Southeast Asian Bulletin of Mathematics (1999) 23: 719–729

Southeast Asian Bulletin of Mathematics

Quasigroup Actions: Markov Chains, Pseudoinverses, and Linear Representations

Jonathan D.H. Smith

Department of Mathematics, Iowa State University, Ames, IA 50011, USA
E-mail: jdhsmith@math.iastate.edu

AMS Subject Classification (1991): 20N05, 20B05

Abstract. The scopes of both character theory and module theory have previously been extended from groups to quasigroups. This paper initiates the extension to quasigroups of a further aspect of group representation theory: transitive permutation representations. Using pseudoinverses of incidence matrices of quasigroups in partitions induced by left multiplications of subquasigroups, a transitive permutation action of a quasigroup is defined as a set of Markov chain actions indexed by the quasigroup. The definition is given a natural graph-theoretical interpretation. A certain non-unital ring is afforded a linear representation by a quasigroup permutation action. If the quasigroup is a group, the linear representation is a factor in the usual linear representation of the group algebra afforded by the transitive permutation action of the group. Finally, Burnside's Lemma for transitive quasigroup actions is derived.

Keywords: quasigroup, Latin square, permutation action, Markov chain, pseudoinverse, generalized inverse, group ring, linear representation, Burnside's Lemma

1. Introduction

A *quasigroup* Q or $(Q, \cdot)$ is a set Q equipped with a binary multiplication, denoted by "$\cdot$" or juxtaposition, such that in the equation

$$x \cdot y = z, \tag{1.1}$$

knowledge of any two of x, y, z specifies the third uniquely. Thus, for each element q of Q, the *right multiplication* $R(q)$ or

$$R_Q(q) : Q \to Q;\ x \mapsto xq \tag{1.2}$$

and *left multiplication* $L(q)$ or

$$L_Q(q) : Q \to Q;\ x \mapsto qx \tag{1.3}$$

are elements of the group $Q!$ of bijections of the set Q. A *subquasigroup* P of a quasigroup Q is a subset P of Q that is itself a quasigroup under the multiplication of Q. The *relative right multiplication group* $\mathrm{RMlt}_Q P$ of P in Q is the subgroup of $Q!$ generated by $\{R_Q(p) | p \in P\}$. The *relative left multiplication group* $\mathrm{LMlt}_Q P$ is defined similarly. The *relative multiplication group* $\mathrm{Mlt}_Q P$ is the join of $\mathrm{RMlt}_Q P$ and $\mathrm{LMlt}_Q P$ in the lattice of subgroups of $Q!$. The *(right, left) multiplication groups* $\mathrm{RMlt}Q$, $\mathrm{LMlt}Q$, $\mathrm{Mlt}Q$ of Q are the relative (right, left) multiplication groups of Q in Q.

Examples of quasigroups are furnished by groups under multiplication, by abelian groups under subtraction, and by the octonions of norm 1 under multiplication. More generally, any Latin square may be construed as the multiplication table of a quasigroup on labeling its rows and columns as in (3.1) below. For other examples and applications, see [3]. The multiplication group of a group Q is given by the exact sequence

$$1 \to Z(Q) \xrightarrow{\Delta} Q^2 \xrightarrow{T} \mathrm{Mlt}Q \to 1 \tag{1.4}$$

with $\Delta : Z(Q) \to Q^2; z \mapsto (z, z)$ as the diagonal embedding of the center in the square, and with $T : Q^2 \to \mathrm{Mlt}Q;\ (x, y) \mapsto L(x)^{-1}R(y)$. Note that the associative law yields the commuting of $\mathrm{LMlt}Q$ with $\mathrm{RMlt}Q$, so that T in (1.2) is indeed a homomorphism. For a subgroup P of a group Q, the orbits of the relative multiplication group $\mathrm{Mlt}_Q P$ acting on Q are the double cosets of P in Q. The set $Q/\mathrm{LMlt}_Q P$ of orbits of the (right) action of the permutation group $\mathrm{LMlt}_Q P$ on Q is the set $P \backslash Q$ of right cosets of P in Q. The map

$$R : P \to \mathrm{Mlt}_Q P;\ p \mapsto R_Q(p) \tag{1.5}$$

is an injective group homomorphism with image $\mathrm{RMlt}_Q P$, so that $\mathrm{RMlt}_Q P$ is isomorphic to P. Indeed, (1.3) is an extension of the right regular representation of P given by Cayley's Theorem.

Much work has been done on extending certain aspects of representation theory from groups to quasigroups. It is convenient to identify three such aspects:

(a) character theory;
(b) modules;
(c) permutation representations.

There is now a very satisfactory character theory for quasigroups, to some extent (but not completely) located within the theory of association schemes [1]. The action of the multiplication group $\mathrm{Mlt}Q$ on a (finite) quasigroup Q is "multiplicity free". In other words, extending by linearity, the $\mathbb{C}\mathrm{Mlt}Q$-module $\mathbb{C}Q$ decomposes as a direct sum of mutually inequivalent submodules. Thus the *centralizer ring* $V(\mathrm{Mlt}Q, Q)$, the ring $\mathrm{End}_{\mathbb{C}\mathrm{Mlt}Q}\mathbb{C}Q$ of $\mathbb{C}\mathrm{Mlt}Q$-endomorphisms of the module $\mathbb{C}Q$, is a commutative $\mathbb{C}$-algebra. As such, it decomposes as a direct sum of copies of $\mathbb{C}$. There are two natural bases for $V(\mathrm{Mlt}Q, Q)$: the orthogonal idempotents yielding the decomposition, and the incidence matrices for the orbits of $\mathrm{Mlt}Q$ in its diagonal action on Q^2. Normalized basis change matrices connecting these bases yield the ordinary character table of Q if Q is a group. In the general case, they thus provide the foundation for extending character theory from groups to quasigroups. Further details are available in [6–13,15].

Modules for quasigroups are defined using category theory and universal algebra. (Readers unfamiliar with these subjects are referred to [21].) A quasigroup may be redefined equivalently as a set Q with three binary operations, namely the multiplication, *right division* $x/y = xR(y)^{-1}$, and *left division* $x\backslash y = yL(x)^{-1}$, satisfying the identities

$(xy)/y = x,\ (x/y)y = x,\ y\backslash(yx) = x$, and $y(y\backslash x) = x$ [21, I§2.2]. A *variety* of quasigroups is the full class of all quasigroups satisfying these and possibly a further set of identities (such as associativity). A variety $\underline{\underline{V}}$ may be construed as a category on admitting homomorphisms between $\underline{\underline{V}}$-quasigroups as the morphisms of the category. For a $\underline{\underline{V}}$-quasigroup Q, a *Q-module* in $\underline{\underline{V}}$ is then defined to be a complex vector space $\pi : E \to Q$ in the slice category $\underline{\underline{V}}/Q$. If $\underline{\underline{V}}$ is the category $\underline{\underline{\mathrm{Gp}}}$ of groups, then such an object $\pi : E \to Q$ is just the projection $\pi : Q[M \to Q;\ (q, m) \mapsto q$ from the split extension $Q[M$ of a module M over the group Q in the traditional sense. For general quasigroups, there is no longer the strong link between the character table and module theory that there is in the group case. General Q-modules are characterized by analytic characters, defined as certain almost-periodic functions on the relative multiplication group of Q in the coproduct $Q[X]$ of Q with the free quasigroup on an indeterminate X. Further details are available in [4, 5, 16, 17, 20].

The aim of the current paper is to initiate development of a concept of permutation representation for quasigroups. At this early stage, it does not yet seem appropriate to attempt formulation of general axioms. Instead, a concrete, model-based approach is adopted. If Q is a group, then each set X acted upon by Q breaks up as a disjoint union of orbits or transitive actions. Each of these transitive actions is of the form $P\backslash Q$ for a subgroup P of Q (namely the stabilizer of an element of the orbit). The elements q of Q act on $P\backslash Q$ by right multiplication

$$R_{P\backslash Q}(q) : Px \mapsto Pxq. \tag{1.6}$$

It is these transitive actions that will be extended here to general quasigroups. For a subquasigroup P of a quasigroup Q, the set $P\backslash Q$ is taken to be the set of orbits of $\mathrm{LMlt}_Q P$ on Q. In Sec. 2, the action of Q on $P\backslash Q$ is then defined probabilistically. For each element q of Q, the set $P\backslash Q$ is the state space of a certain Markov chain. The (transitive) permutation action of Q on $P\backslash Q$ is then defined to be the set of all these Markov chains. In the group case, the transition matrices just turn out to be the usual permutation matrices. Section 3 gives a graphical interpretation of the constructions of Sec. 2, showing how they follow naturally from an incidence matrix and its pseudoinverse. In the group case, a permutation action affords a linear representation of the complex group algebra. Section 4 identifies a non-unital ring represented linearly by a transitive quasigroup permutation representation, and connects this representation with the permutation representation of the group algebra in the group case. Finally, Sec. 5 shows that Burnside's Lemma extends naturally to the quasigroup case.

2. Transition Matrices

Let P be a subquasigroup of a finite quasigroup Q. The relative left multiplication group $\mathrm{LMlt}_Q P$ of P in Q acts on Q. Define the underlying set

$$P\backslash Q := Q/\mathrm{L\,Mlt}_Q P \tag{2.1}$$

of a permutation representation $P\backslash Q$ of Q as the set of orbits of the action of the permutation group $\mathrm{LMlt}_Q P$ of Q. For each element q of Q, a Markov chain will be defined on the set $P\backslash Q$ of states. This set of Markov chains on the state space $P\backslash Q$, one for each element q of Q, will comprise the full structure of the quasigroup permutation representation $P\backslash Q$. Thus the key step is to define the transition matrix $R_{P\backslash Q}(q)$ of the Markov chain corresponding to an element q of Q.

The transition matrices will be defined in terms of an incidence matrix A_P and its pseudoinverse A_P^+. The incidence matrix A_P is the incidence matrix of the membership relation between the set Q and the set $P\backslash Q$ of subsets of Q. As such, it is a $|Q| \times |P\backslash Q|$ matrix. Consider the row corresponding to an element x of Q and the column corresponding to an orbit X of $\mathrm{LMlt}_Q P$ on Q. Then the entry in this row and column is 1 if $x \in X$, and 0 otherwise.

Recall that the *pseudoinverse* A^+ of a complex matrix A is the unique [2, Theorem 1.5; 14] matrix A^+ satisfying the equations

$$\begin{aligned} &\text{(a)}\ AA^+A = A;\\ &\text{(b)}\ A^+AA^+ = A^+;\\ &\text{(c)}\ (A^+A)^* = A^+A;\\ &\text{(d)}\ (AA^+)^* = AA^+, \end{aligned} \tag{2.2}$$

in which the "$*$" denotes the conjugate transpose.

Theorem 2.1 *For a subquasigroup P of a non-empty quasigroup Q, the pseudoinverse A_P^+ of the incidence matrix A_P is the $|P\backslash Q| \times |Q|$ matrix whose entry in the row indexed by $\mathrm{LMlt}_Q P$-orbit X and column indexed by Q-element x is given by*

$$\textbf{if } x \in X, \textbf{ then } |X|^{-1} \textbf{ else } 0. \tag{2.3}$$

Proof. To simplify notation, drop the suffix P from the matrices A_P and A_P^+. Matrix suffices x and y will then correspond to elements of Q, while suffices X and Y will correspond to orbits of $\mathrm{LMlt}_Q P$. The various equations of (2.2) have to be verified. For (a) and (b), consideration of the relationship

$$x \in Y \ni y \in X \tag{2.4}$$

will be critical. For fixed x in Q and X in $P\backslash Q$, note that (2.4) can hold only if $X = Y$, and that it will then hold for each of the $|X|$ elements y of X.

(a) For $x \in Q$ and $X \in P\backslash Q$, consider the equation

$$(AA^+A)_{xX} = \sum_{Y\in P\backslash Q}\sum_{y\in Q} A_{xY}A^+_{Yy}A_{yX}. \tag{2.5}$$

A summand on the right-hand side is non-zero precisely when (2.4) holds. For $x \notin X$, there are no such summands, so $(AA^+A)_{xX}$ takes the value zero of A_{xX} for this case. On the other hand, if $x \in X$, then each of the $|X|$ non-zero summands in (2.5) is $|X|^{-1}$, so that the sum yielding $(AA^+A)_{xX}$ agrees with the value of A_{xX} (namely 1) for this case as well.

(b) For $x \in Q$ and $X \in P\backslash Q$, consider the equation

$$(A^+AA^+)_{Xx} = \sum_{y\in Q}\sum_{Y\in P\backslash Q} A^+_{Xy}A_{yY}A^+_{Yx}. \tag{2.6}$$

A summand on the right-hand side of (2.6) is non-zero precisely when (2.4) holds. For $x \notin X$, there are no such summands, so $(A^+AA^+)_{Xx}$ takes the value zero of A^+_{Xx} for this case. On the other hand, if $x \in X$, then each of the $|X|$ non-zero summands in (2.6) is $|X|^{-2}$ so that the sum yielding $(A^+AA^+)_{Xx}$ agrees with the value of A^+_{Xx} (namely $|X|^{-1}$) for this case as well.

(c) For X and Y in $P\backslash Q$, consider the equation

$$(A^+A)_{XY} = \sum_{y\in Q} A^+_{Xy}A_{yY}. \tag{2.7}$$

Here, the relation

$$X \ni y \in Y, \tag{2.8}$$

holding only if $X = Y$, and then precisely for each of the $|X|$ elements y of X, is critical. If (2.8) holds, then $A^+_{Xy}A_{yY}$ takes the value $|X|^{-1}$. Thus

$$(A^+A)_{XY} = \delta_{XY}, \tag{2.9}$$

from which (c) follows.

(d) For x and y in Q, consider the equation

$$(AA^+)_{xy} = \sum_{X\in P\backslash Q} A_{xX}A^+_{Xy}. \tag{2.10}$$

Note that a summand $A_{xX}A^+_{Xy}$ of (2.10) is non-zero if and only if x and y both lie in X, in which case the non-zero value is the real number $|X|^{-1}$. Since orbit-sharing is a symmetrical relation on Q, (d) holds. □

Corollary 2.2 *By (2.9), it follows that*

$$A_P^+A_P = I_{|P\backslash Q|}, \tag{2.11}$$

the identity matrix of size $|P\backslash Q|$. □

The incidence matrix A_P and its pseudoinverse A_P^+ may now be used to define the transition matrix $R_{P\backslash Q}(q)$ specifying the Markov chain that an element q of Q induces on the state space $P\backslash Q$. Consider $R(q)$ as a permutation matrix with rows and columns indexed by the elements of Q.

Definition 2.3. *The transition matrix on $P\backslash Q$ specified by an element q of Q is*

$$R_{P\backslash Q}(q) = A_P^+R(q)A_P. \tag{2.12}$$

□

Theorem 2.4. *Definition 2.3 yields a Markov chain on the state space $P\backslash Q$ of $\mathrm{LMlt}_Q P$-orbits on Q. The probability of transition from an orbit X to an orbit Y is given as*

$$|X \cap YR(q)^{-1}|/|X|. \tag{2.13}$$

Proof. By (2.12), one has

$$
\begin{aligned}
[R_{P\backslash Q}(q)]_{XY} &= \sum_{x\in Q}\sum_{y\in Q} A^+_{Xx} R(q)_{xy} A_{yY} \\
&= \sum_{x\in Q} A^+_{Xx} A_{(xq)Y} = \sum_{x\in X} A^+_{Xx} A_{(xq)Y} \\
&= |X|^{-1} |\{x | x \in X, xq \in Y\}| \\
&= |X|^{-1} |X \cap Y R(q)^{-1}|,
\end{aligned}
$$

yielding (2.13). Moreover, summing (2.13) over all elements Y of $P\backslash Q$ yields the value 1, since the image of the partition $P\backslash Q$ of Q under the permutation $R(q)^{-1}$ of Q is again a partition of Q. □

3. A Graphical Illustration

In order to visualize the ideas of the preceding section, it is sometimes helpful to use the methods of graph theory. Consider a quasigroup Q with multiplication table

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

(3.1)

Let P be the singleton subquasigroup $\{1\}$. Note that $\mathrm{LMlt}_Q P$ is the cyclic subgroup of $Q!$ generated by $(23)(456)$. Label the respective orbits $\{1\}$, $\{2,3\}$, $\{4,5,6\}$ of $\mathrm{LMlt}_Q P$ on Q by their 2-power representatives 1,2,4, so that $P\backslash Q = \{1,2,4\}$. The Markov chain given by $R_{P\backslash Q}(5)$ may then be determined from the graph of Fig. 1. The bipartite graphs on the left- and right-hand sides of the figure specify the incidence between elements of Q and elements of $P\backslash Q$. Thus A_P is the incidence matrix of these bipartite graphs. Reading from left to right, the central portion of the figure describes the action $2R(5) = 4$, $3R(5) = 5$, etc., of $R(5)$ on Q. (Note that $R(5)$ is actually involutory, so that the edges describing the action of $R(5)$ may be drawn undirected.) The transitions in the Markov chain given by $R(5)$ on $P\backslash Q$ may now be read from left to right across Fig. 1. The probabilities of passage from an element of $P\backslash Q$ across the left-hand bipartite graph to Q are given by the pseudoinverse A_P^+. In other words, if a vertex of $P\backslash Q$ has valency v, the probability of passage along any edge incident to it is $1/v$. For example, there is a probability of $1/3$ for passage from the vertex 4 of $P\backslash Q$ to each of the vertices 4,5,6

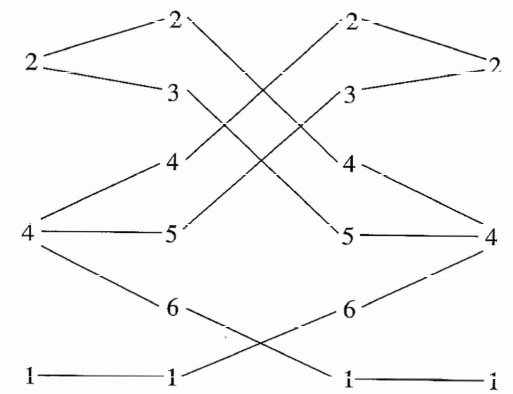

Fig. 1.

of Q. From each vertex of Q on the left-hand side of the central part of Fig. 1, there is then a unique path across to a vertex of $P\backslash Q$ on the right-hand side of the figure. Thus in $R_{P\backslash Q}(5)$, there is a probability $1/3$ of transition from 4 to 1, and probability $2/3$ of transition from 4 to 2.

4. Linear Representations

Let P be a subquasigroup of a finite quasigroup Q. Consider the complex vector spaces $\mathbb{C}Q$ with basis Q and $\mathbb{C}P\backslash Q$ with basis $P\backslash Q$. Identify linear maps between these spaces (and themselves) by their matrices with respect to these bases. Now, Eq. (2.12) yields a function ρ or

$$\rho_{P\backslash Q} : \mathrm{End}_{\mathbb{C}}\mathbb{C}Q \to \mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q;\ C \mapsto A_P^+ C A_P \tag{4.1}$$

from the set of endomorphisms of the vector space $\mathbb{C}Q$ to the set of endomorphisms of the vector space $\mathbb{C}P\backslash Q$. The function (4.1) is linear, but is generally not a homomorphism for the monoid structures of the endomorphism sets under composition. In the example of the previous section, one has

$$R_{P\backslash Q}(5)^2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1/3 & 2/3 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1/3 & 2/3 & 0 \\ 1/3 & 2/3 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{4.2}$$

although $R_Q(5)^2 = 1_{\mathbb{C}Q}$ maps to $A_P^+ A_P$ under $\rho_{P\backslash Q}$, and $A_P^+ A_P = 1_{\mathbb{C}P\backslash Q}$ by Corollary 2.2. The aim of this section is to define a new associative multiplication on $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ such that, with this new multiplication and the old linear structure, $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ becomes a (non-unital) ring and $\rho_{P\backslash Q}$ becomes a ring homomorphism, restricting to representations of various subrings associated with P and Q. To this end, define the element

$$E_P = A_P A_P^+ \tag{4.3}$$

of $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$. By (2.2)(a), E_P is an idempotent of $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ under composition. Consider

$$(C, D) \mapsto CE_P D \tag{4.4}$$

as a binary operation on $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$. It is convenient to denote this binary operation by E_P, regarding the right-hand side of (4.4) as infix notation for the binary operation.

Proposition 4.1 *Under the original $\mathbb{C}$-space structure and the multiplication E_P, the set $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ forms a non-unital ring. The map (4.1) then becomes a ring homomorphism*

$$\rho_{P\backslash Q} : (\mathrm{End}_{\mathbb{C}}\mathbb{C}Q, +, E_P) \to (\mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q, +, \cdot) \tag{4.5}$$

from this non-unital ring $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ to the ring $\mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q$ with the original multiplication given by composition.

Proof. The associative and distributive laws for $(\mathrm{End}_{\mathbb{C}}\mathbb{C}Q, +, E_P)$ are immediate. Then for C and D in $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$, one has $C^\rho D^\rho = A_P^+ C A_P A_P^+ D A_P = (CE_P D)^\rho$, as required. □

In order to restrict the ring homomorphism (4.5), one needs to locate E_P within the image of $\mathbb{C}\mathrm{Mlt}Q$ under its representation π on $\mathbb{C}Q$. For a finite subset S of a $\mathbb{C}$-space V, define the *barycenter*

$$\bar{S} = |S|^{-1} \sum_{v \in S} v. \tag{4.6}$$

Theorem 4.2 *For the subquasigroup P of Q, one has*

$$E_P = \overline{\pi(\mathrm{LMlt}_Q P)}. \tag{4.7}$$

In particular, E_P is an element of $\pi(\mathbb{C}\mathrm{LMlt}_Q P)$.

Proof. To simplify notation, abbreviate $\pi(\mathrm{LMlt}_Q P)$ to L, and drop the suffix P from A_P and A_P^+, as in the proof of Theorem 2.1. For an element x of (the basis) Q (of $\mathbb{C}Q$), it must be shown that the endomorphisms on each side of (4.7) have the same effect on x. Now, $xE_P = xAA^+ = \sum_{y \in Q} x(AA^+)_{xy} = x \sum_{X \in P\backslash Q} \sum_{y \in Q} A_{xX} A_{Xy}^+ = x \sum_{y \in xL} A_{x,xL} A_{xL,y}^+ = \sum_{y \in xL} (xL) A_{xL,y}^+ = |xL|^{-1} \sum_{y \in xL} y = \overline{xL}$. On the other hand, $x\bar{L} = |L|^{-1} \sum_{g \in L} xg = |L|^{-1} \cdot (|L|/|xL|) \sum_{y \in xL} y = \overline{xL}$ as well. □

Corollary 4.3. *The ring homomorphism (4.5) restricts to a representation*

$$\rho_{P\backslash Q} : (\pi(\mathbb{C}\mathrm{Mlt}_Q P), +, E_P) \to \mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q. \tag{4.8}$$

□

Corollary 4.4. *Consider the $\mathbb{C}$-subalgebra $\langle \mathrm{RMlt}Q, E_P \rangle$ of the algebra $(\pi(\mathbb{C}\mathrm{Mlt}Q), +, \cdot)$ generated by $\pi(\mathrm{RMlt}Q)$ and E_P. Then (4.5) restricts to a representation*

$$\rho_{P\backslash Q} : (\langle \mathrm{RMlt}Q, E_P \rangle, +, E_P) \to (\mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q, +, \cdot). \tag{4.9}$$

□

Note that the centralizer ring $V(\mathrm{Mlt}Q, Q) = \mathrm{End}_{\mathbb{C}\mathrm{Mlt}Q}\mathbb{C}Q$ is a ring of endomorphisms of the domain of the representation (4.9).

The following result is quite natural in view of the way that Definition 2.3 set out to generalize from the group case.

Corollary 4.5. *If Q is a group, then (4.1) restricts to a ring homomorphism*

$$\rho : \pi(\mathbb{C}\mathrm{RMlt}Q) \to \mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q. \tag{4.10}$$

Proof. If Q is a group, then $\mathrm{LMlt}Q$ commutes with $\mathrm{RMlt}Q$. By Theorem 4.2, it follows that E_P commutes with $\pi(\mathrm{RMlt}Q)$. Thus for C and D in $\pi(\mathbb{C}\mathrm{RMlt}Q)$, one has $C^\rho D^\rho = A_P^+ C A_P A_P^+ D A_P = A_P^+ C E_P D A_P = A_P^+ E_P C D A_P = A_P^+ A_P A_P^+ C D A_P = A_P^+ C D A_P = (CD)^\rho$, using (4.3) and (2.2)(b). □

Using Corollary 4.5, one may connect the customary linear permutation representation (4.10) of a group Q with its linear quasigroup permutation representation (4.9).

Theorem 4.6 *Let P be a subgroup of a group Q. Then there is a non-unital ring homomorphism*

$$\mathrm{L}(E_P) : \pi(\mathbb{C}\mathrm{RMlt}Q) \to (\langle \mathrm{RMlt}Q, E_P \rangle, +, E_P) \tag{4.11}$$

given via left multiplication $\mathrm{L}(E_P) : C \mapsto E_P C$ by E_P, such that the group representation ρ of (4.10) factors through the quasigroup representation $\rho_{P\backslash Q}$ of (4.9) as

$$\rho = \mathrm{L}(E_P) \cdot \rho_{P\backslash Q}. \tag{4.12}$$

Proof. Arguing as in the proof of Corollary 4.5, one has $(E_P C)(E_P D) = E_P^2 C D = E_P C D$ for C and D in $\pi(\mathbb{C}\mathrm{RMlt}Q)$. Thus, (4.11) is a ring homomorphism. Similarly, for C in $\pi(\mathbb{C}\mathrm{RMlt}Q)$, one has $C\mathrm{L}(E_P)\rho_{P\backslash Q} = A_P^+ E_P C A_P = A_P^+ A_P A_P^+ C A_P = A_P^+ C A_P = C\rho$, verifying (4.12). □

5. Burnside's Lemma

Let q be an element of a quasigroup Q with subquasigroup P. The matrix $R_{P\backslash Q}(q)$ of Definition 2.3 is the transition matrix specifying the Markov chain action of q on $P\backslash Q$. The trace of $R_{P\backslash Q}(q)$ gives the expected number of points fixed by the action of q. In the example of Sec. 3, one has

$$R_{P\backslash Q}(2) = \begin{bmatrix} 0 & 1 & 0 \\ 1/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{5.1}$$

Thus the point 4 of $P\backslash Q$ always stays fixed, the point 1 never stays fixed, while the point 2 is fixed with probability 1/2. Overall, the expected number of fixed points of the quasigroup element 2 acting on $P\backslash Q$ is 1.5, the trace of $R_{P\backslash Q}$ (2). If Q is a group, so that $P\backslash Q$ is a transitive Q-set, then Burnside's Lemma expresses the number of orbits, namely 1 in this case, as the average of the (expected) number of fixed points of the $|Q|$ elements of Q [21, Theorem I3.1.2]. The following theorem shows that Burnside's Lemma still holds in the quasigroup case.

Theorem 5.1. *Let P be a subquasigroup of a finite, non-empty quasigroup Q. Then the average expected number of fixed points of the* $|Q|$ *elements of Q is*

$$\frac{1}{|Q|}\sum_{q\in Q}\operatorname{tr} R_{P\backslash Q}(q) = 1. \tag{5.2}$$

Proof. Consider the action of R Mlt$Q$ on the vector space $\mathbb{C}Q$, as in the previous section. Given x and y in Q, there is a unique element q of Q such that $xq = y$ or $xR(q) = y$. Thus the sum $\Sigma_{q\in Q}R(q)$ of the permutation matrices $R(q)$ over all the elements of q is the $|Q| \times |Q|$ matrix J, each of whose entries is 1. Use notation as in the proof of Theorem 2.1. One then has

$$\begin{aligned}\sum_{q\in Q}\operatorname{tr}R_{P\backslash Q}(q) &= \operatorname{tr}\sum_{q\in Q}R_{P\backslash Q}(q)\\ &= \operatorname{tr}\sum_{q\in Q}A_P^+R(q)A_P\\ &= \operatorname{tr} A_P^+JA_P\\ &= \sum_{X\in P\backslash Q}\ \sum_{y\in Q}\ \sum_{x\in Q}A_{Xy}^+J_{yx}A_{xX}\\ &= \sum_{X\in P\backslash Q}\ \sum_{y\in Q}\ \sum_{x\in Q}A_{Xy}^+A_{xX}\\ &= \sum_{X\in P\backslash Q}\Big(\sum_{y\in Q}A_{Xy}^+\Big)\Big(\sum_{X\in Q}A_{xX}\Big)\\ &= \sum_{X\in P\backslash Q}\Big(\sum_{y\in X}A_{Xy}^+\Big)\Big(\sum_{x\in X}A_{xX}\Big)\\ &= \sum_{X\in P\backslash Q}1\cdot|X| = |Q|,\end{aligned}$$

the final equality holding since $P\backslash Q$ is a partition of Q. Equation (5.2) follows. □

References

1. Bannai, E., Ito, T.: *Algebraic Combinatorics I*, Benjamin Cummings, Menlo Park, 1984.
2. Boullion, T.L., Odell, P.L.: *Generalized Inverse Matrices*, John Wiley & Sons, New York, 1971.
3. Chein, O., Pflugfelder, H., Smith, J.D.H., eds.: *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.
4. Dharwadker, A., Smith, J.D.H.: Split extensions and representations of Moufang loops, *Commun. Alg.* **23**, 4245–4255 (1995).
5. Fuad, T.S.R., Smith, J.D.H.: Quasigroups, right quasigroups and category coverings, *Alg. Univ.* **35**, 233–248 (1996).
6. Johnson, K.W.: Latin square determinants, *Algebraic, Extremal and Metric Combinatorics 1986*, Deza, M.-M., Frankl, P., Rosenberg, I.G., eds., Cambridge University Press, Cambridge, pp. 146–154, 1988.

7. Johnson, K.W.: Some historical aspects of the representation theory of groups and its extension to quasigroups, *Universal Algebra and Quasigroup Theory*, Romanowska, A., Smith, J.D.H., eds., Heldermann, Berlin, pp. 101–117, 1992.
8. Johnson, K.W., Smith, J.D.H.: Characters of finite quasigroups, *Europ. J. Combinatorics* **5**, 43–50 (1984).
9. Johnson, K.W., Smith, J.D.H.: Characters of finite quasigroups II: Induced characters, *Europ. J. Combinatorics* **7**, 131–137 (1986).
10. Johnson, K.W., Smith, J.D.H.: Characters of finite quasigroups III: Quotients and fusion, *Europ. J. Combinatorics* **10**, 47–56 (1989).
11. Johnson, K.W., Smith, J.D.H.: Characters of finite quasigroups IV: Products and superschemes, *Europ. J. Combinatorics* **10**, 257–263 (1989).
12. Johnson, K.W., Smith, J.D.H.: Characters of finite quasigroups V: Linear characters, *Europ. J. Combinatorics* **10**, 449–456 (1989).
13. Johnson, K.W., Smith, J.D.H., Song, S.Y.: Characters of finite quasigroups VI: Critical examples and doubletons, *Europ. J. Combinatorics* **11**, 267–275 (1990).
14. Penrose, R.: A generalized inverse for matrices, *Proc. Camb. Phil. Soc.* **51**, 406–413 (1955).
15. Smith, J.D.H.: Centralizer rings of multiplication groups on quasigroups, *Math. Proc. Camb. Phil. Soc.* **79**, 427–431 (1976).
16. Smith, J.D.H.: *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, Montréal, 1986.
17. Smith, J.D.H.: Quasigroups, association schemes, and Laplace operators on almost-periodic functions, *Algebraic, Extremal and Metric Combinatorics 1986*, Deza, M.-M., Frankl, P., Rosenberg, I.G., eds., Cambridge University Press, Cambridge, pp. 205–218, 1988.
18. Smith, J.D.H.: Entropy, character theory and centrality of finite quasigroups, *Math. Proc. Camb. Phil. Soc.* **108**, 435–443 (1990).
19. Smith, J.D.H.: Combinatorial characters of quasigroups, *Coding Theory and Design Theory Part I: Coding Theory*, Ray-Chaudhuri, D., ed., Springer-Verlag, New York, pp. 163–187, 1990.
20. Smith, J.D.H.: Quasigroup representation theory, *Universal Algebra and Quasigroup Theory*, Romanowska, A., Smith, J.D.H., eds., Heldermann, Berlin, pp. 195–207, 1992.
21. Smith, J.D.H., Romanowska, A.B.: *Post-Modern Algebra*, John Wiley & Sons, New York, 1999.