Quasigroups and Related Systems **14** (2006), 27 – 41

# The construction of loops using right division and Ward quasigroups

*Kenneth W. Johnson*

**Abstract**

Constructions are given of families of loops which can be described in terms of the table obtained from the loop by using the operation of right division. The motivation comes from group representation theory and the group matrix which goes back to Frobenius.

## 1. Introduction

The point of departure of this paper is the study of a group or a loop $Q$ via the multiplication table $W(Q)$ under the operation of right division. The right division operation of a group was used by Frobenius in [3] where group characters and representation theory first appear, and the symmetry of the table corresponding to this operation is used extensively in Frobenius' work. Recently these multiplication tables were discussed in more detail in [9], where Ward quasigroups appear and some comments are made related to the extension to loops. We discuss here how interesting loops can be constructed by relaxing some of the strong symmetry of $W(G)$ for a group $G$. Often families of loops have been constructed by forming extensions

$$1 \to G \to Q \to H \to 1 \tag{1}$$

where $G$ and $H$ are groups, $H$ is normal in $Q$ and $Q/H \simeq G$. For example the family of Moufang loops $M(G,2)$ constructed by Chein in [1] are of this form with an arbitrary non-commutative group $G$ and $H \simeq C_2$, the cyclic group of order 2. A symmetric construction of $W(Q)$ arising from an extension of the form (1) can be given in this case. Several families of

2000 Mathematics Subject Classification: 20N05
Keywords: Quasigroup, Ward quasigroup, right division, Frobenius

such loops are described below. A simple example occurs when $G \simeq C_n$ and $H \simeq C_2$, and the latin square of $(Q, \backslash)$ is defined to be

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

where $A$ is $W(G)$ (which will usually be written in terms of $\{1, ..., n\}$) and $B$ is the ordinary multiplication table of $G$ (usually written in terms of $\{n+1, ..., 2n\}$). Then $(Q, .)$ is $D_{2n}$, the dihedral group of order $2n$. If we take any nonabelian group $G$ then the corresponding loop $(Q, .)$ is non-associative and we call this the $D(G)$, the *dihedral extension* of $G$.

The table $W(G)$ corresponding to a group $G$ has very strict symmetry which is explored in [9]. If some of this symmetry is relaxed, the table will correspond to a non-associative loop, but in general this loop need not have nice properties. We give examples of loops $Q$ of order 6 which have $W(Q)$ (defined analogously) close to $W(G)$ for a group $G$, and which satisfy common algebraic identities. We also show how the Moufang loops $M(G, 2)$ of small orders have $W(Q)$ which can easily be described and that in particular $M(D_{2n}, 2)$ has a Ward table which is made up of block circulants and reverse circulants. In [10] a variation on a group split extension is given which produces a Bol loop. We describe the Ward tables in this case and show the tables of a group and its corresponding loop. The ideas here are in the same direction as those in the works of Drápal on distances between groups and loops [2].

In Section 2 a summary of the relevant work on Ward-Dedekind quasigroups is given, and a discussion of tables for $W(Q)$ for loops of order 6 and Moufang loops is given. The next section first describes $W(D)$ where $D$ is a group split extension $G \times H$ arising from an action of $G$ on $H$ and then points out how this can be modified to produce the Bol split extension described in [10]. In Section 4 there is given the construction and some properties of dihedral extensions and Frobenius extensions and some remarks and conjectures form the remaining section.

## 2. Ward quasigroups and variations

Consider the quasigroup $(Q, *)$ obtained from a finite group $(G, .)$ of order $n$ using right division which we write as $(*)$, i.e. $g * h = gh^{-1}$. It is reasonably well-known that such quasigroups may be characterised as those satisfying the identity

$$(x * z) * (y * z) = x * y.$$

Quasigroups satisfying this identity are called *Ward quasigroups*. We refer to [9] for the details. Suppose that $H =< s >$ is any cyclic subgroup of $G$ of order $m$ and let $\{x_1 = e, x_2, ..., x_r\}$ be a left transversal to $H$ in $G$. If the left cosets of $H$ in $G$ are ordered as $\{eH, x_2H, ..., x_rH\}$ and each coset $x_iH$ is ordered as

$$x_i, x_is, x_is^2, ...x_is^{m-1}$$

the multiplication table $W(Q, H)$ of $(Q, *)$ with rows and columns indexed by the elements of $G$ in this order has the following properties.

(i) It consists of $m \times m$ blocks of circulant matrices. (The *circulant* $C(a_1, a_2, ...a_u)$ is a $u \times u$ matrix each row of which is obtained from the previous one by a right shift with wrap-around:

$$C(a_1, a_2, ...a_u) = \begin{bmatrix} a_1 & a_2 & a_3 & ... & a_u \\ a_u & a_1 & a_2 & ... & a_{u-1} \\ & & ... & & \\ a_2 & a_3 & ... & a_u & a_1 \end{bmatrix}).$$

(ii) Define the *inverse pattern* $\pi : G \to G$ by $\pi(g) = g^{-1}$. Then $W(Q, H)(i, j) = \pi(W(Q, H)(j, i))$.

(iii) $W(Q, H)(i_1, j) * W(Q, H)(i_2, j) = W(Q, H)(i_1, k) * W(Q, H)(i_2, k)$ for all $i_1, i_2, j, k$ , i.e. the product under $*$ of corresponding elements of a fixed pair of rows is constant.

(iv) The identity element appears in the diagonal.

The following examples illustrate the symmetrical tables $W(Q, H)$ described above.

(1) Let $G = S_3$, the symmetric group on 3 objects and $H$ be the subgroup generated by a 3-cycle. Then

$$W(Q, H) = \begin{bmatrix} 1 & 3 & 2 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \\ 3 & 2 & 1 & 5 & 6 & 4 \\ 4 & 6 & 5 & 1 & 2 & 3 \\ 5 & 4 & 6 & 3 & 1 & 2 \\ 5 & 5 & 4 & 2 & 3 & 1 \end{bmatrix}.$$

Usually tables such as that above will be written in abbreviated form as

$$\begin{bmatrix} C(1, 3, 2) & C(4, 5, 6) \\ C(4, 6, 5) & C(1, 2, 3) \end{bmatrix} \tag{2}$$

(2) More generally if $G = D_{2n}$ and $H = C_n$ the table of $W(Q, H)$ is

$$\begin{bmatrix} C(1, n, n-1, ..., 2) & C(n+1, n+2, ..., 2n) \\ C(n+1, 2n, 2n-1, ..., n+2) & C(1, 2, ..., n) \end{bmatrix}$$

which may also be written

$$\begin{bmatrix} A^t & B \\ B^t & A \end{bmatrix}$$

where $A = C(1, 2, ..., n)$ and $B = C(n+1, n+2, ..., 2n)$.

(3) Let $G = A_4$, the alternating group. Here we take

$$H = \{e,\ (1,2)(3,4)\}$$

but we order the left cosets of $H$ by listing the cosets of the normaliser of $H$, which is of course the Klein 4-group $V$. Specifically, the list is

$V = \{e, (1,2)(3,4), (1,4)(2,3), (1,3)(2,4)\} = H + (1,4)(2,3)H$.

$(1,2,3)V = \{(1,2,3), (2,4,3), (1,4,2), (1,3,4)\} = (1,2,3)H + (1,4,2)H$

$(1,3,2)V = \{(1,3,2), (1,4,3), (1,2,4), (2,3,4)\} = (1,3,2)H + (1,2,4)H$.

To simplify the table we write the above cosets as

$$V = \{1^1, 2^1, 3^1, 4^1\},\ (1,2,3)V = \{1^2, 2^2, 3^2, 4^2\},\ (1,3,2)V = \{1^3, 2^3, 3^3, 4^3\}.$$

Then $W(Q, H)$ is

$$\begin{bmatrix} MV(1,2,3,4)^1 & MV(1,4,3,2)^3 & MV(1,3,4,2)^2 \\ MV(1,2,3,4)^2 & MV(1,4,3,2)^1 & MV(1,3,4,2)^3 \\ MV(1,2,3,4)^3 & MV(1,4,3,2)^2 & MV(1,3,4,2)^1 \end{bmatrix}$$

where

$$MV(1,2,3,4)^i = \begin{bmatrix} 1^i & 2^i & 3^i & 4^i \\ 2^i & 1^i & 4^i & 3^i \\ 3^i & 4^i & 1^i & 2^i \\ 4^i & 3^i & 2^i & 1^i \end{bmatrix}.$$

This illustrates how the cosets of the normaliser of $H$ can be used to further organise $W(Q, H)$.

Now consider the loops produced when some of the the restrictions on the symmetry of $W(Q, H)$ are relaxed. Given symbols $c_1, \ldots, c_n$, we denote by $R(c_1, \ldots, c_n)$ the *reversed circulant matrix*

$$\begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_2 & c_3 & \cdots & c_1 \\ \vdots & \vdots & & \vdots \\ c_n & c_1 & \ldots & c_{n-1}. \end{bmatrix}.$$

We first look at some examples of loops of order 6. If we take $G$ as $C_6$ and $H$ as $C_2$ then $W(Q,H)$ is

$$\begin{bmatrix} C(1,2) & C(5,6) & C(3,4) \\ C(3,4) & C(1,2) & C(5,6) \\ C(5,6) & C(3,4) & C(1,2) \end{bmatrix}.$$

There is a unique non-associative loop of order 6 which has a normal subloop of order 2 with $W(Q,H)$ as below

$$\begin{bmatrix} C(1,2) & C(5,6) & C(3,4) \\ C(3,4) & C(1,2) & C(6,5) \\ C(5,6) & C(3,4) & C(1,2) \end{bmatrix}$$

where the difference is seen to be in the $(2,3)$ block. The corresponding loop is commutative, and satisfies the weak inverse and weak inverse abelian properties.

Several loops of order 6 have a normal $C_3$. The closest variation on the table (2) is

$$\begin{bmatrix} C(1,3,2) & C(4,5,6) \\ C(4,6,5) & C(1,3,2) \end{bmatrix} \tag{3}$$

which corresponds to an inverse property loop. It is seen that the circulant in the $(2,2)^{\text{th}}$ place has been modified. The loop is isotopic to the loop with $W(Q,H)$

$$\begin{bmatrix} C(1,3,2) & C(4,5,6) \\ R(4,5,6) & C(1,3,2) \end{bmatrix}$$

which is commutative, and satisfies the inverse property.

Further examples are

$$\begin{bmatrix} C(1,3,2) & R(4,5,6) \\ C(4,6,5) & C(1,3,2) \end{bmatrix}$$

whose corresponding loop satisfies the right inverse property, and

$$\begin{bmatrix} C(1,3,2) & C(5,6,4) \\ R(4,5,6) & C(1,3,2) \end{bmatrix}$$

with corresponding loop satisfying the weak inverse, generalized Moufang and generalized Bol properties.

Now suppose we start with a non-associative loop $G$ which has two-sided inverses and satisfies the automorphic inverse property. In a similar fashion to that above the "generalized Ward quasigroup" $(Q,*)$ may be constructed from $G$ by $x*y = xy^{-1}$. In general the left cosets of a subloop $H$ need not partition $G$ and even if they do the set $(a_iH)(a_jH)^{-1}$ may contain more than $|H|$ elements, but we can avoid this problem if we take $H$ to be a normal cyclic subgroup of $G$. The resulting multiplication table of $(Q,*)$ satisfies (ii) and (iv) above but if $G$ is not associative (iii) cannot be satisfied. We use $W(G,H)$ to denote the multiplication table of $(Q,*)$ with the elements of $G$ ordered by left cosets of $H$ exactly as above for groups.

Let $P$ be the smallest non-associative Moufang loop $M_{12}$ of order 12 and let $H$ be the unique subgroup of order 3. Then $W(P,H)$ is

$$\begin{bmatrix} C(1,3,2) & C(4,5,6) & C(7,8,9) & C(10,11,12) \\ C(4,6,5) & C(1,2,3) & R(10,12,11) & R(7,9,8) \\ C(7,9,8) & R(10,12,11) & C(1,2,3) & R(4,6,5) \\ C(10,12,11) & R(7,9,8) & R(4,6,5) & C(1,2,3). \end{bmatrix} \tag{4}$$

Note that the first row and column (of blocks) and the blocks on the diagonal are determined by diassociativity and it is interesting to note how the remaining part of the table has nice symmetry. The table obviously violates condition (i) above and it is easy to see that (iii) also fails. It may also be remarked that the inverse pattern of $(Q,*)$, which may be read off from the first row of the table could not give rise to a group, as there is no group of order 12 with 9 involutions.

There are 5 nonassociative Moufang loops of order 16 and each of them has a cyclic normal subloop of order 4 (cf. [4]). The multiplication tables of the associated quasigroups can be all written in such a way that every $4\times 4$ block in the first row, first column or along the main diagonal is a circulant, while every other block is a reversed circulant. It seems unlikely that arbitrary Moufang loops with a normal cyclic subgroup would have a table of this form, but if $K$ is $M(D_n,2)$ the table $T(K,C_n)$ is similar to (4) in that the blocks which are not forced by diassociativity to be circulants are reverse circulants of the form $R(m+1,m+n,m+n-1,...,m+2)$. [1]

The Chein construction $M(G,2)$ may be given explicitly as follows. Con-

1. The referee has informed me that there is a loop of order 32 with a normal cyclic subloop of order 4 which has off-diagonal blocks which are neither circulants nor reversed circulants.

sider the set $G \times C_2$ with multiplication

$$\begin{aligned}(g,0)(h,0) &= (gh,0)\\(g,0)(h,1) &= (hg,1)\\(g,1)(h,0) &= (gh^{-1},1)\\(g,1)(h,1) &= (h^{-1}g,0).\end{aligned}$$

It is well known that $M(G,2)$ is Moufang and if $G$ is not commutative it is nonassociative. The table $W(M(G,2))$ may be written

$$\begin{bmatrix} A & B \\ B^T & \pi(A^T)\pi \end{bmatrix}$$

where $A$ is $(W(G),0)$ and $B$ is the table of the multiplication on the set $(G,1)$ given by $(g,1)(h,1) = (gh,1)$, $\pi$ is the inverse map and we also denote by $\pi$ the permutation matrix of order $n \times n$ corresponding to $\pi$.

## 3. Split Extensions

In [10] a variation on the split extension of two groups is used to construct a family of Bol loops. If we have two groups $G$ and $H$ with an homomorphism $\beta : G \to aut(H)$ the split extension $G \rtimes H$ may be constructed on the set $G \times H$ by the explicit multiplication

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1^{\beta(g_2)}h_2).$$

The variation on this construction to given in [10] is

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1^{\beta(g_2^{-1})}h_2)$$

and if $\mathrm{Im}(\beta)$ is noncommutative a non-Moufang loop $G \rtimes_B H$ which satisfies the right Bol identity

$$x(yz.y) = (xy.z)y$$

is produced.

By direct calculation the right inverse $(*)$ operations are

$$(g_1,h_1) * (g_2,h_2) = (g_1g_2^{-1}, (h_1h_2^{-1})^{\beta(g_2^{-1})})$$

in the case of the $G \rtimes H$ and

$$(g_1,h_1) * (g_2,h_2) = (g_1g_2^{-1}, (h_1h_2^{-1})^{\beta(g_2)})$$

in the case of $G \rtimes_B H$. If we suppose that $W(D)$ is produced by ordering the elements of $H$ as $\{h_1 = e, h_2, ..., h_m\}$ according to the left cosets of a cyclic subgroup $S$ as described above and then ordering the elements of $G \times H$ as

$$\{(g_1, h_1), (g_1, h_2), ...., (g_1, h_m), (g_2, h_1), (g_2, h_2), ...., (g_2, h_m),$$
$$..., (g_n, h_1), (g_n, h_2), ...., (g_n, h_m)\}$$

then $W(D)$ has blocks of size $m \times m$ in the $(i,j)^{\text{th}}$ position of the form

$$\{(g_i g_{j^{-1}}, W(H)(h_1^{\beta(g_j)}, ..., h_m^{\beta(g_j)})\}$$

where $(g, W(H)(t_1, ..., t_m))$ is used to denote the square obtained by replacing $h_i$ by $(g, t_i)$ in $W(H)$. There is a similar table for $W(B)$ where in the $(i,j)^{\text{th}}$ block there appears

$$\{(g_i g_{j^{-1}}, W(H)(h_1^{\beta(g_j^{-1})}, ..., h_m^{\beta(g_j^{-1})})\}.$$

**Example.** Let $G = S_3$ and $H = V_4$. Let $\beta$ be the obvious isomorphism from $G$ to $aut(H)$. We introduce the notation $(g, V^\kappa)$ where $\kappa \in S_4$ to mean the table obtained from

$$W(V) = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}$$

by replacing the integer $i$ by the element $(g, i^\kappa)$. The group split extension is isomorphic to $S_4$ and one version of the $W(D)$ is

$$\begin{bmatrix} (e,V) & (\sigma^2, V^{(2,3,4)}) & (\sigma, V^{(2,4,3)}) & (\tau, V^{(2,3)}) & (\mu, V^{(2,4)}) & (\nu, V^{(3,4)}) \\ (\sigma,V) & (e, V^{(2,3,4)}) & (\sigma^2, V^{(2,4,3)}) & (\nu, V^{(2,3)}) & (\tau, V^{(2,4)}) & (\mu, V^{(3,4)}) \\ (\sigma^2,V) & (\sigma, V^{(2,3,4)}) & (e, V^{(2,4,3)}) & (\mu, V^{(2,3)}) & (\nu, V^{(2,4)}) & (\tau, V^{(3,4)}) \\ (\tau,V) & (\nu, V^{(2,3,4)}) & (\mu, V^{(2,4,3)}) & (e, V^{(2,3)}) & (\sigma, V^{(2,4)}) & (\sigma^2, V^{(3,4)}) \\ (\mu,V) & (\tau, V^{(2,3,4)}) & (\nu, V^{(2,4,3)}) & (\sigma^2, V^{(2,3)}) & (e, V^{(2,4)}) & (\sigma, V^{(3,4)}) \\ (\nu,V) & (\mu, V^{(2,3,4)}) & (\tau, V^{(2,4,3)}) & (\sigma, V^{(2,3)}) & (\sigma^2, V^{(2,4)}) & (e, V^{(3,4)}) \end{bmatrix}$$

The corresponding Bol split extension table is

$$\begin{bmatrix} (e,V) & (\sigma^2, V^{(2,4,3)}) & (\sigma, V^{(2,3,4)}) & (\tau, V^{(2,3)}) & (\mu, V^{(2,4)}) & (\nu, V^{(3,4)}) \\ (\sigma,V) & (e, V^{(2,4,3)}) & (\sigma^2, V^{(2,3,4)}) & (\nu, V^{(2,3)}) & (\tau, V^{(2,4)}) & (\mu, V^{(3,4)}) \\ (\sigma^2,V) & (\sigma, V^{(2,4,3)}) & (e, V^{(2,3,4)}) & (\mu, V^{(2,3)}) & (\nu, V^{(2,4)}) & (\tau, V^{(3,4)}) \\ (\tau,V) & (\nu, V^{(2,4,3)}) & (\mu, V^{(2,3,4)}) & (e, V^{(2,3)}) & (\sigma, V^{(2,4)}) & (\sigma^2, V^{(3,4)}) \\ (\mu,V) & (\tau, V^{(2,4,3)}) & (\nu, V^{(2,3,4)}) & (\sigma^2, V^{(2,3)}) & (e, V^{(2,4)}) & (\sigma, V^{(3,4)}) \\ (\nu,V) & (\mu, V^{(2,4,3)}) & (\tau, V^{(2,3,4)}) & (\sigma, V^{(2,3)}) & (\sigma^2, V^{(2,4)}) & (e, V^{(3,4)}) \end{bmatrix}$$

The difference is seen to be that the second members of the second and third columns are interchanged.

## 4. Dihedral Extensions

The author thanks the referee for the following comment. In [12] there is a classification of all constructions of loops of Bol-Moufang type with a subgroup of index 2. The dihedral extensions below appear in their notation as $(\theta_{xy}, \theta_{xy^*}, \theta_{xy^*})$.

Let $G$ be a finite group of order $n$. As above define the quasigroup $(Q(G), *)$ by

$$g * h = gh^{-1}$$

for all $g, h \in G$. Associate to $Q(G)$ the Latin square $A = W(G)$ on the set $\{1, ..., n\}$ and to $(G, .)$ a Latin square $B$ on $\{n+1, ..., 2n\}$. Suppose $\{g_1 = e, g_2, ...\ g_n\}$ is an ordering of $G$. Then $A(i, j) = k$ where $g_i * g_j = g_k$ and $B(i, j) = k + n$ where $g_i g_j = g_k$. It is easily seen that the square $B$ is obtained from square $A$ by operating on the columns by the inverse pattern $\pi$ and then adding $n$ to each entry. For example, if $G$ is the cyclic group of order 3, $A = C(1, 3, 2)$ and $B = R(4, 5, 6)$ . If we form the Latin square $L(G) = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$ we can interpret this as $W(D(G))$ as the Ward table of the loop $D(G)$. It is easily seen that in the above example $D(G)$ is isomorphic to the dihedral group $D_6$ (which is also isomorphic to $S_3$). We call $D(G)$ the *dihedral extension* of $G$. If $G$ is cyclic of order $n$ then $D(G)$ is the usual dihedral group $D_{2n}$. If $G$ is nonabelian $D(G)$ is not associative and we obtain an interesting family of loops. We can write the multiplication for $D(G)$ explicitly as follows. The elements of $D(G)$ may be taken as ordered pairs of the form $(g, \epsilon)$ where $g \in G$ and $\epsilon \in \{0, 1\}$. Then

$$\begin{aligned}
(g, 0)(h, 0) &= (gh, 0) \\
(g, 0)(h, 1) &= (gh, 1) \\
(g, 1)(h, 0) &= (gh^{-1}, 1) \\
(g, 1)(h, 1) &= (gh^{-1}, 0).
\end{aligned}$$

The non-associativity may be proved by calculating the right maps of the form $R(x, y) = R(x)R(y)R^{-1}(xy)$. Let $x = (g, \epsilon_1)$, $y = (h, \epsilon_2)$ and $z = (h, \epsilon_3)$. Then

$$xR(y, z) = \begin{cases} x & \text{if} \quad \epsilon_1 = 0 \\ (g[h, k], \epsilon_1) & \text{if} \quad \epsilon_1 = 1 \end{cases}$$

where $[h,k]$ denotes the usual commutator $h^{-1}k^{-1}hk$. It is clear that $D(G)$ is associative if and only if $G$ is commutative.

One interesting feature of dihedral extensions is that their character theory is similar to that for groups, especially if $G$ is taken to be of odd order. To discuss the character theory we first calculate the conjugacy classes. We calculate the map $T(x) = L(x)R^{-1}(x)$. Let $x = (g, \epsilon_1)$, $y = (h, \epsilon_2)$ . Then

$$xT(y) = \begin{cases} (hgh^{-1}, \epsilon_1) & \text{if} \quad \epsilon_1 = 0, \epsilon_2 = 0 \\ (hg^{-1}h^{-1}, \epsilon_1) & \text{if} \quad \epsilon_1 = 0, \epsilon_2 = 1 \\ (hgh, \epsilon_1) & \text{if} \quad \epsilon_1 = 1, \epsilon_2 = 0 \\ (hg^{-1}h, \epsilon_1) & \text{if} \quad \epsilon_1 = 1, \epsilon_2 = 1. \end{cases}$$

Further calculation shows that for the map $L(y,z) = L(y)L(z)L(yz)^{-1}$

$$xL(y,z) = (g, \epsilon_1) \ \text{ or } \ (hgh^{-1}, \epsilon_1).$$

Since the inner mapping group of $D(G)$ is generated by $\{R(y,z), T(y), L(y,z)\}$ as $y$ and $z$ run through the elements of $D(G)$ it is straightforward to determine that the conjugacy class containing an element of $D(G)$ of the form $(g, 0)$ is $\{(h, 0); h = k^{-1}gk$ or $h = k^{-1}g^{-1}k$ for some $k \in G\}$. For an element of the form $(g, 1)$ the conjugacy class is $\{(h, 1); h = uk^2$, $h = u^{-1}k^2$ for $u = t^{-1}gt$ for some $t \in G$ or $h = gc$ with $c \in G'\}$. If $G$ is of odd order the classes of $D(G)$ are easily described. The class $C_i \neq \{e\}$ of $G$ is distinct from $C_i^* = \{g^{-1} : g \in C\}$, and gives rise to the class $B_i$ of $D(G)$ of the form $\{(g, 0) : g \in C \cup C^*\}$. In addition to the identity class there is only one other class $B'$ which consists of all elements of the form $\{(g, 1) : g \in G\}$. The characters of a loop or quasigroup are defined in [11] in terms of the association scheme arising from the classes of the quasigroup.

**Theorem 1.** *Let $G$ be a group of odd order, with irreducible characters $\{\chi_1 = 1, \chi_2, \bar{\chi}_2, \dots \chi_r, \bar{\chi}_r\}$. Then the characters of $D(G)$ are*

$$\{\mu_1 = 1, \mu_1', \mu_2, \dots, \mu_r\}$$

*where the value of $\mu_i, i > 2$ on the class $\{e\}$ is $2\chi_i$, on the class $B_i$ is $\chi_i(C_i + C_i^*)$ and on the class $B'$ is $0$. The value of $\mu_1'$ on all classes of the form $\{g, 0\}$ is $1$ and on $B'$ is $-1$.*

*Proof.* It is explained in [11] that the conjugacy classes of $D(G)$ are in $1:1$ correspondence with the orbits $\Delta_i$ of $D(G) \times D(G)$ under the action of the left and right maps of $D(G)$ and the adjacency matrices $A_i$ of the corresponding association scheme are the incidence matrices of these orbits: if $\Delta_i$ is an orbit then $A_i(g,h) = 1$ if $(g,h) \in \Delta_i$ and 0 otherwise. Then the $A_i$ are as follows: if $C_j$ is the $n \times n$ incidence matrix of the class $\Phi_j$ of $G$ the $(2n \times 2n)$ incidence matrix of the class of $D(G)$ is of the form

$$\begin{bmatrix} C_j + C_j^* & 0 \\ 0 & C_j + C_j^* \end{bmatrix}.$$

and the incidence matrix of $B'$ is

$$\begin{bmatrix} 0 & J \\ J & 0 \end{bmatrix}$$

where $J$ is the all 1 matrix. Now if $\chi$ is a non-trivial irreducible character of $G$ its value on the class $C_j$ of $G$ is related to an eigenvalue $\lambda$ of $C_j$ by $\chi(C_j) = m_\chi \lambda / |C_j|$, where $m_j$ is a multiplicity. It is clear that a corresponding eigenvalue of $C_j + C_j^*$ is $\lambda + \overline{\lambda}$ where $\overline{\lambda}$ is the complex conjugate of $\lambda$ and which has multiplicity $2m_\chi$. This means that to each pair $\chi, \overline{\chi}$ there is a character $\psi$ of $D(G)$which takes on the value $2\chi(e)$ on the trivial class of $D(G)$ and $\chi(C_j) + \overline{\chi(C_j)}$ on the class $B_j$ of $D(G)$, and 0 on $B'$. The remaining character $\mu_1'$ necessarily takes on the value 1 on the elements of the form $(g, 0)$ and $-1$ on elements of the form $(g, 1)$. □

**Example.** Let $G$ be the nonabelian Frobenius group of order 21. Its character table is

$$\begin{array}{cccccc} & C_0 & C_1 & C_1^T & C_2 & C_2^T \\ \chi_0 & 1 & 1 & 1 & 1 & 1 \\ \chi_1 & 1 & 1 & 1 & \omega & \omega^2 \\ \overline{\chi_1} & 1 & 1 & 1 & \omega^2 & \omega \\ \chi_2 & 3 & \alpha & \overline{\alpha} & 0 & 0 \\ \overline{\chi_2} & 3 & \overline{\alpha} & \alpha & 0 & 0 \end{array}.$$

where $\omega = \exp(2\pi i/3)$ and $\alpha = (-1+\sqrt{7})/2$.
The corresponding table for $D(G)$ is

$$\begin{array}{ccccc} & B_0 & B_1 & B_2 & B' \\ \mu_0 & 1 & 1 & 1 & 1 \\ \mu_1 & 1 & 1 & 1 & -1 \\ \mu_2 & 2 & 2 & -1 & 0 \\ \mu_3 & 6 & -1 & 0 & 0 \end{array}.$$

As in group character theory, the product of two characters of a loop $L$ is defined by

$$(\chi.\psi)(x) = \chi(x)\psi(x).$$

For groups the product of characters is automatically a character since it corresponds to the tensor product of modules. This is no longer the case for loops, and leads to the coefficient ring $\mathbb{Z}(L)$ of a loop $L$ obtained by extending $\mathbb{Z}$ by the coefficients $a_i$ defined by

$$(\chi.\psi) = \sum a_i\chi_i(x).$$

For the dihedral extension in the case where $|G|$ is odd we show that $\mathbb{Z}(D(G)) = \mathbb{Z}$. This follows directly from the calculation

$$(\chi_i + \overline{\chi_i})(\chi_j + \overline{\chi_j}) = (\chi_i\chi_j + \overline{\chi_i\chi_j}) + (\chi_i\overline{\chi_j} + \overline{\chi_i\overline{\chi_j}}).$$

Now if $\chi_i\chi_j = \sum a_k\chi_k$ it follows that $\chi_i\chi_j + \overline{\chi_i\chi_j} = \sum a_k(\chi_k + \overline{\chi_k})$ i.e.

$$\psi_i\psi_j = \sum a_k\psi_k$$

where $i, j \geqslant 3$ and the product $\psi_i\psi_j$ where $i \leqslant 2$ is obviously $\psi_k$ for some $k$.

### 4.1. Frobenius Extensions

Suppose we take a group $G$ and construct the extension $Q = F(G, 2)$ on the set $G \times \{0, 1\}$ with explicit multiplication

$$(g, 0)(h, 0) = (gh, 0) = (g, 1)(h, 1)$$
$$(g, 0)(h, 1) = (hg, 1) = (g, 1)(h, 0).$$

The referee has also indicated that Frobenius extensions also appear in [12] described by the triple $(\theta_{yx}, \theta_{yx}, \theta_{xy})$. It may readily be seen that the multiplication table of $(Q, *)$ has the structure

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

where $A$ is $W(G)$ on the elements $(1, ..., n)$ and $B = (\pi W(G)^t\pi)$ on the elements $\{n+1, n+2, ...2n\}$ is the table under the operation $(g, h) \to h^{-1}g$ (here $\pi$ denotes the permutation matrix corresponding to $\pi$). Such squares occur in the work of Frobenius on group determinant factorisation [3]. It is straightforward to compute that if $G$ is abelian then $Q$ is the group $G \times C_2$ and that if $G$ is nonabelian $Q$ is a nonassociative loop that is not Moufang and unless strong conditions are placed on $G$ it is not diassociative.

As an example we construct the table for $F(G, 2)$ where $G \approx S_3$:We let

$$A = \begin{bmatrix} C(1,3,2) & C(4,5,6) \\ C(4,6,5) & C(1,2,3) \end{bmatrix}$$

and

$$B = \begin{bmatrix} C(7,9,8) & R(10,11,12) \\ R(10,11,12) & C(7,9,8) \end{bmatrix}$$

The table is then

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}.$$

We briefly summarise the character theory. Associated to each conjugacy class $C$ of $G$ there is (a) a conjugacy class of $Q$ of the form $\{(g, 0) : g \in C\}$ where $C$ is a conjugacy class of $G$ and (b) a conjugacy class of the form $\{(gG', 1) : g \in C\}$, where as usual $G'$ denoted the derived group of $G$. From this and using Frobenius' work we can deduce that the character table of $Q$ consists of $2r$ linear characters where $|G/G'| = r$ and for each non-linear irreducible character of degree $m$ of $G$ there is a basic character of $Q$ of degree $\sqrt{2}m$. These exhaust the characters of $Q$.

## 5. Comments and suggestions for further work

1) It appears to be a difficult problem to produce simple loops with interesting properties from methods similar to those above. However, it is certainly true that if $G$ is a simple group with cyclic subgroup $H$ and $W(G, H)$ is modified by rearrangement within the circulant blocks $W(Q)$ is produced for a simple loop $Q$. For example it may be useful to take $G = A_5$ and $H = C_5$ and search for interesting simple loops by modifying the circulant blocks.

2) The following may also be useful. Take the simple Moufang loop $Q$ of order 120 and form $W(Q)$ by listing the cosets either of the Moufang subloop of order 12 or that of order 24.

3) Even the construction of the Moufang loop of order 12 starts with an inverse pattern (i.e. the first row of the $W(Q)$) which is different from that

of any group. It would seem to be a difficult but interesting project to find the kind of inverse patterns which can lead to Moufang or Bol loops.

4) It would seem that there should be a proof that the Moufang loops and Bol loops described in the above work satisfy the corresponding identities using the closure properties in the webs associated to the Ward tables and that such a proof may also be helpful in trying to construct new loops.

5) Non-split extensions for groups can be approached via factor sets. Perhaps one can obtain a combinatorial description of factor sets for groups and loops using the methods here (see also [8]).

6) Call a loop $Q$ *tame* if if $W(Q)$ can be obtained from $W(G)$ for a group $G$ by rearrangements within the circulant blocks without destroying their circulant property. One example is the loop (3) in section 2. Question: can we describe the algebraic properties of tame loops?

7) Group character theory and loop character theory consist of the information remaining in $W(Q)$ when each elements in the table is replaced by a representative of its conjugacy class. For loops it would be interesting to find some intermediate table between $W(Q)$ and this "reduced table" which could play the role of a "super character theory".

Some of the constructions here have appeared in [5], [6] and [7].

The author would like to thank the referee for helpful comments and suggestions.

## References

[1] **O. Chein**: *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. **197**.

[2] **A. Drápal**: *On minimum distances of Latin squares and the quadrangle criterion*, Acta Sci. Math. (Szeged) **70** (2004), no. **1**–**2**, 3 – 11.

[3] **G. Frobenius**: *Über die Primfaktoren der Gruppendeterminante*, Sber. Preuss. Akad. Wiss. Berlin (1896), 1343 – 1382 (1986) (Gesammelte Handlungen V. **3**, 38 – 77).

[4] **E. G. Goodaire, S. May and M. Raman**: *The Moufang loops of order less than* 64, Nova Science Publishers, 1999.

[5] **K. W. Johnson**: *Some recent results on quasigroup determinants*, Demonstratio Math. **24** (1991), 84 – 93.

[6] **K. W. Johnson**: *Latin square determinants II*, Discrete Math. **105** (1992), 111 – 130.

[7] **K. W. Johnson**: *Sharp characters of quasigroups*, European. J. Combinatorics **14** (1993), 103 – 112.

[8] **K. W. Johnson and C. R Leedham-Green**: *Loop cohomology*, Czech. Math. J. **40** (**115**) (1990), 182 – 194.

[9] **K. W. Johnson and P. Vojtěchovský**: *Right division in groups, Dedekind-Frobenius group matrices and Ward quasigroups*, Abh. Math. Sem. Hamburg **75** (2005), 121 – 136.

[10] **K. W. Johnson and B. Sharma**: *On a family of Bol loops*, Boll Un. Math Ital. (Algebra e Geometria Suppl.) V. **2** (1980), 119 – 126.

[11] **K. W. Johnson and J. D. H. Smith**: *Characters of finite quasigroups*, European J. Combin. **5** (1984), no. **1**, 43 – 50.

[12] **M. Kinyon, J. D. Phillips and P. Vojtěchovský**: *Loops of Bol-Moufang type with a subgroup of index* 2, Bul. Acad. Stiinte Rep. Moldova, Matematica **3** (**49**) (2005), 71 – 87.

Abington College
Penn State University
1600 Woodland Road
Abington PA 19001
U.S.A.
e-mail: kwj1@psu.edu

Received November 27, 2005