ON TRANSITIVE COMMUTATIVE IDEMPOTENT QUASIGROUPS

ARNOLD NEUMASTER

(Revised 28 May 1953)

Communicated by W. D. Wallis

Abstract

Commutative idempotent quasigroups with a sharply transitive automorphism group are studied in terms of so-called Room maps of C. Orthogonal Room maps and skew Room maps are defined for local Room maps and skew Room maps. Venn diagrams and pairwise comparison for skew Room maps lead to the existence of skew Room maps of groups of small prime power. Also some existence results are proved.

AMS Mathematics Subject Classification (1950): primary 02 B 31; secondary 32 M 10.

1. Room squares and orthogonal idempotents

1.1. Let \( r \) be an odd integer.

A Room square of side \( r \) is an arrangement of \( r+1 \) distinct objects in a square array of side \( r \) satisfying

(i) each of the \( r^2 \) cells of the array is either empty or contains exactly one cell.

(ii) each row and each column of the array contains each of the \( r+1 \) objects exactly once.

(iii) any unordered pair of distinct objects occurs exactly once in the array.

The array is skew, if in addition,

(iv) cell \((i,j)\) contains the pair \(i,j\),

(v) cell \((i,j)\) is empty if and only if \( j \neq r \) and cell \((r,j)\) is not empty; here cell \((i,j)\) is the cell in row \( i \) and column \( j \).

A Room square is known to exist if and only if \( r \neq 3, 5 \); see for example Wallis (1953a, 1954).
1. We refer to a commutative integral quasigroup $(Q, *)$ as a di-quasigroup.

Two di-quasigroups $(Q, *)$ and $(Q', +)$ are orthogonal if and only if the equations

\[ x + y = z, \quad 2x + y = z \]

have at most one solution $(x, y) \in Q$ (independent pairs). For every $a, b \in Q$, they are skew orthogonal if and only if, in addition, $a + b = a + 1$ is the only possibility to satisfy the equation $a + x = 2x + a + y = a + 1$.

Note that the two orthogonality are never orthogonal if considered simply as quasigroups.

1.5. By row and column permutations and renumbering of elements we may standardize any Room square such that the diagonal cells $(Q, *)$ contain the pair $i, i$, where $i$ is a fixed element. If we define two operations $*$ and $**$ on the set $G = \{1, \ldots, n\}$ by

\[ x * y = z \] if and only if $x + y = z$, or $x + y$ and the pair $x, y$ is in row $z$,  
\[ x ** y = z \] if and only if $x + y = z$, or $x + y$ and the pair $x, y$ is in column $z$.

A simple verification shows that $(Q, *)$ and $(Q, **) are a pair of (above) orthogonal di-quasigroups if and only if the given square is a stanardized (above) Room square.

Conversely, from (above) orthogonal di-quasigroups $(Q, *)$, $(Q, **) one may construct a standardize (above) Room squares, defining

\[ x, y \text{ is in cell } (x, y, x ** y) \text{ for every pair } x, y \in Q, x \neq y, \]

the other cells are empty.

The proofs are straightforward and thus omitted; see Brauer (1965).

3. Room squares and sharply transitive di-quasigroups

A di-quasigroup $(Q, *)$ is sharply transitive if and only if it forms a group $G$ of automorphisms, sharply transitive on $Q$. We describe sharply transitive di-quasigroups within the group $G$.

1. Let $G$ be a finite group. We call a map $p: \mathcal{G} \to G$ a Room map if and only if

1) $p(1) = 1$,

2) $p(x + y) = p(x) \cdot p(y)$,

3) $p(x * y) = p(x) \cdot p(y)$.
A Room map \( p \) satisfying

\[ p(x) = p(y) = z \text{ or } y = x^k \quad (a, b \in G) \]

is called transitive; if moreover,

\[ p(x) = p(y^k) = z = y^l \quad (a, b \in G) \]

then \( p \) is called above.

Example. The trivial map \( p \) with \( p(a) = 1 \) for every \( a \in G \) is a Room map.

Suppose \( p_1 \) and \( p_2 \) are Room maps. If

\[ p_1(x)p_2(y) = p_1(x^k)p_2(y^k) = x^t = y^r \quad (x, y \in G) \]

then we say \( p_1 \) and \( p_2 \) are orthogonal; if, in addition,

\[ p_1(x)p_2(x) = p_1(y)p_2(y) = x = y = 1 \quad (x, y \in G) \]

then \( p_1 \) and \( p_2 \) are said to be slow orthogonal.

From the definitions we see immediately that \( p \) is strong if and only if \( p \) and \( e \) are orthogonal, and \( p \) is slow if and only if \( p \) and \( e \) are slow orthogonal.

3.1. If \( G \) has odd order, and if \( p \) is a Room map of \( G \), define the operation \( *_p \) on \( G \) by

\[ u *_p v = p(uv) \quad \text{where } u^p = v^p = 1 \text{ and } u = v \]

(equivocally, \( u *_p v = u^p \).) Then \( G \) has odd order, the map \( p \longrightarrow *_p \) is a permutation of \( G \), that \( *_p \) is well defined. Because of \( p(1) = 1 = 1^p \), distinct maps \( p \) yield distinct operations.

(3.1.1) \( *_p \) is a ci-quasigroup. Because of \( u \neq 1 \), \( v \neq 1 \) we have

\[ u *_p v = p(uv) \quad \text{where } u^p = v^p = 1 \text{ and } u = v \]

(3.1.2) \( *_p \) has the solution \( u = v \) when \( p(uv) = 1 \) whenever \( u \).

We remark that \( G \) operates on the commutative ci-quasigroup by eight multiplications as a strongly inverse group of automorphisms.

If \( G \) is abelian and written additively then (3) simplifies to

\[ u *_p v = \frac{u + v}{2} = \frac{v + u}{2} \].

As a curiosity, we obtain from every noncommutative group \( G \) of odd order via the trivial Room map a (commutative) ci-quasigroup \((G, *) \) by \( u * v = 0 \) if and only if \( u = x^r v = 1 \) and \( u = y^s v = 1 \) if and only if \( y = x^r v = 1 \) and \( y = y^s v = 1 \) if and only if \( y = x^r y = v \).

An application of Room maps of groups of even order will be made in a forthcoming paper.
Let $(G,\circ)$ be a $G$-equi-group, and $G$ a sharply transitive group of automorphisms of $(G,\circ)$. Fix $a \in G$. Define a map $\phi: G \to G$ by

$$\phi(x) = x^a = x^1 \circ a = (x \circ a) \circ a^{-1} = a^{-1} (x \circ a) = (a^{-1} \circ x) \circ a.$$ 

Then $\phi(ab) = a \circ b = a$, whereas $\phi(1) = 1$; moreover

$$\phi(x^a) = (x^a)^a = a^{-1} \circ x^a \circ a = a^{-1} \circ a = 1$$

and therefore $\phi(x^a) = x^a$. Finally, $G$ has an odd number of elements, since the operation $\circ$ defined by $x \circ y = x$ is an involution fixing only the element $e$. Now the order of $G$ equals that number and thus is odd. Therefore the map $x \to x^a$ is a permutation of $G$. Note $\phi(x^a) = (x^a)^a = x^a$, and we get $\phi(\phi(x^a)) = x^a$, from where $\phi(x^a \circ y^a) = G \circ y$. This $\phi$ is a Room map.

If we fix an element $h \in G \setminus \{e\}$, then we get a Room map $\phi'$. Relative to $h$ we get $\phi'(x) = x^h \circ h^{-1}$. Therefore, $\phi$ and $\phi'$ are equivalent by the automorphism $x \to x^{-1}$ of $G$ (in the sense of the next section).

Because of $\phi(1) = 1$, which can easily be verified, we get distinct Room maps from distinct $G$-equi-groups.

2.4. We may, $G$ is a sharply transitive group of automorphisms of a standardised Room group, if $G$ is a sharply transitive group of automorphisms of $G$-equi-groups $G_{0}$ and $G_{0}$. Then

**Theorem 1.** A (finite) Room group $G$ with a sharply transitive group $G$ of automorphisms exists if and only if $G$ has odd order, and $G$ admits a pair of (finite) orthogonal Room maps. In particular, if there is a group (finite) Room map of $G$ then we may construct from it a (finite) Room space.

**Proof.** From the preceding, it suffices to prove the following.

**Lemma 1.** Let $\phi, \psi$ be Room maps of $G$. $\phi$ and $\psi$ are (finite) orthogonal if and only if $\phi$ and $\psi$ are (finite) orthogonal.

**Proof (of the Lemma).** From the definition, $\phi_{x} = \phi, \psi_{x} = \psi$ if and only if $\phi_{x^{a}} = a^{-1} \circ x^{a} \circ a^{-1} = x^{a}$ if and only if $\phi_{a^{-1}} = a^{-1} \circ x^{a} \circ a^{-1} = x^{a}$. Thus every $a$ leads to at most one solution $[a]$. Hence if $\phi_{x} = \phi, \psi_{x} = \psi$ and $\phi_{y} = \phi, \psi_{y} = \psi$, then $\phi_{x^{a}} = x^{a}$ if and only if $\phi_{y^{a}} = y^{a}$. Hence $\phi_{x^{a}}$ and $\psi_{x^{a}}$ determine $a, x^{a}$ uniquely, or, eliminating $a$ and only if the equation $\phi(x) = \phi(y)$ determines $(a, x^{a})$ uniquely. But this is equivalent to $(a, x^{a})$. In particular, if $\phi_{x} = \phi, \psi_{x} = \psi$, then $\phi_{x^{a}} = \phi_{x}$. Thus $\phi_{x} = \phi_{x^{a}}$. Similarly, $\phi_{y} = \phi_{y^{a}}$. Then $\phi_{x} = \phi_{x^{a}}, \phi_{y} = \phi_{y^{a}}$ if and only if $\phi_{x} = \phi_{y}$, or, eliminating $a$ and $\phi$, to $\phi(x) = \phi(y)$. Now $\phi_{x}$ and $\phi_{y}$ are orthogonal if and only if we may conclude $a = x = 1$, that is if and only if $\phi$ and $\psi$ are finite orthogonal.
3. Equivalence and multipliers

Let \( G \) be a finite group and \( \text{Aut}(G) \) the full group of automorphisms of \( G \).

**Lemma 2.** If \( \phi \) is a Roos map, then, for every \( \alpha \in \text{Aut}(G) \), the map \( \phi^\alpha \) defined by
\[
\phi^\alpha(x) = \phi(\alpha(x))
\]
is a Roos map. We say \( \phi^\alpha \) is a shift of \( \phi \).

(1) and (2) are easily verified; (3) follows from the fact that
\[
\phi^\alpha(x) = \phi(\alpha(x)) = \phi(\phi^{-1}(\alpha(x))) = (\phi^{-1}(\alpha))(x) = \phi^{-1}(\alpha(x)).
\]

Call two Roos maps equivalent if one is a shift of the other. Two equivalent Roos maps lead to isomorphic di-quasigroups \((G, \cdot^\alpha)\) and \((G, \cdot^\beta)\); in fact, \( \alpha \) is an isomorphism from \((G, \cdot^\alpha)\) to \((G, \cdot^\beta)\).

**Problem:** Are there in any group \( G \) inequivalent Roos maps leading to isomorphic di-quasigroups?

**Lemma 3.** Call an automorphism \( \alpha \in \text{Aut}(G) \) a multiplier of \( \phi \), if \( \phi^\alpha = \phi \). Denote by \( \text{Mul}_\phi \) the set of all multipliers of \( \phi \). We show that \( \text{Mul}_\phi \) is a group: If \( \alpha, \beta \in \text{Mul}_\phi \), then, using the multipliers property and the definition
\[
\phi^\alpha(x) = \phi(\alpha(x)) = \phi(\phi^{-1}(\alpha(x))) = (\phi^{-1}(\alpha))(x) = \phi^{-1}(\alpha(x)).
\]
Therefore \( \phi^{\alpha \beta} = \phi^{\alpha} \phi^{\beta} \). Moreover, if \( \alpha \in \text{Mul}_\phi \) is an automorphism of \((G, \cdot^\alpha)\), then it is an automorphism of \( G \), this is equivalent to \( x = \alpha x = \alpha \phi(x) \), \( \phi(x) = \phi^{-1}(x) \). Thus we have \( \omega, \phi = \phi(\phi^{-1}(x)) = (\phi^{-1}(\phi(x))) = (\phi^{-1}(\phi(x))) \).

But \( \alpha \) is a multiplier of \( \phi \), that is \( \phi^\alpha = \phi \). Therefore
\[
(\alpha \cdot^\beta x) = \phi(\alpha \cdot^\beta x) = \phi(\phi(\alpha \cdot^\beta x)) = \phi(\alpha \cdot^\beta x) = \phi(\alpha \cdot^\beta x),
\]
and the lemma is proved.
By a straightforward computation we get the product and inverse rules:

\[ (a,b)(c,d) = (ac,b'd') \]

\[ (a,b)^{-1} = (a^{-1},b'^{-1}) \]

Consequently, \((\text{Mult} \times G) \times G\) is a split (aislewise) product.

3.3. Now we characterize the group \((\text{Mult} \times G) \times G\) within the group of all automorphisms of \(\{(a,b)\}^\times G\).

Theorem 3. Let \(G\) be a group of odd order, and \(x \in G\). Then the split product \((\text{Mult} \times G) \times G\) is the automorphisms \(\text{Aut}(x)\) of \(G\) in the full group of automorphisms of \(\{(a,b)\}^\times G\). Moreover, if \(G\) is abelian and \(x = 0\) in the trivial abelian group, then \(\text{Mult} \times G \subset \text{Aut}(0)\) and \((\text{Mult} \times G) \times G \subset \text{Aut}(0) \times G\).

Proof. (a) We compute easily \((\text{Mult} \times G) \times G\) and \(\text{Aut}(x)\); thus the isomorphism in question contains the group \((\text{Mult} \times G) \times G\).

Let \(s\) be an element of \(\text{Aut}(x)\). Setting \(s = \varphi, \varphi^{-1}\) we have \(\varphi^{-1}x\varphi = 1\), and \(\varphi^{-1}(a,b)\), that is

\[ r^{-1} = s \]

\[ (x, y) \mapsto (x', y') \quad \text{for every} \quad x, y \in G. \]

From (9), for every \(x \in G, G\) contains an element \(x'\) with \(t = (x, y) = (1, y)\). We have \(x' = \varphi x\varphi^{-1} = \varphi x\varphi^{-1} = x\varphi(\varphi^{-1}) = x\). For all \(x \in G\). Then we get

\[ (x, y) \mapsto (x, y') \quad \text{for every} \quad x \in G, y \in G. \]

and \(t\) is an element of \(\text{Aut}(x)\).

Finally, since from (10)

\[ \varphi(x) = \varphi(x') = (\varphi^{-1}x\varphi^{-1})(\varphi^{-1}) = \varphi^{-1}x\varphi^{-1} = \varphi^{-1}x, \]

\(s\) is in \(\text{Mult} \times G\), and we have \(s = (1, 1)\). \(\text{Mult} \times G \subset \text{Aut}(x)\).

Thus proceeding for every \(x \in \text{Aut}(x)\), we arrive at \(\text{Aut}(x) = \text{Mult} \times G\), and the first part follows.

(b) If \(x = 0\) then trivially \(\text{Mult} \times G \subset \text{Aut}(0)\). It remains to show that, if \(G\) is abelian, every automorphism of \(\{(a,b)\}^\times G\) is in \((\text{Mult} \times G) \times G\). We use the additive notation \((a, b, c)\), and we have \(a + b = (a, b)\). The identity automorphism \(x\) of \(\{(a,b)\}^\times G\) satisfies \(x + yz = (x + y)z\). Define the permutation \(s\) by \(x' = s'x\). Then

\[ s + yz = \frac{y + (x + yz)}{2}, \quad 0 = 0. \]

Thus \(s\) gives \((x' + y)' = (x + y)'\) for every \(x \in G\), and (11) simplifies to \((x' + y)' = x' + y\),

and it is an automorphism of \(G\). Thus \((1, 1) = (0, 0) = (\text{Aut}(0) \times G).
4. A general lemma for constructing strong room maps

4.1. We begin with a very general construction lemma and then specialize more and more to get more concrete results.

Lemma 4. Let $G$ be a group of odd order, and $H$ a subset of $G$ with the property

$H\cdot H^{-1} = \{1\},$

where $H^{-1}$ denotes the set of inverses of elements of $H$. If $\pi, \sigma$ are permutations of $G$ such that

$I^* = I^* = I,$

then the map $\rho$ defined by

\[
\rho(x) = \begin{cases} 
1 & \text{if } x = 1, \\
\pi(\sigma(x)^{-1}) & \text{if } x \in H, \\
\sigma(x) & \text{if } x \in H^{-1}
\end{cases}
\]

is a Room map, $\rho$ is strong if

\[
\{\rho(x) | x \in H\} = G.
\]

Remark. (17) is only a necessary sufficient condition for $\rho$ to be strong.

A set $H$ satisfying (12) exists in every group of odd order. For $x \in H$, put one of $x, x^{-1}$ in $H$, the other in $H^{-1}$; we have $x \neq x^{-1}$ since $|G| = 3$ implies $x = 1$.

Proof (of Lemma 4). Verifications of (1) and (2) are trivial. To prove (3), consider $[\rho(x) | x \in H] = [\pi(\sigma(x)^{-1})] = [\rho(x) | x \in H^{-1}]$. By (13) and (16), this is equal to $[\rho(1) | x \in H] = [\rho(x^*x^{-1}) | x \in H] = [\rho(x) | x \in H^{-1}]$. By (15), $H^* = H$, and with (12) the expression reduces to $G = G$. From the definition of
of cocycles, $a$ is strong if all $a^k$ with $k \neq 0$ are different. But this is guaranteed by (7).

The construction of Lemma 4 is very general, since every Rozen map $p$ may be constructed in this way. The permutation $\nu$, defined by $\nu^k = (a^k)^{-1}$ for all $k$, and the identity mapping $\alpha$ satisfy (13)-(15) and the condition (16) below for any $x \in \mathbb{Z}$. If $x$ is a permutation of $\nu$ is a Rozen map and (2) and (3) hold.

The value of the construction lies in the freedom of $H$. If we take for $x$ a suitable permutation, for example a transposition of $\mathbb{Z}$, which satisfy (13), (14) and (15), then we may try to find a set $H$ satisfying (3) and (3) to obtain a strong Rozen map.

4.5. To analyze the conditions under which (12) and (15) are satisfied, denote by $-1$ the permutation $-x^{-1}$. Let $d$ be the group generated by $x$ and $-1$. Then $x \in d$ if and only if it has a representation $x = x^k d^k x^{-k} d^{-k}$ where $k$ is an even integer. Thus we have

\[ (-1) x (-1) = (x^{-1}) (x^k d^k x^{-k}) (x^{-1}) (x^k d^{-k} x^{-k}), \]

and therefore $(-1) d (-1) x (-1)$, define by $x^d$ the set of all $x^k$, $k \in d$.

Lemma 5. A set $H$ satisfying (12) and (15) exists if and only if

(16)

\[ x^{d} \alpha^{d} = 0 \quad \text{for every } x \in d, \]

or, equivalently, if and only if

(16a)

\[ x^{d} \neq 0 \quad \text{for every } x \in d. \]

Proof. The equivalence of (16) and (16a) is trivial.

(1) Necessity: We have $H^{d} = H^{d} = H$, and from (16) we get $H^{d} = H^{d} = H$. Hence $H^{d}$ is fixed under $d$. Let $H = U_{x \in d} x^{d}$ be the partition of $H$ into $d$-orbits. Then $H^{d} = \bigcup_{x \in d} x^{d} d x^{-d}$, and we obtain (16).

(2) Sufficiency: Set $R_{H} = \emptyset$. Suppose we have already found a subset $R_{H} \subseteq H$ with

(17)

\[ H \cap R_{H}^{d} = \emptyset, \quad 1 \not\in H, \text{ and } H^{d} = H. \]

If $R_{H} = \emptyset$, $R_{H} = R_{H}^{d}$ $\neq \emptyset$. Otherwise we take an $x \in G$ with $x \not\in R_{H}$, $x x_{R_{H}} = x_{R_{H}}$, and we define $R_{H} = R_{H}^{d}$. Clearly, $R_{H} = R_{H}$. If $a \in R_{H}$, then $a \not\in R_{H}$, hence we have the contradiction $x = 1$, if $x x_{R_{H}} = x_{R_{H}}$, then by (16), either $x \not\in H$ or $x \not\in H^{d}$, if the second holds, replace $x$ by $x^{-d}$, hence we may assume $x \not\in H$. Now by (16a) $x x_{R_{H}}$, from which we may deduce the contradiction $x x_{R_{H}}$. Therefore such a $x$ cannot exist, and we conclude $R_{H} = R_{H}^{d} = \emptyset$.

Repeating this process we finally arrive at a subset $H = R_{H}$ satisfying (12) and (15).
5. Direct constructions for skew norm maps

5.1. Let $R$ be a commutative, associative ring with identity 1. A (not necessarily stably) group $G$ is an $R$-group provided that $R$ operates on $G$, and the following relations hold:

\[ r \cdot 1 = 1 \quad \text{for all } r \in R, \quad \forall x, y \in G, \]

\[ x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \text{for all } x, y, z \in G, \]

\[ x \cdot r = r \cdot x \quad \text{for all } x \in G, r \in R. \]

Note that nothing is required for the operation of $R$ on products in $G$.

$L^R_G$ denotes the group of units of $R$.

**Lemma 4.** Let $G$ be an $R$-group. Suppose $G$ contains an element $a \neq 0$ such that

\[ a^{-1} = -a, \quad a + a = 0, \quad a^2 = a. \]

Then we may construct a set $H$ satisfying (12) and (13), and for every such set $H$ the map defined by

\[ f(x) = \begin{cases} 1 & \text{if } x = 1, \\ 0 & \text{if } x \in H, \\ x & \text{if } x \notin H. \end{cases} \]

where $x = (1 - x)(1 + x)$, is a skew Riesz map on $G$.

**Proof.** (a) We have $(-1)(-1) = 1$ since $-1 \cdot 1 = 0$ and $R$ is commutative. Hence $d$ is generated by $a$. Now, if $a^{-1} = b$, then $a = b^{-1}$ for some integer $b$. But then $a^2 = 1$. Since $a$ has odd order, $a^2 = 1$ or $a = 1$, whence $a = 1$, and (14) holds. By Lemma 5 we may construct a skew Riesz map on $G$ with the required properties.

(b) Now we want to apply Lemma 4. (13) is satisfied by hypothesis, and so is (14), with $a = 2a$, $a^2 = 1$, $a^{-1} = a$, $a^2 = a$, $a^4 = 1$, $a^8 = 1$. Application of Lemma 4 yields the skew Riesz map (12) from (13): for

\[ x \cdot 1 = x^2 = \ldots = x^{2^n-1} = x^2 (x^{2^n-2}) = x, \]

and similarly for $y^p = y$. Since $a$ is a unit, (17) is valid, and $p$ is chosen.

(c) It remains to show that $p$ is skew. Indeed, if $p(x) = p(y)^p$, $x \neq 1$, then we may assume $a, y \in R$ since $p(y)^p = (p(y))$. But then by (12) $x = y$, or $a(p - 1)$.

Now we need to show that $p(x) = p(y)$ for all $x, y$. First, $x \neq 1$, hence $p(x) = 1$, or $p(x) = x$. But then $G = G$, contradicting (13). Thus, (13) holds, and $p$ is skew.
Remark. If \( R \) operates faithfully on \( G \), and if a subset \( H \) of \( G \) satisfies (12) and (13) then (14) is valid. For suppose the least positive integer with \( a^i = 1 \) is even, \( i = 2^n \). Then \( a^{2^n} = (a^{2^{n-1}})^2 = 1 \), and \( a^{2^{n-1}} = a \), that is there is an \( x \in G \) with \( x^{2^{n-1}} = 1 \). Since \( R \) is faithful on \( G \), taking \( x = x^{2^{n-1}} \), we obtain \( x^x = x^{2^{n-1}x^{2^{n-1}}} = x^{2^{n-1}} = 1 \), thus (14) holds. By Lemma 5.

5.2. Now we are able to prove theorems, that is, existence, results. There are several important classes of groups \( G \): 
- \( G \) is a finite group of order \( n \) and \( R \) is the ring \( \mathbb{Z}/n\mathbb{Z} \) of integers modulo \( n \).
- \( G \) is an additive group, and \( R \) is the ring of all endomorphisms of \( G \).
- \( G \) is a finite group, \( R \) is an automorphism of \( G \) satisfying
  \[
  x^{x^x} = x^x \quad \text{for every } x \in G,
  \]
and \( R \) is the ring of all rational exponents \( \mu \), which are well defined (that is distinct in a homomorphism).\( \mathbb{R} \) operates on \( G \) in an obvious way. We note that \( R \) possesses an inverse if and only if \( (\mu) \) is an automorphism. From Lemma 6 we obtain immediately:

**Theorem 3.** Let \( G \) be a group of odd order. If there is an automorphism \( \mu \) such that

\[
\mu^x = x^x \quad \text{for every } x \in G,
\]

then \( G \) admits a skew-Bruck map.

A formal proof is a group of the form \( 2^k \); from elementary number theory, \( 2^k \) is a group. The only known Brauer classes are the primes \( x, y, z, f_1, f_2, f_3, f_4 = 3, 5, 7, f_5 = 13, f_6 = 23, f_7 = 83, f_8 = 17, f_9 = 67 \). (The Brauer classes are known to be imprimitive.)

**Theorem 4.** If \( G \) is the elementary abelian group of order \( p^n \), \( p \) an odd prime, then, with possible exception of \( p = 3, l = 2, \) and \( p = f_5, l = 3, G \) possesses a skew-Bruck map.

**Proof.** Let \( E = GF(p) \) be the Galois field of order \( p \). We may assume that \( G \) be the additive group of \( E \), if \( p \) is a primitive element of \( GF(p) \), then, with \( p = 2 + 1 \) and odd, \( v = p^n \) is an endomorphism of \( G \) of order \( l = p^{n-1} - 1 \) in the automorphisms of \( G \) that is odd, \( n = 2, \mu, v = v \) are automorphisms of \( G \) if and only if \( x \) is a homomorphism of \( G \) if and only if \( x \) is a skew-Bruck map. Then, if \( v = 1 \), we may apply Lemma 6 to
Given: Let $T$ be a left coset of $O_{G}$, i.e., $T$. The map $\psi$ defined by $r'G = \psi(r)T(p)$ is a derivation of $T$ being only 1. Select one of $F'$ for every $(r', r') \in G - 1$ and call the resulting set $B$. Then we have:

$$T = S \cup B = (1, X, G), \quad rS = \psi(r)T(p), \quad F' = (G, G').$$

The maps

$$r \mapsto f = e^{{-i} g} (\psi(X), e^{{-i} r})$$

are automorphisms of $G$. Considering $g$ as a unit in the ring of automorphisms of $G$, express such as $e^{{-i} g}, e^{{-i} r}, \ldots$ take some.

We identify $G$ with $G(p) = G'$ by

$$G(p) = \psi(1, \psi(X), e^{{-i} r}).$$

and verify the equation

$$G(p) = \psi(e^{{-i} g}, e^{{-i} r}),$$


We may that an integer $a$ satisfying

$$(a, a') = (8 + 1, a' - (a'-1, a') \text{ for every odd } f)$$

(here, for example, $a$ with $a' = 1$, $a = 1$ and $p$ for every prime $p$ dividing $a$; this is possible since there are $(p-1)/2 > 1$ quadratic nonresidues mod $p$). Define

$$n(p) = \left\{ \begin{array}{ll} \psi(p) & \text{if } e^{{-i} p} \text{ is odd}, \\
\psi(p) & \text{if } e^{{-i} p} \text{ is even}. \end{array} \right.$$  

$$\psi(p) = \left\{ \begin{array}{ll} (\psi(p), p) & \text{if } x = 1, \\
(\psi(p), p') & \text{if } x = 2. \end{array} \right.$$  

We verify easily

$$n(p) = \psi(p), \quad n(p) = \psi(p) \quad \text{for } x < 2,$$

$$\psi(p) = n(p), \quad \psi(p') = n(p) \quad \text{for } x < 2,$$

and a straightforward proof of uniqueness: $n$ is a Root map, and it trivial if and only if both $p$ and $P'$ are trivial.

(To prove that $n$ is a Root map just note that

$$\psi(e^{{-i} g}) = n(p).$$

(5.5)}
For \( i = 1 \), the left side equals \( q_i(x) = q_i(x) \), for \( i \neq 1 \) we have

\[ q_i(x) = x \cdot x = x^2 \]

and for \( i = 0 \), \( u_0 \cdot u_0 = u_0 \) since \( u_0 \cdot u_0 = u_0 \).

Now \( q_0(x) = x \cdot x = x^2 \) and by (9), if

\[ x = (\Phi g)(x) \cdot (\Phi g)(x) = (\Phi g)(x) \cdot (\Phi g)(x) \]

\[ = (\Phi g)(x) \cdot (\Phi g)(x) = q_0(x) \]

Therefore (1) and (2) are valid.

Finally suppose \( q_i(x) = q_i(x) \). In the factor group we have

\[ \Phi(x) = \Phi(x) \cdot \Phi(x) = \Phi(x) \cdot \Phi(x) \]

and since \( \Phi \) is a Room map, \( \Phi(x) = \Phi(x) \). Suppose \( \Phi(x) = \Phi(x) \), \( \Phi(y) = \Phi(y) \), where \( \Phi(x) \), \( \Phi(y) \), \( x \), \( y \).

Then

\[ \Phi(x) = \Phi(x) \cdot \Phi(y) = \Phi(x) \cdot \Phi(y) \]

and similarly \( \Phi(y) = \Phi(x) \cdot \Phi(y) \) where \( \Phi(x) = \Phi(x) \).

or

\[ \Phi(x) = \Phi(x) \cdot \Phi(y) = \Phi(x) \cdot \Phi(y) \]

If \( i = 1 \) then we obtain \( \Phi(x) = \Phi(x) \), or \( x = x \) since \( \Phi \) is a Room map, if \( x \neq 0 \) then \( \Phi(x) = \Phi(x) \), or \( x = x \) since \( x \). If \( x \neq 0 \) then \( \Phi(x) = \Phi(x) \), or \( x = x \) since \( \Phi \) is a Room map.

Now the order of \( \Phi \) divides the order of \( G \) and thus \( i \) is valid. By hypothesis, \( (\Phi^{-1}(x) \cdot x = 1 \), and thus \( \Phi(x) = \Phi(x) \), or \( x = x \) since \( \Phi \) is a Room map.

In every case we obtained \( x = x \), or \( x = x \) since \( \Phi \) is a Room map. (4) follows. This \( q_i(x) \) is a Room map.

(4) To prove orthogonality we have to show that

\[ \Phi(x) \phi(x) = \Phi(x) \phi(x) \]

is possible only for \( x = y \) or \( x = y \). Since (2) is valid we may assume \( x = y \). In the factor group we get \( \Phi(x) \phi(x) \phi(y) = \Phi(x) \phi(y) \phi(y) \), whereby \( \phi(x) = \phi(x) \) since \( \Phi \) is orthogonal. Now if \( x = y \) then

\[ \phi(x) \phi(x) \phi(x) = \phi(x) \phi(x) \phi(x) = \phi(x) \phi(x) \phi(x) \]

and \( x = y \) or \( x = y \) from the orthogonality of \( \phi \). And if \( x = y \), \( x = y \). In \( \Phi(x) \phi(x) \phi(y) = \Phi(x) \phi(y) \phi(y) \), we have

\[ \phi(x) \phi(x) \phi(x) = \phi(x) \phi(x) \phi(x) = \phi(x) \phi(x) \phi(x) \]

or

\[ \phi(x) \phi(x) \phi(x) = \phi(x) \phi(x) \phi(x) = \phi(x) \phi(x) \phi(x) \]

and \( x = x \) or \( x = x \). And if \( x = y \), \( x = y \).
and similarly \( \pi(x y) = \pi(x) \phi(y) \). Thus we have

\[
\pi(x y) = \pi(x) \phi(y) = \pi(x) \phi(y) = \pi(x) \phi(y) = \pi(x) \phi(y)
\]

and \( \pi \) because \( g, h \in G \). Therefore \( x = 1 \).

(c) Now suppose \( \pi(x) \) and \( \phi(y) \) are skew eigenvectors. From

\[
\pi(x) \phi(y) = \phi(y) \pi(x)
\]

we get from the skew orthogonality in the factor group \( M = G \), that is

\( x, y \in G \), and then \( x = y = 1 \) since \( x \) and \( y \) are skew eigenvectors in \( G \). Thus \( \pi(x) \) and \( \phi(y) \) are skew orthogonals.

From the proof, we retrieve the following part as

**Corollary.** If \( G \) is a group of odd order, and \( G \) is an abelian group of order prime to 3, and if \( H, H \) are skew eigenvectors in \( G \) resp. \( G \) then the maps \( x, y \) of the direct product \( G \times G \) defined by

\[
\pi(x, y) = \begin{cases}
(0, g) & \text{if } x = 1, \\
(y, \phi(y)) & \text{if } x \neq 1,
\end{cases}
\]

\[
\phi(x, y) = \begin{cases}
0 & \text{if } x = 1, \\
(x, \phi(x)) & \text{if } x = y.
\end{cases}
\]

where \( H \) is a set with \( H = H = G \), \( H = H = G \), \( H = H \), are a pair of skew eigenvectors in \( G \).

**Proof.** If there is a product construction if \( G \) is nonabelian as if the order of \( G \) is not prime to 3.

6.1. Now we use the theorems to prove

**Theorem 1.** Every group \( G \) of order prime to 3 is skew skew.

**Proof.** As has odd order, and that is soluble: Now any maximal normal sub-

\( G \) of \( G \) is a skew skew, and has an order prime to 3. For groups

\( G \) of order prime to 3, Cheng (1972) proved the existence of skew skew skew skew.

\( G \) of prime order. Then by Theorem 3 (Section 8) these groups admit skew skew skew skew skew skew skew skew.

For the other skew skew skew skew skew skew skew skew skew.

\( G \) of prime order. Then \( H \) admits a skew skew skew skew skew.

Induced on the order of \( G \) (beginning with the trivial group of order 1 where \( \pi(a) \) is a skew skew skew skew skew skew skew.)
THEOREM 7a. Let $G$ be a group of odd order, and suppose $G$ possesses a chain
\[(G)\]
with normal subgroups $G_i$ of $G$ and abelian factors $G/G_i$ of an order prime to $3$
(for $i > 1$); let $G = G_1 = G_2 = \cdots = G_3 = 1$. Then, if all factors $G_i/G_{i+1}$ have an odd
power of $3$ (when $3$ does not divide $N$), there exists a strong (above) Room map, if admits a strong (above) map, see.

Proof. The theorem is trivial if $n = 1$. Now, proceed by induction on $n$. If $G$
violates the stated conditions then $G/G_{n+1}$ does, but with $n - 1$ instead of $n$. By
induction, $G/G_{n+1}$ admits a strong (above) Room map. Since $G_{n+1} = G_nG_{n+1}$,
promotes a strong (above) Room map, we apply Theorem 6 yielding a strong
(above) Room map of $G$,

Remark. Every abelian group possesses a chain (7) with normal subgroups $G_i$
of $G$ and abelian factors $G_i/G_{i+1}$ for all $i$.

7. A coexistence theorem for skew room maps

Lemma 8. Let $G$ be a group of odd order, and if $A$ is a set with $|A|^{n-1} = 3$,\n$\{H \in G : G/H = G - |A|\}$. If $G$ is a skew Room map of $G$, then\n$(g, h)(g, h)^{-1} = H = G - |A|$,\nand every element is obtained exactly once on the left.

Proof. Since $g$ is strong, all $g(a)$, where $a$ runs over $H$, are distinct: the same
holds for the $g(a)^{-1}$. But $g$ is skew, and therefore every $g(a)$ is distinct from every
$g(a)^{-1}$ for $a \in A$. Then $(g(a), g(a)^{-1}) \in E$ is a set of $|A|$, $|A| = |A|^{-1}$. Hence,
$g(a)$ is strong and $g(a)^{-1}$ is not to the left, and the assertion follows.

Now let $g$ be a Room map of $G$, and $r: G \rightarrow \mathbb{Z}$ a homomorphism of $G$ onto
$\mathbb{Z}$. Then the kernel $\ker r$ has order $|G|^{1/2}$. From (7), counting multiplicities,
$[|x|=0 = G = (g(a)^{1/2}) - x] = 0$.

Summing up the squares of the elements we obtain (a sum over $G$):
\[
\sum g(a)^{2} = \sum g(a)^{2} + \sum g(a)^{2} - 2 \sum g(a)^{2} \cdot \sum g(a)^{2} = \sum g(a)^{2} \cdot \sum g(a)^{2},
\]
\[
\sum g(a)^{2} = -\sum g(a)^{2} \cdot g(a)^{2} = \sum g(a)^{2} \cdot g(a)^{2} = \sum g(a)^{2} \cdot g(a)^{2} = 0.
\]

Since
\[
g(a)^{2} + g(a)^{2} = g(a)^{2} + g(a)^{2} = g(a)^{2} + g(a)^{2} = 0.
\]
Therefore, if \( p \) is prime,

\[ 0 = 2 \sum (p(p+1)) = \sigma(p)\sigma(p+1) = \sigma(p)\sum_{i=1}^{p} i = \sigma(p)\cdot \frac{p(p+1)}{2} \approx \frac{p^2}{2}. \]

Now, \( \sigma(p) = \sigma(p+1) = \sigma(p) = 2p+1 \) since \( p \) is prime, and the preceding theorem. But

\[ \sum_{i=1}^{p} i = \sigma(p) = 2p+1 = \frac{p(p+1)}{2} \approx \frac{p^2}{2}. \]

Thus

\[ (2p-1)(2p-3) = 4p^2 - 12p + 3 \approx 4p^2 - 8p. \]

or

\[ (2p-1)(2p-3) = 4p^2 - 12p + 3 \approx 4p^2 - 8p. \]

From this we deduce

**Theorem 5.** Suppose a group \( G \) of odd order contains a normal subgroup \( H \) of order prime to 3 with cyclic, factor group of order divisible by 3. Then \( G \) admits a skew Room map.

**Corollary.** An abelian group of odd order possessing a nontrivial cyclic 3-Sylow subgroup admits a skew Room map.

**Proof.** Suppose \( G \) admits a skew Room map. By hypothesis, \( G \times K \) is cyclic, isomorphic to \( Z_3 \times K \). Therefore a homomorphism \( f : G \longrightarrow \text{End}(Z_3) \) exists, and (22) in valid. By assumption, \( f(\alpha) = 1 \). (25) yields \( f(g) = 1 \). But \( f(g)^{-1} = f(g) \) since the order of \( K \) and prime to 3, a contradiction.

**Remark.** The corollary was proved in terms of skew strong starters (compare with Section 8 in White and Wallis (1977)).

8. Room maps and starters

8.1. For Room maps and a skew strongly starter group of automorphisms another description is available: the matrix approach. Matrices are widely used in the literature on Room squares and their constructions of ergodic graphs; see the examples Makra and Nešetřil (1966), Wallis et al. (1972), Wallis (1978), Wallis and Wallis (1972) and Anderson (1978). We derive a one-to-one correspondence between starters and Room maps.

Let \( G \) be a group of odd order.
A monoid is said to be the union of two sets such that 
\[ (a, b, c) \in G \] 
A right order is a subset \( R \) of \( G \) such that for all \( a, b, c \in G \), 
\[ (a, b, c) \in R \] 
A left order is a subset \( L \) of \( G \) such that for all \( a, b, c \in G \), 
\[ (a, b, c) \in L \] 

The order is given by 
\[ a \cdot b = c \] 

1. If \( p \) is a Right Order of \( G \) then 
\[ X = \{(q, r, s) \in G \mid q \cdot r = s \} \]
2. If \( g \) is a Left Order of \( G \) then 
\[ Y = \{(q, r, s) \in G \mid q = s \cdot r \} \]

The order is given by 
\[ a \cdot b = c \] 

1. If \( p \) is a Right Order of \( G \) then 
\[ X = \{(q, r, s) \in G \mid q \cdot r = s \} \]
2. If \( g \) is a Left Order of \( G \) then 
\[ Y = \{(q, r, s) \in G \mid q = s \cdot r \} \]
5.2. During preparation of this paper, a paper of Gross and Leonard (1973) on admissible paths for the patterned matrix is not yet available; the purpose is to provide some of the results above. They work with left admissible paths for the patterned matrix which are related to Roos maps by Theorem 9 via the following.

Theorem 9. If \( d = \{a/(c/a)\} \) is a right admissible path for the patterned matrix then \( d' = \{a/(c/a)\} \) is a left admissible path for the patterned matrix, and conversely.

Proof. Let the patterned matrix be \( X = (a_{ij}) \). Then \( d \) is a right admissible path for \( X \) if and only if \( \forall a_{ij} \in a_{ij} \), \( i \in \{1, \ldots, m\} \), \( j \in \{1, \ldots, n\} \), \( i = j \) hold; and only if \( \forall a_{ij} \in a_{ij} \), \( i \in \{1, \ldots, m\} \), \( j \in \{1, \ldots, n\} \), \( i = j \) hold. Consequently, \( d \) is a right admissible path for \( X \).

Conversely, to every strong Roos map \( \phi \) a left admissible path for the patterned matrix \( (a_{ij}) \) is associated by \( a' = \{a(i,j) \in \phi \} \). Conversely, every left admissible path of the patterned matrix corresponds to a strong Roos map.

By the corollary, Theorem 1 of Gross and Leonard (1973), together with their Theorem 4 in, if \( X \) is abelian, equivalent to the special case of Theorem 6 of this paper, where the patterns of orthogonal Roos maps are decomposed of the normal map and a strong Roos map, each.

By Lemma 3, the existence of right admissible paths is equivalent to the existence of left admissible paths (for the patterned matrix only); in particular, Th. 2 of Gross and Leonard (1973) may be replaced by the 'dual' of Theorem 1, giving an existence criterion for right admissible paths in extensions of abelian groups not depending on the factor system.

Theorem 6 of Gross and Leonard (1973) is equivalent to Theorem 7 here.

References


B. A. Andreasen (1972), "One-to-one maps in the theory of hop and


C. B. Andreasen (1972), "One-to-one maps in the theory of hop and
