Correction of a theorem on the symmetric group generated by transvections

Hau-wen Huang

Abstract

Let $V$ denote a vector space over two-element field $\mathbb{F}_2$ with finite positive dimension and endowed with a symplectic form $B$. Let $\text{SL}(V)$ denote the special linear group of $V$. Let $S$ denote a subset of $V$. Define $Tv(S)$ as the subgroup of $\text{SL}(V)$ generated by the transvections with direction $\alpha$ for all $\alpha \in S$. Define $G(S)$ as the graph whose vertex set is $S$ and where $\alpha, \beta \in S$ are connected whenever $B(\alpha, \beta) = 1$. A well-known theorem states that under the assumption that $S$ spans $V$, the following (i), (ii) are equivalent:

(i) $Tv(S)$ is isomorphic to a symmetric group.
(ii) $G(S)$ is a claw-free block graph.

We give an example which shows that this theorem is not true. We give a modification of this theorem as follows. Assume that $S$ is a linearly independent set of $V$ and no element of $S$ is in the radical of $V$. Then the above (i), (ii) are equivalent.

1 A theorem on the symmetric group generated by transvections

Throughout this note let $V$ denote a vector space over two-element field $\mathbb{F}_2$ with finite positive dimension and endowed with a symplectic form $B$. Let $\text{rad}V$ denote the radical of $V$ with respect to $B$. Let $\text{SL}(V)$ denote the special linear group of $V$. For $\alpha \in V$ define a linear transformation $\tau_\alpha : V \rightarrow V$ by

$$\tau_\alpha \beta = \beta + B(\beta, \alpha)\alpha$$

for all $\beta \in V$.

We call $\tau_\alpha$ the transvection on $V$ with direction $\alpha$. Observe that $\tau_\alpha^2 = 1$ and so $\tau_\alpha \in \text{SL}(V)$. For a subset $S$ of $V$ define $Tv(S)$ to be the subgroup of $\text{SL}(V)$ generated by the transvections $\tau_\alpha$ for all $\alpha \in S$, and define $G(S)$ to be the simple graph which has vertex set $S$ and an edge between vertices $\alpha$ and $\beta$ if and only if $B(\alpha, \beta) = 1$.

Let $G$ denote a simple graph. A cut-vertex of $G$ is a vertex whose deletion increases the number of components. A block of $G$ is a maximal connected subgraph of $G$ that has no cut-vertex. A block graph is a simple connected graph in which every block is a complete graph. A claw is a tree with one internal vertex and three leaves. A simple graph is said to be claw-free if it does not contain a claw as an induced subgraph.
Let $S$ denote a subset of $V$. Let $C$ denote the set consisting of all cut-vertices of $G(S)$. We now view $G(S)$ as a 1-dimensional complex. Let $G_1, G_2, \ldots, G_k$ denote the components of $G(S) \setminus C$. For each $1 \leq i \leq k$ define $G_i^*$ to be the closure of $G_i$ in $G(S)$. Let $H$ denote the graph with $G_1^*, G_2^*, \ldots, G_k^*$ as vertices and an edge between $G_i^*$ and $G_j^*$ if $G_i^* \cap G_j^*$ is nonempty. [3, Theorem 3.1] states that under the assumption that $S$ spans $V$, the group $Tv(S)$ is isomorphic to a symmetric group if and only if the following (i)–(iv) hold:

(i) $G(S)$ is connected;

(ii) for each $\alpha \in S$ the graph $G(S \setminus \{\alpha\})$ contains at most two components;

(iii) for each $1 \leq i \leq k$ the graph $G_i^*$ is a complete graph;

(iv) $H$ is a tree.

We remark that $G_1^*, G_2^*, \ldots, G_k^*$ are the blocks of $G(S)$. Therefore $G(S)$ is a claw-free block graph if and only if (i)–(iii) hold. Condition (ii) implies that $H$ is acyclic and therefore (i), (ii) imply (iv). We can state [3, Theorem 3.1] as follows.

**Theorem 1.1.** [3, Theorem 3.1]. Assume that $S$ spans $V$. Then $Tv(S)$ is isomorphic to a symmetric group if and only if $G(S)$ is a claw-free block graph.

## 2 A counterexample to the necessity of Theorem 1.1

In this section we show a counterexample to the necessity of Theorem 1.1. We begin by recalling some background material from [1, 2].

**Definition 2.1.** [1, Section 3]. Define a binary relation $\mathcal{T}_0$ on the power set of $V$ as follows. For any two $S, S' \subseteq V$ we say that $S$ is $\mathcal{T}_0$-related to $S'$ whenever there exist $\alpha, \beta \in S$ such that $S'$ is obtained from $S$ by changing $\beta$ to $\tau_\alpha \beta$.

**Definition 2.2.** [1, Section 3]. Define $\mathcal{T}$ to be the equivalence relation on the power set of $V$ generated by $\mathcal{T}_0$.

**Lemma 2.3.** [2, Corollary 11.2]. Assume that $S$ is a subset of $V$ and no element of $S$ is in $\text{rad} V$. Let the equivalence relation $\mathcal{T}$ be as in Definition 2.2. Then $Tv(S)$ is isomorphic to a symmetric group if and only if there exists $S'$ in the $\mathcal{T}$-equivalence class of $S$ for which $G(S')$ is a path.

**Example 2.4.** Let $V$ denote a vector space over $\mathbb{F}_2$ with dimension $n \geq 3$. Let $I = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ denote a basis of $V$. Define a symplectic form $B : V \times V \to \mathbb{F}_2$ by

$$B(\alpha_i, \alpha_j) = \begin{cases} 1 & \text{if } |i - j| = 1, \\ 0 & \text{if } |i - j| \neq 1 \end{cases} \quad (1 \leq i, j \leq n).$$

Let $S = I \cup \{\alpha_1 + \alpha_2\}$, which spans $V$. The set $I$ can be obtained from $S$ by changing $\alpha_1 + \alpha_2$ to $\tau_{\alpha_1}(\alpha_1 + \alpha_2) = \alpha_2$. Therefore $S$ is $\mathcal{T}_0$-related to $I$. The graph $G(I)$ is a path. By Lemma 2.3 the group $Tv(S)$ is isomorphic to a symmetric group. We draw $G(S)$ as follows.
The block of $G(S)$ with vertex set $\{\alpha_1 + \alpha_2, \alpha_1, \alpha_2, \alpha_3\}$ is not complete. Therefore $G(S)$ is not a block graph. We get a contradiction to the necessity of Theorem 1.1.

3 A modification of Theorem 1.1

In Section 2 we showed Theorem 1.1 to be incorrect by example. In this section we give a replacement theorem as follows.

**Theorem 3.1.** Assume that $S$ is a linearly independent set of $V$ and no element of $S$ is in rad$V$. Then $Tv(S)$ is isomorphic to a symmetric group if and only if $G(S)$ is a claw-free block graph.

The original proof of the sufficiency of Theorem 1.1 does not use the assumption that $S$ spans $V$. We actually get the following result.

**Lemma 3.2.** Let $S$ denote a subset of $V$. If $G(S)$ is a claw-free block graph of order $n$ then $Tv(S)$ is isomorphic to the symmetric group on $n + 1$ letters.

We will not prove the necessity of Theorem 3.1 by revising the proof of the necessity of Theorem 1.1. Instead we will provide a short proof. To do this we define two binary relations on the set of all linearly independent sets of $V$ and need three lemmas.

**Definition 3.3.** Define $I_0$ to be the restriction of $T_0$ to the set of all linearly independent sets of $V$.

Observe that the binary relation $I_0$ from Definition 3.3 is symmetric.

**Definition 3.4.** Define $I$ to be the equivalence relation on the set of all linearly independent sets of $V$ generated by $I_0$.

The original proof of Lemma 2.3 works for the following lemma.

**Lemma 3.5.** Assume that $S$ is a linearly independent set of $V$ and no element of $S$ is in rad$V$. Let the equivalence relation $I$ be as in Definition 3.4. Then $Tv(S)$ is isomorphic to a symmetric group if and only if there exists $S'$ in the $I$-equivalence class of $S$ for which $G(S')$ is a path.

To state the second lemma we recall the notion of the line graph of a simple graph. Let $G$ denote a simple graph. The **line graph** of $G$ is a simple graph that has a vertex for each edge of $G$, and two of these vertices are adjacent whenever the corresponding edges in $G$ have a common vertex.

**Lemma 3.6.** [4, Theorem 8.5]. Let $G$ denote a simple graph. Then $G$ is a claw-free block graph if and only if $G$ is the line graph of a tree.
Lemma 3.7. Let $S$ denote a linearly independent set of $V$ for which $G(S)$ is a claw-free block graph. Then for each $S'$ in the $I$-equivalence class of $S$ the graph $G(S')$ is a claw-free block graph.

Proof. Let $S'$ denote a subset of $V$ which $S$ is $I_0$-related to. Let $\alpha, \beta \in S$ such that $S'$ is obtained from $S$ by changing $\beta$ to $\tau_{\alpha}\beta$. If $B(\alpha, \beta) = 0$ there is nothing to prove. Thus we assume $B(\alpha, \beta) = 1$. By Lemma 3.6 there exists a tree $T$ whose line graph is $G(S)$. Let $u$ denote the common vertex of the edges $\alpha$ and $\beta$ in $T$. Let $v$ and $w$ denote the other vertices incident to $\alpha$ and $\beta$ in $T$, respectively. Let $T'$ denote the tree obtained from $T$ by removing the edge $\beta$ and adding a new edge between $v$ and $w$. We call the new edge $\tau_{\alpha}\beta$. For each $\gamma \in S'$, $\gamma$ is adjacent to $\tau_{\alpha}\beta$ in $G(S')$ if and only if $\gamma$ is adjacent to exactly one of $\alpha$ and $\beta$ in $G(S)$. Therefore $G(S')$ is the line graph of $T'$ so $G(S')$ is a claw-free block graph by Lemma 3.6. The result follows since $I_0$ is symmetric and generates $I$.

Proof of Theorem 3.1. (sufficiency): Immediate from Lemma 3.2. (necessity): By Lemma 3.5 there exists $S'$ in the $I$-equivalence class of $S$ for which $G(S')$ is a path. Since a path is a claw-free block graph and by Lemma 3.7 the graph $G(S)$ is a claw-free block graph.

Corollary 3.8. Assume that $S$ is a linearly independent set of $V$ and no element of $S$ is in $\text{rad} V$. Let the equivalence relation $I$ be as in Definition 3.4. Then the following (i)–(iv) are equivalent:

(i) $T v(S)$ is isomorphic to a symmetric group.
(ii) $G(S)$ is a claw-free block graph.
(iii) $G(S)$ is the line graph of a tree.
(iv) There exists $S'$ in the $I$-equivalence class of $S$ for which $G(S')$ is a path.

Suppose (i)–(iv) hold. Let $n$ denote the cardinality of $S$. Then $T v(S)$ is isomorphic to the symmetric group on $n + 1$ letters.

Proof. (i) $\iff$ (ii): Immediate from Theorem 3.1.
(i) $\iff$ (iv): Immediate from Lemma 3.5.
(ii) $\iff$ (iii): Immediate from Lemma 3.6.

The last assertion is immediate from Lemma 3.2.

4 Comments

Given Theorem 3.1 it is natural to further study the linearly dependent sets $S$ of $V$ for which the equivalence holds. This section is devoted to a description of these linearly dependent sets.

In view of Lemma 3.2 it is enough to study the linearly dependent set $S$ of $V$ for which $G(S)$ is a claw-free block graph (equivalently, the line graph of a tree). Moreover, replacing $V$ by the subspace of $V$ spanned by $S$ if necessary, we may assume without loss of generality that $S$ spans $V$. 

4
We now describe how to obtain such a set \( S \). For convenience an edge of a tree incident to a leaf will be said to be a *pendant edge*. Assume that \( V \) has zero radical. Let \( I \) denote a basis of \( V \) for which \( G(I) \) is the line graph of a tree \( T \). Pick a vertex \( u \) of \( T \). Since the radical of \( V \) is zero there exists a unique \( \beta \in V \) such that for each \( \alpha \in I \),

\[
B(\alpha, \beta) = \begin{cases} 
1 & \text{if } u \text{ is incident to } \alpha \text{ in } T, \\
0 & \text{if } u \text{ is not incident to } \alpha \text{ in } T. 
\end{cases}
\]

Let \( S = I \cup \{ \beta \} \), which is linearly dependent unless the dimension of \( V \) is two and \( u \) is a leaf of \( T \). Suppose that \( S \) is linearly dependent. Let \( \mathcal{T} \) denote the tree obtained from \( T \) by adding a pendant edge incident to \( u \). We call the new edge \( \beta \). Then \( G(S) \) is the line graph of \( \mathcal{T} \).

At the end of this section we will see that any linearly dependent spanning set \( S \) of \( V \) for which \( G(S) \) is the line graph of a tree can be obtained in the above way. To this end we establish two lemmas.

**Lemma 4.1.** Assume that \( V \) has zero radical. Let \( I \) denote a basis of \( V \) for which \( G(I) \) is connected. Then for any \( k \geq 2 \) mutually distinct vectors \( \beta_1, \ldots, \beta_k \in V \setminus I \), the graph \( G(I \cup \{ \beta_1, \ldots, \beta_k \}) \) is not the line graph of a tree.

*Proof.* Proceed by contradiction. Suppose there exist distinct \( \beta, \gamma \in V \setminus I \) such that \( G(I \cup \{ \beta, \gamma \}) \) is the line graph of a tree \( \mathcal{T} \). Let \( T \) denote the subgraph of \( \mathcal{T} \) induced by all \( \alpha \in I \). Since \( I \) spans \( V \) each of \( \beta \) and \( \gamma \) is a pendant edge of \( \mathcal{T} \). Let \( u \) and \( v \) denote the two vertices of \( T \) incident to \( \beta \) and \( \gamma \), respectively. Since the radical of \( V \) is zero \( u \) and \( v \) are distinct. Let \( \alpha_1, \ldots, \alpha_k \) denote the edges in the path joining \( u \) and \( v \). The incidence relation on \( \mathcal{T} \) implies that \( B(\alpha, \beta + \gamma) = B(\alpha, \alpha_1 + \cdots + \alpha_k) \) for each \( \alpha \in I \). Therefore \( \beta + \gamma = \alpha_1 + \cdots + \alpha_k \). Using this we deduce \( B(\beta, \gamma) = 1 \), a contradiction. \( \square \)

**Lemma 4.2.** Assume that \( I \) is a basis of \( V \) for which \( G(I) \) is the line graph of a tree \( T \). Then the following (i)–(iv) are equivalent:

(i) The radical of \( V \) is zero.

(ii) The dimension of \( V \) is even.

(iii) For some vertex \( u \) in \( T \) there exists \( \beta \in V \) such that (\dag) holds for each \( \alpha \in I \).

(iv) For each vertex \( u \) in \( T \) there exists a unique \( \beta \in V \) such that (\dag) holds for each \( \alpha \in I \).

*Proof.* Let \( V^* \) denote the dual space of \( V \). Define a linear map \( \theta : V \to V^* \) by

\[
\theta(\alpha)\beta = B(\alpha, \beta) \quad \text{for all } \alpha, \beta \in V.
\]

The kernel of \( \theta \) is \( \text{rad}V \). Therefore (i) if and only if (i') the map \( \theta \) is a bijection. We show that (i') and (ii)–(iv) are equivalent. Condition (i') immediately implies (iv). To see that (iv) implies (i') we let \( U \) denote the vertex space of \( T \) over \( \mathbb{F}_2 \) and define a linear map \( \lambda : U \to V^* \) by for all vertices \( u \) of \( T \) and for all \( \alpha \in I \),

\[
\lambda(u)\alpha = \begin{cases} 
1 & \text{if } u \text{ is incident to } \alpha \text{ in } T, \\
0 & \text{if } u \text{ is not incident to } \alpha \text{ in } T. 
\end{cases}
\]
The kernel of $\lambda$ is $\{0, w\}$, where $w$ is the sum of all vertices of $T$. By dimension theorem $\lambda$ is surjective. Therefore (iv) implies that $\theta$ is surjective and so is bijective.

To see the equivalence of (ii)–(iv) we define a linear map $\mu : V \to U$ by for all $\alpha \in I$,

$$\mu(\alpha) = u + v,$$

where $u$ and $v$ are the two distinct vertices incident to $\alpha$ in $T$. Observe that $\theta = \lambda \circ \mu$ and that the image of $\mu$, denoted by $\text{Im} \mu$, consists of all $v \in U$ each of which is equal to the sum of an even number of vertices in $T$. Therefore (ii) if and only if $w + u \in \text{Im} \mu$ for some (resp. each) vertex $u$ of $T$ if and only if (iii) (resp. (iv)). Here $w$ is the nonzero vector in the kernel of $\lambda$.

**Proposition 4.3.** Let $S$ denote a linearly dependent spanning set of $V$. Assume that $G(S)$ is the line graph of a tree $\Upsilon$. Then the following (i)–(iii) hold:

(i) The radical of $V$ is zero.

(ii) The dimension of $V$ is even.

(iii) For each pendant edge $\beta$ of $\Upsilon$ the set $S \setminus \{\beta\}$ is a basis of $V$.

**Proof.** Consider the set consisting of the linearly independent subsets $I$ of $S$ for which $G(I)$ is connected. From this set we choose a maximal element $J$ under inclusion. The maximality of $J$ forces that each $\alpha \in S \setminus J$ is in the subspace of $V$ spanned by $J$. Therefore $J$ is a basis of $V$. Applying Lemma 4.2 to $I = J$, (i) and (ii) follow. To prove (iii) we fix a pendant edge $\beta$ of $\Upsilon$ and show that $S \setminus \{\beta\}$ is linearly independent. Applying Lemma 4.1 to $I = J$ it follows that $S \setminus J$ contains exactly one element, denoted by $\alpha$. If $\alpha = \beta$ there is nothing to prove. Thus we assume $\alpha \neq \beta$. Let $W$ denote the subspace of $V$ spanned by $J \setminus \{\beta\}$, which has odd dimension. Applying Lemma 4.2 to $I' = J \setminus \{\beta\}$ and $V' = W$ we find that $\alpha \notin W$. Therefore $S \setminus \{\beta\}$ is linearly independent.

5 Acknowledgements

The author would like to thank the anonymous referee for valuable suggestions.

References

[1] R. Brown, S. P. Humphries. Orbits under symplectic transvections I. *Proceedings of the London Mathematical Society* 52 (1986) 517–531.

[2] R. Brown, S. P. Humphries. Orbits under symplectic transvections II: the case $K = \mathbb{F}_2$. *Proceedings of the London Mathematical Society* 52 (1986) 532–556.

[3] S. P. Humphries. Graphs and Nielsen transformations of symmetric, orthogonal and symplectic groups. *Quarterly Journal of Mathematics, Oxford* 36 (1985) 297–313.

[4] F. Harary. *Graph Theory*. Addison-Wesley, Massachusetts, 1969.
Hau-wen Huang
Department of Applied Mathematics
National Chiao Tung University
1001 Ta Hsueh Road
Hsinchu, Taiwan, 30050.
Email: poker80.am94g@nctu.edu.tw