Designs, Codes and Cryptography, 4, 313–317 (1994)

An Exponent Bound On Skew Hadamard Abelian Difference Sets

YU QING CHEN, QING XIANG, AND SURINDER K. SEHGAL qxiang@magnus.acs.ohio-state.edu
Department of Mathematics, Ohio State University, Columbus OH 43210

Editor: D. Jungnickel

Received September 27, 1993; Revised December 20, 1993.

Abstract. A difference set D in a group G is called a skew Hadamard difference set (or an antisymmetric difference set) if and only if G is the disjoint union of D, $D^{(-1)}$, and $\{1\}$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$. In this note, we obtain an exponent bound for non-elementary abelian group G which admits a skew Hadamard difference set. This improves the bound obtained previously by Johnsen, Camion and Mann.

1. Introduction

We assume that the reader is familiar with the theory of difference sets as can be found in [3] and [5].

A difference set D in an abelian group G is called skew Hadamard if G is the disjoint union of D, $D^{(-1)}$, and $\{1\}$. The definition gives:

$$1 \notin D, \quad k = \frac{v-1}{2}, \quad \lambda = \frac{v-3}{4}, \quad n = \frac{v+1}{4}$$

where v is the order of the group G, and k is the size of D.

If we employ the group ring notations, then in $Z[G]$, we have

$$\begin{aligned} DD^{(-1)} &= \frac{v+1}{4} + \frac{v-3}{4}G \\ D + D^{(-1)} &= G - 1 \end{aligned}$$

Applying any non-principal character χ of G to the above two equations, one has

$$\chi(D) = \frac{-1 \pm \sqrt{-v}}{2} \tag{1}$$

This is an important property of skew Hadamard abelian difference sets of which we will make use later.

Skew Hadamard difference sets were studied by E. C. Johnsen [2], P. Camion and H. Mann [1], and also by Jungnickel [4] in connection with λ-ovals. The results of Johnsen, Camion and Mann were summarized in [3] as follows:

THEOREM A *Let D be a skew Hadamard difference set in an abelian group G. Then v is a prime power $p^m \equiv 3 (\mathrm{mod}\, 4)$, and the quadratic residues* mod v *are multipliers for*

D. Moreover, if G has exponent p^s with $s \geq 2$, then any basis of G contains at least two elements of order p^s, and hence one has $m \geq 2s+1$. In particular, if $v = p^3$ for a prime p, then G is elementary abelian.

The only known examples of skew Hadamard difference sets are the Paley-Hadamard difference sets formed by the (nonzero) quadratic residues in GF(q), where q is a prime power congruent to 3(mod 4) (see [7]). It is conjectured that there are no further examples. The exponent bound in Theorem A can be viewed as evidence for this conjecture. In this note, we obtain an exponent bound which improves the one in Theorem A. In particular, we prove that if $v = p^5$, for a prime p congruent to 3(mod 4), then G is elementary abelian.

2. Main Results

In this section, we first prove a result concerning subsets D in abelian p-groups with the property that $D + D^{(-1)} = G - 1$ and $D^{(t)} = D$ for any nonzero quadratic residue t of (mod p), then we will use it to get a new exponent bound on skew Hadamard difference sets.

LEMMA 2.1 *Let G be an abelian p-group of order p^m, where p is a prime, $p \equiv 3 (\mathrm{mod}\, 4)$, m is a positive integer, and let $D \subset G$. Suppose that $D + D^{(-1)} = G - 1$, $D^{(t)} = D$ for any nonzero quadratic residue t* (mod p). *Then*

(1) *There exists a non-principal character χ of G such that $\chi(D) \not\equiv \frac{p^{[\frac{m+1}{2}]}-1}{2} (\mathrm{mod}\, p^{[\frac{m+1}{2}]})$.*

(2) *If m is odd, and for any non-principal character χ of G, $\chi(D) \equiv \frac{p^{\frac{m-1}{2}}-1}{2} (\mathrm{mod}\, p^{\frac{m-1}{2}})$, then D is a difference set in G.*

Proof: Since $D^{(t)} = D$, for any nonzero quadratic residue t (mod p), and note that t is a quadratic residue mod p if and only if it is a quadratic residue mod p^m, we have $\sigma_t(\chi(D)) = \chi(D)$, where σ_t is the Galois automorphism $\xi_{p^m} \mapsto \xi_{p^m}^t$, ξ_{p^m} is a primitive p^m-th root of unity, χ is any non-principal character of G, by Galois theory, we have $\chi(D) \in Z[\omega]$, where $\omega = (-1+\sqrt{-p})/2$ and $Z[\omega]$ is the integer ring of $Q(\sqrt{-p})$ (see [6]). Assume that $\chi(D) = a_\chi + b_\chi\omega$, $a_\chi, b_\chi \in Z$. Since $D + D^{(-1)} = G - 1$, applying χ to this equation, we get $\chi(D) + \chi(D^{(-1)}) = -1$. Therefore $2a_\chi + 1 = b_\chi$ and hence $\chi(D) = (-1 + (2a_\chi + 1)\sqrt{-p})/2$.

If $\chi(D) \equiv (p^{[\frac{m+1}{2}]} - 1)/2 (\mathrm{mod}\, p^{[(m+1)/2]})$, for any non-principal character χ of G, then $p^{[(m+1)/2]} \mid (2a_\chi + 1)$. Let $2a_\chi + 1 = p^{[\frac{m+1}{2}]}c_\chi$, where c_χ is a non-zero integer. We have

$$\chi(D)\chi(D^{(-1)}) = \frac{1 + p^{2[\frac{m+1}{2}]+1}c_\chi^2}{4}$$

Calculating the coefficient of 1 in $DD^{(-1)}$ in two ways, one by Fourier inversion formula (see [3]), the other by direct calculation, we have

$$\frac{p^m-1}{2}=\frac{1}{p^m}\left(\frac{(p^m-1)^2}{4}+\frac{p^m-1+p^{2[\frac{m+1}{2}]+1}\sum_{\chi\neq\chi_0}c_\chi^2}{4}\right)$$

Simplifying this equation,

$$p^m(p^m-1)=p^{2[\frac{m+1}{2}]+1}\sum_{\chi\neq\chi_0}c_\chi^2.$$

But, this is impossible because $2[\frac{m+1}{2}]+1\geq m+1$, we thus deduce a contradiction. This finishes the proof of (1).

For the proof of (2), we simply let $2a_\chi+1=p^{\frac{m-1}{2}}d_\chi$, then

$$\chi(D)\chi(D^{(-1)})=\frac{1+p^md_\chi^2}{4}.$$

Similarly,by calculating the coefficient of 1 in $DD^{(-1)}$ in two ways, we have

$$p^m(p^m-1)=p^m\sum_{\chi\neq\chi_0}d_\chi^2$$

This forces $d_\chi^2=1$ for all $\chi\neq\chi_0$. Hence $\chi(D)\chi(D^{(-1)})=\frac{1+p^m}{4}$, for all $\chi\neq\chi_0$. By Fourier inversion formula, D is a skew Hadamard difference set in G. This completes the proof. ■

LEMMA 2.2 *Let $G=Z_{p^m}\times Z_{p^n}$, where m,n are positive integers, p is a prime, $p\equiv 3(\mathrm{mod}\,4)$, and let $D\subset G$. If $D+D^{(-1)}=G-1$, $D^{(t)}=D$ for any t, $t\equiv a^2(\mathrm{mod}\,p)$, for some a, $(a,p)=1$, then there is a non-principal character χ of G such that $\chi(D)\not\equiv\frac{p-1}{2}(\mathrm{mod}\,p)$.*

Proof: Define $\phi: G\to G$ via $x\mapsto x^p$. It is easy to see that ϕ is a homomorphism and $K=Ker\phi\cong Z_p\times Z_p$. Let $D_0=D-D\cap K$. Then $D_0^{(t)}=D_0$ for any t, $t\equiv a^2(\mathrm{mod}\,p)$, for some a, $(a,p)=1$. Noting that D_0 has no element of order p, we have

$$D_0=\cup_x\cup_{1\leq i\leq p-1,\left(\frac{i}{p}\right)=1}x^i\langle x^p\rangle,$$

where x runs through a complete set of representatives of the orbits of D_0 under $\{t\mid t\equiv a^2(\mathrm{mod}\,p)$, for some a, $(a,p)=1\}$, and $\langle x^p\rangle\neq\{1\}$.

Since $\chi(\langle x^p\rangle)=0$ if χ is non-principal on $\langle x^p\rangle$, and $\chi(\langle x^p\rangle)=|\langle x^p\rangle|$ if χ is principal on $\langle x^p\rangle$, we have $\chi(D_0)\equiv 0(\mathrm{mod}\,p)$, for any non-principal character χ of G. If for any $\chi\neq\chi_0$, $\chi(D)\equiv\frac{p-1}{2}(\mathrm{mod}\,p)$, then $\chi(D\cap K)\equiv\frac{p-1}{2}(\mathrm{mod}\,p)$, for any $\chi\neq\chi_0$. But this contradicts (1) of Lemma 2.1, therefore, there is a non-principal character χ of G such that $\chi(D)\not\equiv\frac{p-1}{2}(\mathrm{mod}\,p)$. This completes the proof. ■

Now we are in the position to state the main theorem.

THEOREM 2.1 *Let G be an abelian p-group for some prime $p \equiv 3 (\mathrm{mod}\, 4)$, and let $|G| = p^m$, $\exp G = p^s$. If G admits a skew Hadamard difference set D, and $s \geq 2$, then $s \leq \frac{m+1}{4}$.*

Proof: By Theorem A, we can assume that $G = G' \times Z_{p^s} \times Z_{p^s}$. By equation (1), if $\chi \neq \chi_0$, then

$$\begin{aligned} \chi(D) &= \frac{-1 \pm \sqrt{-p^m}}{2} \\ &= \frac{p^{\frac{m-1}{2}} - 1}{2} + p^{\frac{m-1}{2}} \frac{-1 \pm \sqrt{-p}}{2} \end{aligned}$$

Let $D_1 = D \cap (Z_{p^s} \times Z_{p^s})$, $G' = \{g_1 = 1, g_2, \ldots, g_l\}$. Then

$$D = D_1 + D_2 g_2 + \cdots + D_l g_l \tag{2}$$

where $D_i \subset Z_{p^s} \times Z_{p^s}$, $i = 1, 2, \ldots, l$.

For each non-principal character χ' of $Z_{p^s} \times Z_{p^s}$, we can extend it to G in l ways, assume the extensions are $\chi_1', \chi_2', \ldots \chi_l'$, then $\{\chi_i' |_{G'}, i = 1, 2, \ldots, l\} = (G')^*$.

Applying these characters to equation (2), one has

$$\begin{aligned} \chi_1'(D) &= \chi'(D_1) + \chi'(D_2)\chi_1'(g_2) + \cdots + \chi'(D_l)\chi_1'(g_l) \\ \chi_2'(D) &= \chi'(D_1) + \chi'(D_2)\chi_2'(g_2) + \cdots + \chi'(D_l)\chi_2'(g_l) \\ &\cdots \\ \chi_l'(D) &= \chi'(D_1) + \chi'(D_2)\chi_l'(g_2) + \cdots + \chi'(D_l)\chi_l'(g_l) \end{aligned}$$

Since $\sum_{i=1}^{l} \chi_i'(g_j) = 0$, $j = 2, 3, \ldots, l$, we get

$$\begin{aligned} |G'|\chi'(D_1) &= \sum_{i=1}^{l} \chi_i'(D) \\ &= |G'| \frac{p^{\frac{m-1}{2}} - 1}{2} + p^{\frac{m-1}{2}} \delta \end{aligned}$$

where $\delta \in Z[\omega]$. Therefore

$$\chi'(D_1) = \frac{p^{\frac{m-1}{2}} - 1}{2} + \frac{p^{\frac{m-1}{2}}}{|G'|} \delta$$

Noting that $|G'| = p^{m-2s}$, one has

$$\chi'(D_1) = \frac{p^{\frac{m-1}{2}} - p}{2} + p^{2s - \frac{m+1}{2}} \delta + \frac{p-1}{2}.$$

By the definition of skew Hadamard difference set, and Theorem A, it is easy to see that D_1 satisfies the hypotheses of Lemma 2.2, so by Lemma 2.2, there is a non-principal character

χ' of $Z_{p^s} \times Z_{p^s}$ such that $\chi'(D_1) \not\equiv \frac{p-1}{2} (\mathrm{mod}\ p)$, therefore $2s - \frac{m+1}{2} \leq 0$, so $s \leq \frac{m+1}{4}$. This completes the proof. ■

COROLLARY 2.2 *If an abelian group G admits a skew Hadamard difference set, and* $|G| = p^5$, *then G is elementary abelian.*

The proof of this corollary is immediate from Theorem 2.1 by letting $m = 5$.

COROLLARY 2.3 *If G is an abelian group which admits a skew Hadamard difference set, and G is not elementary abelian, then p-rank*$(G) \geq 4$.

This is an immediate consequence of Theorem 2.1.

In view of Theorem 2.1, the first open cases for testing whether an abelian p-group admits a skew Hadamard difference set or not are: $G = Z_p \times (Z_{p^2})^3$, and $G = (Z_p)^3 \times (Z_{p^2})^2$. These two cases seem to be more difficult than the case $|G| = p^5$.

Acknowledgement

The second author would like to thank Prof. D. K. Ray-Chaudhuri for his guidance and encouragement.

References

1. Camion, P., and Mann, H. B. 1972. Antisymmetric difference sets. *J. Number Theory* 4:266–268.
2. Johnsen, E. C. 1966. Skew-Hadamard abelian group difference sets. *J. Algebra* 4:388–402.
3. Jungnickel, D. 1992. Difference sets. In J. Dinitz, D. R. Stinson, editors, *Contemporary Design Theory, A Collection of Surveys*, pp. 241–324. Wiley-Interscience Series in Discrete Mathematics and Optimization. New York: Wiley.
4. Jungnickel, D. 1990. λ-ovals and difference sets. In R. Bodendieck, editor, *Contemporary Methods in Graph Theory*. Mannheim: Bibliographisches Institut.
5. Lander, E. S. 1983. *Symmetric Designs, An Algebraic Approach*. Oxford: Cambridge University Press.
6. Lang, S. 1970. *Algebraic Number Theory*. Springer-Verlag.
7. Paley, R. E. A. C. 1933. On orthogonal matrices. *J. Math. Phys. MIT* 12:311–320.