ORTHOMORPHISMS OF $Z_p$

Anthony B. EVANS

Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, U.S.A.

Received 25 March 1985
Revised 30 April 1986

Introduction

An orthomorphism of an abelian group $G$ is a bijection $\theta : G \rightarrow G$ for which the mapping $\eta : G \rightarrow G$ defined by $x\eta = x(x\theta)^{-1}$ is also a bijection. We make the additional assumption that, if $1$ is the identity of $G$, $1\theta = 1$, as $\theta$ is an orthomorphism of $G$ if and only if the mapping $x \rightarrow x\theta(1\theta)^{-1}$ is an orthomorphism of $G$. Several authors call the mapping $\phi : x \rightarrow (x\theta)^{-1}$ a complete mapping (see, for example, Hall and Paige [5] and Paige [11]).

Orthomorphisms or complete mappings have been used to construct mutually orthogonal sets of latin squares (see Johnson, Dulmage and Mendelsohn [6] and Mann [7 and 8]), and hence orthomorphisms can be used in the construction of nets (see Bruck [1]). They have also been used in the construction of neofields (see Paige [9]). Under the name of 1-permutations, orthomorphisms of cyclic groups of order eleven or less were studied by Singer [12].

We call two orthomorphisms, $\theta$ and $\phi$ of a group $G$, orthogonal if the mapping $x \rightarrow x\theta(x\phi)^{-1}$ is a bijection. The orthomorphism graph of a group $G$ has, as its vertex set, the orthomorphisms of $G$ and the identity mapping of $G$. Two orthomorphisms of $G$ are adjacent in this graph if and only if they are orthogonal. Also every orthomorphism is adjacent to the identity mapping.

Orthomorphism graphs of groups of small order have been studied by Johnson, Dulmage and Mendelsohn [6], Zhang Li-Quian and Dai Shu-Sen [14], and Zhang Li-Quian, Xiang Ke-Feng and Dai Shu-Sen [15], and the orthomorphism graph of $Z_{11}$ was studied by Evans and McFarland [4].

The authors of the above papers have used either computers or lengthy hand computations to generate portions of the orthomorphism graph.

In the present paper, however, we introduce a theoretical framework by using quadratic residues to generate and study a portion of the orthomorphism graph of $Z_p$. In a subsequent paper (see Evans [3]) we generalize the methods of this paper using the theory of cyclotomy in GF(q). We expect the methods of these two papers to be generalizable to other groups.

Mann [7] used the "automorphism method" to generate cliques of the
orthomorphism graph of a group $G$, using orthomorphisms that are also automorphisms of $G$.

Evans and Mcfarland [4] showed that, if the orthomorphism graph of $\mathbb{Z}_p$ contains a $(p-1)$-clique, other than the $(p-1)$-clique generated by Mann’s “automorphism method”, then there must exist a non-Desarguesian affine plane of order $p$ which admits translations. Mendelsohn and Wolk [9] used orthomorphisms in searching for a non-Desarguesian plane of prime order. It is hoped that further study of the orthomorphism graph of $\mathbb{Z}_p$ will settle the question of the existence or non-existence of non-Desarguesian affine planes of prime order which admit translations. It has long been conjectured that no such planes exist.

1. The orthomorphism graph

Throughout this paper we denote the orthomorphism graph of $\mathbb{Z}_p$ by $G_p$, and we assume $\mathbb{Z}_p$ to be the additive group of the field $GF(p)$, addition and multiplication being modulo $p$.

Note that $I_a : i \to ia \pmod{p}$ is a vertex of $G_p$ for $a = 1, \ldots, p - 1$ and that the set $\{I_a : a = 1, \ldots, p - 1\}$ is a $(p-1)$-clique of $G_p$. Given any $r$-clique $\{I = \theta_1, \ldots, \theta_r\}$ of $G_p$ we can form a mutually orthogonal set of latin squares $\{L_1, \ldots, L_r\}$ by setting the $ij$th entry of $L_k$ equal to $i+j\theta_k$ (see Johnson, Dulmage and Mendelsohn [6]). It was shown in Evans and Mcfarland [4] that there exists a non-desarguesian plane of order $p$, which admits translations, if and only if $G_p$ contains more than one $(p-1)$-clique. It is known that $G_p$ contains only one $(p-1)$-clique if $p \leq 11$ (see Evans and Mcfarland [4] or Johnson, Dulmage and Mendelsohn [6]), but this is unknown for $p > 11$.

Note that if $\theta$ is an orthomorphism so are $\theta^{-1}$ and $I - \theta$. The following are automorphisms of $G_p$.

(i) $\alpha : \theta \mapsto \begin{cases} I - \theta & \text{if } \theta \neq I; \\ I & \text{if } \theta = I; \end{cases}$

(ii) $\beta : \theta \mapsto \phi$, where $i\phi = (i + 1)\theta - 1\theta$;

(iii) $\gamma_a : \theta \mapsto I_a^{-1}\theta I_a$, $a \neq 0$.

It is easy to verify the following relations between $\alpha$, $\beta$ and $\gamma_a$.

(a) $\alpha^2 = \beta^p = \text{identity}$;

(b) $\alpha \beta = \beta \alpha$ and $\alpha \gamma_a = \gamma_a \alpha$;

(c) $\gamma_a \gamma_b = \gamma_{ab}$, where the subscripts are multiplied modulo $p$;

(d) $\beta \gamma_a = \gamma_a \beta^a$, where $\beta^a, a \in \mathbb{Z}_p$ is defined in the natural way.

The following theorem gives information on the fixed points of these automorphisms. The proof is left to the reader.

**Theorem 1.1.** (i) If $\theta \alpha = \theta$, then $\theta = I$ or $I_{3(p+1)}$;

(ii) If $\theta \beta^m = \theta (m \neq 0 \pmod{p})$, then $\theta = I_a$ for some $a$;
(iii) \( I_a \gamma_b = I_a \) for all \( a \);  
(iv) If \( \langle a \rangle = \text{GF}(p)^* \), then \( \theta \gamma_a \beta^m = \theta \) implies that \( \theta = I_b \) for some \( b \).

Data for \( p = 11 \) suggest that, if \( \theta \in G_p \) has degree 2 or greater, then \( \theta \gamma_a \beta^m = \theta \) for some \( a, m \) \((a \neq 1)\). In the next section we deal with the fixed points of \( \gamma^2 \) where \( \langle g \rangle = \text{GF}(p)^* \). The general case is considered in Evans [3].

We finish this section with two results concerning adjacencies in \( G_p \).

**Theorem 1.2.** \( \theta \in G_p \) cannot be adjacent to \( \theta \beta^m \).

**Proof.** Suppose \( m = 1 \). Then \( i(\theta \beta - \theta) = (i + 1)\theta - 1\theta - i\theta \). Hence, if \( \theta \) is adjacent to \( \theta \beta \), we must have \((i + 1)\theta - i\theta, i = 0, \ldots, p - 1\), all distinct. But then, for some \( i \), we must have \((i + 1)\theta - i\theta = 0\). But then \( \theta \notin G_p \). Hence \( \theta \) cannot be adjacent to \( \theta \beta \).

If \( m \neq 1 \) and \( \theta \) is adjacent to \( \theta \beta^m \) then \( \theta \gamma_{m-1} \) is adjacent to \( \theta \beta^m \gamma_{m-1} = \theta \gamma_{m-1} \beta \). But then \( \theta \gamma_{m-1} \notin G_p \). Hence the result. \[ \]

**Theorem 1.3.** Let \( \theta \in G_p - \{I_a : a = 1, \ldots, p - 1\} \). Then \( \theta \) is adjacent to \( \theta \alpha \) if and only if \( \theta \) is adjacent to \( I_{\frac{1}{2}(p+1)} \).

**Proof.** \( \theta \) is adjacent to \( \theta \alpha \) if and only if \( \theta - \theta \alpha = \theta + \theta - I \) is a bijection, if and only if \( \theta - I_{\frac{1}{2}(p+1)} \) is a bijection, if and only if \( \theta \) is adjacent to \( I_{\frac{1}{2}(p+1)} \). \[ \]

2. The orthomorphisms \( \theta_{A,B} \).

The mapping \( \theta_{A,B} \) is defined as follows:

\[
\theta_{A,B} : i \rightarrow \begin{cases} 
A_i & \text{if } i \text{ is square}, \\
B_i & \text{if } i \text{ is non-square}, \\
0 & \text{if } i = 0.
\end{cases}
\]

In this section we study those \( \theta_{A,B} \) that are orthomorphisms of \( Z_p \). Note that Mendelsohn and Wolk [9] use \( \{A, B\} \) to denote \( \theta_{A,B} \).

**Theorem 2.1** (i) \( \theta_{A,B} \) is an orthomorphism if and only if both \( A/B \) and \( (A - 1)/(B - 1) \) are squares;  
(ii) If \( \theta_{A,B}, \theta_{C,D} \in G_p \), then \( \theta_{A,B} \) is adjacent to \( \theta_{C,D} \) if and only if \( (A - C)/(B - D) \) is a square.

Theorem 2.1 follows directly from the definitions of orthomorphisms and orthogonality. See also Mendelsohn and Wolk [9]. The following is an immediate corollary.
Corollary 2.1. (i) \( \theta_{A,B} \in G_p \) if and only if \( \theta_{B,A} \in G_p \);
(ii) Let \( \theta_{A,B}, \theta_{C,D} \in G_p \). Then \( \theta_{A,B} \) is adjacent to \( \theta_{C,D} \) if and only if \( \theta_{B,A} \) is adjacent to \( \theta_{D,C} \);
(iii) If \( p \equiv 1 \pmod{4} \) and \( \theta_{A,B} \in G_p, A \neq B \), then \( \theta_{A,B} \) is adjacent to \( \theta_{B,A} \).

Note that \( \theta_{A,A} = I_A, A = 1, \ldots, p - 1 \).

Set \( S = \{ \theta_{A,B} : \theta_{A,B} \in G_p \} \). Theorem 2.2 discusses the actions of \( \alpha \) and \( \gamma_a \) on \( S \).

Theorem 2.2. Let \( \theta_{A,B} \in S \). Then the following hold:

(i) \( \theta_{A,B} \gamma_a = \begin{cases} \theta_{A,B} & \text{if } a \text{ is a square,} \\ \theta_{B,A} & \text{if } a \text{ is a non-square;} \end{cases} \)

(ii) If \( \theta \in G_p \) and \( \theta \gamma_a^2 = \theta \) for \( a = 1, \ldots, \frac{1}{2}(p - 1) \), then \( \theta \in S \);

(iii) \( \alpha \) and \( \gamma_a \) permute the elements of \( S \);

(iv) If \( \theta \in S - \{ I_a : a = 1, \ldots, p - 1 \} \), then \( \theta \beta \notin S \).

Proof. (i) This follows from the definitions of \( \theta_{A,B} \) and \( \gamma_a \).

(ii) \((a^{-2}i)\theta a^2 = i\theta \) for all \( i \) and all \( a \).

Hence \((a^2)\theta = 16a^2 \) and if \( \delta \) is a non-square \((a^2\delta)\theta = \delta\theta a^2 \). Hence \( \theta \in S \).

(iii) This follows as \( \alpha \) and \( \gamma_a \) commute with \( \gamma_b^2 \) for all \( b \).

(iv) \( \theta \beta \gamma_a^2 = \theta \gamma_b^2 \beta a^2 \). Thus, if \( \theta \) and \( \theta \beta \in S \), we must have \( \theta \beta = \theta \beta a^2 \) for all \( a \).

Hence \( \theta \beta^m = \theta \) for all \( m \) of the form \( a^2 - 1 \). Thus \( \theta = I_a \) for some \( a \), by Theorem 1.1(ii).

Let us consider the subgraph \( H \) of \( G_{11} \) induced by the elements of \( S - \{ I \} \). In Table 1 vertices of \( H \), of the form \( I_A \) are denoted by \( A \) and the other vertices are denoted by \( U, \ldots, Z \) and \( U^1, \ldots, Z^1 \).

The neighbourhood of \( U \), in \( H \), is depicted in Fig. 1. The neighbourhoods, in \( H \), of \( V, \ldots, Z \) and \( U^1, \ldots, Z^1 \) are isomorphic to this. It should be noted that

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Vertex</th>
<th>Neighbours</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U = \theta_{2,6} )</td>
<td>( W W^1 X X^1 V V^1 Y 7 8 )</td>
<td></td>
</tr>
<tr>
<td>( U^1 = \theta_{6,2} )</td>
<td>( W W^1 X X^1 V V^1 Y 7 8 )</td>
<td></td>
</tr>
<tr>
<td>( V = \theta_{2,10} )</td>
<td>( X X^1 Z Z^1 U V^1 3 9 )</td>
<td></td>
</tr>
<tr>
<td>( V^1 = \theta_{10,2} )</td>
<td>( X X^1 Z Z^1 U Y 3 9 )</td>
<td></td>
</tr>
<tr>
<td>( W = \theta_{3,9} )</td>
<td>( U U^1 Y Y^1 X^1 Z^1 5 7 )</td>
<td></td>
</tr>
<tr>
<td>( W^1 = \theta_{9,3} )</td>
<td>( U U^1 Y Y^1 X X 5 7 )</td>
<td></td>
</tr>
<tr>
<td>( X = \theta_{4,5} )</td>
<td>( U U^1 V V^1 W^1 Z^1 8 9 )</td>
<td></td>
</tr>
<tr>
<td>( X^1 = \theta_{5,4} )</td>
<td>( U U^1 V V^1 W Z^1 8 9 )</td>
<td></td>
</tr>
<tr>
<td>( Y = \theta_{6,10} )</td>
<td>( W W^1 Z Z^1 U V^1 4 5 )</td>
<td></td>
</tr>
<tr>
<td>( Y^1 = \theta_{10,6} )</td>
<td>( W W^1 Z Z^1 U^1 V 4 5 )</td>
<td></td>
</tr>
<tr>
<td>( Z = \theta_{7,8} )</td>
<td>( V V^1 Y Y^1 W^1 X 3 4 )</td>
<td></td>
</tr>
<tr>
<td>( Z^1 = \theta_{8,7} )</td>
<td>( V V^1 Y Y^1 W X^1 3 4 )</td>
<td></td>
</tr>
</tbody>
</table>
this contradicts data given by Zhang Li-Qian, Xiang Ke-Feng, and Dai Shu-Sen [15]. They state, without proof, that the only orthogonalities between orthomorphisms of $Z_{11}$ are between those of the form $I_a$.

Theorem 2.3 gives a method for generating the elements of $S - \{I_a: a = 1, \ldots, p-1\}$.

**Theorem 2.3.** Let $R$ and $S$ be squares, $R, S \neq 1, R \neq S$. Set $A = S(1-R)/(S-R)$, and $B = (1-R)/(S-R)$. Then $\theta_{A,B} \in S - \{I_a: a = 1, \ldots, p-1\}$. Furthermore, any element of $S - \{I_a: a = 1, \ldots, p-1\}$ is uniquely expressible in this form.

**Proof.** $A/B = S$ and $(A-1)/(B-1) = R$. Hence, by Theorem 2.1(i), $\theta_{A,B} \in S - \{I_a: a = 1, \ldots, p-1\}$.

If $\theta_{A,B} \in S - \{I_a: a = 1, \ldots, p-1\}$, then $A/B = S$ is a square and $(A-1)/(B-1) = R$ is a square and $R \neq S, R, S \neq 1$ and so we can solve for $A$ and $B$ uniquely in terms of $R$ and $S$. □

As a result, we obtain the following lower bound on the number of vertices of $G_p$.

**Corollary 2.2.** (i) $|S - \{I_a: a = 1, \ldots, p-1\}| = \frac{1}{4}(p-3)(p-5)$;

(ii) $|G_p| \geq \frac{1}{4}p(p-3)(p-5) + p - 1$.

**Proof.** (i) Count the number of ordered pairs $(R, S)$, $R, S \neq 1, R \neq S$, and $R$ and $S$ both squares. See Mendelsohn and Wolk [9] for an alternative proof of this.

(ii) It follows from Theorem 2.2(iv) that the sets $S - \{I_a: a = 1, \ldots, p-1\} = K, K\beta, \ldots, K\beta^{p-1}$ are mutually disjoint and, by (i), each set contains $\frac{1}{4}(p-3)(p-5)$ elements. □

For a given $\theta_{A,B} \in S, A \neq B$ we can generate the set $\{I_a: \theta_{A,B} \text{ adjacent to } I_a\}$ as follows.
Theorem 2.4. Let $\theta_{A,B} \in S$, $A \neq B$ and let $L$ be a square, $L \neq 1$, $A/B$. Let $C = (LB - A)/(L - 1)$. Then $I_C$ is adjacent to $\theta_{A,B}$. Furthermore, if $I_C$ is adjacent to $\theta_{A,B}$, then $I_C$ is uniquely expressible in this form.

Proof. $(A - C)/(B - C) = L$, a square. Hence, by Theorem 2.1(ii), $I_C$ is adjacent to $\theta_{A,B}$. On the other hand, if $I_C$ is adjacent to $\theta_{A,B}$, then setting $(A - C)/(B - C) = L$ and solving for $C$ leads to $C = (LB - A)/(L - 1)$. □

Corollary 2.3. If $\theta_{A,B} \in S$, $A \neq B$, then

$$|\{I_C : I_C \text{ adjacent to } \theta_{A,B}\}| = \frac{1}{2}(p - 5).$$

Proof. Count the number of squares $L$ for which $L \neq 1$, $A/B$.

It might seem that, given $\theta_{A,B} \in S$, $A \neq B$, there would be similar simple methods to generate those $\theta_{C,D} \in S$ for which $C \neq D$ and $\theta_{C,D}$ is adjacent to $\theta_{A,B}$. But, if we let $H$ be the subgraph of $G_p$ induced by the elements of $S - \{I_a : a = 1, \ldots, p - 1\}$, then, for $p = 13$, $H$ has 12 vertices of degree 9, 6 of degree 11, and 2 of degree 13. Similar results hold for larger values of $p$. □

We can however generate some of the neighbourhood of $\theta_{A,B}$ as follows.

Theorem 2.5. Let $\theta_{A,B} \in S$, $A \neq B$.

(i) If $\theta_{C,D} \in S - \{\theta_{A,B}\}$, $C \neq D$ satisfies $C/D = A/B$, then $\theta_{C,D}$ is adjacent to $\theta_{A,B}$;

(ii) If $\theta_{C,D} \in S - \{\theta_{A,B}\}$, $C \neq D$ satisfies $(C - 1)/(D - 1) = (A - 1)/(B - 1)$, then $\theta_{C,D}$ is adjacent to $\theta_{A,B}$.

Proof. (i) $(A - C)/(B - D) = (A/C - 1)/(B/D - 1)$. Hence, by Theorem 2.1(ii), $\theta_{C,D}$ is adjacent to $\theta_{A,B}$.

(ii) $$(A - C)/(B - D) = (A/C - 1)/(B/D - 1) = \frac{(A - 1)/(C - 1)}{(B - 1)/(D - 1)} = \frac{C - 1}{D - 1}$$

is a square. Hence, by Theorem 2.1(ii), $\theta_{C,D}$ is adjacent to $\theta_{A,B}$. □

Corollary 2.4. Let $\theta_{A,B} \in S$, $A \neq B$.

(i) $|\{\theta_{C,D} : \theta_{C,D} \in S, C \neq D, C/D = A/B, \theta_{C,D} \text{ adjacent to } \theta_{A,B}\}| = \frac{1}{2}(p - 7)$;

(ii) $|\{\theta_{C,D} : \theta_{C,D} \in S, C \neq D, (C - 1)/(D - 1) = (A - 1)/(B - 1), \theta_{C,D} \text{ adjacent to } \theta_{A,B}\}| = \frac{1}{2}(p - 7)$;

(iii) degree $\theta_{A,B} \geq \frac{1}{2}(3p - 19)$.

Proof. (i) Suppose $\theta_{C,D} \in S$, $C \neq D$, $C/D = A/B$, and $\theta_{C,D}$ is adjacent to $\theta_{A,B}$. Using the method of Theorem 2.3, set $R = (C - 1)/(D - 1)$. Then $R \neq 1$, $C/D$, $(A - 1)/(B - 1)$. We have $\frac{1}{2}(p - 7)$ choices for $R$.

(ii) Similar to (i).
Orthomorphisms of $Z_p$

(iii) It follows from (i), (ii) and Corollary 2.3 that the degree of $\theta_{A,B}$ is at least
\[ \frac{1}{2} \cdot 2(p - 7) + \frac{1}{2}(p - 5) = \frac{1}{2}(3p - 19). \]

It is natural to ask if $\theta_{A,B}$ can be adjacent to $\theta_{C,D}\beta^m$. This question is answered
negatively in the next theorem.

**Theorem 2.6.** Let $\theta_{A,B}, \theta_{C,D} \in S$, $A \neq B$, $C \neq D$. Then $\theta_{A,B}$ is not adjacent to
$\theta_{C,D}\beta^m$ for $m \not\equiv 0 \pmod{p}$.

**Proof.** See Evans [3].


Let $H$ denote the subgraph of $G_p$ induced by the elements of $S = \{\theta_{A,B}: \theta_{A,B} \in G_p\}$. The set $\{I_A: A = 1, \ldots, p - 1\}$ is a $(p - 1)$-clique of $H$ and any other
$(p - 1)$-clique of $H$ would give rise to a non-desarguesian plane of order $p$ (see Evans and Mcfarland [4]). It is natural to ask whether $H$ could contain another
$(p - 1)$-clique. Mendelsohn and Wolk [9] have shown, via a computer search, that
this cannot happen for $p = 13$ or 17. We extend this result to $p \leq 47$, using graphs
and simple hand calculations.

**Theorem 3.1.** If $p \leq 47$, then the only $(p - 1)$-clique of $H$ is $\{I_A: A = 1, \ldots, p - 1\}$.

**Proof.** If $p = 3, 5$, then $S = \{I_A: A = 1, \ldots, p - 1\}$. If $p = 7$, then $S = \{I_A: A = 1, \ldots, 6\} \cup \{\theta_{3,5}, \theta_{5,3}\}$ and $\theta_{3,5}, \theta_{5,3}$ are both adjacent to $I$ only. For $p \geq 11$ we
assume that $\{\theta_{A,B}: i = 1, \ldots, p - 1\}$ is a $(p - 1)$-clique of $H$. We may assume
without loss of generality that $A_i = i$ and $B_i = 1$. For all $i \neq 1$ both $A_i/B_i = i/B_i$
and $(A_i - 1)/(B_i - 1) = (i - 1)/(B_i - 1)$ must be squares. Thus $B_i$ is a square if and
only if $i$ is a square and $B_i - 1$ is a square if and only if $i - 1$ is a square.

There are two cases to consider.

**Case 1.** $p = 3 \pmod{4}$

For $p = 11$ consider the digraphs of Fig. 2. The vertices of I are those elements
$i$ of $GF(p)$ for which $i$ and $i - 1$ are both squares; the vertices of II are those
elements $i$ of $GF(p)$ for which $i$ is a square and $i - 1$ is a non-square; the vertices
of III are those elements $i$ of $GF(p)$ for which $i$ and $i - 1$ are both non-squares,
and the vertices of IV are those elements $i$ of $GF(p)$ for which $i$ is a non-square
and $i - 1$ is a square. In each of the digraphs I, II, III and IV there is a directed
edge from $i$ to $j$ whenever $j - i$ is a square.

For each digraph I, II, III and IV the mapping $i \rightarrow B_i$ must induce an
isomorphism. Hence $B_i = i$ for $i = 1, 3, 4, 5, 7, 8, 9$. But then, by Corollary 2.3,
$B_i = i$ for all $i$.

The same method is used for $p = 19, 23, 31, 43$ and 47.
Case 2. $p \equiv 1 \pmod{4}$

For $p = 13$ consider the graphs of Fig. 3. The vertices of graphs I, II, III and IV are defined as for the vertices of the digraphs I, II, III and IV of Case 1.

In each of the graphs I, II, III and IV we set $i$ adjacent to $j$ whenever $j - i$ is a square. Again, for each of the graphs I, II, III and IV, the mapping $i \rightarrow B_i$ induces an isomorphism. Hence $B_i = i$ for $i = 1, 2, 7, 12$.

If $B_3 = 9$, then $(A_3 - A_2)/(B_3 - B_2) = \frac{1}{3}$ a non-square. Hence by Theorem 2.1(ii), $\theta_{A_3,B_3}$ would not be adjacent to $\theta_{A_2,B_2}$. Thus $B_3 = 3$ and $B_9 = 9$ and so, by Corollary 2.3, $B_i = i$ for all $i$.

The same method is used for $p = 17, 29, 37, 41$. □

Corollary 3.1. If $p \leq 47$, then the subgraph of $G_p$ induced by the elements of $\{\theta_{A,B}^{m}: \theta_{A,B} \in S, m = 0, \ldots, p - 1\}$ contains only one $(p - 1)$-clique, $\{I_A: A = 1, \ldots, p - 1\}$.

Proof. This follows from Theorem 2.6 and Theorem 3.1 □
In our last result we give a necessary and sufficient condition for $H$ to contain a $(p - 1)$-clique other than \{$I_A$: $A = 1, \ldots, p - 1$\}.

**Theorem 3.2.** $H$ contains a $(p - 1)$-clique other than \{$I_A$: $A = 1, \ldots, p - 1$\} if and only if there exists an orthomorphism $\theta \in G_p - \{\theta_{A,B}\beta^m: \theta_{A,B} \in S, \ m = 0, \ldots, p - 1\}$ adjacent to $I_A$ for all $A$ square.

**Proof.** Let \{$\theta_{A,B}: i = 1, \ldots, p - 1$\}, $A_i = i, \ B_i = 1$ be a $(p - 1)$-clique of $H$ for which there exists a $j$ such that $B_j \neq j$. Let $M$ be the $(p - 1) \times (p - 1)$ matrix whose $ij$th entry, $m_{ij}$, is $j\theta_{i,B_i}$. Define a mapping $\Psi_j, \ j = 1, \ldots, p - 1$ by $0\Psi_j = 0$ and $i\Psi_j = m_{ij}$. Then $\Psi_j \in G_p$ for all $j$ and $\Psi_j = I_j$ whenever $j$ is a square.

Note that, if $j$ is a non-square then $\Psi_j \neq I_j$ and $\Psi_j$ is adjacent to $I_A$ for all squares $A$ and so, by Corollary 2.3, $\Psi_j \notin \{\theta\beta^m: \theta \in S, \ m = 0, \ldots, p - 1\}$.

Let $A \in G_p$ - \{\theta\beta^m: \theta \in S, \ m = 0, \ldots, p - 1\} be adjacent to $I_A$ for all squares $A$. Let $g = 1\Psi$. Then $g$ is a non-square. Let $i\Psi = gB_i$ and, for $h$ a non-square, define a mapping $\Psi_h: i \mapsto hB_i$. Then, if $A$ is a square, the mapping $i \mapsto i\Psi_h - i\Psi_k = A_i - hB_i = (h^{-1}gA)i - gB_i$ is a bijection and, if $h$ and $k$ are distinct non-squares, the mapping $i \mapsto i\Psi_k - i\Psi_h = (k - h)B_i$ is a bijection. Hence the set \{$I_A$: $A$ a square\} $\cup \{\Psi_k: k$ a non-square\} is a $(p - 1)$-clique of $G_p$ and the set \{\theta_{i,B_i}: i = 1, \ldots, p - 1\} is a $(p - 1)$-clique of $H$. This concludes the proof of Theorem 3.2.

**Acknowledgments**

I wish to thank the referee for bringing my attention to the paper by Mendelsohn and Wolk [9].

**References**