Two Congruence Classes for Symmetric Binary Matrices over $\mathbb{F}_2$

YONG-HYUK KIM
Department of Computer Science and Engineering
Kwangwoon University
Wolge-dong, Nowon-gu
Seoul, 139-701
KOREA
yhdfly@kw.ac.kr

KEOMKYO SEO
School of Mathematics
Korea Institute for Advanced Study
Cheongnyangni 2-dong, Dongdaemun-gu
Seoul, 130-722
KOREA
kseo@kias.re.kr

Abstract: We provide two congruence classes for symmetric binary matrices over a finite field of characteristic 2. We use standard methods of matrix analysis to prove directly that there exist two congruence classes. Our proof gives explicit algorithms to compute the congruence classes.

Key–Words: congruence of matrices, binary matrices, finite field of characteristic 2.

1 Introduction

We call two square matrices A and B *congruent* when there exists a nonsingular matrix Q satisfying $B = Q^tAQ$. For such A and B, we denote $A \sim_c B$. Clearly, $\sim_c$ is an equivalence relation. In [7], Gow computed the number of congruence classes for invertible matrices over finite fields. Waterhouse[9] extended the result of Gow to find the number of congruence classes where $B^{-1}B^t$ is unipotent. Recently Corbas and Williams[4, 5] have determined the sizes of congruence classes of (2×2) and (3×3) matrices over a finite field $\mathbb{F}_q$.

A matrix A is called *binary* if $A \in M_{n\times n}(\mathbb{F}_2)$. Binary matrices have been widely used to deal with the adjacency of a graph.(See [1, 2, 3]) In particular, Anderson and Feil[1] transformed the *light bulb puzzle* into the problem of solving a linear system $Ax = b$ from its graphical structure, where $A \in M_{n\times n}(\mathbb{F}_2)$ and $x, b \in \mathbb{F}_2^n$. Then the solution could be obtained by computing the inverse of A, i.e., $x = A^{-1}b$. Binary matrices are also useful for dealing with the *cut/cycle* subspace of a graph, which is a vector space over $\mathbb{F}_2$.([2]) Moreover they can be used to represent a basis change of a vector space over $\mathbb{F}_2$ in many combinatorial problems.

Define $J_n = (\mathrm{j}_{ij}) \in M_{n\times n}(\mathbb{F}_2)$ as follows:

$$\mathrm{j}_{ij} = \begin{cases} 1 & \text{if } (i - j = 1 \text{ and } i \text{ is even}) \\ & \quad \text{or } (j - i = 1 \text{ and } j \text{ is even}) \\ 0 & \text{otherwise.} \end{cases}$$

For instance, $J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $J_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, and $J_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

Let $A \in M_{n\times n}(\mathbb{F}_2)$. We assume that $A \sim_c I_k$ $(k \le n)$ means $A \sim_c \begin{pmatrix} I_k & 0 \\ 0 & O_{n-k} \end{pmatrix}$ and also $A \sim_c J_k$ $(k \le n)$ means $A \sim_c \begin{pmatrix} J_k & 0 \\ 0 & O_{n-k} \end{pmatrix}$. By the definition of J_n, one can easily see that $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \nsim_c J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

In page 171 of [8], it was proven that if $\mathbb{F}$ has characteristic two and $g(x, y)$ is a non-alternate symmetric bilinear form in a vector space V over $\mathbb{F}$, then there exists a basis of V such that the matrix of $g(x, y)$ is congruent to a symmetric diagonal matrix. In this paper, however, we deal with arbitrary symmetric binary matrices and give a classification of these matrices.

Theorem 1. *Let $A \in M_{n\times n}(\mathbb{F}_2)$ be symmetric with rank k. Then we have the following.*
(i) If every diagonal element of A is 0, then $A \sim_c J_k$ and hence k is even.
(ii) If at least one diagonal element of A is 1, then $A \sim_c I_k$.

In particular, when $n = 2$ or 3, this result is the same as [5]. As an immediate consequence, we have the following.

Corollary 1. *Let $A \in M_{n\times n}(\mathbb{Z}_2)$ be symmetric with rank k. If k is odd, then $A \sim_c I_k$.*

2 Preliminaries

We need some useful lemmas.

Lemma 1. *Let $A, B \in M_{n\times n}(\mathbb{F}_2)$. If $A \sim_c B$, then we have* $\mathrm{rank}(A) = \mathrm{rank}(B)$.

Definition 2. *Let $A \in M_{n\times n}(\mathbb{F}_2)$. Any one of the following two operations on the rows of A is called an* elementary row operation*:*
(i) interchanging any two rows of A
(ii) adding a row of A to another row.

Elementary row operations are of *type 1* or *type 2* depending on whether they are obtained by (i) or (ii). An $n \times n$ *elementary matrix* over $\mathbb{F}_2$ field is a matrix obtained by performing an elementary row operation on I_n. The elementary matrix is said to be of *type 1* or *type 2* according to whether the elementary row operation performed on I_n is a type 1 or type 2, respectively.

Lemma 3. *Suppose that $Q \in M_{n\times n}(\mathbb{F}_2)$ is a nonsingular matrix. Then Q is a product of elementary matrices, i.e., $Q = E_1E_2\cdots E_k$. So $Q^tAQ = E_k^t(\cdots(E_2^t(E_1^tAE_1)E_2)\cdots)E_k$ for any $A \in M_{n\times n}(\mathbb{F}_2)$.*

Lemma 4. $\mathrm{rank}(J_n) = 2\cdot[n/2]$, *where* [ ] *means Gauss symbol.*

Furthermore we have

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim_c \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad (1)$$

since taking $Q = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ gives $Q^tI_3Q = Q^tQ = Q^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Proposition 5. *Let $A \in M_{n\times n}(\mathbb{F}_2)$. If $A \sim_c I_k$ or $A \sim_c J_k$ for some $k \in \mathbb{N}$, then A is symmetric.*

Proof. See [6], which gives more general theorem.
On the other hand, we have the following as a criterion of symmetric binary matrices.

Lemma 6. *Let $A = (a_{ij}) \in M_{n\times n}(\mathbb{F}_2)$ be symmetric. If every diagonal element of A is 0, then $A \nsim_c I_k$ for some $k \in \mathbb{N}$. In particular, $I_n \nsim_c J_n$ for every $n \in \mathbb{N}$.*

Proof. By Lemma 3, it is enough to show that, for the elementary matrix E of each type, every diagonal element of E^tAE is 0. First we consider the elementary matrix E_1 of type 1. We may assume that E_1 interchanges row i and row j ($i < j$). Let $a_{ij} = a_{ji} = \bigstar$ ($\bigstar = 0$ or 1). Then we have

$$A = \begin{pmatrix} \ddots & & & & \\ & 0 & & \bigstar & \\ & & \ddots & & \\ & \bigstar & & 0 & \\ & & & & \ddots \end{pmatrix},$$

$$E_1 = E_1^t = \begin{pmatrix} I_{i-1} & & & & \\ & 0 & & 1 & \\ & & I_{j-i-1} & & \\ & 1 & & 0 & \\ & & & & I_{n-j} \end{pmatrix},$$

$$E_1^tA = \begin{pmatrix} I_{i-1} & & & & \\ & 0 & & 1 & \\ & & I_{j-i-1} & & \\ & 1 & & 0 & \\ & & & & I_{n-j} \end{pmatrix} \times \begin{pmatrix} \ddots & & & & \\ & 0 & & \bigstar & \\ & & \ddots & & \\ & \bigstar & & 0 & \\ & & & & \ddots \end{pmatrix}$$

$$= \begin{pmatrix} \ddots & & & & \\ & \bigstar & & 0 & \\ & & \ddots & & \\ & 0 & & \bigstar & \\ & & & & \ddots \end{pmatrix}, \text{ and}$$

$$E_1^tAE_1 = \begin{pmatrix} \ddots & & & & \\ & \bigstar & & 0 & \\ & & \ddots & & \\ & 0 & & \bigstar & \\ & & & & \ddots \end{pmatrix} \times \begin{pmatrix} I_{i-1} & & & & \\ & 0 & & 1 & \\ & & I_{j-i-1} & & \\ & 1 & & 0 & \\ & & & & I_{n-j} \end{pmatrix}$$

$$= \begin{pmatrix} \ddots & & & & \\ & 0 & & \bigstar & \\ & & \ddots & & \\ & \bigstar & & 0 & \\ & & & & \ddots \end{pmatrix}.$$

So every diagonal element of $E_1^tAE_1$ is 0. Next we consider the elementary matrix E_2 of type 2 which adds row i to row j ($i < j$). Let $a_{ij} = a_{ji} = \clubsuit$ ($\clubsuit =$

0 or 1).

$$A = \begin{pmatrix} \ddots & & & & \\ & 0 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix},$$

$$E_2 = \begin{pmatrix} I_{i-1} & & & & \\ & 1 & & 0 & \\ & & I_{j-i-1} & & \\ & 1 & & 1 & \\ & & & & I_{n-j} \end{pmatrix}, \text{ and}$$

$$E_2^t A = \begin{pmatrix} I_{i-1} & & & & \\ & 1 & & 1 & \\ & & I_{j-i-1} & & \\ & 0 & & 1 & \\ & & & & I_{n-j} \end{pmatrix} \times$$

$$\begin{pmatrix} \ddots & & & & \\ & 0 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}$$

$$= \begin{pmatrix} \ddots & & & & \\ & \clubsuit & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}.$$

Since $\clubsuit + \clubsuit = 0$, we get

$$E_2^t A E_2 = \begin{pmatrix} \ddots & & & & \\ & \clubsuit & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix} \times$$

$$\begin{pmatrix} I_{i-1} & & & & \\ & 1 & & 0 & \\ & & I_{j-i-1} & & \\ & 1 & & 1 & \\ & & & & I_{n-j} \end{pmatrix} =$$

$$\begin{pmatrix} \ddots & & & & \\ & 0 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}.$$

Hence every diagonal element of $E_2^t A E_2$ is still 0.

3 Proof of the theorem

First we show that by a sequence of elementary operations

$$A \sim_c \begin{pmatrix} I_m & & 0 \\ & J_{k-m} & \\ 0 & & O_{n-k} \end{pmatrix}, \tag{2}$$

where $k - m$ is even. To prove this, we need the following claim.

Claim 1. *A is congruent to one of the following three types:*

$$\text{Type(I)} : \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right),$$

$$\text{Type(II)} : \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right), \textit{ and}$$

$$\text{Type(III)} : \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & * & \\ 0 & 0 & & & \end{array}\right).$$

Once we prove the above claim, then by induction and applying a sequence of elementary matrices of type 1, we can obtain (2). Now we prove the claim. If all the elements of the first column of A are zero, trivially $A \sim_c$ Type(I). Otherwise, at least one element of the first column of A are one. If $a_{11} = 1$, by applying a sequence of elementary matrices of type 2, we remove the remaining 1's in the first column of A. So $A \sim_c$ Type(II). If $a_{11} = 0$, by applying an elementary matrix E_1 of type 1, we can make $a_{21} = 1$ (i.e., $(E_1^t A E_1)_{21} = 1$). Then by applying a sequence of elementary matrices of type 2, we remove the remaining 1's in the first column of A. So

$$A \sim_c \left(\begin{array}{c|cccc} 0 & 1 & 0 & \cdots & 0 \\ \hline 1 & & & & \\ 0 & & & & \\ \vdots & & & * & \\ 0 & & & & \end{array}\right).$$

Also by applying a sequence of elementary matrices of type 2 to remove 1's in the second column of A,

$$A \sim_c \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & * & \\ 0 & 0 & & & \end{array}\right)$$

$$\text{or Type(S)} := \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & * & \\ 0 & 0 & & & \end{array}\right).$$

If $A \nsim_c$ Type(S), then $A \sim_c \mathrm{Type(III)}$. In the case that $A \sim_c$ Type(S), we consider the elementary matrix E_2 of type 2 such that E_2 adds row 1 to row 2. If we apply E_2 to Type(S), i.e., E_2^t Type(S) E_2,

$$A \sim_c \text{Type(S)} \sim_c \left(\begin{array}{cc|ccc} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & * & \\ 0 & 0 & & & \end{array}\right),$$

which is Type(II). Hence the claim is proved.

If $m = 0$, then $A \sim_c \begin{pmatrix} J_k & 0 \\ 0 & O_{n-k} \end{pmatrix}$.

If $m > 0$, using the equivalence relation (1), one can get $A \sim_c \begin{pmatrix} I_k & 0 \\ 0 & O_{n-k} \end{pmatrix}$.

Hence we have

$$A \sim_c I_k \text{ or } A \sim_c J_k. \tag{3}$$

Proof of (i): By Lemma 6, $A \nsim_c I_k$. Then $A \sim_c J_k$ by (3). Moreover we have

$$\begin{aligned} k &= \mathrm{rank}(A) \\ &= \mathrm{rank}(J_k) \text{ (by Lemma 1)} \\ &= 2 \cdot [k/2] \text{ (by Lemma 4)}. \end{aligned}$$

Therefore k is even.

Proof of (ii): By Lemma 3, if the following claim is proved, then we have $A \nsim_c J_k$ since every diagonal element of J_k is 0. Therefore $A \sim_c I_k$ by (3).

Claim 2. *When at least one diagonal element of A is 1, for an elementary matrix E of each type, E^tAE also has at least one nonzero diagonal element.*

To prove the claim, we first consider an elementary matrix E_1 of type 1. As in the proof of Lemma 6, it is easy to see that the number of 1's in the diagonal part of $E_1^tAE_1$ is equal to that of A. Next we consider the elementary matrix E_2 of type 2. We may assume that E_2 adds row i to row j ($i < j$). Let $a_{ij} = a_{ji} = \clubsuit$ ($\clubsuit$ = 0 or 1). There are four cases depending on the values of a_{ii} and a_{jj} in the following.

Case (1):

$$\text{If } A = \begin{pmatrix} \ddots & & & & \\ & 0 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}, \text{ then}$$

$$E_2^tAE_2 = \begin{pmatrix} \ddots & & & & \\ & 0 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}.$$

Case (2):

$$\text{If } A = \begin{pmatrix} \ddots & & & & \\ & 1 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}, \text{ then}$$

$$E_2^tAE_2 = \begin{pmatrix} \ddots & & & & \\ & 1 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 0 & \\ & & & & \ddots \end{pmatrix}.$$

Case (3):

$$\text{If } A = \begin{pmatrix} \ddots & & & & \\ & 0 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 1 & \\ & & & & \ddots \end{pmatrix}, \text{ then}$$

$$E_2^tAE_2 = \begin{pmatrix} \ddots & & & & \\ & 1 & & 1+\clubsuit & \\ & & \ddots & & \\ & 1+\clubsuit & & 1 & \\ & & & & \ddots \end{pmatrix}.$$

Case (4):

$$\text{If } A = \begin{pmatrix} \ddots & & & & \\ & 1 & & \clubsuit & \\ & & \ddots & & \\ & \clubsuit & & 1 & \\ & & & & \ddots \end{pmatrix}, \text{ then}$$

$$E_2^t A E_2 = \begin{pmatrix} \ddots & & & & \\ & 0 & & 1+\clubsuit & \\ & & \ddots & & \\ & 1+\clubsuit & & 1 & \\ & & & & \ddots \end{pmatrix}.$$

For all the cases, at least one diagonal element of $E_2^t A E_2$ is 1.

References:

[1] M. Anderson and T. Feil, Turning lights out with linear algebra, *Mathematics Magazine*, 71(1998), 300–303.

[2] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, second edition, 1994.

[3] R. A. Brualdi and H. J. Ryser, *Combinatorial Matrix Theory*, Cambridge University Press, 1991.

[4] B. Corbas and G. Williams, Congruence classes in $M_3(\mathbb{F}_q)(q\ odd)$, *Discrete Math.*, 219(2000), 37–47.

[5] B. Corbas and G. Williams. Congruence classes in $M_3(\mathbb{F}_q)(q\ even)$, *Discrete Math.*, 257(2002), 15–27.

[6] S. H. Friedberg, A. J. Insel, and L. E. Spence, *Linear Algebra*, Prentice-Hall, third edition, 1997.

[7] R. Gow, The number of equivalence classes of nondegenerate bilinear and sesquilinear forms over a finite field, *Linear Algebra Appl.*, 41(1981), 175–181.

[8] N. Jacobson, *Lectures in Abstract Algebra II, Linear Algebra*, Springer-Verlag, 1975.

[9] W. Waterhouse, The number of congruence classes in $M_n(\mathbb{F}_q)$, *Finite Fields Appl.*, 1(1995), 57–63.