Discussiones Mathematicae
General Algebra and Applications 27 (2007) 147–167

THE TABLE OF CHARACTERS OF SOME QUASIGROUPS

Grzegorz Bińczak*

Institute of Mathematics, Warsaw University of Technology
Pl. Politechniki 1, 00–661 Warszawa, Poland

e-mail: binczak@mini.pw.edu.pl

and

Joanna Kaleta

Department of Applied Mathematics, Warsaw Agriculture University
Nowoursynowska 166, PL–02–766 Warsaw, Poland

e-mail: kaleta@alpha.sggw.waw.pl

Abstract

It is known that $(\mathbb{Z}_n, -_n)$ are examples of entropic quasigroups which are not groups. In this paper we describe the table of characters for quasigroups $(\mathbb{Z}_n, -_n)$.

Keywords: quasigroups, eigenvectors, eigenspaces, characters of quasigroups.

2000 Mathematics Subject Classification: 20N05.

1. Introduction

The theory of characters of finite quasigroup has been already considered by J.D.H. Smith in [3].

*The author was partially supported by the statutory grant of Warsaw University of Technology No. 504G 1120 0013 000.

A *quasigroup* $(Q,\cdot)$ is a set Q equipped with a binary *multiplication* operation denoted by $\cdot$ or juxtaposition of the two arguments, in which specification of any two of x, y, z in the equation $x\cdot y = z$ determines the third uniquely.

A quasigroup $(Q,\cdot)$ is called *entropic* if

$$(x\cdot y)\cdot(z\cdot t) = (x\cdot z)\cdot(y\cdot t)$$

for all $x, y, z, t \in Q$.

Let $(Q,\cdot)$ be a finite quasigroup. Now we describe how to obtain the character table of Q (see [3], Chapter 5).

Let $R\colon Q \to Q!$; $x \mapsto R(x)$ and $L\colon Q \to Q!$; $x \mapsto L(x)$, where $R(x)(q) = q\cdot x$ and $L(x)(q) = x\cdot q$. Then the subgroup $G = Mlt(Q,\cdot)$ of $Q!$ generated by the union $R(Q)\cup L(Q)$ is called the *multiplication group* of the quasigroup $(Q,\cdot)$.

The group G acts onto $Q\times Q$ in the following way:

$$g\colon Q\times Q \to Q\times Q;\quad (x,y)\mapsto (g(x),g(y)).$$

The orbits $\{C_1,\dots,C_s\}$ of G on $Q\times Q$ under this action are called the *conjugacy classess* of Q.

We consider the incidence matrix a_i of the conjugacy class C_i. This is $0-1$-matrix having 1 as its xy-component if $(x,y)\in C_i$ and 0 otherwise.

The space $\mathbb{C}Q$ can be decomposed as a direct sum of subspaces E_j such that

(a) $\forall_{1\le i\le s}, \exists_{\xi_{ij}\in\mathbb{C}} E_j(a_i - \xi_{ij} I) = \{0\}$;

(b) $\forall_{j\neq k}, \exists_i \xi_{ij} \neq \xi_{ik}$;

(c) $E_1 = \mathbb{C}\Big(\sum\limits_{q\in Q} q\Big)$.

To get (a) and (b), decompose $\mathbb{C}Q$ into a_1-eigenspaces, then decompose each of these into a_2-eigenspaces,and so on. In the case of quasigroup $(\mathbb{Z}_n, -_n)$ it is enough to end this process with a_2-eigenspaces. Let $e_j\colon \mathbb{C}Q \to E_j$ be the projection onto E_j. Define $(s\times s)$-matrix $\Xi = (\xi_{ij})$ by $a_i = \sum_{j=1}^{s} \xi_{ij} e_j$.

Finally the *character table* of the quasigroup Q is the complex $(s \times s)$ matrix Ψ with components

$$\psi_{il} = (f_i)^{\frac{1}{2}} \xi_{li} n_l^{-1},$$

for $i, l = 1, \ldots, s$, where $f_i = dim_{\mathbb{C}} E_i$ and $n_l = \frac{|C_l|}{|Q|}$.

For more details see [1, 3, 5].

In this paper we find the character tables of quasigroups $(\mathbb{Z}_n, -_n)$.

If $i, j \in \mathbb{Z}_n$ then

$$i -_n j = \begin{cases} i - j & \text{for } i \geq j \\ n + i - j & \text{for } i < j \end{cases} .$$

Every quasigroup $(\mathbb{Z}_n, -_n)$ has the following conjugacy classes:

$$C_i = \{(k, t) \in \mathbb{Z}_n^2 \colon |k - t| = i - 1 \text{ or } |k - t| = n - i + 1\}$$

for $i = 1, \ldots, \left[\frac{n}{2}\right]$.

One can check that $|C_j| = n$ if $j = 1$ or $(j = \frac{n}{2} + 1$ and $2|n)$ and $|C_j| = 2n$ otherwise.

This is a „road map" through the lemmas in this paper:

$$\begin{tikzcd}
 & L2 \arrow[d] & L4 \arrow[r] & L6 \arrow[d] & L5 \arrow[l] & L4 \arrow[d] & & L7 \arrow[d] \\
L1 \arrow[r] & L3 \arrow[rr] & & L9 \arrow[rr] & & T1 \arrow[r] & L12 \arrow[r] & T2 \\
 & & L8 \arrow[ur] & & L4 \arrow[r] & L10 \arrow[r] \arrow[ur] & L11 \arrow[u] &
\end{tikzcd}$$

2. Notations

For $n \in \mathbb{N}$, $0 \leq m \leq \left[\frac{n}{2}\right]$ and $m \in \mathbb{N}$ let

$$x_{n,m} = \begin{cases} 2\cos\frac{2m\pi}{n} & \text{if} \quad 2|n \\ \\ (-1)^m 2\cos\frac{m\pi}{n} & \text{otherwise.} \end{cases}$$

For $n \in \mathbb{N}$ define the function $g_n \colon \mathbb{Z} \to \{0, 1, \ldots, \left[\frac{n}{2}\right]\}$ in the following way $g_n(x) = dist(x, n\mathbb{Z})$. Let a_i be the incidence matrix of the conjugacy class C_i. This is $0-1$-matrix having 1 as its xy-component if $(x, y) \in C_i$ and 0 otherwise. Let w_n be the characteristic polynomial of a_2.

3. Main theorem

In this section we prove a recursive formula for the characteristic polynomial of the matrix a_2. Before that we give and prove necessary lemmas.

Lemma 1. *For every $n \geq 3$ we have*

$$w_{n+2}(x) = -xw_{n+1}(x) - w_n(x) + (-1)^n(2x - 4).$$

Proof. Let $v_n = (b_{ij})_{1 \leq i,j \leq n}$ be the matrix such that

$$b_{ij} = \begin{cases} 0 & \text{for} \quad |i-j| \geq 2 \\ 1 & \text{for} \quad |i-j| = 1 \\ -x & \text{for} \quad i = j\,. \end{cases}$$

By Laplace's expansion of the determinant along 1 column we have

$$v_n(x) = -xv_{n-1} - v_{n-2}(x)\,. \tag{1}$$

Using again Laplace's formula to expand the determinant along 1 column and 1 row we have

$$\begin{aligned} w_n(x) &= -xv_{n-1}(x) - (v_{n-2} + (-1)^n) + (-1)^{n+1}(1 + (-1)^n v_{n-2}(x)) \\ &= -xv_{n-1}(x) - 2v_{n-2}(x) + 2 \cdot (-1)^{n+1} \ . \end{aligned} \tag{2}$$

Now we obtain

$$\begin{aligned} w_{n+2}(x) &\overset{(2)}{=} -xv_{n+1} - 2v_n + 2 \cdot (-1)^{n+1} \overset{(1)}{=} -x(-xv_n(x) - v_{n-1}(x)) \\ &-2v_n(x) + 2 \cdot (-1)^{n+1} = v_n(x)(x^2 - 2) + xv_{n-1}(x) + 2 \cdot (-1)^{n+1} \\ &= \underbrace{x^2 v_n(x) + 2xv_{n-1} - 2x(-1)^n}_{=-xw_{n+1}(x)} - 2v_n(x) - xv_{n-1}(x) + 2x(-1)^n \\ &+2(-1)^{n+1} \overset{(2)}{=} -xw_{n+1}(x) + \underbrace{xv_{n-1}(x) + 2v_{n-2}(x) - 2(-1)^{n+1}}_{=-w_n(x)} \\ &\underbrace{-2xv_{n-1}(x) - 2v_n(x) - 2v_{n-2}(x)}_{=0 \ by \ (1)} + 4(-1)^{n+1} + 2x(-1)^n \\ &= -xw_{n+1}(x) - w_n(x) + (-1)^n(2x - 4). \end{aligned}$$

■

Let $u_n(x)$ be a polynomial such that $u_{2n+2}(x) = u_{2n+1}(x) - u_{2n}(x)$, $u_{2n+1}(x) = (x+2)u_{2n}(x) - u_{2n-1}(x)$ and $u_1(x) = u_2(x) = 1$.

Lemma 2. *For every $n \in \mathbb{N}$ we have*

(a) $\quad (x+2)u_{2n}(x)u_{2n+1}(x) = u^2_{2n+1}(x) + (x+2)u^2_{2n}(x) - 1,$

(b) $\quad (x+2)u_{2n+2}(x)u_{2n+1}(x) = u^2_{2n+1}(x) + (x+2)u^2_{2n+2}(x) - 1.$

Proof. For $n = 1$ it is clear. Assume that lemma is true for n. We prove this lemma for $n + 1$.

$u_{2n+3}^2(x) + (x + 2)u_{2n+2}^2(x) - 1 = ((x + 2)u_{2n+2}(x) - u_{2n+1}(x))u_{2n+3}(x)+$

$(x + 2)u_{2n+2}^2(x) - 1 = (x + 2)u_{2n+2}(x)u_{2n+3}(x) - u_{2n+1}(x)((x + 2)u_{2n+2}(x)$

$-u_{2n+1}(x)) + (x + 2)u_{2n+2}^2(x) - 1 \overset{by (b)}{=} (x + 2)u_{2n+2}(x)u_{2n+3}(x)$

$-(u_{2n+1}^2(x) + (x + 2)u_{2n+2}^2(x) - 1) + u_{2n+1}^2(x) + (x + 2)u_{2n+2}^2(x) - 1$

$= (x + 2)u_{2n+2}(x)u_{2n+3}(x),$

hence (a) is true for $n + 1$.

$$
\begin{aligned}
u_{2n+3}^2(x) \quad & +(x + 2)u_{2n+4}^2(x) - 1 = u_{2n+3}^2(x) + (x + 2)u_{2n+4}(x)(u_{2n+3}(x) \\
& -u_{2n+2}(x)) - 1 = u_{2n+3}^2(x) + (x + 2)u_{2n+4}(x)u_{2n+3}(x) \\
& -(x + 2)u_{2n+4}(x)u_{2n+2}(x) - 1 \\
& = u_{2n+3}^2(x) + (x + 2)u_{2n+4}(x)u_{2n+3}(x) \\
& -(x + 2)(u_{2n+3}(x) - u_{2n+2}(x))u_{2n+2}(x) - 1 \\
& = u_{2n+3}^2(x) + (x + 2)u_{2n+2}^2(x) - 1 + (x + 2)u_{2n+4}(x)u_{2n+3}(x) \\
& -(x + 2)u_{2n+3}(x)u_{2n+2}(x) \overset{by\ (a)\ for\ n+1}{=} (x + 2)u_{2n+2}(x)u_{2n+3}(x) \\
& +(x + 2)u_{2n+4}(x)u_{2n+3}(x) - (x + 2)u_{2n+3}(x)u_{2n+2}(x) \\
& = (x + 2)u_{2n+4}(x)u_{2n+3}(x)
\end{aligned}
$$

so we obtain (b) for $n + 1$. ■

Now we pass to the lemma expressing polynomial w_n by u_n.

Lemma 3. *For every* $n \geq 1$

$$(\alpha) \qquad w_{2n+1}(x) = (2-x)u^2_{2n+1}(x),$$

$$(\beta) \qquad w_{2n}(x) = (x^2-4)u^2_{2n}(x).$$

Proof. For $n = 2$ it is obvious. Assume that lemma is true for n. We prove lemma for $n+1$. Using Lemma 1 and Lemma 2 we have

$$\begin{aligned}
w_{2n+2}(x) &\overset{L1}{=} -xw_{2n+1}(x) - w_{2n}(x) + 2x - 4 = -x(2-x)u^2_{2n+1}(x) \\
&- (x^2-4)u^2_{2n}(x) + 2x - 4 \\
&\overset{L2a}{=} (x^2-2x)u^2_{2n+1}(x) - (x^2-4)u^2_{2n}(x) + 2x - 4 \\
&+(2x-4)(u^2_{2n+1}(x) - (x+2)u_{2n}(x)u_{2n+1}(x) - 1 + u^2_{2n}(x)(x+2)) \\
&= (x^2-4)u^2_{2n+1}(x) + (x^2-4)u^2_{2n}(x) - 2(x^2-4)u_{2n}(x)u_{2n+1}(x) \\
&= (x^2-4)(u^2_{2n+1}(x)u^2_{2n}(x) - 2u_{2n}(x)u_{2n+1}(x)) \\
&= (x^2-4)(u_{2n+1}(x) - u_{2n}(x))^2 = (x^2-4)u^2_{2n+2}(x)
\end{aligned}$$

so we obtain (β) for $n+1$.

By Lemma 1 and 2 and (β) for $n+1$ we have

$$\begin{aligned}
(2-x)u^2_{2n+3}(x) \quad &= (2-x)((x+2)u_{2n+2}(x) - u_{2n+1}(x))^2 \\
&\overset{L2b}{=} (2-x)((x+2)u_{2n+2}(x) - u_{2n+1}(x))^2 \\
&+ (2x-4)((x+2)u^2_{2n+2}(x) + u^2_{2n+1}(x) \\
&- 1 - (x+2)u_{2n+2}(x)u_{2n+1}(x)) =
\end{aligned}$$

$$= (x-2)(-(x+2)^2u_{2n+2}^2(x)$$

$$+ 2(x+2)u_{2n+1}(x)u_{2n+2}(x) - u_{2n+1}^2(x)$$

$$+ 2(x+2)u_{2n+2}^2(x) + 2u_{2n+1}^2(x) - 2$$

$$- 2(x+2)u_{2n+2}(x)u_{2n+1}(x)$$

$$= (x-2)(u_{2n+2}^2(x)(-x^2-2x) + u_{2n+1}^2 - 2)$$

$$= -x(x^2-4)u_{2n+2}^2(x) - (2-x)u_{2n+1}^2(x) - 2x + 4$$

$$\overset{(\beta)}{=} -xw_{2n+2}(x) - w_{2n+1}(x) - 2x + 4 \overset{L1}{=} w_{2n+3}(x)$$

hence (α) is true for $n+1$. ■

Lemma 4. *Let $n \in N$ and $0 \leq j,k \leq \left[\frac{n}{2}\right]$. Then*

$$x_{n,j} \cdot x_{n,k} = x_{n,|k-j|} + x_{n,g_n(k+j)}.$$

Proof. Consider the following cases:

1. n is odd and $j+k \leq \left[\frac{n}{2}\right]$. Then

$$x_{n,j} \cdot x_{n,k} = 2\cos\left(\frac{2j\pi}{n}\right) 2\cos\left(\frac{2k\pi}{n}\right)$$

$$= 2\left(\cos\left(\frac{2(j-k)\pi}{n}\right) + \cos\left(\frac{2(j+k)\pi}{n}\right)\right)$$

$$= x_{n,|k-j|} + x_{n,g_n(k+j)}.$$

2. n is odd and $j+k > \left[\frac{n}{2}\right]$. Then $g_n(j+k) = n-(j+k)$ and

$$x_{n,j}\cdot x_{n,k} = 2\cos\left(\frac{2j\pi}{n}\right)2\cos\left(\frac{2k\pi}{n}\right)$$

$$= 2\left(\cos\left(\frac{2(j-k)\pi}{n}\right)+\cos\left(\frac{2(j+k)\pi}{n}\right)\right)$$

$$= 2\left(\cos\left(\frac{2(j-k)\pi}{n}\right)+\cos\left(2\pi-\frac{2(j+k)\pi}{n}\right)\right)$$

$$= 2\cos\left(\frac{2(j-k)\pi}{n}\right)+\cos\left(\frac{2(n-(j+k))\pi}{n}\right) = x_{n,|k-j|}+x_{n,g_n(k+j)}.$$

3. n is even and $j+k \leq \left[\frac{n}{2}\right]$. Then

$$x_{n,j}\cdot x_{n,k} = (-1)^j 2\cos\left(\frac{j\pi}{n}\right)(-1)^k 2\cos\left(\frac{k\pi}{n}\right)$$

$$= (-1)^{j+k}2\left(\cos\left(\frac{(j-k)\pi}{n}\right)+\cos\left(\frac{(j+k)\pi}{n}\right) = x_{n,|k-j|}+x_{n,g_n(j+k)}\ .\right.$$

4. n is even and $j+k > \left[\frac{n}{2}\right]$. Then

$$x_{n,j}\cdot x_{n,k} = (-1)^j 2\cos\left(\frac{j\pi}{n}\right)(-1)^k 2\cos\left(\frac{k\pi}{n}\right)$$

$$= (-1)^{j+k}2\left(\cos\left(\tfrac{(j-k)\pi}{n}\right)+\cos\left(\tfrac{(j+k)\pi}{n}\right)\right)$$

$$= (-1)^{k-j}2\cos\left(\tfrac{(j-k)\pi}{n}\right)+(-1)^{j+k}2(-1)\cos\left(\pi-\tfrac{(j+k)\pi}{n}\right)$$

$$= (-1)^{k-j}2\cos\left(\frac{(j-k)\pi}{n}\right)+(-1)^{n-(j+k)}2\cos\left(\pi-\frac{(j+k)\pi}{n}\right)$$

$$= x_{n,|k-j|}+x_{n,g_n(j+k)}.$$

■

Lemma 5. *Let $n \in \mathbb{N}$, $y \in \mathbb{Z}$ and $j \in \{0, 1, \ldots, \left[\frac{n}{2}\right]\}$. Then*

$$\{g_n(j + g_n(y)), |g_n(y) - j|\} = \{g_n(y - j), g_n(y + j)\}.$$

Proof. There exists $k \in \mathbb{Z}$ such that $kn \leq y \leq kn + n$. Let us consider the following cases:

1. If $y - kn \leq \left[\frac{n}{2}\right]$ then $g_n(y) = y - kn$ and

$$g_n(y + j) = dist(y + j, n\mathbb{Z}) = dist(y - kn + j, n\mathbb{Z})$$

$$= dist(g_n(y) + j, n\mathbb{Z}) = g_n(g_n(y) + j)$$

and

$$g_n(y - j) = dist(y - j, n\mathbb{Z}) = dist(y - kn - j, n\mathbb{Z})$$

$$= dist(g_n(y) - j, n\mathbb{Z}) = |g_n(y) - j|.$$

2. If $kn + n - y \leq \left[\frac{n}{2}\right]$ then $g_n(y) = kn + n - x$ and

$$g_n(y - j) = dist(y - j, n\mathbb{Z}) = dist(j - y, n\mathbb{Z})$$

$$= dist(kn + n - y + j, n\mathbb{Z}) = dist(g_n(y) + j, n\mathbb{Z}) = g_n(g_n(y) + j)$$

and

$$g_n(y + j) = dist(y + j, n\mathbb{Z}) = dist(-y - j, n\mathbb{Z}) =$$

$$dist(kn + n - y - j, n\mathbb{Z}) = dist(g_n(y) - j, n\mathbb{Z}) = |g_n(y) - j|.$$

∎

Now we find eigenvectors for the matrix a_2.

Let $n \in \mathbb{N}$ and $0 \leq j \leq \left[\frac{n}{2}\right]$. Let

$$v_{n,j} = [x_{n,g_n(0)}, x_{n,g_n(j)}, x_{n,g_n(2j)}, \ldots, x_{n,g_n(kj)}, \ldots, x_{n,g_n((n-1)j))}] \in \mathbb{C}^n.$$

Lemma 6. *Let* $0 \le j \le \left[\frac{n}{2}\right]$. *Then vector* $v_{n,j}$ *is an eigenvector of the matrix* a_2 *corresponding to an eigenvalue* $x_{n,j}$.

Proof. We must show that

$$(*) \qquad x_{n,j} \cdot x_{n,g_n(kj)} = x_{n,g_n((k-1)j)} + x_{n,g_n((k+1)j)}$$

for $k = 1, 2, \ldots, n-1$ and

$$(**) \qquad x_{n,j} \cdot x_{n,g_n(0)} = x_{n,g_n(j)} + x_{n,g_n((n-1)j)}$$

and

$$(***) \qquad x_{n,j} \cdot x_{n,g_n((n-1)j)} = x_{n,g_n(0)} + x_{n,g_n((n-2)j)}.$$

By Lemma 4 we have

$$x_{n,j} \cdot x_{n,g_n(kj)} = x_{n,|j-g_n(kj)|} + x_{n,g_n(j+g_n(kj))}.$$

Hence

$$x_{n,j} \cdot x_{n,g_n(kj)} = x_{n,g_n((k-1)j)} + x_{n,g_n((k+1)j)},$$

by Lemma 5 for $y = kj$ and this ends the proof of $(*)$.

Obviously $g_n(0) = 0$ and $g_n(j) = j$. Moreover

$$g_n((n-1)j) = dist(nj - j, n\mathbb{Z}) = dist(-j, n\mathbb{Z}) = dist(j, n\mathbb{Z}) = g_n(j).$$

Therefore

$$x_{n,j} \cdot x_{n,g_n(0)} = x_{n,j} \cdot x_{n,0} = x_{n,j} + x_{n,g_n(j)} = x_{n,g_n(j)} + x_{n,g_n((n-1)j)}$$

and $(**)$ was proved.

We have

$$x_{n,j} \cdot x_{n,g_n((n-1)j)} = x_{n,j} \cdot x_{n,g_n(j)} = x_{n,j} \cdot x_{n,j} = x_{n,0} + x_{n,g_n(2j)}$$

$$= x_{n,g_n(0)} + x_{n,g(-2j)} = x_{n,g_n(0)} + x_{n,g_n((n-2)j)}$$

and $(***)$ was shown. ■

Notice that if the vector $[y_1, y_2, \ldots, y_n]$ is an eigenvector for the matrix a_2 then the vector $[y_n, y_1, y_2, \ldots, y_{n-1}]$ is also an eigenvector for the matrix a_2.

Let $n \in \mathbb{N}$ and $0 \le j \le \left[\frac{n}{2}\right]$. Let

$u_{n,j} =$

$[x_{n,g_n((n-1)j))}, x_{n,g_n(0)}, x_{n,g_n(j)}, x_{n,g_n(2j)}, \ldots, x_{n,g_n(kj)}, \ldots, x_{n,g_n((n-2)j))}] \in \mathbb{C}^n.$

Let $E_{n,j+1} = lin(v_{n,j}, u_{n,j})$ and $e_{n,j+1}$ be a matrix of the projection $\mathbb{C}^n$ onto $E_{n,j+1}$.

Lemma 7.

$$dimE_{n,j} = \begin{cases} 1 & for\ j = 1\ or\ (j = \frac{n}{2} + 1\ and\ 2|n) \\ 2 & otherwise. \end{cases}$$

Proof. If $j = 1$ then $E_{n,1} = lin(v_{n,0}, u_{n,0}) = lin([x_{n,0}, \ldots, x_{n,0}], [x_{n,0}, \ldots, x_{n,0}])$, so $dimE_{n,1} = 1$.

If $2|n$ and $j = \frac{n}{2} + 1$ then $v_{n,j-1} = [2, -2, 2, \ldots, (-1)^{n+1}2]$ (since $x_{n,\frac{n}{2}} = -2$, $x_{n,0} = 2$ and $g_n(\frac{nk}{2}) = 0$ for k odd and $g_n(\frac{nk}{2}) = \frac{n}{2}$ for k even) and $u_{n,j-1} = (-1)^{n+1} v_{n,j-1}$ hence $dimE_{n,j} = 1$.

Otherwise

$$\det \begin{bmatrix} x_{n,g_n(0)} & x_{n,g_n(j-1)} \\ x_{n,g_n((n-1)(j-1))} & x_{n,g_n(0)} \end{bmatrix} = x_{n,0}^2 - x_{n,j-1}^2 = 4 - x_{n,j-1}^2 \neq 0$$

hence $v_{n,j-1}$ and $u_{n,j-1}$ are linear independent vectors. ∎

Observe that $dimE_{n,1} + \ldots + dimE_{n,[\frac{n}{2}]+1} = n$ and $\mathbb{C}^n = E_{n,1} \oplus \ldots \oplus E_{n,[\frac{n}{2}]+1}$.

Lemma 8. *If* $n = 2r + 1$ *and* $r > 3$ *then*

$$u_n(x) = x^r + x^{r-1} + (1 - r)x^{r-2} + \ldots$$

If $n = 2r$ *and* $r > 2$ *then*

$$u_n(x) = x^{r-1} + 0 \cdot x^{r-2} + (2 - r)x^{r-3} + \ldots$$

Proof. $u_5(x) = x^2 + x - 1$ and $u_6(x) = x^2 - 1$. Therefore lemma is true for $n = 5$ and $n = 6$.

If lemma is true for $n = 2r$ and $n = 2r - 1$ then

$u_{2r+1}(x) = (x + 2)u_{2r} - u_{2r-1}(x)$

$= (x + 2)(x^{r-1}+(2 - r)x^{r-3}+\dots) - (x^{r-1}+x^{r-2}+(1-(r - 1))x^{r-3}+\dots)$

$= x^r + (2 - 1)x^{r-1} + ((2 - r) - 1)x^{r-2} + \dots$

and

$u_{2r+2}(x) = u_{2r+1}(x) - u_{2r}(x)$

$= x^r + x^{r-1} + (1 - r)x^{r-2} + \dots - (x^{r-1} + (2 - r)x^{r-3} + \dots)$

$= x^r+(1-1)x^{r-1}+(1 - r - 0)x^{r-2} + \dots = x^r + 0 \cdot x^{r-1}+(1 - r)x^{r-2}+ \dots$

Hence lemma is true for $n = 2r + 1$ and $n = 2r + 2$. ∎

Lemma 9.

$$x^2_{n,0} + \dots + x^2_{n,[\frac{n}{2}]} = \begin{cases} n + 2 \ for\ n\ even \\ n + 4 \ for\ n\ odd \end{cases}.$$

Proof. Consider the following cases:

1. If n is even and $n = 2k + 1$. By Lemma 6 we know that $x_{n,1}, \dots, x_{n,k}$ are eigenvalues of the matrix a_2. Hence they are roots of w_n. Obviously $x_{n_i} \neq 2$ for $i = 1, \dots, k$, so by Lemma 3 they are roots of u_n. Therefore we have

$$(*) \qquad u_n(x) = (x - x_{n,1})(x - x_{n,2}) \dots (x - x_{n,k}).$$

Using Lemma 8 we obtain $x_{n,1} + \dots + x_{n,k} = -1$ and $\sum_{1\le i<j\le k} x_{n,i}x_{n,j} = 1 - k$.

Hence

$$x^2_{n,1} + \dots + x^2_{n,k} = (x_{n,1} + \dots + x_{n,k})^2 - 2 \sum_{1\le i<j\le k} x_{n,i}x_{n,j}$$
$$= 1 - 2(1 - k) = 2k - 1 = n - 2$$

and $x^2_{n,0} + x^2_{n,1} + \dots + x^2_{n,k} = 4 + n - 2 = n + 2$.

2. Assume that n is odd and $n = 2k$. Then

$$(**) \qquad u_n(x) = (x - x_{n,1})(x - x_{n,2}) \dots (x - x_{n,k-1})$$

because $x_{n,1}, \dots, x_{n,k-1}$ are eigenvalues of the matrix a_2 by Lemma 6, hence they are roots of w_n and by Lemma 3 they are also roots of u_n. So by Lemma 8 we have $(**)$.

By Lemma 8 it turns out that $x_{n,1}+\dots+x_{n,k-1} = 0$ and $\sum_{1\le i<j\le k-1} x_{n,i}x_{n,j} = 2-k$.

Hence

$$x_{n,1}^2 + \dots + x_{n,k-1}^2 = (x_{n,1} + \dots + x_{n,k-1})^2 - 2 \sum_{1\le i<j\le k-1} x_{n,i}x_{n,j}$$

$$= 0 - 2(2-k) = 2k - 4 = n - 4$$

and $x_{n,0}^2 + x_{n,1}^2 + \dots + x_{n,k-1}^2 + x_{n,k} = 4 + (n-4) + 4 = n + 4$.

■

Lemma 10. *Let $n, k \in \mathbb{N}$ and $gcd(n,k) = 1$. Let $A = \{0, 1, \dots, \left[\frac{n}{2}\right]\}$ and $f\colon A \to A$ be a function such that $f(x) = g_n(kx)$. Then f is a bijection.*

Proof. It is sufficient to show that f is $1-1$. Suppose $i, j \in A$, $i < j$ and $f(i) = f(j)$. Let $x = dist(ik, n\mathbb{Z}) = dist(jk, n\mathbb{Z})$. There exist $p, q \in \mathbb{Z}$ such that $|ik - pn| = |jk - qn|$.

If $ik - pn = jk - qn$ then $(i-j)k = (p-q)n$ hence $n|j-i$ (since $gcd(n,k) = 1$) but $j - i \in A$ and we have a contradiction.

If $ik - pn = -jk + qn$ then $(i+j)k = (p+q)n$ hence $n|i+j$ but $i, j \in A$ so $0 < i + j \le \left[\frac{n}{2}\right] + \left[\frac{n}{2}\right] - 1 < n$ and we obtain a contradiction. ■

Lemma 11. *Let $n, k, p \in \mathbb{N}$ and $0 \le k \le \left[\frac{n}{2}\right]$. Then $|v_{pn,pk}|^2 = p|v_{n.k}|^2$.*

Proof. Let us note that $g_{pn}(px) = dist(px, pn\mathbb{Z}) = p \cdot dist(x, n\mathbb{Z}) = pg_n(x)$ for any $x \in \mathbb{Z}$, $v_{np,kp} = [(x_{pn,g_{pn}((i-1)pk))})_{i=1,\dots,pn}] = [(x_{pn,pg_n((i-1)k)})_{i=1,\dots,pn}]$ and $g_n((n+i-1)k) = g_n((i-1)k)$.

Consider the following cases:

1. If $2|n$ then $x_{pn,pj} = 2\cos(\frac{2pj\pi}{pn}) = 2\cos(\frac{2j\pi}{n}) = x_{n,j}$. Hence $v_{np,nk} = [(x_{n,g_n((i-1)k)})_{i=1,\dots,pn}]$ and $v_{pn,pk} = [\underbrace{v_{n,k}, v_{n,k}, \dots, v_{n,k}}_{p-times}]$ and $|v_{n,k}|^2 = p|v_{n,k}|^2$.
2. If $2 \not| n$ and $2 \not| p$ then $x_{pn,pj} = (-1)^{pj} 2\cos(\frac{pj\pi}{pn}) = (-1)^j 2\cos(\frac{j\pi}{n}) = x_{n,j}$, $v_{pn,pk} = [\underbrace{v_{n,k}, v_{n,k}, \dots, v_{n,k}}_{p-times}]$ and $|v_{n,k}|^2 = p|v_{n,k}|^2$.
3. If $2 \not| n$ and $2|p$ then $x_{pn,pj} = 2\cos(\frac{2pj\pi}{pn}) = 2\cos(\frac{2j\pi}{n}) = 2(2\cos^2(\frac{j\pi}{n}) - 1) = 4\cos^2(\frac{j\pi}{n}) - 2 = x_{n,j}^2 - 2$ and by Lemma 4 we have $x_{pn,pj} = x_{n,0} + x_{n,g_n(2j)} - 2 = x_{n,g_n(2j)}$. By Lemma 10 $v_{pn,pk} = [\underbrace{\widetilde{v_{n,k}}, \widetilde{v_{n,k}}, \dots, \widetilde{v_{n,k}}}_{p-times}]$ (since $gcd(2,n) = 1$), where coordinates of $\widetilde{v_{n,k}}$ arise as a result of the permutation of coordinates of $v_{n,k}$. Hence $|v_{pn,pk}|^2 = p|v_{n.k}|^2$.

■

Theorem 1. *Let $n \in \mathbb{N}$ and $0 \le j \le \left[\frac{n}{2}\right]$. Then*

$$|v_{n,j}|^2 = \begin{cases} 4n & for\ j = 0\ or\ (j = \frac{n}{2}\ and\ 2|n) \\ 2n & otherwise. \end{cases}$$

Proof. Assume that $gcd(n,j) = 1$.

Let $n = 2r+1$. According to the fact that $g_n((i-1)k) = g_n((n-i+1)k)$ and by Lemma 10 we have

$$|v_{n,j}|^2 = |[x_{n,0}, x_{n,1}, \dots, x_{n,r}, x_{n,r}, \dots, x_{n,1}]|^2 = 2(x_{n,0}^2 + \dots + x_{n,r}^2) - x_{n,0}^2$$
$$= 2(n+2) - 4 = 2n$$

using Lemma 9.

Let $n = 2r$. Then

$$|v_{n,j}|^2 = |[x_{n,0}, x_{n,1}, \dots, x_{n,r-1}, x_{n,r}, x_{n,r-1}, \dots, x_{n,1}]|^2,$$

by Lemma 10. Hence

$$|v_{n,j}|^2 = 2(x_{n,0}^2 + \dots + x_{n,r}^2) - x_{n,0}^2 - x_{n,r}^2 = 2(n+4) - 4 - 4 = 2n,$$

by Lemma 9.

Assume that $gcd(n,j) \neq 1$. Let $p = gcd(n,j)$, $n = pn'$, $j = pj'$, where $gcd(n',j') = 1$. By Lemma 11 we have $|v_{n,j}|^2 = p|v_{n',j'}|^2$.

One needs to consider the following cases:

1. If $j = 0$ then $v_{n,j} = [\underbrace{2, 2, \ldots 2}_{n-times}]$ and $|v_{n,j}|^2 = 4n$.
2. If $2 \not| n$ and $j \neq 0$ then $2 \not| n'$ and $|v_{n,j}|^2 = p|v_{n',j'}|^2 = p2n' = 2n$.
3. If $2|n$, $2 \not| n'$ and $j \neq 0$ then $2|p$ and $j \neq \frac{n}{2}$ (because if $j = \frac{n}{2}$ then $\frac{p}{2}n' = j = pj' = \frac{p}{2}2j'$ and $n' = 2j'$ but $2 \not| n'$). Hence $|v_{n,j}|^2 = p|v_{n',j'}|^2 = p2n' = 2n$.
4. If $2|n$, $2|n'$ and $j' = \frac{n'}{2}$ then $j = pj' = p\frac{n'}{2} = \frac{n}{2}$ and $|v_{n,j}|^2 = p|v_{n',j'}|^2 = p4n' = 4n$.
5. If $2|n$, $2|n'$, $j \neq 0$ and $j' \neq \frac{n'}{2}$ then $j' \neq 0$, $j \neq \frac{n}{2}$ and $|v_{n,j}|^2 = p|v_{n',j'}|^2 = p2n' = 2n$. ■

Let $b = (b_{ij})_{1 \leq i,j \leq n} \in M_n(\mathbb{C})$ be a matrix. Then let $\bar{b} = [b_{11}, \ldots, b_{1n}]$. Obviously $^-$ is a linear operation.

For $1 \leq i \leq \left[\frac{n}{2}\right]$ let e_i be a matrix of the projection of $\mathbb{C}^n$ onto $E_{n,i}$. We know (see [3]) that $lin(a_1, \ldots, a_{\left[\frac{n}{2}\right]+1}) = lin(e_1, \ldots, e_{\left[\frac{n}{2}\right]+1})$.

Let $n \in \mathbb{N}$, $1 \leq i \leq \left[\frac{n}{2}\right]$ and $a_i = \sum_{j=1}^{\left[\frac{n}{2}\right]+1} \xi_{ij} e_j$.

Lemma 12. *Let $n \in \mathbb{N}$ and $1 \leq i,j \leq \left[\frac{n}{2}\right] + 1$. Then*

$$\xi_{i,j} = \begin{cases} 1 \; for \; i = 1 \; or \; \left(i = \dfrac{n}{2} + 1, (2|n) \; and \; j = 1\right) \\ 2 \; for \; j = 1 \; and \; i \neq 1 \; and \; \left(if \; 2|n \; then \; i \neq \dfrac{n}{2} + 1\right) \\ \dfrac{1}{2} x_{n, g_n((i-1)(j-1))} \; for \; 2|n \; and \; i = \dfrac{n}{2} + 1 \; and \; j \neq 1 \\ x_{n, g_n((i-1)(j-1))} \; otherwise. \end{cases}$$

Proof. It is obvious that

$$\bar{a}_i = \sum_{j=1}^{[\frac{n}{2}]+1} \xi_{ij}\bar{e}_j \quad \text{and} \quad \bar{e}_j = \frac{[1,0,\dots,0]\circ v_{n,j-1}}{|v_{n,j-1}|^2} v_{n,j-1} = \frac{2v_{n,j-1}}{|v_{n,j-1}|^2},$$

where $\circ$ means the scalar product of vectors. Using Theorem 1 we have

$$\bar{e}_j = \begin{cases} \dfrac{1}{2n} v_{n,j-1} & \text{for } j = 1 \text{ or } \left(j = \dfrac{n}{2} + 1 \text{ and } 2|n\right) \\ \dfrac{1}{n} v_{n,j-1} & \text{otherwise.} \end{cases}$$

Hence $\bar{e}_1, \dots, \bar{e}_{[\frac{n}{2}]+1}$ are pairwise orthogonal. Therefore $\xi_{i,j} = \dfrac{\bar{a}_i \circ \bar{e}_j}{|\bar{e}_j|^2}$.

Consider the following cases:

1. If $i = 1$ and $j = 1$ or $(j = \frac{n}{2} + 1$ and $2|n)$ then

$$\xi_{1,j} = \frac{\bar{a}_1 \circ \bar{e}_j}{|\bar{e}_j|^2} = \frac{\frac{1}{2n}2}{\frac{1}{4n^2}|v_{n,j-1}|} = \frac{\frac{1}{n}}{\frac{1}{4n^2}4n} = 1.$$

2. If $i = 1$ and $j \neq 1$ and $(j \neq \frac{n}{2} + 1$ if $2|n)$ then

$$\xi_{1,j} = \frac{\bar{a}_1 \circ \bar{e}_j}{|\bar{e}_j|^2} = \frac{\frac{1}{n}2}{\frac{1}{n^2}|v_{n,j-1}|} = \frac{\frac{2}{n}}{\frac{1}{n^2}2n} = 1.$$

3. If $i = \frac{n}{2} + 1$, $2|n$ and $j = 1$ then

$$\xi_{i,1} = \frac{\bar{a}_i \circ \bar{e}_1}{|\bar{e}_1|^2} = \frac{\frac{1}{n}}{\frac{1}{4n^2}4n} = 1.$$

4. If $j = 1$ and $i \neq 1$ and $(i \neq \frac{n}{2} + 1$ if $2|n)$ then

$$\xi_{i,1} = \frac{\bar{a}_i \circ \bar{e}_1}{|\bar{e}_1|^2} = \frac{\frac{2}{n}}{\frac{1}{4n^2}4n} = 2.$$

5. If $2|n$ and $i = \frac{n}{2}+1$, $j \neq 1$ and $j \neq \frac{n}{2}+1$ then

$$\xi_{i,j} = \frac{\bar{a}_i \circ \bar{e}_j}{|\bar{e}_j|^2} = \frac{\frac{1}{n}x_{n,g_n(\frac{n}{2}(j-1))}}{\frac{1}{n^2}|v_{n,j-1}|^2} = \frac{1}{2}x_{n,g_n(\frac{n}{2}(j-1))}.$$

6. If $2|n$ and $i = \frac{n}{2}+1$ and $j = \frac{n}{2}+1$ then

$$\xi_{i,j} = \frac{\bar{a}_i \circ \bar{e}_j}{|\bar{e}_j|^2} = \frac{\frac{1}{2n}x_{n,g_n(\frac{n}{2}\frac{n}{2})}}{\frac{1}{4n^2}|v_{n,j-1}|^2} = \frac{1}{2}x_{n,g_n(\frac{n}{2}\frac{n}{2})}.$$

7. If $2|n$ and $j = \frac{n}{2}+1$, $i \neq 1$ and $i \neq \frac{n}{2}+1$ then $\bar{a}_i = [b_1, \ldots, b_n]$, where

$$b_j = \begin{cases} 1 & \text{for } j = i \text{ or } j = n-i+2 \\ 0 & \text{for } j \neq i \text{ and } j \neq n-i+2. \end{cases}$$

Moreover $v_{n,\frac{n}{2}} = [2, -2, \ldots 2(-1)^{n+1}]$. Hence

$$\xi_{i,j} = \frac{\frac{1}{2n}(2(-1)^{i+1} + 2(-1)^{n-i+1})}{\frac{1}{4n^2}4n} = 2(-1)^{i+1} = x_{n,g_n((i-1)\frac{n}{2})}.$$

8. If $i \neq 1$, $j \neq 1$, ($i \neq \frac{n}{2}+1$ and $j \neq \frac{n}{2}+1$ if $2|n$) then

$$\begin{aligned}\xi_{i,j} &= \frac{\frac{1}{n}\big(x_{n,g_n((i-1)(j-1))} + x_{n,g_n((n-i+1)(j-1))}\big)}{\frac{1}{n^2}2n} \\ &= \frac{\frac{2}{n}x_{n,g_n((i-1)(j-1))}}{\frac{1}{n^2}2n} = x_{n,g_n((i-1)(j-1))}.\end{aligned}$$

■

Let $f_i = dim_{\mathbb{C}}E_{n,i}$, $n_j = \frac{|C_j|}{n}$ and $\varphi_{i,j} = \sqrt{f_i}\xi_{j,i}n_j^{-1}$ for $i, j \in \{1, \ldots, \left[\frac{n}{2}\right]\}$. Then $(\varphi_{i,j})_{1\leq i,j\leq\left[\frac{n}{2}\right]}$ is the character table of the quasigroup $(\mathbb{Z}_n, -_n)$.

The next Theorem gives the description of the character table of the quasigroup $(\mathbb{Z}_n, -_n)$.

Theorem 2. *Let $n \in \mathbb{N}$ and $1 \le i, j \le \left[\frac{n}{2}\right] + 1$. Then*

$$\varphi_{i,j} = \begin{cases} 1 \; for \; i = 1 \; or \; (i = \frac{n}{2} + 1, (2|n) \; and \; j = 1) \\ \sqrt{2} \; for \; j = 1 \; and \; i \neq 1 \; and \; \left(if \;\; 2|n \; then \; i \neq \dfrac{n}{2} + 1\right) \\ (-1)^{j-1} \; for \; 2|n \; and \; i = \dfrac{n}{2} + 1 \; and \; j \neq 1 \\ \dfrac{\sqrt{2}}{2} x_{n, g_n((i-1)(j-1))} \; otherwise. \end{cases}$$

Hence for n even we obtain

	$j = 1$	$j \neq 1$
$i = 1$	$\varphi_{i,j} = 1$	$\varphi_{i,j} = 1$
$i \neq 1$	$\varphi_{i,j} = \sqrt{2}$	$\varphi_{i,j} = \frac{\sqrt{2}}{2} x_{n,g_n((i-1)(j-1))}$

and for n odd we have

	$j = 1$	$j \neq 1, j \neq \frac{n}{2} + 1$	$j = \frac{n}{2} + 1$
$i = 1$	$\varphi_{i,j} = 1$	$\varphi_{i,j} = 1$	$\varphi_{i,j} = 1$
$i \neq 1, i \neq \frac{n}{2} + 1$	$\varphi_{i,j} = \sqrt{2}$	$\varphi_{i,j} = \frac{\sqrt{2}}{2} x_{n,g_n((i-1)(j-1))}$	$\varphi_{i,j} = \frac{\sqrt{2}}{2} x_{n,g_n((i-1)(j-1))}$
$i = \frac{n}{2} + 1$	$\varphi_{i,j} = 1$	$\varphi_{i,j} = (-1)^{j-1}$	$\varphi_{i,j} = (-1)^{\frac{n}{2}}$

Proof. We must consider the following cases (we use Lemma 7 to calculate f_i):

1. If $i = 1$ and ($j = 1$ or ($j = \frac{n}{2} + 1$ and $2|n$)) then

$$\varphi_{i,j} = \sqrt{1} \xi_{j,i} \frac{n}{n} = 1.$$

2. If $i=1$, $j\neq 1$ and (if $2|n$ then $j\neq \frac{n}{2}+1$) then

$$\varphi_{i,j}=\sqrt{1}\xi_{j,i}\frac{n}{2n}=1.$$

3. If $2|n$, $i=\frac{n}{2}+1$ and $j=1$ then

$$\varphi_{i,j}=\sqrt{1}\xi_{j,i}\frac{n}{n}=1.$$

4. If $2|n$, $i=\frac{n}{2}+1$ and $j=\frac{n}{2}+1$ then

$$\varphi_{i,j}=\sqrt{1}\xi_{j,i}\frac{n}{n}=\frac{1}{2}x_{n,g_n(\frac{n}{2}\frac{n}{2})}=(-1)^{\frac{n}{2}}=(-1)^{j-1}.$$

5. If $2|n$, $i=\frac{n}{2}+1$ and $j\neq 1$ and $j\neq \frac{n}{2}+1$ then

$$\varphi_{i,j}=\sqrt{1}\xi_{j,i}\frac{n}{2n}=\frac{1}{2}x_{n,g_n((j-1)\frac{n}{2})}=(-1)^{j-1}.$$

6. If $i\neq 1$ and $j=1$ and (if $2|n$ then $i\neq \frac{n}{2}+1$)then

$$\varphi_{i,j}=\sqrt{2}\xi_{j,i}\frac{n}{n}=\sqrt{2}.$$

7. If $i\neq 1$ and $i\neq \frac{n}{2}+1$ and $2|n$ and $j=\frac{n}{2}+1$ then

$$\varphi_{i,j}=\sqrt{2}\xi_{j,i}\frac{n}{n}=\sqrt{2}\frac{1}{2}x_{n,g_n(\frac{n}{2}(i-1))}=\sqrt{2}(-1)^{\frac{n}{2}}=\sqrt{2}\frac{1}{2}x_{n,g_n((i-1)(j-1))}.$$

8. If $i\neq 1$ and (if $2|n$ then $i\neq \frac{n}{2}+1$) and $j\neq 1$ and (if $2|n$ then $j\neq \frac{n}{2}+1$) then

$$\varphi_{i,j}=\sqrt{2}\xi_{j,i}\frac{n}{2n}=\frac{\sqrt{2}}{2}x_{n,g_n((i-1)(j-1))}.$$

$\blacksquare$

Acknowledgement

We are grateful to Prof. J.D.H. Smith for help in finding the bibliography.

We are indebted to the referee for several suggestions that have improved the exposition of these results.

REFERENCES

[1] O. Chein, H.O. Pflugfelder and J.D.H. Smith, *Quasigroups and loops: theory and applications*, Berlin 1990.

[2] K.W. Johnson and J.D.H. Smith, *Characters of finite quasigroups*, Eur. J. Comb. **5** (1984), 43–50.

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

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

[5] J.D.H. Smith, *Representation Theory of quasigroups*, Sci. Math. Japonicae **60** (2004), 171–204.

Received 29 April 2006
Revised 18 July 2006