J Algebr Comb (2013) 38:785–795
DOI 10.1007/s10801-013-0425-1

On difference sets in high exponent 2-groups

Joško Mandić · Mario Osvin Pavčević · Kristijan Tabak

Received: 8 November 2011 / Accepted: 21 January 2013 / Published online: 16 February 2013

Abstract We investigate the existence of difference sets in particular 2-groups. Being aware of the famous necessary conditions derived from Turyn's and Ma's theorems, we develop a new method to cover necessary conditions for the existence of $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$ difference sets, for some large classes of 2-groups.

If a 2-group G possesses a normal cyclic subgroup $\langle x\rangle$ of order greater than 2^{d+3+p}, where the outer elements act on the cyclic subgroup similarly as in the dihedral, semidihedral, quaternion or modular groups and 2^p describes the size of $G' \cap \langle x\rangle$ or $C_G(x)' \cap \langle x\rangle$, then there is no difference set in such a group. Technically, we use a simple fact on how sums of 2^n-roots of unity can be annulated and use it to characterize properties of norm invariance (prescribed norm). This approach gives necessary conditions when a linear combination of 2^n-roots of unity remains unchanged under homomorphism actions in the sense of the norm.

Keywords Difference set · Norm invariance · Hadamard group · Modular 2-group · Group representation

J. Mandić
Faculty of Natural Sciences and Mathematics, Mathematical Department, University of Split,
Teslina 12, 21000 Split, Croatia
e-mail: Josko.Mandic@pmfst.hr

M.O. Pavčević · K. Tabak (✉)
Faculty of Electrical Engineering and Computing, Department of Applied Mathematics,
University of Zagreb, Unska 3, 10000 Zagreb, Croatia
e-mail: ktabak@acmt.hr

M.O. Pavčević
e-mail: mario.pavcevic@fer.hr

1 Introduction and known results

A (v,k,λ) difference set in a finite group G of order v is a set D, of cardinality k, such that the collection $\{d_1d_2^{-1} \mid d_1 \neq d_2,\ d_i \in D\}$ consists of λ copies of every element of $G \setminus \{1_G\}$. For given parameters v, k and λ, the existence question for a (v,k,λ) difference set is often hard to be solved and it includes approaches which are not commonly used in this theory, such as character theory or algebraic number theory. A suggested reference for further reading in this field would be [1].

If we want to determine whether an abelian difference set exists, the following classical result is very often decisive:

Lemma 1 *Let G be a finite abelian group of order v. A subset D of order k is a (v,k,λ) difference set if and only if $|\chi(D)| = \sqrt{k-\lambda}$, for every non-principal character χ of the group G.*

A more general sufficient condition for a difference set in any finite group can be stated in the group representation theory language (for proofs and examples see [3] and [6]).

Theorem 1 *Let D be a subset of size k of a group G of order v. Let S be a complete set of distinct, inequivalent, nontrivial, irreducible representations for G. If $\phi(D)\phi(D^{(-1)}) = (k-\lambda)I$ for all $\phi \in S$, then D is a (v,k,λ) difference set in G.*

Also, it can be shown that if D is a difference set, then the relation from the previous theorem is fulfilled for all nontrivial representations. In fact, this will be our main approach in testing hypothetical difference sets.

The group G of order $4u^2$, which possesses a difference set with parameters $(4u^2, 2u^2-u, u^2-u)$, is called a *Hadamard group*. The problem of existence of difference sets in 2-groups has been studied extensively in recent years, whereas the starting point can be found in Turyn [8], where the following important result was proved.

Theorem 2 *Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is cyclic. If $|H| < 2^d$, then G is not a Hadamard group.*

Using Dillon's and Ma's results (see [4]), an important claim of similar kind holds.

Theorem 3 *Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is dihedral. If $|H| < 2^d$, then G is not a Hadamard group.*

One general necessary condition on the group structure of an abelian Hadamard 2-group is that its exponent is not too large. The important result in [8] which we quote next is nowadays called the Turyn exponent bound.

Theorem 4 *If G is an abelian Hadamard group of order 2^{2s+2}, then G has exponent at most 2^{s+2}.*

Some other useful results on difference sets and 2-groups can be found in [5].

A series of non-abelian 2-groups, which are in a sense close to abelian ones, are modular groups. A modular group M_{2^n} is defined in terms of generators and relations by

$$M_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1,\ yxy = x^{2^{n-2}+1} \rangle.$$

It is easy to see that its every maximal subgroup is abelian. Note that M_{2^n} is non-abelian for $n > 2$.

The smallest non-abelian candidate is

$$M_{16} = \langle x, y \mid x^8 = y^2 = 1,\ yxy = x^5 \rangle,$$

and that group is shown to be Hadamard, because the set (written in the group ring $\mathbb{Z}[M_{16}]$)

$$1 + x + x^2 + x^5 + x^4 y + x^2 y$$

is a $(16, 6, 2)$ Hadamard difference set in M_{16}.

Dillon [2] led a research programme in order to examine which of the 267 groups of order 64 are Hadamard groups. The last stone in the complete classification was the construction of a $(64, 28, 12)$ difference set in the modular group M_{64}, found by Smith in [5]. This is indeed a very special case, because it was the first example which showed that the Turyn exponent bound cannot be extended to non-abelian groups.

Notice that in every modular group M_{2^n}, the subgroup $\langle x^{2^{n-2}}, y\rangle$ is normal of order 4. It is then easy to check that $M_{2^n}/\langle x^{2^{n-2}}, y\rangle$ is cyclic, thus by Theorem 2 we see that modular groups M_{2^n}, where $n \geq 8$, are not Hadamard. We wanted to examine next the situation in a larger class of groups. Their structure is characterized by the existence of a normal cyclic subgroup, on which the outer elements act in a way similar to the modular case. Of course, modular groups are contained in this class and we shall call this class modular type groups. We tried to carry out a construction of a difference set in a modular type group of order greater than 64 for several cases using different explicit methods. In doing so, we achieved constantly only negative results, which led us to the hypothesis that difference sets in modular type groups do not exist. One of the main results of this paper is the proof of this hypothesis.

The next (natural) step of investigation was towards dihedral type groups. Theorem 3 solves the case when a factor group is dihedral, while we had a look at the situation when there exists a normal cyclic subgroup on which the outer elements act similarly as in a dihedral group. We were able to prove that neither this class of groups allows the existence of Hadamard difference sets. A slight modification in the proofs mentioned above leads to analogous negative results for semi-dihedral and quaternion type groups.

Using the representation theory techniques, it can be shown that there is a strong link between the existence of difference sets in modular 2-groups and polynomials of the form $f(\eta) = \sum_{j=1}^{w} k_j \eta^{r_j}$, where $r_j \in \{0, 1, \ldots, 2^n - 1\}$, $r_i \neq r_j$ for $i \neq j$, $\eta = \exp(\frac{2\pi\sqrt{-1}}{2^n})$, $k_j \in \mathbb{Z}$, $n, w \in \mathbb{N}$, having the additional property that $|f(\eta^p)|$ is constant for every $p \in \mathbb{Z}$ where $\eta^p \neq 1$. Throughout the paper we shall use the standard notation

$$f\left(\eta^p\right) = \sum_{j=1}^{w} k_j \eta^{pr_j} = \left(\sum_{j=1}^{w} k_j \eta^{r_j}\right)^{(p)}.$$

Definition 1 Let η be a root of unity and $f(\eta) = \sum_{j=1}^{w} k_j \eta^{r_j} \in \mathbb{Z}[\eta]$. If there is some c, such that $|f(\eta^p)| = c$, for all integers p where $\eta^p \neq 1$, then we say that $f(\eta)$ is *norm invariant.*

2 Norm invariant polynomials

In the following result we manage to find out more about the nature of zero-sums of 2-roots of unity. More precisely, we prove that in order to achieve a zero-sum of 2-roots, it is necessary to do it in the simplest way, i.e. the only possibility is to force a cancellation in pairs. It is obvious that this is definitely one way to create a zero-sum, but surprisingly, it is also the only way.

Theorem 5 *Let* $\varepsilon = \exp(\frac{2\pi\sqrt{-1}}{2^k})$, $k \geq 1$. *Suppose that*

$$\varepsilon^{\alpha_1} + \varepsilon^{\alpha_2} + \cdots + \varepsilon^{\alpha_l} = 0,$$

where α_i*'s need not to be mutually different. Then* l *is even and there is a partition of the multiset* $\{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ *in* 2*-element subsets* $\{\alpha_i, \alpha_j\}$ *such that*

$$\varepsilon^{\alpha_i} + \varepsilon^{\alpha_j} = 0.$$

Proof Let $f(x) = x^{\alpha_1} + x^{\alpha_2} + \cdots + x^{\alpha_l}$. Then $g(x) = x^{2^{k-1}} + 1$ is the minimal polynomial for the algebraic number ε. We have assumed that ε is a root of $f(x)$, therefore $g(x)$ divides $f(x)$. Thus $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$ with nonnegative coefficients, thus we have proved our assertion. □

Next we want to find out when a polynomial $f(\eta)$ is norm invariant. First, we need one classical result (for example see [7]).

Lemma 2 *Let* A *be an element of the group ring* $\mathbb{Z}[G]$, *where* G *is an abelian group. Let* χ *be a character of* G *of order* w. *Let a prime* p *be self-conjugate modulo* w, *i.e.* $p^j \equiv -1 \pmod{w'}$ *for some* $j \in \mathbb{N}$ *where* $m = p^a w'$, w' *not divisible by* p. *If* $\chi(A)\overline{\chi(A)} \equiv 0 \pmod{p^{2i}}$, *then* $\chi(A) \equiv 0 \pmod{p^i}$.

Now, we can present our main technical result which is broadly used in the introduced norm invariance method.

Theorem 6 *Let* $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ *be a norm invariant polynomial of norm* 2^d *where* $q = 2^d(2^{d+1} - 1)$ *and* η *is a root of unity of order* 2^{2d+2}. *Let* $2^n = \max\{o(\eta^{r_i})\}$. *Then for every* $k = 0, 1, 2, \ldots, n-1$ *there is an* $r_{(k)} \in \mathbb{Z}$ *such that* $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. *We call such polynomials* $f(\eta^{2^k})$ *maximally abbreviated.*

Proof Let $G = \langle x\rangle \cong \mathbb{Z}_{2^{2d+2}}$ and let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a polynomial satisfying conditions of the theorem. Then

$$f(\eta)\overline{f(\eta)} = 2^{2d}.$$

Notice that $f(\eta)$ can be seen as

$$f(\eta) = \chi(A),$$

where

$$A = x^{r_1} + \cdots + x^{r_q} \in \mathbb{Z}[G],$$

while χ is a character of order 2^{2d+2}. Therefore

$$\chi(A)\overline{\chi(A)} \equiv 0 \pmod{2^{2d}}.$$

Using the notation from Lemma 2, we have $w = 2^{2d+2}$, $p = 2$. Furthermore $w = p^{2d+2}w'$, where $w' = 1$. It is obvious that $p^j \equiv -1 \pmod{w'}$. By Lemma 2 we have

$$\chi(A) = f(\eta) \equiv 0 \pmod{2^d}.$$

Thus, $f(\eta)$ is of the form $f(\eta) = 2^d X$, where $X = \eta^{s_1} + \cdots + \eta^{s_{q_1}}$. From here it is necessary that

$$\left|\eta^{s_1} + \cdots + \eta^{s_{q_1}}\right| = 1.$$

Assume that in X there are no two roots which can be abbreviated, i.e. there are no two distinct $i, j \in \{1, 2, \ldots, q_1\}$ such that $\eta^{s_i} + \eta^{s_j} = 0$, and that $q_1 \geq 2$. Then

$$|X|^2 = \sum_{i,j=1}^{q_1} \eta^{s_i - s_j} = 1.$$

From here we can write

$$\sum_{i\neq j}^{q_1} \eta^{s_i - s_j} + q_1 - 1 = 0.$$

Since $q_1 - 1 \geq 1$, by Theorem 5, it is necessary that $\sum_{i\neq j} \eta^{s_i - s_j}$ has at least one copy of -1. Assume that $\eta^{s_1 - s_2} = -1$, then $\eta^{s_1} + \eta^{s_2} = 0$, but that is a contradiction with our assumption. Thus $q_1 = 1$ and $f(\eta) = 2^d \eta^{s_1}$. □

3 Modular type groups

Denote standardly by $\Phi(G)$ the Frattini subgroup of G, which is the intersection of all maximal subgroups of G. Recall that elements $g \in G \setminus \Phi(G)$ are generators of the group G.

In this section we define groups which are, in some sense, a generalization of modular groups.

Definition 2 Let G be a group of order 2^{2d+2}, and let $\langle x\rangle$ be its normal cyclic subgroup of order 2^t, where x is a generator. If every $g \in G$ acts on x like $x^g = x$ or $x^g = xx^{2^{t-1}}$, then the group G will be called a modular type group and such an $x \in G$ will be called a modular generator.

Theorem 7 *Let G be a modular type group of order 2^{2d+2}, $d \geq 3$, let $x \in G$ be a modular generator and $G' \cap \langle x\rangle \leq \langle x^{2^{t-p}}\rangle$, where $p \in \{1, 2, \dots, t-1\}$. If $|\langle x\rangle| \geq 2^{d+3+p}$, then G is not a Hadamard group.*

Proof Suppose that G possesses a Hadamard difference set D with parameters

$$(v, k, \lambda) = \bigl(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d\bigr),$$

and additionally assume that $o(x) = 2^t$, $t \geq d + 3 + p$.

We may assume that D is of the form

$$D = \sum_{i=1}^{a} x^{n_i} + \sum_{j=1}^{r} \Biggl(\sum_{s=1}^{t_j} x^{m_{j_s}}\Biggr) g_j \tag{1}$$

where g_j are coset representatives of $G/\langle x\rangle$, $\langle x\rangle g_j \neq \langle x\rangle$. Obviously, $r \leq [G : \langle x\rangle] - 1$. Notice that it is always possible to achieve that $D \cap \langle x\rangle \neq \emptyset$.

Observe that (modulo 2^t)

$$n_{i_1} \neq n_{i_2}, \quad i_1 \neq i_2.$$

For a fixed j, m_{j_s} are mutually different and $z = x^{2^{t-1}} \in Z(G)$.

Let ε be a root of unity of order 2^t and let $w = 1, 2, \dots, 2^{t-p}$. Since G/G' is abelian and xG' is its generator we have

$$G/G' = \bigl\langle xG'\bigr\rangle \times A$$

for some abelian group $A \leq G/G'$. There is a natural epimorphism $\varphi : G \to G/G'$ defined by $\varphi(g) = gG'$. Let θ_w be a character of G/G' defined by

$$\theta_w\bigl(x^i G', a\bigr) = \varepsilon^{2^p wi}.$$

Finally, introduce $\phi_w : G \to \mathbb{C}$ by

$$\phi_w = \theta_w \circ \varphi.$$

Since ϕ_w is a composition of homomorphisms, so is ϕ_w. In fact, ϕ_w is a 1-dimensional representation on G. Since D is a difference set, we must have

$$\bigl|\phi_w(D)\bigr| = \sqrt{k - \lambda} = 2^d, \quad w = 1, 2, \dots, 2^{t-p} - 1.$$

Considering the form of the difference set D, the previous relation can be written as

$$\left|\sum_{i=1}^{a} \varepsilon^{2^p wn_i} + \sum_{j=1}^{r} \Biggl(\sum_{s=1}^{t_j} \varepsilon^{2^p wm_{j_s}}\Biggr)\right| = 2^d, \quad w = 1, 2, \dots, 2^{t-p} - 1.$$

Now, we conclude that the polynomial (in terms of ε^{2^p}) $f(\varepsilon^{2^p}) = \sum_{i=1}^{a} \varepsilon^{2^p n_i} + \sum_{j=1}^{r}(\sum_{s=1}^{t_j} \varepsilon^{2^p m_{j_s}})$ is norm invariant, and so by Theorem 6, there is some integer r_p such that $\phi_1(D) = 2^d \varepsilon^{2^p r_p}$. But then, by Theorem 5, we conclude that we must have 2^d addends $\varepsilon^{2^p r_p}$ in $\phi_1(D)$. By (1), we have

$$\phi_1(D) = \sum_{j=0}^{r} \phi_1\bigl(D \cap \langle x\rangle g_j\bigr),$$

where $g_0 = 1$. In those $r + 1$ sums, which can be treated as boxes, we can find 2^d addends $\varepsilon^{2^p r_p}$, which can be seen as elements to be distributed into mentioned boxes. Now we use Dirichlet's principle. The number of objects that are distributed is 2^d. The number of boxes over which distribution is done is $r + 1$. Thus, there is some $j' \in \{0, 1, \dots, r\}$ such that $\phi_1(D \cap \langle x\rangle g_{j'})$ has ω copies of $\varepsilon^{2^p r_p}$, where

$$\begin{aligned}\omega &\geq \left\lfloor \frac{2^d - 1}{r + 1} \right\rfloor + 1 \geq \left\lfloor \frac{2^d - 1}{2^{2d+2-t}} \right\rfloor + 1 = \left\lfloor 2^{t-d-2} - \frac{1}{2^{2d+2-t}} \right\rfloor + 1 \\ &= 2^{t-d-2} \geq 2^{d+3+p-d-2} = 2^{p+1}.\end{aligned}$$

Then we have

$$\begin{aligned}2^{p+1} &\leq \left|\left\{i \mid 0 \leq i < 2^t,\ \phi_1\left(x^i g_{j'}\right) = \varepsilon^{2^p r_p}\right\}\right| \\ &= \left|\left\{i \mid 0 \leq i < 2^t,\ \phi_1\left(x^i\right) = \varepsilon^{2^p r_p}\right\}\right| \\ &= \left|(\phi_1|_{\langle x\rangle})^{-1}\left(\varepsilon^{2^p r_p}\right)\right| \\ &= \left|\operatorname{Ker}(\phi_1|_{\langle x\rangle})\right| \\ &= 2^p,\end{aligned}$$

which is a contradiction. □

4 Dihedral type groups

As in the previous section, we start with a definition of a class of groups on which we shall apply our techniques.

Definition 3 Let G be a group of order 2^{2d+2}, and let $\langle x\rangle$ be its normal cyclic subgroup of order 2^t, where x is a generator. If every $g \in G$ acts on x like $x^g = x$ or $x^g = x^{-1}$, then the group G will be called a dihedral type group and such an x will be called a dihedral generator.

On dihedral type groups we cannot apply 1-dimensional representations in order to find out something about the possibilities of possessing a difference set. The reason for that is that the commutator subgroup of a dihedral group is too large. It is of index 4, hence we would have at most four 1-dimensional representations, and so with the original norm invariance method we would not be able to find anything new. But with a few tricks, we shall show how to use 2-dimensional representations, in order to apply successfully the norm invariance method.

Theorem 8 *Let G be a dihedral type group of order 2^{2d+2}, $d \geq 3$, let $x \in G$ be a modular generator and $C_G(x)' \cap \langle x\rangle \leq \langle x^{2^{t-p}}\rangle$, $p \in \{1, 2, \dots, t - 1\}$. If $|\langle x\rangle| \geq 2^{d+3+p}$, then G is not a Hadamard group.*

Proof Suppose that the claim of the theorem is not true, thus suppose that D is a difference set with parameters:

$$(v, k, \lambda) = \left(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d\right),$$

and additionally assume that $o(x) = 2^t$, $t \geq d + 3 + p$.

We may again assume that D is of the form

$$D=\sum_{i=1}^{a}x^{n_i}+\sum_{j=1}^{r}\left(\sum_{s=1}^{t_j}x^{m_{js}}\right)g_j=\sum_i x^{n_i}+\sum_j x^{m_j}g_j \tag{2}$$

where g_j are coset representatives of $G/\langle x\rangle$, $\langle x\rangle g_j\neq\langle x\rangle$. Notice that $r\leq[G:\langle x\rangle]-1$.

Define $\delta : G\to\{-1,1\}$ by $x^g=x^{\delta(g)}$. Since $x^{\delta(g_1g_2)}=x^{g_1g_2}=(x^{g_1})^{g_2}=(x^{\delta(g_1)})^{g_2}=(x^{g_2})^{\delta(g_1)}=x^{\delta(g_2)\delta(g_1)}$, we conclude that δ is a homomorphism and its kernel $\mathrm{Ker}(\delta)=C_G(x)$ is a subgroup of index 2 in G. If δ is not a surjection, then we would have $x\in Z(G)$, thus G would be of modular type, so that case has been covered by our previous result. Therefore, from now on, we assume that δ is surjective.

Thus, every $g\in G$ can be presented as cy^u, where $c\in C_G(x)$ and $u\in\{0,1\}$. From the definition of G we have $x^y=x^{-1}$. Similarly as in the previous proof, there is a natural epimorphism $\varphi : C_G(x)\to C_G(x)/C_G(x)'$ defined by $\varphi(c)=cC_G(x)'$. The factor group $C_G(x)/C_G(x)'$ is abelian, where $xC_G(x)'$ is its generator. Hence, there is some abelian group A such that

$$C_G(x)/C_G(x)'=\langle xC_G(x)'\rangle\times A.$$

Let ε be a root of unity of order 2^t. For $w=1,2,\dots,2^{t-p}$, we define a character of the abelian group $C_G(x)/C_G(x)'$ as follows:

$$\theta_w\bigl(x^iC_G(x)',a\bigr)=\varepsilon^{2^pwi}.$$

Finally, now we can define a representation of the maximal subgroup $C_G(x)$ by

$$\phi_w=\theta_w\circ\varphi.$$

If $c\in C_G(x)$, then $c=x^ic_1$, for some $c_1\in C_G(x)\setminus\langle x\rangle$. Therefore, we have

$$\phi_w(c)=\phi_w\bigl(x^ic_1\bigr)=\varepsilon^{2^pwi}.$$

Now, we are interested in 2-dimensional representations of G. Since every $g\in G$ is of the form $g=c$ or $g=cy$, where $c\in C_G(x)$, we define a map $\Phi_w : G\to GL(2,\mathbb{C})$ for $w=1,2,\dots,2^{t-p}$ as follows:

$$\Phi_w(c)=\begin{pmatrix}\phi_w(c) & 0\\ 0 & \phi_w(c^y)\end{pmatrix},\qquad \Phi_w(cy)=\begin{pmatrix}0 & \phi_w(cy^2)\\ \phi_w(c^y) & 0\end{pmatrix}.$$

Indeed, Φ_w are induced 2-dimensional representations of G. Thus,

$$\Phi_w(D)\Phi_w\bigl(D^{(-1)}\bigr)=2^{2d}I_2 \tag{3}$$

where I_2 is a 2×2 identity matrix. Now, we have

$$\Phi_w(D)=\sum_i\Phi_w\bigl(x^{n_i}\bigr)+\sum_j\Phi_w\bigl(x^{m_j}g_j\bigr).$$

In the second sum we will use index j_1 for those g_j with the property $x^{g_j}=x$, and index j_2 if $x^{g_j}=x^{-1}$. When we apply the introduced notation, we get

$$\Phi_w(D)=\sum_i\Phi_w\bigl(x^{n_i}\bigr)+\sum_{j_1}\Phi_w\bigl(x^{m_{j_1}}g_{j_1}\bigr)+\sum_{j_2}\Phi_w\bigl(x^{m_{j_2}}g_{j_2}\bigr).$$

Notice that $\phi_w(C_G(x)) = \phi_w(\langle x\rangle)$, thus, in every class $\langle x\rangle g$, $g \in C_G(x)$, there is an element g' such that $\phi_w(g') = 1$. So $\Phi_w(g') = I$.

For other representatives outside of $C_G(x)$, like y or $g_j y$, where $g_j \in C_G(x)$, the following holds:

$$\Phi_w(y) = \Phi_w(g_j y) = \begin{pmatrix} 0 & \phi_w(y^2) \\ 1 & 0 \end{pmatrix}.$$

If we define

$$A_w = \sum_i \varepsilon^{2^p w n_i} + \sum_{j_1} \varepsilon^{2^p w m_{j_1}}, \qquad B_w = \sum_{j_2} \varepsilon^{2^p w m_{j_2}},$$

then we get

$$\phi_w(D) = \begin{pmatrix} A_w & B_w \phi_w(y^2) \\ B_w^{(-1)} & A_w^{(-1)} \end{pmatrix}.$$

Similarly,

$$\phi_w\bigl(D^{(-1)}\bigr) = \begin{pmatrix} A_w^{(-1)} & B_w \\ B_w^{(-1)} \phi_w(y^2)^{-1} & A_w \end{pmatrix}.$$

Now, (3) becomes

$$\begin{pmatrix} A_w & B_w \phi_w(y^2) \\ B_w^{(-1)} & A_w^{(-1)} \end{pmatrix} \cdot \begin{pmatrix} A_w^{(-1)} & B_w \\ B_w^{(-1)} \phi_w(y^2)^{-1} & A_w \end{pmatrix} = \begin{pmatrix} 2^{2d} & 0 \\ 0 & 2^{2d} \end{pmatrix},$$

and after multiplication we get

$$|A_w|^2 + |B_w|^2 = 2^{2d}, \qquad A_w B_w = 0$$

for all $w = 1, 2, \dots, 2^{t-p} - 1$.

Because $A_w = 0$ or $B_w = 0$, we conclude that

$$|A_w|^2 + |B_w|^2 = |A_w + B_w|^2 = 2^{2d},$$

for all $w = 1, 2, \dots, 2^{t-p} - 1$. Hence, the polynomial $g(\varepsilon^{2^p}) := A_1 + B_1$ is norm invariant, and by Theorem 6, there is some $\varepsilon^{2^p r_p}$ such that

$$A_1 + B_1 = 2^d \varepsilon^{2^p r_p}.$$

Therefore, 2^d copies of the $\varepsilon^{2^p r_p}$ have to be distributed over 2^{2d+2-t} cosets of $G/\langle x\rangle$, hence, from Dirichlet's principle, we conclude that there is a coset image with at least $\Omega \geq 2^{p+1}$ copies of $\varepsilon^{2^p r_p}$. Here we get a contradiction, with the same argument as in Theorem 7. □

5 Semi-dihedral and quaternion type groups

We begin with the definition of groups which possess a generator x, with an additional property that other generators act via conjugation on x like in a semi-dihedral 2-group.

Definition 4 Let G be a group of order 2^{2d+2}, and let $\langle x\rangle$ be its normal cyclic subgroup of order 2^t, where $x \in G \setminus \Phi(G)$ i.e. x is a generator. If every $g \in G$ acts on x like $x^g = x$ or $x^g = x^{-1}x^{2^{t-1}}$, then the group G will be called a semi-dihedral type group, and x will be called a semi-dihedral generator.

Using the same techniques as before, we are going to prove the following result.

Theorem 9 *Let G be a semi-dihedral type group of order 2^{2d+2}, $d \geq 3$, let $x \in G$ be a semi-dihedral generator and $C_G(x)' \cap \langle x\rangle \leq \langle x^{2^{t-p}}\rangle$, $t \in \{1, 2, \dots, t-1\}$. If $|\langle x\rangle| \geq 2^{d+3+p}$, then G is not a Hadamard group.*

Proof We use the same notation as before i.e. $z = x^{2^{t-1}}$. Notice that $z \in Z(G)$.

Assume the opposite. Let D be a difference set with parameters $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$. As we have seen before, the set D can be written as

$$D = \sum_{i=1}^{t} x^{n_i} + \sum_{j=1}^{r} x^{m_j} g_j \tag{4}$$

where each $g_j \neq 1_G$ is a class representative in $G/\langle x\rangle$. Define a map $\delta : G \to \{1, 2^{t-1} - 1\}$, where $\{1, 2^{t-1} - 1\}$ is a group of order 2 with multiplication modulo 2^t. As seen before, δ is homomorphism. The remaining part of the proof follows the previous one. □

It remains to define quaternion type groups.

Definition 5 Let G be a group of order 2^{2d+2}, and let $\langle x\rangle$ be its normal cyclic subgroup of order 2^t, where $x \in G \setminus \Phi(G)$ i.e. x is a generator. If every $g \in G$ acts on x like $x^g = x$ or $x^g = x^{-1}$, with an additional property $g^2 = x^{2^{t-1}}$, then the group G will be called a quaternion type group, and x will be called a quaternion generator.

Although it is easy to confirm that every quaternion type group is basically of dihedral type, we have defined such a class for the completeness sake. In a similar way, the following result can be proved, using the same type of 2-dimensional representations as in the semi-dihedral case, so we omit the proof.

Corollary 1 *Let G be a quaternion type group of order 2^{2d+2}, $d \geq 3$, let $x \in G$ be a quaternion generator and $C_G(x)' \cap \langle x\rangle \leq \langle x^{2^{t-p}}\rangle$. If $|\langle x\rangle| \geq 2^{d+3+p}$, then G is not a Hadamard group.*

Acknowledgements We wish to thank Ken W. Smith from Sam Houston State University for helpful suggestions and advices, in particular considering the use of algebraic number theory enabling us to present some proofs in a shorter and more elegant way.

References

1. Beth, T., Jungnickel, D., Lenz, H.: Design Theory. Bibliographisches Institut, Manheim-Wien-Zürich (1985)

2. Dillon, J.F.: A survey of difference sets in 2-groups, presented at "Marshall Hall Memorial Conference", Vermont (1990)
3. Jungnickel, D., Pott, A., Smith, K.W.: Difference sets. In: Colbourn, C.J., Dinitz, J.H. (eds.) The Handbook of Combinatorial Designs, 2nd edn., pp. 419–435. CRC Press, Boca Raton (2007)
4. Leung, K.H., Ma, S.L.: Partial difference triples. J. Algebr. Comb. **2**, 397–409 (1993)
5. Liebler, R.A., Smith, K.W.: On difference sets in certain 2-groups. In: Jungnickel, D., Vanstone, S.A. (eds.) Coding Theory, Design Theory, Group Theory, pp. 195–212. Wiley, New York (1993)
6. Schmidt, B.: Characters and Cyclotomic Fields in Finite Geometry. Springer, Berlin (2002)
7. Pott, A.: Finite Geometry and Character Theory. Springer, Berlin (1995)
8. Turyn, R.J.: Character sums and difference sets. Pac. J. Math. **15**, 319–346 (1965)