THE GENERATION BY TWO OPERATORS OF THE SYMPLECTIC GROUP OVER $GF(2)$*

T. G. ROOM

(rec. 8 Aug. 1958)

The main result obtained in this paper is

THEOREM 1. *The symplectic group on the skew matrix Γ of $2m$ rows and columns over $GF(2)$ ** can be generated by the two matrices Q, R, where*

$$\begin{aligned} &Q^{2m+1} = R^2 = \mathbf{1} \\ &(RQ)^{2m-1} = T_{1,3} \\ &(RQ^2)^{2m-1} = T_{1,2} \\ &Q^r T_{i,j} Q^{-r} = T_{i+r,j+r} \quad i+r, \quad j+r \leqq 2m \end{aligned}$$

$T_{i,j}$ being the substitution matrix which interchanges the elements numbered i and j, ($m \geqq 2$).

This symplectic group is Dickson's group $A(2m, 2)$ (**1**, *p.* 97).

In the case $m = 2$ the matrices are

$$\Gamma = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad R = R^0 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

To define the matrices for general values of m write

$$\begin{aligned} &\boldsymbol{v}_r : \text{a succession of } r \text{ digits } 1 \\ &\boldsymbol{v} = \boldsymbol{v}_{2m} \\ &\mathbf{0}_r : \text{a succession of } r \text{ digits } 0, \end{aligned}$$

these being treated as parts of column vectors, the corresponding row vectors being $\boldsymbol{v}_r^T$, $\mathbf{0}_r^T$

Γ and Q are of the same patterns as for $m = 2$, and $R = R^0 \oplus \mathbf{1}_{2m-4}$, direct sum, namely

* The results described in this paper were obtained while the author was a member of the Institute for Advanced Study, Princeton.

** A skew matrix over $GF(2)$ differs from a symmetric matrix in that all its diagonal elements are 0.

https://doi.org/10.1017/S1446788700025052 Published online by Cambridge University Press

$$\Gamma = \boldsymbol{v}\boldsymbol{v}^T + \mathbf{1}_{2m}$$

$$Q = \begin{bmatrix} \mathbf{0}^T_{2m-1} & 1 \\ \mathbf{1}_{2m-1} & \boldsymbol{v}_{2m-1} \end{bmatrix} \qquad R = \begin{bmatrix} R^0 & \\ & \mathbf{1}_{2m-4} \end{bmatrix}$$

Write also

$T*$: any substitution matrix as described in the text.

The group generated by Q, R will be denoted by $\langle Q, R\rangle$; it is to be proved isomorphic to $A(2m, 2)$.

From the conditions satisfied by R and Q it is clear that one of the subgroups of $\langle Q, R\rangle$ is the symmetric group S_{2m}; it is to be proved that in fact S_{2m+2} is a subgroup of $A(2m, 2)$.

The present solution of the problem of the generation of $A(2m, 2)$ has its origin in an investigation of the group CG of the Clifford units, and the relations among the matrices stated in Theorem 1 are best obtained in terms of substitutions on the elements of CG.

We assume a basic set of $2m$ Clifford units γ_i with the properties:

every pair anti-commutes: $\gamma_i\gamma_j = -\gamma_j\gamma_i, \quad i \neq j$
each unit is involutory: $\gamma_i^2 = 1.$

These units generate the free Abelian group CG of order 2^{2m} the elements of which are the products $\gamma_i\gamma_j\gamma_k \cdots$ without regard to sign. Every element of the group is involutory. Any set of $2m$ elements of CG such that every pair of the set anti-commutes will be called a *Clifford set*; the connection between CG and $A(2m, 2)$ which is to be established in this:

THEOREM 2. *$A(2m, 2)$ is isomorphic to the group of automorphisms of CG which transform Clifford sets into Clifford sets.*

In CG there is exactly one element which anti-commutes with each of the $2m$ units γ_i, namely,

$$\gamma_{2m+1} = \prod_1^{2m} \gamma_i$$

γ_{2m+1} is in all senses symmetric with the original $2m$ units, and any $2m$ members of the whole set of $2m+1$ may be taken as generators of CG. We shall denote by χ_0 the set of $2m+1$ matrices $\gamma_1, \gamma_2, \cdots, \gamma_{2m+1}$ in any order, and shall describe any corresponding set in CG as a *complete Clifford set.*

To establish the connection between the group of automorphisms of CG and $A(2m, 2)$ we need to introduce the *index vector* of an element of CG. Every element of CG may be written as $\gamma_1^{\alpha_1}\gamma^{\alpha_2}\cdots\gamma_{2m}^{\alpha_{2m}}$, $\alpha_i = 0$ or 1, and thus determines an *index vector*

$$\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \cdots, \alpha_{2m}] \text{ over } GF(2).$$

There is of course a one-to-one correspondence between the index vectors and the elements of CG.

https://doi.org/10.1017/S1446788700025052 Published online by Cambridge University Press

γ_i corresponds to the index vector $\boldsymbol{\varepsilon}_i$ of the basis, $i = 1, \cdots, 2m$, and γ_{2m+1} corresponds to $\boldsymbol{\nu}$.

We have

$$Q\boldsymbol{\varepsilon}_i = \boldsymbol{\varepsilon}_{i+1},\ Q\boldsymbol{\varepsilon}_{2m} = \boldsymbol{\nu},\ Q\boldsymbol{\nu} = \boldsymbol{\varepsilon}_1,\ i = 1, \cdots, 2m - 1.$$

i.e., Q corresponds to the cyclic permutation of the units $\gamma_1, \gamma_2, \cdots, \gamma_{2m+1}$; also

$$T_{i,j}\boldsymbol{\varepsilon}_i = \boldsymbol{\varepsilon}_j,$$

so that Q and $T_{1,2}$ generate a group isomorphic to S_{2m+1}. Moreover, it is easily verified that

$$Q^r T_{1,2} Q^{-r} = T_{r+1,r+2},$$

so that the operators $Q^r T_{1,2} Q^{-r}$, $r = 0, \cdots, 2m-1$ generate the matrix substitution group S_{2m} (i.e., the group of all substitution matrices of order $2m$).

The elements of CG corresponding to the index vectors $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ either commute or anti-commute according as the number of transpositions in rearranging

$$\gamma_1^{\alpha_1} \cdots \gamma_{2m}^{\alpha_{2m}} \gamma_1^{\beta_1} \cdots \gamma_{2m}^{\beta_{2m}} \text{ as } \gamma_1^{\beta_1} \cdots \gamma_{2m}^{\beta_{2m}} \gamma_1^{\alpha_1} \cdots \gamma_{2m}^{\alpha_{2m}}$$

is even or odd. There is a change of sign as $\gamma_i^{\beta_i}$ moves over $\gamma_j^{\alpha_j}$ if and only if $i \neq j$ and $\alpha_i \beta_j = 1$.

Thus the number of sign changes arising from moving $\gamma_1^{\beta_1}$ from right to left of $\Pi\gamma_i^{\alpha_i}$ is

$$\beta_1(\alpha_2 + \alpha_3 + \cdots + \alpha_{2m}) = \beta_1(\boldsymbol{\nu}^T + \boldsymbol{\varepsilon}_1^T)\boldsymbol{\alpha}.$$

The total number of sign changes is therefore

$$\begin{aligned}\sum_i \beta_i(\boldsymbol{\nu}^T + \boldsymbol{\varepsilon}_i^T)\boldsymbol{\alpha} &= \boldsymbol{\beta}^T(\boldsymbol{\nu}\boldsymbol{\nu}^T + \mathbf{1})\boldsymbol{\alpha} \\ &= \boldsymbol{\beta}^T\Gamma\boldsymbol{\alpha}.\end{aligned}$$

Thus the elements corresponding to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ commute or anti-commute according $\boldsymbol{\alpha}^T\Gamma\boldsymbol{\beta} = 0$ or 1 over $GF(2)$.

Now take a set of $2m$ elements of CG with index vectors $\boldsymbol{\alpha}_1, \cdots, \boldsymbol{\alpha}_{2m}$, and write A for the *index matrix* of the set;

$$A = [\boldsymbol{\alpha}_1,\ \boldsymbol{\alpha}_2, \cdots, \boldsymbol{\alpha}_{2m}].$$

The set is a Clifford set, if, for each i, j,

$$\boldsymbol{\alpha}_i^T\Gamma\boldsymbol{\alpha}_j = 1 \quad i \neq j.$$

Always

$$\boldsymbol{\alpha}_i^T\Gamma\boldsymbol{\alpha}_i = 0,$$

so that for a Clifford set $A^T\Gamma A = \Gamma$ over $GF(2)$.

Every Clifford set determines a matrix A with this property, and the condition that a given set should be a Clifford set is that its index matrix should satisfy this condition.

Suppose now A and B are matrices satisfying this condition, and that B is the index matrix of a Clifford set. Let A generate an automorphism of CG in which the element with index vector $\varkappa$ becomes the element with index vector $A\varkappa$. The vectors which are the columns of B are transformed into the columns of AB, which satisfy the condition $(AB)^T\Gamma(AB) = \Gamma$, so that AB is also the matrix of a Clifford set. A itself is the index matrix of the set into which the basic set (with index matrix $\mathbf{1}$) is transformed. Theorem 2 now follows.

By reading their columns as index vectors we see that the matrices Q, R correspond to the substitutions

$$Q(\chi_0) = \gamma_2, \gamma_3, \cdots, \gamma_{2m}, \gamma_{2m+1}, \gamma_1$$
$$R(\chi_0) = \gamma_1\gamma_2\gamma_3, \gamma_1\gamma_2\gamma_4, \gamma_1\gamma_3\gamma_4, \gamma_2\gamma_3\gamma_4, \gamma_5, \cdots, \gamma_{2m}, \gamma_{2m+1}.$$

Using the substitution we now derive some relations between Q and R and introduce certain products of Q and R which are needed in the proof of Theorem 1. First

THEOREM 3. *From Q and R we derive the $2m-2$ matrices*

$$R_1 = R,\ R_2 = QRQ^{-1}, \cdots, R_{r+1} = Q^rRQ^{-r},\ r = 0, \cdots, 2m-3,$$

where

$$R_{r+1} = \begin{bmatrix} \mathbf{1}_r & & \\ & R^0 & \\ & & \mathbf{1}_{2m-r-4} \end{bmatrix} \quad r = 0, \cdots, 2m-4$$

and

$$R_{2m-2} = \left[\begin{array}{c|ccc} \mathbf{1}_{2m-3} & \mathbf{0}_{2m-3} & \boldsymbol{\nu}_{2m-3} & \boldsymbol{\nu}_{2m-3} \\ \hline & 1 & 0 & 0 \\ & 1 & 0 & 1 \\ & 1 & 1 & 0 \end{array}\right]$$

Writing $ijk\cdots$ for $\gamma_i\gamma_j\gamma_k\cdots$, s' for $2m+2-s$, and r_i for $r+i$, we find that $R_{r+1} = Q^rRQ^{-r}$ generates the substitution:

$$\begin{array}{lcccccccccc} \chi_0: & 1 & 2 & \cdots & r & r_1 & r_2 & r_3 & r_4 & \cdots & 2' \ 1' \\ Q^rRQ^{-r}(\chi_0): & 1 & 2 & \cdots & r & r_1r_2r_3 & r_1r_2r_4 & r_1r_3r_4 & r_2r_3r_4 & \cdots & 2' \ 1' \end{array}$$

Thus in a symbol $ijk\cdots$ the only components changed by R_{r+1} are r_1, r_2, r_3, r_4. The complete set of involutory pairs is:

$$\begin{Bmatrix} r_1 & r_2 & r_3 & r_4 & r_1r_2 & r_1r_3 & r_1r_4 & r_2r_3 \\ r_1r_2r_3 & r_1r_2r_4 & r_1r_3r_4 & r_2r_3r_4 & r_3r_4 & r_2r_4 & r_1r_4 & r_2r_3 \end{Bmatrix}$$

For $R_{2m-2} = Q^{-4}R\,Q^4$ we have

$$\begin{array}{lcccccccc} \chi_0: & 1 & 2 & \cdots & 5' & 4' & 3' & 2' & 1' \\ R_{2m-2}\chi_0: & 1 & 2 & \cdots & 5' & 4'3'2' & 4'3'1' & 4'2'1' & 3'2'1'. \end{array}$$

The last three columns of the matrix correspond to $4'3'2'$, $4'3'1'$, $4'2'1'$ and are therefore $\varepsilon_{2m-2}+\varepsilon_{2m-1}+\varepsilon_{2m}$, $\varepsilon_{2m-2}+\varepsilon_{2m-1}+\nu$, $\varepsilon_{2m-2}+\varepsilon_{2m}+\nu$, which are the forms given in Theorem 3.

For the relation $(RQ)^{2m-1} = T_{1,3}$ we use

$$\begin{aligned}(RQ)^{2m-1} &= R(QRQ^{-1})(Q^2RQ^{-2}) \cdots (Q^{2m-2}RQ^{-m+2})Q^{-2} \\ &= R_1R_2 \cdots R_{2m-1}Q^{-2}.\end{aligned}$$

Writing out the successive stages in the substitution and using $c'' = 2r' - c$, we have

	1	2	3	$4 \cdots 2r' =$	$0''$	$\cdots$	$2'$	$1'$
Q^{-2}	$2'$	$1'$	1	$2 \cdots$	$2''$	$\cdots$	$4'$	$3'$
$R_{3'}$	$3'2'1'$	$3'1'1'$	$2'1'1'$	$2 \cdots$	$2''$	$\cdots$	$4'$	$3'2'1'$
$R_{4'}$	$3'2'1'$	$4'2'1'$	$4'3'1'$	$2 \cdots$	$2''$	$\cdots$	$4'3'2'$	$1'$
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
$R_{2r'}$	$1''2''1$	$0''2''1$	$0''1''1$	$2 \cdots$	$0''1''2''$	$\cdots$	$2'$	$1'$
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
R_2	341	241	231	$234 \cdots$	$0''$	$\cdots$	$2'$	$1'$
R_1	3	2	1	$4 \cdots$	$0''$	$\cdots$	$2'$	$1'$.

Thus $R_1R_2 \cdots R_{2m-1}(\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_{2m+1}) = (\gamma_3, \gamma_2, \gamma_1, \cdots, \gamma_{2m+1})$ which is the required result.

We have further

$$T_{1,3} = (RQ)^{2m-1} = ((RQ)^{2m-1})^{-1} = (Q^{-1}R)^{2m-1}$$

and

$$(QR)^{2m-1} = Q(RQ)^{2m-1}Q^{-1} = T_{2,4}.$$

The other relation

$$(RQ^2)^{2m-1} = T_{1,2}$$

may be proved similarly, using $(RQ^2)^{2m-1} = R_1 R_3 \cdots R_{2m+1} R_2 \cdots R_{2m-4}, Q^{-4}$, but the table is considerably more elaborate.

We are now in a position to prove Theorem 1, namely, that $\langle Q, R\rangle = A(2m, 2)$. We use as operators the matrices Q; $R_1, \cdots, R_{2m-2}$; T_{ij}, T_*, all of which have been proved to belong to $\langle Q, R\rangle$, and show how a given matrix A for which

$$A^T\Gamma A = \Gamma$$

can be reduced column by column to $\mathbf{1}_{2m}$, by multiplying on the left by these matrices. Since we have proved that the matrix substitution group S_{2m} is a subgroup of $\langle Q, R\rangle$, we may at any stage rearrange the rows of A by multiplying on the left by the appropriate substitution matrix T_*.

https://doi.org/10.1017/S1446788700025052 Published online by Cambridge University Press

Column 1

Let $\boldsymbol{\alpha}$ be the first column of A; we find a product X of matrices from $\langle Q, R\rangle$ such that $X\boldsymbol{\alpha} = \boldsymbol{\varepsilon}_1$.

(1) Assume that the number of 1's in $\boldsymbol{\alpha}$ is odd, i.e.,

$$\boldsymbol{\nu}^T\boldsymbol{\alpha} = 1$$

(i) If $\boldsymbol{\alpha} = \boldsymbol{\varepsilon}_i$, take $X = T_{1,i}$, then $X\boldsymbol{\alpha} = \varepsilon_1$.

(ii) If there are $2r-1$ zeros in $\boldsymbol{\alpha}$ $(r < m)$ rearrange the rows of A so that $\boldsymbol{\alpha}$ becomes:

$$T_*\boldsymbol{\alpha} = \overline{\boldsymbol{\alpha}} = [\mathbf{0}_{2r-1}, \boldsymbol{\nu}_{2m-2r+1}]$$

we have

$$R_{2r-1}\overline{\boldsymbol{\alpha}} = \begin{bmatrix} \mathbf{1}_{2r-2} & & \\ & \begin{matrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{matrix} & \\ & & \mathbf{1}_{2m-2r-2} \end{bmatrix} \begin{bmatrix} \mathbf{0}_{2r-2} \\ 0 \\ 1 \\ 1 \\ 1 \\ \boldsymbol{\nu}_{2m-2r-2} \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{2r-2} \\ 0 \\ 0 \\ 0 \\ 1 \\ \boldsymbol{\nu}_{2m-2r-2} \end{bmatrix}$$

i.e. $R_{2r-1}\overline{\boldsymbol{\alpha}} = [\mathbf{0}_{2r+1}, \boldsymbol{\nu}_{2m-2r+1}]$. Similarly

$$R_r^*\overline{\boldsymbol{\alpha}} = R_{2m-3}R_{2m-5}\cdots R_{2r-1}\overline{\boldsymbol{\alpha}} = \boldsymbol{\varepsilon}_{2m},$$

so that, if

$$X = T_{1,2m}R_r^*T_*,$$

then

$$X\overline{\boldsymbol{\alpha}} = \boldsymbol{\varepsilon}_1.$$

(2) Assume that $\boldsymbol{\nu}^T\boldsymbol{\alpha} = 0$.

(i) If $\boldsymbol{\alpha} = \boldsymbol{\nu}$, then $Q\boldsymbol{\alpha} = \boldsymbol{\varepsilon}_1$, i.e., $X = Q$.

(ii) If $\boldsymbol{\alpha}$ contains $2s$ 0's find a T_* such that

$$T_*\boldsymbol{\alpha} = \overline{\boldsymbol{\alpha}} = [\boldsymbol{\nu}_{2m-2s-1}, \mathbf{0}_{2s}, 1].$$

Then

$$R_{2m-2}\overline{\boldsymbol{\alpha}} = [\mathbf{0}_{2m-s-1}, \boldsymbol{\nu}_{2s-2}, 0, 1, 0]$$

and therefore, for another suitable T_*,

$$T_*R_{2m-2}T_*\boldsymbol{\alpha} = [\mathbf{0}_{2m-2+1}, \boldsymbol{\nu}_{2s-1}].$$

We may now proceed as in (1) (ii) to find the required X.

Column r

Suppose the first $r-1$ columns have been transformed, so that

$$YA = A_{r-1} = [\boldsymbol{\varepsilon}_1, \cdots, \boldsymbol{\varepsilon}_{r-1}, \boldsymbol{\varkappa}, \boldsymbol{\lambda}_{r+1}, \cdots, \boldsymbol{\lambda}_{2m}].$$

We are to construct $Z, \in \langle Q, R\rangle$, such that

$$ZA_{r-1} = A_r = [\varepsilon_1, \cdots \varepsilon_r, \mu_{r+1}, \cdots, \mu_{2m}].$$

Since $A_{r-1}^T \Gamma A_{r-1} = \Gamma$, from the first $r-1$ rows of A_{r-1}^T in conjunction with the rth column of A_{r-1}, we find:

$$1 = (\nu^T + \varepsilon_i^T)\varkappa = \nu^T\varkappa + \varkappa_i, \quad i = 1, \cdots, r-1.$$

$$\kappa_1 = \kappa_2 = \cdots = \kappa_{r-1} = 1, \text{ if } \nu^T\varkappa = 0$$
$$= 0, \text{ if } \nu^T\varkappa = 1.$$

1. Suppose $\kappa_i = 0$, $\nu^T\varkappa = 1$, so that

$$\varkappa = [\mathbf{0}_{r-1}, \kappa_r, \kappa_{r+1}, \cdots, \kappa_{2m}].$$

Rearrange the elements of $\varkappa$, so that

$$T_*\varkappa = [\mathbf{0}_{r-1}, \mathbf{0}_{2s-r}, \nu_{2m-2s+1}]$$

(i) If $2s - r > 0$, then, as in the first column,

$$R_{2m-3}R_{2m-5}\cdots R_{2s+1}T_*\varkappa = \varepsilon_{2m},$$

so that

$$Y\varkappa = T_{r,2m}R_{2m-3}\cdots R_{2s+1}T_*\varkappa = \varepsilon_r.$$

The first $r-1$ columns of each of the factors of Y are $\varepsilon_1, \cdots, \varepsilon_{r-1}$, so that Y does not disturb the columns of A_{r-1} which have already been reduced.

(ii) If $2s - r = 0$, so that $\varkappa = [\mathbf{0}_{2s-1}, \nu_{2m-2s+1}]$ multiply first by R_{2m-2}, thus

$$R_{2m-2}\varkappa = [\mathbf{0}_{2s-1}, \nu_{2m-2s-1}, 0, 0]$$

and

$$T_*R_{2m-2}\varkappa = [\mathbf{0}_{2s+1}, \nu_{2m-s-1}].$$

We may now proceed as in 1(i).

2 Suppose $\varkappa = [\nu_{r-1}, \kappa_r, \kappa_{r+1}, \cdots, \kappa_{2m}]$.

(i) If there are no zero components, so that $\varkappa = \nu_{2m}$, then

$$Q[\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{r-1}, \nu_{2m}] = [\varepsilon_2, \varepsilon_3, \cdots, \varepsilon_r, \varepsilon_1].$$

Use T_* to permute these cyclically into the proper order.

(ii) The number of zero components is even, suppose it is $2m - 2s > 0$. Find T_* operating on rows r to $2m$, such that

$$T_*\varkappa = [\nu_{r-1}, \nu_{2s-r}, \mathbf{0}_{2m-2s}, 1]$$

Then

$$R_{2m-2}T_*\varkappa = [\mathbf{0}_{2s-1}, \nu_{2m-2s-2}, 0, 1, 0].$$

Find T_* such that

$$T_*R_{2m-2}T_*\varkappa = [\mathbf{0}_{2s+1}, \nu_{2m-2s-1}]$$

and proceed as in 1(i).

Thus in all cases, $r = 2, 3, \cdots, 2m-3$ if the first $r-1$ columns are $\varepsilon_1, \cdots, \varepsilon_{r-1}$, we can reduce the rth column to ε_r by matrices belonging to

https://doi.org/10.1017/S1446788700025052 Published online by Cambridge University Press

$\langle Q, R\rangle$, this provision, $r \leqq 2m-3$, being necessary on account of the form of R_{2m-2}.

For the last three columns we have, as at the rth column,

either $\kappa_1 = \kappa_2 = \cdots = \kappa_{2m-3} = 1,\ \kappa_{2m-2} + \kappa_{2m-1} + \kappa_{2m} = 1$

or $\kappa_1 = \kappa_2 = \cdots = \kappa_{2m-3} = 0,\ \kappa_{2m-2} + \kappa_{2m-1} + \kappa_{2m} = 1.$

We consider the possible cases separately, and suppose that where necessary a transposition of the last three rows has been effected to give the form named:

Column $2m-2$

$\boldsymbol{\varkappa} = [\boldsymbol{\nu}_{2m-3},\ 0,\ 0,\ 1] : T_{2m-2,\, 2m-1} R_{2m-2} \boldsymbol{\varkappa} = \boldsymbol{\varepsilon}_{2m-2}$

$\boldsymbol{\varkappa} = [\boldsymbol{\nu}_{2m-3},\ 1,\ 1,\ 1] = \boldsymbol{\nu} : Q[\boldsymbol{\varepsilon}_1,\ \boldsymbol{\varepsilon}_2, \cdots, \boldsymbol{\varepsilon}_{2m-3},\ \boldsymbol{\nu}] = [\boldsymbol{\varepsilon}_2,\ \boldsymbol{\varepsilon}_3, \cdots, \boldsymbol{\varepsilon}_{2m-2},\ \boldsymbol{\varepsilon}_1]$

Cyclically permute as in 2(i) above.

$\boldsymbol{\varkappa} = [\mathbf{0}_{2m-3},\ 1,\ 0,\ 0] = \boldsymbol{\varepsilon}_{2m-2}.$

$\boldsymbol{\varkappa} = [\mathbf{0}_{2m-3},\ 1,\ 1,\ 1] : T_* R_{2m-2} \boldsymbol{\varkappa} = \boldsymbol{\varepsilon}_{2m-2}.$

Column $2m-1$

$\boldsymbol{\varkappa} = [\boldsymbol{\nu}_{2m-2},\ 1,\ 1] = \boldsymbol{\nu}$: reduce as above.

$\boldsymbol{\varkappa} = [\mathbf{0}_{2m-2},\ 1,\ 0] = \boldsymbol{\varepsilon}_{2m-1}$

Column $2m$

$\boldsymbol{\varkappa} = [\boldsymbol{\nu}_{2m},\ 1] = \boldsymbol{\nu}$: reduce as above.

$\boldsymbol{\varkappa} = [\mathbf{0}_{2m-1},\ 1] = \boldsymbol{\varepsilon}_{2m}.$

The reduction is therefore complete.

Γ itself belongs to $A(2m, 2)$, since $\Gamma^2 = \mathbf{1}$, $\Gamma = \Gamma^T$, so that $\Gamma^T \Gamma \Gamma = \Gamma$. To express Γ as a member of $\langle Q, R\rangle$ we may apply the simple process **1 (i)** to column 1, and inductively to succeeding columns, thus:

$$R_{2m-3} R_{2m-5} \cdots R_3 R_1 \Gamma = \begin{bmatrix} \mathbf{0}_{2m-2} & \mathbf{0}_{2m-2} & \Gamma_{2m-2} \\ 0 & 1 & \mathbf{0}^T_{2m-2} \\ 1 & 0 & \mathbf{0}^T_{2m-2} \end{bmatrix}$$

By repetition, with one fewer factor each time, we may reduce Γ by means of

$$R_1(R_3 R_1)(R_5 R_3 R_1) \cdots (R_{2m-3} R_{2m-5} \cdots R_3 R_1)$$

to $[\boldsymbol{\varepsilon}_{2m},\ \boldsymbol{\varepsilon}_{2m-1}, \cdots, \boldsymbol{\varepsilon}_2,\ \boldsymbol{\varepsilon}_1]$.

But

$$\begin{aligned} R_{2r-1} R_{2r-3} \cdots R_3 R_1 &= Q^{2r-2} R Q^{-2} R Q^{-2} \cdots Q^{-2} R Q^{-2} R \\ &= Q^{2r} (Q^{-2} R)^r. \end{aligned}$$

Thus, after inverting the product,

https://doi.org/10.1017/S1446788700025052 Published online by Cambridge University Press

$$\Gamma = (RQ^2)^{m-1}Q^3(RQ^2)^{m-2}Q^5 \cdots (RQ^2)^2Q^{2m-3}RT_{1,2m}T_{2,2m-1}\cdots T_{mm+1}.$$

Finally it is to be proved that S_{2m+2} is a subgroup of $A(2m, 2)$; explicitly:

THEOREM 4. *$\langle Q, \Gamma\rangle$ is isomorphic to S_{2m+2}.*

Denote by χ_0 the basic complete Clifford set $\gamma_1, \cdots, \gamma_{2m+1}$ and define a sequence $\chi_1, \chi_2, \cdots, \chi_{2m+1}$ of complete Clifford sets thus:

$$\chi_{2m+1} = \Gamma(\chi_0) = (\gamma_1\gamma_{2m+1}, \gamma_2\gamma_{2m+1}, \cdots, \gamma_{2m}\gamma_{2m+1}, \gamma_{2m+1})$$
$$\chi_r = Q^r(\chi_{2m+1}) = (\gamma_r\gamma_{r+1}, \gamma_r\gamma_{r+1}, \cdots, \gamma_r\gamma_{2m+1}, \gamma_r\gamma_1, \cdots \gamma_r\gamma_{r-1}, \gamma_r)$$

It is to be shown that the operators $\langle Q, \Gamma\rangle$ generate the permutations of the sets $\chi_0, \cdots, \chi_{2m+1}$ (the order of the members of a set being disregarded). Thus, writing only the subscripts of the χ_i, we find the following permutations

0	1	2	$\cdots$	$2m$	$2m+1$
$Q: 0$	2	3	$\cdots$	$2m+1$	1
$\Gamma: 2m+1$	1	2	$\cdots$	$2m$	0

So that either $\langle Q, \Gamma\rangle$ is isomorphic to S_{2m+2}, or contains it as a subgroup, in which case some matrices of $\langle Q, \Gamma\rangle$ would permute the members of various sets χ_i, while leaving each set as a whole unchanged. But a permutation of χ_0 which interchanges γ_i and γ_j necessarily interchanges the sets χ_i and χ_j. It follows that S_{2m+2} is isomorphic to the whole group.

It may be noted that Q and $Q\Gamma Q^{-1}$ are formally the same as matrices Q and D of Room and Smith [2], which are used to generate $A(2m, p)$ in the cases $p > 2$.

References

[1] Dickson, L. E., *Linear Groups*, Teubner, (1901).
[2] Room and Smith, A generation of the Symplectic Group, *Quart. Journ. Math.* (2) 9, (1958), 177–182.

University of Sydney

https://doi.org/10.1017/S1446788700025052 Published online by Cambridge University Press