Residue Matrix and not Distributive Lattice

T.SrinivasaRao , Dr. L.Sujatha

Asst.Professor , Dept. of Mathematics

AdikaviNannaya University , Rajamahendravaram

Andhra Pradesh

Abstract

The residue classes modulo 4 do not form a field and having the divisors of zero that will help us in residue classes as considered as the entries showing the lattice suitably constructed is not distributive. The of $n \times n$ matrix and the respective determinant is considered.

$$M_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, M_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \ldots, M_{255} = \begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix} \qquad \ldots\ldots\ 2.1$$

Considering the determinants of these matrices, it can be followed as the determinants vary from – 9 through 9. The set of matrices are partitioned into equivalence classes depending on the determinant and the partition is not regular. So, it is suitable to fit the structure into lattice and the 19 equivalence classes are having unequal number of members that are the $n \times n$ matrices. The equivalence classes and the respective number of members in each class are specified in the following chapter. The set of the equivalence classes form a lattice and is not distributive.

Keywords: *Residue classes, multiplication modulo m, equivalence classes, maximum and minimum*

I. Introduction

It is the day in day out problem that cyber security and update to keep the data not hacked. Mathematical tools are the key role players in providing security key that helps the people who are the producers of the data/information and who to share the information. Algebra is less explored in the direction of security key construction when compared to number theory. But if algebra is used for the construction of encrypting and decrypting the code, which helps the information is secured more than the present day security systems. Among the algebraic systems, the non commutative and non associative algebraic structures are helpful to retrieve the data by the tools that are the creators of the information rather than a decrypting tool constructed by an illegal hand. A step ahead in anticipation is the present activity that deals with non associative lattice defined over the classes of matrices that are unevenly divided into equivalence classes in some sense or other.

1. Statement: the equivalence classes comprising matrices of residue classes modulo 4 form a lattice that is not distributive.

The comparability is dependent of the least member or greatest member of each equivalence class.

…… 1.1

The set of matrices that yield – 9 is seen as

$$[m-9] = \{M_{60}, M_{61} M_{62}, M_{63}, M_{124}, M_{188}, M_{252}\}, \left|[m-9]\right| = 7$$

$$[m-8] = \{M_{125}\}, \left|[-8]\right| = 1,$$

$$[m-7] = \{M_{126}, M_{189}\}, \left|[-7]\right| = 2,$$

$$[m-6] =$$

$$\{M_{44}, M_{45} M_{46}, M_{56}, M_{57}, M_{58}, M_{59}, M_{108}, M_{120}, M_{127}, M_{172}, M_{184}, M_{236}, M_{248}, M_{253}\}$$

$$\left|[m-6]\right| = 16$$

$$[m-5]=\{M_{109},M_{121}M_{190}\},\ \|[m-5]\|=3$$

$$[m-4]=\{M_{40},M_{41}M_{42},M_{43},M_{104},M_{110},M_{122},M_{168},M_{173},M_{185},M_{232}\}\ \|[m-4]\|=11$$

$$[m-3]=\{M_{28},M_{29}M_{30},M_{31},M_{52},M_{53},M_{54},M_{55},M_{92},M_{105},M_{111},M_{116},M_{123},$$
$$M_{156},M_{180},\ M_{191},M_{220},M_{237},M_{244},M_{249},M_{254}\},\ \|[m-3]\|=21,$$

$$[m-2]=\{M_{24},M_{25}M_{26},M_{27},M_{36},M_{37},M_{38},M_{39},M_{88},M_{93},M_{100},M_{117},M_{152},$$
$$M_{164},M_{169},\ M_{174},M_{186},M_{216},M_{228}\},\ \|[m-2]\|=20$$

$$[m-1]=\{M_{20},M_{21}M_{22},M_{23},M_{84},M_{89},M_{94},M_{101},M_{107},M_{118},M_{148},$$
$$M_{157}\ M_{181},M_{212},M_{233},\|[m-1]\|=15$$

$$[m+0]=\{M_{0},M_{1},M_{2},M_{3},M_{4},M_{5},M_{6},M_{7},M_{8},M_{9},M_{10},M_{11},M_{12},M_{13},M_{14},M_{15},$$
$$M_{16},M_{17},M_{18},M_{19},M_{32},M_{33},M_{34},M_{35},M_{48},M_{49},M_{50},M_{51},M_{64},M_{68},M_{72},M_{76},M_{80},$$
$$M_{85},M_{90},M_{95},M_{96},M_{102},M_{119},M_{128},M_{132},M_{136},M_{140},M_{144},M_{153},M_{160},M_{165},$$
$$M_{170},M_{175},M_{176},M_{187},M_{192},M_{196},M_{200},M_{204},M_{208},M_{221},M_{224},$$
$$M_{238},M_{240},M_{245},M_{250},M_{255}\},\ \|[m+0]\|=64$$

$$[m+1]=$$
$$\{M_{65},M_{69},M_{73},M_{77},M_{81},M_{86},M_{91},M_{97},M_{103},M_{113},M_{149},M_{158},M_{\ 182},M_{217},M_{229}\},$$
$$\|[m+1]\|=15$$

$$[m+2]=\{M_{66},M_{70},M_{74},M_{78},M_{82},M_{87},M_{98},M_{114},M_{129},M_{133},M_{137},M_{141},M_{145},$$
$$M_{154},M_{161},\ M_{166},M_{171},M_{213},M_{234}\},\ \|[m+2]\|=20$$

$$[m+3]=\{M_{67},M_{71},M_{75},M_{79},M_{83},M_{99},M_{115},M_{150},M_{159},M_{183},M_{193},M_{197},M_{201},$$
$$M_{205},M_{209},\ M_{222},M_{225},M_{239},M_{241},M_{246},M_{251}\},\|[m+3]\|=21$$

$$[m+4]=\{M_{130},M_{134}M_{138},M_{142},M_{146},M_{155},M_{162},M_{167},M_{178},M_{218},M_{230}\},$$
$$\|[m+4]\|=11$$

$$[m+5]=\{M_{151},M_{214},M_{235}\}\ \|[m+5]\|=3$$

$$[m+6]=\{M_{131},M_{135}M_{139},M_{143},M_{147},M_{163},M_{179},M_{194},M_{198},M_{202},M_{206},M_{210},$$
$$M_{223},M_{226},M_{242},M_{247}\}$$
$$\|[m+6]\|=16$$

$$[m+7]=\{M_{219},M_{231}\},\|[m+7]\|=2$$

$$[m+8]=\{M_{215}\},\|[m+8]\|=1$$

$$[m+9]=\{M_{195},M_{199},M_{203},M_{207},M_{211},M_{227},M_{243}\},\|[m+9]\|=7$$

$$\sum_{k=-9}^{9}\|[m+k]\|=256$$

It is easily verified that the orders of the equivalence classes are symmetricabout theorder of the class $[m+0]$

Suppose $L_{2\times 2}=\{[m+k]:-9\le k\le 9,k\in\square\}$ and define the operations $\vee$ and $\wedge$ by

$$[m+i]\vee[m+j]=\max\{[m+k]:\det(M_iM_j)=k\}\text{ and}$$

$$[m+i]\wedge[m+j]=\min\{[m+k]:\det(M_iM_j)=k\}$$

See that $[m-3]\wedge\{[m-1]\vee[m+3]\}=[m-3]\wedge\max\{\det M_{20}M_{67}=[m+k]\}$

$$=[m-3]\wedge\{\max[m+k]:k=\det M_{20}M_{67}\}$$

$$=[m-3]\wedge\max\{[m+0]\}$$

$$=\min\{[m+k]:k=\det M_{28}\times M_{255}\}$$

$$=\min\{M_{119}\}$$

$$=[m+0] \qquad \ldots\ldots 1.2$$

On the other hand, $\{[m-3]\wedge[m-1]\}\vee\{[m-3]\wedge[m+3]\}=$

$$[m-3]\wedge[m-1]=\min\{[m+k]:k=\det M_{28}M_{20}\}$$

$$=\min\{[m+k]:k=\det M_{193}\}$$

$$=\min\{M_{67}\}$$

$$=[m+3]$$

$$[m-3]\wedge[m+3]=\min\{[m+k]:k=\det M_{28}M_{67}\}$$

$$=\min\{[m+k]:k=\det M_{20}\}$$

$$=\min\{M_{20}\}$$

$$=[m-1]$$

$$\{[m-3]\wedge[m-1]\}\vee\{[m-3]\wedge[m+3]\}=[m+3]\vee[m-1]$$

$$=\max\{[m+k]:k=\det M_{67}M_{20}\}$$

$$=\max\{[m+k]:k=\det M_{52}\}$$

$$=\max\{M_{52}\}$$

$$=[m-3] \qquad \ldots\ldots\ 1.3$$

The equations 1.2 and 1.3 verify that the lattice formed is non distributive.

While the other parts of the definition of lattice are routine to verify, there are illustrations in this lattice that dissatisfy the distributive property. So, this lattice is not distributive and there should not be an ambiguity in non – distributive lattice.

Conclusion: the present paper is a gesture to send a signal to one end from the root and retrieving the direction from the leaf to the root may be difficult while the distributivity fails in some incidents.

References

[1] Charles S. Peirce(1880), “On the Algebra of Logic”, American Journal of Mathematics

[2] Garrett Birkhoff(1967) Lattice Theory Colloquium Publications 25, American Mathematical Society

[3] Rota, Glan – Carlo(1997), “The many lives of lattice Theory”, Notices of the American Mathematical Society