Relative difference sets fixed by inversion (III)—Cocycle theoretical approach

Yu Qing Chen\textsuperscript{a}, K.J. Horadam\textsuperscript{b}, Wei-Hung Liu\textsuperscript{b,1}

\textsuperscript{a}Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435-0001, USA
\textsuperscript{b}School of Mathematical and Geospatial Science, RMIT-City Campus, GPO Box 2476V, Melbourne, Vic. 3001, Australia

Received 3 June 2003; received in revised form 2 June 2004; accepted 21 June 2006
Available online 6 June 2007

Abstract
In this paper, we give a characterization of a group $G$ which contains a semiregular relative difference set $R$ relative to a central subgroup $N$ containing the commutator subgroup $[G, G]$ of $G$ such that $1 \in R$ and $rRr^{-1} = R$ for all $r \in R$. In particular, these relative difference sets are fixed by inversion and inner automorphisms of the group are multipliers. We also present a construction of such relative difference sets.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Relative difference set; Orthogonal cocycle; Special $p$-group; Generalized Hadamard matrix

1. Introduction

Let $G$ be a finite group. A subset $R \subset G$ is called a relative difference set relative to a subgroup $N < G$ if there exists a constant $\lambda$ such that

(i) for every element $g \in G \setminus N$, there are exactly $\lambda$ pairs of elements $r_1, r_2 \in R$ such that $g = r_1r_2^{-1}$;

(ii) for every $g \in N \setminus \{1\}$, there exist no elements $r_1, r_2 \in R$ such that $g = r_1r_2^{-1}$.

A relative difference set $R$ is said to be fixed by inversion, or reversible when $G$ is abelian, if $R = R^{-1} := \{r^{-1} | r \in R\}$. In the case where $N$ has order $n$, $G$ has order $mn$, and $R$ has size $k$, the relative difference set $R$ is called an $(m, n, k, \lambda)$-relative difference set. If $k = m$, the relative difference set is said to be semiregular. The subgroup $N$ is called forbidden subgroup. An $(m, n, k, \lambda)$-relative difference set in a group $G$ gives rise to an $(m, n, k, \lambda)$-divisible design on which the group $G$ acts regularly and transitively. The forbidden subgroup is the stabiliser of a point class of the design. An automorphism $\alpha \in \text{Aut}(G)$ of the group $G$ is called a multiplier of the relative difference set $R$ contained in $G$ if there is an element $g_2 \in G$ such that

$$\alpha(R) := \{\alpha(r) | r \in R\} = \{g_2r | r \in R\}.$$ Multipliers induce automorphisms of the divisible design obtained from the relative difference set.

\textsuperscript{1} Parts of this work are contained in the third author’s Ph.D thesis, taken under the supervision of the first two authors.

E-mail addresses: yuqing.chen@wright.edu (Y.Q. Chen), horadam@rmit.edu.au (K.J. Horadam), weihung_liu@hotmail.com (W.-H. Liu).
Let $G$ be a finite group and $\mathbb{Z}[G]$ the integral group ring of $G$. For a subset $S \subset G$, we identify it with the group ring element
\[
\sum_{g \in S} g \in \mathbb{Z}[G]
\]
and denote it again by $S$. For an element
\[
a = \sum_{g \in G} a_g g \in \mathbb{Z}[G],
\]
we define
\[
a^{(t)} = \sum_{g \in G} a_g g^t \in \mathbb{Z}[G]
\]
for any integer $t \in \mathbb{Z}$. With these group ring notations, a subset $R$ of $G$ is an $(m, n, k, \lambda)$-relative difference set in $G$ relative to a subgroup $N$ of $G$ if and only if
\[
RR^{(-1)} = k + \lambda(G - N)
\]
and $R$ is fixed by inversion if and only if $R = R^{(-1)}$. An automorphism $\alpha \in \text{Aut}(G)$ is a multiplier if and only if $\alpha(R) = g_2 R$ for some $g_2 \in G$.

Relative difference sets fixed by inversion have been investigated by Arasu et al. [1], Leung and Ma [7] and Ma [9]. In the first paper of this sequence [4], we discovered a $(30_2, 29, 14)$-relative difference set fixed by inversion in the alternating group $A_5$ and established connection between relative difference sets fixed by inversion and distance regular graphs, while in the second one [3], we constructed a family of reversible relative difference sets with forbidden subgroup $N \cong \mathbb{Z}_4$ and strengthened the results in [9]. In this paper, we continue our investigation of these relative difference sets using the theory of orthogonal cocycles developed in [11].

Let $H$ be a finite group (written multiplicatively) and $N$ a finite abelian group (written additively). Let $\psi : H \times H \rightarrow N$ be a map. Then the set $N \times H$ equipped with the binary operation
\[
(x_1, y_1) \cdot (x_2, y_2) = (x_1 + x_2 + \psi(y_1, y_2), y_1 y_2)
\]
for all $(x_1, y_1), (x_2, y_2) \in N \times H$ forms a group, which we denote by $E(N, H, \psi)$, if and only if the map $\psi$ satisfies
\[
\psi(y_1, y_2) + \psi(y_1 y_2, y_3) = \psi(y_1, y_2 y_3) + \psi(y_2, y_3) \quad \text{for all } y_1, y_2, y_3 \in H.
\]
A map satisfying (1) is called a 2-cocycle of $H$ with coefficients in $N$ (see [2]). Since we are not interested in cocycles in any other dimensions, we will simply call these maps cocycles. If $\psi$ is a cocycle, then the group $N$ can be embedded in the center of $E(N, H, \psi)$ by
\[
i : N \rightarrow E(N, H, \psi),
i(x) = (x, 1) \quad \text{for all } x \in N.
\]
On the other hand, if an abelian $N$ can be embedded into the center of a given group $G$ via an embedding $i : N \rightarrow G$ and $G / i(N) \cong H$, then any transversal function $\tau : H \rightarrow G$ (so that $\pi \circ \tau = 1_H$, where $\pi : G \rightarrow H$ is the natural projection) gives rise to a cocycle
\[
\psi_{\tau} : H \times H \rightarrow N,
\]
\[
\psi_{\tau}(g, h) = i^{-1}(\tau(g)\tau(h)\tau(gh)^{-1}).
\]
and the group $G$ is isomorphic to $E(N, H, \psi_{\tau})$. The simplest cocycles of $H$ with coefficients in $N$ are given as follows. Let $\phi : H \rightarrow N$ be a map. Then the map
\[
\hat{\phi} : H \times H \rightarrow N,
\]
\[
\hat{\phi}(g, h) = \phi(g) + \phi(h) - \phi(gh)
\]
is a cocycle. A cocycle of this form is called a coboundary. For instance, if \( \tau_1 \) and \( \tau_2 \) are two transversal functions from \( H = G/i(N) \) to \( G \), where \( i(N) \) is contained in the center of \( G \), then the difference between \( \psi_{\tau_1} \) and \( \psi_{\tau_2} \) is a coboundary, that is the cocycle

\[
\psi_{\tau_1} - \psi_{\tau_2} : H \times H \to N,
\]

\[
(\psi_{\tau_1} - \psi_{\tau_2})(g, h) = \psi_{\tau_1}(g, h) - \psi_{\tau_2}(g, h)
\]

is a coboundary. The structures of the groups obtained from these simple cocycles are also quite simple. In fact, the group \( E(N, H, \psi) \) is isomorphic to \( N \times H \) if and only if \( \psi \) is a coboundary. More generally, if two cocycles \( \psi_1 \) and \( \psi_2 \) differ by a coboundary, then \( E(N, H, \psi_1) \cong E(N, H, \psi_2) \). Hence we may normalise a cocycle \( \psi \) by replacing it with \( \psi - \psi(1, 1) \). In the remainder of this paper, all cocycles \( \psi : H \times H \to N \) and transversal functions \( \tau : H \to G \) are normalised, that is \( \psi(1, 1) = 0 \) and \( \tau(1) = 1 \). From (1), all cocycles \( \psi \) considered here satisfy

\[
\psi(1, h) = \psi(h, 1) = \psi(1, 1) = 0 \quad \text{for all } h \in H.
\]

When \( \psi \) is a cocycle of \( H \) with coefficients in \( N \), we define its transpose \( \psi^T \) to be

\[
\psi^T : H \times H \to N,
\]

\[
\psi^T(g, h) = \psi(h, g) \quad \text{for all } g, h \in H.
\]

Note that \( \psi^T \) is usually not a cocycle. However, if \( H \) is abelian, then \( \psi^T \) is also a cocycle if \( \psi \) is. A cocycle \( \psi \) is said to be symmetric if \( \psi = \psi^T \) and skew symmetric if \( \psi + \psi^T = 0 \) and \( \psi(x, x) = 0 \) for all \( x \in H \). Note that when \( |N| \) is odd, condition \( \psi + \psi^T = 0 \) implies \( \psi(x, x) = 0 \). The following lemma is easy to verify.

**Lemma 1.1.** The group \( E(N, H, \psi) \) is abelian if and only if \( H \) is abelian and \( \psi \) is symmetric.

Let \( H \) be a group of order \( m \) and \( N \) an abelian group of order \( n \) such that \( n|m \). A cocycle \( \psi : H \times H \to N \) is said to be orthogonal if, for each \( h \in H \setminus \{1\} \) and each \( x \in N \), the number of elements \( g \in H \) such that \( \psi(h, g) = x \) is \( m/n \). This is equivalent to

\[
\sum_{g \in H} \psi(h, g) = \frac{m}{n} N \in \mathbb{Z}[N]
\]

for all \( h \in H \setminus \{1\} \). The following theorem of [11] shows that orthogonal cocycles are essentially semiregular relative difference sets.

**Theorem 1.2** (Perera and Horadam [11]). Let \( G \) be a finite group of order \( mn \) and \( N \) a subgroup of order \( n \) of \( G \) such that \( N \) is contained in the center \( Z(G) \) of \( G \). Let \( \tau : G/N \to G \) be a transversal function. Then the following statements are equivalent,

1. the set \( R = \{\tau(x)|x \in G/N\} \) is an \((m, n, m, m/n)\)-relative difference set in \( G \) relative to \( N \),
2. the cocycle \( \psi_\tau \) of \( G/N \) with coefficients in \( N \) is orthogonal.

Theorem 1.2 has been used in construction of new semiregular relative difference sets in certain non-abelian groups [6]. The main results of this paper are:

**Theorem 1.3.** Let \( G \) be a finite group such that \( [G, G] \leq Z(G) \), where \( [G, G] \) is the commutator subgroup of \( G \) and \( Z(G) \) is the center of \( G \). Let \( N \) be a subgroup of \( G \) such that \( [G, G] \leq N \leq Z(G) \) and \( |N| \) divides \( |G/N| \). The group \( G \) contains a semiregular relative difference set \( R \) relative to \( N \) such that \( 1 \in R \) and \( rRr = R \) for all \( r \in R \) if and only if \( G \) is either an elementary abelian 2-group with \( |N|^3 \leq |G| \) and \( |G/N| \) a perfect square, or a special \( p \)-group of exponent \( p \) with \( |Z(G)| + |G/Z(G)| - 1 \) conjugacy classes for some odd prime \( p \).

Furthermore, if \( |G| \) is odd and \( R_1 \) and \( R_2 \) are two such relative difference sets in \( G \) relative to \( N \), then there is a homomorphism \( \delta : G \to N \) with \( N \leq \ker(\delta) \) such that \( R_1 = \{\delta(r)r|r \in R_2\} \).
**Remark.** If $R$ is a such relative difference set and $r \in R$, then $r^2 = r \cdot 1 \cdot r \in R$. Inductively, we can see that $r^n \in R$ for all integers $n$ and all $r \in R$. Hence these relative difference sets are necessarily fixed by inversion. Also, it is clear that when $G$ is non-abelian, all inner automorphisms of $G$ are multipliers of $R$. It should be noted that the conditions $1 \in R$ and $rr = r$ for all $r \in R$ are much stronger than $R = R^{(-1)}$. There are examples of relative difference sets fixed by inversion in [4,3,7] which do not have these properties.

**Theorem 1.4.** Let $p$ be a prime. For any positive integers $n \leq m$, there exists a $(p^n, p^m, p^{m-n})$-relative difference set $R$ in a group $G$ described in Theorem 1.3 if and only if $m$ is even and $2n \leq m$.

The rest of the paper is organized as follows. In Section 2, we discuss multiplicative cocycles and skew symmetric cocycles. The connection between orthogonal cocycles and generalized Hadamard matrices is also discussed. The proofs of Theorems 1.3 and 1.4 are presented in Section 3.

2. Multiplicative cocycles and skew symmetric cocycles

Let $H$ be a finite group and $N$ a finite abelian group. A cocycle $\psi$ of $H$ with coefficients in $N$ is called a multiplicative cocycle if for every $h \in H$, the maps $\psi(h, \cdot) : H \to N$ and $\psi(\cdot, h) : H \to N$ are group homomorphisms. That is for every $x, y, z \in H$, one has

\[
\psi(x, yz) = \psi(x, y) + \psi(x, z), \\
\psi(xy, z) = \psi(x, z) + \psi(y, z).
\]

By the definition of orthogonal cocycle, it is easy to see that:

**Lemma 2.1.** A multiplicative cocycle $\psi$ of $H$ with coefficients in $N$ is orthogonal if and only if for every $h \in H \setminus \{1\}$, the map $\psi(h, \cdot) : H \to N$ is onto.

Therefore it is relatively easy to obtain orthogonal cocycles from multiplicative ones, and hence semiregular relative difference sets by Theorem 1.2. However, there are only very restricted families of groups of $H$ and $N$ that provide multiplicative orthogonal cocycles.

**Lemma 2.2.** If $\psi : H \times H \to N$ is a multiplicative orthogonal cocycle, then $H$ and $N$ are elementary abelian $p$-groups for some prime $p$.

**Proof.** We only need to show that $H$ is an elementary abelian $p$-group as $N$ is a homomorphic image of $H$. Note that if $f : N \to N'$ is a surjective homomorphism from $N$ to another abelian group $N'$, then $f \circ \psi$ is a multiplicative orthogonal cocycle with coefficients in $N'$ whenever $\psi$ is a multiplicative orthogonal cocycle. Hence, we may assume that $N \cong \mathbb{Z}/p\mathbb{Z}$ for some prime $p$. Now if $H$ is not elementary abelian, then there is an element $x \neq 1$ such that $x \in [H, H]$ or $x = y^p$ in $H$ for some $y \in H$. Clearly $x$ lies in the kernel of all homomorphisms $\psi(\cdot, h) : H \to N$ as $N \cong \mathbb{Z}/p\mathbb{Z}$, and this contradicts the fact that $\psi$ is orthogonal. □

We now take a close look at these multiplicative orthogonal cocycles. Let $H$ and $N$ be two elementary abelian $p$-groups, where $p$ is a prime. Suppose $|H| = p^m$ and $|N| = p^n$. Then $H$ and $N$ can be viewed as $m$ and $n$ dimensional vector spaces over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, respectively, that is we can assume

\[
H = \{ (x_1, x_2, \ldots, x_m) | x_i \in \mathbb{F}_p, \quad i = 1, 2, \ldots, m \}
\]

and

\[
N = \{ (x_1, x_2, \ldots, x_n) | x_i \in \mathbb{F}_p, \quad i = 1, 2, \ldots, n \}.
\]

If $\psi$ is a multiplicative cocycle of $H$ with coefficients in $N$, then there are $n$ multiplicative cocycles $\psi_1, \psi_2, \ldots, \psi_n$ of $H$ with coefficients in $\mathbb{F}_p$ such that

\[
\psi(x, y) = (\psi_1(x, y), \psi_2(x, y), \ldots, \psi_n(x, y)).
\]
for all \( x, y \in H \). It is clear that each \( \psi_i \) is simply a bilinear form over \( \mathbb{F}_p \), and there is an \( m \times m \) matrix \( M_i \) over \( \mathbb{F}_p \), such that
\[
\psi_i(x, y) = x M_i y^\top
\]
for all \( x, y \in H \) and \( i = 1, 2, \ldots, n \).

**Lemma 2.3.** \( \psi \) is a multiplicative orthogonal cocycle of \( H \) with coefficients in \( N \) if and only if for any \((z_1, z_2, \ldots, z_n) \neq 0\) in \( N \), the matrix
\[
\sum_{k=1}^{n} z_k M_k
\]
is a non-singular matrix.

**Proof.** Since \((z_1, z_2, \ldots, z_n) \neq 0\), the \( \mathbb{F}_p \) linear map
\[
(z_1, z_2, \ldots, z_n) : N \rightarrow \mathbb{Z}/p\mathbb{Z},
\]
\[
(z_1, z_2, \ldots, z_n)((x_1, x_2, \ldots, x_n)) = \sum_{k=1}^{n} z_k x_k
\]
is surjective. Hence
\[
\sum_{k=1}^{n} z_k \psi_k = (z_1, z_2, \ldots, z_n) \circ \psi
\]
is a multiplicative orthogonal cocycle of \( H \) with coefficients in the finite field \( \mathbb{F}_p \), and, by Lemma 2.1, the matrix \( \sum_{k=1}^{n} z_k M_k \) is non-singular.

Conversely, let \( x \in H \) be a non-zero vector and define
\[
M = \begin{pmatrix} x M_1 \\ x M_2 \\ \vdots \\ x M_n \end{pmatrix}.
\]
The matrix \( M \) is an \( n \times m \) matrix. For any non-zero vector \( z = (z_1, z_2, \ldots, z_n) \in N \), one has
\[
z M = \sum_{k=1}^{n} z_k (x M_k) = x \left( \sum_{k=1}^{n} z_k M_k \right) \neq 0
\]
since \( x \neq 0 \) and \( \sum_{k=1}^{n} z_k M_k \) is non-singular. Therefore \( M \) has rank \( n \) and the linear map
\[
M : H \rightarrow N,
\]
\[
M y^\top = (x M_1 y^\top, x M_2 y^\top, \ldots, x M_n y^\top) = \psi(x, y)
\]
is surjective. By Lemma 2.1, \( \psi \) is orthogonal. \( \square \)

**Remark.** A similar version of Lemma 2.3 is proved in [10].

We now turn our attention to skew symmetric cocycles. Recall that a cocycle of \( H \) with coefficients in \( N \) is skew symmetric if \( \psi + \psi^\top = 0 \) and \( \psi(x, x) = 0 \) for all \( x \in H \).

**Lemma 2.4.** If \( \psi + \psi^\top = 0 \), then \( 2\psi \) is a multiplicative skew-symmetric cocycle. In particular, if \( |N| \) is odd, then skew symmetric cocycles are multiplicative.
**Proof.** Let \( \psi \) be a cocycle of \( H \) with coefficients in \( N \) satisfying \( \psi + \psi^T = 0 \). Then clearly \( 2\psi \) is a skew symmetric cocycle. From Eq. (1), one has

\[
0 = \psi(g, h) + \psi(gh, k) - \psi(h, k) - \psi(g, hk)
= \psi(g, h) + 2\psi(gh, k) + \psi(k, gh) + \psi(k, h) + \psi(hk, g)
= 2\psi(gh, k) + \psi(k, g) + \psi(kg, h) + \psi(k, h) + \psi(hk, g)
= 2\psi(gk, h) + \psi(k, g) + \psi(gh, k) + \psi(hk, g) + \psi(h, k) - \psi(h, k)
= 2(\psi(gk, h) + \psi(k, g) + \psi(kg, h) + \psi(k, h) + \psi(gh, k))
\]

for all \( g, h, k \in H \).

Therefore \( 2\psi(gk, h) = 2\psi(kg, h) + 2\psi(h, k) \) for all \( g, h, k \in H \). A similar argument shows that \( 2\psi(gk, h) = 2\psi(kg, h) + 2\psi(h, k) \) for all \( g, h, k \in H \) and \( 2\psi \) is multiplicative. If \( |N| \) is odd, then \( \psi = \frac{1}{2}(2\psi) \) is also multiplicative. \( \square \)

Recall that an \( m \times m \) matrix \( M \) over any field \( \mathbb{F} \) is said to be skew-symmetric if \( xMx^T = 0 \) for any vector \( x \in \mathbb{F}^m \). If such a matrix is non-singular, then \( m \) must be even. From Lemma 2.3 and the definition of a skew-symmetric cocycle, we can see that the existence of a skew-symmetric orthogonal multiplicative cocycle of \( H = \mathbb{F}_p^m \) with coefficients in \( N = \mathbb{F}_p^n \) is equivalent to the existence of \( m \times m \) skew-symmetric matrices \( M_1, M_2, \ldots, M_n \) over the finite field \( \mathbb{F}_p \) such that

\[
\sum_{i=1}^n x_i M_i
\]

is non-singular for all \( 0 \neq (x_1, x_2, \ldots, x_n) \in \mathbb{F}_p^n \). The following result is due to MacDonald [10].

**Lemma 2.5 (MacDonald [10, Theorem 3.2]).** If \( \psi \) is a multiplicative skew-symmetric orthogonal cocycle of \( H = \mathbb{F}_p^m \) with coefficients in \( N = \mathbb{F}_p^n \), then \( m \) is even and \( 2n \leq m \).

Before we prove Theorems 1.3 and 1.4, we want to discuss the connection between orthogonal cocycles and generalized Hadamard matrices. An \( n \times n \) matrix \( M = [m_{ij}]_{n \times n} \) with entries in a finite group \( G \) is called a generalized Hadamard matrix if

\[
\sum_{k=1}^n m_{ik}m_{jk}^{-1} = \lambda G \in \mathbb{Z}[G]
\]

for some positive integer \( \lambda \) and for all \( i \neq j \). When \( |G| = 2 \), these matrices are precisely Hadamard matrices. Generalized Hadamard matrices and their applications have been studied by many authors, and were an early interest of Jennie Seberry [12–14]. When \( G \) is abelian, we call a generalized Hadamard matrix \( M = [m_{ij}]_{n \times n} \) skew symmetric if \( m_{ij} + m_{ji} \geq 0 \) and \( m_{ij} = 0 \) in \( G \). Cocycles provide a natural source in finding generalized Hadamard matrices since each cocycle \( \psi \) of a group \( H \) with coefficients in a group \( N \) can be displayed as a \( |H| \times |H| \) matrix \( M = [\psi(g, h)]_{(g, h) \in H \times H^*} \), whose rows and columns are labelled by the elements in the group \( H \). According to [11], such a matrix is a generalized Hadamard matrix if and only if the cocycle is orthogonal. By Theorem 1.4, we have

**Proposition 2.6.** For any odd prime \( p \) and any two positive integers \( b \leq a \), there exist \( p^{2a} \times p^{2a} \) skew symmetric generalized Hadamard matrices over \( (\mathbb{Z}/p\mathbb{Z})^b \).

More interestingly, if the relative difference set obtained from \( \psi \) is fixed by inversion, then we can produce a skew symmetric generalized Hadamard matrix from \( \psi \) by reversing the labelling of its rows or columns.

**Proposition 2.7.** If there exists an \( (m, n, m, m/n) \)-relative difference set fixed by inversion in a group \( G \) relative to a subgroup \( N \) of \( G \) which is contained in the center of \( G \), then there exists an \( m \times m \) skew symmetric generalized Hadamard matrix with entries in \( N \).

**Proof.** Let \( R \) be a central \( (m, n, m, m/n) \)-relative difference set fixed by inversion in \( G \) relative to \( N \) and let \( H = G/N \). By Theorem 1.2, the cocycle \( \psi_\tau \) of \( H \) with coefficients in \( N \) is orthogonal, where \( \tau \) is the transversal function corresponding
to \( R \). Since \( R = \{ \tau(x) | x \in H \} \) and \( R^{-1} = \{ (-\psi_{\tau}(x, x^{-1})) \tau(x^{-1}) | x \in H \} = R \), one has \( \psi_{\tau}(x, x^{-1}) = 0 \) for all \( x \in H \).

From (1), one has
\[
\begin{align*}
\psi_{\tau}(g, h^{-1}) + \psi_{\tau}(gh^{-1}, h) &= \psi_{\tau}(g, 1) + \psi_{\tau}(h, h^{-1}), \\
\psi_{\tau}(gh^{-1}, h) + \psi_{\tau}(g, g^{-1}) &= \psi_{\tau}(gh^{-1}, (gh^{-1})^{-1}) + \psi_{\tau}(g, g^{-1})
\end{align*}
\]
for all \( g, h \in H \). Hence \( \psi_{\tau}(g, h^{-1}) + \psi_{\tau}(h, g^{-1}) = 0 \) for all \( g, h \in H \) and the matrix \( M = [\psi_{\tau}(g, h)]_{(g, h^{-1}) \in H \times H} \) is a skew symmetric generalized Hadamard matrix.  

**3. Proof of Theorems 1.3 and 1.4**

We first recall some basic knowledge concerning special \( p \)-groups. See [15] for details. Let \( G \) be a group. An element \( g \in G \) is said to be a non-generator of \( G \) if for any subset \( X \) of \( G \), the group \( G = \langle X \rangle \) whenever \( G = \langle g, X \rangle \). The set of non-generators of \( G \) forms a subgroup, called the Frattini subgroup, of \( G \) and is denoted by \( \Phi(G) \). It is the intersection of all proper maximum subgroups of \( G \). A finite \( p \)-group \( G \) is called a special \( p \)-group if
\[
Z(G) = \Phi(G) = [G, G].
\]

The Frattini subgroup of a finite \( p \)-group \( G \) can be characterized as the smallest normal subgroup \( N \) of \( G \) such that \( G/N \) is an elementary abelian \( p \)-group. In the case of special \( p \)-groups, the Frattini subgroups are always elementary abelian \( p \)-groups.

Before we prove the main results of this paper, we need the following lemmas for preparation.

**3.1. Caution of notations**

In this section, any central subgroup \( N \) of a group \( G \) is understood to be embedded in \( G \), i.e. there is an embedding \( i : N \to G \). We will continue to use additive notations for \( N \) and cocycles with coefficients in \( N \) and multiplicative notations for \( G \) and \( G/N \) without mentioning the embedding \( i \) and its inverse \( i^{-1} \).

In the first lemma, we define a cocycle \( \gamma_{\tau}^{G} \) which plays an important role in the subsequent lemmas.

**Lemma 3.1.** Let \( G \) be a finite group and \( N \) a subgroup of \( G \) such that \([G, G] \leq N \leq Z(G)\). Let \( \tau : G/N \to G \) be a transversal function. Then
\[
\gamma_{\tau}^{G} : G/N \times G/N \to N,
\]
\[
\gamma_{\tau}^{G}(x, y) = \tau(x)\tau(y)\tau(x)^{-1}\tau(y)^{-1}
\]
is a skew symmetric multiplicative cocycle of \( G/N \) with coefficients in \( N \). Furthermore, for any transversal function \( \tau' : G/N \to G \), \( \gamma_{\tau'}^{G} = \psi_{\tau'} - \psi_{\tau'}^{T}. \)

**Proof.** Clearly, \( \gamma_{\tau}^{G} = \psi_{\tau} - \psi_{\tau}^{T} \) and therefore \( \gamma_{\tau}^{G} \) is a skew symmetric cocycle. For any \( x, y, z \in G/N \),
\[
\gamma_{\tau}^{G}(x, yz) = \tau(x)\tau(yz)\tau(x)^{-1}\tau(yz)^{-1}
\]
\[
= \tau(x)(-\psi_{\tau}(y, z))\tau(y)\tau(z)\tau(x)^{-1}\tau(z)^{-1}\tau(y)^{-1}\psi_{\tau}(y, z)
\]
\[
= \tau(x)\tau(y)\tau(z)\tau(x)^{-1}\tau(z)^{-1}\tau(y)^{-1}
\]
\[
= \tau(x)\tau(y)(\tau(x)\tau(z)\tau(x)^{-1}\tau(z)^{-1}\tau(y)^{-1})
\]
\[
= \gamma_{\tau}^{G}(x, y) + \gamma_{\tau}^{G}(x, z).
\]
Similarly,
\[
\gamma_{\tau}^{G}(xy, z) = \gamma_{\tau}^{G}(x, z) + \gamma_{\tau}^{G}(y, z)
\]
for all \( x, y, z \in G/N \) and \( \gamma_{\tau}^{G} \) is multiplicative. Finally, we know that \( \psi_{\tau} - \psi_{\tau'} \) is a coboundary. Therefore \( (\psi_{\tau} - \psi_{\tau'}) - (\psi_{\tau} - \psi_{\tau'})^{T} = 0 \) and \( \gamma_{\tau}^{G} = \psi_{\tau'} - \psi_{\tau'}^{T} \).  \( \square \)
The next lemma shows that in the case of special $p$-groups, the orthogonality of $\gamma_N^G$ is related to the number of conjugacy classes in $G$.

**Lemma 3.2.** A special $p$-group $G$ has at least $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes. It has exactly $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes if and only if the cocycle $\gamma_N^G$ is orthogonal.

**Proof.** Let $\pi : G \to G/Z(G)$ be the natural projection from $G$ to $G/Z(G)$ and $\gamma_N^G$ the cocycle defined in Lemma 3.1. For any element $g \in G$, if another element $g' \in G$ is conjugate to $g$, then $g' = g$ when $g \in Z(G)$, or $g' = hgh^{-1} = (hgh^{-1}g^{-1})g = \gamma_N^G(g, h, g)g \in Z(G)g$ for some $h \in G \setminus C(g)$, where $C(g)$ is the centralizer of $g$ in $G$, when $g \notin Z(G)$. Therefore $G$ has at least $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes.

If $G$ has exactly $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes, then the coset $Z(G)g$ must be the conjugacy class of $G$ containing $g$ for every $g \notin Z(G)$. Hence the centralizer of $g$ has size $|C(g)| = |G|/|Z(G)|$, while the kernel of the linear map $$\gamma_N^G : G/Z(G) \to Z(G)$$

must have size $|\operatorname{Ker}(\gamma_N^G)| = |G|/|Z(G)|^2$. Consequently the size of the image of $\gamma_N^G$ is $|Z(G)|$.

This shows that $\gamma_N^G$ is surjective for all $x \neq 1$ in $G/Z(G)$. By Lemma 2.1, $\gamma_N^G$ is orthogonal.

Conversely, by Lemma 2.1, the coset $Z(G)g$ forms a conjugacy class containing $g$ for every $g \in G \setminus Z(G)$. Therefore $G$ has $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes. \[\square\]

**Remark.** Special $p$-groups $G$ with exactly $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes are studied in [10]. They are $p$-groups of Frobenius type.

The next lemma characterizes all special $p$-groups of which the group extensions by their centers are given by the cocycles $\gamma_N^G$. We say that a cocycle $\psi$ is non-degenerated if $\psi(x, y) = 0$ for all $y$ implies $x = 1$ and $\psi(x, y) = 0$ for all $x$ implies $y = 1$.

**Lemma 3.3.** Let $p$ be an odd prime and $G$ a $p$-group such that $\Phi(G)$ is an elementary abelian $p$-group and $\Phi(G) \leq Z(G)$. The group $G$ is a special $p$-group of exponent $p$ if and only if there is an elementary abelian subgroup $N$ of $G$ such that $\Phi(G) \leq N \leq Z(G)$ and a transversal function $\tau : G/N \to G$ such that the cocycle $\psi_{/\tau}$ is skew symmetric, non-degenerated and onto.

**Proof.** If $\psi_{/\tau}$ is skew symmetric, and hence multiplicative by Lemma 2.4 as $p$ is odd, one has $\psi_{/\tau}(x, x^k) = k \psi_{/\tau}(x, x) = 0$ for all $x \in G/N$ and all integers $k$. By induction, we have $\tau(x) = \tau(x^p)$ and $(\tau(x))^p = \tau(x^p) = 1$ for all $x \in G/N$. Since every element in $G$ is the product of an element in the subgroup $N$ of $G$ and an element $\tau(x)$ for some $x \in G/N$ and the exponent of $N$ is $p$, the exponent of $G$ must be $p$. By Lemma 3.1, $\gamma_N^G = 2\psi_{/\tau}$ is non-degenerated and onto. The non-degeneracy of $\gamma_N^G$ implies $N = Z(G)$ while surjectivity of $\gamma_N^G$ implies $N = [G, G]$. Therefore, $Z(G) = \Phi(G) = [G, G]$ and $G$ is a special $p$-group.

Conversely, suppose $G$ is a special $p$-group of exponent $p$. Let $N = Z(G)$ and $\tau' : G/N \to G$ be a transversal function. Then for any $x \in G/N$, the fact that $\tau'(x)^p = 1$ is equivalent to

$$\sum_{k=1}^{p-1} \psi_{/\tau'}(x, x^k) = \sum_{k=1}^{p-1} \psi_{/\tau'}(x^k, x) = 0.$$ 

Since $p$ is odd, we can define

$$\phi = \frac{1}{2} (\psi_{/\tau'} + \psi_{/\tau'})^T.$$ 

Clearly, $\phi$ is a cocycle as $G/N$ is abelian and also has the property that

$$\sum_{k=1}^{p-1} \phi(x, x^k) = \sum_{k=1}^{p-1} \phi(x^k, x) = 0.$$
This ensures that the group $E(N, G/N, \phi)$ has exponent $p$. Furthermore, $\phi$ is symmetric, which, by Lemma 1.1 ensures that the group $E(N, G/N, \phi)$ is abelian. This implies that $E(N, G/N, \phi)$ is elementary abelian and $E(N, G/N, \phi) \cong N \times (G/N)$. Therefore $\phi$ is a cocycle and there is a map $\delta : (G/N) \rightarrow N$ such that $\phi(x, y) = \delta(x) + \delta(y) - \delta(xy)$.

Now we define a transversal function

$$\tau : G/N \rightarrow N,$$

$$\tau(x) = \tau'(x)\delta(x)^{-1}.$$  

The cocycle

$$\psi_\tau = \psi_\tau' - \phi = \frac{1}{2}(\psi_\tau' - \psi_\tau'^\top) = \frac{1}{2}g^G_N$$

is skew symmetric. By Lemma 3.1, the fact that $N = Z(G)$ is equivalent to the non-degeneracy of $g^G_N = 2\psi_\tau$, and hence, of $\psi_\tau$, while $N = [G, G]$ is equivalent to the surjectivity of $g^G_N = 2\psi_\tau$ and of $\psi_\tau$. □

**Remark.** All skew symmetric orthogonal cocycles are non-degenerated and onto.

**Lemma 3.4.** Let $G$ be a finite group such that $[G, G] \trianglelefteq Z(G)$ and $N$ a subgroup of $G$ such that $[G, G] \trianglelefteq N \trianglelefteq Z(G)$. If $G$ contains a semiregular relative difference set $R$ relative to $N$ such that $1 \in R$ and $rRr = R$ for all $r \in R$, then the cocycle $\psi_\tau$ of the transversal function $\tau : G/N \rightarrow G$ obtained from $R$ such that $R = \{\tau(x) | x \in G/N\}$ is a skew symmetric orthogonal cocycle and

$$\psi_\tau(x, y) + \psi_\tau(xy, x) = 0$$

for all $x, y \in G/N$.

**Proof.** By Theorem 1.2, $\psi_\tau$ is orthogonal. Since $1 \in R$ and $rRr = R$ for all $r \in R$, one has $r^2 = r \cdot 1 \cdot r \in R$. Hence $\tau(x)^2 = \psi_\tau(x, x)\tau(x^2) \in R$. Since $R$ is a transversal of $G$ with respect to $N$, we have $\tau(x)^2 = \tau(x^2)$ and $\psi_\tau(x, x) = 0$ for all $x \in G/N$. From $rRr = R$ for all $r \in R$, we have

$$\tau(x)\tau(y)\tau(x) = \psi_\tau(x, y)\tau(xy)\tau(x)$$

$$= (\psi_\tau(x, y) + \psi_\tau(xy, x))\tau(xyx) \in R$$

for all $x, y \in G/N$.

Because $R$ is a transversal of $G$ with respect to $N$, we get

$$\psi_\tau(x, y) + \psi_\tau(xy, x) = 0$$

for all $x, y \in G/N$.

Also, for any $x, y \in G/N$, we have $\tau(y)^2 \in R$ and $\tau(x)\tau(y)^2\tau(x) \in R$. Now

$$\tau(x)\tau(y)^2\tau(x) = (\tau(x)\tau(y))\tau(y)\tau(x)$$

$$= (\psi_\tau(x, y)\tau(xy))(\psi_\tau(y, x)\tau(xy))$$

$$= (\psi_\tau(x, y) + \psi_\tau(y, x))\tau(xy)^2.$$

Since $\tau(xy)^2 \in R$, one has $\psi_\tau(x, y) + \psi_\tau(y, x) = 0$ and hence $\psi_\tau$ is skew symmetric.

We now prove Theorem 1.3. □

**Proof of Theorem 1.3.** Let $G$ be a finite group such that $[G, G] \trianglelefteq Z(G)$ and $N$ a subgroup of $G$ such that $[G, G] \trianglelefteq N \trianglelefteq Z(G)$. Suppose that $G$ contains a relative difference set $R$ relative to $N$ such that $1 \in R$ and $rRr = R$ for all $r \in R$.

Then, by Lemma 3.4, the cocycle $\psi_\tau$ is skew symmetric orthogonal, where $\tau : G/N \rightarrow G$ is the transversal function such that $R = \{\tau(x) | x \in G/N\}$. We define a homomorphism

$$d : N \rightarrow N,$$

$$d(x) = 2x$$

for all $x \in N$.

Let $K = \text{Im}(d)$ be the image of $d$. Then $K$ is a subgroup of $N$ and the homomorphism $d : N \rightarrow K$ is surjective. Hence $d \circ \psi_\tau$ is a skew symmetric orthogonal cocycle of $G/N$ with coefficients in $K$. We now divide the proof into two cases.
Case I: \( K \neq \{0\} \). Since \( d \circ \psi_r = 2\psi_r \) and \( \psi_r \) is skew symmetric, by Lemmas 2.4 and 2.1, \( d \circ \psi_r \) is a multiplicative orthogonal cocycle. By Lemma 2.2, both \( G/N \) and \( K \) are elementary abelian \( p \)-groups for some prime \( p \). Since \( |N| \) divides \( |G/N| \), the group \( G \) is a \( p \)-group and \( |G| \leq \Phi(G) \leq N \leq Z(G) \). We want to show that \( p \) is odd. Suppose to the contrary, Then \( p = 2 \) and, by Lemma 3.4, \( \tau(x)^2 = \psi_r(x, x) = 1 \). This shows that the set \( R \) consists entirely of elements of order 2 and the identity of \( G \). From Lemma 3.4 (3), we get

\[
\tau(x)\tau(y)\tau(x) = \tau(xy) = \tau(y) \quad \text{for all } x, y \in G/N,
\]
or equivalently,

\[
\tau(x)\tau(y) = \tau(y)\tau(x) \quad \text{for all } x, y \in G/N.
\]

This implies that \( \psi_r(x, y) = \psi_r(y, x) \) for all \( x, y \in G/N \). Therefore the cocycle \( \psi_r \) is both symmetric and skew symmetric. Hence \( 2\psi_r = 0 \). This contradicts the fact that \( d \circ \psi_r \) is orthogonal, and therefore, \( p \) must be odd. It follows immediately that \( |N| \) is odd and \( K = N \). By Lemmas 3.1 and 3.4, \( \gamma^G_N = \psi_r - \psi^2_r = 2\psi_r \) is orthogonal. By Lemmas 3.2 and 3.3, the group \( G \) is a special \( p \)-group of exponent \( p \) with \( |Z(G)| + |G/Z(G)| - 1 \) conjugacy classes.

Case II \( K = \{0\} \). In this case, \( N \) is an elementary abelian 2-group. Hence the cocycle \( \psi_r \) is symmetric as it is skew symmetric. By Lemma 1.1, the group \( G \) is abelian. From the results of [9], we have \( |N|^3 \leq |G/N| \leq |G/N| \) a perfect square and \( G \cong N \times G/N \). Therefore \( \psi_r \) is a coboundary, i.e. there is a map \( \phi : G/N \to N \) with \( \phi(1) = 0 \) such that \( \psi_r(x, y) = \phi(x) + \phi(y) - \phi(xy) \) for all \( x, y \in G/N \). By Lemma 3.4 (3), one has

\[
\phi(x) + \phi(y) - \phi(xy) = \phi(x) + \phi(y) - \phi(x) = 0,
\]
for all \( x, y \in G/N \). Consequently, one has \( \phi(x^2y) = \phi(y) \) for all \( x, y \in G/N \). If we let \( y = 1 \), then \( \phi(x^2) = 0 \) for all \( x \in G/N \). Given any \( x \in G/N \), \( \psi_r(x^2, y) = \phi(x^2) + \phi(y) - \phi(x^2y) = 0 \) for all \( y \in G/N \). By the orthogonality of \( \psi_r \), \( x^2 = 1 \) for all \( x \in G/N \). Now we have shown that both \( N \) and \( G/N \) are elementary abelian 2-groups, therefore \( G \cong N \times G/N \) is also an elementary abelian 2-group.

Conversely, by the construction of [7], every elementary abelian 2-group \( G \) contains a semiregular relative difference set \( R \) relative to a subgroup \( N \) of \( G \) provided that \( |N|^3 \leq |G| \) and \( |G/N| \) a perfect square. By translation, we can easily make \( 1 \in R \) and it is trivial that \( rRr = R \) for all \( r \in R \) since \( G \) is elementary abelian 2-group. If \( p \) is an odd prime and \( G \) is special \( p \)-group of exponent \( p \) with \( |Z(G)| + |G/Z(G)| - 1 \) conjugacy classes, then by Lemma 3.2, the cocycle \( \gamma^G_Z(G) \) is orthogonal, and by Lemma 3.3, there is a transversal function \( \tau : G/Z(G) \to G \) such that \( \psi_r \) is skew symmetric. By Lemma 3.1, the cocycle \( \psi_r = \frac{1}{2}\gamma^G_N \) is orthogonal. Hence \( R = \{\tau(x) | x \in G/Z(G)\} \) is a relative difference set in \( G \) relative to \( Z(G) \) and \( 1 \in R \). Moreover, since \( \psi_r \) is skew symmetric and \( |Z(G)| \) is odd, one has \( \psi_r(x, x) = 1/2(\psi_r(x, x) + \psi^r(x, x)) = 0 \) for all \( x \in G/Z(G) \). Also it follows from Lemma 2.4 that \( \psi_r \) is multiplicative. Hence

\[
\tau(x)\tau(y)\tau(x) = \psi_r(x, y)\tau(xy)\tau(x) = (\psi_r(x, y) + \psi_r(xy, x))\tau(xy) = (\psi_r(x, y) + \psi_r(x, x) + \psi_r(y, x))\tau(xy) = \tau(xy) = \tau(x)\tau(y)
\]
for all \( x, y \in G/Z(G) \). Therefore \( rRr = R \) for all \( r \in R \).

Finally, if \( |G| \) is odd and \( R_1 \) and \( R_2 \) are two such semiregular relative difference sets relative to \( N \), then two cocycles \( \psi_{r_1} \) and \( \psi_{r_2} \) obtained from \( R_1 \) and \( R_2 \) respectively are both skew symmetric cocycles. If we define

\[
\delta : G/N \to N,
\]
\[
\delta(x) = \tau_1(x)\tau_2(x)^{-1},
\]
then \( \delta = \psi_{r_1} - \psi_{r_2} \). By Lemma 3.1, \( \psi_{r_1} = \frac{1}{2}\gamma^G_N = \psi_{r_2} \). Therefore \( \delta \psi = 0 \) and \( \delta \) is a homomorphism, which can be extended to \( G \) with \( N \subseteq \ker(\delta) \). □

We end this paper with the proof of Theorem 1.4. The construction of these relative difference sets and orthogonal cocycles could also be found in [5] in terms of distance regular graphs and [10] in terms of \( p \)-groups of Frobenius type.
Proof of Theorem 1.4. Let $p$ be a prime and $m$ and $n$ be two integers such that $m$ even and $2n \leq m$. Let $H = (\mathbb{F}, +) \times (\mathbb{F}, +)$, where $\mathbb{F}$ is a finite field with $|\mathbb{F}| = p^{m/2}$ and $(\mathbb{F}, +)$ is the additive group of $\mathbb{F}$. Let $N$ be an elementary abelian $p$-group of order $p^n$ and $p : (\mathbb{F}, +) \to N$ a surjective homomorphism from $(\mathbb{F}, +)$ to $N$. Define

$$
\psi : H \times H \to N,
$$

$$
\psi((x_1, y_1), (x_2, y_2)) = \rho(x_1y_2 - x_2y_1).
$$

It is easy to verify that $\psi$ is a cocycle of $H$ with coefficients in $N$. Suppose $(g_1, h_1) \neq 0$. Without loss of generality, we assume $g_1 \neq 0$. Then

$$
\sum_{(g,h) \in \mathbb{F} \times \mathbb{F}} \psi((g_1, h_1), (g, h)) = \sum_{(g,h) \in \mathbb{F} \times \mathbb{F}} \rho(g_1h - gh_1) = \sum_{g \in \mathbb{F}} \left( \sum_{h \in \mathbb{F}} \rho(g_1h - gh_1) \right) = \sum_{g \in \mathbb{F}} \left( \sum_{h \in \mathbb{F}} \rho(h) \right) = \sum_{g \in \mathbb{F}} \frac{|\mathbb{F}|}{|N|} \sum_{g \in \mathbb{F}} |\mathbb{F}| = \frac{|\mathbb{F}|^2}{|N|} N,
$$

and $\psi$ is orthogonal. From

$$
\psi((g_1, h_1), (g_2, h_2)) + \psi((g_2, h_2), (g_1, h_1)) = \rho(g_1h_2 - g_2h_1) + \rho(g_2h_1 - g_1h_2) = \rho(g_1h_2 - g_2h_1 + g_2h_1 - g_1h_2) = 0
$$

and

$$
\psi((g, h), (g, h)) = \rho(gh - gh) = 0,
$$

the cocycle $\psi$ is skew-symmetric. Let $G = E(N, H, \psi)$. When $p = 2$, the group $G$ is an elementary 2-abelian group and, by Theorem 1.2, $R = \{(0, x)|x \in H\}$ is a $(2^m, 2^n, 2^{m-n})$-relative difference set relative to $N$. When $p$ is odd, since $H$ is an elementary abelian $p$-group, we have $[G, G] \leq \Phi(G) \leq N \leq Z(G)$. By Lemmas 3.2 and 3.3, $G$ is a special $p$-group of exponent $p$ with $|Z(G)| + |G/Z(G)| - 1$ conjugacy classes and $R = \{(0, x)|x \in H\}$ is a $(p^m, p^n, p^m, p^{m-n})$-relative difference set relative to $N = Z(G)$ with $1 \in R$ and $rRr \in R$ for all $r \in R$.

Conversely, the results of [1,9] ensure that any $(2^m, 2^n, 2^{m-n})$-relative difference sets $R$ in elementary abelian 2-groups must have $m$ even and $2n \leq m$. If a $p$-group $G$ contains a $(p^m, p^n, p^m, p^{m-n})$-relative difference set $R$ relative to a subgroup $N$ of $G$ as described in Theorem 1.3 for some odd prime $p$, then Lemmas 3.4 and 2.5 also ensure that $m$ even and $2n \leq m$. \[Q.E.D.\]

Acknowledgments

We thank Prof. N. Ito for pointing out Ref. [10] to us and the referees for constructive comments. Parts of this work are contained in third author’s Ph.D. thesis [8].

References


