

Canonical forms under similarity for involutory matrices over the ring of integers modulo 2^m

Chen Xi

Department of Computer Science and Technology, Xi'an Jiaotong University,

Xi'an, Shaanxi, China

Abstract

Involutory matrices are of great importance in matrix theory and algebraic cryptography. This paper is concerned with involutory matrices over Z_2^m (the ring of integers modulo 2^m). We use the straightforward way to establish the canonical forms under similarity for involutory matrices over Z_2^m and reduce the canonical forms into the very simple structure. By the definite procedure presented in the paper, an arbitrary involutory matrix over Z_2^m can be easily transformed into one of the canonical matrices.

AMS classification: 15A33; 15A21

Keywords: involutory matrix; the ring of integers modulo 2^m ; canonical form under similarity

1. Introduction

A square matrix A is called involutory matrix if $A^2=I$. In particular A is an involutory matrix over the ring Z_k (the ring of integers modulo k) if $A^2 \equiv I \pmod{k}$. The construction of involutory matrices is a classical mathematical problem with applications in many areas of mathematics, especially in algebraic cryptography. (see [11], [12]) The involutory matrices over finite field have been investigated by Hodges [1]. Reiner [3] and Brawley [4] determined all the involutory matrices over the ring Z_p^m , where p is an odd prime. In [5], [6], Levine and Korfhage have also made studies of involutory matrices over residue class rings of integers and obtained the formula to calculate the numbers of these involutory matrices. In this work, we use the straightforward way based on similar transformation to prove that the involutory matrices of any order over the ring Z_2^m are similar to the matrices with the very simple structure. The matrices with the simple structure called canonical form under similarity can be represented as

$$(I + 2^{m-1}F) \oplus (-I + 2^{m-1}F') \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \dots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where matrices F, F' are in the well known rational canonical form of matrices over the field Z_2 .

2. Canonical forms under similarity for involutory matrices over the ring of Z_2^m

Let $\varphi : Z_2^m \rightarrow Z_2$ be a homomorphism. $\forall a \in Z_2^m$, if a is an odd number $a^\varphi=1$, otherwise $a^\varphi=0$. For involutory matrix A of order n over Z_2^m , H is the homomorphic image of A ($h_{ij} = a_{ij}^\varphi$). Certainly H is an involutory matrix over the field Z_2 . It is well known that there exists an invertible matrix P over the field Z_2 ,

$$P^{-1}HP = H' = \text{diag}(I_r, E_1, \dots, E_t) \quad \text{where } E_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (1 \leq i \leq t) \quad r + 2t = n.$$

P is also an invertible matrix over Z_2^m , so

E-mail address: chenxi@mail.xjtu.edu.cn

$$A \sim \begin{pmatrix} g_1 & & & & & & & b_{1n-1} & 0 \\ & \ddots & & & & & & b_{2n-1} & 0 \\ & & g_r & & & & & \vdots & \vdots \\ & & & g_{r+1} & & & & \vdots & \vdots \\ & & & & g_{r+2} & & & \vdots & \vdots \\ & & & & & \ddots & & b_{n-2n-1} & 0 \\ b_{n-11} & b_{n-12} & \cdots & \cdots & \cdots & & b_{n-1n-2} & b_{n-1n-1} & g_{n-1} \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 & g_n & b_{nn} \end{pmatrix}.$$

Since the matrix above is an involutory matrix, by the dot product of i th row and n th column, we obtain $b_{in-1}g_{n-1} \equiv 0 \pmod{2^m}$ ($1 \leq i \leq n-2$) and similarly $g_n b_{n-1j} \equiv 0 \pmod{2^m}$ ($1 \leq j \leq n-2$). g_{n-1}, g_n are odd numbers, so $b_{in-1} \equiv 0 \pmod{2^m}$ and $b_{n-1j} \equiv 0 \pmod{2^m}$. Hence

$$A \sim \begin{pmatrix} g_1 & & & & & & & 0 & 0 \\ & \ddots & & & & & & 0 & 0 \\ & & g_r & & & & & \vdots & \vdots \\ & & & g_{r+1} & & & & \vdots & \vdots \\ & & & & g_{r+2} & & & \vdots & \vdots \\ & & & & & \ddots & & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & & 0 & b_{n-1n-1} & g_{n-1} \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 & g_n & b_{nn} \end{pmatrix}.$$

Perform the similar transformations successively, finally A is similar to

$$\begin{pmatrix} g_1 & b_{12} & \cdots & b_{1r} \\ b_{21} & g_2 & \cdots & b_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \cdots & g_r \end{pmatrix} \oplus \begin{pmatrix} b_{r+1r+1} & g_{r+1} \\ g_{r+2} & b_{r+2r+2} \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} b_{r+1r+1} & g_{r+1} \\ g_{r+2} & b_{r+2r+2} \end{pmatrix},$$

where all the diagonal blocks are involutory matrices. It is clear that the diagonal block of the form

$$\begin{pmatrix} b & g \\ g' & b' \end{pmatrix} \text{ is similar to } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$
 Therefore

$$A \sim \begin{pmatrix} g_1 & b_{12} & \cdots & b_{1r} \\ b_{21} & g_2 & \cdots & b_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & \cdots & \cdots & g_r \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad \square$$

Theorem 2. *The involutory matrix of order n*

$$A_n = \begin{pmatrix} g_1 & b_{12} & \cdots & b_{1n} \\ b_{21} & g_2 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & \cdots & \cdots & g_n \end{pmatrix}$$

over the ring Z_2^m is similar to the matrix

$$\begin{pmatrix} g'_1 & k & \cdots & k & k \\ k & g'_2 & \cdots & k & k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k & k & \cdots & g'_{n-1} & k \\ k & k & \cdots & k & g'_n \end{pmatrix}.$$

k denotes 0 or 2^{m-1} , $g'_i (1 \leq i \leq n)$ is ± 1 or $2^{m-1} \pm 1$.

Proof. If $m=2$, since $b_{ij}=0$ or 2, $g_i=1$ or 3, A_n itself is

$$\begin{pmatrix} g'_1 & k & \cdots & k & k \\ k & g'_2 & \cdots & k & k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k & k & \cdots & g'_{n-1} & k \\ k & k & \cdots & k & g'_n \end{pmatrix}.$$

When $m \geq 3$, we use the mathematical induction to prove theorem 2.

At first, we prove that any 2×2 involutory matrix A_2 of the form

$$\begin{pmatrix} g_1 & b_{12} \\ b_{21} & g_2 \end{pmatrix}$$

is similar to

$$\begin{pmatrix} g'_1 & k \\ k & g'_2 \end{pmatrix}.$$

Suppose $b_{12} \neq k$, perform the similar transformation

$$\begin{pmatrix} g_1 & b_{12} \\ b_{21} & g_2 \end{pmatrix} \xrightarrow{\frac{c_2+c_1(-l)}{b_2+b_1(-l)}} \begin{pmatrix} g_1+b_{21}l & b_{12}+(g_2-g_1)l-b_{21}l^2 \\ b_{21} & g_2-b_{21}l \end{pmatrix}$$

Let $f(l) = b_{12} + (g_2 - g_1)l - b_{21}l^2$. It is easy to verify that the coefficients of the polynomial $f(l)$ can assure that the quadratic congruence equation $f(l) \equiv 0 \pmod{2^m}$ has solution (see [17]), i.e.

$$\begin{pmatrix} g_1 & b_{12} \\ b_{21} & g_2 \end{pmatrix} \sim \begin{pmatrix} g'_1 & 0 \\ b_{21} & g'_2 \end{pmatrix}, \quad g'_1 = g_1 + b_{21}l, \quad g'_2 = g_2 - b_{21}l$$

Perform the similar transformation again

$$\begin{pmatrix} g'_1 & 0 \\ b_{21} & g'_2 \end{pmatrix} \xrightarrow{\frac{c_1+c_2 l}{b_2+b_1(-l)}} \begin{pmatrix} g'_1 & 0 \\ b_{21}+(g'_2-g'_1)l & g'_2 \end{pmatrix}$$

The congruence equation $b_{21} + (g'_2 - g'_1)l = b_{21} + (g_2 - g_1)l - 2b_{21}l^2 \equiv 0 \pmod{2^m}$ has solution. So

$$A_2 \sim \begin{pmatrix} g'_1 & 0 \\ 0 & g'_2 \end{pmatrix}.$$

If $b_{21} \neq k$, similarly we can transform A_2 into

$$\begin{pmatrix} g'_1 & 0 \\ 0 & g'_2 \end{pmatrix}$$

Consequently, A_2 is similar to

$$\begin{pmatrix} g'_1 & k \\ k & g'_2 \end{pmatrix} \quad (k = 0 \text{ or } 2^{m-1})$$

Since the matrix above is an involutory matrix, $(g'_1)^2 \equiv 1 \pmod{2^m}$ and $(g'_2)^2 \equiv 1 \pmod{2^m}$. So $g'_1, g'_2 = \pm 1$ or $2^{m-1} \pm 1$.

Now we assume (as the hypothesis of the induction) that $(n-1) \times (n-1)$ involutory matrix of the form

$$\begin{pmatrix} g_1 & b_{12} & \cdots & b_{1n-1} \\ b_{21} & g_2 & \cdots & b_{2n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-11} & b_{n-12} & \cdots & g_{n-1} \end{pmatrix}$$

is similar to

$$\begin{pmatrix} g'_1 & k & \cdots & k \\ k & g'_2 & \cdots & k \\ \vdots & \vdots & \ddots & \vdots \\ k & k & \cdots & g'_{n-1} \end{pmatrix}.$$

We prove the law still holds for $n \times n$ involutory matrix.

We use $R(a)$ to denote the number of factor 2 in an arbitrary number a .

Suppose

$$A_n = \begin{pmatrix} g_1 & b_{12} & \cdots & b_{1n-1} & b_{1n} \\ b_{21} & g_2 & \cdots & b_{2n-1} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n-11} & b_{n-12} & \cdots & g_{n-1} & b_{n-1n} \\ b_{n1} & b_{n2} & \cdots & b_{nn-1} & g_n \end{pmatrix}$$

Through the interchange of i th, j th row and i th, j th column at the same time successively, we arrange b_{1r} in the order that $R(b_{1i}) \leq R(b_{1j})$ when $i < j$. If $b_{1r} = 0$, it will be put at the end of the first row.

$$A_n \sim \begin{pmatrix} g_1 & b_{12} & \cdots & b_{1n-1} & b_{1n} \\ b_{21} & g_2 & \cdots & b_{2n-1} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n-11} & b_{n-12} & \cdots & g_{n-1} & b_{n-1n} \\ b_{n1} & b_{n2} & \cdots & b_{nn-1} & g_n \end{pmatrix} \quad R(b_{12}) \leq R(b_{13}) \leq \dots \leq R(b_{1n})$$

If $b_{12} = k$, then b_{1j} ($3 \leq j \leq n$) is k . Otherwise suppose $b_{12} = 2^q s$, ($1 \leq q \leq m-2$). s and s' denote arbitrary odd number in the paper. Since b_{12} divides b_{1j} over the ring Z_2^m . Perform the similar transformations until all the entries in the first row become zero except for g_1 , b_{12} and the parity of each entry remains the same. Then

$$A_n \sim \begin{pmatrix} g_1 & b_{12} & 0 & \cdots & 0 \\ b_{21} & g_2 & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix}.$$

Now perform the similar transformation to make b_{21} be zero.

$$\begin{pmatrix} g_1 & b_{12} & 0 & \cdots & 0 \\ b_{21} & g_2 & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix} \xrightarrow{\begin{matrix} c_1 + c_2(l) \\ r_2 + r_1(-l) \end{matrix}} \begin{pmatrix} g_1 + b_{12}l & b_{12} & 0 & \cdots & 0 \\ b_{21} + (g_2 - g_1)l - b_{12}l^2 & g_2 - b_{12}l & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix}$$

Let D be the matrix above. We know that $b_{21} + (g_2 - g_1)l - b_{12}l^2 \equiv 0 \pmod{2^m}$ has solution. Moreover, $g_1 + b_{12}l$ and $g_2 - b_{12}l$ are odd numbers. For convenience, we still use g_1 , g_2 to denote them. Perform the similar transformation.

$$D = \begin{pmatrix} g_1 & b_{12} & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix} \xrightarrow{\begin{matrix} r_1 + r_2(h) \\ c_2 + c_1(-h) \end{matrix}} \begin{pmatrix} g_1 & b_{12} + (g_2 - g_1)h & b_{23}h & \cdots & b_{2n}h \\ 0 & g_2 & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix}$$

Since D is an involutory matrix and we are given that $b_{12} = 2^q s$, ($1 \leq q \leq m-2$). By the dot product of the first row and the second column, we obtain that

$$\sum_{i=1}^n d_{1i} d_{i2} = b_{12}(g_1 + g_2) \equiv 0 \pmod{2^m}$$

So $(g_1 + g_2) \equiv 0 \pmod{2^{m-q}}$, ($m-q \geq 2$), thus $g_2 - g_1 = g_2 + g_1 - 2g_1 = 2s'$. Let h in the above similar transformation be $-2^{q-1}s(s')^{-1}$, ($R(h) = q-1$). It is easy to see that $b_{12} + (g_2 - g_1)h \equiv 0 \pmod{2^m}$. Now by the dot product of the first row and j th ($3 \leq j \leq n$) column of the matrix D , we obtain that

$$\sum_{i=1}^n d_{1i} d_{ij} = b_{12} b_{2j} \equiv 0 \pmod{2^m}$$

Then $b_{2j} \equiv 0 \pmod{2^{m-q}}$, i.e. $R(b_{2j}) \geq (m-q)$. Hence $R(b_{2j}h) = R(b_{2j}) + R(h) \geq m-1$, i.e. $b_{2j}h = k$. ($3 \leq j \leq n$). Consequently

$$A_n \sim \begin{pmatrix} g_1 & 0 & k & \cdots & k \\ 0 & g_2 & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix}.$$

Therefore, no matter b_{12} in the matrix A_n is k or not, A_n is always similar to

$$\begin{pmatrix} g_1 & k & k & \cdots & k \\ b_{21} & g_2 & \cdots & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & \cdots & g_n \end{pmatrix} = \begin{pmatrix} g_1 & C \\ B & A_{n-1} \end{pmatrix}.$$

$$B = (b_{21}, b_{31}, \dots, b_{n1})^T, C = (k, k, \dots, k), A_{n-1} = \begin{pmatrix} g_2 & b_{23} & \cdots & b_{2n} \\ b_{32} & g_3 & \cdots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \cdots & g_n \end{pmatrix}.$$

Since over the ring Z_2^m

$$\begin{pmatrix} g_1 & C \\ B & A_{n-1} \end{pmatrix}^2 = I, CB=0 \text{ and } BC \text{ is the zero matrix of order } n-1.$$

So A_{n-1} is the $(n-1) \times (n-1)$ involutory matrix. According to the inductive hypothesis, there exists an invertible matrix Q ,

$$Q^{-1}A_{n-1}Q = \begin{pmatrix} g'_2 & k & \cdots & k & k \\ k & g'_3 & \cdots & k & k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k & k & \cdots & g'_{n-1} & k \\ k & k & \cdots & k & g'_n \end{pmatrix} \quad g'_i = \pm 1 \text{ or } 2^{m-1} \pm 1 \quad (2 \leq i \leq n)$$

$$A_n \sim \begin{pmatrix} 1 & & & & \\ & Q^{-1} & & & \\ & & \begin{pmatrix} g_1 & C \\ B & A_{n-1} \end{pmatrix} & & \\ & & & \begin{pmatrix} 1 & \\ & Q \end{pmatrix} & \\ & & & & \begin{pmatrix} g_1 & CQ \\ Q^{-1}B & Q^{-1}A_{n-1}Q \end{pmatrix} \end{pmatrix}$$

CQ is the $1 \times (n-1)$ matrix with entries k and $Q^{-1}B$ is the $(n-1) \times 1$ matrix with even numbers.

$$A_n \sim \begin{pmatrix} g_1 & k & \cdots & k & k \\ b_{21} & g'_2 & \cdots & k & k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n-11} & k & \cdots & g'_{n-1} & k \\ b_{n1} & k & \cdots & k & g'_n \end{pmatrix}$$

By the dot product of the first row and the second column of the matrix above, we obtain $g_1^2 \equiv 1 \pmod{2^m}$, so $g_1 = \pm 1$ or $2^{m-1} \pm 1$. As before we use g'_1 to denote it. For any b_{i1} , ($2 \leq i \leq n$), if $b_{i1} \neq k$, transform b_{i1} into zero as follows.

$$\begin{pmatrix} g'_1 & k & \cdots & k & \cdots & k \\ b_{21} & g'_2 & \cdots & k & \cdots & k \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ b_{i1} & k & \cdots & g'_i & \cdots & k \\ \vdots & \vdots & & \ddots & & \vdots \\ b_{n1} & k & \cdots & \cdots & \cdots & g'_n \end{pmatrix} \xrightarrow{\begin{matrix} c_1 + c_i(l) \\ r_i + r_1(-l) \end{matrix}} \begin{pmatrix} g'_1 + kl & k & \cdots & k & \cdots & k \\ b_{21} + kl & g'_2 & \cdots & k & \cdots & k \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ b_{i1} + (g'_i - g'_1)l - kl^2 & k & \cdots & g'_i - kl & \cdots & k \\ \vdots & \vdots & & \ddots & & \vdots \\ b_{n1} + kl & k & \cdots & \cdots & \cdots & g'_n \end{pmatrix}$$

We know that $b_{i1} + (g'_i - g'_1)l - kl^2 \equiv 0 \pmod{2^m}$ has solution. Moreover, $g'_1 + kl$, $g'_i - kl$ are still equal to ± 1 or $2^{m-1} \pm 1$. Now, b_{i1} has been transformed into zero. Perform the similar transformations until all the even numbers in the first column become k .

Consequently, any $n \times n$ involutory matrix of the form

$$\begin{pmatrix} g_1 & b_{12} & \cdots & b_{1n-1} & b_{1n} \\ b_{21} & g_2 & \cdots & b_{2n-1} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n-11} & b_{n-12} & \cdots & g_{n-1} & b_{n-1n} \\ b_{n1} & b_{n2} & \cdots & b_{nn-1} & g_n \end{pmatrix}$$

is similar to

$$\begin{pmatrix} g'_1 & k & \cdots & k & k \\ k & g'_2 & \cdots & k & k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k & k & \cdots & g'_{n-1} & k \\ k & k & \cdots & k & g'_n \end{pmatrix} \quad (k=0 \text{ or } 2^{m-1}, g'_i = \pm 1 \text{ or } 2^{m-1} \pm 1). \quad \square$$

Theorem 3. The involutory matrix A over the ring Z_2^m of the form

$$\begin{pmatrix} g_1 & k & \cdots & k & k \\ k & g_2 & \cdots & k & k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k & k & \cdots & g_{n-1} & k \\ k & k & \cdots & k & g_n \end{pmatrix} \quad (k=0 \text{ or } 2^{m-1}, g_i = \pm 1 \text{ or } 2^{m-1} \pm 1)$$

is similar to the direct sum of $(I + 2^{m-1}F)$ and $(-I + 2^{m-1}F')$ where F, F' are matrices in the rational canonical form of matrices over the field Z_2 .

Proof. If $m=2$, the diagonal entries only have 2 values, 1 and $3=2^{2-1}+1$. Interchange i th, j th row and i th, j th column at the same time successively, then

$$A \sim \begin{pmatrix} 1 & k & \cdots & \cdots & \cdots & k \\ k & \ddots & & & & \vdots \\ \vdots & & 1 & & & \vdots \\ \vdots & & & 2^{m-1}+1 & & \vdots \\ \vdots & & & & \ddots & \vdots \\ k & \cdots & \cdots & \cdots & k & 2^{m-1}+1 \end{pmatrix} = (I + 2^{m-1}F)$$

When $m \geq 3$, after the similar interchange,

$$A \sim \left(\begin{array}{cccccc|cccccc} 1 & k & \cdots & \cdots & \cdots & k & & & & & & \\ k & \ddots & & & & \vdots & & & & & & \\ \vdots & & 1 & & & \vdots & & & & & & \\ \vdots & & & 2^{m-1}+1 & & \vdots & & & & & & \\ \vdots & & & & \ddots & k & & & & & & \\ k & \cdots & \cdots & \cdots & k & 2^{m-1}+1 & & & & & & \\ \hline & & & & & & k & & & & & \\ & & & & & & & 2^{m-1}-1 & k & \cdots & \cdots & k \\ & & & & & & & k & \ddots & & & \vdots \\ & & & & & & & \vdots & & 2^{m-1}-1 & & \vdots \\ & & & & & & & \vdots & & & -1 & \vdots \\ & & & & & & & \vdots & & & & \ddots & k \\ & & & & & & & k & \cdots & \cdots & \cdots & k & -1 \end{array} \right) = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

If the entry b_{ij} in A_{12} is unequal to zero, i.e. $b_{ij}=2^{m-1}$. Perform the similar transformation as follows.

$$\begin{pmatrix} 1 & k & \cdots & \cdots & \cdots & \cdots & k \\ k & \ddots & & & & & \vdots \\ \vdots & & u & \cdots & b_{ij} & & \vdots \\ \vdots & & & \ddots & \vdots & & \vdots \\ \vdots & & & & v & & \vdots \\ \vdots & & & & & \ddots & k \\ k & \cdots & \cdots & \cdots & \cdots & k & -1 \end{pmatrix} \xrightarrow{\begin{matrix} c_j+c_i(l) \\ r_i+r_j(-l) \end{matrix}} \begin{pmatrix} 1 & k & \cdots & \cdots & \cdots & \cdots & k \\ k & \ddots & & & & & \vdots \\ \vdots & & u-kl & \cdots & b_{ij}+(u-v)l-kl^2 & & \vdots \\ \vdots & & & \ddots & \vdots & & \vdots \\ \vdots & & & & v+kl & & \vdots \\ \vdots & & & & & \ddots & k \\ k & \cdots & \cdots & \cdots & \cdots & k & -1 \end{pmatrix}$$

$u=1$ or $2^{m-1}+1$, $v=-1$ or $2^{m-1}-1$, $u-v=2s$. Let $l=2^{m-2}$, then $b_{ij}+(u-v)l-kl^2 \equiv 0 \pmod{2^m}$. Moreover, $u-kl \equiv u \pmod{2^m}$, $v-kl \equiv v \pmod{2^m}$. Therefore, we can make A_{12} and A_{21} become the zero matrices. So

$$A \sim \begin{pmatrix} 1 & k & \cdots & \cdots & \cdots & k \\ k & \ddots & & & & \vdots \\ \vdots & & 1 & & & \vdots \\ \vdots & & & 2^{m-1}+1 & & \vdots \\ \vdots & & & & \ddots & \vdots \\ k & \cdots & \cdots & \cdots & k & 2^{m-1}+1 \end{pmatrix} \oplus \begin{pmatrix} 2^{m-1}-1 & k & \cdots & \cdots & \cdots & k \\ k & \ddots & & & & \vdots \\ \vdots & & 2^{m-1}-1 & & & \vdots \\ \vdots & & & -1 & & \vdots \\ \vdots & & & & \ddots & \vdots \\ k & \cdots & \cdots & \cdots & k & -1 \end{pmatrix} = (I+2^{m-1}F) \oplus (-I+2^{m-1}F')$$

where F, F' are the matrices over the field Z_2 . (Note: F, F' are not necessarily involutory matrices).

If F, F' are in the rational canonical form of the matrices over the field Z_2 , any involutory matrix over the ring Z_2^m is similar to one and only one matrix which has a representation as $(I+2^{m-1}F) \oplus (-I+2^{m-1}F')$. \square

3. Conclusion

According the theorems 1, 2, 3, we know that any $n \times n$ involutory matrix over the ring Z_2^m is similar to

$$\begin{aligned} m=2 & (I+2^{m-1}F) \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ m \geq 3 & (I+2^{m-1}F) \oplus (-I+2^{m-1}F') \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

where matrices F, F' are in the rational canonical form of matrices over the field Z_2 . The matrices with very simple structure above are all dissimilar and any involutory matrix over Z_2^m is similar to one and only one of them, so these matrices are the canonical forms under similarity for involutory matrices over Z_2^m . Since 2 and power of 2 are of especial importance in computer science, the result of this paper has its own cryptographic advantage. We will present these applications in a further paper.

4. Example

As an illustration, now we show how to obtain the 3×3 canonical form under similarity for involutory matrices over the ring Z_8 , i.e. $m=3$.

1×1 rational canonical matrices over Z_2 are

$$(0) \quad (1)$$

2 in total.

2×2 rational canonical matrices over Z_2 are

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

6 in total.

3×3 rational canonical matrices over Z_2 are

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

14 in total.

For an 3×3 involutory matrix A over Z_8

- . If $A \sim (I_{3 \times 3} + 2^{m-1} F_{3 \times 3})$, there are 14 canonical matrices.
- . If $A \sim (-I_{3 \times 3} + 2^{m-1} F'_{3 \times 3})$, there are 14 canonical matrices.
- . If $A \sim (I_{1 \times 1} + 2^{m-1} F_{1 \times 1}) \oplus (-I_{2 \times 2} + 2^{m-1} F'_{2 \times 2})$, there are $2 \times 6 = 12$ canonical matrices.
- . If $A \sim (I_{2 \times 2} + 2^{m-1} F_{2 \times 2}) \oplus (-I_{1 \times 1} + 2^{m-1} F'_{1 \times 1})$, there are $2 \times 6 = 12$ canonical matrices.
- . If $A \sim (I_{1 \times 1} + 2^{m-1} F_{1 \times 1}) \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, there are 2 canonical matrices.
- . If $A \sim (-I_{1 \times 1} + 2^{m-1} F'_{1 \times 1}) \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, there are 2 canonical matrices.

Consequently, the number of 3×3 canonical involutory matrices under similarity on Z_8 is 56 in total.

Acknowledgement

The author wishes to thank Dr. J R Wang, Professor of the Department of Mathematical Sciences of Xi'an Jiaotong University, Dr. Yi Li, Professor and Chair of Department of Mathematics of University of Iowa and Dr. Victor Camillo, Professor of Department of Mathematics of University of Iowa for reading the paper and their useful advice and comments.

Reference

- [1] John H. Hodges, The matrix equation $X^2 - I = 0$ over a finite field, The American Mathematical Monthly. 65 (1958) 518–520.
- [2] Jack Levine, H.M.Nahikian, On the Construction of Involutory Matrices, The American Mathematical Monthly. 69 (1962) 267–272.
- [3] Irma Reiner, The Matrix Congruence $X^2 \equiv I \pmod{P^n}$, The American Mathematical Monthly. 67 (1960) 773–775.
- [4] Joel Brawley, Similar Involutory Matrices (mod P^m). The American Mathematical Monthly. 73 (1966) 499–501.
- [5] Jack Levine, Robert R. Korfhage, Automorphisms of abelian groups induced by involutory matrices, Duke Math. J., 29 (1962) 631–646.
- [6] R. R. Korfhage, Solutions of $X^2 = I$ over finite rings with unity, The American Mathematical Monthly. 75 (1968) 634–636.
- [7] Arlinghaus, F. A., Vaserstein, L. N., Hong, You, Products of Involutory Matrices Over Rings, Linear Algebra and its Appl. 229 (1995) 37–47.
- [8] Horn, Roger A., Sergeichuk, Vladimir V, Congruences of a square matrix and its transpose, Linear Algebra and its Appl. 389 (2004) 347–353.
- [9] Yongge Tian, George P.H. Styan, Rank equalities for idempotent and involutory matrices, Linear Algebra and its Appl. 335 (2001) 101–117.
- [10] Carmen Coll, Nestor Thome, Oblique projectors and group involutory matrices, Linear Algebra and its Appl. 140 (2003) 517–522.
- [11] C. S. Ballantine, Some involutory similarities, Linear and Multilinear Algebra 5 (1975) 19–23.
- [12] L. S. Hill, Concerning certain linear transformation apparatus of cryptography, The American Mathematical Monthly. 38 (1931) 135–154.
- [13] Jack Levine, Variable matrix substitution in algebraic cryptography, The American Mathematical Monthly. 65 (1958) 170–179.
- [14] Joseph J. Rotman, Advanced Modern Algebra, Prentice Hall, 2002.
- [15] Setven Roman, Advanced Linear Algebra, Springer-Verlag, New York, 1992.
- [16] I.Martin Isaacs, Algebra: A Graduate Course, Wadsworth Inc., 1994.
- [17] W. Narkiewicz, Number Theory, World Scientific Publishing Co, Singapore, 1983.