International Scholarly Research Network
ISRN Algebra
Volume 2012, Article ID 520148, 9 pages
doi:10.5402/2012/520148

Research Article

Cogredient Standard Forms of Symmetric Matrices over Galois Rings of Odd Characteristic

Yonglin Cao

School of Sciences, Shandong University of Technology, Shandong, Zibo 255091, China

Correspondence should be addressed to Yonglin Cao, ylcao@sdut.edu.cn

Received 20 March 2012; Accepted 13 May 2012

Academic Editors: A. V. Kelarev, D. Kressner, and W. A. Rodrigues

Let $R = \mathrm{GR}(p^s, p^{sm})$ be a Galois ring of characteristic p^s and cardinality p^{sm}, where s and m are positive integers and p is an odd prime number. Two kinds of cogredient standard forms of symmetric matrices over R are given, and an explicit formula to count the number of all distinct cogredient classes of symmetric matrices over R is obtained.

1. Introduction and Preliminaries

Let p be a prime number, s and m be positive integers, and $R = \mathrm{GR}(p^s, p^{sm})$ a Galois ring of characteristic p^s and cardinality p^{sm}. Then $\mathrm{GR}(p^s, p^{sm})$ is isomorphic to the ring $\mathbb{Z}_{p^s}[x]/(h(x))$ for any basic irreducible polynomial $h(x)$ of degree m over $\mathbb{Z}_{p^s}$. It is clear that $R = \mathbb{F}_{p^m}$, that is, a finite field of p^m elements, if $s = 1$, and $R = \mathbb{Z}_{p^s}$, that is the ring of residue classes of $\mathbb{Z}$ modulo its ideal $p^s\mathbb{Z}$, if $m = 1$.

We denote by R^* the group of units of R. R is a local ring with the maximal ideal $(p) = pR$, and all ideals of R are given by $(0) = (p^s) \subset (p^{s-1}) \subset \cdots \subset (p) \subset (p^0) = R$. By [1, Theorem 14.8], there exists an element $\xi \in R^*$ of multiplicative order $p^m - 1$, which is a root of a basic primitive polynomial $h(x)$ of degree m over $\mathbb{Z}_{p^s}$ and dividing $x^{p^m-1} - 1$ in $\mathbb{Z}_{p^s}[x]$, and every element $a \in R$ can be written uniquely as

$$a = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}, \quad a_0, a_1, \ldots, a_{n-1} \in \mathcal{T}, \tag{1.1}$$

where $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{p^m-2}\}$. Moreover, a is a unit if and only if $a_0 \neq 0$, and a is a zero divisor or 0 if and only if $a_0 = 0$. Define the p-exponent of a by $\tau(0) = s$ and $\tau(a) = i$ if $a = a_i p^i + \cdots + a_{n-1} p^{n-1}$ with $a_i \neq 0$. By [1, Corollary 14.9], $R^* \cong \langle \xi \rangle \times [1 + (p)]$, where $\langle \xi \rangle$ is the cyclic group of order $p^m - 1$, and $1 + (p) = \{1 + x \mid x \in (p)\}$ is the one group of Galois ring R, so $|R^*| = (p^m - 1)p^{(s-1)m}$.

For a fixed positive integer n, let $\mathrm{M}_n(R)$ and $\mathrm{GL}_n(R)$ be the set of all $n \times n$ matrices and the multiplicative group of all $n \times n$ invertible matrices over R, and denote by $I^{(n)}$ and $0^{(n)}$ the $n \times n$ identity matrix and zero matrix, respectively. In this paper, for $l \times n$ matrix A and $q \times r$ matrix B over R, we adopt the notation $A \oplus B := \left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ which is a $(l+q) \times (n+r)$ matrix over R.

For any matrix $A \in \mathrm{M}_n(R)$, A is said to be *symmetric* if $A^T = A$, where A^T is the transposed matrix of A. We denote the set of all $n \times n$ symmetric matrices over R by $\mathcal{S}(n, R)$. Then $(\mathcal{S}(n, R), +)$ is a group under the addition of matrices. For any matrices $S_1, S_2 \in \mathrm{M}_n(R)$, if there exists matrix $P \in \mathrm{GL}_n(R)$ such that $PS_1P^T = S_2$, we say that S_1 is *cogredient* to S_2 over R. It is clear that $S_1 \in \mathcal{S}(n, R)$ if and only if $S_2 \in \mathcal{S}(n, R)$. So cogredience of matrices over R is an equivalent relation on $\mathcal{S}(n, R)$. If $S_1 \in \mathcal{S}(n, R)$, we call $\{PS_1P^T \mid P \in \mathrm{GL}_n(R)\}$ the *cogredient classes* of $\mathcal{S}(n, R)$ containing S_1 over R. Let $\mathcal{S}_0 = \{0\}, \mathcal{S}_1, \ldots, \mathcal{S}_d$ be all distinct cogredient classes of $\mathcal{S}(n, R)$. As in [2] we define relations on $\mathcal{S}(n, R)$ by

$$\Gamma_i := \{(A, B) \mid A, B \in \mathcal{S}(n, R), A - B \in \mathcal{S}_i\}, \quad i = 0, 1, \ldots, d. \tag{1.2}$$

Then the system $(\mathcal{S}(n, R), \{\Gamma_i\}_{0 \le i \le d})$ is an association scheme of class d on the set $\mathcal{S}(n, R)$ and denoted by $\mathrm{Sym}(n, R)$.

Let p stand for an odd prime number in the following. When $s = 1$, we know that the class number of $\mathrm{Sym}(n, \mathbb{F}_{p^m})$ is given by $d = 2n$ and the association scheme $\mathrm{Sym}(n, \mathbb{F}_{p^m})$ has been investigated in [2]. When $m = 1$, two kinds of cogredient standard forms of symmetric matrices over $\mathbb{Z}_{p^s}$ are given in [3, 4]. If $n \ge 2$, $s > 1$ and $p \equiv 1 \pmod 4$, a complex formula to count the number of all distinct cogredient classes of $\mathcal{S}(n, \mathbb{Z}_{p^s})$ is given in [3], which shows that, for example,

if m' is odd and s is odd, then

$$\begin{aligned} d + 1 = {} & \left(\frac{m' - 1}{2} + 1\right) + \sum_{s_1 \ne 0, \text{ or } s'_i, \exists i} \left(\frac{m' - 1}{2} - s_1 - \frac{s'_2 + s'_3 + s'_4 + s'_5 + \varepsilon}{2} + 1\right) \\ & \times \left[\binom{s-1}{1} + \binom{s-1}{2}\binom{s_1 - 1}{1} + \cdots + \binom{s-1}{s_1}\right] \\ & \times \binom{\frac{s-1}{2}}{s'_2}\binom{\frac{s+1}{2}}{s'_3}\binom{\frac{s-1}{2}}{s'_4}\binom{\frac{s+1}{2}}{s'_5}, \end{aligned} \tag{1.3}$$

where the meanings of $m', s_1, s'_2, s'_3, s'_4, s'_5, \varepsilon$ and formulas for other cases are referred to [3].

Then two problems arise. (1) Is there a simple and explicit formula to count the number of all distinct cogredient classes of $\mathcal{S}(n, \mathbb{Z}_{p^s})$? (2) For arbitrary Galois ring R, in order to determine precisely the class number d of the association scheme $\mathrm{Sym}(n, R)$, we have to count the number of all distinct cogredient classes of $\mathcal{S}(n, R)$.

In Section 2 we give two kinds of cogredient standard forms for every symmetric matrix over arbitrary Galois ring R of odd characteristic. In Section 3 we obtain an explicit formula to count the number of all distinct cogredient classes of $\mathcal{S}(n,R)$, which is simpler than that of [3] for the special case $R=\mathbb{Z}_{p^s}$.

Now, we list some properties for the Galois ring R which will be needed in the following sections. For general theory of Galois rings, one can refer to [1].

Lemma 1.1 (see [1, Theorem 14.11]). *$R^*=G_1\times G_2$ where G_1 is a cyclic group of order p^m-1, and $G_2=1+\langle p\rangle$ is a group of order $p^{(s-1)m}$.*

Proposition 1.2. (i) *R^{*2} is a subgroup of R^* with index $[R^*:R^{*2}]=2$.*

(ii) *For any $z\in R^*\setminus R^{*2}$, $R^*\setminus R^{*2}=zR^{*2}$, and $|R^{*2}|=|zR^{*2}|=(1/2)|R^*|$.*

(iii) *For any $u\in R^*$ and $a\in\langle p\rangle$, there exists $c\in R^*$ such that $c^2(u+a)=u$.*

Proof. In the notation of Lemma 1.1. Let ξ be a generator of the cyclic group G_1. Then ξ is of order p^m-1. Since p is odd and p^m-1 is even, ξ^2 is of order $(1/2)(p^m-1)$ and $G_1^2=\langle\xi^2\rangle$. Since $p^{(s-1)m}$ is odd and G_2 is a commutative group of order $p^{(s-1)m}$ by Lemma 1.1, for every $a\in G_2$, there exists a unique $b\in G_2$ such that $a=b^2$, so $G_2^2=G_2$. Moreover, by Lemma 1.1 each $u\in R^*$ can be uniquely expressed as $u=gh$ where $g\in G_1$ and $h\in G_2$.

(i) For every $u=gh\in R^*$ where $g\in G_1$ and $h\in G_2$, $u\in R^{*2}$ if and only if there exist $g_1\in G_1$ and $h_1\in G_2$ such that $gh=(g_1h_1)^2=g_1^2h_1^2$, which is then equivalent to that $g=g_1^2$ and $h=h_1^2$. So $u\in R^{*2}$ if and only if $u\in G_1^2\times G_2$ by Lemma 1.1. Then $R^{*2}=G_1^2\times G_2$ and so $|R^{*2}|=|G_1^2|\cdot|G_2|=(1/2)(p^m-1)\cdot p^{(s-1)m}=(1/2)|R^*|$. Hence, $[R^*:R^{*2}]=2$ by group theory.

(ii) Since $[R^*:R^{*2}]=2$, for any $z\in R^*\setminus R^{*2}$, we have $R^*=R^{*2}\cup zR^{*2}$ and $R^{*2}\cap zR^{*2}=\emptyset$ by group theory. So $|zR^{*2}|=|R^*|-|R^{*2}|=(1/2)|R^*|$ by the proof of (i).

(iii) Let $u\in R^*$ and $a\in\langle p\rangle$. Then $u^{-1}(u+a)=1+u^{-1}a\in 1+\langle p\rangle=G_2$. From this and by Lemma 1.1, there exists a unique element $b\in G_2\subseteq R^*$ such that $u^{-1}(u+a)=b^2$. Now, let $c=b^{-1}$. Then $c\in R^*$ satisfying $c^2(u+a)=u$. □

Proposition 1.3. *Let $-1\notin R^{*2}$. Then for any $z\in R^*\setminus R^{*2}$, there exist $x,y\in R^*$ such that $z=(1+x^2)y^2$.*

Proof. Let $u\in R^*$. Suppose that $1+u^2\notin R^*$. Then there exists $a\in R$ such that $1+u^2=ap$. So $u^2=-(1-ap)$. Since p is odd and $p^s=0$ in R, there exists $b\in R$ such that $(u^{p^s})^2=-(1-ap)^{p^s}=-(1-p^{p^s}b)=-1$. From $u^{p^s}\in R^*$ we deduce $-1\in R^{*2}$, which is a contradiction. Hence $1+u^2\in R^*$. Therefore, $\sigma: w\mapsto 1+w$ (for all $w\in R^{*2}$) is a mapping from R^{*2} to R^*. Suppose that $\sigma(R^{*2})\subseteq R^{*2}$. Then for $1\in R^{*2}$, there exists $w_0\in R^{*2}$ such that $\sigma(w_0)=1+w_0=1$, which implies that $w_0=0$, and we get a contradiction. So there exists $x\in R^*$ such that $1+x^2\notin R^{*2}$, that is, $1+x^2\in R^*\setminus R^{*2}=zR^{*2}$ by Proposition 1.2. Then there exists $c\in R^*$ such that $1+x^2=zc^2$, so $(1+x^2)y^2=z$, where $y=c^{-1}\in R^*$. □

2. Cogredient Standard Forms of Symmetric Matrices

In this section, we give two kinds of cogredient standard forms of symmetric matrices over R corresponding to that of cogredient standard forms of symmetric matrices over finite fields (see [5], or [6], Theorems 1.22 and 1.25).

Notation 1. For any nonnegative integer ν and $z \in R^* \setminus R^{*2}$, define

$$H_{2\nu} = \begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \qquad H_{2\nu+2,\Delta} = H_{2\nu} \oplus \Delta, \quad \text{where } \Delta = \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix},$$
$$H_{2\nu+1,(1)} = H_{2\nu} \oplus (1), \qquad H_{2\nu+1,(z)} = H_{2\nu} \oplus (z). \tag{2.1}$$

Lemma 2.1. *For any $\nu \in \mathbb{Z}^+$ and $z \in R^* \setminus R^{*2}$, $zI^{(2\nu)}$ is cogredient to $I^{(2\nu)}$.*

Proof. Let $-1 \in R^{*2}$. Then there exists $u \in R^*$ such that $u^2 = -1$, that is, $1 + u^2 = 0$. Since p is an odd prime number, we have $\gcd(2, p^s) = 1$ and so $2 \in R^*$. Let $P = 2^{-1}\begin{pmatrix} (1+z) & u^{-1}(1-z) \\ u(1-z) & (1+z) \end{pmatrix}$. Since R is a commutative ring, we have $\det P = (2^{-1})^2[(1+z)(1+z) - u^{-1}(1-z)u(1-z)] = (2^{-1})^2 \cdot 2 \cdot 2z = z \in R^*$. Hence, $P \in \mathrm{GL}_2(R)$. Then by $(u^{-1})^2 = (u^2)^{-1} = -1$ and $u(1-z^2) + u^{-1}(1-z^2) = u^{-1}(u^2+1)(1-z^2) = 0$, we get

$$\begin{aligned} PI^{(2)}P^T &= \left(2^{-1}\right)^2 \begin{pmatrix} (1+z) & u^{-1}(1-z) \\ u(1-z) & (1+z) \end{pmatrix} \begin{pmatrix} (1+z) & u(1-z) \\ u^{-1}(1-z) & (1+z) \end{pmatrix} \\ &= \left(2^{-1}\right)^2 \begin{pmatrix} 2 \cdot 2z & 0 \\ 0 & 2 \cdot 2z \end{pmatrix} = zI^{(2)}, \end{aligned} \tag{2.2}$$

so $zI^{(2)}$ is cogredient to $I^{(2)}$.

Let $-1 \notin R^{*2}$. Then by Proposition 1.3 there exist $x, y \in R^*$ such that $(1+x^2)y^2 = z$. Let $Q = \begin{pmatrix} xy & y \\ -y & xy \end{pmatrix}$. Then $\det Q = (1+x^2)y^2 = z \in R^*$ and so $Q \in \mathrm{GL}_2(R)$. By $(1+x^2)y^2 = z$, a matrix computation shows that $QI^{(2)}Q^T = QQ^T = zI^{(2)}$. Hence, $zI^{(2)}$ is cogredient to $I^{(2)}$ as well.

Then $zI^{(2\nu)} = \overbrace{zI^{(2)} \oplus \cdots \oplus zI^{(2)}}^{\nu's}$ is cogredient to $I^{(2\nu)} = \overbrace{I^{(2)} \oplus \cdots \oplus I^{(2)}}^{\nu's}$. □

Lemma 2.2. *Let $z \in R^* \setminus R^{*2}$ and $\nu \in \mathbb{Z}^+$.*

(i) *If $-1 \in R^{*2}$, then $I^{(2\nu)}$ is cogredient to $H_{2\nu}$.*

(ii) *If $-1 \notin R^{*2}$, then $I^{(\nu)} \oplus zI^{(\nu)}$ is cogredient to $H_{2\nu}$.*

Proof. We select $P_1 = 2^{-1}\begin{pmatrix} I^{(\nu)} & -I^{(\nu)} \\ I^{(\nu)} & I^{(\nu)} \end{pmatrix}$ and denote that $M = 2\begin{pmatrix} I^{(\nu)} & 0 \\ 0 & -I^{(\nu)} \end{pmatrix}$. From $P_1\begin{pmatrix} I^{(\nu)} & I^{(\nu)} \\ 0 & I^{(\nu)} \end{pmatrix} = \begin{pmatrix} 2^{-1}I^{(\nu)} & 0 \\ 2^{-1}I^{(\nu)} & I^{(\nu)} \end{pmatrix}$ we deduce $\det P_1 = \det(2^{-1}I^{(\nu)}) = (2^{-1})^\nu \in R^*$. Hence $P_1 \in \mathrm{GL}_{2\nu}(R)$. Then by $P_1MP_1^T = 2^{-1}\begin{pmatrix} I^{(\nu)} & -I^{(\nu)} \\ I^{(\nu)} & I^{(\nu)} \end{pmatrix}\begin{pmatrix} I^{(\nu)} & I^{(\nu)} \\ I^{(\nu)} & -I^{(\nu)} \end{pmatrix} = H_{2\nu}$, we see that M is cogredient to $H_{2\nu}$.

(i) By $-1 \in R^{*2}$ there exists $u \in R^*$ such that $-1 = u^2$. Then M is cogredient to $2I^{(2\nu)}$. If $2 \notin R^{*2}$, $2I^{(2\nu)}$ is cogredient to $I^{(2\nu)}$ by Lemma 2.1. If $2 \in R^{*2}$, there exists $w \in R^*$ such that $2 = w^2$, so $2I^{(2\nu)}$ is cogredient to $I^{(2\nu)}$ as well. Therefore, $I^{(2\nu)}$ is cogredient to $H_{2\nu}$ in this case.

(ii) Let $-1 \notin R^{*2}$. Then by Proposition 1.2 there exists $c \in R^*$ such that $-1 = zc^2$. Hence $I^{(\nu)} \oplus zI^{(\nu)}$ is cogredient to $\begin{pmatrix} I^{(\nu)} & 0 \\ 0 & -I^{(\nu)} \end{pmatrix}$. If $2 \in R^{*2}$, there exists $w \in R^*$ such that $2 = w^2$, so $\begin{pmatrix} I^{(\nu)} & 0 \\ 0 & -I^{(\nu)} \end{pmatrix}$ is cogredient to M. If $2 \notin R^{*2}$, then $-2 = (-1)2 \in R^{*2}$, and hence there exists $a \in R^*$ such that $-2 = a^2$, so $(aI^{(2\nu)})H_{2\nu}\left(\begin{smallmatrix} I^{(\nu)} & 0 \\ 0 & -I^{(\nu)} \end{smallmatrix}\right)H_{2\nu}^T(aI^{(2\nu)}) = M$. Hence, $\left(\begin{smallmatrix} I^{(\nu)} & 0 \\ 0 & -I^{(\nu)} \end{smallmatrix}\right)$ is cogredient to M as well. Therefore, $I^{(\nu)} \oplus zI^{(\nu)}$ is cogredient to $H_{2\nu}$. □

Lemma 2.3. *Let $z \in R^* \setminus R^{*2}$ and $D = \operatorname{diag}(u_1, \ldots, u_r)$, where $u_i \in R^*$, $i = 1, \ldots, r$ and $r \in \mathbb{Z}^+$. Then, One has the following.*

(i) *D is necessarily cogredient to either $I^{(r)}$ or $I^{(r-1)} \oplus (z)$. Moreover, these two matrices are not cogredient over R.*

(ii) *If $r = 2\nu + 1$ is odd, then D is necessarily cogredient to either $H_{2\nu+1,(1)}$ or $H_{2\nu+1,(z)}$. Moreover, these two matrices are not cogredient. If $r = 2\nu$ is even, then D is necessarily cogredient to either $H_{2\nu}$ or $H_{2(\nu-1)+2,\Delta}$. Moreover, these two matrices are not cogredient.*

Proof. (i) We may assume that $u_1, \ldots, u_t \in R^{*2}$ and $u_{t+1}, \ldots, u_r \in zR^{*2}$, where $0 \le t \le r$. Then D is cogredient to $I^{(t)} \oplus zI^{(r-t)}$. If $r - t$ is even, by Lemma 2.1 $zI^{(r-t)}$ is cogredient to $I^{(r-t)}$ and hence D is cogredient to $I^{(t)} \oplus I^{(r-t)} = I^{(r)}$. Now, let $r - t$ be odd. If $r - t = 1$, D is obviously cogredient to $I^{(1)} \oplus (z)$. If $r - t \ge 3$, by Lemma 2.1 $zI^{(r-t-1)}$ is cogredient to $I^{(r-t-1)}$, and hence D is cogredient to $I^{(t)} \oplus I^{(r-t-1)} \oplus (z) = I^{(r-1)} \oplus (z)$.

Suppose that $I^{(r)}$ is cogredient to $I^{(r-1)} \oplus (z)$ over R. Then there exists $Q \in \mathrm{GL}_r(R)$ such that $QI^{(r)}Q^T = I^{(r-1)} \oplus (z)$. From this and by $\det Q \in R^*$, we obtain that $z = (\det Q)^2 \in R^{*2}$, which is a contradiction. So $I^{(r)}$ and $I^{(r-1)} \oplus (z)$ are not cogredient over R.

(ii) We have one of the following two cases.

(ii-1) Let $r = 2\nu + 1$ be an odd number. Then $r - 1 = 2\nu$ is even and we have one of the following two cases.

(ii-1-1) Let $-1 \in R^{*2}$. Then $I^{(2\nu)}$ is cogredient to $H_{2\nu}$ by Lemma 2.2(i). From this and by (i) we deduce that D is cogredient to $H_{2\nu+1,(1)}$ when D is cogredient to $I^{(r)}$, or D is cogredient to $H_{2\nu+1,(z)}$ when D is cogredient to $I^{(r-1)} \oplus (z)$.

(ii-1-2) Let $-1 \in zR^{*2}$. Then we have one of the following two cases.

(α) Let $(1/2)(r-1) = \nu$ be even. Then $I^{(\nu)}$ is cogredient to $zI^{(\nu)}$ by Lemma 2.1, so $I^{(2\nu)}$ is cogredient to $I^{(\nu)} \oplus zI^{(\nu)}$. Since $I^{(\nu)} \oplus zI^{(\nu)}$ is cogredient to $H_{2\nu}$ by Lemma 2.2(ii), by (i) we see that: D is cogredient to $H_{2\nu+1,(1)}$ when D is cogredient to $I^{(r)}$, or D is cogredient to $H_{2\nu+1,(z)}$ when D is cogredient to $I^{(r-1)} \oplus (z)$.

(β) Let $(1/2)(r-1) = \nu$ be odd. Then $\nu = 2\omega + 1$ for some nonnegative integer ω and so $r - 1 = 4\omega + 2$. By Lemma 2.1 we see that $I^{(2\omega)}$ is cogredient to $zI^{(2\omega)}$, and $I^{(2)}$ is cogredient to $zI^{(2)}$. Hence $I^{(r)} = I^{(2\omega)} \oplus I^{(2\omega)} \oplus I^{(2)} \oplus (1)$ is cogredient to $I^{(2\omega)} \oplus zI^{(2\omega)} \oplus zI^{(2)} \oplus (1)$, which is then cogredient to $I^{(2\omega+1)} \oplus zI^{(2\omega+1)} \oplus (z)$. Since $I^{(2\omega+1)} \oplus zI^{(2\omega+1)}$ is cogredient to $H_{2(2\omega+1)} = H_{2\nu}$ by Lemma 2.2(ii), $I^{(r)}$ is cogredient to $H_{2\nu+1,(z)}$. Moreover, $I^{(r-1)} \oplus (z) = I^{(2\omega)} \oplus I^{(2\omega)} \oplus I^{(2)} \oplus (z)$ is cogredient to $I^{(2\omega)} \oplus zI^{(2\omega)} \oplus I^{(2)} \oplus (z)$, which is then cogredient to $I^{(2\omega+1)} \oplus zI^{(2\omega+1)} \oplus (1)$. Since $I^{(\nu)} \oplus zI^{(\nu)}$ is cogredient to $H_{2\nu}$ by Lemma 2.2(ii), $I^{(r-1)} \oplus (z)$ is cogredient to $H_{2\nu+1,(1)}$. Therefore, D is necessarily cogredient to either $H_{2\nu+1,(1)}$ or $H_{2\nu+1,(z)}$ by (i).

(ii-2) Let $r = 2\nu$ be an even number. Then $r - 2 = 2(\nu - 1)$ is also even and we have one of the following two cases.

(ii-2-1) Let $-1 \in R^{*2}$. Then $-1 = u^2$ for some $u \in R^*$ and so $\left(\begin{smallmatrix} 1 & 0 \\ 0 & z \end{smallmatrix}\right)$ is cogredient to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -z \end{smallmatrix}\right) = \Delta$. By Lemma 2.2(i) D is cogredient to $H_{2\nu}$ when D is cogredient to $I^{(r)}$, or D is cogredient to $H_{2(\nu-1)+2,\Delta}$ when D is cogedient to $I^{(r-1)} \oplus (z) = I^{(2(\nu-1))} \oplus \left(\begin{smallmatrix} 1 & 0 \\ 0 & z \end{smallmatrix}\right)$.

(ii-2-2) Let $-1 \in zR^{*2}$. Then $-1 = zc^2$ for some $c \in R^*$. By $1 = (-z)c^2$, we see that $I^{(2)}$ is cogredient to Δ. Now, we have one of the following two cases.

(α) Let ν be even. Then $I^{(\nu)}$ is cogredient to $zI^{(\nu)}$ by Lemma 2.1 and so $I^{(r)} = I^{(\nu)} \oplus I^{(\nu)}$ is cogredient to $I^{(\nu)} \oplus zI^{(\nu)}$. From this and by Lemma 2.2(ii), we see that $I^{(r)}$ is cogredient to $H_{2\nu}$. Let $\nu = 2$. Since $I^{(2)}$ is cogredient to Δ and $I^{(1)} \oplus (z)$ is cogredient to H_2 by Lemma 2.2(ii), $I^{(3)} \oplus (z) = I^{(2)} \oplus I^{(1)} \oplus (z)$ is cogredient to $H_2 \oplus \Delta = H_{2\cdot 1+2,\Delta}$. Now, let $\nu \geq 4$. Since $\nu - 2$ is even, $I^{(\nu-2)}$ is cogredient to $zI^{(\nu-2)}$ by Lemma 2.1, so $I^{(\nu-2)} \oplus I^{(\nu-2)}$ is cogredient to $I^{(\nu-2)} \oplus zI^{(\nu-2)}$. Hence, $I^{(r-1)} \oplus (z) = I^{(\nu-2)} \oplus I^{(\nu-2)} \oplus I^{(3)} \oplus (z)$ is cogredient to $I^{(\nu-2)} \oplus zI^{(\nu-2)} \oplus I^{(3)} \oplus (z)$, which is then cogredient to $I^{(\nu-1)} \oplus zI^{(\nu-1)} \oplus I^{(2)}$. Since $I^{(2)}$ is cogredient to Δ, we see that $I^{(r-1)} \oplus (z)$ is cogredient to $H_{2(\nu-1)+2,\Delta}$ by Lemma 2.2(ii). Therefore, D is necessarily cogredient to either $H_{2\nu}$ or $H_{2(\nu-1)+2,\Delta}$ by (i).

(β) Let ν be odd. Then there exists nonnegative integer ω such that $\nu = 2\omega + 1$ and so $r = 4\omega + 2$. Since $I^{(2\omega)}$ is cogredient to $zI^{(2\omega)}$ by Lemma 2.1, $I^{(r)} = I^{(2\omega)} \oplus I^{(2\omega)} \oplus I^{(2)}$ is cogredient to $I^{(2\omega)} \oplus zI^{(2\omega)} \oplus \Delta$, that is then cogredient to $H_{2(2\omega)+2,\Delta} = H_{2(\nu-1)+2,\Delta}$ by Lemma 2.2(ii). Now, $I^{(r-1)} \oplus (z) = I^{(2\omega)} \oplus I^{(2\omega)} \oplus (1) \oplus (z)$ is cogredient to $I^{(2\omega)} \oplus zI^{(2\omega)} \oplus (1) \oplus (z)$ by Lemma 2.1, which is then cogredient to $I^{(2\omega+1)} \oplus zI^{(2\omega+1)}$. Hence $I^{(r-1)} \oplus (z)$ is cogredient to $H_{2(2\omega+1)} = H_{2\nu}$ by Lemma 2.2(ii). Therefore, D is necessarily cogredient to either $H_{2\nu}$ or $H_{2(\nu-1)+2,\Delta}$ by (i). □

Theorem 2.4. *Let $z \in R^* \setminus R^{*2}$. Then every $n \times n$ symmetric matrix A over R is necessarily cogredient to one of the following matrices:*

$$D_{(n,k,t;k_1,\ldots,k_t;r_1,\ldots,r_t)} := \operatorname{diag}\Big(p^{r_1}D_1, p^{r_2}D_2, \ldots, p^{r_t}D_t, 0^{(n-k)}\Big), \tag{2.3}$$

where $0 \leq t \leq k \leq n$, $D_i = I^{(k_i)}$ or $I^{(k_i-1)} \oplus (z)$ for all $i = 1, \ldots, t$, $0 \leq r_1 < r_2 < \cdots < r_t \leq s-1$, and $k_i \in \mathbb{Z}^+$ satisfy $\Sigma_{i=1}^t k_i = k$.

Proof. The statement holds obviously if $A = 0$ (corresponding to the case $k = 0$) or $n = 1$. Now, let $n \geq 2$ and $A = (a_{ij})_{n\times n} \neq 0$. Then, there exist $1 \leq i_0, j_0 \leq n$ such that $a_{i_0j_0} \neq 0$ and $\tau(a_{i_0j_0}) = \min\{\tau(a_{ij}) \mid a_{ij} \neq 0,\ 1 \leq i,j \leq n\}$. Let $s_1 = \nu(a_{i_0j_0})$. Then $0 \leq s_1 \leq s-1$, and there exists $P_1 \in \mathrm{GL}_n(R)$ such that $P_1AP_1^T = \operatorname{diag}(u_1p^{s_1}, B)$ where $u_1 \in R^*$ and $B = (b_{ij})$ is a $(n-1)\times(n-1)$ symmetric matrix over R satisfying $B = 0$ or $\tau(b_{ij}) \geq s_1$ for all $b_{ij} \neq 0$, $1 \leq i,j \leq n-1$. By induction there exists $X \in \mathrm{GL}_{n-1}(R)$ such that $XBX^T = \operatorname{diag}(u_2p^{s_2}, \ldots, u_kp^{s_k}, 0^{(n-k)})$, where $u_2, \ldots, u_k \in R^*$ and $s_2 \leq \cdots \leq s_k \leq s-1$. Then $P = \operatorname{diag}(1, X)P_1 \in \mathrm{GL}_n(R)$ satisfies $PAP^T = \operatorname{diag}(u_1p^{s_1}, \ldots, u_kp^{s_k}, 0^{(n-k)})$.

Now, there must exist $t, k_i \in \mathbb{Z}^+$, $i = 1, \ldots, t$ and $0 \leq r_1 < \cdots < r_t \leq s-1$ such that $s_1 = \cdots = s_{k_1} = r_1 < s_{k_1+1} = \cdots = s_{k_1+k_2} = r_2 < \cdots < s_{k_1+k_2+\cdots+k_{t-1}+1} = \cdots = s_{k_1+k_2+\cdots+k_{t-1}+k_t} = r_t$. Then $\Sigma_{i=1}^t k_i = k$ and A is cogredient to $M = \operatorname{diag}(p^{r_1}M_1, p^{r_2}M_2, \ldots, p^{r_t}M_t, 0^{(n-k)})$, where $M_i = \operatorname{diag}(u_{k_1+\cdots+k_{i-1}+1}, \ldots, u_{k_1+\cdots+k_{i-1}+k_i})$ is a $k_i \times k_i$ matrix over R for all $i = 1, \ldots, t$. Since M_i is cogredient to D_i for every $1 \leq i \leq t$ by Lemma 2.3(i), we deduce that A is cogredient to $\operatorname{diag}(p^{r_1}D_1, p^{r_2}D_2, \ldots, p^{r_t}D_t, 0^{(n-k)})$. □

Theorem 2.5. *Let $z \in R^* \setminus R^{*2}$. Then every $n \times n$ symmetric matrix A over R is necessarily cogredient to one of the following matrices:*

$$H_{(n,k,t;k_1,\ldots,k_t;r_1,\ldots,r_t)} := \operatorname{diag}\Big(p^{r_1}H_1, p^{r_2}H_2, \ldots, p^{r_t}H_t, 0^{(n-k)}\Big), \tag{2.4}$$

where H_i is a $k_i \times k_i$ matrix over R such that H_i is equal to either $H_{2\nu_i+1,(1)}$ or $H_{2\nu_i+1,(z)}$ when $k_i = 2\nu_i + 1$ is odd, and H_i is equal to either $H_{2\nu_i}$ or $H_{2(\nu_i-1)+2,\Delta}$ when $k_i = 2\nu_i$ is even, for all $i = 1,\dots,t$; $0 \le t \le k \le n$, $0 \le r_1 < r_2 < \cdots < r_t \le s-1$, and $k_i \in \mathbb{Z}^+$ satisfy $\Sigma_{i=1}^{t} k_i = k$.

Proof. It follows from Theorem 2.4 and the proof of Lemma 2.3(ii).

For any $n \times n$ symmetric matrix A, we call $D_{(n,k,t;k_1,\dots,k_t;r_1,\dots,r_t)}$ the *cogredient standard form of kind* (I) of A if A is cogredient to $D_{(n,k,t;k_1,\dots,k_t;r_1,\dots,r_t)}$, and call $H_{(n,k,t;k_1,\dots,k_t;r_1,\dots,r_t)}$ the *cogredient standard form of kind* (II) of A if A is cogredient to $H_{(n,k,t;k_1,\dots,k_t;r_1,\dots,r_t)}$. □

3. The Number of Cogredient Classes of Symmetric Matrices

In order to count the number of all distinct cogredient classes of $n\times n$ symmetric matrices over R, we show that every $n \times n$ symmetric matrix over R has only one cogredient standard form of kind (I) first, then the number of all distinct cogredient classes of $n \times n$ symmetric matrices over R is equal to the number of all cogredient standard forms of kind (I) by Theorem 2.4.

Theorem 3.1. *The number $\mathcal{C}_{s,n}$ of all distinct cogredient classes of $n \times n$ symmetric matrices over R is given by the following:*

(i) *If $n \le s$, then $\mathcal{C}_{s,n} = 1 + \sum_{j=0}^{n-1} \sum_{i=j}^{n-1} \binom{i}{j} \binom{s}{j+1} 2^{j+1}$;*

(ii) *If $n \ge s+1$, then $\mathcal{C}_{s,n} = 1 + \sum_{j=0}^{s-1} \sum_{i=j}^{n-1} \binom{i}{j} \binom{s}{j+1} 2^{j+1}$.*

Proof. Let $\widehat{D} := \operatorname{diag}(p^{\widehat{r}_1}\widehat{D}_1, p^{\widehat{r}_2}\widehat{D}_2, \dots, p^{\widehat{r}_{\widehat{t}}}\widehat{D}_{\widehat{t}}, 0^{(n-\widehat{k})})$, where $\widehat{D}_i = I^{(\widehat{k}_i)}$ or $I^{(\widehat{k}_i-1)} \oplus (z)$ for all $i = 1,\dots,\widehat{t}$, $0 \le \widehat{t} \le \widehat{k} \le n$, $0 \le \widehat{r}_1 < \widehat{r}_2 < \cdots < \widehat{r}_{\widehat{t}} \le s-1$, and $\widehat{k}_i \in \mathbb{Z}^+$ satisfy $\Sigma_{i=1}^{\widehat{t}} \widehat{k}_i = \widehat{k}$. In the notation of Theorem 2.4, by [7, Theorem D], it follows that $D = \widehat{D}$ if $D := D_{(n,k,t;k_1,\dots,k_t;r_1,\dots,r_t)}$ is cogredient to $\widehat{D}$ over R. Hence, every $n \times n$ symmetric matrix over R has only one cogredient standard form of kind (I).

For any $1 \le t \le k \le n$, denote that $S_1 = \{(k_1,\dots,k_t) \mid k_i \in \mathbb{Z}^+, \Sigma_{i=1}^{t} = k\}$ and $S_2 = \{(r_1,\dots,r_t) \mid r_i \in \mathbb{Z}, 0 \le r_1 < r_2 < \cdots < r_t \le s-1\}$. Then $|S_1| = \binom{k-1}{t-1}$, $|S_2| = \binom{s}{t}$ if $t \le s$ and, $|S_2| = 0$ if $t \ge s$. From this and by Theorem 2.4 it follows that $\mathcal{C}_{s,n} = 1 + \sum_{k=1}^{n} (\sum_{t=1}^{k} |S_1| \cdot |S_2| \cdot 2^t)$. Therefore, $\mathcal{C}_{s,n} = 1 + \sum_{j=0}^{n-1} \sum_{i=j}^{n-1} \binom{i}{j} \binom{s}{j+1} 2^{j+1}$ if $n \le s$ and, $\mathcal{C}_{s,n} = 1 + \sum_{j=0}^{s-1} \sum_{i=j}^{n-1} \binom{i}{j} \binom{s}{j+1} 2^{j+1}$ if $n \ge s+1$.

In the notations of Section 1, we see that the class number d of the association scheme $\operatorname{Sym}(n, R)$ is determined by $d+1 = \mathcal{C}_{s,n}$. Then by Theorem 3.1, we have the following corollary. □

Corollary 3.2. *The class number of the association scheme $Sym(n, R)$ is given by the following.*

(i) *If $n \le s$, then $d = \sum_{j=0}^{n-1} \sum_{i=j}^{n-1} \binom{i}{j} \binom{s}{j+1} 2^{j+1}$;*

(ii) *If $n \ge s+1$, then $d = \sum_{j=0}^{s-1} \sum_{i=j}^{n-1} \binom{i}{j} \binom{s}{j+1} 2^{j+1}$.*

Example 3.3. Let p be an odd prime number and $s = 2$. Then by Theorem 3.1 the number $\mathcal{C}_{2,2}$ of all cogredient classes of 2×2 symmetric matrices over Galois ring $\mathrm{GR}(p^2, p^{2m})$ is given by $\mathcal{C}_{2,2} = 1 + \sum_{j=0}^{1} \sum_{i=j}^{1} \binom{i}{j} \binom{2}{j+1} 2^{j+1} = 13$. In fact, for a fixed element $z \in R^* \setminus R^{*2}$, all cogredient standard forms of kind (I) of 2×2 symmetric matrices over $\mathrm{GR}(p^2, p^{2m})$ are given by the following:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} z & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} zp & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix},$$
$$\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} p & 0 \\ 0 & zp \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} z & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & zp \end{pmatrix}, \begin{pmatrix} z & 0 \\ 0 & zp \end{pmatrix}. \tag{3.1}$$

The number $\mathcal{C}_{2,3}$ of all cogredient classes of 3×3 symmetric matrices over $\mathrm{GR}(p^2, p^{2m})$ is given by $\mathcal{C}_{2,3} = 1 + \sum_{j=0}^{1} \sum_{i=j}^{2} \binom{i}{j} \binom{2}{j+1} 2^{j+1} = 25$. In fact, all cogredient standard forms of kind (I) of 3×3 symmetric matrices over $\mathrm{GR}(p^2, p^{2m})$ are given by the following: $\begin{pmatrix} J & 0 \\ 0 & 0 \end{pmatrix}$ where J is one of matrices in (3.1), and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & z \end{pmatrix}, \begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix}, \begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & zp \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & p \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & zp \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & zp \end{pmatrix}, \tag{3.2}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix}, \begin{pmatrix} z & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & zp \end{pmatrix}, \begin{pmatrix} z & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & zp \end{pmatrix}.$$

Example 3.4. Let p be an odd prime number and $s = 5$. Then by Theorem 3.1 the number $\mathcal{C}_{5,4}$ of all cogredient classes of 4×4 symmetric matrices over Galois ring $\mathrm{GR}(p^5, p^{5m})$ is given by $\mathcal{C}_{5,4} = 1 + \sum_{j=0}^{3} \sum_{i=j}^{3} \binom{i}{j} \binom{5}{j+1} 2^{j+1} = 681$; the number $\mathcal{C}_{5,7}$ of all cogredient classes of 7×7 symmetric matrices over $\mathrm{GR}(p^5, p^{5m})$ is given by $\mathcal{C}_{5,7} = 1 + \sum_{j=0}^{4} \sum_{i=j}^{6} \binom{i}{j} \binom{5}{j+1} 2^{j+1} = 6943$.

Acknowledgment

This reaserach is supported in part by the National Science Foundation of China (No. 10971160) and Natural Science Foundation of Shandong provence (Grant No. ZR2011AQ004).

References

[1] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific, River Edge, NJ, USA, 2003.
[2] Y. J. Huo and Z. X. Wan, "Non-symmetric association schemes of symmetric matrices," *Chinese Science Bulletin*, vol. 36, no. 18, pp. 1501–1505, 1991.
[3] Y. Liu and J.-Z. Nan, "Some Anzahl theorems in symmetric matrices over finite local rings," *Journal of Mathematical Research and Exposition*, vol. 26, no. 3, pp. 423–439, 2006.
[4] Y. Wu, *Classifications of Certain Matrices over Special Galois Rings*, Scientific Publishing, Beijing, China, 2006.

[5] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, Dover, New York, NY, USA, 1958.
[6] Z. X. Wan, *Geometry of Classical Groups over Finite Fields*, Studentlitteratur, 1993.
[7] Y. Cao and F. Szechtman, "Congruence of symmetric matrices over local rings," *Linear Algebra and Its Applications*, vol. 431, no. 9, pp. 1687–1690, 2009.