Enumeration of the Roots of Boolean Matrices

N. Assimakis[1, a)], M. Adam[2, b)], Ch. Massouros[3, c)], M. Etairidis[4, d)]

[1]*Department of Electronic Engineering, Technological Educational Institute of Central Greece, Greece*
[2]*Department of Computer Science and Biomedical Informatics, University of Thessaly, Greece*
[3]*Faculty of Management and Economics, Technological Educational Institute of Central Greece, Greece*
[4]*Beck IPC GmbH, Germany*

[a)] assimakis@teiste.gr, [b)] madam@dib.uth.gr, [c)] Ch.Massouros@gmail.com, [d)] m.g.eteridis@gmail.com

Abstract. The number of the roots of certain Boolean matrices is calculated in this paper. In particular, the roots of the Boolean Identity, Exchange, Total and Zero matrices are enumerated and an algorithmic method is introduced for this purpose.

INTRODUCTION

An algebraic system $(S,+,\cdot)$ is called *semiring* if $(S,+)$ and $(S,\cdot)$ are semigroups which are connected by a ring-like distributivity. The Boolean domain $B=\{0,1\}$ becomes a semiring under the addition: 0+1=1+0=1+1=1, 0+0=0 and the multiplication: 0·0 = 0·1=1·0=0, 1·1=1. This semiring is called *binary Boolean semiring*. A *Boolean matrix* is a matrix with entries from the binary Boolean semiring. A *square* Boolean matrix is a Boolean matrix, which has the same number of rows and columns and hereafter it is referred to as $n \times n$. A square Boolean matrix is called *identity matrix,* denoted by I, when its only non-zero entries are its diagonal elements. An $n \times n$ Boolean matrix, J, is called *exchange matrix* if the only non-zero entries are its counter diagonal (or antidiagonal) elements. The *total matrix*, T, is an $n \times n$ Boolean matrix, which has all its entries equal to 1, while the *zero matrix*, Z, has all its entries equal to 0. For $\nu \geq 2$, the ν-th power A^ν of an $n \times n$ Boolean matrix A is the ν-th matrix product of A by itself. The ν-th root of an $n \times n$ Boolean matrix, B, is a matrix A such that $A^\nu=B$. A is called *basic* ν-root, if A is not a ν-root any more, when any one of its unit entries is replaced by zero [22]. The number of the entries, which are equal to 1 is not constant in all basic ν-roots. A basic ν-root is called *minimum*, if it is the basic matrix with minimum number of unit entries.

Every binary relation ρ in a finite set H, with $cardH = n,\ n \neq 0$, can be represented by an $n \times n$ Boolean matrix M_ρ and conversely every $n \times n$ Boolean matrix defines on H a binary relation. Indeed, let H be the set $\{a_1,\ldots,a_n\}$. Then, a $n \times n$ Boolean matrix is constructed as follows: the element (i, j) of the matrix is 1 if $(a_i,a_j) \in \rho$ and 0 if $(a_i,a_j) \notin \rho$ and vice versa. Binary relations are frequently used to define hypercompositional structures. A *hypercomposition* in a non-empty set H is a function from $H \times H$ to the powerset $P(H)$ of H. This notion was introduced in mathematics, alongside the notion of the *hypergroup*, by Marty in 1934 [21]. The axioms that endow the pair $(H,\circ)$ with the hypergroup structure, where H is a non-empty set and ‘‘ $\circ$ ’’ is a hypercomposition on H, are:

i) $a \circ (b \circ c) = (a \circ b) \circ c$, for all $a,b,c \in H$ (*associativity*);

ii) $a \circ H = H \circ a = H$, for all $a \in H$ (*reproductivity*).

Among others, Corsini [6,7], Chvalina [3,4,5], S. Hoskova-Mayerova [2,4,5,15], Rosenberg [27], Ameri et al. [1,2], Corsini and Leoreanu [8], Cristea et al. [9,10,11,12,16], De Salvo and Lo Faro [13,14], Jančić-Rašović [17,18], M. Novák [24,25], Křehlík and M. Novák [19], Račková [26], studied hypercompositional structures defined in terms of binary relations. Rosenberg, for example, introduced in a non-empty set H the hypercomposition:

International Conference of Numerical Analysis and Applied Mathematics (ICNAAM 2017)
AIP Conf. Proc. 1978, 340008-1–340008-5; https://doi.org/10.1063/1.5043951
Published by AIP Publishing. 978-0-7354-1690-1/$30.00

$$x \circ x = \{z \in H \mid (x,z) \in \rho\} \quad \text{and} \quad x \circ y = x \circ x \cup y \circ y$$

where ρ is a binary relation on H [27]. In [28] it is proved that the square roots of the total Boolean matrices produce Rosenberg hypergroups and moreover that the Rosenberg hypergroup which is produced from the minimum basic Boolean matrix is a join one. Many more examples emphasize on the importance of examining the roots of certain types of Boolean matrices. The complexity of the Boolean matrix root computation is studied in [20] where it is proved that determining the roots of Boolean matrices is an NP-hard (non-deterministic polynomial-time) problem. The interpretation of Boolean matrices as directed graphs or digraphs, highlighted a connection between Boolean matrix roots and graph isomorphisms, which led to the proof that the complexity of determining the roots of a certain subclass of Boolean matrices is the same as in the graph-isomorphism problem. The ν-th roots, $\nu=2,\ldots,10$, of the identity, exchange, total and zero Boolean matrices, when their dimensions are $n=2,3,4$ are enumerated herein.

ROOTS OF THE IDENTITY MATRIX

All the roots of the $n\times n$, ($n=2,3,4,5$) identity matrix, are matrices which have n entries equal to 1. Therefore, all the roots are basic. For $\nu=2$, all the square roots of the matrix I, are permutation matrices with only one unit per row and column. Thus, for $n=2$ there exist two square roots of the identity matrix: I itself and the exchange matrix J. For $n=3$ the square roots of I are:

$$\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}, \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}, \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}, \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}.$$

Apparently, the exchange matrix is always a square root of the identity matrix. For $n=3$ the cube roots of I are:

$$\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}, \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}, \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}.$$

For $n=3$ and $\nu=4$ the 4th degree root matrices of I are the same as for the square root matrices of I. For $n=3$ and $\nu=5$, I itself is only the 5th degree root of I. For $n=3$ and $\nu=6$ the 6th degree root matrices of I are:

$$\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}, \begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}, \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}, \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}, \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}, \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}.$$

For n=3 and ν=7 the only 7th degree root matrix of I is I itself.

ROOTS OF THE EXCHANGE MATRIX

The matrix J does not have any roots when $n=2$, for every ν. For $n>2$, all $n\times n$ matrices, which are roots of the matrix J, have n entries equal to 1. All the roots of the exchange matrix are basic. For $n=3$ there are no roots of even degree, while J itself is the only one root, when ν is odd. For $n=4$ and $\nu=2$ the square roots of J are:

$$\begin{bmatrix}0&0&1&0\\1&0&0&0\\0&0&0&1\\0&1&0&0\end{bmatrix}, \begin{bmatrix}0&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&1&0\end{bmatrix}.$$

For $n=4$ and $\nu=3$ the only cube root matrix of J is J itself. For $n=4$ and $\nu=4$ there are no forth degree roots of J. For $n=4$ and $\nu=5$ the only 5th degree root matrix of J is J itself.

ROOTS OF THE TOTAL MATRIX

In [22] the square roots of the total Boolean matrix with dimension 2, 3, 4, 5 are enumerated, while [23] presents a detailed study on these roots. In [22] it is proved that the $n\times n$ matrices which have all their i row and their i column, $i=1,\ldots,n$, entries equal to 1 are basic square roots and moreover these are the minimum ones. Hence the number of the minimum square roots of the $n\times n$ total matrix T is n. For n=2, the square roots of T are:

$$\begin{bmatrix}0&1\\1&1\end{bmatrix},\ \begin{bmatrix}1&1\\0&1\end{bmatrix},\ \begin{bmatrix}1&1\\1&1\end{bmatrix}.$$

The first two of the above matrices are the minimum square roots of T. The total Boolean matrix T is always a square root of itself but it is not a basic one. For n=3, the minimum square roots of T are:

$$\begin{bmatrix}1&1&1\\1&0&0\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&1&0\\1&1&1\\0&1&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\0&0&1\\1&1&1\end{bmatrix}.$$

Each one of the above minimum square roots produces a set of basic square roots, by replacing 1 with 0 and 0 with 1 in the same either column, or row or diagonal [22]. Thus, for example, the first one gives:

$$\begin{bmatrix}1&1&1\\1&0&0\\1&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&0&1\\1&1&0\\1&1&0\end{bmatrix},\ \begin{bmatrix}1&1&0\\1&0&1\\1&0&1\end{bmatrix},\ \begin{bmatrix}1&1&1\\0&1&1\\1&0&0\end{bmatrix},\ \begin{bmatrix}1&1&1\\1&0&0\\0&1&1\end{bmatrix},\ \begin{bmatrix}0&1&1\\1&1&0\\1&0&1\end{bmatrix}$$

ROOTS OF THE ZERO MATRIX

Z is always a root of itself, which is obviously the minimum one as well. It is interesting though to try to find its maximum roots, i.e. roots with the maximum possible unit entries. The elements of the main diagonal of a root of the zero matrix is always equal to zero. Thus, for n=3 the square roots of Z are 13, Z itself and the following ones:

$$\begin{bmatrix}0&1&0\\0&0&0\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\0&0&0\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&1&1\\0&0&0\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\1&0&0\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\0&0&1\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&0&1\\0&0&1\\0&0&0\end{bmatrix},$$

$$\begin{bmatrix}0&0&0\\1&0&1\\0&0&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\0&0&0\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\1&0&0\\1&0&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\0&0&0\\0&1&0\end{bmatrix},\ \begin{bmatrix}0&1&0\\0&0&0\\0&1&0\end{bmatrix},\ \begin{bmatrix}0&0&0\\0&0&0\\1&1&0\end{bmatrix}.$$

For n=3 and ν=3 the cube roots of Z are 25 and they remain so many for ν>3 as well (see Table 1).

CONCLUSIONS

The number of the roots of the Boolean Identity, Exchange, Total and Zero matrix, for n=2,3,4 and ν=2,...,10, is summarized in Table 1.

TABLE 1. Number of roots of Boolean Identity, Exchange, Total and Zero matrix.

Identity matrix I

ν \ n	2	3	4
2	2	4	10
3	1	3	9
4	2	4	16
5	1	1	1
6	2	6	18
7	1	1	1
8	2	4	16
9	1	3	9
10	2	4	10

Exchange matrix J

ν \ n	2	3	4
2	0	0	2
3	1	1	1
4	0	0	0
5	1	1	1
6	1	0	2
7	1	1	1
8	0	0	0
9	1	1	1
10	0	0	2

Total matrix T

ν \ n	2	3	4
2	3	73	6 003
3	3	115	19 599
4	3	133	24 027
5	3	139	25 215
6	3	139	25 527
7	3	139	25 527
8	3	139	25 527
9	3	139	25 551
10	3	139	25 575

Zero matrix Z

ν \ n	2	3	4
2	3	13	87
3	3	25	351
4	3	25	543
5	3	25	543
6	3	25	543
7	3	25	543
8	3	25	543
9	3	25	543
10	3	25	543

The number of the minimum roots of the Boolean Total matrix and the minimum number of units in them, when n=2..5 and ν=2,...,10, is summarized in Table 2.

TABLE 2. Total matrix: Number of minimum roots and minimum number of "1"

Number of minimum roots

v \ n	2	3	4	5
2	2	3	4	5
3	2	27	304	1865
4	2	6	144	60
5	2	12	420	420
6	2	12	612	3060
7	2	12	612	5460
8	2	12	612	120
9	2	12	636	120
10	2	12	636	120

Minimum number of "1"

v \ n	2	3	4	5
2	3	5	7	9
3	3	5	7	9
4	3	4	6	7
5	3	4	6	7
6	3	4	6	7
7	3	4	6	7
8	3	4	6	6
9	3	4	6	6
10	3	4	6	6

The basic conclusions are:

- All roots of the Identity matrix and the Exchange matrix are also minimum roots.
- The number of minimum roots of the Total matrix is less than the number of its basic roots.
- It is obvious that the derivation of all the roots of a Boolean matrix requires checking of all the possible 2^{n^2} solutions, a process that requires long computational time which is prohibitive, while, all the minimum roots can be determined in significantly less computational time. The proposed algorithmic process needs to check $\sum_{i=0}^{N}\binom{n^2}{i}$ solutions only, where N is the minimum possible number of units. So, after resetting the system with the zero matrix (i=0), in every next loop (i=1, 2 and so on) units are added in place of zeros and the deriving matrices are tested whether they are solutions or not. Of course, N represents the first occurrence of a solution, which is thus a minimum solution. The remaining minimum solutions, if any, will still have N unit entries. Hence the number of the possible minimum roots is $\binom{n^2}{N} = \dfrac{n^2!}{N!(n^2-N)!}$.

From $\sum_{i=0}^{N}\binom{n^2}{i} = 2^{n^2} - \dfrac{n^2!}{N!(n^2-N-1)!}\int_1^2 (2-x)^N x^{n^2-N-1}dx < 2^{n^2}$ it derives that $\sum_{i=0}^{N}\binom{n^2}{i} < 2^{n^2}$. The second part of the previous equality can be computed in Matlab as follows:

```
2^(n^2) - factorial(n^2)/(factorial(N)*factorial(n^2-N-1)) * int((2-x)^N*x^(n^2-N-1),1,2)
```

In certain occasions when there are properties which determine the form and the number of the roots, the above process is much shorter or not even required. For instance, in [22] it is shown that in an $n \times n$ total matrix the minimum square roots are the $n \times n$ matrices which have all the entries of their *i* row and their *i* column, $i = 1,\ldots,n$, equal to 1. Hence the $n \times n$ total matrix has *n* square roots and each one of them has $N = 2n-1$ unit entries. Furthermore, in an $n \times n$ matrix $B = (b_{ij})$ with unit entries in one entire row or (one entire) column e.g. the *j*-column, if $A = (\alpha_{ij})$ is a square root of *B*, then *A* must have at least *n* unit entries. Indeed, since $b_{kj} = 1$, for $k = 1,\ldots,n$, then among the products $a_{km}a_{mj}$, $k,m = 1,\ldots,n$, the sum of which equals to b_{kj}, there must be *n* products equal to 1. Hence at least *n* elements of *A* must be equal to 1. Therefore, the algorithmic process needs to perform only $\sum_{i=n}^{N}\binom{n^2}{i}$ checks for solutions.

ACKNOWLEDGMENT

The authors thank Dr. Aristides Kechriniotis for his valuable comments about the expression of the sum $\sum_{i=0}^{N}\binom{n^2}{i}$.

REFERENCES

1. R. Ameri, I. G. Rosenberg, “Congruences of Multialgebras”, J. Mult.-Valued Logic Soft Comput.,10 (2009), pp. 1–12.
2. R. Ameri, M. Amiri-Bideshki, A. Borumand Saeid, Š. Hošková-Mayerová, “Prime filters of hyperlattices”, An. Stiint. Univ. “Ovidius” Constanta, Ser. Mat. **24**(2), (2016) pp. 15-26.
3. J. Chvalina, “Commutative hypergroups in the sense of Marty and ordered sets”, Proceedings of the Summer School on General Algebra and Ordered Sets 1994, Olomouc (Czech Republic), pp. 19-30 (1994).
4. J. Chvalina and Š. Hošková-Mayerová, “General ω-hyperstructures and certain applications of those”, Ratio Math. **23**, (2012) pp. 3-20
5. J. Chvalina, Š. Hošková-Mayerová, A. Deghan Nezhad, “General Actions of Hypergroups and Some Applications“, An. Stiint. Univ. “Ovidius” Constanta, Ser. Mat. **21**(1), 2013, pp. 59-82.
6. P. Corsini, “Binary relations and hypergroupoids”, Ital. J. Pure Appl. Math. **7** (2000), pp. 11–18.
7. P. Corsini, “On the hypergroups associated with a binary relation”, Multi.-Val. Logic **5** (2000), pp. 407–419.
8. P. Corsini and V. Leoreanu, “Hypergroups and binary relations”, Algebra Universalis **43** (2000), pp. 321–330.
9. I. Cristea, “Several aspects on the hypergroups associated with n-ary relations”, An. Stiint. Univ. Ovidius Constanta, Ser. Mat. **17** (3) (2009) pp. 99–110.
10. I. Cristea, M. Jafarpour, S.S. Mousavi and A. Soleymani, “Enumeration of Rosenberg hypergroups”, Comput. Math. Appl. **60** (2010), pp. 2753-2763.
11. I. Cristea and M. Stefanescu, “Binary relations and reduced hypergroups”, Discrete Math. **308** (2008), pp. 3537–3544.
12. I. Cristea, M. Stefanescu and C. Angheluta, “About the fundamental relations defined on the hypergroupoids associated with binary relations”, European J. Combin. **32** (2011), pp. 72–81.
13. M. De Salvo and G. Lo Faro, “Hypergroups and binary relations”, Multi.-Val. Log. **8** (2002), pp. 645–657.
14. M. De Salvo and G. Lo Faro, “A new class of hypergroupoids associated to binary relations”, J. Mult.-Valued Logic Soft Comput. **9** (2003) pp. 361–375.
15. Š. Hošková-Mayerová, “Quasi-order hypergroups determinated by T-hypergroups”, Ratio Math., 32 (2017), pp. 37-44.
16. M. Jafarpour, I. Cristea, A. Tavakoli, “A method to compute the number of regular reversible Rosenberg hypergroup”, Ars Combin. 128 (2016), pp. 309–329.
17. S. Jančić-Rašović, “On hyperrings associated with L-fuzzy relations”, Mathematica Montisnigri Vol XXIV (2012), pp. 137-149
18. S. Jančić-Rašović, “On hyperrings associated with binary relations on semihypergroups”, Ital. J. Pure Appl. Math. **30**, (2013) pp. 279-288.
19. Š. Křehlík and M. Novák, “From lattices to Hv-matrices”, An. Stiint. Univ. ‘‘Ovidius’’ Constanta, Ser. Mat. 24 (3) (2016), pp. 209-222.
20. M. Kutz, “The complexity of Boolean matrixroot computation”, Theoretical Computer Science, vol. 325 (2004), pp. 373-390.
21. F. Marty, “Sur une généralisation de la notion de groupe”, Huitieme Congres des Mathématiciens Scand., Stockholm 1934, 45-59.
22. Ch. G. Masouros, C. Tsitouras and S. Voliotis, “Square Roots of Total Boolean Matrices Enumeration Issues”, Proceedings of 16th International Workshop on Systems, Signals and Image Processing (IWSSIP), 2009.
23. Ch. G. Massouros and Ch. Tsitouras, “Enumeration of hypercompositional structures defined by binary relations”, Ital. J. Pure Appl. Math. **28**, (2011) pp. 43-54.
24. M. Novák, “Some basic properties of EL-hyperstructures”, European J. Combin. **34** (2013), pp. 446–459.
25. M. Novák, “On EL-semihypergroups”, European J. Combin. **44** (B) (2015), pp. 274–286.
26. P. Račková, “Hypergroups of symmetric matrices”, Proceedings of the 10th International Congress on Algebraic Hyperstructures and Applications, Brno 2008, pp. 267-271
27. I.G. Rosenberg, “Hypergroups and join spaces determined by relations”, Ital. J. Pure Appl. Math. **4** (1998), pp. 93–101
28. Ch. Tsitouras and Ch. G. Massouros, “Enumeration of Rosenberg type Hypercompositional structures defined by binary relations”, European J. Combin., **33** (1) (2012), pp. 1777–1786.