J Indian Inst. Sci., May–June 1991, **71**, 271–275.

Short Communication

Square root of the Boolean matrix $J-I$

K. Raghavan
Department of Mathematics, National College, Tiruchirapalli 620 001, India.

Received on December 5, 1990; Revised on February 6, 1991.

Abstract

Kim (*Boolean matrix theory and applications*, 1982, Marcel Dekker) studied the square root of a Boolean matrix $J-I$ and stated the necessary and sufficient conditions for its existence. In this paper, the actual square root is found out if the order $J-I$ is $p \geqslant 7$ where p is a prime number of the form $4k+3$, $k \geqslant 1$. A more general case is also studied if the order is $2p+2$.

Key words: Quadratic residue mod p Boolean matrix, ith row set S_i, and the jth column set S'_j.

1. Introduction

We assume familiarity with the concept of Boolean algebra. In the next section, we introduce a quadratic residue mod p, matrix and in the last section we examine the actual square root of $J-I$. We follow the definitions given by Smeds[1].

2. Quadratic residue notation

Let p be a prime number of the form $4k+3$ and $k \geqslant 1$. The numbers $1^2, 2^2, \ldots, ((p-1)/2)^2$ reduced to mod p are called quadratic residue or simply residue and are written as q_i, $1 \leqslant i \leqslant ((p-1)/2)$.

Construction of the matrix Q_p is based on residues on $GF(p)$ and $Q_p = (q_{ij})_{p \times p}$. We describe its entries in terms of the symbol x which is defined on the elements of $GF(p)$ as follows

$$\chi(0) = 0;$$

$$\chi(i) = 1 \quad \text{if } i \text{ is a residue;}$$

$$= 0 \quad \text{if } i \text{ is non-residue.}$$

Let $q_{ij} = \chi(j-i)$. As an example we write Q_7

	0	1	2	3	4	5	6
0	0	1	1	0	1	0	0
1	0	0	1	1	0	1	0
2	0	0	0	1	1	0	1
3	1	0	0	0	1	1	0
4	0	1	0	0	0	1	1
5	1	0	1	0	0	0	1
6	1	1	0	1	0	0	0

Each row except the first is a cyclic shift of the previous row as $q_{ij} = q_{i+1,j+1}$, addition in $i+1, j+1$ being taken over modulo p.

Definition 1. ith row set S_i. For the ith row R_i of Q the set S_i, $0 \leqslant i \leqslant p-1$ is defined as $S_i = \{j : q_{ij} = 1\}$ and in the above case Q_7, $S_5 = \{0, 2, 6\}$.

Definition 2. jth column set S'_j. For the jth column C_j of Q the set S'_j, $0 \leqslant j \leqslant p-1$ is defined as $S'_j = \{i : q_{ij} = 1\}$. For Q_7, $S'_5 = \{1, 3, 4\}$.

Theorem 1. If q_i, $1 \leqslant i \leqslant (p-1)/2$ are residues mod p, $p - q_i$ are non-residues.

Proof: Since no prime number of the form $4k+3$ can be written as sum of two squares[2] the result follows.

The above theorem is restated as follows:

Theorem 2. For the matrix Q_p

(i) $q_{ij} = 0$ if $i = j$;

(ii) at least one q_{ij}, q_{ji} is zero for each i, j.

Theorem 3. The set S_{i+k} can be set from S_i by adding k to every element of S_i (addition is done over modulo p), $1 \leqslant k \leqslant p-1$.

Proof: If j belongs to S_i, $q_{ij} = 1$, $q_{i+k,j+k} = 1$ as $\psi(j+k, i+k) = 1$, which implies $j+k$ belongs to S_{i+k}.

Theorem 4. The sets $\{i\}$, S_i and S'_j are

(i) disjoint if $i = j$;

(ii) the latter two sets have at least one common element if $i \neq j$.

Proof: The result (i) is true for $i = 0$ as S_0 contains residues and S'_0 contains non-residues. If equal increment k is given to each member of the sets, we get the sets $\{k\}$, S_{i+k} and S'_{i+k}. These three sets are disjoint as $\{0\}$, S_0 and S'_0 are disjoint. To prove the result (ii), assume that there exists no common element between the sets S_i and S'_j. Hence, S_i and the set $\{j\}$ U S_j will have a common element as $\{j\}$ U S_j is the complement of S'_j. As $i \neq j$, i belongs to $\{j\} U S_j$ and j belongs to S_i. Hence, $q_{ij} = 1$ and $q_{ji} = 1$ which is a contradiction.

Considering the case Q_7 we give below the sets $\{i\} = \{j\}$, S_i and S'_j

$\{i\}$	S_i	S'_j
0	1, 2, 4	3, 5, 6
1	2, 3, 5	0, 4, 6
2	3, 4, 6	0, 1, 5
3	0, 4, 5	1, 2, 6
4	1, 5, 6	0, 2, 3
5	0, 2, 6	1, 3, 4
6	0, 1, 3	2, 4, 5

3. Main result

After the survey of basic principles of the quadratic residue matrix Q_p, we now introduce Q_p as a quadratic residue Boolean matrix. The definition given below establishes a link between Q_p and corresponding Boolean matrix.

Definition 3. By a Boolean matrix we mean matrix over $\{0, 1\}$ and arithmetic operations on the elements of the matrix are Boolean operations.

Definition 4. A square matrix Q is called a square root of B if $Q^2 = B$. Defined by the Boolean rules

$$0 + 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 0 = 0$$

$$1 + 0 = 0 + 1 = 1 + 1 = 1 \cdot 1 = 1.$$

Theorem 5. For a quadratic residue Boolean matrix Q_p

$$\text{(i)}\, R_i \cdot C_j = 0 \quad \text{if } i = j$$

$$\text{(ii)}\, R_i \cdot C_j = 1 \quad \text{if } i \neq j$$

where R_i and C_j are the ith row and jth column of Q_p and the dots represent the scalar product.

Proof: If $i = j$, $R_i \cdot C_j = \Sigma_{k=0}^{p-1} q_{ik} \cdot q_{ki}$ which is equal to zero by theorem 1. If $i \neq j$, let the common element of S_i and S'_j be r. Then $q_{ir} = q_{rj} = 1$. Hence, $R_i\ C_j = \Sigma_{k=0}^{p-1} q_{ik} \cdot q_{ij}$ which is equal to one as $q_{ir} \cdot q_{rj} = 1$.

Theorem 6. If J is a square matrix of order p with all entries 1, then Q_p is the square root of $(J-I)_p$.

Proof: Follows from theorem 5.

Kim[3] studied the nature of the necessary and sufficient conditions for the existence of the square root of $J-I$ and established the following theorem.

The Boolean matrix $J-I$ has a square root if and only if its dimension is at least 7 or is 1.

The author has found out the exact square root, when the dimension is a prime p of the form $4k+3$ $K \geqslant 1$ or when the dimension is $2(p+1)$, $p=4k+3$ $K \geqslant 1$.

The proof of the above theorem given by Kim runs as follows.

Let Q be a square root of $J-I$ of dimension less than 7. Then all diagonal entries of Q are zero and at least one of q_{ij}, q_{ji} is zero for each i, j and thus for each i the three sets $\{i\}$, $\{j: q_{ij}=1\}$ and $\{j: q_{ji}=1\}$ are disjoint. So one of the latter two sets contains at most two elements. By possibly transposing Q, assume the third set has at most two elements.

If $\{j: q_{ji}=1\}=\{a,b\}$ then $q_{ai}=1$ and $q_{ji}=0$ for $j \neq a, b$. Moreover, $i \neq a$ and $i \neq b$ since all diagonal entries are zero. Since $Q^2=j-I$, we have $\Sigma q_{ax}q_{xi}=1$. But the only non-zero term of this sum is $q_{ab}q_{bi}$. Thus, $q_{ab}=1$. Also $\Sigma q_{bx}q_{xi}=1$. Its only non-zero term is $q_{ba}q_{ab}$. Thus $q_{ab}=q_{ba}=1$. But this implies $q_{aa}^{(2)}=1$ which is false. Likewise, the case $\{j: q_{ij}=1\}=\{a\}$ and is equal to 0 is impossible, unless the dimension is 1. Kim studies the cases when n is odd and at least 9 and when n is even and at least 12.

Theorem 7. Let $l=(l_i)_{i=1}^p$ be a p elemental frame of order $1 \times p$ of all 1*s* and $h=(h_i)_{i=1}^p$ is a p elemental frame of order $1 \times p$ of all 0s. The Boolean matrix $Q_{2(p+1)}$ is a square root of the matrix $(J-I)_{2(p+1)}$ where p is a prime number of the form $4k+3$, $k \geqslant 1$.

Proof: $Q_{(p+1)}$ is defined as follows

$$\left[\begin{array}{c|c|c|c} 0 & l & h & 0 \\ \hline h^T & Q_p & Q_p & l^T \\ \hline l^T & Q_p & Q_p & h^T \\ \hline 0 & h & l & 0 \end{array}\right]$$

where the top and bottom diagonal blocks are 1×1, the edge blocks are p elemental frame, entirely 1 or entirely 0 as indicated and the inner four blocks are quadratic residue mod p (Boolean). By applying theorem 6 we get the result.

Corollary

$$\left[\begin{array}{c|c} Q_p & Q_p \\ \hline Q_p & Q_p \end{array}\right] \quad \text{is a square root of } (J-I)_{2p}.$$

4. Application of the Boolean matrix Q_p

In a Q_p where $p+1=2^n$, where n is an integer, replace all 0*s* by -1 and call the new matrix as Q'_p. Insert Q'_p in a frame l_p of all 1*s* row vector of order $1 \times p$, l_p^T and an edge diagonal block of order 1×1 containing 1. The matrix Q_p'' so formed is a Hadamard matrix and has many applications[4]. The figure given below will explain Q_p''.

$$Q_p'' = \left[\begin{array}{c|c} 1 & l_p \\ \hline l_p^T & Q_p' \end{array}\right].$$

References

1. SMEDS, P. A. Line digraphs and Moore-Penrose inverse, *Linear Algebra Applic.*, 1981, **36**, 165–172.
2. HERSTEIN, I. N. *Topics in algebra*, 1983, Vikas Publishing Co., Madras.
3. KIM, K. H. *Boolean matrix theory and applications*, 1982, Marcel Dekker.
4. MCWILLIAMS, F. J. AND SLOANE, N. J. A. *The theory of error correcting codes*, 1978, North-Holland.