Skew-Hadamard Abelian Group Difference Sets*

E. C. JOHNSON

Department of Mathematics, University of California, Santa Barbara, California

Communicated by R. H. Bruck

Received August 8, 1965

1. INTRODUCTION

A \( v, k, \lambda \) group difference set \((G, D)\) is a \( k \)-subset \( D = \{d_i\}, i = 1, \ldots, k, \)
taken from a group \( G \) of order \( v \) such that each element different from the
identity \( e \) in \( G \) appears exactly \( \lambda \) times in the set of differences \( \{d_id_i^{-1}\}, \)
where \( 0 < \lambda < k < v - 1. \) Combinatorially, a \( v, k, \lambda \) group difference set
is equivalent to a \( v, k, \lambda \) design having a collineation group which is transitive
and regular on the elements and on the blocks of the design \([1]\). Thus, \( v, k, \)
and \( \lambda \) satisfy the relation \([11]\)

\[
(v - 1)\lambda = k(k - 1). \tag{1.1}
\]

We call \((G, D)\) Abelian when \( G \) is Abelian and cyclic when \( G \) is cyclic. A
multiplier of a group difference set \((G, D)\) is an automorphism \( \omega \) of \( G \) under
which

\[
D\omega = bDa \tag{1.2}
\]

for some \( a, b \in G. \) When \( G \) is Abelian, \(1.2\) simplifies to

\[
D\omega = Da \tag{1.3}
\]

for some \( a \in G. \)

A skew-Hadamard design is a \( v, k, \lambda \) design with parameter values \( v = 4m - 1, \)
\( k = 2m - 1, \lambda = m - 1, m \geq 1 \) an integer, having a 0,1 incidence matrix
\( A \) of order \( v \) which satisfies

\[
AA^T = A^TA = mI + (m - 1)J \tag{1.4}
\]

and

\[
A + A^T = J - I, \tag{1.5}
\]

---

* This work was supported in part by a National Academy of Sciences—National
Research Council Postdoctoral Research Associateship at the National Bureau of
Standards, Washington, D.C., and in part by Air Force Office of Scientific Research
Grant AFOSR 698-65.
where $A^T$ is the transpose of $A$, $I$ is the identity matrix of order $v$, and $J$ is the matrix consisting entirely of 1's of order $v$. Skew-Hadamard designs have been studied via their equivalent 1, -1 skew-Hadamard matrices of orders $v + 1 = 4m$, and have been shown to exist for infinitely many values of $v [3, 5, 10, 13]$. Skew-Hadamard design incidence matrices have a number of applications. They are a special type of round robin tournament matrix [12], which occurs in the statistical method of paired comparisons [2] and has application in the behavioral sciences [7, 8]. They have also been used in certain matrix constructions of combinatorial interest [5].

Here we shall be concerned with Abelian group difference sets which are also skew-Hadamard designs. We abbreviate “Abelian group difference set” to AGDS and “skew-Hadamard Abelian group difference set” to SHAGDS. Now the AGDS’s $(G, D)$ with the inverse multiplier

$$
u : g \rightarrow g^{-1}, g \in G$$

form a class of $v, k, \lambda$ group difference sets for which a certain factorization of $k - \lambda$ in the cyclotomic number field involved can be handled [see Eq. (2.15), p. 789, in 4]. As will be presently shown, the SHAGDS’s form another such class. This factorization is a key to obtaining further information about these difference sets. Now Bruck [1] has constructed SHAGDS’s for all orders $v = p^{2\alpha+1}$, $p \equiv 3(\text{mod } 4)$ a prime, and $\alpha \geq 0$ an integer. He showed that the set $D$ of all nonzero squares in the finite field $GF(p^{2\alpha+1})$, when taken as elements of the elementary Abelian additive group $G$ of $GF(p^{2\alpha+1})$, form a SHAGDS $(G, D)$. We shall show that a SHAGDS $(G, D)$ can exist only when order $(G) = v = p^{2\alpha+1}$, $p \equiv 3(\text{mod } 4)$ a prime, and $\alpha \geq 0$ an integer, and when all the cyclic subgroups of $G$ are of sufficiently small order relative to $v$. In particular, we shall show that if $G$ is cyclic then $v = p$ and, taking $G$ as the additive group of integers modulo $p$, $D$ must be either the set of quadratic residues or the set of quadratic nonresidues modulo $p$, and that if $v = p^2$ then $G$ must be elementary Abelian. Thus the results in this paper, together with Bruck’s construction, go a certain distance towards characterizing SHAGDS’s.

2. Preliminaries

Following Bruck, we may characterize a $v, k, \lambda$ AGDS $(G, D)$ as a $v, k, \lambda$ design having a collineation group which is transitive and regular on the elements and on the blocks of the design as follows. Let the elements of the design be the elements in $G$, $g_1 = e, g_2, ..., g_v$, and the blocks of the design the sets $Dg_r = \{dg_r | i = 1, ..., k\}$, $r = 1, ..., v$. Then every block has exactly $k$ elements and, since $d_rg_r = d_sg_s$ if and only if $d_\nu d_\gamma^{-1} = g_r^{-1}g_s$ for $r \neq s$,
every pair of distinct blocks have exactly $\lambda$ elements in common, which shows that we indeed have a $v,k,\lambda$ design. The right regular representation of $G$ is a collineation group of the design with the required properties. Let the 0,1 incidence matrix for this design be $A = [a_{ij}]$, of order $v$, where

$$a_{ij} = \begin{cases} 1, & g_j \in Dg_i \\ 0, & g_j \notin Dg_i \end{cases}. \quad (2.1)$$

Now suppose that $(G,D)$ is a SHAGDS where $v = 4m - 1$, $k = 2m - 1$, $\lambda = m - 1$, $m \geq 2$ an integer. Then $A$ satisfies (1.4) because $(G,D)$ is a $v,k,\lambda$ design and satisfies (1.5) because the design is skew-Hadamard. Now by (1.5), $a_{ii} = 0$, and $a_{ij} = 0$ if and only if $a_i = 1$, $i \neq j$, $i,j = 1,...,v$. By (2.1) this means that $e \notin D$ and that for all $g \in G$, $g \neq e, g \in D$ if and only if $g^{-1} \notin D$.

**Lemma 2.1.** If $(G,D)$ is a SHAGDS and $\omega$ is an automorphism of $G$ then $(G,D^\omega)$ is also a SHAGDS.

**Proof.** Since $\omega$ is an automorphism of $G$ it is clear that if $(G,D)$ is an AGDS then so is $(G,D^\omega)$. Since $e \notin D$ and $(e)\omega = e$ we have $e \notin D^\omega$. Now let $h = (g)\omega \in G$, where $h \neq e$ and so $g \neq e$. Then $h \in D^\omega$ if and only if $g \in D$ if and only if $g^{-1} \notin D$ if and only if $h^{-1} = (g^{-1})\omega \notin D^\omega$. This proves the lemma.

From here on we let $(G,D)$ be a SHAGDS where order $(G) = v = 4m - 1$, $k = 2m - 1$, and $\lambda = m - 1$, $m \geq 2$ an integer. Now let $H$ be an Abelian group of order $u > 1$ which is a homomorphic image of $G$ given by $H = (G)^\Psi$, and let $\Gamma = \{\chi_i\}$, $i = 0,1,...,u - 1$ be the Abelian character group of $H$, where $\chi_0$ denotes the principal character (for a very nice set of exercises which develop most of the basic properties of Abelian group characters see [9, pp. 302–303, Exercises 3, 5, and 6]). For the positive integer $r$ we let $\xi_r$ denote $\exp(2\pi i/r)$, the principal primitive $r$th root of 1, and let $R(\xi_r)$ denote the field of the $r$th roots of 1 over the rational field. We define on $G$ the function

$$\Delta(g) = \begin{cases} 1, & g \in D \\ 0, & g \notin D \end{cases}. \quad (2.2)$$

On $H$ we define the function

$$\Delta(h) = \sum_{(g)\Psi = h} \Delta(g), \quad (2.3)$$

i.e., $\Delta(h)$ is the number of elements in $D$ whose image in $H$ is $h$. We further define

$$\xi(s) = \sum_{h_1 \in H} \Delta(h_1)\chi_s(h_1), \quad 0 \leq s \leq u - 1, \quad (2.4)$$
\[ \xi'(s) = \sum_{h_2 \in H} \Delta(h_2) \chi_s(h_2^{-1}), \quad 0 \leq s \leq u - 1. \quad (2.5) \]

Finally, for any set \( S \) we let \( \delta \) denote the "Kronecker delta" defined on \( S \) in the obvious way, i.e., for \( x, y \in S \),

\[ \delta(x, y) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}. \]

The particular meaning of \( \delta \) should be clear from the context in which it is used. Now for any integer \( s, 0 \leq s \leq u - 1 \), we have by (2.4) and (2.5) that

\[ \xi'(s) = \sum_{h_1 \in H} \sum_{h_2 \in H} \Delta(h_1) \Delta(h_2) \chi_s(h_1 h_2^{-1}). \quad (2.6) \]

Letting \( h = h_1 h_2^{-1} \), (2.6) becomes

\[ \xi'(s) = \sum_{h \in H} \left( \sum_{h_2 \in H} \Delta(h_2) \Delta(hh_2) \right) \chi_s(h). \quad (2.7) \]

Now by Bruck [I, p. 469], letting \( e \) also denote the identity element in \( H \),

\[ \sum_{h_2 \in H} \Delta(h_2) \Delta hh_2 = (k - \lambda) \delta(h, e) + \lambda w \quad (2.8) \]

where \( w = u/v \). Hence (2.7) becomes

\[ \xi'(s) = \sum_{h \in H} \left[ (k - \lambda) \delta(h, e) + \lambda w \right] \chi_s(h) \]

\[ = (k - \lambda) + \lambda w \sum_{h \in H} \chi_s(h) \]

\[ = (k - \lambda) + \lambda w \delta(s, 0) \]

or

\[ \xi'(s) = k - \lambda + \lambda w \delta(s, 0). \quad (2.9) \]

Now by (2.4) and (2.5)

\[ \xi(s) + \xi'(s) = \sum_{h \in H} \left( \Delta(h) + \Delta(h^{-1}) \right) \chi_s(h). \quad (2.10) \]

By (2.3),

\[ \Delta(h) + \Delta(h^{-1}) = \sum_{\gamma \varphi = h} \Delta(g) + \sum_{\gamma \varphi = h^{-1}} \Delta(g) \]

\[ = \sum_{\gamma \varphi = h} (\Delta(g) + \Delta(g^{-1})). \quad (2.11) \]
If \( h = (g)^y \neq e \) then \( g \neq e \) whence \( \Delta(g) + \Delta(g^{-1}) = 1 \) and (2.11) becomes
\[
\Delta(h) + \Delta(h^{-1}) = \sum_{(g)^y = h} 1 = w, h \neq e.
\] (2.12)

Also,
\[
\sum_{h \in H} \Delta(h) = k = \frac{1}{2}(v - 1)
\]
or
\[
\Delta(e) + \frac{1}{2} \sum_{h \in H, h \neq e} (\Delta(h) + \Delta(h^{-1})) = \frac{1}{2}(uvw - 1)
\]
or
\[
\Delta(e) + \frac{1}{2}(u - 1)w = \frac{1}{2}(uvw - 1),
\]
whence
\[
\Delta(e) = \frac{1}{2}(w - 1).
\] (2.13)

Thus by (2.12) and (2.13), (2.10) becomes
\[
\xi(s) + \xi'(s) = w - 1 + w \sum_{h \in H, h \neq e} \chi_i(h)
\]
\[
= -1 + w \sum_{h \in H} \chi_i(h)
\]
\[
= -1 + wu\delta(s, 0)
\]
or
\[
\xi(s) + \xi'(s) = -1 + wu\delta(s, 0).
\] (2.14)

Hence by (2.14),
\[
\xi(s)\xi'(s) = -\xi(s) - \xi^2(s) + w\xi(s)\delta(s, 0).
\] (2.15)

Combining (2.9) with (2.15), noting that \( k - \lambda = m \) and \( v = 4m - 1 \), we get
\[
4\xi^2(s) + 4\xi(s) + 1 = -v + 4v(\xi(s) - \lambda)\delta(s, 0)
\]
or
\[
2\xi(s) + 1 = \begin{cases} \frac{v}{\sqrt{-v} \epsilon(s)}, & s = 0 \\ \frac{1}{s \epsilon(s)}, & s \neq 0, \epsilon(s) = \pm 1. \end{cases}
\] (2.16)

Before proceeding further, we need the following result. We give here an elementary proof using only the basic properties of finite-dimensional vector spaces and cyclotomic number fields.
LEMMA 2.2. If \( p \) and \( q \) are prime numbers, \( p < q \), then \( R(\zeta_p) \cap R(\zeta_q) = R \).

**Proof.** If \( p = 2 \) then \( R(\zeta_p) = R \) and the lemma is trivial. Suppose then that \( p > 2 \). We consider \( R(\zeta_p) \), \( R(\zeta_q) \), and \( R(\zeta_{pq}) \) as vector spaces over \( R \). Now \( L = \{ \zeta_p^i \mid i = 0, 1, \ldots, p - 2 \} \) is a basis for \( R(\zeta_p) \) over \( R \) and \( M = \{ \zeta_q^j \mid j = 0, 1, \ldots, q - 2 \} \) is a basis for \( R(\zeta_q) \) over \( R \). We form \( \mathcal{N} = \{ \zeta_p^i \zeta_q^j \mid i = 0, 1, \ldots, p - 2; \ j = 0, 1, \ldots, q - 2 \} \) consisting of \( (p - 1)(q - 1) = \phi(pq) \) elements, where \( \phi \) denotes Euler’s phi-function. Now \( \mathcal{N} \subseteq R(\zeta_{pq}) \) and \( \dim(R(\zeta_{pq}) \mid R) = \phi(pq) \), hence, if we can show that \( \mathcal{N} \) spans \( R(\zeta_{pq}) \) then we will know that \( \mathcal{N} \) is a basis for \( R(\zeta_{pq}) \) over \( R \). Now it is easy to show for any integer \( r \) satisfying \( 0 \leq r \leq pq - 1 \) that there exist integers \( s \) and \( t \), \( 0 \leq s \leq p - 1, 0 \leq t \leq q - 1 \), such that

\[
r \equiv sq + tp \pmod{pq}.
\]

Then

\[
\zeta_{pq}^r = \zeta_p^s \zeta_q^t = \zeta_p^s \cdot \zeta_q^t,
\]

and since \( \zeta_p^s \) and \( \zeta_q^t \) are in the linear spans of \( L \) and \( M \), respectively, \( \zeta_{pq}^r \) is in the linear span of \( \mathcal{N} \). Since \( r \) was arbitrary, every element of \( R(\zeta_{pq}) \) is in the linear span of \( \mathcal{N} \). Hence \( \mathcal{N} \) is a basis for \( R(\zeta_{pq}) \) over \( R \). Now if \( \eta \in R(\zeta_p) \cap R(\zeta_q) \) then \( \eta \) is in the linear span of both \( L \) and \( M \) or

\[
\eta = \sum_{i=0}^{p-2} a_i \zeta_p^i = \sum_{j=0}^{q-2} b_j \zeta_q^j,
\]

where \( a_i, b_j \in R, i = 0, 1, \ldots, p - 2, j = 0, 1, \ldots, q - 2 \). But then

\[
(a_0 - b_0) + \sum_{i=1}^{p-2} a_i \zeta_p^i - \sum_{j=1}^{q-2} b_j \zeta_q^j = 0,
\]

and since \( L \subseteq \mathcal{N}, \mathcal{N} \subseteq M \), and \( L \cap M = \{1\} \), we must have \( a_0 = b_0 \); \( a_i = 0, i = 1, \ldots, p - 2 \); \( b_j = 0, j = 1, \ldots, q - 2 \), whence \( \eta \in R \). Hence \( R(\zeta_p) \cap R(\zeta_q) = R \).

3. **Main Results**

We first prove a theorem which strongly restricts the orders \( v \) for which SHAGDS’s can exist.

**Theorem 3.1.** Let \((G, D)\) be a SHAGDS where \( G \) is of order \( v \). Then \( v = p^{2\alpha+1} \) where \( p = 3(\mod 4) \) is a prime and \( \alpha \geq 0 \) is an integer.
Proof. Let $H = G$ so that $\Gamma$ becomes the Abelian character group of $G$. Suppose that $p$ is a prime divisor of $v$. Then since $\Gamma$ is isomorphic to $G$, there is an element $\chi_r$ of order $p$ in $\Gamma$. This means that $\chi_r(g)$ is a $p$th root of unity for every $g \in G$. Thus by (2.4), $\xi(f) \in R(\zeta_p)$, whence by (2.16), $\sqrt{-v} \in R(\zeta_p)$. If $q \neq p$ were another prime divisor of $v$, then by this same argument we would have $\sqrt{-v} \in R(\zeta_q)$, whence by Lemma 2.2, $\sqrt{-v} \in R$, which is impossible for $v > 0$. Hence $v$ is divisible only by the prime $p$. Since $v \equiv 3(\text{mod } 4)$, this means that we must have $v = p^{2\alpha+1}$ where $p \equiv 3(\text{mod } 4)$ and $\alpha \geq 0$ is an integer.

From here on we take $v = p^{2\alpha+1}$, $p \equiv 3(\text{mod } 4)$ a prime, $\alpha \geq 0$ an integer, and let order $(H) = u = p^\beta$, where $\beta$ is an integer satisfying $1 \leq \beta \leq 2\alpha + 1$.

**Theorem 3.2.** Let $(G, D)$ be a SHAGDS where $v = p^{2\alpha+1}$ and let $H$ be a homomorph image of $G$ of order $p^\beta$. If $H$ is cyclic then $\beta \leq \alpha + 1$.

Proof. From (2.16) and (2.4), with $k = \frac{1}{2}(v - 1)$, we obtain

$$
\sum_{h \in H} \Delta(h) \chi_s(h) = \begin{cases} 
 k, & s = 0 \\
 -\frac{1}{2} + \frac{1}{2} \sqrt{-v} \epsilon(s), & s \neq 0
\end{cases}.
$$

(3.1)

Now for any $h_\ast \in H$, we have from (3.1) that

$$
\sum_{h \in H} \Delta(h) \chi_s(hh_\ast^{-1}) = \begin{cases} 
 k, & s = 0 \\
 -\frac{1}{2} (1 - \sqrt{-v} \epsilon(s)) \chi_s(h_\ast^{-1}), & s \neq 0
\end{cases},
$$

whence

$$
\sum_{s=0}^{u-1} \sum_{h \in H} \Delta(h) \chi_s(hh_\ast^{-1}) = k - \frac{1}{2} \sum_{s=1}^{u-1} (1 - \sqrt{-v} \epsilon(s)) \chi_s(h_\ast^{-1}).
$$

or

$$
\sum_{h \in H} \Delta(h) \sum_{s=0}^{u-1} \chi_s(hh_\ast^{-1}) = k - \frac{1}{2} \sum_{s=1}^{u-1} \chi_s(h_\ast^{-1}) + \frac{1}{2} \sqrt{-v} \sum_{s=1}^{u-1} \epsilon(s) \chi_s(h_\ast^{-1}).
$$

(3.2)

Now

$$
\sum_{s=0}^{u-1} \chi_s(hh_\ast^{-1}) = u \delta(h, h_\ast),
$$

whence the left side of (3.2) is $u \Delta(h_\ast)$. Also

$$
\sum_{s=1}^{u-1} \chi_s(h_\ast^{-1}) = u \delta(h_\ast, e) - 1.
$$
Hence (3.2) becomes
\[ u\Delta(h_*) = h - \frac{1}{2}(u\delta(h_*, e) - 1) + \frac{1}{2} \sqrt{-v} \sum_{s=1}^{u-1} \epsilon(s)x_s(h_*)^{-1} \]
or
\[ \Delta(h_*) = \frac{1}{2u} \left[ u - u\delta(h_*, e) + \sqrt{-v} \sum_{s=1}^{u-1} \epsilon(s)x_s(h_*)^{-1} \right]. \quad (3.3) \]

Taking \( h_* \neq e \) and replacing \( u \) and \( v \) by their respective powers of \( p \) in (3.3), we obtain
\[ \Delta(h_*) = \frac{1}{2} \left[ p^{2s+1} + p^{2s} \sqrt{-p} \sum_{s=1}^{u-1} \epsilon(s)x_s(h_*)^{-1} \right]. \quad (3.4) \]

We now take \( H \) to be cyclic of order \( u = p^\beta \). Then \( \Gamma \) is also cyclic of order \( u \). Let \( H \) be generated by the element \( h \) and let \( \Gamma \) be generated by the character \( \chi \) for which \( \chi(h) = \zeta_u \). We set \( \chi_s = \chi^s, s = 0, 1, \ldots, u - 1 \). Then letting \( h_* = h^r \neq e \), where \( r \) is any integer satisfying \( 1 \leq r \leq u - 1 \) and denoting \( \Delta(h^r) \) by \( \Delta(r) \), (3.4) becomes
\[ \Delta(r) = \frac{1}{2} \left[ p^{2s+1} + p^{2s} \sqrt{-p} \sum_{s=1}^{u-1} \epsilon(s)\zeta_u^{-rs} \right]. \quad (3.5) \]

Thus, in order to evaluate \( \Delta(r) \) in (3.5) we will need to obtain a simple expression for
\[ Q(r) = \sum_{s=1}^{u-1} \epsilon(s)\zeta_u^{-rs}. \quad (3.6) \]

This is accomplished by the following lemma, the proof of which is given in Section 4. We let \((x \mid p)\) denote the Legendre symbol with respect to \( p \) applied to the integer \( x \).

**Lemma 3.3.** Let \( r = np^\nu \) where \( n \) and \( \nu \) are integers satisfying \( (n, p) = 1 \), \( 0 \leq \nu \leq \beta - 1 \), and \( 1 \leq n \leq p^{\beta-\nu} - 1 \). Then
\[ Q(r) = -(n \mid p)e(p^{\beta-\nu-1})p^{\nu} \sqrt{-p}. \quad (3.7) \]

Hence by (3.6) and (3.7), (3.5) becomes
\[ \Delta(r) = \frac{1}{2} \left[ p^{2s+1} + (n \mid p)e(p^{\beta-\nu-1})p^{\beta-\nu+1} \right]. \quad (3.8) \]

Now \( \Delta(r) \) must be an integer for every integer \( r, 1 \leq r \leq u - 1 \). Hence by (3.8), \( p^{\beta-\nu+1} \) must be an integer or
\[ \beta \leq \alpha + 1 + \nu \quad (3.9) \]
for every \( \nu \) satisfying \( 0 \leq \nu \leq \beta - 1 \). By taking \( \nu = 0 \) in (3.9) we obtain \( \beta \leq \alpha + 1 \). This concludes the proof of Theorem 3.2.

**Corollary 3.4.** Let \((G, D)\) be a cyclic SHAGDS. Then \( \nu = p \) and, taking \( G \) as the additive group of integers modulo \( p \), \( D \) is either the set of quadratic residues or the set of quadratic nonresidues modulo \( p \).

**Proof.** Since \( G \) is cyclic we may take \( H = G \) in Theorem 3.2. Then
\[
2\alpha + 1 = \beta \leq \alpha + 1
\]
for \( \alpha \geq 0 \), which can only be satisfied for \( \alpha = 0 \). Hence \( \nu = p \). Now take \( G \) as the additive group of integers modulo \( p \). Then \( 0 \notin D \) and for any \( n \in G, 1 \leq n \leq p - 1 \), (3.8) becomes
\[
\Delta(n) = \frac{1}{2\mu} [1 + (n \mid p)e(1)].
\] (3.10)

By (3.10) and (2.2), \( n \in D \) if and only if \( (n \mid p) = e(1) \). Hence \( D \) consists of either the quadratic residues or the quadratic nonresidues modulo \( p \).

As an Abelian group, \( G \) is a direct product of cyclic subgroups of orders which are powers of \( p \),
\[
G = \bigotimes_{i=1}^{f} C(p^{\theta_i}); \quad \theta_i > 0, \quad i = 1, \ldots, f,
\] (3.11)
where \( C(p^{\theta_i}) \) denotes the cyclic component of \( G \) of order \( p^{\theta_i} \),
\[
\sum_{i=1}^{f} \theta_i = 2\alpha + 1,
\] (3.12)
and we take
\[
1 \leq \theta_1 \leq \cdots \leq \theta_f.
\] (3.13)

We let \( b_i \) be the generator of \( C(p^{\theta_i}) \), \( i = 1, \ldots, f \); whence the set of these generators is a basis for \( G \), i.e., we can express any \( g \in G \) in the form
\[
g = \prod_{i=1}^{f} b_i^{\gamma_i}, \quad 0 \leq \gamma_i \leq p^{\theta_i} - 1.
\] (3.14)

**Theorem 3.5.** Let \((G, D)\) be a SHAGDS for which we have (3.11), (3.12), and (3.13), where \( \alpha \geq 1 \). Then \( \theta_f \leq \alpha \).

**Proof.** Now for \( g \in G \) as given in (3.14) the mapping
\[
\Psi: g \rightarrow b_\gamma, \quad \text{all} \quad g \in G,
\]
is a homomorphism of \( G \) onto its cyclic component \( C(p^{\theta_f}) \). Hence by Theorem...
3.2, \( \theta_\ell \leq \alpha + 1 \). Suppose that \( \theta_\ell = \alpha + 1 \) where \( \alpha \geq 1 \). By Corollary 3.4, \( f > 1 \). Then for \( r = n p^\alpha \), where \( (n, p) = 1 \) and \( 1 \leq n \leq p - 1 \), we have in (3.8) that
\[
\Delta(r) = \begin{cases} 
( p^\alpha, (n \mid p) = \epsilon(1) \\
0, (n \mid p) = -\epsilon(1) 
\end{cases} .
\]
(3.15)

We note that (3.15) must hold for any SHAGDS \((G, D)\). Now let \( r_0 = n_0 p^\alpha \) be such that \( \Delta(r_0) = p^\alpha \) and thus \( \Delta(p^{\alpha r} - r_0) = 0 \). Since the order of the group
\[
\mathcal{G} = \bigotimes_{i=1}^{f-1} C(p^{\alpha_i})
\]
is \( p^\alpha \), this means that every element \( g \in G \) of the form
\[
g = \tilde{g} B_j^{r_0}, \tilde{g} \in \mathcal{G},
\]

must be an element of \( D \). Now for \( g \in G \) as given in (3.14) let \( \omega \) be the automorphism of \( G \) given by
\[
\omega: g \mapsto \left( \prod_{i=1}^{f-1} B_i^{\eta_i} \right) B_j^\eta, \quad \text{all } g \in G,
\]
(3.16)

where
\[
\eta \equiv \gamma_f + \gamma_1 p_\ell r - \eta_i \pmod{p^{\alpha_i}}.
\]
(3.17)

Then by Lemma 2.1, \((G, D^\omega)\) is also a SHAGDS. Now in particular, we have by (3.16) and (3.17) for \( \gamma_1 = m p^{\alpha_1 - 1}, 0 \leq m \leq p - 1 \), that
\[
\omega: B_j^{r_0} B_j^{r_0} \rightarrow B_j^{r_0} B_j^{r_0} \in D^\omega,
\]
(3.18)

where
\[
\eta_0 \equiv r_0 + m p^{\alpha_1} \pmod{p^{\alpha_1 + 1}}.
\]
(3.19)

Examining (3.18) and (3.19), we see that for \( m = 0 \) we have \( B_j^{r_0} \in D^\omega \), while for \( m = -2n_0 \pmod{p} \) we have \( B_j^{r_0} B_j^{r_0} \in D^\omega \) for some integer \( \lambda \), \( 0 \leq \lambda \leq p^{\alpha_1} - 1 \). Hence for \((G, D^\omega)\) with \( C(p^{\alpha_1}) = (G)^\omega \) we have \( \Delta(r_0) > 0 \) and \( \Delta(p^{\alpha_1 r} - r_0) > 0 \). This contradicts (3.15). Hence we cannot have \( \theta_\ell = \alpha + 1 \); whence \( \theta_\ell \leq \alpha \).

**Corollary 3.6.** If \((G, D)\) is a SHAGDS where \( v = p^\alpha \), then \( G \) is elementary Abelian.

**Proof.** Here \( \alpha = 1 \); hence by Theorem 3.5, \( \theta_1 = \theta_2 = \theta_3 = 1 \) in (3.11).
4. Proof of Lemma 3.3

For convenience, we restate Lemma 3.3. Recall that \( u = p^\beta, p = 3 \text{ (mod } 4) \) a prime, \( \beta \geq 1 \) an integer, and

\[
Q(r) = \sum_{s=1}^{u-1} \epsilon(s) \zeta_u^{-rs},
\]

where \( r \) is an integer satisfying \( 1 \leq r \leq u - 1 \) and \( \epsilon(s) = \pm 1, s = 1, \ldots, u - 1 \).

**Lemma 3.3.** Let \( Y = ny \) where \( n \) and \( v \) are integers satisfying \( (n, p) = 1 \), \( 0 \leq v \leq \beta - 1 \), and \( 1 \leq n \leq p^{\beta-v} - 1 \). Then

\[
Q(r) = -(n \mid p) \epsilon(p^{\beta-v-1}) p^v \sqrt{-p}.
\]

**Proof.** We first show that certain of the values \( \epsilon(s) \) in (4.1) must be equal. Now the Galois group \( \mathfrak{G} \) of \( R(\zeta_u) \) over \( R \) is cyclic of order \( \phi(u) = 2^{u-2} \) and is generated by the automorphism \( \tau \) determined by

\[
\tau : \zeta_u \rightarrow \zeta_u^t,
\]

where \( t \) is a primitive root modulo \( u \). Since \( \mathfrak{G} \) is cyclic and \( \phi(u) \) is divisible by 2 there exists a unique subgroup \( \mathfrak{H} \) of index 2 in \( \mathfrak{G} \) consisting of all automorphisms of \( R(\zeta_u) \) fixing a quadratic subfield \( F \) over \( R \) elementwise. Since \( \mathfrak{H} \) is unique, \( F \) is unique, and since \( R(\sqrt{-p}) \subset R(\zeta_u) \subset R(\zeta_u) \) we must have \( F = R(\sqrt{-p}) \). The automorphisms in \( \mathfrak{G} - \mathfrak{H} \), then, send \( \sqrt{-p} \) into \( -\sqrt{-p} \).

We note that \( \mathfrak{H} \) is also cyclic and is generated by \( \tau^2 \). Now from (3.1) we have

\[
\sum_{i=0}^{u-1} A(i) \zeta_u^{ts} = -\frac{1}{2} + \frac{1}{2} p^s \sqrt{-p} \epsilon(s), s \neq 0.
\]

Applying \( \tau^{2c} \), \( c \) an integer satisfying \( 0 \leq c \leq \frac{1}{2} \phi(u) - 1 \), to both sides of (4.3), we see that

\[
\epsilon(st^{2c}) = \epsilon(s), s \neq 0,
\]

where \( st^{2c} \) is taken modulo \( u \). Similarly, applying \( \tau^{2c+1} \), \( c \) an integer satisfying \( 0 \leq c \leq \frac{1}{2} \phi(u) - 1 \), to both sides of (4.3), we see that

\[
\epsilon(st^{2c+1}) = -\epsilon(s), s \neq 0,
\]

where \( st^{2c+1} \) is taken modulo \( u \).

Now any integer \( s, 1 \leq s \leq u - 1 \), may be written as \( s = mp^u \) where \( m \)
and \( \mu \) are integers satisfying \((m, p) = 1\), \(0 \leq \mu \leq \beta - 1\), and \(1 \leq m \leq p^{\beta - \mu} - 1\). Hence (4.1) becomes

\[
Q(r) = \sum_{\mu=0}^{\beta-1} \sum_{m=1}^{p^{\beta-\mu}-1} e(m \mu) \exp(2\pi i (-rm)/p^{\beta-\mu}).
\]

Now for every integer \( m \), \((m, p) = 1\), \(1 \leq m \leq p^{\beta - \mu} - 1\), there exists a unique integer \( \rho \), \(0 \leq \rho < \phi(u) - 1\), for which \( m \equiv \rho^e (\mod u)\). If \( n \) is any integer, \( p^{\beta - \mu} + 1 \leq n \leq p^\beta - 1\), for which \( m \equiv n \mod p^{\beta-\mu} \) then \((n, p) = 1\)

whence \( n \equiv \rho^{-e} \mod u \) for a unique integer \( \sigma \), \(0 \leq \sigma < \phi(u) - 1\). Then \( \rho^{-e} \equiv \rho^e (\mod p^{\beta-\mu})\), and since \((t, p) = 1\) we have \( t^{e-\sigma} \equiv 1 \mod p^{\beta-\mu}\). Now \( t \) is a primitive root modulo \( p^{\beta-\mu}\) of order \( \phi(p^{\beta-\mu}) = p^\beta - \mu - 1(p - 1)\), which is an even integer. Hence \( \rho - \sigma \) is even, whence \( m \) and \( n \) are both obtained as either even powers or odd powers of \( t \) modulo \( u \). Now for each such integer \( m \) there are \((u/p^{\beta-\mu}) - 1 = p^{\mu} - 1\) such integers \( n \) for which \( m \equiv n \mod p^{\beta-\mu}\), and all \( p^{\mu} \) of these integers are generated as either even powers or odd powers of \( t \) modulo \( u \). Hence, letting \((x \mid p)\) denote the Legendre symbol with respect to \( p \) applied to \( x \), we have by (4.4) and (4.5),

\[
\epsilon(p^{\mu}) \sum_{e=0}^{\phi(u)-1} \exp(2\pi i (-rt^{2e})/p^{\beta-\mu}) = p^{\mu} \sum_{m=1}^{p^{\beta-\mu}-1} e(m \mu) \exp(2\pi i (-rm)/p^{\beta-\mu}).
\]

and

\[
-\epsilon(p^{\mu}) \sum_{e=0}^{\phi(u)-1} \exp(2\pi i (-rt^{2e+1})/p^{\beta-\mu})
\]

\[
= p^{\mu} \sum_{m=1}^{p^{\beta-\mu}-1} e(m \mu) \exp(2\pi i (-rm)/p^{\beta-\mu}).
\]

Hence by (4.6), (4.7), and (4.8), we obtain

\[
Q(r) = \sum_{\mu=0}^{\beta-1} p^\mu \epsilon(p^{\mu}) \left\{ \sum_{e=0}^{\phi(u)-1} \exp(2\pi i (-rt^{2e})/p^{\beta-\mu}) - \sum_{e=0}^{\phi(u)-1} \exp(2\pi i (-rt^{2e+1})/p^{\beta-\mu}) \right\}.
\]

Now since \(1 \leq r \leq u - 1\), we can write \( r = np^v \) where \( n \) and \( v \) are integers satisfying \((n, p) = 1\), \(0 \leq v \leq \beta - 1\), and \(1 \leq n \leq p^{\beta - v}\). We let

\[
R_0(\mu, v, n) \equiv \sum_{e=0}^{\phi(u)-1} \exp(2\pi i (-nt^{2e})/p^{\beta-\mu}) = \sum_{e=0}^{\phi(u)-1} \exp(2\pi i (-rt^{2e})/p^{\beta-\mu})
\]

(4.10)
and
\[ R_1(\mu, v, n) = \sum_{c=0}^{\frac{1}{2}\phi(u)-1} \exp(2\pi i(-nt^{2c+1})/p^\nu) = \sum_{c=0}^{\frac{1}{2}\phi(u)-1} \exp(2\pi i(-rt^{2c+1})/p^{\beta-\mu}), \] (4.11)

where \( \gamma = \beta - \nu - \mu \). Now if \( \gamma \leq 0 \), then every term in each of the sums in (4.10) and (4.11) is 1, whence
\[ R_0(\mu, v, n) - R_1(\mu, v, n) = 0, \mu \geq \beta - \nu. \] (4.12)

Now suppose that \( \gamma > 0 \). Since \( p \equiv 3 \text{(mod 4)} \) we have \( (n \mid p) = +1 \) if and only if \( (-n \mid p) = -1 \). For any integer \( x \) which is a prime power of \( p \), let us denote the set of quadratic residues modulo \( x \) and relatively prime to \( p \) by \( QR(x) \) and the set of quadratic nonresidues modulo \( x \) and relatively prime to \( p \) by \( QNR(x) \). Now as \( c \) runs from 0 to \( \frac{1}{2}\phi(u) - 1 \), \( t^{2c} \) runs once through \( QR(u) \) and \( t^{2c+1} \) runs once through \( QNR(u) \); whence \( -nt^{2c} \) runs once through \( QR(u) \) or \( QNR(u) \) according as \( (n \mid p) = -1 \) or \( (n \mid p) = +1 \), and \( -nt^{2c+1} \) runs once through \( QR(u) \) or \( QNR(u) \) according as \( (n \mid p) = \pm 1 \) or \( (n \mid p) = 1 \). Hence as \( c \) runs from 0 to \( \frac{1}{2}\phi(u) - 1 \), \( nt^{2c} \) runs \( \mu + \nu \) times through \( QR(p^\nu) \) or \( QNR(p^\nu) \) according as \( (n \mid p) = -1 \) or \( (n \mid p) = +1 \), and \( nt^{2c+1} \) runs \( \mu + \nu \) times through \( QR(p^\nu) \) or \( QNR(p^\nu) \) according as \( (n \mid p) = +1 \) or \( (n \mid p) = -1 \). Hence by (4.10) and (4.11), \( R_0(\mu, v, n) \) and \( R_1(\mu, v, n) \) are
\[ p^{\mu+\nu} \sum_{q \in QR(p^\nu)} \exp(2\pi iq/p^\nu) \quad \text{and} \quad p^{\mu+\nu} \sum_{q \in QNR(p^\nu)} \exp(2\pi iq/p^\nu) \]
in some order. Now suppose further that \( \gamma \geq 2 \). If \( \bar{q} \in QR(p^\nu) \) is such that \( 1 \leq \bar{q} \leq p^{\nu-1} - 1 \) then \( \bar{q} \in QR(p^{\nu-1}) \), and if \( \bar{q}' \), \( 1 \leq \bar{q}' \leq p^\nu - 1 \), satisfies \( \bar{q}' \equiv \bar{q} \pmod{p^{\nu-1}} \) then \( \bar{q}' \in QR(p^\nu) \). Furthermore, every \( \bar{q}' \in QR(p^\nu) \) satisfies \( \bar{q}' \equiv \bar{q} \pmod{p^{\nu-1}} \) for some \( \bar{q} \in QR(p^{\nu-1}) \). Hence
\[ \sum_{q \in QR(p^\nu)} \exp(2\pi iq/p^\nu) = \sum_{q \in QR(p^{\nu-1})} \sum_{j=0}^{p-1} \exp(2\pi i(q + jp^{\nu-1})/p^\nu) \]
\[ = \sum_{q \in QR(p^{\nu-1})} \exp(2\pi i\bar{q}/p^\nu) \sum_{j=0}^{p-1} \exp(2\pi ij/p) \]
\[ = 0 \] (4.13)
since
\[ \sum_{j=0}^{p-1} \exp(2\pi ij/p) = 0. \]
By a similar argument we also have
\[ \sum_{q \in QNR(p^n)} \exp(2\pi iq/p^n) = 0. \] (4.14)

Thus by (4.13) and (4.14), we have
\[ R_0(\mu, \nu, n) = R_1(\mu, \nu, n) = 0, \gamma \geq 2, \] or
\[ R_0(\mu, \nu, n) - R_1(\mu, \nu, n) = 0, \mu \leq \beta - \nu - 2. \] (4.15)

There remains, then, the case where \( \gamma = 1 \) or \( \mu = \beta - \nu - 1 \). Here, according to the argument following (4.12),
\[ R_0(\mu, \nu, n) = \begin{cases} p^{p-1} \sum_{q \in QR(p)} \zeta_p^q, (n \mid p) = -1 \\ p^{p-1} \sum_{q \in QNR(p)} \zeta_p^q, (n \mid p) = +1, \end{cases} \] (4.16)
and
\[ R_1(\mu, \nu, n) = \begin{cases} p^{p-1} \sum_{q \in QNR(p)} \zeta_p^q, (n \mid p) = -1 \\ p^{p-1} \sum_{q \in QR(p)} \zeta_p^q, (n \mid p) = +1. \end{cases} \] (4.17)

Thus
\[ R_0(\mu, \nu, n) - R_1(\mu, \nu, n) = -(n \mid p)p^{p-1} \left\{ \sum_{q \in QR(p)} \zeta_p^q - \sum_{q \in QNR(p)} \zeta_p^q \right\}. \] (4.18)

Now
\[ \sum_{q \in QR(p)} \zeta_p^q + \sum_{q \in QNR(p)} \zeta_p^q = -1, \]
hence
\[ \sum_{q \in QR(p)} \zeta_p^q - \sum_{q \in QNR(p)} \zeta_p^q = 2 \sum_{q \in QR(p)} \zeta_p^q + 1. \] (4.19)

Furthermore,
\[ 2 \sum_{q \in QR(p)} \zeta_p^q + 1 = \sum_{j=0}^{p-1} \zeta_p^j. \] (4.20)
Now the value of the Gaussian sum on the right side of (4.20) is $\sqrt{-p}$ [6, p. 197]; hence by (4.19), (4.18) becomes

$$R_0(\mu, \nu, n) - R_1(\mu, \nu, n) = -(n \mid p)p^{\beta-1} \sqrt{-p}, \mu = \beta - \nu - 1.$$  \hspace{1cm} (4.21)

Hence by (4.10), (4.11), (4.12), (4.15), and (4.21), (4.9) becomes

$$Q(r) = -(n \mid p)e(\rho^{\beta-\nu} - 1)\rho^r \sqrt{-p},$$

which is (4.2).

**Note added in Proof.** The author is grateful to Dr. Richard Turyn for calling to his attention that Corollary 3.4 was essentially also proved in [I].

**References**

5. Johnsen, E. C. Integral solutions to the incidence equation for finite projective plane cases of orders $n \equiv 2 (\text{mod } 4)$. *Pacific J. Math.* 17 (1966), 97-120.