SPECIAL ABELIAN GROUP DIFFERENCE SETS

E. C. JOHNSEN

1. Introduction. A v, k, λ *abelian group difference set* (abbreviated AGDS) (G, D) is a k-subset $D = \{d_i\}_1^k$ taken from an abelian group G of order v such that each element different from the identity e in G appears exactly λ times in the set of differences $\{d_i d_j^{-1}\}$, where $0 < \lambda < k < v - 1$. Combinatorially, a v, k, λ AGDS is equivalent to a v, k, λ design having an abelian collineation group which is transitive and regular on the elements and on the blocks of the design (1). Thus, v, k, and λ satisfy the following relation (cf. **5**)

$$(1.1) \qquad (v - 1)\lambda = k(k - 1).$$

Two AGDSs (G, D) and (G, E) are called *equivalent* if there exists an automorphsim ω of G under which

$$(1.2) \qquad E^{\omega} = Da$$

for some $a \in G$. If $E = D$ in (1.2), then ω is called a *multiplier* of (G, D), and if ω is the identity automorphism in (1.2), then (G, E) is called a *translate* of (G, D).

Two special classes of AGDSs have been investigated recently in (**2**) and (**3**). One is the class of AGDSs (G, D) with the inverse multiplier (abbreviated IMAGDSs)

$$\iota\colon g \to g^{-1}, \qquad g \in G,$$

and the other is the class of skew-Hadamard AGDSs (G, D) (abbreviated SHAGDSs), where $e \notin D$ and for all $g \in G$, $g \neq e$, $g \in D$ if and only if $g^{-1} \notin D$. In this paper we shall obtain a classification of AGDSs in which these two classes together with the AGDSs complementary to the SHAGDSs (abbreviated co-SHAGDSs) become the simplest and the most prominent classes.

2. Preliminaries. Let (G, D) be a v, k, λ AGDS and let

$$\Gamma = \{\chi_i \mid 0 \leqq i \leqq v - 1\}$$

be the abelian character group of G, where χ_0 denotes the principal character. For the positive integer r let ζ_r denote $\exp(2\pi\mathbf{i}/r)$, the principal primitive rth root of unity, and let $R(\zeta_r)$ denote the field of the rth roots of unity over the rational field R. We define on G the function

$$(2.1) \qquad \Delta_D(g) = \begin{cases} 1, & g \in D, \\ 0, & g \notin D, \end{cases}$$

Received June 5, 1967. This paper was presented to the American Mathematical Society at the Annual Meeting in Chicago, Illinois, January 25, 1966. This work was supported by Air Force Office of Scientific Research Grants AFOSR 698-65 and 698-67.

and set

$$\xi_D(s) \equiv \sum_{g \in G} \Delta_D(g)\chi_s(g), \qquad 0 \leqq s \leqq v-1, \tag{2.2}$$

and

$$\xi_D'(s) \equiv \sum_{g \in G} \Delta_D(g)\chi_s(g^{-1}) = \sum_{g \in G} \Delta_D(g^{-1})\chi_s(g), \qquad 0 \leqq s \leqq v-1. \tag{2.3}$$

Note that $\xi_D'(s) = \bar{\xi}_D(s)$ (complex conjugate) and that if χ_s is of order r in Γ, then $\xi_D(s)$ and $\xi_D'(s)$ are algebraic integers in $R(\zeta_r)$, $1 \leqq s \leqq v-1$. Finally, for any set S we define the "Kronecker δ" in the obvious way, i.e., for $x, y \in S$

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

Now, as previously derived in (**3**), we have that

$$\xi_D(s)\xi_D'(s) = k - \lambda + \lambda v \delta(s, 0), \qquad 0 \leqq s \leqq v-1. \tag{2.4}$$

From this we see that

$$|\xi_D(s)| = \sqrt{(k-\lambda)} > 0, \qquad 1 \leqq s \leqq v-1. \tag{2.5}$$

3. A classification. Consider the possibility of solving the system of $v - 1$ linear equations

$$\xi_D'(s) = a_1 + a_2\xi_D(s) + \ldots + a_{v-1}\xi_D^{v-2}(s), \qquad 1 \leqq s \leqq v-1, \tag{3.1}$$

for the values of $a_1, a_2, \ldots, a_{v-1}$ in $R(\zeta_f)$, where $f = \text{lcm}_{g \in G}\{\text{order }(g)\}$. Let

$$\Xi = [\xi_D^{j-1}(i)], \qquad i = 1, \ldots, v-1, \; j = 1, \ldots, v-1.$$

Suppose that there are exactly ρ_D distinct values among

$$\{\xi_D(s) | \, 1 \leqq s \leqq v-1\}.$$

Let them be $\xi_D(i_1), \xi_D(i_2), \ldots, \xi_D(i_{\rho_D})$. Now, clearly, rank $(\Xi) \leqq \rho_D$. However, the $\rho_D \times \rho_D$ submatrix

$$\Xi_{\rho_D} = [\xi_D^{j-1}(i_r)], \qquad r = 1, \ldots, \rho_D, \; j = 1, \ldots, \rho_D,$$

is a non-singular Vandermonde matrix; hence, $\text{rank}(\Xi) \geqq \rho_D$. Thus, $\text{rank}(\Xi) = \rho_D$. Since the rank of Ξ is attained by the non-singular submatrix Ξ_{ρ_D}, the system of ρ_D linear equations

$$\xi_D'(i_r) = b_1 + b_2\xi_D(i_r) + \ldots + b_{\rho_D}\xi_D^{\rho_D - 1}(i_r), \qquad 1 \leqq r \leqq \rho_D, \tag{3.2}$$

has a unique solution for $b_1, b_2, \ldots, b_{\rho_D}$ in $R(\zeta_f)$. Now, by (2.4), (3.2) becomes

$$k - \lambda = b_1\xi_D(i_r) + b_2\xi_D^2(i_r) + \ldots + b_{\rho_D}\xi_D^{\rho_D}(i_r), \qquad 1 \leqq r \leqq \rho_D. \tag{3.3}$$

Applying Cramer's rule to (3.3) to find b_{ρ_D} we obtain

$$b_{\rho_D} = (-1)^{\rho_D - 1}(k-\lambda) \Big/ \prod_{r=1}^{\rho_D} \xi_D(i_r) \neq 0. \tag{3.4}$$

We have thus shown the following result.

THEOREM 3.1. *Let* (G, D) *be an AGDS, where* $f = \text{lcm}_{g\in G}\{\text{order}(g)\}$ and ρ_D *is the number of distinct values among* $\{\xi_D(s) \mid 1 \leqq s \leqq v-1\}$. *Then there exists a unique polynomial* $q_D(x) = b_1 + b_2 x + \ldots + b_{\rho_D} x^{\rho_D - 1}$, $b_{\rho_D} \neq 0$, *with coefficients in* $R(\zeta_f)$ *and of lowest degree for which*

$$\xi_D'(s) = q_D(\xi_D(s)), \qquad 1 \leqq s \leqq v-1. \tag{3.5}$$

Now consider the representation of G as a direct product of cyclic groups,

$$G = C(e_1) \otimes \ldots \otimes C(e_n), \tag{3.6}$$

where $C(e_i)$ is cyclic of order e_i, $1 \leqq i \leqq n$, $e_i \mid e_{i+1}$ for $1 \leqq i \leqq n-1$, and $v = \prod_{i=1}^{n} e_i$, where $e_n = f$. Let $g_{(i)}$ be a generator of $C(e_i)$, $1 \leqq i \leqq n$. Corresponding to (3.6) we have a representation of Γ as a direct product of cyclic groups,

$$\Gamma = K(e_1) \otimes \ldots \otimes K(e_n), \tag{3.7}$$

where $K(e_i)$ is cyclic of order e_i, $1 \leqq i \leqq n$, and where we may take $\chi_{(j)}$ as a generator of $K(e_j)$, $1 \leqq j \leqq n$, where

$$\chi_{(j)}(g_{(i)}) = \begin{cases} \zeta_{e_j}, & i = j, \\ 1, & i \neq j, \end{cases} \qquad 1 \leqq i \leqq n,\ 1 \leqq j \leqq n. \tag{3.8}$$

Now if $g \in G$ has the representation $g = g_{(1)}^{\gamma_1} \ldots g_{(n)}^{\gamma_n}$, then we will set $\Delta_D(\gamma_1, \ldots, \gamma_n) \equiv \Delta_D(g)$, and if $\chi_s \in \Gamma$ has the representation

$$\chi_s = \chi_{(1)}^{\sigma_1} \ldots \chi_{(n)}^{\sigma_n},$$

then we will set $\xi_D(\sigma_1, \ldots, \sigma_n) \equiv \xi_D(s)$, where we always take the exponents of $g_{(i)}$ and $\chi_{(i)}$ as non-negative integers modulo e_i, $1 \leqq i \leqq n$. Thus, with this new notation, (2.2) becomes

$$\xi_D(\sigma_1, \ldots, \sigma_n) = \sum_{\gamma_1=0}^{e_1-1} \ldots \sum_{\gamma_n=0}^{e_n-1} \Delta_D(\gamma_1, \ldots, \gamma_n) \prod_{j=1}^{n} \zeta_{e_j}^{\sigma_j \gamma_j}, \qquad 0 \leqq \sigma_i \leqq e_i - 1,\ 1 \leqq i \leqq n. \tag{3.9}$$

Now $e_i | e_n = f$, hence, let $e_i u_i = f$ whence $\zeta_{e_i} = \zeta_f^{u_i}$, $1 \leqq i \leqq n$. Then (3.9) becomes

$$\xi_D(\sigma_1, \ldots, \sigma_n) = \sum_{\gamma_1=0}^{e_1-1} \ldots \sum_{\gamma_n=0}^{e_n-1} \Delta_D(\gamma_1, \ldots, \gamma_n) \exp\left(2\pi \mathbf{i} \sum_{j=1}^{n} \sigma_j \gamma_j u_j / f\right), \qquad 0 \leqq \sigma_i \leqq e_i - 1,\ 1 \leqq i \leqq n. \tag{3.10}$$

LEMMA 3.2. *Let* (G, D) *be an ADGS, where* $f = 1\text{cm}_{g\in G}\{\text{order}(g)\}$ *and* $\xi_D(i_1), \ldots, \xi_D(i_{\rho_D})$ *are the distinct values among* $\{\xi_D(s) \mid 1 \leqq s \leqq v-1\}$. *Then the polynomial*

$$Q_D(x) = \prod_{\tau=1}^{\rho_D} (x - \xi_D(i_\tau))$$

has rational integral coefficients.

https://doi.org/10.4153/CJM-1968-124-2 Published online by Cambridge University Press

Proof. Now $\xi_D(\sigma_1, \ldots, \sigma_n) \in R(\zeta_f)$. The automorphisms of $R(\zeta_f)$ fixing R elementwise are all of the form

$$\phi_w: \zeta_f \to \zeta_f^{\,w}, \qquad 1 \leqq w \leqq f,\ \gcd(w, f) = 1. \tag{3.11}$$

Under such an automorphism we have

$$\phi_w: \exp\left(2\pi\mathbf{i}\sum_{j=1}^{n} \sigma_j\gamma_j u_j/f\right) \to \exp\left(2\pi\mathbf{i}\sum_{j=1}^{n} (w\sigma_j)\gamma_j u_j/f\right),$$

whence by (3.10),

$$\phi_w: \xi_D(\sigma_1, \ldots, \sigma_n) \to \xi_D(w\sigma_1, \ldots, w\sigma_n), \qquad \gcd(w, e_i) = 1,\ 1 \leqq i \leqq n, \tag{3.12}$$

which means that ϕ_w induces a permutation on the set of values

$$\xi_D(i_1), \ldots, \xi_D(i_{\rho_D}).$$

But then the coefficients of the polynomial

$$Q_D(x) = \prod_{r=1}^{\rho_D} (x - \xi_D(i_r))$$

are invariant under all automorphisms of $R(\zeta_f)$ fixing R elementwise; hence these coefficients must be in R. Since these coefficients are also algebraic integers, they are, in fact, rational integers. This proves the lemma.

We can now obtain some additional information about the polynomial $q_D(x)$ in Theorem 3.1.

THEOREM 3.3. *The coefficients of* $q_D(x) = b_1 + b_2 x + \ldots + b_{\rho_D} x^{\rho_D - 1}$ *are rational and of the form*

$$b_i = c_i(k - \lambda)^{-\frac{1}{2}(\rho_D - 2)},$$

where c_i *is a rational integer*, $1 \leqq i \leqq \rho_D$, *and* $c_{\rho_D} = \epsilon = \pm 1$.

Proof. The polynomial $b_{\rho_D}^{-1}(xq_D(x) - (k - \lambda))$ is monic of degree ρ_D and has $\xi_D(i_1), \ldots, \xi_D(i_{\rho_D})$ as roots, hence by Lemma 3.2,

$$b_{\rho_D}^{-1}(xq_D(x) - (k - \lambda)) = Q_D(x)$$

or

$$-\frac{(k-\lambda)}{b_{\rho_D}} + \left(\frac{b_1}{b_{\rho_D}}\right)x + \ldots + \left(\frac{b_{\rho_D - 1}}{b_{\rho_D}}\right)x^{\rho_D - 1} + x^{\rho_D} = c_0' + c_1' x + \ldots + c_{\rho_D - 1}' x^{\rho_D - 1} + x^{\rho_D}, \tag{3.13}$$

where $c_0', \ldots, c_{\rho_D - 1}'$ are rational integers. Now, by (3.4),

$$|b_{\rho_D}| = (k - \lambda)^{-\frac{1}{2}(\rho_D - 2)}$$

whence

$$b_{\rho_D} = \epsilon(k - \lambda)^{-\frac{1}{2}(\rho_D - 2)}, \qquad \epsilon = \pm 1. \tag{3.14}$$

By (3.13), $b_{\rho_D} = -(k - \lambda)/c_0'$ which is rational. Again, by (3.13) and (3.14),

$$b_i = b_{\rho_D} c_i' = \epsilon c_i'(k - \lambda)^{-\frac{1}{2}(\rho_D - 2)} = c_i(k - \lambda)^{-\frac{1}{2}(\rho_D - 2)}$$

is rational, where $c_i = \epsilon c_i'$ is a rational integer, $1 \leqq i \leqq \rho_D - 1$.

COROLLARY 3.4. *If an AGDS (G, D) exists, then either ρ_D is even or $k - \lambda$ is the square of a rational integer.*

Proof. By Theorem 3.3, $b_{\rho_D} = \epsilon(k - \lambda)^{-\frac{1}{2}(\rho_D - 2)}$ is rational. Thus, if ρ_D is odd, then $k - \lambda$ must be the square of a rational integer.

LEMMA 3.5. *If an AGDS (G, D) exists, then $\rho_D \geqq 2$.*

Proof. Now $\rho_D \geqq 1$. Suppose that $\rho_D = 1$. Then, by Corollary 3.4, $k - \lambda$ is a rational integral square, m^2, where $m > 0$ is an integer. By Theorem 3.3, $b_1 = \epsilon\sqrt{(k - \lambda)} = \epsilon m$, $\epsilon = \pm 1$, whence by Theorem 3.1

$$\xi_D(s) = \epsilon m, \qquad 1 \leqq s \leqq v - 1,$$

or

$$\sum_{g \in G} \Delta_D(g)\chi_s(g) = \epsilon m, \qquad 1 \leqq s \leqq v - 1. \tag{3.15}$$

Now, multiplying both sides of (3.15) by $\chi_s(g_*^{-1})$, $g_* \in G$, and summing on s, we obtain:

$$\Delta_D(g_*) = v^{-1}(k - \epsilon m) + \epsilon m \delta(g_*, e). \tag{3.16}$$

By (3.16) we must have $v \mid k \pm m$. Since $0 < k - m < v$ we cannot have $v \mid k - m$. Hence $v \mid k + m$ and thus $v \leqq k + m$. Now

$$(k + m)(k - m) = k^2 - k + \lambda = v\lambda,$$

whence $\lambda \geqq k - m$ or $\sqrt{(k - \lambda)} = m \geqq k - \lambda$, which is impossible for $k - \lambda > 1$. Hence $\rho_D = 1$ is impossible, whence $\rho_D \geqq 2$.

We now consider the special case where $\rho_D = 2$.

THEOREM 3.6. *Let (G, D) be an AGDS for which $\rho_D = 2$. Then $q_D(x)$ is either x, $-1 - x$, or $1 - x$. Furthermore,*

(i) *$q_D(x) = x$ if and only if $\Delta_D(g^{-1}) = \Delta_D(g)$ for all $g \in G$ (i.e., if and only if (G, D) is an IMAGDS, where $D^\iota = D$);*

(ii) *$q_D(x) = -1 - x$ if and only if $\Delta_D(e) = 0$ and $\Delta_D(g^{-1}) + \Delta_D(g) = 1$ for all $g \in G$, $g \neq e$ (i.e., if and only if (G, D) is an SHAGDS);*

(iii) *$q_D(x) = 1 - x$ if and only if $\Delta_D(e) = 1$ and $\Delta_D(g^{-1}) + \Delta_D(g) = 1$ for all $g \in G$, $g \neq e$ (i.e., if and only if (G, D) is a co-SHAGDS).*

Remark. By a theorem of McFarland and Mann (**4**), every multiplier of an AGDS fixes some translate of the AGDS. Hence, every IMAGDS is a translate of an IMAGDS (G, D), where $D^\iota = D$.

Proof. For $\rho_D = 2$ we have, by Theorem 3.3, that $q_D(x) = c_1 + \epsilon x$, where c_1 is a rational integer and $\epsilon = \pm 1$.

Case 1. $\epsilon = +1$. Here $\xi_D'(s) = c_1 + \xi_D(s)$, $1 \leqq s \leqq v-1$. However, $\xi_D'(s) = \bar{\xi}_D(s)$; hence, $\mathrm{Re}(\xi_D'(s)) = \mathrm{Re}(\xi_D(s))$, whence $c_1 = 0$ and $q_D(x) = x$. Thus, $\xi_D'(s) = \xi_D(s)$ or

$$(3.17) \qquad \sum_{g \in G} \Delta_D(g^{-1})\chi_s(g) = \sum_{g \in G} \Delta_D(g)\chi_s(g), \qquad 1 \leqq s \leqq v-1.$$

Multiplying both sides of (3.17) by $\chi_s(g_*^{-1})$, $g_* \in G$, and summing on s, we obtain $\Delta_D(g_*^{-1}) = \Delta_D(g_*)$ for all $g_* \in G$. Hence, (G, D) is an IMAGDS, where $D^\iota = D$. The converse is trivial.

Case 2. $\epsilon = -1$. Here $\xi_D'(s) = c_1 - \xi_D(s)$ or

$$(3.18) \qquad \sum_{g \in G} \Delta_D(g^{-1})\chi_s(g) = c_1 - \sum_{g \in G} \Delta_D(g)\chi_s(g), \qquad 1 \leqq s \leqq v-1.$$

Multiplying both sides of (3.18) by $\chi_s(g_*^{-1})$, $g_* \in G$, and summing on s, we obtain

$$\Delta_D(g_*^{-1}) + \Delta_D(g_*) = v^{-1}(2k - c_1) + c_1\delta(g_*, e),$$

or

$$(3.19) \qquad \Delta_D(g_*^{-1}) + \Delta_D(g_*) = v^{-1}(2k - c_1), \qquad g_* \neq e,$$

and

$$(3.20) \qquad 2\Delta_D(e) = v^{-1}(2k - c_1) + c_1.$$

Now we cannot have $\Delta_D(g_*^{-1}) + \Delta_D(g_*) = 0$ for all $g_* \in G$, $g_* \neq e$, or $\Delta_D(g_*^{-1}) + \Delta_D(g_*) = 2$ for all $g_* \in G$, $g_* \neq e$, for otherwise, D would have either 0, 1, $v-1$, or v elements, contradicting $0 < \lambda < k < v-1$. Hence, $\Delta_D(g_*^{-1}) + \Delta_D(g_*) = 1$ for all $g_* \in G$, $g_* \neq e$, whence by (3.19), $c_1 = 2k - v$. Then by (3.20) we have that $2\Delta_D(e) = 2k + 1 - v$. Thus, $v = 2k+1$, whence $c_1 = -1$ and $q_D(x) = -1 - x$ for $\Delta_D(e) = 0$, and $v = 2k-1$, whence $c_1 = 1$ and $q_D(x) = 1 - x$ for $\Delta_D(e) = 1$. In the first case, (G, D) is an SHAGDS and in the latter case, (G, D) is a co-SHAGDS. The converse in each case is easily verified.

4. A further result. If (G, D) is an AGDS of one of the types given in Theorem 3.6 and $E = D^\omega$ under the automorphism ω of G, then it is not difficult to show that (G, E) is of the same type as (G, D). This is, in fact, a special case of the following more general result.

THEOREM 4.1. *Let (G, D) and (G, E) be two AGDSs and let $E = D^\omega$ under the automorphism ω of G. Then $q_E(x) = q_D(x)$.*

Proof. Now

$$(4.1) \qquad \xi_E(s) = \sum_{g \in G} \Delta_E(g)\chi_s(g), \qquad 1 \leqq s \leqq v-1,$$

where

$$(4.2) \qquad \Delta_E(g) = \begin{cases} 1, & (g)\omega^{-1} \in D \\ 0, & (g)\omega^{-1} \notin D \end{cases} = \Delta_D((g)\omega^{-1}).$$

Hence, letting $\tilde{g} = (g)\omega^{-1}$ or $g = (\tilde{g})\omega$, we obtain, from (4.1) and (4.2),

$$\xi_E(s) = \sum_{\tilde{g} \in G} \Delta_D(\tilde{g})\chi_s((\tilde{g})\omega), \qquad 1 \leqq s \leqq v - 1. \tag{4.3}$$

Now, for all $g \in G$, we define

$$\theta_s(g) \equiv \chi_s((g)\omega), \qquad 1 \leqq s \leqq v - 1.$$

Then $\theta_s(g) \neq 0$ and $\theta_s(g) \in R(\zeta_f)$ for all $g \in G$, where $f = \mathrm{lcm}_{g \in G}\{\mathrm{order}(g)\}$. Furthermore, for all $g_1, g_2 \in G$ and all s, $1 \leqq s \leqq v - 1$,

$$\theta_s(g_1g_2) = \chi_s((g_1g_2)\omega) = \chi_s((g_1)\omega \cdot (g_2)\omega) = \chi_s((g_1)\omega) \cdot \chi_s((g_2)\omega) = \theta_s(g_1) \cdot \theta_s(g_2),$$

hence θ_s is a character on G or $\theta_s = \chi_{t_s}$ for some t_s, $0 \leqq t_s \leqq v - 1$. If $t_s = 0$ so that $\theta_s = \chi_0$, then $\chi_s = \chi_0$, which is impossible since $1 \leqq s \leqq v - 1$; hence, $1 \leqq t_s \leqq v - 1$ for all s, $1 \leqq s \leqq v - 1$. Thus by (4.3),

$$\xi_E(s) = \sum_{\tilde{g} \in G} \Delta_D(\tilde{g})\chi_{t_s}(\tilde{g}) = \xi_D(t_s), \qquad 1 \leqq s \leqq v - 1,\ 1 \leqq t_s \leqq v - 1, \tag{4.4}$$

which states that every value in $\{\xi_E(s) | 1 \leqq s \leqq v - 1\}$ is a value in $\{\xi_D(s) | 1 \leqq s \leqq v - 1\}$. Writing $D = E^{\omega^{-1}}$ and interchanging the roles of D and E in the above argument, we see that every value in $\{\xi_D(s) | 1 \leqq s \leqq v - 1\}$ is a value in $\{\xi_E(s) | 1 \leqq s \leqq v - 1\}$. Hence, the distinct values in

$$\{\xi_E(s) | 1 \leqq s \leqq v - 1\}$$

are the same as those in $\{\xi_D(s) | 1 \leqq s \leqq v - 1\}$, whence $\rho_E = \rho_D$. Furthermore,

$$\xi_E'(s) = \xi_D'(t_s) = q_D(\xi_D(t_s)) = q_D(\xi_E(s)), \qquad 1 \leqq s \leqq v - 1. \tag{4.5}$$

Now, by Theorem 3.1, the polynomial $q_E(x)$ of degree $\rho_E - 1$ for which $\xi_E'(s) = q_E(\xi_E(s))$, $1 \leqq s \leqq v - 1$, is unique. Hence, by (4.5), $q_E(x) = q_D(x)$.

It is not difficult to show that the conclusion of Theorem 4.1 does not follow if we merely assume that (G, D) and (G, E) are equivalent. An example is given for $v = 7$, $k = 3$, $\lambda = 1$, and $G = \{g^i | 0 \leqq i \leqq 6\}$ (the cyclic group of order 7) by $D = \{g, g^2, g^4\}$ and $E = Dg^{-1} = \{e, g, g^3\}$. Here, $\rho_D = 2$, while $\rho_E = 6$.

References

1. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc. *78* (1955), 464–481.
2. E. C. Johnsen, *The inverse multiplier for abelian group difference sets*, Can. J. Math. *16* (1964), 787–796.
3. ——— *Skew-Hadamard abelian group difference sets*, J. Algebra *4* (1966), 388–402.
4. Robert McFarland and H. B. Mann, *On multipliers of difference sets*, Can. J. Math. *17* (1965), 541–542.
5. H. J. Ryser, *A note on a combinatorial problem*, Proc. Amer. Math. Soc. *1* (1950), 422–424.

University of California,
Santa Barbara, California