

On central digraphs constructed from left loops and loops

Raja Rawat

Abstract. Let \mathcal{A}_n be the set of $n \times n$ zero-one matrices satisfying the matrix equation $A^2 = J_n$, where J_n is $n \times n$ matrices of all ones. In this article, it is proved that the number of non-isomorphic left loops of order k gives the lower bound to the size of \mathcal{A}_n for $n = k^2$. Mainly we have established that any matrix in \mathcal{A}_n corresponding to loop has rank $2k - 2$, where $n = k^2$, for some positive integer k .

1. Introduction

A central groupoid is an algebraic system with one binary operation, satisfying the identity

$$(x.y).(y.z) = y \tag{1}$$

for all x, y and z . In a directed graph D , if there is a unique path of length two between any two vertices, then it has Property C . That is for vertices $x, y \in D$, there exists unique vertex $z \in D$, such that,

$$x \rightarrow z \rightarrow y \tag{2}$$

Such a graph is also called central digraph. Equivalently, the corresponding adjacency matrix $A(T)$ satisfies the matrix equation $A^2 = J$. In [4], the author shows the size of the vertex set $V(D)$ of D is $n = k^2$, (k is some positive integer), where each vertex has both indegree and outdegree k . Then such a digraph is called k -central. Throughout the article, we will denote \mathcal{A}_n as the set of $n \times n$ zero-one matrices satisfying $A^2 = J_n$ for all $A \in \mathcal{A}_n$, where J_n is the $n \times n$ matrices of all ones and $n = k^2$ for some positive integer k . Due to very rich and peculiar algebraic and combinatorial structures,

2010 Mathematics Subject Classification: 20D60, 20N05, 05C20, 05C50.

Keywords: Left quasigroups, loops, central digraph, central groupoid.

central groupoid and central digraph have attracted the attention of many researchers, see [3, 4, 5, 6].

A groupoid (S, \circ) is called a left quasigroup if the equation $a \circ X = b$ has a unique solution in S for all $a, b \in S$. A left quasigroup with identity is called a left loop. A left loop (S, \circ) is called a loop if the equation $X \circ a = b$ has a unique solution in S for all $a, b \in S$. The problem of finding all the matrices in \mathcal{A}_n is very difficult. However, this article gives a lower bound to the size of \mathcal{A}_n through left loops.

In [3], Hoffman posed the problem of determining the number of solutions of the matrix equation $A^2 = J_n$, where $A \in \mathcal{A}_n$. In [4], it has been shown that Hoffman's problem is equivalent to an algebraic problem and also equivalent to a graph-theoretic problem. In [5], the existence of the solution of $A^2 = J_n$ of all ranks r , where $k \leq r \leq \lfloor \frac{(k^2+1)}{2} \rfloor$ ($n = k^2$), is proven.

The rest of the paper is organized as follows. In Section 2, we mention the necessary results and definitions for the sake of completeness of the article. In Section 3, we give a lower bound to the size of \mathcal{A}_n through the left loop. In Section 4, we show that the matrix in \mathcal{A}_n corresponding to the loops of order k has rank $2k - 2$, $n = k^2$.

2. Preliminaries

Suppose that D is a directed graph with Property C having a vertex set denoted as $V(D)$. Define a binary operation “.” on $V(D)$ as $x.y = z$, where $x, y, z \in V(D)$ and z is the vertex through which there is a unique path of length two from x to y . By [4, Lemma 1], $(V(D), .)$ is a central groupoid. Also, given any central groupoid $(C, .)$, define a directed graph whose vertices are elements of C , and there is an edge from vertex x to z if $z = x.y$ for some $y \in C$. By [4, Lemma 2], this directed graph satisfies Property C . Suppose (S, \circ) is a left quasigroup such that for some element $0 \in S$, $x \circ 0 = 0$ for all $x \in S$. Define a directed graph D_S on the vertices $S \times S$ having an edge defined by the rule; $(x_1, x_2) \rightarrow (y_1, y_2)$ if and only if $[x_2 = y_1 \text{ and } y_2 \neq 0]$ or $[x_1 \circ x_2 = y_1 \text{ and } y_2 = 0]$. By [4, Theorem 2], D_S is a directed graph with Property C ; that is, D_S is a central groupoid, and the corresponding central groupoid has the multiplication rule (consequence of

Theorem 2 of [4, p. 378])

$$(x_1, x_2) \cdot (y_1, y_2) = \begin{cases} (x_2, y_1), & \text{if } y_1 = 0 \text{ and } y_2 \neq 0 \\ (x_2, z_2), & \text{if } x_2 * z_2 = y_1 \neq 0 \text{ and } y_2 = 0 \\ (x_1 * x_2, 0), & \text{if } y_1 = 0 \end{cases}$$

where $x_1, x_2, y_1, y_2, z_2 \in S$ Further, the following theorem gives more insight into this construction.

Theorem 2.1. [4, Theorem 7, p. 388] *Let S be a finite set on which two binary operations \circ and $*$ are defined, such that, for all a and b , $0 \circ b = 0 * b = b$, $a \circ 0 = a * 0 = 0$, and the equations $a \circ x = b$, $a * y = b$ have unique solution (x, y) . Let D_1 be the directed graph on the vertices $S \times S$ defined by the rule $(x_1, x_2) \rightarrow (y_1, y_2)$ if and only if $[x_2 = y_1 \text{ and } y_2 \neq 0]$ or $[x_1 \circ x_2 = y_1 \text{ and } y_2 = 0]$; and let D_2 be the directed graph defined similarly with $*$ replacing \circ . Then D_1 and D_2 are isomorphic if and only if the binary operations \circ and $*$ are isomorphic.*

Theorem 2.2. [1, Theorem 2.1, p. 37] *Let n be a positive integer. Then $\mathcal{A}_n \neq \emptyset$ if and only if $n = k^2$ for some positive integer k . Furthermore, if $n = k^2$ and $A \in \mathcal{A}_n$, then*

- (a) *all row sums and column sums of $A = k$,*
- (b) *A has eigenvalues $k, 0, \dots, 0$,*
- (c) *A has exactly k 1's on its main diagonal.*

Theorem 2.3. [1, Theorem 2.2, p. 38] *The Jordan forms of the matrices in \mathcal{A}_n are precisely:*

$$[\sqrt{n}] \oplus \underbrace{B \oplus B \oplus \dots \oplus B}_p \oplus 0_{n-2p-1}, \sqrt{n} - 1 \leq p \leq \frac{n-1}{2} \text{ and } B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Consequently, if $A \in \mathcal{A}_n$, then $\sqrt{n} \leq \text{rank}(A) \leq \frac{n+1}{2}$.

3. Left loop as directed graph with Property C

In this section we will show that for each left loop of order k , there is a unique (upto isomorphism) central groupoid of order k^2 , that is a directed graph on vertex $V(D)$ of size k^2 with property C . Now onwards, by S we mean the set $\{0, 1, 2, \dots, k-1\}$. Suppose $(S, *)$ is a left quasigroup with left identity 0 and $x * 0 = 0$ for all $x \in S$. We call $(S, *)$ as left quasigroup with

left identity and right zero. By [4], for each $(S, *)$ there exists a unique (upto isomorphism) directed graph with property C on $S \times S$. So to establish a correspondence between left loop and central groupoid, it is sufficient to show a correspondence between left loop and left quasigroup with identity and right zero.

Proposition 3.1. *Let $(S, *)$ be left quasigroup such that $x * 0 = 0$ and $0 * x = x$ for all $x \in S$. Consider $T_S = S$. Define a binary operation “ \circ ” on T_S as follows: $0 \circ i = i \circ 0 = i$; for all $i \in S$ and $i, j \neq 0$,*

$$i \circ j = \begin{cases} i * j & ; i * j \neq i, \\ 0 & ; i * j = i. \end{cases}$$

Then (T_S, \circ) is a left quasigroup with identity 0.

Proof. Clearly 0 is the identity element of (S, \circ) . Consider the equation

$$i \circ X = j. \quad (3)$$

If $i * X \neq i$, then $i \circ X = j = i * X$, which has a unique solution. Suppose $i * X = i$. Since $i \neq 0$ then for $i * X = i$ implies $X \neq 0$. Since $(S, *)$ is left quasigroup, $i * X = i$ has unique solution t (say). That is $i \circ X = 0$ has a unique solution, t . This completes the proof. \square

We call (T_S, \circ) the left loop corresponding to $(S, *)$.

Proposition 3.2. *Let $S = \{0, 1, 2, \dots, k-1\} = T_S$ be a set such that (T_S, \circ) is a left quasigroup with identity 0. Let $*$ be the binary operation on S defined by the rule; $x * 0 = 0$, $0 * x = x$ for all $x \in S$ and*

$$i * j = \begin{cases} i & ; i \circ j = 0, \\ i \circ j & ; i \circ j \neq 0. \end{cases}$$

*Then $i * X = j$ has unique solution in S whenever $i, j \in S$.*

Proof. Consider, $i * X = j$. Now $i \circ X \neq 0$ implies $i \circ X = j = i * X$, which has a unique solution. Suppose $i \circ X = 0$ then $i * X = i$. For $i \neq 0$, $X \neq 0$. Since (T_S, \circ) is a left quasigroup, $i \circ X = 0$ has a unique non-zero solution t (say). Therefore $i * X = i$ have a unique solution, t . This completes the proof. \square

Let \mathcal{A} be the set of all left quasigroups with left identity and right zero structure on S and \mathcal{B} be the set of all left quasigroup structures on S . Define a map $\phi : \mathcal{A} \rightarrow \mathcal{B}$ by $\phi(S) = T_S$. Then by Proposition. 3.1 and Proposition 3.2, ϕ is bijective.

Proposition 3.3. *Let $(S_1, *_1), (S_2, *_2)$ be two right quasigroup with left identity and right zero such that $S_1 = S_2 = \{0, 1, 2, \dots, k - 1\}$. Let $(T_{S_1}, \circ_1), (T_{S_2}, \circ_2)$ be the corresponding quasigroup structures. Then $S_1 \cong S_2$ if and only if $T_{S_1} \cong T_{S_2}$.*

Proof. Let $f : S_1 \rightarrow S_2$ be an isomorphism. Let us define a map $\phi_f : T_{S_1} \rightarrow T_{S_2}$ such that $\phi_f(i) = f(i)$. Since, f is bijective implies ϕ_f is bijective. Now,

$$\phi_f(i \circ_1 j) = \begin{cases} \phi_f(i *_1 j) & ; i *_1 j \neq i, \\ 0 & ; i *_1 j = i. \end{cases}$$

We have, $\phi_f(i) \circ_2 \phi_f(j) = l \circ_2 k$ for $f(i) = l$ and $f(j) = k$. Then we get,

$$l \circ_2 k = \begin{cases} l *_2 k & ; l *_2 k \neq l, \\ 0 & ; l *_2 k = l. \end{cases}$$

Now,

$$l *_2 t = l \Leftrightarrow f(i) *_2 f(j) = f(i) \Leftrightarrow f(i *_1 j) = f(i) \Leftrightarrow i *_1 j = i.$$

(f is one-to-one).

Similarly, we get,

$$l *_2 t \neq l \Leftrightarrow f(i) *_2 f(j) \neq f(i) \Leftrightarrow f(i *_1 j) \neq f(i) \Leftrightarrow i *_1 j \neq i.$$

Therefore $\phi_f(i \circ_1 j) = \phi_f(i) \circ_2 \phi_f(j)$. The converse is easy to verify. \square

Remark 3.4. It is clear from above Proposition that if T_S is a loop then each column of multiplication table of $(S, *)$ (except first column) has exactly two entries repeated (see example 4.2).

Following theorem is the immediate consequence of Theorem 2.1, Proposition 3.1, Proposition 3.2 and Proposition 3.3.

Theorem 3.5. $|\mathcal{A}_n| \geq$ number of non-isomorphic left loops of order k where $n = k^2$.

4. Rank of the matrix in \mathcal{A}_n

Theorem 4.1. *Let (T, \circ) be a left loop of order k and $(S, *)$ denote a left quasigroup with left identity and right zero such that $T_S = T$. Let D_S be the associated directed graph with Property C and $A(T)$ be the adjacency matrix of D_S . Then rank of $A(T)$ is $2k - 2$.*

Proof. As argued in Section 2, we define directed graph D_S on the vertex set $S \times S$ by the rule: $(l_1, l_2) \rightarrow (m_1, m_2)$ if and only if $[l_2 = m_1 \text{ and } m_2 \neq 0]$ or $[l_1 * l_2 = m_1 \text{ and } m_2 = 0]$ and its corresponding central groupoid has the multiplication rule

$$(l_1, l_2) \cdot (m_1, m_2) = \begin{cases} (l_2, m_1), & \text{if } m_1 = 0 \text{ and } m_2 \neq 0, \\ (l_2, m_2), & \text{if } l_2 * m_2 = m_1 \neq 0 \text{ and } m_2 = 0, \\ (l_1 * l_2, 0), & \text{if } m_1 = 0. \end{cases}$$

Then using this multiplication rule the adjacency matrix $A(T)$ of the directed graph D_S so obtained can be viewed as blocks of a column of size k (see Figure 1 below). Label the blocks of column as $0, 1, 2, \dots, k - 1$. We represent any row vector of $A(T)$ by $[x, y]$, which would denote $(k - 1)$ 1's in the x^{th} block and single 1 in the y^{th} block for $x \neq y$. Infact it has single 1 in the position $(l * m, 0)$, for $l, m \neq 0$. We denote standard row vectors by $[x, x]$ (all 1's in x^{th} block). Therefore first k rows of $A(T)$ will be represented by $[0, 0], [1, 1], \dots, [k - 1, k - 1]$ which are in standard form, hence linearly independent. So rank of $A(T)$ is atleast k . By our construction, every row vector different from standard row vector contains $(k - 1)$ 1's in one block and a single 1 in another block. The following relation gives the addition and subtraction of any two row vector of $A(T)$;

$$[x_1, y_1] + [x_2, y_2] = [(x_1, x_2), (y_1, y_2)]$$

Hence rank of $A(T)$ is atmost $2k - 2$ where $[(x_1, x_2), (y_1, y_2)]$ denote a row with $(k - 1)$ 1's in x_1 and x_2 blocks and 1 in y_1 and y_2 blocks. Consider the set of following row vectors $\{[1, 2], [1, 3], \dots, [1, k - 1]\}$. Clearly, these can be reduced to echelon form and so linearly independent. Now we show that the set $M := \{[0, 0], [1, 1], \dots, [k - 1, k - 1], [1, 2], [1, 3], \dots, [1, k - 1]\}$ of $2k - 2$ vectors is linearly independent. But if it is not, then a vector, say $[1, x]$ can be written as a sum and difference of the other row vectors in the set, with at least one of them being $[1, y]$, for $y \neq x$. To obtain single 1 in the x^{th} block, we need to add or subtract with the vector that ends with x , the only

choice is $[x, x]$, and again we need to add or subtract with the row vector that starts with x . The only choice for this also $[x, x]$. Hence this addition and subtraction cannot be done. And so, $[1, x]$ is not a linear combination of other vectors of the set M . Therefore, it is linearly independent. Also, any row vector $[x, y]$ which is not in M is a linear combination of vectors in M , which is clear from the following relation:

$$[x, y] = [1, y] + [x, x] - [1, x].$$

Now we show that if (T_S, \circ) is the loop corresponding to $(S, *)$, all the row vectors from the set M are in $A(T)$. It is clear that $2 * 1 = 3$ would give the row vector $[1, 3]$ (see Figure 1, 12th row). By Remark 3.4 there is exactly $k - 2$ solutions of the equation $y * 1 = x$ for all $2 \leq x \leq k - 1$. This would correspond to $k - 2$ row vectors $[1, x]$, $2 \leq x \leq k - 1$. Hence, the matrix $A(T)$ has rank exactly equal to $k + (k - 2) = 2k - 2$. This completes the proof. \square

Following illustration gives more insight to the above Theorem.

Example 4.2. Consider the following multiplication table of loop structure (T_S, \circ) :

\circ	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Then corresponding left quasigroup with left identity and right zero $(S, *)$ is given by

$*$	0	1	2	3	4
0	0	1	2	3	4
1	0	2	3	4	1
2	0	3	4	2	1
3	0	4	3	1	2
4	0	4	1	2	3

Here $k = 5$. Following is the adjacency matrix $A(T)$ (Figure 1) formed by using the rule mentioned in the above Theorem. The first five row represents the standard row vectors $[0, 0], [1, 1], [2, 2], [3, 3], [4, 4]$. So the

rank of $A(T) \geq 5$. Clearly, the 7th row has 4 1's in block 1 and lone 1 in block 2, representing the row vector $[1, 2]$. Similarly, the 12th and 17th rows represent the vectors $[1, 3]$ and $[1, 4]$, respectively. Therefore the set of vectors $M := \{[0, 0], [1, 1], [2, 2], [3, 3], [4, 4], [1, 2], [1, 3], [1, 4]\}$ are in $A(T)$. By above theorem rank of $A(T) = 2k - 2 = 8$.

	0	1	2	3	4
[0,0]	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
[1,1]	0 0 0 0 0	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
[2,2]	0 0 0 0 0	0 0 0 0 0	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0
[3,3]	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	1 1 1 1 1	0 0 0 0 0
[4,4]	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	1 1 1 1 1
[1,2]	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 1 1 1 1	1 0 0 0 0	0 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	0 1 1 1 1	1 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 1 1 1 1	1 0 0 0 0
	0 0 0 0 0	1 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 1 1 1 1
[1,3]	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 1 1 1 1	0 0 0 0 0	1 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	0 1 1 1 1	0 0 0 0 0	1 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	1 0 0 0 0	0 1 1 1 1	0 0 0 0 0
	0 0 0 0 0	1 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 1 1 1 1
[1,4]	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 1 1 1 1	0 0 0 0 0	0 0 0 0 0	1 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	0 1 1 1 1	1 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	1 0 0 0 0	0 0 0 0 0	0 1 1 1 1	0 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	1 0 0 0 0	0 0 0 0 0	0 1 1 1 1
	1 1 1 1 1	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 1 1 1 1	0 0 0 0 0	0 0 0 0 0	1 0 0 0 0
	0 0 0 0 0	1 0 0 0 0	0 1 1 1 1	0 0 0 0 0	0 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	1 0 0 0 0	0 1 1 1 1	0 0 0 0 0
	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	1 0 0 0 0	0 1 1 1 1

Figure 1: Adjacency matrix $A(T)$.

Remark 4.3. However, the converse need not be true. Consider the following multiplication table of (T_S, \circ) ;

\circ	0	1	2	3	4
0	0	1	2	3	4
1	1	0	2	3	4
2	2	0	1	3	4
3	3	0	2	1	4
4	4	0	2	3	1

Then it has following adjacency matrix (Figure 2) of rank 8.

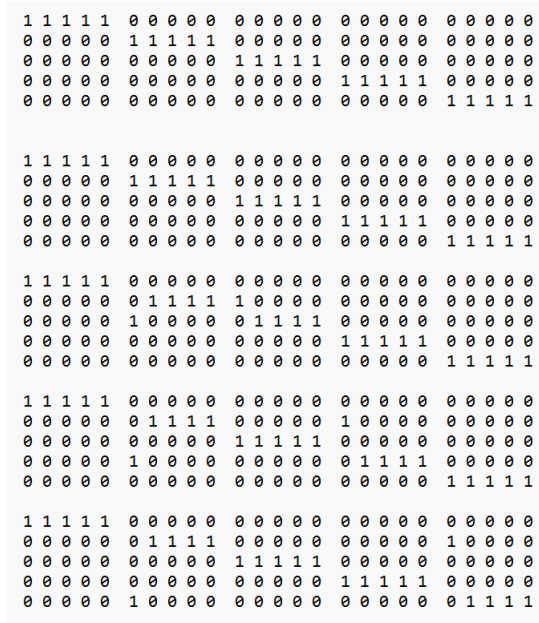


Figure 2.

Corollary 4.4. *If there are m number of non-isomorphic loops of order k , then there exists at least m non-permutationally similar matrices in \mathcal{A}_n of rank $2k - 2$.*

Remark 4.5. It is clear that the minimal polynomial of any matrix in \mathcal{A}_n is $x^2(x - k)$ and so the maximum size of the block in Jordan form is 2. Then any matrix in \mathcal{A}_n corresponding to the loop (T, \circ) will have Jordan canonical form, $[\sqrt{n}] \oplus \underbrace{B \oplus B \oplus \dots \oplus B}_p \oplus 0_{n-2p-1}$, where $p = 2k - 3$.

Acknowledgement. The author is supported by UGC, Government of India (Grant number 415975). The author is thankful to the referee for valuable comments and suggestions. I would also like to thank Dr. Vivek Kumar Jain for his immense support to complete this article.

References

- [1] **F. Curtis, J. Drew, C.K. Li and D. Pragel**, *Central groupoids, central digraphs, and zero-one matrices A satisfying $A^2 = J$* , J. Combin. Theory, Series A, **105**(1) (2014), 35 – 50.
- [2] **T. Evans**, *Products of points—some simple algebras and their identities*, Amer. Math. Monthly, **74**(4) (1967), 362 – 372.
- [3] **A.J. Hoffman**, *Research Problem*, J. Combin. Theory 2, **393** (1967), 2 – 11.
- [4] **D.E. Knuth**, *Notes on central groupoids*, J. Combin. Theory, **8**(4) (1970), 376 – 390.
- [5] **L.E. Shader**, *On the existence of finite central groupoids of all possible ranks*, J. Combin. Theory (A), **16** (1974), 221 – 229.
- [6] **Y. K. Wu, R.Z. Jia, and Q. Li**, *g -Circulant solutions to the $(0, 1)$ matrix equation $A^m = J_n$* , Linear Algebra Appl., **345** (2002), 195 – 224.

Received July 22, 2022

Department of Mathematics
 Central University of South Bihar
 Gaya - 824236
 Bihar, India
 E-mail: 20rawraj@gmail.com, rajarawat@cusb.ac.in