The Number of Conjugates of the Standard Representation of S_n in the General Linear Group over GF(2)

Peter M. Maurer
Department of Computer Science
Baylor University
Waco, Texas 76798
Peter_Maurer@Baylor.edu

1. Introduction.

The set of all $n \times n$ matrices over GF(2) is called the *general linear group* of degree *n* over GF(2) and is designated $GL_n(2)$. The set of all permutations on a set of *n* elements is called the *symmetric group* of degree *n*, and is designated S_n. A matrix that contains a single one in each row and in each column is called a *permutation matrix*. The set of all $n \times n$ permutation matrices forms a group under matrix multiplication. This group is designated $SR_n(2)$, and is isomorphic to the symmetric group of degree *n*. $SR_n(2)$ is called the *standard representation* of S_n over GF(2).

The purpose of this note is first to determine the normalizer of $SR_n(2)$ in $GL_n(2)$. Let *G* be any group and $x, y \in G$. The elements x and y are said to be *conjugate* to one another, if there is an element $g \in G$ such that $x = gyg^{-1}$. The concept of conjugacy can be extended to subgroups of *G* in a natural way. A subgroup $N \subseteq G$ is normal in *G* if $N = gNg^{-1}$ for all $g \in G$. Let *S* be a subgroup of *G*. The normalizer $\mathfrak{N}(S)$ of S in G is the largest subgroup of G in which S is normal. In other words $\mathfrak{N}(S) = \{g \mid gsg^{-1} \in S$ for all $s \in S\}$.

The normalizer of $SR_n(2)$ is important because knowing its size will allow us to determine the number of conjugates of $SR_n(2)$ in $GL_n(2)$. It is well known that the number of conjugates of a subgroup *S* in *G* is equal to $\frac{o(G)}{o(\mathfrak{N}(S))}$ [1].

2. Lemmas and Theorems

Lemma 1: If $M \in \mathfrak{N}(SR_n(2))$, then every column permutation of M is also a row permutation of M, and vice versa.

Proof: Let $M \in \mathfrak{N}(SR_n(2))$ and $P \in SR_n(2)$. Then $MPM^{-1} = Q$ where $Q \in SR_n(2)$, and $MP = QM$. The matrix MP is a column permutation of *M*. In fact, any permutation of the columns of *M* can be expressed in the form MP where $P \in SR_n(2)$. Furthermore QM is a row permutation of *M*, and any permutation of the rows of *M* can be expressed in this form.

Lemma 2: If $M \in \mathfrak{N}(SR_n(2))$, then every column of *M* has the same number of ones, and every row of *M* has the same number of 1's.

Proof: Every column permutation of *M* can be expressed in the form *MP* where *P* is a permutation matrix. In particular, the permutation (1,i) in which columns 1 and i are interchanged can be expressed in the form MP where P is a permutation matrix. But by Lemma 1, *MP*=*QM* where *QM* is a row permutation of *M*. Because *QM* is a row permutation of M, the number of 1's in column 1 of *M* must be the same as the number of 1's in column 1 of *QM*. Therefore column *i* must have the same number of 1's as column 1. Since no restrictions were placed on *i*, all columns must have the same number of 1's. The argument for rows is identical.

Lemma 3: If $M \in \mathfrak{N}(SR_n(2))$, then the number of 1's in each row of *M* must equal the number of 1's in each column of *M*.

Proof: By Lemma 2, each column of *M* must have the same number of 1's. Let's assume that each column has *k* ones. Then the total number of 1's in *M* is *nk*. However, M must have the same number of 1's in each row, so the number of 1's in each row must be *nk*/*n*=*k*.

Lemma 4: If $M \in \mathfrak{N}(SR_n(2))$, and *k* is the number of 1's in each row or column, then *k*=1 or *k*=n-1.

Proof. Suppose that M has *k* ones in each row and column, where $1 < k < n-1$. The number of different rows containing *k* ones and $n-k$ zeros is equal $q = \binom{n}{k} = \frac{n!}{k!(n-k)!}$. Because $1 < k < n-1$, *q* must be greater than *n*. Therefore there must be at least one row *r* with *k* ones that is not contained in *M*. Let s be the first row of *M*. Since r and s have the same weight, there is a permutation *p* that will transform *s* into *r*. Let *P* be the permutation matrix corresponding to *p*. The matrix *MP* is a column permutation of *M* which has *r* as its first row. But *r* is not contained in *M*, so *MP* cannot be a row-permutation of *M*. By Lemma 1, *M* cannot be a member of $\mathfrak{N}(SR_n(2))$.

Theorem 1. If *n* is odd, then $\mathfrak{N}(SR_n(2)) = SR_n(2)$.

Proof. Let *M* be an $n \times n$ matrix with $n-1$ zeros in each row and column. Since $n-1$ is even, each column of *M* has an even number of ones, and the sum of the column is zero. Thus if we add all rows of *M*, the result is the zero vector, and *M* is singular. That is, $M \notin GL_n(2) \supseteq \mathfrak{N}(SR_n(2))$. Since the only other possibility is that each row and column contain a single 1, every element of $\mathfrak{N}(SR_n(2))$ must be a permutation matrix, and $\mathfrak{N}(SR_n(2)) = SR_n(2)$.

Lemma 5. If *n* is even and *v* and *w* are two *n*-element vectors of weight $n-1$, then $v \bullet w = 1$ if v=w and $v \bullet w = 0$ when $v \neq w$.

Proof. Suppose *v*=*w*. Then the single zeros in *v* and *w* are in the same position. The product of the other $n-1$ positions is 1, because both elements are 1. The product of the zero position is zero. Thus the dot product is the sum of an odd number of ones, and is equal to one. If *v* and *w* are different, then the single zero in *v* is in position *i*, and the single zero in *w* is in position *j*, and $i \neq j$. Since there is a zero in position *i*, the product in that position is zero. The product for position *j* is also zero. Since $i \neq j$, there are $n-2$ additional positions whose product is ones. Since *n* is even, $n-2$ is also even, and the dot product is the sum of an even number of ones which is zero.

Lemma 6. If n is even and M is a matrix with $n-1$ ones in each row and in each column, then M is nonsingular.

Proof. Note that M must have a single zero in each row and in each column. If M is singular, then some subset of k>0 rows of M must add up to zero. If $k=n$, then the subset contains every row in M. Each column of M contains an odd number of 1's and adds up to 1. Therefore, k must be less than n. No single row is the zero vector, so assume we have chosen some subset of size $k>1$. If we arrange these k rows into a $k \times n$ matrix, Z, at least one column must contain all ones. If k is odd, then the sum of any column containing all ones must be one. So let us assume that k is even. There must be at least one column containing a zero, and because M contains a single zero in each column, any column of Z containing a zero must contain only a single zero. Thus this column must contain an odd number of ones, and its sum is one. Thus it is impossible for any nonempty subset of the rows of M to add up to zero, and M must be nonsingular.

Lemma 7. Let n be even and let M and N be two matrices with $n-1$ zeros in each row and each column. Then MN is a permutation matrix.

Proof. By Lemma 5 the dot product of any row M and any column of N is equal to 1 when the row and column are the same vector, and is equal to zero otherwise. Every row of M will equal one and only one column of N. Thus every column of MN can contain only a single one. Since by Lemma 6 both M and N are nonsingular, then so is MN. Since MN cannot contain a zero row, and there are a total of n ones in MN, each column must contain a single one.

Lemma 8. Let n be even and M be a matrix with $n-1$ ones in each row and each column. Then $MM^T = I$, where M^T is the transpose of M.

Proof. The i^{th} row of M is equal to the i^{th} column of M^T, so the main diagonal of MM^T is all ones. If $i \neq j$ then row i of M does not equal row j of M. Thus row i of M does not equal column j of M^T and element (i,j) of MM^T is equal to zero. Thus MM^T is the identity matrix.

Note that M^T has $n-1$ ones in each row and in each column.

Theorem 2. If n is even, then $\mathfrak{N}(SR_n(2))$ contains all permutation matrices, all matrices containing $n-1$ ones in each row and each column, and nothing else.

Proof. $\mathfrak{N}(SR_n(2))$ trivially contains all permutation matrices. Let M be a matrix with $n-1$ ones in each row and each column. Given a permutation matrix P, consider MPM^{-1}. The matrix MP is a column permutation of M, and is a matrix containing $n-1$ rows in each row and in each column. By Lemma 8, $M^{-1} = M^T$. Thus M^{-1} is a matrix containing $n-1$ ones in each row and in each column. By Lemma 7, $(MP)M^{-1}$ is a permutation matrix. Thus, $MPM^{-1} \subseteq SR_n(2)$. Thus $M \in \mathfrak{N}(SR_n(2))$. By Lemmas 2, 3, and 4, $\mathfrak{N}(SR_n(2))$ can contain nothing else.

The size of $SR_n(2)$ is $\prod_{i=0}^{n-1}\left(2^n - 2^i\right)$ [2] and the size of S_n is n!. Thus we have the following theorem.

Theorem 3. If *n* is odd, then the number of conjugates of $SR_n(2)$ is given by

$$\frac{\prod_{i=0}^{n-1}\left(2^n - 2^i\right)}{n!}$$

If $n > 2$ is even then the number of conjugates of $SR_n(2)$ is given by

$$\frac{\prod_{i=0}^{n-1}\left(2^n - 2^i\right)}{2n!}$$

Theorem 3 does not apply to 2×2 matrices because any matrix with $n-1$ ones in each row and each column is a permutation matrix.

3. Examples

The following table gives the number of conjugates of $SR_n(2)$ for various values of *n*.

n	$o(\mathfrak{N}(SR_n(2)))$	$o(GL_n(2))$	Number of Conjugates
2	2	6	3
3	6	168	28
4	48	20,160	420
5	120	9,999,360	83,328
6	1,440	20,158,709,760	13,999,104
7	5,040	163,849,992,929,280	32,509,919,232
8	80,640	5,348,063,769,211,699,200	66,320,235,233,280
9	362,880	699,612,310,033,197,642,547,200	1,927,943,976,061,501,440
10	7,257,600	366,440,137,299,948,128,422,802,227,200	50,490,539,200,279,448,911,872

4. References

1. Robinson, D., A Course in the Theory of Groups, Springer, New York, 1995.
2. Lidl, R., Niederreiter, H., Finite Fields and Their Applications, Elsevier, Amsterdam, 1996.