the open unit interval $]0,1[$. For p in I°, define $p' = 1-p$.

Definition 7.1. A *barycentric algebra* A or (A, I°) is an algebra of type $I^\circ \times \{2\}$, equipped with a binary operation

$$\underline{p} : A \times A \to A; \quad (x,y) \mapsto xy\,\underline{p}$$

for each p in I°, satisfying the identities

$$xx\,\underline{p} = x \tag{7.1}$$

of *idempotence* for each p in I°, the identities

$$xy\,\underline{p} = yx\,\underline{p'} \tag{7.2}$$

of *skew-commutativity* for each p in I°, and the identities

$$xy\,\underline{p}\ z\,\underline{q} = x\ yz\,\underline{q/(p'q')'}\ \underline{(p'q')'} \tag{7.3}$$

of *skew-associativity* for each p, q in I°. The variety of all barycentric algebras, construed as a category with the homomorphisms as morphisms, is denoted by $\mathbf{B}$. The corresponding free algebra functor is $B : \mathbf{Set} \to \mathbf{B}$.

A convex set C forms a barycentric algebra (C, I°), with $xy\,\underline{p} = (1-p)x + py$ for x, y in C and p in I°. A semilattice $(S, \cdot)$ becomes a barycentric algebra on setting $xy\,\underline{p} = x \cdot y$ for x, y in S and p in I°.

For the following result, see [12], [15, §2.1], [16, §5.8]. The equivalence of the final two structures in the theorem corresponds to the identification of the barycentric coordinates in a simplex with the weights in finite probability distributions.

Theorem 7.2. *Let X be a finite set. The following structures are equivalent:*

(*a*) *The free barycentric algebra XB on X;*

(*b*) *The simplex spanned by X;*

(*c*) *The set of all probability distributions on X.*

Definition 7.3. Let Q be a finite set. The functor $B^Q : \mathbf{Set} \to \mathbf{Set}$ sends a set X to the set XB^Q of functions from Q to the free barycentric algebra XB over X. For a function $f : X \to Y$, its image under the functor B^Q is the function $fB^Q : XB^Q \to YB^Q$ defined by

$$fB^Q : (Q \to XB; q \mapsto w) \mapsto (Q \to YB; q \mapsto wf^B).$$

Theorem 7.4. *Let Q be a finite set. Then the category $\mathbf{IFS}_Q$ is isomorphic with the category of finite B^Q-coalgebras.*

Proof. Given a Q-IFS (X, Q) with action map R as in (5.1), define a B^Q-coalgebra $L_X : X \to XB^Q$ with structure map

$$L_X : X \to XB^Q; x \mapsto (Q \to XB; q \mapsto xR_X(q)). \tag{7.4}$$

(Note the use of Theorem 7.2 interpreting the vector $xR_X(q)$, lying in the simplex spanned by X, as an element of XB.) Given a Q-IFS morphism $\phi : (X, Q) \to (Y, Q)$ as in (5.4), with incidence matrix F, one has

$$xL_X.\phi B^Q : Q \to YB; q \mapsto xR_X(q)F \tag{7.5}$$

for each x in X, by Definition 7.3. On the other hand, one also has

$$x\phi L_Y : Q \to YB; q \mapsto xFR_Y(q). \tag{7.6}$$

By (5.5), it follows that the maps (7.5) and (7.6) agree. Thus $\phi : X \to Y$ is a coalgebra homomorphism. These constructions yield a functor from $\mathbf{IFS}_Q$ to the category of finite B^Q-coalgebras.

Conversely, given a finite B^Q-coalgebra with structure map $L_X : X \to XB^Q$, define a Q-IFS (X, Q) with action map

$$R_X : Q \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}X); q \mapsto (x \mapsto qL_X(x)), \tag{7.7}$$

well-defined by Theorem 7.2. Let $\phi : X \to Y$ be a coalgebra homomorphism with incidence matrix F. Then the maps (7.5) and (7.6) agree for all x in the basis X of $\mathbb{C}X$, whence (5.5) holds and $\phi : (X, Q) \to (Y, Q)$ becomes a Q-IFS morphism. In this way one obtains mutually inverse functors between the two categories. □

Corollary 7.5. *Each homogeneous space over a finite quasigroup Q yields a B^Q-coalgebra.*

Example 7.6. Consider the structure map of the coalgebra corresponding to the homogeneous space presented in Section 4. In accordance with (4.1), the image of the state $\{4, 5, 6\}$ sends the element 5 of Q to the convex combination weighting the state $\{1\}$ with $1/3$ and the state $\{2, 3\}$ with $2/3$.

Corollary 7.7. *Let Q be a finite group. Then the category of finite Q-sets embeds faithfully as a full subcategory of the category of B^Q-coalgebras.*

Proof. Apply Theorem 7.4 and Proposition 5.3. □

8. Irreducibility

Definition 8.1. Let Q be a finite set. Let Y be a B^Q-coalgebra with structure map $L : Y \to YB^Q$. For elements y, y' of Y, the element y' is said to be *reachable* from y in Y if there is an element q of Q such that y' appears in the support of the distribution $qL(y)$ on Y. The *reachability graph* of Y is the directed graph of the reachability relation on Y. The coalgebra Y is said to be *irreducible* if its reachability graph is strongly connected.

Proposition 8.2. *If $P \setminus Q$ is a homogeneous space over a finite quasigroup Q, realised as a B^Q-coalgebra according to Corollary 7.5, then $P \setminus Q$ is irreducible.*

Proof. Let H be the relative left multiplication group of P in Q. For an arbitrary pair x, x' of elements of Q, consider the corresponding elements xH and $x'H$ of $P \setminus Q$. For $q = x \setminus x'$ in Q, the element $x'H$ then appears in the support of $qL(xH)$. □

Corollary 8.3. *Let Q be a finite quasigroup. Suppose that Y is a B^Q-coalgebra that is a homomorphic image of a homogeneous space S over Q. Then Y is irreducible.*

Proof. Since S and Y are finite, one may use the correspondence of Theorem 7.4. Let $\phi : S \to Y$ be the homomorphism, with incidence matrix F. Consider elements y and y' of Y. Suppose x and x' are elements of S with $x\phi = y$ and $x'\phi = y'$. By Proposition 8.2, there is an element q of Q with x' in the support of the distribution $xR_S(q)$. Then $yR_Y(q) = xFR_Y(q) = xR_S(q)F$, so the support of $yR_Y(q)$, as the image of the support of $xR_S(q)$ under ϕ, contains $x'\phi = y'$. □

9. Regular representations

For a quasigroup Q, the *regular* homogeneous space or permutation representation is the homogeneous space (Q, Q) or $(\varnothing \setminus Q, Q)$. Recall that the relative left multiplication group of the empty subquasigroup is trivial. If Q is a loop with identity element e, then the regular homogeneous space may also be described as $(\{e\} \setminus Q, Q)$. (This definition was used in [22, §7].) A finite, non-empty quasigroup Q may be recovered from its regular representation. For example, the multiplication table of Q may be realised as the formal sum $\Sigma_{q \in Q} q R_{\varnothing \setminus Q}(q)$ of multiples of the action matrices of $\varnothing \setminus Q$.

For a group Q, each homogeneous space $(P \setminus Q, Q)$ is obtained as a homomorphic image of the regular permutation representation. The following considerations show that the corresponding property does not hold for general quasigroups.

Definition 9.1. Let Q be a finite set. A Q-IFS (X, Q) is said to be *crisp* if, for each q in Q, the action matrix $R_X(q)$ is a 0-1-matrix. A B^Q-coalgebra $L : X \to XB^Q$ is said to be *crisp* if its structure map corestricts to $L : X \to X^Q$.

Note that crisp Q-IFS and finite crisp B^Q-coalgebras correspond under the isomorphism of Theorem 7.4.

Proposition 9.2. *Homomorphic images of finite crisp B^Q-coalgebras are crisp.*

Proof. Using Theorem 7.4, it is simpler to work in the category $\mathbf{IFS}_Q$. Let $\phi : X \to Y$ be a surjective $\mathbf{IFS}_Q$-morphism with incidence matrix F and crisp domain. For an element y of Y, suppose that x is an element of X

with $x\phi = y$. Then for each element q of Q, one has $yR_Y(q) = x\phi R_Y(q) = xFR_Y(q) = xR_X(q)F$, using (5.5) for the last step. Since X is crisp, there is an element x' of X with $xR_X(q) = x'$. Then $yR_Y(q) = x'F = y'$ for the element $y' = x'\phi$ of Y. Thus Y is also crisp. □

For each finite quasigroup Q, the regular permutation representation is crisp. On the other hand, the homogeneous space exhibited in Section is not crisp. Proposition 9.2 shows that such spaces are not homomorphic images of the regular representation.

10. The covariety of Q-sets

Definition 10.1. Let Q be a finite quasigroup. Then the *category* $\underline{\underline{Q}}$ *of* Q*-sets* or of *permutation representations* of Q is defined to be the covariety of B^Q-coalgebras generated by the (finite) set of homogeneous spaces over Q.

For a finite quasigroup Q, the terms "Q-set" or "permutation representation of Q" are used for objects of the category of Q-sets, and also for those Q-IFS which correspond to finite Q-sets via Theorem 7.4. (For a finite loop Q, these terms were used in a different, essentially broader sense — at least for the finite case — in [22, Defn. 5.2]. If necessary, one may refer to "loop Q-sets" in that context, and to "proper Q-sets" or "quasigroup Q-sets" in the present context.)

Theorem 10.2. *For a finite quasigroup Q, the Q-sets are precisely the sums of homomorphic images of homogeneous spaces.*

Proof. Let $\mathcal{H}$ be the set of homogeneous spaces over Q. By [9, Prop. 2.4], the covariety generated by $\mathcal{H}$ is $\mathrm{HS}\Sigma(\mathcal{H})$. By [9, Prop. 2.5], the operators S and Σ commute. By Proposition 8.2, the homogeneous spaces do not contain any proper, non-empty subcoalgebras. Thus the covariety generated by $\mathcal{H}$ becomes $\mathrm{H}\Sigma(\mathcal{H})$. By [9, Prop. 2.4(iii)], one has $\Sigma\mathrm{H}(\mathcal{H}) \subseteq \mathrm{H}\Sigma(\mathcal{H})$. It thus remains to be shown that each homomorphic image of a sum of homogeneous spaces is a sum of homomorphic images of homogeneous spaces.

Let Y be a Q-set, with structure map L_Y, that is a homomorphic image of a sum X of homogeneous spaces under a homomorphism ϕ. It will first be shown that each element y of Y lies in a subcoalgebra Y_y of Y that is a homomorphic image of a homogeneous space. Since y lies in the image Y of X under ϕ, there is an element x of X such that $x\phi = y$. Since X is a sum of homogeneous spaces, the element x lies in such a space S. Consider

the restriction of ϕ to S. Let Y_y be the image of this restriction. Then Y_y is a subcoalgebra of Y that is a homomorphic image of a homogeneous space (cf. [7, Lemma 4.5]).

Now suppose that for elements y and z of Y, the corresponding images Y_y and Y_z of homogeneous spaces intersect non-trivially, say with a common element t. By Corollary 8.3, there is an element q of Q such that z lies in the support of $qL_Y(t)$. On the other hand, since t lies in the subcoalgebra Y_y, the support of the distribution $qL_Y(t)$ lies entirely in Y_y. Thus z is an element of Y_y, and for each q in Q, the support of the distribution $qL_Y(z)$ lies entirely in Y_y. It follows that Y_z is entirely contained in Y_y. Similarly, one finds that Y_y is contained in Y_z, and so the two images agree. Thus Y is a sum of such images. □

Corollary 10.3. *A finite quasigroup Q has only finitely many isomorphism classes of irreducible Q-sets.*

Proof. By Theorem 10.2, the irreducible Q-sets are precisely the homomorphic images of homogeneous spaces. Since Q is finite, it has only finitely many homogeneous spaces. The (First) Isomorphism Theorem for coalgebras (cf. [7, Th. 4.15]) then shows that each of these homogeneous spaces has only finitely many isomorphism classes of homomorphic images. □

Corollary 10.4. *For a finite group Q, the quasigroup Q-sets coincide with the group Q-sets.*

Proof. For a group Q, each homomorphic image of a homogeneous space is isomorphic to a homogeneous space, and each group Q-set is isomorphic to a sum of homogeneous spaces. □

In considering the final corollary of Theorem 10.2, recall that the intersection of a family of subcoalgebras of a coalgebra is not necessarily itself a subcoalgebra (cf. [7, Cor. 4.9]).

Corollary 10.5. *Let y be an element of a Q-set Y over a finite quasigroup Q. Then the intersection of the subcoalgebras of Y containing y is itself a subcoalgebra of Y.*

Proof. In the notation of the proof of Theorem 10.2, this intersection is the subcoalgebra Y_y. □

11. Burnside's Lemma

Definition 11.1. For a Q-set Y over a finite quasigroup Q, the irreducible summands of Y given by Theorem 10.2 are called the *orbits* of Y. For an element y of Y, the smallest subcoalgebra of Y containing y (guaranteed to exist by Corollary 10.5) is called the *orbit* of the element y.

Burnside's Lemma concerns itself with finite permutation representations. In the quasigroup case, its formulation (and proof) rely on the identification given by Theorem 7.4. Recall that the classical Burnside Lemma for a finite group Q (cf. e.g. Theorem 3.1.2 in [23, Ch. I]) states that the number of orbits in a finite Q-set X is equal to the average number of points of X fixed by elements q of Q. The number of points fixed by such an element q is equal to the trace of the permutation matrix of q on X. In the IFS terminology of §3, this permutation matrix is the action matrix $R_X(q)$ of q on the corresponding Q-IFS (X, Q). Thus the following theorem does specialise to the classical Burnside Lemma in the associative case.

Theorem 11.2. Burnside's Lemma for quasigroups
Let X be a finite Q-set over a finite, non-empty quasigroup Q. Then the trace of the Markov matrix of X is equal to the number of orbits of X.

Proof. Consider the Q-IFS (X, Q). By Theorem 7.4, Theorem 10.2 and (5.6), its Markov matrix decomposes as a direct sum of the Markov matrices of its orbits. Thus it suffices to show that the trace of the Markov matrix of a homomorphic image of a homogeneous space is equal to 1.

Consider a Q-set $Y = \{y_1, \ldots, y_m\}$ which is the image of a homogeneous space $P\backslash Q$ under a surjective homomorphism $\phi : P\backslash Q \to Y$ with incidence matrix F. Let F^+ be the pseudoinverse of F. Note that each row sum of F^+ is 1. Suppose that the Markov matrix Π of $P \setminus Q$ is given by (5.3). By (5.5), one has

$$R_Y(q) = F^+ R_{P\backslash Q}(q) F$$

for each q in Q. Thus the trace of the Markov matrix of Y is given by

$$\begin{aligned} tr(F^+ \Pi F) &= \sum_{i=1}^{m} \sum_{j=1}^{r} \sum_{k=1}^{r} F^+_{ij} \Pi_{jk} F_{ki} \\ &= |Q|^{-1} \sum_{i=1}^{m} (\sum_{j=1}^{r} F^+_{ij})(\sum_{k=1}^{r} |P_k| F_{ki}) \\ &= |Q|^{-1} \sum_{k=1}^{r} |P_k| = 1, \end{aligned}$$

the penultimate equality following since for each $1 \leq k \leq r$, there is exactly one index i (corresponding to $P_k\phi = y_i$) such that $F_{ki} = 1$, the other terms of this type vanishing. □

Remark 11.3. Burnside's Lemma may fail for a Q-IFS which does not correspond to a Q-set. For example, the square $P \setminus Q \times P \setminus Q$ of the homogeneous space $P \setminus Q$ of Section 4 (in the category of Q-IFS) has a 9×9 Markov matrix of trace 1.875, which is not even integral.

12. Lagrangean properties of loops

For a group Q, Lagrange's Theorem states that the order of a subgroup always divides the order of Q. For a general loop Q, the order of a subloop need not divide $|Q|$. In [14], a subloop P of Q is called "Lagrange-like" in Q if $|P|$ does divide $|Q|$. The loop Q is said to satisfy the *weak Lagrange property* if each subloop is Lagrange-like. It is said to satisfy the *strong Lagrange property* if each of its subloops satisfies the weak Lagrange property. Non-associative loops satisfying the strong Lagrange property were discussed in [3], [5], [6]. Recalling that Lagrange's Theorem for a group Q relies on the uniformity of the sizes of the elements of a homogeneous space $P \setminus Q$, this section formulates Lagrangean properties for loops in homogeneous space terms. Let P be a subloop of a finite loop Q. The *type* of the homogeneous space $P \setminus Q$ is the partition of $|P \setminus Q|$ given by the sizes of the orbits of the relative left multiplication group of P in Q. Note that the type of a homogeneous space is determined by its Markov matrix, according to (5.3). The type of a homogeneous space $P \setminus Q$ is said to be *uniform* if all the parts of the partition are equal. A subloop P of Q is said to be (*right*) *Lagrangean* in Q if the type of $P \setminus Q$ is uniform, i.e. if the relative left multiplication group of P in Q acts semitransitively (in the sense of [10, Defn. II.1.14b]). Note that a Lagrangean subloop P is Lagrange-like in Pflugfelder's sense, since P is one of the states of $P \setminus Q$. On the other hand, the subloop P of the loop Q of Example 12.6 below is Lagrange-like in Q, but not right Lagrangean in Q.

The Lagrangean property is more robust than Lagrange-likeness. It may happen that a subloop P of a loop Q is Lagrange-like in Q, but not in a subloop of Q that contains P. For example, suppose that a loop Q has a subloop P that is not Lagrange-like in Q. Then $P \times \{e\}$ is Lagrange-like in the loop $Q \times P$, but not in the subloop $Q \times \{e\}$. The following proposition shows that the Lagrangean property does not exhibit such pathology.

Proposition 12.1. *Let P be a Lagrangean subloop in a finite loop Q. Then P is Lagrangean in each subloop S of Q that contains P.*

Proof. Since P is a subloop of the loop S, the action of the relative left multiplication group $\mathrm{LMlt}_S P$ of P in S is just a restriction to S of the action of the relative left multiplication group $\mathrm{LMlt}_Q P$ of P in Q. Thus the uniformity of the sizes of the orbits of $\mathrm{LMlt}_Q P$ implies the uniformity of the sizes of the orbits of $\mathrm{LMlt}_S P$. □

Definition 12.2. A finite loop Q is said *to satisfy the (right) Lagrange property* if each subloop of Q is (right) Lagrangean in Q.

Example 12.3. The only proper, non-trivial subloop of the loop T with multiplication table

1	2	3	4	5	6
2	1	6	5	4	3
3	6	5	1	2	4
4	5	1	6	3	2
5	3	4	2	6	1
6	4	2	3	1	5

is the subloop $\{1, 2\}$, which is Lagrangean in T. Thus T is a non-associative loop satisfying the right Lagrange property.

In contrast with the global properties based on Lagrange-likeness, Proposition 12.1 shows that one does not need to make a distinction between "weak" and "strong" versions of the Lagrangean property of Definition 12.2.

Corollary 12.4. *Suppose that a finite loop Q satisfies the right Lagrange property. Then each subloop of Q also satisfies the right Lagrange property.*

Proof. Let P be a subloop of a subloop Q' of Q. Then by Proposition 12.1, P is Lagrangean in Q'. □

Corollary 12.5. *If a finite loop Q satisfies the right Lagrange property, then it also satisfies the strong Lagrange property.*

Proof. Let P be a subloop of a subloop Q' of Q. By Corollary 12.4, Q' satisfies the right Lagrange property, so that P is Lagrangean in Q'. It then follows that P is Lagrange-like in Q'. Thus each subloop Q' of Q satisfies the weak Lagrange property, i.e. Q itself satisfies the strong Lagrange property. □

Example 12.6. The converse of Corollary 12.5 is false: the strong Lagrange property is too weak to imply the right Lagrange property. Consider the loop Q whose multiplication table is the following Latin square:

1	2	3	4	5	6
2	1	4	5	6	3
3	4	5	6	1	2
4	3	6	1	2	5
5	6	1	2	3	4
6	5	2	3	4	1

.

The proper, non-trivial subquasigroups of Q are $P = \{1, 2\}$, $P' = \{1, 4\}$, and $P'' = \{1, 6\}$, each Lagrange-like in Q, and without mutual containments. Thus Q does satisfy the strong Lagrange property. On $P \setminus Q$, the action matrices (3.3) of the elements of P are the identity I_2, while the action matrices of the remaining elements of Q are

$$A = \begin{bmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

The type of $P \setminus Q$ is $2 + 4$, so that P is not Lagrangean in Q, and Q does not satisfy the right Lagrange property.

Corollary 12.4 shows that the right Lagrange property is inherited by subloops. The property is also inherited by homomorphic images.

Proposition 12.7. *Suppose that a finite loop Q satisfies the right Lagrange property. Then each homomorphic image of Q also satisfies the right Lagrange property.*

Proof. Suppose that $\overline{Q}$ is a quotient of Q by a projection

$$Q \to \overline{Q}; q \mapsto \overline{q}. \tag{12.1}$$

Let $\overline{P}$ be a subloop of $\overline{Q}$ whose preimage under (12.1) is the subloop P of Q. The projection (12.1) induces a group epimorphism

$$\mathrm{LMlt}_Q P \to \mathrm{LMlt}_{\overline{Q}} \overline{P}; l \mapsto \overline{l}$$

acting on the set (2.1) of generators of its domain by $L(p) \mapsto L(\overline{p})$. Set $L = \mathrm{LMlt}_Q P$ and $\overline{L} = \mathrm{LMlt}_{\overline{Q}} \overline{P}$. Now for q in Q, one has

$$\overline{q}\overline{L} = \overline{qL}. \tag{12.2}$$

To see this, consider an element $\overline{q}\overline{l}$ of the left hand side of (12.2), where the element l of $\mathrm{LMlt}_Q P$ is given by

$$l = L(p_1) \dots L(p_r)$$

with elements $p_1, \dots, p_r$ of P. Then

$$\overline{q}\overline{l} = \overline{q}L(\overline{p_1}) \dots L(\overline{p_r}) = \overline{qL(p_1) \dots L(p_r)} \in \overline{qL},$$

the second equality holding since (12.1) is a loop homomorphism. Conversely, the typical element of the right hand side of (12.2) is of the form

$$\overline{qL(p_1) \dots L(p_r)}$$

with q in Q and elements $p_1, \dots, p_r$ of P. Such an element may be rewritten in the form

$$\overline{q}L(\overline{p_1}) \dots L(\overline{p_r}),$$

exhibiting it as an element of the left hand side of (12.2).

Since the homogeneous space $P \backslash Q$ has uniform type, it follows that for each element q of Q the injection

$$R(q) : P \to qL; p \mapsto pq$$

bijects. In other words, $qL = \{pq \mid p \in P\}$. Then by (12.2), one has

$$\overline{q}\overline{L} = \overline{qL} = \{\overline{pq} \mid p \in P\} = \{\overline{p} \cdot \overline{q} \mid \overline{p} \in \overline{P}\},$$

so that each state of $\overline{P} \backslash \overline{Q}$ has cardinality $|\overline{P}|$. Thus $\overline{P}$ is Lagrangean in $\overline{Q}$, as required. □

In view of Corollary 12.4 and Proposition 12.7, it is natural to pose the following:

Problem 12.8. Suppose that loops Q_1 and Q_2 satisfy the right Lagrange property. Does the product $Q_1 \times Q_2$ also satisfy this property?

The asymmetry inherent in Definition 12.2 means that one should also consider matters from the other side. Thus a subloop P of a loop Q is said to be (*left*) *Lagrangean* in Q if the relative right multiplication group of P in Q acts semitransitively. A loop Q is said to satisfy the *left Lagrange property* if each subloop P of Q is left Lagrangean in Q. It is said to satisfy the *bilateral Lagrange property* if it satisfies both left and right Lagrange properties. Note that the subloop P of the loop Q of Example 12.6 is left Lagrangean in Q, although it is not right Lagrangean in Q.

Finally, Chein's paper [3] suggests the following:

Problem 12.9. Which loops satisfying Pflugfelder's M_k-laws possess the right, left, or bilateral Lagrange properties?

References

[1] **M. F. Barnsley**: *Fractals Everywhere*, Academic Press, San Diego, CA, 1988.

[2] **M. Barr**: *Terminal coalgebras in well-founded set theory*, Theoret. Comput. Sci. **1**14 (1993), 299 – 315.

[3] **O. Chein**: *Lagrange's Theorem for M_k-loops*, Arch. Math. **24** (1973), 121 – 122.

[4] **W. Feller**: *An Introduction to Probability Theory and its Applications*, 2nd. Ed., Vol. I, Wiley, New York, NY, 1957.

[5] **G. Glauberman**: *On loops of odd order II*, J. Alg. **8** (1968), 393 – 414.

[6] **G. Glauberman and C. R. B. Wright**: *Nilpotence of finite Moufang 2-loops*, J. Alg. **8** (1968), 415 – 417.

[7] **H.-P. Gumm**: *Elements of the general theory of coalgebras*, LUATCS'99, Rand Afrikaans University, Johannesburg, 1999.

[8] **H.-P. Gumm**: *Birkhoff's variety theorem for coalgebras*, Contributions to General Algebra **13** (2001), 159 – 173.

[9] **H.-P. Gumm and T. Schröder**: *Covarieties and complete covarieties*, pp. 43 – 56 in "Coalgebraic Methods in Computer Science," (eds. B. Jacobs et al.), Electronic Notes in Theoretical Computer Science, vol. 11, Elsevier Science, 1998.

[10] **B. Huppert**: *Endliche Gruppen I*, Springer, Berlin, 1967.

[11] **K. W. Johnson**: *Some historical aspects of the representation theory of groups and its extension to quasigroups*, pp. 101 – 117 in "Universal Algebra and Quasigroup Theory," (eds. A. Romanowska and J.D.H. Smith), Heldermann, Berlin, 1992.

[12] **W. D. Neumann**: *On the quasivariety of convex subsets of affine spaces*, Arch. Math. **21** (1970), 11 – 16.

[13] **R. Penrose**: *A generalised inverse for matrices*, Proc. Camb. Phil. Soc. **51** (1955), 406 – 413.

[14] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[15] **A. B. Romanowska and J. D. H. Smith**: *Modal Theory*, Heldermann, Berlin, 1985.

[16] **A. B. Romanowska and J. D. H. Smith**: *Modes*, World Scientific, Singapore, 2002.

[17] **J. J. M. M. Rutten**: *Universal coalgebra: a theory of systems*, Theoret. Comput. Sci. **249** (2000), 3 – 80.

[18] **J. D. H. Smith**: *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, Montreal, 1986.

[19] **J. D. H. Smith**: *Combinatorial characters of quasigroups*, pp. 163 – 187 in "Coding Theory and Design Theory, Part I: Coding Theory," (ed. D. Ray-Chaudhuri), Springer, New York, NY, 1990.

[20] **J. D. H. Smith**: *Quasigroup actions: Markov chains, pseudoinverses, and linear representations*, Southeast Asian Bull. Math. **23** (1999), 719 – 729.

[21] **J. D. H. Smith**: *Quasigroup homogeneous spaces and linear representations*, J. Alg. **241** (2001), 193 – 203.

[22] **J. D. H. Smith**: *Permutation representations of loops*, J. Alg., to appear.

[23] **J. D. H. Smith and A. B. Romanowska**: *Post-Modern Algebra*, Wiley, New York, NY, 1999.

Department of Mathematics
Iowa State University
Ames
Iowa 50011
U.S.A.
e-mail: jdhsmith@math.iastate.edu
http://www.math.iastate.edu/jdhsmith/

Received March 10, 2003