ORBITS UNDER SYMPLECTIC TRANSVECTIONS I

RONALD BROWN *and* STEPHEN P. HUMPHRIES

[Received 17 January 1984—Revised 25 June 1985]

Dedicated to the memory of Peter Stefan

Introduction

Let V be a symplectic space over a field K with alternating bilinear form $(x, y) \mapsto x.y$, for x, y in V. Let $Sp_0(V)$ be the group of strict isometries of V, that is, the isometries of V which are the identity on $\mathrm{rad}(V) = \{x \in V\colon x.V = 0\}$. Particular examples of such isometries are the well-known transvections $A^k\colon x \mapsto x + k(a.x)a$, defined by an element $a \in V$ and $k \in K$. If $S \subset V$ then we define $Tv(S)$ to be the subgroup of $Sp_0(V)$ generated by the transvections A^k for all $a \in S$ and $k \in K$. We assume throughout that $V\backslash\mathrm{rad}(V)$ is non-empty, and that V is finite-dimensional.

Also associated with the subset S of V is a graph $G(S)$, which has vertices the elements of S and an edge between vertices a and b if and only if $a.b \neq 0$ or equivalently, if and only if A^1 and B^1 do not commute. Note that if K has only two elements, and S is a basis for V, then $G(S)$ determines the form on V.

The object of this paper and its sequel [**3**] is to develop techniques for studying the orbits of the action of $Tv(S)$ on $V\backslash\mathrm{rad}(V)$ in terms of properties of the graph $G(S)$. Essentially this idea was used in [**9**] to prove that the minimum number of twist generators of the mapping class group M_g is greater than $2g$. We return to this type of application towards the end of [**3**].

Consider the following conditions on a subset S of $V\backslash\mathrm{rad}(V)$:

(A) *$Tv(S)$ acts transitively on* $V\backslash\mathrm{rad}(V)$;

(B) $Tv(S) = Sp_0(V)$;

(C) *S spans V and the graph $G(S)$ is connected.*

We first establish in §2 that

$$(A) \Leftrightarrow (B) \Rightarrow (C).$$

This is not difficult. The principal result of this paper is that if K has more than two elements, then (C) $\Rightarrow$ (B).

In the case where the symplectic space V is regular (i.e. when $\mathrm{rad}(V) = \{0\}$) this result may be deduced from results of McLaughlin [**16**], as was pointed out to us in a private communication by W. Kantor. The reason for considering the non-regular case is that regularity is not preserved by taking either subspaces or extensions of a regular symplectic space, where by an extension of V is meant a symplectic space V' together with a linear surjection $p\colon V' \to V$ preserving the forms. This extension process will be found a useful tool in this and the following paper and so it will be discussed in detail in §6. In particular we obtain relationships between $Tv(S')$ and $Tv(S)$ when S' is a subset of V' and $p(S') = S$.

The key methods of this paper, which will also prove essential in the sequel, are given in §§3 and 4. Given $S \subset V$, the process of *t-equivalence*, defined in §3, changes S but not $Tv(S)$ nor the number of components of $G(S)$; however, if S is finite, there is a t-equivalence from S to S' such that $G(S')$ is a forest (Theorem 3.3).

A.M.S. (1980) subject classification: 20 H 20, 51 F 99.
Proc. London Math. Soc. (3), 52 (1986), 517-531.

Suppose that S is a basis for V, and $x \in V$. The support (or graph) of x is the full subgraph of $G(S)$ with vertices those elements of S occurring with non-zero coefficient in the expression of x in terms of the basis S. This support will be written $x\,|_S$ or simply $x\,|$. If $G(S)$ is a forest, so also is $x\,|$, and it is proved in §4 that x can be transformed by $Tv(S)$ to an element y such that $y\,|$ is discrete and has no more components than does $x\,|$. The basic technique in the case where $G(S)$ is a tree is then to act on such a y by $Tv(S)$ so as to decrease the number of components of $y\,|$, by moving the components (vertices) of $y\,|$ around $G(S)$.

In this paper we show that if K has more than two elements, y is not radical, and $G(S)$ is a tree, then we can reduce the number of components of $y\,|$ to one. This will prove (for $K \neq \mathbf{F}_2$) our implication (C) ⇒ (B) in the case when S is a basis. The general case is obtained by applying an extension process developed in §6.

The case when K has only two elements is more complicated, but more interesting, since even under assumption (C) there is more than one orbit. In the sequel we describe these orbits and give conditions for $Tv(S)$ to be equal to $Sp_0(V)$. It is the necessity of developing techniques appropriate to the case $K = \mathbf{F}_2$ which makes us not attempt (what might be possible) a direct deduction of (C) ⇒ (B), for the case where $K \neq \mathbf{F}_2$, from the results of [**16**] for the regular case. The novelty of the methods has also necessitated a complete and not too terse exposition.

Our methods, though new, are elementary, and we have written this paper so that little knowledge of symplectic algebra is required by the reader. Some background to the literature on transvections is given at the end of this paper.

The genesis of this paper and its sequel is as follows. The ideas leading to [**9**] were developed while S. P. Humphries was a research student at Bangor in 1974–77 under the supervision of Dr P. Stefan, and the basic scheme of this paper and its sequel was worked out by Humphries in 1977–78. Peter Stefan died tragically in a mountaineering accident in June 1978, and R. Brown then became involved as supervisor. The material of this paper forms a revised version of Chapter 3 of [**10**], and the main results were announced in [**11**].

2. *Symplectic spaces and graphs of subsets*

Let V be a symplectic space over the field K. A basis of the form $e_1, \ldots, e_n, f_1, \ldots, f_n$ where $e_i . e_j = f_i . f_j = 0$, $e_i . f_j = -f_j . e_i = \delta_{ij}$ for $i, j = 1, \ldots, n$ is known as a *symplectic basis* for V. If such exists, then V is regular. Conversely, any regular V has such a basis, and so any two regular symplectic spaces are isometric if and only if they have the same dimension. For all V the space $V/\operatorname{rad}(V)$ inherits from V a regular symplectic structure, and if U is a complementary subspace in V of $\operatorname{rad}(V)$, then the form is regular on U. These results may be found in [**2**].

As explained in the Introduction, the transvections on V are the linear mappings $A^k\colon x \mapsto x + k(a.x)a$, for a given $a \in V$ and $k \in K$. Note that $A^k A^h = A^{k+h}$, and that A^k is a strict isometry. We abbreviate A^1 to A, and call A^k a *power* of A. If $k \neq 0$, then A^k is the identity if and only if $a \in \operatorname{rad}(V)$. If α is a product of powers of transvections $A_1, \ldots, A_r$ and $x \in V$, then $\alpha(x)$ belongs to the subspace of V spanned by x and $a_1, \ldots, a_r$. Another easily verified and useful fact is that if θ is an isometry of V and $b = \theta(a)$, then

$$B^k = \theta A^k \theta^{-1}.$$

Let S be a subset of V. We now continue the methods initiated in [**9**] to study the groups $Sp_0(V)$ and $Tv(S)$ via properties of the graph $G(S)$. We are particularly interested in the orbits of the action of $Tv(S)$.

PROPOSITION 2.1. *Under the action of $Tv(S)$ on V, two elements of S lie in the same orbit if and only if they lie in the same component of $G(S)$.*

Proof. Let a and b be members of S and assume $a \neq b$.

If $a.b \neq 0$ then $A^kB^k(a) = b$ where $k = (b.a)^{-1}$. So if a and b are adjacent in $G(S)$ they lie in the same orbit of $Tv(S)$. Thus if a and b lie in the same component of $G(S)$ they lie in the same orbit of $Tv(S)$.

Suppose conversely that a and b lie in the same orbit of $Tv(S)$. Then there are a sequence of distinct elements $b_1 = a, b_2, \dots, b_{r+1} = b$, of V, and elements $a_1, \dots, a_r$ of S, $k_1, \dots, k_r$ of K such that $b_{i+1} = A_i^{k_i}(b_i)$, for $i = 1, \dots, r$. Since $b_{i+1} \neq b_i$, a_i is adjacent to at least one of $b_1, a_1, \dots, a_{i-1}$. It follows by induction that $a_1, \dots, a_i$ lie in the same component of $G(S)$ as a, for $i = 1, \dots, r$. But $b_r = A_r^{-k_r}(b) \neq b$. So a_r is adjacent to b, and so a and b lie in the same component of $G(S)$.

COROLLARY 2.2. *The set S is contained in a single orbit of the action of $Tv(S)$ on V if and only if $G(S)$ is connected.*

The following (essentially well-known) result gives the largest subset of V with $G(S)$ connected.

PROPOSITION 2.3. *The graph $G(V\backslash\mathrm{rad}(V))$ is connected.*

Proof. Let $x, y \in V\backslash\mathrm{rad}(V)$. If $x.y \neq 0$ then x and y are adjacent in $G(V\backslash\mathrm{rad}(V))$. Suppose $x.y = 0$. Then we can find z adjacent to both x and y as follows. The annihilator x^* of x in V is a hyperplane, as $x \notin \mathrm{rad}(V)$. If $x^* = y^*$ then choose z not in x^*.

If $x^* \neq y^*$ then choose $u \in x^*\backslash y^*$, $v \in y^*\backslash x^*$ and set $z = u+v$.

COROLLARY 2.4. *The group $Tv(V)$ acts transitively on $V\backslash\mathrm{rad}(V)$.*

The above corollary is well known: for the regular case see [**2**, p. 138] and for the non-regular case with K of characteristic not 2 see [**20**].

PROPOSITION 2.5. *If $V\backslash\mathrm{rad}(V) \neq 0$ and $Tv(S) = Tv(V)$, then S spans V.*

Proof. Since $V\backslash\mathrm{rad}(V) \neq 0$, the group $Tv(V)$ is non-trivial. Since also $Tv(S) = Tv(V)$, there is an element $a \in S\backslash\mathrm{rad}(V)$.

Let $x \in V$. If x is not contained in $\mathrm{rad}(V)$ then Corollary 2.4 gives an element α of $Tv(V)$ such that $\alpha(a) = x$. Then α also belongs to $Tv(S)$ and so $x \in \langle S\rangle$ (the subspace spanned by S).

Suppose $x \in \mathrm{rad}(V)$. Then $a+x \notin \mathrm{rad}(V)$ and so $a+x \in \langle S\rangle$. Hence, again, $x \in \langle S\rangle$.

It is proved in Theorem 3.25 of [**2**] that if V is regular, then $Tv(V) = Sp(V)$. We now show how the same type of proof extends to the non-regular case.

PROPOSITION 2.6. *The group $Sp_0(V)$ is generated by transvections, that is, $Sp_0(V) = Tv(V)$.*

Proof. Choose a splitting $V = U \oplus \mathrm{rad}(V)$ and a symplectic basis $B = \{e_1, f_1, \ldots, e_n, f_n\}$ for the regular symplectic space U. Let $\theta \in Sp_0(V)$ and suppose θ is the identity on $B_r = \{e_1, f_1, \ldots, e_r, f_r\}$, where $0 \leqslant r < n$. Let U_r be spanned by B_r, and let V_r be spanned by $\mathrm{rad}(V)$ and $B \backslash B_r$. Then $U_r . V_r = \{0\}$. Hence $U_r . \theta V_r = 0$, and so $\theta V_r \subset V_r$. By Corollary 2.4, there is an element α of $Tv(V_r)$ such that $\alpha\theta e_{r+1} = e_{r+1}$. Let $x = e_{r+1}$, $y = f_{r+1}$, $z = \alpha\theta f_{r+1}$. If $y.z \neq 0$, $k = (y.z)^{-1}$, $a = z - y$, then $A^k z = y$, $A^k x = x$. If $y.z = 0$, let $b = x + y$. Then $x.b = 1$, $b.z \neq 0$, $b.y \neq 0$, and so we can move z to b and then to y keeping x fixed. Hence there is $\beta \in Tv(V_r)$ such that $\beta\theta$ leaves B_{r+1} fixed.

It follows by induction that there is a $\gamma \in Tv(V)$ such that $\gamma\theta$ leaves B_n fixed. But $\gamma\theta$ is also fixed on $\mathrm{rad}(V)$. So $\gamma\theta = 1$, and the proof is complete.

Remarks. 1. This proposition was noted in [**20**, p. 153] for the case in which K is of characteristic not 2.

2. It is easy to show that there is a split exact sequence

$$1 \to Sp_0(V) \to Sp(V) \to \mathrm{GL}(\mathrm{rad}(V)) \to 1.$$

We now summarize our results so far.

Theorem 2.7. *Let S be a non-empty subset of $V \backslash \mathrm{rad}(V)$. Consider the following conditions on S:*

(A) *$Tv(S)$ acts transitively on $V \backslash \mathrm{rad}(V)$;*

(B) *$Tv(S) = Sp_0(V)$;*

(C) *S spans V and $G(S)$ is connected.*

Then (A) $\Leftrightarrow$ (B) $\Rightarrow$ (C).

Proof. (A) $\Rightarrow$ (B). Since $Tv(V) = Sp_0(V)$, it is sufficient to show that if $x \in V \backslash \mathrm{rad}(V)$ and $k \in K$, then $X^k \in Tv(S)$. By (A) there are $a \in S$ and $\alpha \in Tv(S)$ with $\alpha(a) = x$. But then $X^k = \alpha A^k \alpha^{-1}$, and so $X^k \in Tv(S)$.

(B) $\Rightarrow$ (A). This follows immediately from Corollary 2.4 since (B) and Proposition 2.6 imply that $Tv(S) = Tv(V)$.

(B) $\Rightarrow$ (C). This follows from Corollaries 2.2 and 2.4 and Proposition 2.5.

Because of Theorem 2.7 we shall rarely consider the case where $G(S)$ is not connected. However in this case we have:

Proposition 2.8. *Let S be a spanning set for V such that S is the union $S_1 \cup \ldots \cup S_r$ of non-empty subsets S_j such that $S_i . S_j = 0$ for $i \neq j$, $i, j = 1, \ldots, r$. Then $Tv(S)$ is the direct product of the subgroups $Tv(S_1), \ldots, Tv(S_r)$.*

Proof. Clearly the subgroups $Tv(S_1), \ldots, Tv(S_r)$ generate $Tv(S)$, and if $i \neq j$ then the elements of $Tv(S_i)$ commute with all the elements of $Tv(S_j)$, since $S_i . S_j = 0$. Let L_i be the subgroup of $Tv(S)$ generated by all the $Tv(S_j)$ for $j \neq i$, and let $\alpha \in L_i \cap Tv(S_i)$. Then α leaves each member of S_i fixed (since $\alpha \in L_i$), and α fixes each element of S_j (since $\alpha \in Tv(S_i)$ and $S_i . S_j = 0$). Since S spans V it follows that $\alpha = \mathrm{id}$.

3. *t-equivalence*

In studying $Tv(S)$ we try to change S so as to simplify $G(S)$ without changing $Tv(S)$.

Definition. Let S and S' be subsets of the symplectic space V. A surjection $f\colon S \to S'$ is called an *elementary t-equivalence* if there are elements a, b of S and k of K

such that

$$f(x) = \begin{cases} x & \text{if } x \neq b, \\ A^k(b) & \text{if } x = b. \end{cases}$$

We denote such an f by t^k_{ab}. Note that if S is a linearly independent set, then an elementary t-equivalence is a bijection. The relation *t-equivalence* between subsets of V is the equivalence relation generated by the relation 'there exists an elementary t-equivalence'.

We apply the term t-equivalence not only to subsets of V but also to the corresponding graphs.

PROPOSITION 3.1. *If S and S' are t-equivalent subsets of V, then $Tv(S) = Tv(S')$.*

Proof. It clearly suffices to consider an elementary t-equivalence t^k_{ab}: $S \rightarrow S'$. Let $c = A^k(b)$. Then $C^h = A^kB^hA^{-k}$ for $h \in K$, and it follows that $Tv(S) = Tv(S')$.

PROPOSITION 3.2. *A t-equivalence t: $S \rightarrow S'$ induces a bijection $\pi_0(G(S)) \rightarrow \pi_0(G(S'))$ of the sets of components of the corresponding graphs.*

Proof. It will be sufficient to consider the case where $t = t^k_{ab}$.

Suppose that x, y in S are joined by a path p in $G(S)$. If p does not pass through b, or if $a.b = 0$, then p is a path in $G(S')$. Suppose that $a.b \neq 0$ and p contains successive vertices d, b, e. Let $b' = t(b)$. Figure 1 shows the known adjacencies in $G(S)$ and $G(S')$.

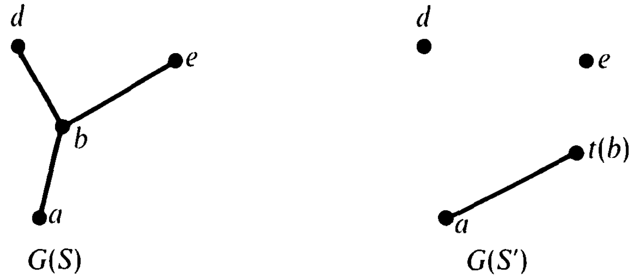

FIG. 1

We now show that d can be joined to b' in $G(S')$. If $d.b' \neq 0$ then this is clearly so. Suppose $d.b' = 0$. Then $d.(b+k(a.b)a) = 0$ and we see that $d.a \neq 0$, since $d.b \neq 0$. So d, a, b' are successive vertices of a path in $G(S')$. Similarly b' may be joined to e in $G(S')$. So tx may be joined to ty in $G(S')$.

If t is a bijection, then $t^{-1} = t^{-k}_{ab}$. If t is not a bijection then $b' \in S\backslash\{b\}$. In either case, points x, y are joined in $G(S)$ if and only if tx, ty are joined in $G(S')$.

Our main result on t-equivalence is the following:

THEOREM 3.3. *If S is a finite subset of a symplectic space V, then S is t-equivalent to a subset S' such that $G(S')$ is a forest.*

Proof. By Proposition 3.2 it is sufficient to assume that $G(S)$ is connected, and to prove that S is t-equivalent to S' where $G(S')$ is a tree. We use the following lemma:

LEMMA. *Let $a \in S$ and let C be a component of $G(S\backslash\{a\})$. Then there is a t-*

equivalence $C \to C'$ such that a is adjacent to at most one vertex of C'. Further C' is a component of $G(S' \backslash \{a\})$.

Proof. For any graph Γ and vertices b, c of Γ, let $\delta_\Gamma(b, c)$ denote the distance from b to c in Γ.

Let A be the set of pairs (b, c) in $C \times C$ such that $b \neq c$ and a is adjacent to both b and c. If A is empty there is at most one edge from a to C and we have finished. Suppose that A is not empty and let $\mu(C)$ be the minimum distance $\delta_C(b, c)$ for pairs (b, c) in A.

Suppose $\mu(C) = 1$. Then there is a pair (b, c) in A such that $b.c \neq 0$. Let $k \in K$ satisfy $a.c + k(b.c)(a.b) = 0$. Then in $G(t^k_{bc}(S))$, $t^k_{bc}(C)$ has one less edge to a than does C.

Thus if $\mu(C) = 1$ then we can reduce the number of edges from a to C.

Now suppose $\mu(C) > 1$. Choose $(b, c) \in A$ so that $\delta_C(b, c) = \mu(C)$, and let $u_1 = b$, $u_2, \ldots, u_r = c$ be the vertices along a minimal path in C from b to c. Then $a.u_2 = 0$ by the two minimality conditions. Let $b' = U_2(b)$. Then $b'.a \neq 0$ and $b'.u_3 \neq 0$ as in Fig. 2. So we change S to $S' = t_{u_2 b}(S)$ and C to $C' = t_{u_2 b}(C)$ so that $\mu(C') < \mu(C)$, the set A remaining unaltered. In this way we may reduce to the case where $\mu(C) = 1$.

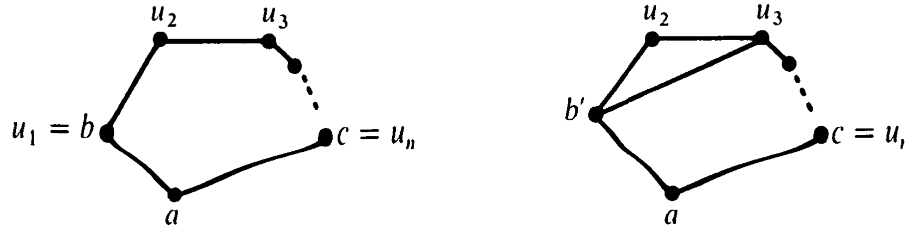

FIG. 2

The final part of the lemma follows from Proposition 3.2.

By repeated application of the above lemma we can find a t-equivalence $f\colon S \to S'$, not changing a, and such that each component C_i of $G(S' \backslash \{a\})$ is joined to a by exactly one edge, from a to a_i, say, for $i = 1, \ldots, r$. The lemma may now be applied to $a_1, \ldots, a_r$. Continuing in this way reduces S to a tree.

DEFINITION. Let $a, b \in S$. We say *a is similar to b in S* if there is a non-zero $h \in K$ such that $(a - hb).S = \{0\}$. We write this relation as $a \simeq_S b$; it is clearly an equivalence relation.

Note that if $a \simeq_S b$, then $a.b = 0$ and for all $c \in S$, $a.c = 0$ if and only if $b.c = 0$. The converse of this statement holds if $K = \mathbf{F}_2$. Thus if $a \simeq_S b$, then a and b are not adjacent in $G(S)$, but have the same adjacency relations in $G(S)$.

The following proposition will be particularly useful in the sequel to this paper, where we require a finer analysis than here of the kinds of trees which arise in a t-equivalence class. However, we give the result here since it is valid for all fields.

PROPOSITION 3.4. *Let S be a linearly independent, connected subset of $V \backslash \mathrm{rad}(V)$. Let a, c be distinct elements of S and suppose there is an element b of S, distinct from a, such that b is similar in S to a. Then there is a t-equivalence $f\colon S \to S'$ which alters only a and is such that fa is similar in S' to c.*

Proof. Suppose first that $c.a \neq 0$, and let $k = (c.a)^{-1}$. Then operating by t_{ca}^{k} fixes $S\backslash\{a\}$ and sends a to $u = a+c$. Since $a \simeq_S b$, there is a non-zero h in K such that $(a-hb).S = \{0\}$. Also $b.u = b.c \neq 0$ since $c.a \neq 0$. So, operating by t_{bu} fixes $S\backslash\{u\}$ and sends u to

$$v = a+c+h^2k(b.c)b = a+c+hk(a.c)b = a-hb+c.$$

Hence $(v-c).S' = \{0\}$ where S' is obtained from S by changing a to v. Note also that $a-hb \neq 0$ since S is linearly independent and so $v \neq c$.

If $c.a = 0$, then a, c are joined by a path $a = c_1, c_2, \ldots, c_r = c$ in $G(S)$. We now use the above process after the first step replacing b in turn by $c_1, c_2, \ldots, c_{r-1}$ to make a similar in turn to $c_2, c_3, \ldots, c_r = c$.

Typical applications of Proposition 3.4 give, in the case $K = \mathbf{F}_2$ and for the pairs of graphs shown in Fig. 3, t-equivalences f such that f maps a to v and leaves all other vertices fixed.

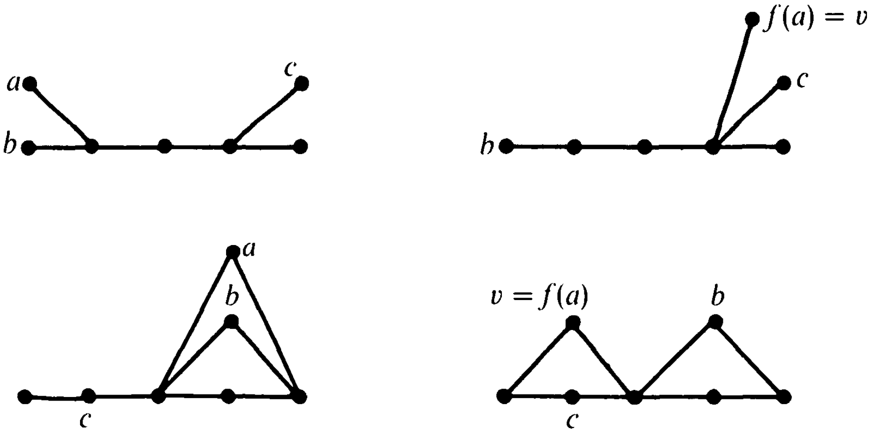

FIG. 3

EXAMPLES. Let $S = \{e_1, \ldots, e_n\}$ be a basis of the symplectic space V over $\mathbf{F}_2$. We consider here some representatives of t-equivalence classes of connected graphs. By Theorem 3.3, we may assume $G(S)$ is a tree.

A simple tree with S as vertices is the line graph L_n, with e_i adjacent to e_{i+1} for $i = 1, \ldots, n-1$ and no other adjacencies. This gives all trees for $n = 1, 2$, and 3.

In [3] we will also deal with the *blown up line graph* L_n^m in which $\{e_1, \ldots, e_n\}$ forms a line graph L_n, and $d_1, \ldots, d_m$ are adjacent only to e_{n-1}.

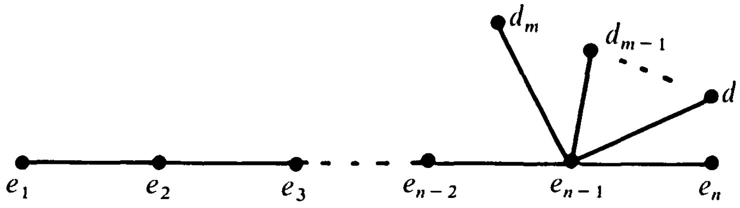

FIG. 4

The symplectic forms of L_3^1 and L_4 have rank 2 and 4 respectively, so the graphs cannot arise from the same symplectic space (and hence are not t-equivalent). However the forms of L_4^1 and L_5 both have rank 4, and so we introduce another invariant to prove these are not t-equivalent.

Let S be a connected subset of V. By Corollary 2.2, the number of elements in the orbit of $a \in S$ under the action of $Tv(S)$ is independent of the choice of $a \in S$; we write this number as $N(S)$. If S is t-equivalent to S', then $Tv(S) = Tv(S')$ by Proposition 3.1, and S and S' are contained in the same orbit under the action of $Tv(S)$. So we have:

PROPOSITION 3.5. *If $G(S)$ is connected and S is t-equivalent to S', then $N(S) = N(S')$.*

In [3, §7] we will use a characterization of orbits to show that $N(L_n^m) = n(n+1)2^{m-1}$ for $m \geqslant 0$, $n \geqslant 1$. It follows that for $n \geqslant 2$, L_n^1 is not t-equivalent to L_{n+1}.

4. *Graphs of elements and basic moves*

A basis P for the symplectic space V is supposed fixed for the rest of this section. Let $G = G(P)$ be the graph of P. For any $x \in V$ we may write uniquely

$$x = \sum_{a \in P} x(a)a, \quad \text{where } x(a) \in K.$$

Let $x| = x|_P$ be the full subgraph of G on vertices a of P such that $x(a) \neq 0$. If a is a vertex of $x|$ we will also say that a is a vertex of x.

We can now apply graph-theoretic language to elements of V. For example, we say that x is a *tree* if $x|$ is a tree; x is *connected* if $x|$ is connected; x is *discrete* if $x|$ is discrete, that is, has no edges; and so on. Also, if H is a component of the graph $x|$, we refer to $\sum_{a \in H} x(a)a$ as a *component* (relative to P) of x.

If Γ is a graph, a *free vertex* of Γ is a vertex w incident to exactly one edge of Γ. Given such a free vertex an *elementary collapse* of Γ to Γ' removes the vertex w and its incident edge. A *collapse* is a sequence of elementary collapses. We use the standard fact that a finite tree may be collapsed to any one of its vertices.

In order to model collapsing by operations of transvections, we introduce some notation. Given $x \in V$ the notation $x = x_1 \oplus \ldots \oplus x_r$ will mean that there is a partition $P = P_1 \cup \ldots \cup P_r$ into disjoint non-empty sets and that $x = x_1 + \ldots + x_r$ where, for $i = 1, \ldots, r$, $x_i = \sum x(a)a$, the sum being over all members a of P_i. We write $x \sim y$ if x and y lie in the same orbit under the action of $Tv(P)$.

LEMMA 4.1. *Let $x = ka \oplus y$ where a is a free vertex of x. Then $x \sim a \oplus y$ and $x \sim y$.*

Proof. Suppose that a is adjacent to the vertex b of x and that $x(b) = l$. Then for any $h \in K$ we have

$$A^h(x) = \{(k + hl(a.b))a\} \oplus y.$$

Since l and $a.b$ are both non-zero, h can be chosen as required.

LEMMA 4.2. *Let $x \in V$ and suppose that a component of x has precisely two vertices a, b and $x = ka \oplus lb \oplus y$. Then $x \sim a \oplus y$.*

Proof. By Lemma 4.1,

$$x \sim a \oplus lb \oplus y = lb \oplus a \oplus y \sim a \oplus y.$$

PROPOSITION 4.3. *Let $x \in V$ be the disjoint union of trees $T_1, \ldots, T_r$. Choose a vertex a_i in each tree T_i. Then*

$$x \sim k_1 a_1 \oplus \ldots \oplus k_r a_r$$

where $k_i \neq 0$ and k_i may be chosen to be 1 *if*

(i) *T_i has more than one vertex, or*

(ii) *$K = \mathbf{F}_2$, or*

(iii) *$G(S)$ is connected with more than one vertex and $r = 1$.*

In particular, $x \sim y$ where y is discrete and has the same number of components as x.

Proof. This uses Lemmas 4.1 and 4.2 and a collapse of a tree to any one of its vertices. To obtain $k_i = 1$ in Case (i) use Lemma 4.2 after collapsing T_i to one edge. Case (ii) is trivial. In Case (iii) choose b adjacent to a_1; then $B(k_1 a_1)$ is a tree with two vertices, which is Case (i).

5. *Orbits of $Tv(P)$ for P a basis, $K \neq \mathbf{F}_2$*

This section contains our main results on orbits of $Tv(P)$ for the case where P is a basis of V. We will deal with the orbits of $Tv(S)$ where S is a spanning set of V after we have discussed the extension process in the next section.

THEOREM 5.1. *Let P be a basis for the symplectic space V over a field K with more than two elements. Let $G(P)$ be connected. Then $Tv(P)$ acts transitively on $V\backslash\mathrm{rad}(V)$.*

Proof. Since $G(P)$ is connected, $V\backslash\mathrm{rad}(V)$ non-empty implies that $P \subset V\backslash\mathrm{rad}(V)$. So by Proposition 2.1 it is sufficient to show that if $x \in V\backslash\mathrm{rad}(V)$, then $x \sim a$ for some $a \in P$. By Proposition 3.1 and Theorem 3.3 we may assume that $G(P)$ is a tree T. Then T has more than one element since $V/\mathrm{rad}(V)$ has positive even dimension.

Let $x \in V$. Then x is a forest. By Proposition 4.3 we may assume x is discrete. If x has one vertex, we have finished, by Proposition 4.3(iii). Suppose that x has more than one vertex. We show that $x \sim y$ where y is discrete and has fewer vertices than x, so reducing to the one-vertex case.

For any $y \in V$, let $m(y)$ be the minimal distance in T between vertices of y. Then $m(x) > 1$ since x is discrete.

LEMMA. *If $m(x) > 2$, then $x \sim y$ where y is discrete, has the same number of vertices as x, and $m(y) = m(x) - 1$.*

Proof. Let a, b be vertices of x whose distance apart in T is $m(x)$. Let $a, c, d, \ldots, b$ be vertices along a path of length $m(x)$ in T from a to b. Then a, c, d, b are distinct, since $m(x) > 2$. Also a is the only vertex of x adjacent to c, since $m(x) > 2$. So if $x = ka \oplus z$, we can reverse Lemma 4.1 to obtain $x \sim x \oplus c$ and then apply Lemma 4.2 to replace the component $ka \oplus c$ of $x \oplus c$ by c. Hence $x \sim c \oplus z$ and the lemma is proved.

We now assume that $m(x) = 2$. Then x has vertices $a_1, \ldots, a_r$ $(r > 1)$ adjacent to some vertex c of T. Suppose that $c.x \neq 0$. Then $C(x) = x \oplus (c.x)c$ and the component of $C(x)$ containing c is a tree which collapses to c. So $x \sim y$ where y is discrete and has fewer vertices than x.

We now assume that $c.x = 0$. Since x is not contained in $\mathrm{rad}(V)$ and P is a basis, there is an element e of P such that $e.x \neq 0$. This implies that e is not a vertex of x, since x is discrete. Among all such e, choose the one nearest in T to $\{a_1, \ldots, a_r\}$ and without loss of generality we may assume that e is nearest to a_1. Let $v(x)$ be the distance in T from e to a_1. Then $v(x) > 0$.

Assume first that $v(x) = 1$. Then $c.e = 0$, as in Fig. 5, since T is a tree. Also $a_1.x = 0$ since a_1 is a vertex of x, which is discrete. Thus $a_1.E(x) \neq 0$. If the coefficient of a_1 in x is k_1, then the coefficient of a_1 in $A_1^k E(x)$ is

$$h = k_1 + k(a_1.E(x)).$$

Now we use for the first and only time the fact that K has more than two elements: because of this assumption we may choose $k \neq 0$ such that $h \neq 0$. Also $c.x = c.e = 0$, and e is not a vertex of x. So if

$$z = CA_1^k E(x) = x + (e.x)e + k(a_1.E(x))a_1 + k(a_1.E(x))(a_1.c)c$$

then $e, c, a_1, \dots, a_r$ all lie in the same component of z. Now apply Proposition 4.3 to collapse this component of z to a vertex, and so obtain $z \sim y$ where y is discrete. Then $x \sim y$ where y is discrete, and has fewer components than x.

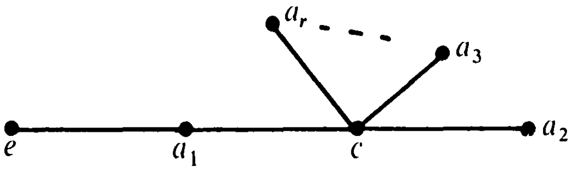

FIG. 5

Assume now that $v(x) > 1$. We show how to reduce to the case where $v(x) = 1$. Let $e, d, \dots, a_1$ be a minimal path in T from e to a_1. Consider $w = E(x) = x + (e.x)e$ and recall that $e.x \neq 0$. Then $d.w = (e.x)(d.e)$ since $d.x = 0$ by our choice of e. Thus $v(w) = v(x) - 1$. Also e is not a vertex of x and so e is a vertex of w. Since $e.x \neq 0$, e is adjacent to some vertex of x and so w has no more components than does x. This now completes the proof.

6. *Extensions of symplectic spaces*

In this section we develop an extension process which will enable us to replace in Theorem 5.1 the basis P by a spanning set S. We do this by 'extending' the symplectic space V with spanning set S to a symplectic space V' with basis P and map $p\colon V' \to V$ which preserves the form and satisfies $p(P) = S$. More generally, we suppose given the symplectic spaces V', V, a symplectic map $p\colon V' \to V$ (that is, p preserves the form), and also a subset S' of V'. We then describe $Tv(S')$ in terms of $Tv(S)$ where $S = p(S')$. This description will be used in the sequel [3], but is given here as it is valid for all fields.

DEFINITION 6.1. Let V be a symplectic space, and W a vector space. Let $V' = W \oplus V$ and let $p\colon V' \to V$ be the projection. The symplectic structure on V lifts uniquely to a symplectic structure on V' such that $W \subset \operatorname{rad}(V')$. Suppose a subset S of V is given and that S' is a subset of V' such that $p(S') = S$. We then call the pair (S', V') together with the projection $p\colon V' \to V$ an *extension* of (S, V).

Two examples of this structure will be crucial.

EXAMPLE-6.2. Let S be a spanning set for V, where $\dim(V) = n$, and where S has r elements. Let $W = K^{r-n}$, $V' = W \oplus V$; then we may choose $S' \subset V'$ such that S' is a basis for V' and p maps S' bijectively to S.

EXAMPLE 6.3. Let $S \subset V$ and let $e \in S$. We 'blow up e to $m+1$ elements' by forming $V' = K^m \oplus V$ and letting $d_0 = (0, e)$ and

$$S' = (\{0\} \times S) \cup \{d_1, \ldots, d_m\}$$

where $d_1 - d_0, \ldots, d_m - d_0$ is the standard basis of $K^m \oplus \{0\}$. Then $p(d_i) = e$, for $i = 0, \ldots, m$.

The first major result on extensions is

THEOREM 6.4. *Let p: $V' \to V$ be a surjective symplectic map of symplectic spaces V', V. Let $W = \ker(p)$ and let i: $V \to V'$ be a linear mapping such that $pi = 1_V$. Then the following hold.*

(i) *$W \subset \operatorname{rad}(V')$ and $p(\operatorname{rad}(V')) = \operatorname{rad}(V)$.*

(ii) *The maps p and i determine a split exact sequence*

$$1 \longrightarrow L(V/\operatorname{rad}(V), W) \xrightarrow{\xi} Sp_0(V') \longrightarrow Sp_0(V) \longrightarrow 1$$

in which the action so determined of $Sp_0(V)$ on $L(V/\operatorname{rad} V, W)$ is induced by the action of $Sp_0(V)$ on V.

(iii) *If $S' \subset V'$ and $S = p(S')$, then $\varphi(Tv(S')) = Tv(S)$. If $x, y \in V$ and $\alpha \in Sp_0(V')$ then $i(y) = \alpha(i(x))$ if and only if $y = \varphi(\alpha)(x)$. So if $Tv(S')$ acts transitively on $V' \backslash \operatorname{rad}(V')$, then $Tv(S)$ acts transitively on $V \backslash \operatorname{rad}(V)$.*

Proof. (i) For $x \in W$ and all y in V' we have $x.y = p(x).p(y) = 0$ and so $x \in \operatorname{rad}(V')$. Thus $W \subset \operatorname{rad}(V')$. The rest is just as easy.

(ii) Let $\alpha \in Sp_0(V')$. Then α leaves $W \subset \operatorname{rad}(V')$ invariant and so α induces a linear mapping $\varphi(\alpha)$: $V \to V$ by $\varphi(\alpha)(x) = p(\alpha(x'))$ where x' is any element of V' such that $p(x') = x$. It is easily checked that $\varphi(\alpha) \in Sp_0(V)$, and that φ: $Sp_0(V') \to Sp_0(V)$ is well defined and is a homomorphism.

The map i is a symplectic map and with p determines a decomposition $V' = W \oplus i(V)$ for which $\operatorname{rad}(V') = W \oplus i(\operatorname{rad}(V))$. For this decomposition of V' the elements α of $Sp_0(V')$ can be written as matrices $\begin{bmatrix} 1 & \alpha_1 \\ 0 & \alpha_2 \end{bmatrix}$ where $\alpha_2 \in Sp_0(V)$ and α_1: $V \to W$ is a linear mapping such that $\alpha_1(\operatorname{rad}(V)) = 0$. The splitting of φ is given by $\alpha_2 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & \alpha_2 \end{bmatrix}$. The mapping ξ is determined by $\alpha_1 \mapsto \begin{bmatrix} 1 & \alpha_1 \\ 0 & 1 \end{bmatrix}$. This proves (ii).

(iii) Let $k \in K$, $a \in S'$, and let $b = p(a)$. If $x' \in V'$ and $p(x') = x$, then

$$\varphi(A^k)(x) = p(A^k(x)) = p(x' + k(a.x')a) = x + k(p(a).p(x'))b = B^k(x).$$

Hence $\varphi(Tv(S')) = Tv(S)$, since p is surjective. For the last part we note that $\varphi(\alpha)(x) = p(\alpha(i(x)))$, whence the result follows.

THEOREM 6.5. *Let V be a symplectic space over a field with more than two elements and let S be a spanning set for V such that $G(S)$ is connected. Then $Tv(S)$ acts transitively on $V \backslash \operatorname{rad}(V)$.*

Proof. If S is finite, the theorem follows from Theorem 5.1, Example 6.2, and (iii) of Theorem 6.4.

Suppose S is not finite. Choose a basis P for V such that P is contained in S. Since $G(S)$ is connected, and P is finite, we can find a finite subset S' of S, containing P, and such that $G(S')$ is connected. So $Tv(S')$ acts transitively on $V\backslash \mathrm{rad}(V)$, and hence so also does $Tv(S)$.

We now carry the argument of Theorem 6.4 further, to relate $Tv(S')$ and $Tv(S)$. The result will be used in [**3**].

PROPOSITION 6.6. *Let $p\colon V' \to V$ be a surjective symplectic map of symplectic spaces V', V, let $W = \mathrm{ker}(p)$, and let $i\colon V \to V'$ be a linear map such that $pi = 1_V$. Let S' be a subset of V' and let $S = p(S')$. Let $\varphi\colon Sp(V') \to Sp(V)$ be the map induced by p, and let $\varphi'\colon Tv(S') \to Tv(S)$ be the restriction of φ. Then $\mathrm{ker}(\varphi') = \mathrm{ker}(\varphi)$ if the following conditions hold:*

(a) *S spans V, and*

(b) *W has a basis Q such that for all $c \in Q$ and $b \in S$, there are $a \in S$ and $\beta \in Tv(S')$ such that $i(a)$ and $c+i(a)$ belong to S' and $\beta(c+i(a)) = i(b)$.*

If, further, $i(S) \subset S'$ then we have a split exact sequence

$$\begin{tikzcd} 1 \arrow[r] & L(V/\mathrm{rad}(V), W) \arrow[r] & Tv(S') \arrow[r, shift left, "\varphi"] & Tv(S) \arrow[l, shift left, "\psi"] \arrow[r] & 1. \end{tikzcd}$$

Proof. Clearly $\mathrm{ker}(\varphi') \subset \mathrm{ker}(\varphi)$, so we need only prove that $\mathrm{ker}(\varphi) \subset Tv(S')$.

Let $\alpha \in \mathrm{ker}(\varphi)$. With respect to the decomposition $V' = W \oplus i(V)$, α has matrix $\begin{bmatrix} 1 & \alpha_1 \\ 0 & 1 \end{bmatrix}$ where $\alpha_1\colon V \to W$ is linear with $\alpha_1(\mathrm{rad}(V)) = 0$ as shown in Theorem 6.4. Let Q be a basis of W. Then we may write α_1 as a sum $\sum_{c\in Q}\lambda_c c$ where $\lambda_c \in V^*$ and $\lambda_c(\mathrm{rad}(V)) = 0$. But the symplectic form . induces a regular form on $V/\mathrm{rad}(V)$ and so an isomorphism $V/\mathrm{rad}(V) \to (V/\mathrm{rad}(V))^*$. So each λ_c is of the form $x \mapsto a_c.x$ for some $a_c \in V$. By Condition (a) the element a_c is a linear combination of elements of S. So we have shown that α_1 can be written as a sum of linear mappings of the form $\eta\colon x \mapsto k(b.x)c$ for some $k \in K$, $b \in S$, $c \in Q$, and so to prove that $\alpha \in Tv(S')$ it is sufficient to prove that for such an η the element $\begin{bmatrix} 1 & \eta \\ 0 & 1 \end{bmatrix}$ belongs to $Tv(S')$.

Choose an $a \in S$ and $\beta \in Tv(S')$ such that $i(a)$ and $c+i(a)$ belong to S' and $\beta(c+i(a)) = i(b)$. Let $a_1 = i(a)$, $a_2 = c+i(a)$, and let $\gamma = \beta A_1^{-k}A_2^{k}\beta^{-1}$. Then $\gamma \in Tv(S')$, $\varphi(\gamma) = 1$, and, for $x \in V$,

$$\begin{aligned} \gamma(i(x)) &= \beta A_1^{-k}(\beta^{-1}(i(x)) + k(a_2.\beta^{-1}(i(x)))a_2) \\ &= \beta(\beta^{-1}(i(x)) + k(i(b).i(x))c) \\ &= i(x) + k(b.x)c \\ &= i(x) + \eta(x). \end{aligned}$$

This completes the proof that $\mathrm{ker}(\varphi) \subset Tv(S')$.

The last part follows as in Theorem 6.4.

EXAMPLE 6.7. Our main use of the last result is for the 'blowing up an element' process of Example 6.3. In this case W has a basis $d_1 - d_0, \ldots, d_m - d_0$, and the mapping $i\colon V \to V'$ is given by $x \mapsto (0, x)$, so that $i(S) \subset S'$. If $c = d_j - d_0$ ($j \neq 0$) then $c + i(e) \in S'$, and the existence of β as required in (b) of Proposition 6.6 is satisfied if $G(S)$ is connected. Thus if S is connected, there is a split exact sequence

$$1 \to L(V/\mathrm{rad}(V), K^m) \to Tv(S') \to Tv(S) \to 1.$$

7. *Generation by transvections*, $K \neq \mathbf{F}_2$

The previous results give all the necessary information for results on generation of symplectic groups by transvections.

Recall that $Sp_0(V)$ is always generated by transvections, that is, $Sp_0(V) = Tv(V)$.

THEOREM 7.1. *Let V be a symplectic space over a field K with more than two elements, and let S be a subset of $V \backslash \mathrm{rad}(V)$ such that S spans V. Then $Tv(S) = Sp_0(V)$ if and only if $G(S)$ is connected.*

Proof. This is immediate from Theorems 2.7 and 6.5.

EXAMPLE 7.2. Let $P = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ be the standard symplectic basis for K^{2n}, where K has more than two elements. Let $d = e_1 + \ldots + e_n$, and let $S = P \cup \{d\}$. Then $Tv(S) = Sp(2n, K)$.

EXAMPLE 7.3. Let $L = \{e_1, \ldots, e_{2n}\}$, where for $i = 1, \ldots, 2n-1$, $e_i . e_{i+1} = 1 = -e_{i+1} . e_i$ are the only non-zero products of L. The induced form is non-singular, $Tv(L) = Sp(K^{2n})$ is isomorphic to $Sp(2n, K)$, and $2n$ is the minimal number of transvections generating $Sp(2n, K)$.

REMARK. The subject of groups generated by transvections is related to geometry (as in [**2**, **18**, **22**]), to the study of classical groups [**6**, **7**, **14**, **15**, **21**], to coding theory (as in [**24**, **25**]) and has its own interest [**16**, **17**, **19**, **20**]. These groups also arise in the theory of monodromy groups of isolated singularities of surfaces. In this case the transvections are the monodromy operators associated to the Picard–Lefschetz vanishing cycles, and the monodromy group is the subgroup of the group of automorphisms of homology generated by the monodromy operators [**1**]. This viewpoint is developed in [**5**, **13**, **23**], which, as we have recently become aware, have methods closely related to some of ours.

Some aspects of our results are well known to experts (for example, the author of [**21**] referred us to Lemma 1.3 of that paper for the minimal number of transvections generating $Sp(n, K)$). In [**18**, p. 31] it is shown that $Sp(2n, K)$ is not generated by transvections from the standard basis, and the author goes on to consider generation of $Sp(2n, K)$ by other sets of 'elementary matrices'. He also studies the problem of finding the *length* of an element σ of $Sp(2n, K)$, defined as the minimal number of factors in the expression σ as a product of transvections. This problem was originally considered by Dieudonné in 1955 (see [**4**] for a recent account correcting some earlier errors), and is considered in [**20**] for the non-regular case and for characteristic of the field not 2.

Our graph $G(S)$ has been considered also in [**24**] for certain subsets S of a symplectic space over $\mathbf{F}_2$.

J. I. Hall drew our attention to a paper by K. B. Farmer and M. P. Hale Jr ('Dual affine geometries and alternative bilinear forms', *Linear Algebra Appl.*, 30 (1980), 183–199), and showed how our Theorem 7.1 may be deduced from Theorem 5.1 of that paper. However, the results of Farmer and Hale assume throughout that K has morethan two elements, and so do not immediately apply to the case considered in our sequel, for which the present methods are a foundation.

Hall in [**8**] surveys results related to the transvection problem for symplectic groups over $\mathbf{F}_2$. Ishibashi in [**12**] generalizes our results in this paper to symplectic groups over local rings.

Acknowledgements

S. P. Humphries is grateful to the U.K. Science and Engineering Research Council for a maintenance grant for three happy years 1974–77 at Bangor. He is deeply indebted to Peter Stefan for the understanding of mathematics which he acquired during those years of learning.

We would both like to thank R. H. Dye, W. Kantor, F. Timmesfeld, and A. Wagner for helpful letters, and supplying offprints of their work, and C. Maclachlan, H. Ishibashi, J. I. Hall, and the referee for helpful comments on a draft of this paper.

References

1. N. A'Campo, 'Tresses, monodromie et le groupe symplectique', *Comm. Math. Helv.*, 54 (1979), 318–327.

2. E. Artin, *Geometric algebra* (Interscience, New York, 1957).

3. R. Brown and S. P. Humphries, 'Orbits under symplectic transvections II: the case $K = \mathbf{F}_2$', *Proc. London Math. Soc.* (3), 52 (1986), 532-556.

4. D. Callan, 'The generation of $Sp(\mathbf{F}_2)$ by transvections', *J. Algebra*, 42 (1976), 378–390.

5. S. V. Chmutov, 'Monodromy groups of critical points of functions', *Invent. Math.*, 67 (1982), 121–131; *Invent. Math.*, 73 (1983), 491–510.

6. J. Dieudonné, *Sur les groupes classiques*, 3rd edn, Actualités Scientifiques et Industrielles 1040 (Hermann, Paris, 1973).

7. R. H. Dye, 'Symmetric groups as maximal subgroups of orthogonal and symplectic groups over the field of two elements', *J. London Math. Soc.* (2), 20 (1979), 227–237.

8. J. I. Hall, 'Symplectic geometry and mapping class groups', *Geometrical combinatorics* (ed. F. C. Holroyd and R. J. Wilson), Research Notes in Mathematics 114 (Pitman, London, 1985), pp. 21–33.

9. S. P. Humphries, 'Generators for the mapping class group', *Topology of low-dimensional manifolds: Proceedings, Sussex 1977* (ed. R. Fenn), Lecture Notes in Mathematics 722 (Springer, Berlin, 1979), pp. 44–47.

10. S. P. Humphries, 'Graphs, groups and symplectic geometry', Ph.D. thesis, University of Wales, 1983.

11. S. P. Humphries and R. Brown, 'Orbits under symplectic transvections I', *Notices Amer. Math. Soc.*, 1 (1980), 561.

12. H. Ishibashi, 'Generation of symplectic groups by transvections over local rings with at least three residue classes', *J. Algebra*, to appear.

13. W. A. M. Janssen, 'Skew-symmetric vanishing lattices and their monodromy groups', *Math. Ann.*, 266 (1983), 115–133; *Math. Ann.*, 272 (1985), 17–22.

14. W. Kantor, 'Subgroups of classical groups generated by long root elements', *Trans. Amer. Math. Soc.*, 248 (1979), 347–379.

15. W. Kantor, *Classical groups from a non-classical viewpoint*, Lecture Notes, Mathematical Institute, Oxford, 1978.

16. J. McLaughlin, 'Some groups generated by transvections', *Arch. Math. Basel*, 18 (1967), 364–368.

17. J. McLaughlin, 'Some subgroups of $\mathrm{SL}_n(\mathrm{F}_2)$', *Illinois J. Math.*, 13 (1969), 108–115.

18. O. T. O'Meara, *Symplectic groups*, Mathematical Surveys and Monographs 16 (American Mathematical Society, Providence, R.I., 1978).

19. H. Pollatsek, 'Irreducible groups generated by transvections over fields of characteristic two', *J.Algebra*, 39 (1976), 328–333.

20. U. Spengler and H. Wolff, 'Die Lange einer symplektischen Abbildung', *J. reine angew. Math.*, 274/275 (1975), 150–157.

21. F. G. Timmesfeld, 'A condition for the existence of a weakly closed TI-set', *J. Algebra*, 60 (1979), 472–484.

22. A. Wagner, 'Groups generated by elations', *Abh. Math. Sem. Univ. Hamburg*, 41 (1974), 190–205.

23. B. Wajnryb, 'On the monodromy group of plane curve singularities', *Math. Ann.*, 246 (1980), 141–154.

24. H. N. Ward, 'Centre sets and ternary codes', *J. Algebra*, 65 (1980), 206–224.

25. H. N. Ward, 'Binary views of ternary codes', *The geometric vein: the Coxeter Festschrift* (ed. C. Davis, B. Grunbaum, and F. A. Sherk, Springer, Berlin, 1981), pp. 593–598.

Department of Pure Mathematics
University College of North Wales
Bangor
Gwynedd LL57 2UW
U.K.

Department of Mathematics
University of California
Santa Barbara
California 93106
U.S.A.