# ORBITS UNDER SYMPLECTIC TRANSVECTIONS II: THE CASE $K = \mathbf{F}_2$

RONALD BROWN *and* STEPHEN P. HUMPHRIES

[Received 17 January 1984—Revised 25 June 1985]

*Dedicated to the memory of Peter Stefan*

## 1. *Introduction*

Let $V$ be a not necessarily regular, finite-dimensional symplectic space (with symplectic form . ) over a field $K$ where $V\backslash\mathrm{rad}(V)$ is non-empty. Our previous paper [**27**] (hereinafter referred to as [I]) began the study of the orbits of $V\backslash\mathrm{rad}(V)$ under the action of the group $Tv(S)$ of isometries which are products of transvections from a subset $S$ of $V$. Let $G(S)$ be the graph with vertex set $S$ and an edge between $a, b \in S$ if $a.b \neq 0$. The main result of [I] was that if $K$ has more than two elements, then the action of $Tv(S)$ on $V\backslash\mathrm{rad}(V)$ is transitive if and only if $S$ spans $V$ and $G(S)$ is connected.

In this paper we consider the more difficult case where $K$ is the field $\mathbf{F}_2$ of two elements, and we assume this throughout.

Let $P$ be a basis for $V$. Then the graph $G(P)$ determines the symplectic form on $V$. Moreover, if $H$ is a full subgraph of $G(P)$, then the sum of the vertices of $H$ is an element of $V$. This gives a one-one correspondence between the elements $x$ of $V$ and the full subgraphs $x\,|_P$ of $G(P)$, and enables us to use lattice-theoretic terminology for elements of $V$. That is, inclusion of subgraphs of $G(P)$ determines a lattice ordering $\subset_P$ on elements of $V$, with union $\cup_P$ and intersection $\cap_P$.

Let $Q_P$ be the quadratic form associated to the symplectic form . on $V$ such that $Q_P(a) = 1$ for all $a \in P$. Then $Tv(P)$ preserves the form $Q_P$. We show that for $x \in V$, $Q_P(x)$ is the Euler characteristic mod 2 of the graph $x\,|_P$. Thus this quadratic form is that introduced in [**9**] for the case where $V = H_1(T_g; \mathbf{F}_2)$ with the intersection symplectic form. It is easy to prove that if $P, R$ are $t$-equivalent bases of $V$, as defined in [I], then $Q_P = Q_R$.

Let $E_6$ denote the graph shown in Fig. 1. The vertex $v$ will be called the *centre* of $E_6$. A graph $G$ is said to be of *orthogonal type* if $G$ is a tree and contains $E_6$ as a subgraph. A basis $P$ of $V$ is of *orthogonal* type if $P$ is $t$-equivalent to $P'$ where $G(P')$ is a graph of orthogonal type.

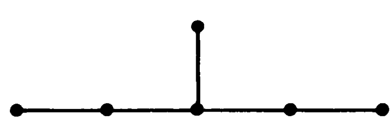


FIG. 1

Our main result is:

THEOREM 10.1. *Let $P$ be a basis of $V$ of orthogonal type. Let $x, y \in V\backslash\mathrm{rad}(V)$. Then $x, y$ belong to the same orbit under the action of $Tv(P)$ if and only if $Q_P(x) = Q_P(y)$.*

*A.M.S. (1980) subject classification*: 20 H 30, 51 F 99.
*Proc. London Math. Soc.* (3) 52 (1986) 532-556.

We shall use this result to give necessary and sufficient conditions on a spanning set $S$ of $V$ for it to be true that $Tv(S) = Sp_0(V)$ (Theorem 11.1). We shall also describe the group $Tv(P)$, together with its action on $V\backslash\mathrm{rad}(V)$ in the case where $G(P)$ is connected but $P$ is not of orthogonal type. Here we find that $Tv(P)$ is an extension of an abelian group by a symmetric group.

We mention here some further developments. The paper [**32**] gives necessary and sufficient conditions for a connected graph $G(S)$ to be $t$-equivalent to a graph having no valency-3 vertices. This allows a complete description of subsets $S$ such that $Tv(S)$ is isomorphic to a symmetric group, thus answering a question of J. I. Hall. It is also shown in [**32**] that if $P$ and $R$ are two bases for the regular symplectic space $V$ over $\mathbf{F}_2$ such that $G(P)$ and $G(R)$ are connected and $Tv(P) = Tv(R)$, then $P$ and $R$ are $t$-equivalent.

Related techniques are used in [**33**] to classify all sets of $n$ transvections generating $\mathrm{SL}(n, F)$ where $F$ is a finite field.

This paper forms a revised version of Chapters 4–6 of [**10**].

## 2. *Outline of the argument*

Let $P$ be a basis for the symplectic space $V$ over the field $\mathbf{F}_2$ of two elements, and suppose that the graph $G(P)$ is connected. According to § 3 of [I] we may assume that $G(P)$ is a tree. Let $x \in V\backslash\mathrm{rad}(V)$. By § 4 of [I] we see that the orbit of $x$ under $Tv(P)$ contains elements having discrete graphs. Thus we assume $x|_P$ is discrete. The idea, as in [I], is to reduce the number of components (vertices) of $x|_P$.

Let $L_n$ be a basis for $V$ where $L_n = \{e_1, \ldots, e_n\}$ with $e_i . e_{i+1} = 1$ for $i = 1, \ldots, n-1$, all other products being zero. We call $L_n$ a *line graph.*

In § 3 we show that if $G(P)$ is connected and is not of orthogonal type then $P$ is $t$-equivalent either to some $L_n$, or to a 'blow-up' of some $L_n$ (for which see Example 6.3 of [I]).

If $G(P)$ is a line graph then we cannot change the number of components of $x|_P$ by an action of $Tv(P)$, and we show that this number is a complete invariant of the orbit of $x$.

If $G(P)$ is a blown-up line graph, then there is a symplectic projection $p: V \to U$ such that $p(P)$ has graph a line graph $L$. Also for $x \in V\backslash\mathrm{rad}(V)$, the number of components of $(px)|_L$ is a complete invariant of the orbit of $x$ under the action of $Tv(P)$.

Thus non-orthogonal cases are relatively simple. However, if $G(P)$ is a tree of orthogonal type then the idea is to move around the vertices (components) of $x|_P$ by an action of $Tv(P)$ so as to have vertices $a_1, \ldots, a_r$, where $r > 1$, of $x|_P$ all adjacent to a vertex $c$, say, of $G(P)$, as in Fig. 2. Note that $c$ is not a vertex of $x|_P$ since $x|_P$ is discrete. Now if $c.x = 1$ (that is, if $r$ is odd), then $C(x)|_P$ has less components than does $x|_P$. However, if $c.x = 0$, then $r$ is even and if there are vertices of $x|_P$ which are not adjacent to $c$, we try to 'bring them in closer to $c$'. For example, imagine that $G(P)$ is as

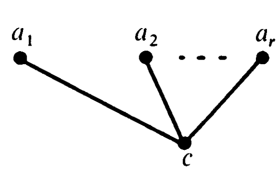


FIG. 2

in Fig. 3, where $x = a_1 + a_2 + a$. Then $c.x = 0$. Here we increase the number of vertices of $x|_P$ adjacent to $c$ by acting on $x$ by $DAED$, the composite of the transvections corresponding to $d, e, a, d$. Now $DAED(x) = a_1 + a_2 + e$ and $CDAED(x)|_P$ has fewer components than does $x|_P$.

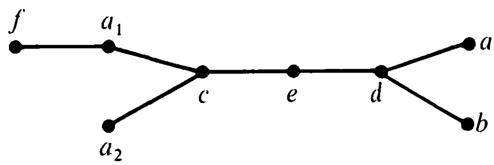


FIG. 3

However, not all cases are as nice as this. For example, if, in the above situation, we had $x = a_1 + a_2 + a + b$, then $x \in V \backslash \mathrm{rad}(V)$ but $d.x = 0$ and so we cannot move one of the vertices $a$ or $b$ closer to $c$.

The problem stems from the fact that $a + b$ is in $\mathrm{rad}(V)$ and so we cannot move it about by an action of $Tv(P)$. To overcome this type of difficulty we show that there is $z$ in the orbit of $x$ under $Tv(P)$ such that $z|_P$ is discrete and has no more components than does $x|_P$, and further if $w \in V \backslash \{0\}$ with $w \subset_P z$, then $w \notin \mathrm{rad}(V)$. This gives us more freedom to move subgraphs of $z$ around, and allows us to show that it is always possible to reduce the number of components to one or two. The rest follows easily.

## 3. *The line geometry*

Let $L_n$ be the line graph with vertices $e_1, e_2, \ldots, e_n$ in order, as in the last section. We write $\langle L_n \rangle$ for the symplectic space over $\mathbf{F}_2$ with basis the vertices of $L_n$ and symplectic form determined by $L_n$. Note that $\mathrm{rad}\langle L_n \rangle$ is 0 if $n$ is even, and is spanned by $e_1 + e_3 + \ldots + e_n$ if $n$ is odd.

For the rest of this section we write $L = L_n$, $V = \langle L \rangle$.

We shall need the following result. We abbreviate '$x|_L$ is connected' to '$x$ is connected'.

PROPOSITION 3.1. *Let $x, y$ be connected elements of $\langle L \rangle$. Then $Y(x)$ is connected. Further, if $\alpha \in Tv(L)$, then $\alpha(x)$ is connected.*

*Proof.* Clearly, if $y.x = 0$, then $Y(x) = x$ is connected.

We now assume that $y.x = 1$. Figure 4 shows various possibilities for the relative placements of $x$ and $y$ (note that $x$ connected implies $x$ is of the form $e_h + e_{h+1} + \ldots + e_k$ where $h \leqslant k$). The only cases in which $x.y = 1$ are (i) and (iv), and in these cases $Y(x) = x + y$ is connected.

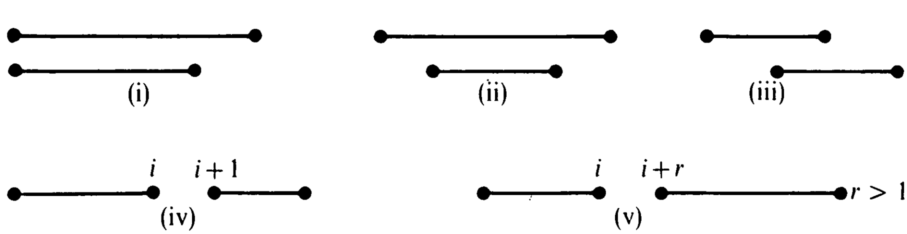


FIG. 4

That $\alpha(x)$ is connected now follows, since $\alpha$ is a product of transvections $E_i$ for $e_i$ a vertex of $L$.

THEOREM 3.2. *Let $R$ be a set of connected elements of $V = \langle L \rangle$ such that $T = G(R)$ is a tree with $x_1$ as an end vertex. Then there is an $\alpha \in Tv(L)$ such that $\alpha$ maps $R$ into $L$ and $x_1$ to $e_1$. Also $G(R)$ is a line graph.*

*Proof.* Since $x_1$ is connected, it collapses by operations of $Tv(L)$ to a vertex [I, Proposition 4.3] and this vertex may, by further operations of $Tv(L)$, be moved to $e_1$ [I, Proposition 2.1]. Hence there is an $\alpha_1 \in Tv(L)$ such that $\alpha_1 x_1 = e_1$.

Let $1 \leqslant q$ and suppose inductively that $\alpha_q \in Tv(L)$ and $x_1, x_2, \ldots, x_q \in T$ have been chosen so that $\alpha_q x_i = e_i$, where $1 \leqslant i \leqslant q$. This has been done for $q = 1$. If $T = \{x_1, \ldots, x_q\}$, we set $\alpha = \alpha_q$. Suppose $T \neq \{x_1, \ldots, x_q\}$; we show how to choose $x_{q+1}, \alpha_{q+1}$.

Since $T$ is connected, there is an element $x_{q+1}$ of $T$ distinct from $x_1, \ldots, x_q$ but adjacent to one of them. Now $y = \alpha_q x_{q+1}$ is connected, and so, for some $h \leqslant k$,

$$y = e_h + e_{h+1} + \ldots + e_k.$$

Suppose $h = 1$. Then $y \neq e_1$ implies $e_1 . y = 1$ and so $x_1 . x_{q+1} = 1$. If $q = 1$, we must also have $k > 1$, since $y \neq e_1$, and so we can find $\alpha' \in Tv(L)$ such that $\alpha' e_1 = e_1$ and $\alpha' y = e_2$. We then set $\alpha_2 = \alpha' \alpha_1$. Also we cannot have $q > 1$, since $x_1$ is an end vertex of $T$.

Suppose $1 < h < q+1$. Then $e_{h-1} . y = e_h . y = 1$ and so $x_{h-1} . x_{q+1} = x_h . x_{q+1} = 1$, contradicting the fact that $T$ is a tree. Therefore $h = q+1$, and $e_q . y = 1$, whence $x_q . x_{q+1} = 1$. Choose $\alpha''$ involving $E_t$ for $t > q+1$ such that $\alpha'' y = e_{q+1}$. Set $\alpha_{q+1} = \alpha'' \alpha_q$.

That $G(R)$ is a line graph follows from the existence of $\alpha$.

COROLLARY 3.3. *Let $\beta \in Sp(V)$ be such that $\beta e_i$ is connected for $i = 1, \ldots, n$. Then $\beta \in Tv(L)$.*

*Proof.* Clearly $\beta(L)$ is also a line graph and hence a tree. By the proposition, there is an $\alpha \in Tv(L)$ such that $\alpha\beta(L) = L$. Hence $\beta = \alpha^{-1}$.

As an application of Theorem 3.2, we determine $Tv(L_n)$.

THEOREM 3.4. *The group $Tv(L_n)$ is isomorphic to $S_{n+1}$, the symmetric group on $n+1$ symbols.*

*Proof.* A connected, non-trivial element of $\langle L_n \rangle$ may be written

$$x_{ij} = e_i + e_{i+1} + \ldots + e_{j-1}, \quad \text{where } 1 \leqslant i < j \leqslant n+1.$$

We regard $x_{ij}$ as an edge between vertices $v_i$ and $v_j$ of the simplex $\Delta^n$ with vertices $v_1, v_2, \ldots, v_{n+1}$. Then the edges $x_{ij}, x_{kl}$ meet if and only if $x_{ij} . x_{kl} = 1$. (See Fig. 5.)

Let $\alpha \in Tv(L_n)$. Then $\alpha$ permutes the connected elements of $\langle L_n \rangle$, and preserves the symplectic form. Hence $\alpha$ determines an automorphism $\varphi(\alpha)$ of $\Delta^n$. This gives a morphism $\varphi$: $Tv(L_n) \to \operatorname{Aut} \Delta^n$. But $\varphi$ is injective, since $\alpha, \beta \in Tv(L_n)$ are determined by their effects on the $e_i$.

Let $g \in \operatorname{Aut} \Delta^n$ and let $x_i$ be the edge $g(e_i)$ of $\Delta^n$, for $1 \leqslant i \leqslant n$. Then $\{x_1, \ldots, x_n\}$ is a line graph. By Theorem 3.2, there is an $\alpha \in Tv(L_n)$ and a permutation $\sigma$ of $1, \ldots, n$ such

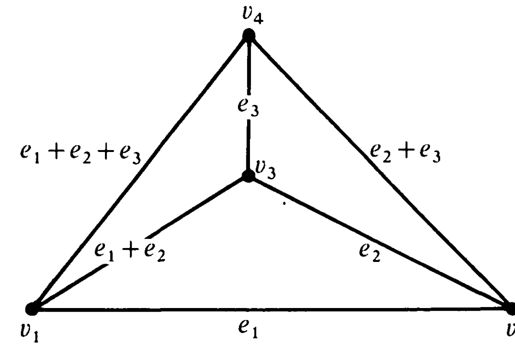


FIG. 5

that $\sigma 1 = 1$ and $\alpha(x_{\sigma i}) = e_i$, for $1 \leqslant i \leqslant n$. By adjacency considerations, $\sigma$ is the identity. Then $\varphi(\alpha^{-1})$ and $g$ agree on the vertices of $\Delta^n$, and so coincide. Hence $\varphi$: $Tv(L_n) \to \operatorname{Aut}\Delta^n$ is an isomorphism.

The theorem follows, since the isomorphism $\operatorname{Aut}\Delta^n \cong S_{n+1}$ is well known.

REMARK. The above determination of $Tv(L_n)$ has been obtained in the regular case, that is, when $n$ is even, also in [1, § 3], where it is attributed to Serre.

In § 7 we show that for any subset $S$ of $V$, if $G(S) = L_n$, then $Tv(S) \cong S_{n+1}$.

## 4. *The blown-up line geometry*

Let $L_n^m$ denote the graph shown in Fig. 6. We call $L_n^m$ (as in Example 6.3 of [I]) the graph obtained from $L_n$ by blowing up $e_n$ to $m+1$ elements $d_0 = e_n, d_1, \ldots, d_m$. We identify $L_n$ as a subgraph of $L_n^m$ in the obvious way.

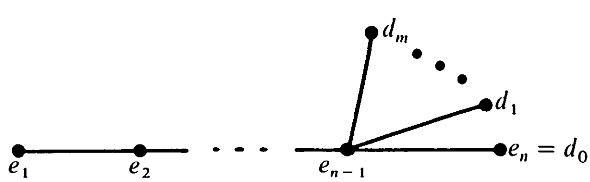


FIG. 6

The symplectic space over $\mathbf{F}_2$ with basis the vertices of $L_n^m$ and symplectic form determined by the edges, is written $\langle L_n^m \rangle$. Note that $\operatorname{rad}\langle L_n^m \rangle$ is spanned by $\operatorname{rad}\langle L_n \rangle$ and the elements $d_1 - d_0, \ldots, d_m - d_0$.

If $G$ is a graph, we say $G$ *contains* $E_6$ if $G$ has a subgraph isomorphic to $E_6$.

Let $G$ be a finite tree. If $G$ does not contain $E_6$, and $G$ is finite, as we always assume, then $G$ must be obtained from a line graph $L_n = \{e_1, \ldots, e_n\}$ by blowing up $e_1$ to $r$ elements (say), and $e_n$ to $s$ elements with $r, s \geqslant 1$.

PROPOSITION 4.1. *If $V$ is a symplectic space over $\mathbf{F}_2$ and $S$ is a subset of $V$ such that $G(S)$ is a tree not containing $E_6$, then $S$ is t-equivalent to some $L_n^m$.*

*Proof.* We know that $G(S)$ is a line graph $\{e_1, \ldots, e_n\}$ with $e_1$ blown up to $r+1$ elements $e_1, u_1, \ldots, u_r$ and $e_n$ blown up to $s$ elements. If $r > 0$, then by Proposition 3.4 of [I], we can find a $t$-equivalence moving $u_1, \ldots, u_r$ to have the same adjacencies as $e_n$.

We now prove a converse to this proposition.

THEOREM 4.2. *Let $V = \langle L_n^m \rangle$, and let $f\colon L_n^m \to S$ be a t-equivalence such that $G(S)$ is a tree. Then $G(S)$ does not contain $E_6$.*

*Proof.* Let $U = \langle L_n \rangle$, and let $p\colon V \to U$ be the symplectic map such that $p(e_i) = e_i$, for $i = 1, \ldots, n$, and $p(d_j) = e_n$, for $j = 1, \ldots, m$. We say $x \in U$ is connected if it is so in terms of the graph $L_n$.

Note that if $x, y \in V$ and $z = p(y)$, then $p(Y(x)) = Z(p(x))$. Hence if $px, py$ are connected, so also is $p(Y(x))$. From this it follows that $p(a)$ is connected for all vertices $a$ of $S$.

We now repeat the argument for the proof of Theorem 3.2 but with $S$ replacing $R$, to show that there is an $\alpha \in Tv(L_n)$ and elements $x_1, \ldots, x_n \in S$ such that $\alpha p(x_i) = e_i$, for $i = 1, \ldots, n$, and $x_1$ is an end vertex of $G(S)$.

Let $y \in S \backslash \{x_1, \ldots, x_n\}$. Then $y$ is adjacent to at most one of $x_1, \ldots, x_n$ since $G(S)$ is a tree. Hence $\alpha y$ is adjacent to at most one of $\alpha x_1, \ldots, \alpha x_n$.

Now we can write $\alpha x_i = e_i + a$, for $i < n$, and $\alpha x_n = b$, and, since $p\alpha y$ is connected,

$$\alpha y = e_h + e_{h+1} + \ldots + e_k + c$$

where $1 \leqslant h \leqslant k \leqslant n$ and $a, c$ are sums of an even number of $d_j$ including possibly $j = 0$, while $b$ is the sum of an odd number of $d_j$.

An examination of cases shows that $\alpha y$ can be adjacent only to $\alpha x_2$ or $\alpha x_{n-1}$. Hence $\alpha G(S)$ does not contain $E_6$. Hence $G(S)$ does not contain $E_6$.

We can also determine $Tv(L_n^m)$.

THEOREM 4.3. *If $n > 1$ and $m > 0$, then there is a split exact sequence*

$$1 \to (\mathbf{F}_2)^{mp} \to Tv(L_n^m) \to S_{n+1} \to 1,$$

*where $p$ is $n-1$ or $n$ according as $n$ is odd or even.*

*Proof.* By Proposition 6.6 of [I], we have a split exact sequence,

$$1 \to L(V/\mathrm{rad}(V), \mathbf{F}_2^m) \to Tv(L_n^m) \to Tv(L_n) \to 1.$$

The result follows.

COROLLARY 4.4. *If $n > 1$ and $m > 0$, then $Tv(L_n^m)$ is not isomorphic to a symmetric group.*

*Proof.* By Theorem 4.3, $Tv(L_n^m)$ has a normal, abelian subgroup consisting of elements of order 2. Such elements in a symmetric group of degree $q$ are products of disjoint transpositions; if $q \geqslant 3$ then conjugates of such elements generate a non-abelian group, and this gives a contradiction.

## 5. *Sociable elements*

Let $V$ be a symplectic space over the field $\mathbf{F}_2$. Let $P$ be a basis for $V$. Then the elements of $V$ and the full subgraphs of $G(P)$ form equivalent sets, as pointed out in § 1.

Non-zero elements of rad($V$) will be called *isolated* elements of $V$. We will say that

$x \in V$ is *part-isolated* (in $P$) if there is a $y \in V$ such that $y \subset_P x$ and $y$ is isolated. If $x$ is not part-isolated, then we will call $x$ *sociable* (in $P$).

We let $I_P(x)$ denote the element of $V$ whose graph is $\cup_P y$ where the union is over all isolated elements $y$ with $y \subset_P x$. Note that if $x$ is isolated, then $I_P(x) = x$ for all bases $P$. However it is not true that if $I_P(x) = x$ then $x$ is isolated. For example, let $P = L_4^3$ and $x = d_1 + d_2 + d_3$. Then $d_1 + d_2$ and $d_1 + d_3$ are both isolated elements and so $I_P(x) = x$; however $e_3.x = 1$ and so $x$ is not isolated. Note further that $x$ is sociable in $P$ if and only if $I_P(x)$ is zero.

PROPOSITION 5.1. *Let $P$ be a basis for $V$ with $G(P)$ a tree. Let $x \in V$. Then $I_P(x)$ is discrete. In particular, if $x$ is isolated then $x$ is discrete.*

*Proof.* Suppose that $I_P(x)$ is not discrete. Let $C$ be a component of $I_P(x)$ which is not a vertex. Then $C$ is a tree since $G(P)$ is a tree. Let $e$ be an end vertex of $C$ and let $f$ be the unique vertex of $C$ adjacent to $e$. Let $y \subset_P x$ be an isolated element of $V$ containing $f$. Then the only vertex of $y$ adjacent to $e$ is $f$ and so $e.y = e.f = 1$, which is a contradiction as $y$ is isolated. Thus $I_P(x)$ is discrete.

If $x$ is isolated, then $I_P(x) = x$ and so $x$ is discrete.

The next result shows that if $P$ is a basis with $G(P)$ a tree, then we can act on $x \in V \setminus \mathrm{rad}(V)$ by $Tv(P)$, the result being sociable. Write $x \sim_P y$, or simply $x \sim y$, if $x$ and $y$ belong to the same orbit of the action of $Tv(P)$.

PROPOSITION 5.2. *Let $P$ be a basis of $V$ with $G(P)$ a tree. Then for $x \in V \setminus \mathrm{rad}(V)$, $x \sim x_0$ where $x_0$ is sociable, discrete and has no more components than does $x$.*

*Proof.* By Proposition 4.3 of [1] we may assume that $x$ is discrete. If $x$ is sociable we have finished, so we suppose that $I_P(x)$ is non-zero.

CLAIM. *There is a $z \in V$ such that $x \sim z$, $z$ is discrete, $z$ has no more components than $x$, and $I_P(z)$ is properly contained in $I_P(x)$.*

Since $x$ is not isolated, there is a vertex $s$ of $G(P)$ such that $s.x \neq 0$. Let $\delta(\ ,\ )$ be the distance function in $G(P)$. We will need the following lemma:

LEMMA 5.3. *Suppose $x$ is discrete and $s \in P$ with $s.x \neq 0$. Let $u_1, \ldots, u_r$ be all the vertices of $x$ adjacent to $s$. Then $r > 0$ and $s$ is not a vertex of $x$. If $y = U_1 \ldots U_r S(x)$, then $u_i$ is not a vertex of $y$ for all $i = 1, \ldots, r$, $I_P(y) \subset I_P(x)$, $y$ is discrete, $y$ has no more components than does $x$, and*

(i) *if $\delta(s, I_P(x)) > 1$, then $I_P(y) = I_P(x)$,*

(ii) *if $\delta(s, I_P(x)) = 1$, then $I_P(y)$ is properly contained in $I_P(x)$ and $y$ has fewer components than $x$.*

*Proof.* Since $s.x \neq 0$ we have $r > 0$, and as $x$ is discrete we see that $s$ is not a vertex of $x$ and that $u_i.x = 0$ for all $i = 1, \ldots, r$. Thus

$$y = U_1 \ldots U_r S(x) = x + s + u_1 + \ldots + u_r,$$

and $y$ is obtained from $x$ by replacing $u_1, \ldots, u_r$, by $s$. Now $s.v = 0$ for all other vertices $v$ of $x$ and so we easily see that $y$ is discrete and has no more components than does $x$.

We now prove that $I(y) \subset I(x)$ (we will omit the reference to $P$ in the rest of the proof). Suppose that this is not true. Then there is an isolated element $w$ in $V$ with $w \subset y$ and $w$ not contained in $x$. Now the only vertex of $y$ which is not a vertex of $x$ is $s$, and so $s$ must be a vertex of $w$. Now $u_1.s = 1$ and since $w$ is isolated we have $w.u_1 = 0$. Thus, as $s$ is a vertex of $w$, there is another vertex, $t$ say, of $w$, adjacent to $u_1$. Then $t$ is a vertex of $x$, since the only vertex of $y$ which is not in $x$ is $s$. Thus $t$ and $u_1$ are vertices of $x$ and so $x$ is not discrete contrary to our assumption. Thus $I(y) \subset I(x)$.

For (i) suppose that $\delta(s, I(x)) > 1$. Then no $u_i$ is a vertex of $I(x)$ and so we have $I(x) \subset I(y)$ and (i) follows.

If now $\delta(s, I(x)) = 1$, then we may assume that $u_1$ is a vertex of some isolated $w$ in $V$ where $w \subset x$. Since $s.u_1 = 1$ and $s.w = 0$, $w$ contains some other $u_j$, where $j \neq 1$. Thus $r > 1$ and (ii) follows.

We now return to the proof of the claim.

If $\delta(s, I(x)) = 1$, then we may take $z = y$ where $y$ is as given by Lemma 5.3.

Suppose now that $\delta(s, I(x)) > 1$. Let $y$ be as given in Lemma 5.3. Then $y$ is discrete, $I(y) = I(x)$, and $y$ has no more components than does $x$.

We now assume (as we may) that any vertex $s'$ of $G(P)$ nearer to $I(x)$ than $s$ satisfies $x.s' = 0$.

Let $t$ be a vertex of $I(x)$ nearest to $s$ and let $s, u, v, \ldots, t$ be the vertices along a shortest path from $s$ to $t$ in $G(P)$. Then $v.x = u.x = 0$ by our choice of $s$, and $u.u_i = 0$ since $G(P)$ is a tree. Thus

$$u.y = u.(x+s+u_1+\ldots+u_r) = u.s = 1$$

and so we have reduced $\delta(s, I(x))$. Continuing in this way we eventually get the situation $\delta(s, I(x)) = 1$.

Thus if $I(x)$ is not empty we can always find $z$ such that $z$ is discrete, $z \sim x$, $z$ has no more components than does $x$, and $I(z)$ is a proper subset of $I(x)$. This proves the claim.

By repeating this construction, replacing $x$ by $z$, and so on, we eventually arrive at $x_0$ as required by the proposition.

## 6. *Basic moves*

Let $V$ be a finite-dimensional symplectic space over the field $\mathbf{F}_2$. Throughout this section we assume that $P$ is a basis of $V$ such that $T = G(P)$ is a tree. We let $x \in V \setminus \mathrm{rad}(V)$ be discrete.

The two basic moves are to move $x$ either off one of its vertices, or onto a specified vertex. We abbreviate $\sim_P$ to $\sim$.

PROPOSITION 6.1. *Let $a$ be a vertex of $x$. Then $x \sim y$ where*
(i) *$y$ is discrete, and has no more components than $x$,*
(ii) *$a$ is not a vertex of $y$,*
(iii) *$I_P(y) \subset I_P(x)$, so that if $x$ is sociable, so also is $y$.*

*Proof.* Since $x$ is not isolated, we can choose a vertex $s$ of $T$ such that $s.x \neq 0$, but any vertex $s'$ of $T$ closer to $a$ satisfies $s'.x = 0$. Let $m(x) = \delta(s, a)$.

Let $u_1, \ldots, u_r$ be all the vertices of $x$ adjacent to $s$. If some $u_i = a$, then Lemma 5.3 gives the result. Suppose then that $a$ is not adjacent to $s$, so that $m(x) > 1$.

Let $s, u, \ldots, a$ be the vertices along a shortest path (so of length $m(x)$) from $s$ to $a$. Then $u.x = 0$. Since $T$ is a tree, we have $u.u_i = 0$ for $i = 1, \ldots, r$. Let $w = U_1 \ldots U_r S(x)$. Then $u.w = u.s = 1$, and $a$ is still a vertex of $w$. But $m(w) < m(x)$, and Lemma 5.3 tells us that $w$ is discrete, has no more components than $x$, and $I_P(w) \subset I_P(x)$. So we may reduce to the case where $m(x) = 1$, considered above.

PROPOSITION 6.2. *Let $a$ be a vertex of $T$. Then $x \sim y$ where*
(i) *$y$ is discrete, and has no more components than $x$,*
(ii) *$a$ is a vertex of $y$,*
(iii) *$I_P(y) \subset I_P(x)$, so that if $x$ is sociable, so also is $y$.*

*Proof.* We may assume $a$ is not a vertex of $x$.

If $a.x \neq 0$, then the result follows from Lemma 5.3 (with $s = a$).

Assume $a.x = 0$. Since $x$ is not isolated, there is a vertex $s$ of $T$ such that $s.x \neq 0$, but any vertex $s'$ of $T$ closer to $a$ satisfies $s'.x = 0$. Let $m(x) = \delta(s, a)$. Then $m(x) \geqslant 1$.

Suppose $m(x) = 1$. Let $u_1, \ldots, u_r$ be the vertices of $x$ adjacent to $s$. Then $a.u_i = 0$, for $i = 1, \ldots, r$, since $T$ is a tree. So if $w = U_1 \ldots U_r S(x)$, then $a.w = a.s = 1$. Now apply Lemma 5.3 first with $x$, then with $x$ replaced by $w$, to obtain the result.

If $m(x) > 1$, then we reduce $m(x)$ to 1 exactly as we did in the proof of the previous proposition.

## 7. *Orbits for line and blown up line graphs*

Let $L_n = \{e_1, \ldots, e_n\}$ be the line graph as in §3. Our main result on orbits is the following:

THEOREM 7.1. *Let $V = \langle L_n \rangle$ and let $x, y \in V \backslash \mathrm{rad}(V)$. Then $x$ and $y$ lie in the same orbit under the action of $Tv(L_n)$ if and only if $x$ and $y$ have the same number of components.*

*Proof.* In the terminology used in the proof of Theorem 3.4, any element $x$ of $V$ corresponds to a union of disjoint edges of $\Delta^n$, one for each connected component of $x$. Further, if $f_1, \ldots, f_m$ and $g_1, \ldots, g_m$ are two sets of disjoint edges of $\Delta^n$, then there is an $\alpha$ in $\mathrm{Aut}\,\Delta^n$ such that $\alpha f_i = g_i$, for $i = 1, \ldots, m$. (The proof is an easy induction on $m$.) The theorem follows.

We continue by determining orbits for the blown-up line graph.

As in §4, let $\langle L_n^m \rangle$ denote the symplectic space determined by $L_n^m$ and let $p: \langle L_n^m \rangle \to \langle L_n \rangle$ denote the standard projection.

THEOREM 7.2. *Let $V = \langle L_n^m \rangle$, and let $x, y \in V \backslash \mathrm{rad}(V)$. Then $x, y$ lie in the same orbit under the action of $Tv(L_n^m)$ if and only if $px, py$ have the same number of components relative to $L_n$. If $n \geqslant 4$, $m \geqslant 1$, then $Tv(L_n^m) \neq Sp_0(V)$.*

*Proof.* Let $P = L_n^m$, $L = L_n$, and abbreviate $\sim_P$ to $\sim$.

Suppose first that $y = Ax$ where $a$ is a vertex of $L_n^m$. Then $py = Bpx$ where $b$ is a vertex of $L_n$. Hence $py, px$ have the same number of components, by Theorem 7.1. From this we deduce the necessity part of the theorem.

We know from Theorem 7.1 that $px \sim_L py$ if and only if $\pi px = \pi py$ (where $\pi$ gives the number of components with respect to $L$). However $px \sim_L py$ implies $px \sim py$. So it is sufficient for the first part of the theorem to prove that if $z \in V \backslash \mathrm{rad}(V)$, then $z \sim pz$.

By [I, Proposition 4.3] we may assume $z$ is discrete. By Proposition 6.2, we may assume $z$ is sociable. Then $z$ contains at most one of the vertices $d_0 = e_n, d_1, \ldots, d_m$. If $z$ is contained in $L = L_n$, we have finished. Otherwise, assume $d_i$ is a vertex of $z$. Let $L'$ be the line graph $\{e_1, \ldots, e_{n-1}, d_i\}$. Then $z$ is not isolated in $L'$ and so $z$ may by operations of $Tv(L')$ be moved to $w$ where $d_i$ is not a vertex of $w$. Further, $\pi pz = \pi pw$, by Theorem 7.1 (applied to $L'$). Since $pw = w$, and $w, pz \in \langle L \rangle$, we have $w \sim_L pz$, by Theorem 7.1. Hence $z \sim pz$.

The last statement now follows, since $Tv(L_n^m)$ then does not act transitively on $V \backslash \mathrm{rad}(V)$.

EXAMPLE 7.3. Using this last result, we determine $v_n^m = N(L_n^m)$ the number of elements in the orbit of a vertex under the action of $Tv(L_n^m)$. For this purpose it is convenient to assume $d_1, \ldots, d_m$ are adjacent to $e_2$ (rather than to $e_{n-1}$, as before). Then we have the recurrence relation

$$v_n^m = v_{n-1}^m + n2^m, \quad \text{where } n \geqslant 3.$$

*Proof.* The term $v_{n-1}^m$ corresponds to elements of the orbit whose graph does not include $e_n$. If $e_n$ is included, then it must be part of a connected element $e_i + e_{i+1} + \ldots + e_n$, by Proposition 7.2. If $i \geqslant 3$ and $e_{i-1}$ is not included, we may also add in any even number of $e_1, d_1, \ldots, d_m$, giving $2^m$ possibilities. If $i = 2$, we may add in any number of $e_1, d_1, \ldots, d_m$, giving $2^{m+1}$ possibilities. Hence

$$v_n^m = v_{n-1}^m + (n-2)2^m + 2^{m+1},$$

as required.

Note also that $v_2^m = v_3^{m-1}$. By induction on $m$ one finds $v_3^m = 3.2^{m+1}$, and it follows easily that

$$v_n^m = 2^{m-1} n(n+1).$$

We now consider some line and blown-up line graphs $G(S)$ where $S$ spans a symplectic space $V$ over $\mathbf{F}_2$ but is not a basis.

PROPOSITION 7.4. *Let $S$ be a subset of $V \backslash \mathrm{rad}(V)$ such that $S$ is linearly dependent, $S$ spans $V$, and the graph $G(S)$ is a line graph $L_n = \{e_1, e_2, \ldots, e_n\}$. Then $n$ is odd, $n \geqslant 5$,* $\dim V = n - 1$, *and*

$$e_1 + e_3 + \ldots + e_{n-2} + e_n = 0.$$

*Further $Tv(S) = Sp_0(V)$ if and only if $n = 5$.*

*Proof.* Clearly $n > 1$ (since $S \subseteq V \backslash \mathrm{rad}(V)$).

Let $i$ be the largest integer such that $\{e_1, e_2, \ldots, e_i\}$ is linearly independent. Then $i > 1$. If $i = 2$ then $e_3 = e_1 + e_2$ and $G(S)$ is not a tree. So $i > 2$.

The incidence relations on $\{e_1, e_2, \ldots, e_{i+1}\}$ imply that $i$ is even and

$$e_{i+1} = e_1 + e_3 + \ldots + e_{i-1}.$$

If $i + 1 < n$, then $e_{i+2} \cdot e_{i+1} = 1$ and so $e_{i+2} \cdot e_j = 1$ for some $j \leqslant i$, contradicting the fact that $G(S) = L_n$. So $i + 1 = n$ and $n$ is odd.

Suppose $n = 5$, so that $S = \{e_1, e_2, e_3, e_4, e_1+e_3\}$. The elements of $V\backslash \mathrm{rad}(V)$ have one or two components with respect to the basis $L_4 = \{e_1, e_2, e_3, e_4\}$ of $V$. But $E_5(e_4) = e_1+e_3+e_4$ has two components and so Theorem 7.1 implies that $Tv(S)$ acts transitively on $V\backslash \mathrm{rad}(V)$. Hence $Tv(S) = Sp_0(V)$.

Suppose $n$ is odd and $n > 5$. Let

$$x = e_i + e_{i+1} + \ldots + e_j,$$

where $i \leqslant j$, be a connected element of $V$ (with respect to the basis $L_{n-1}$). If $e_n.x = 1$ then $j = n$ and $e_n + x$ has $\frac{1}{2}(n-1)$ components. Conversely, if $y$ has $\frac{1}{2}(n-1)$ components then $y = e_n$ or $y = e_n + e_i + e_{i+1} + \ldots + e_{n-1}$ for some $1 \leqslant i \leqslant n-1$. So $E_n(y)$ has $\frac{1}{2}(n-1)$ components or 1 component. It follows that $Tv(S)$ does not act transitively on $V\backslash \mathrm{rad}(V)$.

We now wish, in the circumstances of this last proposition, to compute $Tv(S)$. We follow the method of §3, but only sketch the argument. We first need a result corresponding to Theorem 3.2.

PROPOSITION 7.5. *Let $n$ be odd, let $L = L_{n-1} = \{e_1, e_2, \ldots, e_{n-1}\}$ be a line graph, let $V = \langle L_{n-1}\rangle$, and let*

$$e_0 = e_2 + e_4 + \ldots + e_{n-1}.$$

*Let $L' = L \cup \{e_0\}$.*

*Let $R$ be a set of elements of $V$ such that $T = G(R)$ is a tree and each element of $R$ has one component or $\frac{1}{2}(n-1)$ components with respect to $L$. Let $x_0$ be an end vertex of $T$. Then there is an $\alpha \in Tv(L')$ such that $\alpha$ maps $R$ into $L'$ and $x_0$ to $e_0$. Hence $T$ is a line graph.*

We leave the proof to the reader. It is similar to that of Theorem 3.2, but uses the fact that the elements of $V$ with $\frac{1}{2}(n-1)$ components are of the form $e_0$ or $f_i + e_0$, where $f_i$ is the connected element $e_1 + e_2 + \ldots + e_i$, with $1 \leqslant i \leqslant n-1$.

COROLLARY 7.6. *Under the assumptions of Proposition 7.4 on $L$ and $L'$, we have $Tv(L') \cong S_{n+1}$.*

*Proof.* The proof is similar to that of Theorem 3.4, but one introduces a vertex $v_0$ and edges $e_0$ and $e_0 + e_1 + e_2 + \ldots + e_i$ joining $v_0$ to $v_1$ and to $v_{i+1}$, for $1 \leqslant i \leqslant n-1$ respectively.

PROPOSITION 7.7. *Let the symplectic space $V'$ be spanned by a subset $S'$ such that $G(S') = L_n^m$, where $m \geqslant 1$. Then $Tv(S')$ is not isomorphic to a symmetric group, and if $n > 5$ then $Tv(S') \neq Sp_0(V')$.*

*Proof.* Let $S' = \{e_1, \ldots, e_{n-1}, d_0, \ldots, d_m\}$ as usual with $\{e_1, \ldots, e_{n-1}\}$ forming a line graph $L_{n-1}$, and $d_i.e_{n-1} = 1$, for $i = 0, \ldots, m$, all other products being zero.

If some set $\{e_1, \ldots, e_{n-1}, d_i\}$ is linearly dependent, then, as in Proposition 7.3, $n$ is odd and $d_i = e_1 + e_3 + \ldots + e_{n-2}$. This relation can hold for at most one $i$, and since $m \geqslant 1$, we may assume that $\{e_1, \ldots, e_{n-1}, d_0\}$ is linearly independent, forming a line graph which we write $L_n$.

Let $M$ be a non-empty minimal linearly dependent subset of $S'$. If some $e_i$ belongs to $M$, then the adjacency relations imply that $n$ is odd, that $e_1, e_3, \ldots, e_{n-2} \in M$, and that the other distinct elements of $M$ are $d_{i_1}, \ldots, d_{i_s}$, say, where $s$ is odd. By minimality, the sum of the elements of $M$ is zero, and $M' = \{e_1, e_2, \ldots, e_{n-1}, d_{i_2}, \ldots, d_{i_s}\}$ is linearly independent. Extend $M'$ to a basis $P$ of $V'$ by adding various $d_i$ to $M'$. Define $p$: $V' \to \langle L_n \rangle$ by sending the $e_i$ identically and by sending the $d_i$ in $P$ to $d_0$. Let $C_k$ be the set of elements $x$ of $V'$ such that $p(x)$ has $k$ components relative to $L_n$, and let $n = 2r+1$. Then the orbit of a vertex of $S'$ under the action of $Tv(S')$ is $C_1 \cup C_r$, by Theorem 7.2. Let $S'' = S' \cup C_1 \cup C_r$. Then $Tv(S') = Tv(S'')$.

Let $V$ be the subspace of $V'$ with basis $M'$, and define $p'$: $V' \to V$ by mapping $M'$ identically and defining $p'(d_i) = d_{i_1}$ for $d_i \in P \backslash M'$. Then $\operatorname{Ker} p'$ has a basis $Q$ of elements $d_i + d_{i_1}$, for $d_i \in P \backslash M'$. Let $S = p'(S'')$. It can be checked that $S \subset S''$. We now show that Theorem 6.6 of [I] applies to $p'$ and $S''$. Let $c = d_i + d_{i_1}$, where $d_i \in P \backslash M'$. Then $a = d_i \in S$ and $c + d_{i_1} \in S''$; also $p(d_i) = d_0 \in S''$. So Theorem 6.6 of [I] applies and $Tv(S'')$ contains a normal, abelian subgroup whose elements are of order 2. As in the proof of Corollary 4.4, this shows that $Tv(S'')$ is not a symmetric group. Also $V' \backslash \operatorname{rad}(V') \neq S''$, since $n > 5$. So $Tv(S'') \neq Sp_0(V')$.

We now consider the case where no $e_i$ belongs to $M$. Then $M = \{d_{i_1}, \ldots, d_{i_s}\}$, and the sum of the elements of $M$ is zero. Hence $s$ is even, since $d_{i_1} . e_{n-1} = 1$. Theorem 7.2 shows that $d_{i_1}$ lies in the orbit of $e_{n-1}$ under the action of $Tv(S' \backslash \{d_{i_1}\})$. Hence $Tv(S') = Tv(S' \backslash \{d_{i_1}\})$, and we can reduce to the case where $\{d_0, d_1, \ldots, d_m\}$ is linearly independent. This completes the proof.

We now extend some of the above results to arbitrary subsets $S$ of $V$. For this, we need a more precise notation than $Tv(S)$.

Let $S$ be a subset of $W$, where $W$ is a subspace of the symplectic space $V$. Then transvections from $S$ can be considered as operating on $W$ or on $V$. The subgroups of $Sp_0(V)$, $Sp_0(W)$ generated by transvections from $S$ will for the rest of this section be written $Tv(S; V)$, $Tv(S; W)$ respectively. Clearly the action of $Tv(S; V)$ on $V$ leaves $W$ invariant, and the restriction map gives an epimorphism $p$: $Tv(S; V) \to Tv(S; W)$. In general, $\operatorname{Ker} p$ is non-trivial, as is seen by taking $V = \langle L_2 \rangle$, $W = \langle L_1 \rangle$, $S = \{e_1\}$.

PROPOSITION 7.8. *Let $S$ be a subset of $V$ such that $G(S) = L_n$. Then $Tv(S; V) \cong S_{n+1}$.*

*Proof.* Let $W$ be the subspace of $V$ spanned by $S$. By Theorem 3.4 and Corollary 7.6, $Tv(S; W) \cong S_{n+1}$. Now for any $a, b \in V$, the following relations hold in $Tv(S; V)$: $AB = BA$ if $a.b = 0$; $ABA = BAB$ if $a.b = 1$. This is proved by evaluating on $v \in V$, and examining the cases given by various adjacencies of $v$ with $a, b$. It follows that the relations $E_i E_j = E_j E_i$ if $|i-j| > 1$, and $E_k E_{k+1} E_k = E_{k+1} E_k E_{k+1}$, for $1 \leqslant i, j \leqslant n$, $1 \leqslant k \leqslant n$, hold in $Tv(S; V)$. But these are a complete set of relations for the corresponding generators of $Tv(S; W) \cong S_{n+1}$. Hence $p$: $Tv(S; V) \to Tv(S; W)$ is an isomorphism.

PROPOSITION 8.9: *If $S$ is a subset of $V$ and $G(S) = L_n^m$, for $n > 2$ and $m > 0$, or for $n = 2$ and $m > 1$, then $Tv(S; V)$ is not isomorphic to a symmetric group.*

*Proof.* Suppose $Tv(S; V)$ is isomorphic to $S_k$. By the conditions on $m, n$, we have $L_3 \subset L_n^m$ and so $Tv(S; V)$ contains a proper subgroup isomorphic to $S_4$, by the previous proposition. Hence $k \geqslant 5$.

Let $W$ be the subspace of $V$ spanned by $S$ and let $p$: $Tv(S; V) \to Tv(S; W)$ be the restriction map. By Proposition 7.7, $Tv(S, W)$ contains a normal subgroup of index not 2, and hence so also does $Tv(S; V)$. This contradicts the simplicity of the alternating group $A_k$, for $k \geqslant 5$.

## 8. *Quadratic forms*

Throughout this section, $V$ is a symplectic space over $\mathbf{F}_2$. As usual, a function $Q$: $V \to \mathbf{F}_2$ is called a *quadratic form* on $V$ if, for all $x, y \in V$,

$$Q(x+y) = Q(x)+Q(y)+x.y.$$

Such a quadratic form is determined by its values on a basis for $V$. The following two facts are well known [**29**].

PROPOSITION 8.1. *Let $Q$ be a quadratic form on $V$. If $a \in V$ satisfies $Q(a) = 1$, then, for all $x \in V$,*

$$Q(Ax) = Q(x).$$

*Proof.* If $Ax = x$, then $Q(Ax) = Q(x)$. Otherwise $Ax = a+x$ and $a.x = 1$. In this case,

$$Q(a+x) = Q(a)+Q(x)+a.x = Q(x).$$

COROLLARY 8.2. *Let $Q$ be a quadratic form on $V$, and let $S$ be a subset of $V$ such that $Q(a) = 1$ for all $a \in S$. Then $Tv(S)$ is contained in the group of isometries of $Q$.*

Let $P$ be a basis of $V$. We write $Q_P$ for the quadratic form on $V$ which takes value 1 on each element of $P$. The following alternative description of $Q_P$ is useful.

PROPOSITION 8.3. *Let $P$ be a basis of $V$, and let $x \in V$. Then $Q_P(x)$ is the* mod 2 *Euler characteristic of the graph $x\,|_P$.*

*Proof.* Let $Q'$ be the function which assigns to $x \in V$ the mod 2 Euler characteristic of $x\,|_P$. We prove that $Q'$ is a quadratic form on $V$. Since $Q'$ and $Q_P$ coincide on $P$, this will prove that $Q' = Q_P$.

Let $x, y \in V$. We have to prove that

$$Q'(x+y) = Q'(x)+Q'(y)+x.y. \qquad (*)$$

Suppose first that $y \in P$. If $x.y = 0$, then there are an even number $2p$, say, of vertices of $x$ adjacent to $y$. Thus adding $y$ to $x$ changes $x\,|_P$ by adding (or subtracting) $2p$ edges and the vertex $y$. So

$$Q'(x+y) = Q'(x)+2p+1 = Q'(x)+Q'(y)+x.y.$$

If $x.y = 1$, then there are an odd number $2p+1$, say, of vertices of $x$ adjacent to $y$. In this case

$$Q'(x+y) = Q'(x)+2p+2 = Q'(x)+Q'(y)+x.y.$$

The general case is proved by induction on the number of vertices of $y\,|_P$, the above being the case of one vertex.

Suppose $y = u+w$ where $u\,|_P$, $w\,|_P$ both have fewer vertices than $y$. Then by the inductive hypothesis

$$\begin{aligned} Q'(x+u+w) &= Q'(x+u)+Q'(w)+(x+u).w \\ &= Q'(x)+Q'(u)+x.u+Q'(w)+(x+u).w \\ &= Q'(x)+Q'(u+w)+x.(u+w). \end{aligned}$$

This concludes the proof.

PROPOSITION 8.4. *Let $P, R$ be bases for $V$ such that $P$ is $t$-equivalent to $R$. Then $Q_P = Q_R$.*

*Proof.* Clearly, we need only consider the case where $R$ is obtained from $P$ by an elementary $t$-operation $t = t_{ab}$ where $a.b = 1$. Thus $P = \{a, b, \ldots\}$, $R = \{a, a+b, \ldots\}$. But then $Q_P(a+b) = 1 = Q_R(a+b)$. Hence $Q_P = Q_R$.

As an application of this result, let $L$ be the line graph $L_4$ and let $L' = \{e_1+e_3, e_4, e_3, e_2\}$ in that order. Then $L'$ is also a line graph, $Q_L(e_1) \neq Q_{L'}(e_1)$. Hence $L$ is not $t$-equivalent to $L'$. Thus isomorphic graphs in a symplectic space need not be $t$-equivalent.

We now give results on the realizability of a quadratic form as $Q_P$ for some $P$.

Recall that the *rank* of $V$ is the dimension of $V/\mathrm{rad}(V)$, and that rank$(V)$ is even.

THEOREM 8.5. *Suppose* rank$(V) \geqslant 4$ *and $Q$ is a quadratic form on $V$. Then there is a basis $P$ for $V$ such that $G(P)$ is a forest and $Q = Q_P$. Moreover, if* rank$(V) \geqslant 6$, *we can find such a basis $P$ with $G(P)$ a tree. If* rank$(V) \geqslant 8$, *we can find a basis $P$ with $G(P)$ a tree containing $E_6$.*

*Proof.* By the definition of quadratic form, it is sufficient to find a basis $P$ for $V$ such that $Q(a) = 1$ for all $a \in P$.

Since rank$(V) > 3$ there is a regular subspace $W$ of $V$ of dimension 4. Let $\{e_1, e_2, f_1, f_2\}$ be a symplectic basis for $W$.

We first show that we may assume $Q(e_1) = 1$. If $Q(e_1) = 1$ then we have finished. If not, but $Q(f_1) = 1$, then we interchange $e_1$ and $f_1$, and we have finished. If $Q(e_1) = 0 = Q(f_1)$, then $Q(e_1+f_1) = 1$ and we replace $e_1$ by $e_1+f_1$, the basis remaining symplectic.

A similar argument shows that we may assume that $Q(e_2) = 1$.

Let $g_1 = f_1$ if $Q(f_1) = 1$, and $g_1 = f_1+e_2$ if $Q(f_1) = 0$. Then $Q(g_1) = 1$, $e_1.g_1 = 1$.

Extend $R = \{e_1, g_1\}$ to a basis $R'$ of $V$, and let $d \in R'\setminus R$. We now show that there is an element $d_1 \in \langle R\rangle$ such that $Q(d+d_1) = 1$.

If $Q(d) = 1$, we take $d_1 = 0$. Suppose $Q(d) = 0$. If $d.e_1 = 0$, we take $d_1 = e_1$. If $d.e_1 = 1$, $d.f_1 = 0$, we take $d_1 = f_1$. If $d.e_1 = d.f_1 = 1$, we take $d_1 = e_1+f_1$.

Let $S$ be the basis obtained from $R'$ by replacing each $d \in R'\setminus R$ by $d+d_1$. Then $Q(a) = 1$ for all $a \in S$, and so $Q = Q_S$. By Theorem 3.3 of [I], $S$ is $t$-equivalent to a forest $P$, and $Q_S = Q_P$ by Theorem 8.3.

Now suppose that rank$(V) \geqslant 6$ and that $P$ has three or more components. Let $a, b, c$ be vertices in different components and assume $c$ belongs to a component with more than one vertex. Then $Q(a+b+c) = 1$. We thus replace $a$ by $a+b+c$ and it is clear that the new graph has at least one less component than the original.

By this argument and Theorem 3.3 of [I] we may assume that $G(P)$ is a forest with at most two components. If $G(P)$ has two components, choose vertices $a, b, c$ of $G(P)$ such that $a.b = a.c = b.c = 0$ and $c$ lies in a different component than $a$ (this is possible since $G(P)$ is a forest and $\mathrm{rank}(V) \geqslant 6$). Then $Q(a+b+c) = 1$ and we replace the element $a$ of $P$ by $a+b+c$. Now $G(P)$ has only one component and Theorem 3.3 of [I] gives the result.

Lastly, if $\mathrm{rank}(V) \geqslant 8$ and $G(P)$ does not contain $E_6$ then by Theorems 4.2 and 8.3 we may assume that $G(P) = L_n^m$ where $n \geqslant 8$. Here we replace $e_1$ by $e_1+e_3+e_5$ to get $P'$. It is easily checked that $e_6$ is a centre for an $E_6$ in $G(P')$. This completes the proof.

REMARKS. (1) The last result is not true if $\mathrm{rank}(V) = 2$. To see this let $V$ be a symplectic space with $\mathrm{rank}(V) = 2$. Then there is a basis $P$ with elements $a, b$ of the basis $P$ such that $a.b = 1$ and $P \backslash \{a, b\} \subset \mathrm{rad}(V)$. Let $Q$ be the quadratic form with $Q(d) = 0$ for all $d \in P$. Then $Q \neq Q_P$ and it is easily seen that if $x \in V$, then $Q(x) = 1$ if and only if both $a$ and $b$ are vertices of $x$. Thus if $x.y = 1$, then we have either $Q(x) = 0$ or $Q(y) = 0$. Now if $R$ is another basis for $V$ then there are elements $c, d$ in $R$ such that $c.d = 1$ and $Q_R(c) = Q_R(d) = 1$. Thus $Q \neq Q_R$.

(2) Theorem 8.5 gives a way of visualizing quadratic forms $Q$. For if $Q = Q_F$ where $F$ is a forest, then $Q(x)$ is simply the number of components (mod 2) of $x|_F$.

PROPOSITION 8.6. *Suppose that $P$ and $R$ are bases of $V$ with connected graphs, and satisfying $Tv(P) = Tv(R)$. Then $Q_P = Q_R$.*

*Proof.* Suppose $Q_P \neq Q_R$. Since a quadratic form is determined by its values on any basis, there is an $x \in P$ such that $Q_R(x) \neq Q_P(x)$, that is, such that $Q_R(x) = 0$. Now $X \in Tv(P) = Tv(R)$ and so $X$ preserves $Q_R$, by Proposition 8.1. However, since $P$ is connected with more than one element, there is a $y \in P$ with $y.x = 1$. Then

$$Q_R(X(y)) = Q_R(x+y) = Q_R(x)+Q_R(y)+1 = Q_R(y)+1.$$

This contradiction completes the proof.

We now recall the classification of quadratic forms $Q$ associated to a symplectic space $V$ over $\mathbf{F}_2$. A convenient reference is [**26**, Chapter III, § 1]. The cardinality of a set $S$ is written $|S|$.

8.7. *Let $V$ be a symplectic space of dimension $2m+s$, where $s =$ $\mathrm{dim}(\mathrm{rad}(V))$. Let $Q$ be a quadratic form associated to $V$.*

(i) *If $Q$ is zero on* $\mathrm{rad}(V)$ *then an element* $\mathrm{Arf}(Q) \in \mathbf{F}_2$ *is defined and determines $Q$ up to equivalence. Further, if $\varepsilon = 0, 1$ then*

$$|Q^{-1}(\varepsilon)| = (2^{2m-1}+2^{m-1})2^s \qquad \textit{if } \mathrm{Arf}(Q) = \varepsilon,$$
$$|Q^{-1}(1-\varepsilon)| = (2^{2m-1}-2^{m-1})2^s \quad \textit{if } \mathrm{Arf}(Q) = 1-\varepsilon.$$

(ii) *If $Q$ is not zero on* $\mathrm{rad}(V)$ *then $Q$ is determined up to equivalence by $V$. Further,*

$$|Q^{-1}(0)| = |Q^{-1}(1)| = 2^{(\dim V)-1}.$$

PROPOSITION 8.8. *If $Q$ is the quadratic form determined by the basis $L_n$ of $V$ then* $\mathrm{Arf}(Q)$ *is undefined if* $n \equiv 1 \bmod 4$, $\mathrm{Arf}(Q) = 1$ *if* $n \equiv 2, 3, 4 \bmod 8$, *and* $\mathrm{Arf}(Q) = 0$ *if* $n \equiv 0, 6, 7 \bmod 8$.

*Proof.* Two non-equivalent quadratic forms on $V$ for $n = 2$ are $Q_0$ and $Q_1$ which take values 0 and 1 respectively on each of $e_1, e_2$. Then $Q_0$ and $Q_1$ have Arf invariants 0 and 1 respectively.

In general, $\mathrm{rad}(V)$ is non-zero if and only if $n$ is odd; also $Q(\mathrm{rad}(V)) = \{1\}$ if and only if $n = 4r+1$. A symplectic basis for $V/\mathrm{rad}(V)$ is given by the image of the set

$$\{e_1, e_2; e_1+e_3, e_4; e_1+e_3+e_5, e_6; e_1+e_3+e_5+e_7, e_8; \ldots\},$$

and so the induced quadratic form on $V/\mathrm{rad}(V)$ is of the type $Q_1+Q_0+Q_1+Q_0+\ldots$. Since $Q_1+Q_1$ is equivalent to $Q_0+Q_0$, and the forms $mQ_0$, $Q_1+(m-1)Q_0$ have Arf invariants 0, 1 respectively, the result follows.

Let $M_n^p$ denote the graph $L_n \cup \{g_p\}$ where $g_p$ is adjacent only to $e_p$. Thus $M_5^3 = E_6$. We determine the type of the quadratic form $Q$ determined by $M_n^p$ for $p = 3, 5$.

PROPOSITION 8.9. *Let $V$ be the symplectic space with basis $M_n^p$, where $p = 3$ or 5, $n \geqslant 5$, and let $Q$ be the quadratic form determined by $M_n^p$. Then $\mathrm{Arf}(Q)$ is undefined if $p = 3$ and $n \equiv 2 \bmod 4$, or if $p = 5$ and $n \equiv 0 \bmod 4$. Otherwise,*

$$\mathrm{Arf}(Q) = \begin{cases} 0 & \text{if } n+p \equiv 2, 3, \text{ or } 4 \bmod 8, \\ 1 & \text{if } n+p \equiv 6, 7, \text{ or } 0 \bmod 8. \end{cases}$$

*Proof.* First consider the case where $p = 3$. Then we obtain a basis for $V$ of the following type:

$$\{e_1, e_2+g_3; e_3, g_3; g_3+e_4, e_5; g_3+e_4+e_6, e_7; g_3+e_4+e_6+e_8, e_9; \ldots\}$$

ending at $e_n$ if $n$ is odd, and $w = g_3+e_4+e_6+\ldots+e_n$ if $n$ is even. If $n$ is odd, this basis is symplectic and $V$ is regular. If $n$ is even, then rad $V$ has $w$ as a basis, and $Q(w) = 1$ if and only if $n \equiv 2 \bmod 4$, in which case $\mathrm{Arf}(Q)$ is not defined. It is now easily checked that $\mathrm{Arf}(Q) = 0$ if $n \equiv 7, 0, 1 \bmod 8$, and $\mathrm{Arf}(Q) = 1$ if $n \equiv 3, 4, 5 \bmod 8$.

The case where $p = 5$ is similar using the basis of the type

$$\{e_1, e_2+e_4+g_5; e_3, e_4+e_5; e_5, g_5; g_5+e_6, e_7;$$
$$g_5+e_6+e_8, e_9; g_5+e_6+e_8+e_{10}, e_{11}; \ldots\}.$$

## 9. *More basic moves*

Throughout this section $V$ is a symplectic space over $\mathbf{F}_2$ and $P$ is a basis for $V$ such that $T = G(P)$ is a tree.

Let $d \in P$. Let $C$ be a component of $G(P\backslash\{d\})$. Let $\langle C\rangle$ denote the subspace of $V$ spanned by the vertices of $C$. For $x \in V$, we let $x_C$ denote the element of $V$ corresponding to $x|_P \cap C$. We say $x$ is *isolated* in $C$ (*sociable* in $C$) if $x_C$ is isolated (sociable) in $\langle C\rangle$.

LEMMA 9.1. *Let $x \in V$ be sociable. Then either $x$ is sociable in $C$ or $d.x_C = 1$. In the latter case, if $y$ is isolated in $C$ and $y \subset_C x_C$, then $d.y = 1$.*

*Proof.* Suppose that $x$ is not sociable in $C$. Let $y$ be isolated in $C$ and such that $y \subset_C x_C$. Then $y.C = \{0\}$. Also if $f$ is a vertex of $T\backslash(C \cup \{d\})$, then $\delta(f, C) > 1$ since $T$ is a tree, and so $f.y = 0$. Since $x$ is sociable, $y$ is not isolated and so $d.y = 1$.

Let $e$ be the unique vertex of $C$ adjacent to $d$. Then $e$ is a vertex of $y$, and so of $x$. Thus $d.x_C = d.e = 1$.

Our next result will describe a standard situation in which we are able to reduce the number of vertices of $x \in V \backslash \mathrm{rad}(V)$ by an action of $Tv(P)$.

LEMMA 9.2. *Let $d \in T$ and let $x$ be a discrete, sociable element of $V$ which does not contain the vertex $d$. Assume that $x$ meets at least three different components of $T \backslash \{d\}$. Then $x \sim y$ where $y$ has less components than does $x$.*

*Proof.* Let $C$ be a component of $T \backslash \{d\}$ where $x_C$ has no vertex adjacent to $d$. Then by Lemma 9.1, $x$ is sociable in $C$. By Proposition 6.2 applied to $x_C$ and $C$, there is $\alpha \in Tv(C)$ such that $\alpha(x_C)$ is discrete, has a vertex adjacent to $d$, has no more components than does $x_C$ and is sociable in $C$. Since $d$ is not a vertex of $x$, $\alpha(x)_C = \alpha(x_C)$, and so replacing $x$ by $\alpha(x)$ increases the number of vertices of $x$ adjacent to $d$ by one.

A similar argument (using Proposition 6.1), shows that if $x$ is sociable in $C$ and $x_C$ has a vertex adjacent to $d$, then $x \sim y$ where $y$ is discrete, has no more components than does $x$, $y$ is sociable, and $y$ has one less component next to $d$ than does $x$.

By the above argument, the conditions on $x$, and Lemma 9.1, we may assume that $x$ has $r > 2$ vertices adjacent to $d$.

If $d.x = 1$, then $D(x)$ has fewer components than has $x$.

If $d.x = 0$, then $r > 3$ is even.

Suppose that there is a component $C$ of $T \backslash \{d\}$ with $x$ sociable in $C$ and let $e$ be the unique vertex of $C$ adjacent to $d$. If $e$ is a vertex of $x$ then by the above we may move $x$ off $e$ by an action of $Tv(P)$ changing only $x_C$. Now we have the case where $d.x = 1$ and since $r > 3$ we have finished. If $x$ is sociable in $C$ and $e$ is not a vertex of $x$, then by the above, we may move $x$ onto $e$ by an action of $Tv(P)$. Now $d.x = 1$ and we have finished.

Now suppose that $x_C$ is not sociable for all components $C$ of $T \backslash \{d\}$. Let $C$ and $D$ be two such components and let $w \subset x_C$, $u \subset x_D$ be isolated in $C$, $D$ respectively. By Lemma 9.1 we have $w.d = u.d = 1$. Thus $d.(w+u) = 0$. If $e$ is a vertex of $C$ or $D$ then $e.w = e.u = 0$. If $e$ is a vertex which is not in $C$ or $D$ then $e.(w+u) = 0$ and so $u+w$ is isolated. This is a contradiction and so there is always a component $C$ of $T \backslash \{d\}$ such that $x_C$ is sociable.

The result now follows.

In [I] we showed that the action of $Tv(S)$ on $V$ is transitive on $S$ if $G(S)$ is connected. We now prove:

THEOREM 9.3. *Let $S$ be a spanning set of $V$ such that $T = G(S)$ is a tree. Let*

$$dS = \{(a, b) \in S \times S \colon a+b \notin \mathrm{rad}(V) \text{ and } a.b = 0\}.$$

*Then the set $\{ a + b : (a,b) \in dS\}$ is contained in a single orbit of the action of $Tv(S)$ on $V$.*

*Proof.* Suppose first that $S$ is a basis for $V$. Let $(a,b) \in dS$.

As $dS \neq \varnothing$ then $\dim(V) > 2$ and $T$ has a vertex $c$, say, which is not an end vertex. Let $e$ be an end vertex of $T$ furthest away from $c$. If $e$ is adjacent to $c$ then $T$ is an $L_2^m$ for some $m > 0$. In this situation $dS = \varnothing$. Thus we may assume that $e$ is not adjacent to $c$.

Let $f$ be another end vertex of $T$ not in the same component of $T \backslash \{c\}$ as that of $e$. If

$g$ is a vertex of $T$ adjacent to $f$, we have $g.(e+f) = 1$ and so $e+f$ is not isolated. Also $e.f = 0$. Thus $(e, f) \in dS$.

We now show that $e+f \sim a+b$. By Propositions 6.2 and 8.1 we see that $a+b \sim y$ where $y$ is not isolated, $y$ is discrete, $y$ has no more components than does $a+b$, $Q_T(y) = Q_T(a+b) = 0$, and $e$ is a vertex of $y$. Thus $y = e+h$ where $h$ is a vertex of $T$ with $e.h = 0$.

Since $e$ is an end vertex of $T$ at maximal distance from $c$ we have $\delta(h, c) \leqslant \delta(e, c)$. Let $h, u, s, \ldots, f$ be the vertices along a shortest path $\zeta$ in $T$ from $h$ to $f$. Let $v$ be the unique vertex of $T$ adjacent to $e$. If $v$ is not a vertex of $\zeta$, then by Corollary 2.2 of [I] we may find $\alpha \in Tv(T\backslash\{v\})$ such that $\alpha(h) = f$ and so $\alpha(h+e) = e+f$ and we have finished.

If $v$ is a vertex of $\zeta$, then $u.e \neq 0$ (that is, $v = u$) since $\delta(e, c)$ is maximal (Fig. 7). Here $e+h$ is isolated, contradicting our assumption on $a+b$.

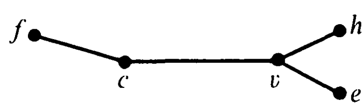


FIG. 7

Thus $e+f \sim a+b$ as required.

Suppose now that $S$ is a spanning set for $V$. Then we may apply the above argument to a symplectic extension $p$: $V' \to V$ of $V$ with basis $S'$ of $V'$ such that $pS' = S$. The result for $S$ and $V$ follows.

## 10. *Orbits: orthogonal case*

Our main result in this section, and one of the major results of this paper, is the following description of the orbits in the orthogonal graph case.

THEOREM 10.1. *Let $V$ be a symplectic space over $\mathbf{F}_2$ and let $P$ be a basis of $V$ of orthogonal type. Let $x$ and $y$ be elements of $V\backslash\mathrm{rad}(V)$. Then $x$ and $y$ lie in the same orbit under the action of $Tv(P)$ if and only if $Q_P(x) = Q_P(y)$.*

*Proof.* By Theorem 3.3 of [I] and our assumption on $P$, we may assume that $T = G(P)$ is a tree graph containing $E_6$.

The necessity follows from the fact that $Q_P$ is an invariant of the action (Proposition 8.1).

The sufficiency will follow if we can show that $x \in V\backslash\mathrm{rad}(V)$ is in the orbit of either a vertex of $T$ or the sum of two vertices $a$ and $b$ where $a.b = 0$ and $a+b$ is not isolated (see Corollary 2.2 of [I] and Theorem 9.3). This fact is immediate from the following proposition, which uses the fact that if $d$ is a centre of an $E_6$ in a tree $T$, then $T\backslash\{d\}$ has at least three components at least two of which have more than two vertices.

PROPOSITION 10.2. *Let $P$ be a basis for $V$ with $T = G(P)$ a tree containing $E_6$. If $x \in V\backslash\mathrm{rad}(V)$ has more than two components, then $x \sim y$ where $y$ has less components than does $x$.*

*Proof.* By Proposition 5.2 we may assume that $x$ is discrete and sociable. The idea of the proof is to reduce to the situation in Lemma 9.2.

Let $d$ be the centre of an $E_6$ in $T$. By Proposition 6.1 we may assume that $d$ is not a vertex of $x$.

If $x$ meets at least three components of $T\backslash\{d\}$ then Proposition 9.2 gives the result. So we prove that $x$ can be changed by the action of $Tv(T)$ to obtain this condition.

Assume that $x$ is contained in a component $C$ of $T\backslash\{d\}$ and let $e$ be the unique vertex of $C$ adjacent to $d$. If $e$ is not a vertex of $x$, then Lemma 9.1 shows that $x$ is sociable in $C$. By Proposition 6.2, $x \sim z$ where $e$ is a vertex of $z$. Let $f \neq e$ be another vertex of $T$ adjacent to $d$. Then $z' = DFED(z)$ is $z$ with $f$ replacing the vertex $e$, no other vertices being changed. So $x \sim z'$ where $z'$ meets two components of $T\backslash\{d\}$.

Assume that $x$ meets two components $C_1, C_2$ of $T\backslash\{d\}$. Then we may write uniquely $x = x_1 + x_2$ where $x_1, x_2$ are contained in $C_1, C_2$ respectively. Since $x$ has more than two components, we may assume that $x_1$ has more than one vertex. Let $e, f$ be respectively the vertices of $C_1$ and $C_2$ adjacent to $d$ (Fig. 8). Let $h$ be another vertex of $T$ adjacent to $d$. If $C_2 = \{f\}$, we assume $h$ is in a component $C_3$ of $T\backslash\{d\}$ with more than one vertex.

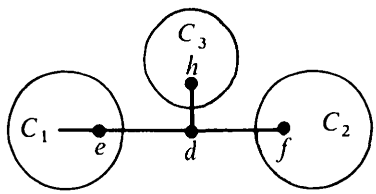


FIG. 8

*Case* (i): *$f$ is not a vertex of $x$.* Then we can, as above, assume $e$ is a vertex of $x_1$; so $z = DHED(x)$ meets $C_1, C_2, C_3$ and we have finished.

*Case* (ii): *$f$ is a vertex of $x_2$ and $C_2$ has more than one vertex.* (a) If $x_2$ is not isolated in $C_2$ then by Proposition 6.1 we may move $x_2$ in $C_2$ off $f$, bringing us back to Case (i).

(b) If $x_2$ is isolated in $C_2$, then $x_2$ has more than one component; for if $x_2 = f$ and $b$ is a vertex of $C_2$ adjacent to $f$, then $b.f = 1$ and so $x_2$ is not isolated. If also $x$ is isolated in $C_1$, then $e$ is a vertex of $x$ (by Lemma 9.1) and $x.d = 0$; hence $x$ is isolated, and we have a contradiction. So $x$ is not isolated in $C_1$. Hence we can move $x_1$ in $C_1$ off $e$ (if necessary) and change $f$ to $h$ by operating with $DHFD$.

*Case* (iii): *$x_2 = f$ and $C_2 = \{f\}$.* (a) If $e$ is not a vertex of $x_1$, then $DHFD(x)$ is $x$ with $f$ replaced by $h$. So we are in Case (ii) with $C_2$ replaced by $C_3$.

(b) If $e$ is a vertex of $x_1$ then $x.d = 0$ and so $x$ is not isolated in $C_1$ (since $x$ is not isolated). Hence $x_1$ can be moved in $C_1$ off $e$, and we are back to Case (iii)(a).

COROLLARY 10.3. *Let $V$ be a regular symplectic space over $\mathbf{F}_2$ and let $P$ be a basis of $V$ such that $G(P)$ is of orthogonal type, with associated quadratic form $Q_P$. Let $S$ be a subset of $V$ containing $P$ and such that $Q_P(a) = 1$ for all $a \in S$. Then $Tv(S)$ is the group of isometries of the quadratic form $Q_P$.*

*Proof.* Let $O_P$ be the group of isometries of the quadratic form $Q_P$. We know already that $Tv(S) \subset O_P$. Since $V$ is regular and $\dim V \leqslant 6$, Proposition 14 on p. 42 of [**29**] gives that $O_P \subset Tv(S')$ where $S'$ is the set of elements $a$ of $V$ such that $Q_P(a) = 1$. However, by Theorem 10.1, if $a \in S'$ then there are an $\alpha \in Tv(P)$ and $b \in P$ such that $a = \alpha(b)$, whence $A = \alpha B \alpha^{-1} \in Tv(P)$. It follows that $Tv(S') \subset Tv(P)$, and so $Tv(S) = O_P$.

REMARK. Without the assumption in this corollary that $V$ is regular we expect that $Tv(S)$ is the group of isometries of $Q_P$ which are the identity on $\mathrm{rad}(V)$ (see Appendix).

## 11. *Generation of symplectic groups by sets of transvections*

Let $V$ be a symplectic space over $\mathbf{F}_2$. Recall from [I, Theorem 2.7] that if $S$ is a subset of $V\backslash\mathrm{rad}(V)$ such that $Tv(S) = Sp_0(V)$, then $S$ spans $V$ and $G(S)$ is connected.

THEOREM 11.1. *Let $V$ be a symplectic space over $\mathbf{F}_2$ with* $\mathrm{rank}(V) \geqslant 6$. *Suppose that $S$ is a subset of $V\backslash\mathrm{rad}(V)$ and $S = P \cup R$ where $P$ is a basis of $V$.*

*Then $Tv(S) = Sp_0(V)$ if and only if*

(a) *$G(S)$ is connected,*

(b) *$G(S)$ satisfies an orthogonal geometry, and*

(c) *there is an $a \in R$ such that $Q_P(a) = 0$.*

*Proof.* We already have the necessity of (a). The necessity of (b) follows from Propositions 7.3 and 7.6 using the assumption on $\mathrm{rank}(V)$.

To prove the necessity of (c), suppose $Q_P(a) = 1$ for all $a \in S$. Then by Corollary 8.2, $Tv(S)$ preserves the quadratic form $Q_P$. Since $\mathrm{rank}(V) \geqslant 6$, there is an element $x \in V\backslash\mathrm{rad}(V)$ with $Q_P(x) = 0$. Therefore $Tv(S)$ does not act transitively on $V\backslash\mathrm{rad}(V)$. Hence $Tv(S) \neq Sp_0(V)$.

Suppose now that (a), (b), and (c) are satisfied. Choose a symplectic space $V'$ containing $V$ and symplectic projection $p\colon V' \to V$, such that $V'$ has basis $S' = P \cup R'$ where $p$ maps $S'$ bijectively to $S$ and is the identity on $P$. Then $G(S')$ is connected and of orthogonal type. Let $\varphi\colon Tv(S') \to Tv(S)$ be induced by $p$ and the inclusion $i\colon V \to V'$, as in [I, Theorem 6.4]. Let $x \in V\backslash\mathrm{rad}(V)$. Then $ix \in V'$ and $Q_{S'}(ix) = Q_P(x)$. If $Q_P(x) = 1$, there are, by Theorem 10.1, an element $\alpha'$ of $Tv(S')$ and $s \in P$ such that $\alpha'(ix) = is$. Hence $(\varphi\alpha')(x) = s$. If $Q_P(x) = 0$, choose $a \in R$ such that $Q_P(a) = 0$. Then $Q_{S'}(ix) = 0 = Q_{S'}(ia)$. Again by Theorem 10.1, there is an element $\alpha'$ of $Tv(S')$ such that $\alpha'(ix) = ia$. Hence $(\varphi\alpha')(x) = a$.

It follows that $Tv(S)$ acts transitively on $V\backslash\mathrm{rad}(V)$, as required.

REMARK. The cases where $r = \mathrm{rank}(V) < 6$ are easily discussed.

If $r = 2$, then any tree graph in $V$ is some $L_2^m$. A classical result tells us that if $V = \langle L_2 \rangle$, then $Tv(L_2) = Sp(V) = Sp(2, \mathbf{F}_2)$. This is also a special case of our results.

If $r = 4$, then any tree graph in $V$ is some $L_4^m$ or $L_5^m$. If $S$ is a basis for $V$, we know from §7 that $Tv(S)$ does not act transitively on $V\backslash\mathrm{rad}(V)$. If $S$ is not a basis, but is a spanning line graph, then Propositions 7.3 and 7.6 give us that $S = L_5$, and $Tv(S) = Sp_0(V) \cong S_6$.

We now give a result needed in [32]. Recall that if $S$ is a subset of $V$ spanning a subspace $W$ of $V$, then $Tv(S; V)$, $Tv(S; W)$ are the subgroups of $Sp_0(V)$, $Sp_0(W)$ generated by transvections from $S$.

COROLLARY 11.2. *Let $S$ be a subset of $V\backslash\mathrm{rad}(V)$. Then $Tv(S; V)$ is isomorphic to a symmetric group if and only if $S$ is t-equivalent to a line graph.*

*Proof.* Suppose $Tv(S; V)$ is isomorphic to a symmetric group $S_k$. Then $k > 1$, since $S \subset V\backslash\mathrm{rad}(V)$. If $k = 2$, then $S$ is a singleton, which is a line graph $L_1$. If $k > 2$, then $G(S)$ is connected; for if $G(S)$ is the union of two disjoint, non-empty graphs $G(S_1)$,

$G(S_2)$, then the elements of $Tv(S_1; V)$ commute with those of $Tv(S_2; V)$ and so $Tv(S; V)$ is not $S_k$.

By Proposition 7.9, $S$ is not $t$-equivalent to a blown-up line graph. Suppose $S$ is not $t$-equivalent to a line-graph. Then we may suppose $S$ is a tree containing $E_6$. Let $W$ be the subspace of $V$ spanned by $S$. Let $U$ be the subspace of $V$ spanned by $L_5 \subset E_6$. Then $Tv(L_5; V)$ maps onto $Tv(L_5; U)$ which is isomorphic to $S_6$. Hence $k > 5$.

Let $p$: $W \to W' = W/\mathrm{rad}(W)$ be the projection. Let $S' = p(S)$. Then $p$ preserves the form and so $p$ maps $E_6$ isomorphically into $S'$. Hence $S'$ is a tree containing $E_6$, and so $Tv(S'; W')$ is either a symplectic or an orthogonal group on the regular space $W'$. Hence $Tv(S'; W')$ is not a symmetric group. We have surjections

$$S_k = Tv(S; V) \to Tv(S; W) \to Tv(S'; W').$$

Since $k \geqslant 5$ and $Tv(S'; W') \neq \mathbb{Z}_2$, this is a contradiction.

The converse part of the corollary is Proposition 7.8.

We now give some examples and other applications.

EXAMPLE 11.3. Let $L = L_{2n}$ be a line graph where $n > 2$. Let $V = \langle L_{2n} \rangle$, and let $a_i = e_1 + e_3 + \ldots + e_{2i+1}$, for $1 \leqslant i \leqslant n-1$. Then $Q_L(a_i) = i \pmod 2$, and so, by Theorem 11.1,

$$Tv(L_{2n} \cup \{a_i\}) = Sp(2n, \mathbf{F}_2)$$

if and only if $i$ is even and $i \neq n-1$.

EXAMPLE 11.4. Let $P = \{e_1, f_1, \ldots, e_n, f_n\}$ be the standard symplectic basis for $V = \langle P \rangle$, and let $g = f_1 + f_2 + \ldots + f_n$. Then $Tv(P \cup \{g\}) = Sp(2n, \mathbf{F}_2)$ if and only if $n$ is even.

EXAMPLE 11.5. We return to the subject of [9] and give more sets of $2g+1$ Dehn twists which do not generate $M_g$, the mapping class group of the orientable closed surface $T_g$ of genus $g$. Define the following curves on $T_g$ as in Fig. 9.

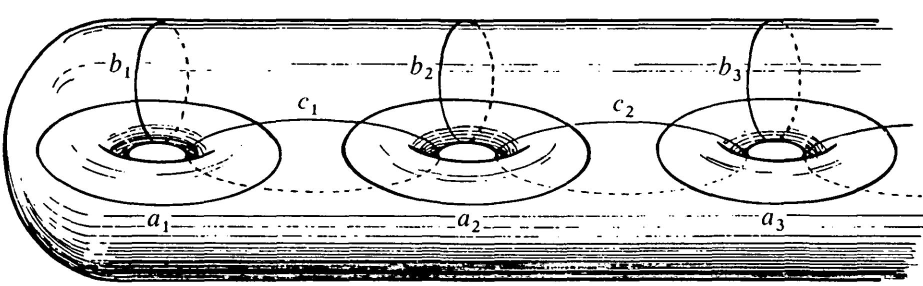


FIG. 9

Let $\theta$: $M_g \to Sp(2g, \mathbf{F}_2)$ be the epimorphism given by the action of $M_g$ on $H_1(T_g; \mathbf{F}_2)$. Recall that if $c$ is a simple closed curve on $T_g$, then $\theta$ maps (the class of) the Dehn twist about $c$ to the transvection $C$ determined by the homology class of $c$. So if the Dehn twists about a set $S$ of curves generate $M_g$, then the corresponding transvections generate $Sp(2g; \mathbf{F}_2)$. Let $S$ be the set $\{a_1, \ldots, a_g, c_1, \ldots, c_{g-1}, b_i, b_j\}$, where $g > 2$. Then $P = \{a_1, \ldots, a_g, c_1, \ldots, c_{g-1}, b_i\}$ is a basis for $H_1(T_g; \mathbf{F}_2)$. Suppose $i = 1$ and

$j = g$. Then $G(P \cup \{b_j\})$ is a line graph. Suppose $i-j$ is even. Then $Q_P(b_j) = 1$. Thus in either case $Tv(S) \neq Sp(2g; \mathbf{F}_2)$ and so the Dehn twists from $S$ do not generate $M_g$.

REMARKS. (1) In [30], examples are given of sets $S$ of closed curves on $T_g$ such that the corresponding transvections generate $Sp(2g; \mathbb{Z})$ but the Dehn twists from the curves in $S$ do not generate $M_g$. The method involves a new invariant $\eta$ which has values in $\mathbb{Z}_{12}$ and which generalizes the winding number with respect to a vector field (see also [31]).

(2) In [35] the minimal set of twist generators for $M_g$ given in [9] is used to give a finite presentation for $M_g$.

## 12. *Symmetric groups as maximal subgroups of orthogonal and symplectic groups*

The previous methods give a strategy for finding faithful representations of symmetric groups by finding a spanning set $S$ in a known symplectic space $V$ such that $S$ is a line graph. Then $Tv(S)$ is a symmetric group and the inclusion $Tv(S) \subset Sp_0(V)$ gives the representation. In some cases one can prove that $Tv(S)$ is contained in an orthogonal group, and that the inclusion is a maximal subgroup.

We illustrate these ideas by showing how to recover embedding results of Dye [7] and refer the reader to the first paragraph of his Introduction for a discussion of the relation of his embeddings to results of Dickson [28].

As explained in §8, there are two non-equivalent quadratic forms associated to a regular symplectic form on a vector space over $\mathbf{F}_2$ of dimension $n$. We denote the corresponding orthogonal groups by $O^1(n)$, $O^0(n)$ according as the Arf invariant of the quadratic form is 1 or 0 respectively.

We now use our methods to prove three standard isomorphisms.

PROPOSITION 12.1. *There are isomorphisms*
(i) $S_6 \cong Sp(4; \mathbf{F}_2)$,
(ii) $S_5 \cong O^1(4)$,
(iii) $S_8 \cong O^0(6)$.

*Proof.* Let $L$ be the line graph $L_4$ and let $V = \langle L_4 \rangle$. Then $V$ is regular and $Sp(V) = Sp(4; \mathbf{F}_2)$.

Let $x = e_2 + e_4$, and let $L' = L \cup \{x\}$. By Corollary 7.6, $Tv(L') \cong S_6$. Let $\alpha \in Sp(V)$. The non-zero elements of $V$ have one or two components with respect to $L$ and so are equivalent, under the action of $Tv(L)$, to $e_1$ or $x$. It follows from Proposition 7.5 (as in Corollary 3.3) that $\alpha \in Tv(L)$. This proves (i).

For (ii), we note that $Tv(L) \cong S_5$, and that the elements of $Tv(L)$ preserve the quadratic form $Q_L$ which by §8 has Arf invariant 1. Let $\alpha \in Sp(V)$ preserve $Q_L$. Then $\alpha e_i$ is connected for $i = 1, \ldots, 4$. Hence $\alpha \in Tv(L)$, by Corollary 3.3. This proves (ii).

For (iii), let $V = \langle L_6 \rangle$, $x = e_2 + e_4 + e_6$, $L' = L_6 \cup \{x\}$. Then $Tv(L') \cong S_8$. Since $Q_L(x) = 1$, it follows that $X$ belongs to $O^0(6)$, the orthogonal group of $Q_L$. Hence $Tv(L') \subset O^0(6)$. Let $\alpha \in O^0(6)$. Then for each vertex $e_i$, $\alpha e_i$ has 1 or 3 components with respect to $L$. Proposition 7.5 now implies that $\alpha \in Tv(L')$. This proves (iii).

THEOREM 12.2 [7]. *Let $m > 3$. There is an embedding of $S_{2m+2}$ as a subgroup of $Sp(2m; \mathbf{F}_2)$, an embedding which is maximal if $m$ is even.*

*Proof.* Let $V$ be the symplectic space $\langle L_{2m}\rangle$ over $\mathbf{F}_2$. Then $V$ is regular and $Sp(V) = Sp_0(V) = Sp(2m;\mathbf{F}_2)$.

Let $x_{2r} = e_2+e_4+\dots+e_{2r}$, and let $L' = L_{2m}\cup\{x_{2m}\}$. By Corollary 7.6 (with $n = 2m+1$), $Tv(L')\cong S_{2m+2}$. This gives our embedding.

Let $H$ be a subgroup of $Sp(V)$ properly containing $Tv(L')$. Let $\alpha\in H\setminus Tv(L')$. By Proposition 7.5 (cf. also Corollary 3.3) there is a vertex $a$ of $L'$ such that $\alpha a$ has $r$ components with $1<r<m$.

Suppose $r$ is odd. By Theorem 7.1, there is $\beta\in Tv(L_{2m})$ such that $y = \beta\alpha a$ is given by

$$y = e_{2s}+e_{2(s+1)}+\dots+e_{2m},\quad \text{where } s = m-r+1.$$

Let $S = L'\cup\{y\}$, $P = L'\setminus\{e_{2m}\}$. Then $S$ is a tree of orthogonal type, $P$ is a basis of $V$, and $x_{2m} = e_2+e_4+\dots+e_{2(s-1)}+y$, so that

$$Q_P(x_{2m}) = s \mod 2.$$

Suppose now that $m$ is even. Then $s$ also is even. So Theorem 11.1 gives us that $Tv(S) = Sp(V)$, whence $H = Sp(V)$.

Suppose we can find $a$ as above but only with $r$ even. Choose $\beta'\in Tv(L_{2m})$ such that

$$\beta'\alpha a = e_2+e_4+\dots+e_{2r} = x_{2r}.$$

Then $z = X_{2r}X_{2m}(e_1) = e_1+e_{2(r+1)}+\dots+e_{2m}$ has an odd number (namely $1+m-r$) of components, and so we are back to the first case.

For our next application, we let $M_n$ denote the graph $L_n\cup\{g\}$, where $g$ is adjacent only to $e_5$. We will use the obvious relations $L_n\subset M_n\subset M_{n+1}$. Note that if $n\geqslant 7$, then $M_n$ is of orthogonal type. Also, it is easily checked that $V = \langle M_n\rangle$ is regular if and only if $n$ is odd, and then the Arf invariant of the quadratic form $Q$ determined by $M_n$ is computed in Proposition 8.9.

THEOREM 12.3 [7]. *Let $m>3$. There is an embedding of $S_{2m+1}$ as a subgroup of an orthogonal group $O^\varepsilon(2m)$, an embedding which is maximal if $m$ is even. Further $\varepsilon = 1$ if $m\equiv 2, 3 \bmod 4$ and $\varepsilon = 0$ if $m\equiv 0, 1 \bmod 4$.*

*Proof.* Let $V = \langle M\rangle$ where $M = M_{2m-1}$.

Since $m>3$, $Tv(M)$ is the orthogonal group of the quadratic form $Q_M$ and $Tv(M)$ is an $O^\varepsilon(2m)$.

Let $x = e_2+e_4+g$. Then $Q_M(x) = 1$ and so $X\in Tv(M)$, by Theorem 10.1. However, $L = L_{2m-1}\cup\{x\}$ is a line graph and a basis for $V$. Hence $Tv(L)\cong S_{2m+1}$. This gives our embedding.

Let $H$ be a subgroup of $Tv(M)$ properly containing $Tv(L)$, and let $\alpha\in H\setminus Tv(L)$. By Corollary 3.3, there is a vertex $a$ of $L$ such that $\alpha a$ is not connected with respect to $L$. By Theorem 7.1, there is a $\beta\in Tv(L)$ such that $y = \beta\alpha a$ satisfies

$$y = x+e_2+e_4+\dots+e_{2r},\quad \text{where } r\geqslant 1.$$

Since $\beta, \alpha\in Tv(M)$, we have $Q_M(y) = 1$ and so

$$1 = Q_M(y) = 1+r.$$

Hence $r$ is even. Assume now that $m$ is even. Then $2r\neq 2m-2$, and so $2r<2m-2$. Hence the graph $P = L_{2m-1}\cup\{y\}$ (which is a basis for $V$) is orthogonal. But

$Q_M(y) = 1$. It follows easily that $Q_P = Q_M$ and hence $H = Tv(M)$. This proves maximality.

The computation of $\varepsilon$ follows from Proposition 8.9.

THEOREM 12.4 [7]. *Let $m > 1$. There is an embedding of $S_{4m+4}$ as a maximal subgroup of an orthogonal group $O^{\varepsilon}(4m+2)$. Further, $\varepsilon = 1$ or $0$ according as $m$ is even or odd.*

*Proof.* Let $V = \langle N \rangle$ where $N = M_{4m+1}$. Then $N$ is orthogonal and $Tv(N)$ is the orthogonal group of the quadratic form $Q_N$; hence $Tv(N)$ is an $O^{\varepsilon}(4m+2)$.

Let $x = e_2+e_4+g$, $y = e_6+e_8+e_{12}+\ldots+e_{4m}+g$. Then $Q_N(x) = Q_N(y) = 1$ and so $X, Y \in Tv(N)$. Let $L = L_{4m-1} \cup \{x\}$, $L' = L \cup \{y\}$. Then $L, L'$ are line graphs and $L$ is a basis for $V$. By Corollary 7.6, $Tv(L') \cong S_{4m+4}$. This gives our embedding.

Let $H$ be a subgraph of $Tv(N)$ properly containing $Tv(L')$, and let $\alpha \in H \setminus Tv(L')$. By Proposition 7.5, there is a vertex $a$ of $L'$ such that $\alpha a$ has $r$ components with respect to $L$, where $1 < r < 2m+1$. By Theorem 7.1, there is a $\beta \in Tv(L)$ such that $u = \beta\alpha a$ satisfies

$$u = x+e_2+\ldots+e_{2(r-1)}.$$

But $N' = \{e_1, e_2, \ldots, e_{4m+1}, u\}$ is orthogonal, since $r < 2m+1$. Also $Q_N(u) = 1$, since $\beta, \alpha \in Tv(N)$, $a \in L'$, and $Q_N(x) = Q_N(y) = 1$. Hence $Tv(N') = Tv(N)$, and so $H = Tv(N)$. This proves maximality.

The computation of $\varepsilon$ follows from Proposition 8.9.

## *Appendix*

Since these papers were submitted, we have been able to consider the paper [13] by Janssen. He considers symplectic forms on spaces over $\mathbb{Z}$ or $\mathbf{F}_2$, and his principal results are over $\mathbf{F}_2$. The notion of 'equivalence' of bases used in [13] is the same as our $t$-equivalence. The graphs $G(P)$, $x\,|_P$ are used in [13] with the notations $gr(P)$, $gr(P, x)$ respectively. The overall method of [13] is to replace a connected $P$ by an equivalent $P'$ which has a point adjacent to all other points of $P'$; this is almost the opposite of our method, which is to replace a connected $P$ by a tree. We have also found it convenient to follow the definition of $Q_P$ given in [13], and to deduce the computation of $Q_P$ as an Euler characteristic rather than define $Q_P$ in the latter way.

There seems to be some overlap of our results and those of [13], but the overall aims are not exactly the same. A fully detailed account of [13] is given in [34], which in Theorem 4.8 generalizes our Corollary 10.3 to the non-regular case.

## *References*

References [1–25] are given in the previous paper [27].

26. W. BROWDER, *Surgery on simply connected manifolds* (Springer, Berlin, 1972).
27. R. BROWN and S. P. HUMPHRIES, 'Orbits under symplectic transvections I', *Proc. London Math. Soc.* (3), 52 (1986), 517–531.
28. L. E. DICKSON, *Linear groups* (Teubner, Leipzig, 1901).
29. J. DIEUDONNÉ, *La géometrie des groupes classiques*, 3rd edn, Ergebnisse der Math. u.i. Grundz. 5 (Springer, Berlin, 1971).
30. S. P. HUMPHRIES, 'Dehn twists not generating the mapping class group', Pure Mathematics preprint 83.8, University College of North Wales, 1983.
31. S. P. HUMPHRIES, 'A generalisation of winding number functions on surfaces', Pure Mathematics preprint 83.11, University College of North Wales, 1983.

32. S. P. HUMPHRIES, 'Graphs and Nielsen transformations of symmetric, orthogonal and symplectic groups', *Quart. J. Math. Oxford* (2), 36 (1985), 297–313.
33. S. P. HUMPHRIES, 'Generation of special linear groups by transvections', *J. Algebra*, to appear.
34. W. A. M. JANSSEN, 'Skew-symmetric vanishing lattices', Doctoral thesis, Nijmegen, 1985.
35. B. WAJNRYB, 'A simple presentation for the mapping class group of an orientable surface', *Israel J. Math.*, 45 (1983), 157–174.

*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.*