EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 8, No. 4, 2015, 450-457
ISSN 1307-5543 – www.ejpam.com

On Hadamard Groups with Relatively Large 2-Subgroup

Kristijan Tabak

Rochester Institute of Technology, Zagreb Campus, D.T. Gavrana 15, 10000 Zagreb, Croatia

Abstract. A Hadamard group is any group of order $4u^2$ that contain a difference set. In this paper we obtain some new conditions for Hadamard groups with relatively large 2-subgroup. We use norm invariant polynomials $f(\varepsilon) \in \mathbb{Z}[\varepsilon]$, $|f(\varepsilon^t)| = \text{const.}$, where ε is root of unity of order 2^n. Necessary condition on a size of normal cyclic 2-subgroup are given. Also, we have covered cases when 2-subgroup has generators similar to a modular or dihedral 2-group. Additionally, we construct such two infinite series of groups. Obtained results are natural generalization of a case when entire group is 2-group.

2010 Mathematics Subject Classifications: 05B10, 20E07, 20E28

Key Words and Phrases: Difference set, Norm invariance, Hadamard group, Group representation

1. Introduction and Known Results

We start by introducing a standard definition of a difference set. Let G be a group where $|G| = 4u^2$. If $D \subseteq G$, where $|D| = 2u^2 - u$, is such that

$$\{d_1 d_2^{-1} \mid d_1, d_2 \in D\} = \{(u^2 - u) \cdot g \mid g \in G \setminus \{1_G\}\},$$

then we call D a **difference set**. In that case group G is called a Hadamard group (see [1, 2]). In difference set theory is usual to deal with linear combinations of some roots of unity. Good example is classical paper [6]. We will analyze polynomials like $f(\varepsilon) = \sum_{j=1}^{w} k_j \varepsilon^{r_j}$, where $k_i \in \mathbb{Z}$ and ε is some root of unity.

As it can be seen from some publications (i.e. [5]), algebraic approach to difference set problems induce a significant progress. Elements of representation theory played important role in this paper. The main theoretical result which served as technical tool in difference set theory is

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.*

Email address: kxtcad@rit.edu

If hypothesized Hadamard group has some cyclic image of order equal to the order of ε, then using representation theory tools it can be shown that there is some polynomial $f(\varepsilon)$ such that $|f(\varepsilon^p)|$ is constant for every $p \in \mathbb{Z}$ (assuming $f(\varepsilon^p)$ is nontrivial).

In paper [3] Hadamard groups of order 2^{2d+2} were considered. Consequent polynomials were fully described, after which new necessary conditions have been proven. Pairwise abbreviation theorem [3] is also used in this paper. Results that follow will show us again that 'Fourier type' approach, by comparing coefficients of respective powers, can lead us to some new conditions.

Main goal of this paper is to offer generalization of results in [3]. That will be provided by proving result where norm of polynomials is not necessary some power of 2.

We will denote $f(\varepsilon)$ as nontrivial if it has some nonzero coefficient next to some $\varepsilon^i \neq 1$.

Definition 1. *Let ε be a root of unity and $f(\varepsilon) \in \mathbb{Z}[\varepsilon]$ is nontrivial. If there is some c, such that $|f(\varepsilon^p)| = c$, for all $p \in \mathbb{Z}$ such that $f(\varepsilon^p)$ is nontrivial, then we shall say $f(\varepsilon)$ is* **norm invariant**.

Following result describes pairwise abbreviation.

Theorem 2. *Let ε be a root of unity of order 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 $\varepsilon^{\alpha_i} + \varepsilon^{\alpha_j} = 0$.*

Next result (see [3]) gives a characterization of norm invariant polynomials of norm 2^d.

Theorem 3. *Let $f(\varepsilon) = \varepsilon^{r_1} + \cdots + \varepsilon^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and ε is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\varepsilon^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\varepsilon^{2^k}) = 2^d \varepsilon^{r_{(k)}}$. We call such polynomials $f(\varepsilon^{2^k})$ maximally abbreviated.*

2. Some Algebraic Tools

Let us introduce some notation. For $n \in \mathbb{N}$ we denote $[n] = \{1, 2, \ldots, n\}$ and $[n]_0 = \{0, 1, 2, \ldots, n\}$. Next result describes distribution of coefficients standing by ε^0 in norm invariant polynomial from $\mathbb{Z}[\varepsilon]$, where $\varepsilon^{2^t} = 1$.

Theorem 4. *Let ε be root of unity of order 2^t and $F(\varepsilon) = \sum k_i \varepsilon^i$, $k \in \mathbb{N}_0$. Let sum of coefficients is $2u^2 - u$, for some $u \in \mathbb{N}$. If every nontrivial $F(\varepsilon^{2^s})$ is of norm u, then*

$$\sum_{i \in A_0} k_i^2 + 2 \sum_{j=1}^{s} \sum_{(a,b) \in A_j} k_a k_b - 2 \sum_{(a,b) \in A_{s+1}} k_a k_b = u^2$$

where $A_0 = [2^t - 1]_0$ and $A_j = \{(a, b) \in A_0^2 \mid a < b,\ 2^{j-1}(a - b) \equiv 2^{t-1} (mod\ 2^t)\}$.

Proof. We start by taking $s = 0$. By assumption we have $|F(\varepsilon)| = u$. Then $u^2 = |F(\varepsilon)|^2 = \sum_{i,j \in A_0} k_i k_j \beta^{i-j}$, where $A_0 = [2^t - 1]_0$. By Theorem 2, after comparing coefficients next to 1, we get

$$\sum_{\varepsilon^{i-j}=1} k_i k_j \beta^{i-j} - \sum_{\varepsilon^{i-j}=-1} k_i k_j \beta^{i-j} = u^2. \tag{1}$$

If $\varepsilon^{i-j}=1$, then $k_i=k_j$. If $\varepsilon^{i-j}=-1$, then $i-j\equiv 2^{t-1}(mod\ 2^t)$. It is clear that also $j-i\equiv 2^{t-1}(mod\ 2^t)$. Therefore, it is natural to introduce

$$A_1=\{(a,b)\in A_0^2 \mid a<b,\ a-b\equiv 2^{t-1}\ (mod\ 2^t)\}.$$

Then, from (1) we get

$$\sum_{i\in A_0} k_i^2-2\sum_{(a,b)\in A_1} k_ak_b=u^2. \tag{2}$$

Now in next step, let's take $|F(\varepsilon^2)|$. After expanding we get $|F(\varepsilon^2)|^2=\sum_{i,j\in A_0} k_ik_j\varepsilon^{2(i-j)}=u^2$. Comparing coefficients next to 1 gives

$$\sum_{\varepsilon^{2(i-j)}=1} k_ik_j\varepsilon^{2(i-j)}-\sum_{\varepsilon^{2(i-j)}=-1} k_ik_j\varepsilon^{2(i-j)}=u^2. \tag{3}$$

If $\varepsilon^{2(i-j)}=1$, then $\varepsilon^{i-j}=1$ or $\varepsilon^{i-j}=-1$. Hence

$$\sum_{\varepsilon^{2(i-j)}=1} k_ik_j\varepsilon^{2(i-j)}=\sum_{i\in A_0} k_i^2+2\sum_{(a,b)\in A_1} k_ak_b. \tag{4}$$

On the other hand, if $\varepsilon^{2(i-j)}=-1$, then $2(i-j)\equiv 2^{t-1}(mod\ 2^t)$ and $2(j-i)\equiv 2^{t-1}(mod\ 2^t)$. Thus

$$\sum_{\varepsilon^{2(i-j)}=-1} k_ik_j\varepsilon^{2(i-j)}=2\sum_{(a,b)\in A_2} k_ak_b$$

where $A_2=\{(a,b)\in A_0^2 \mid a<b,\ 2(a-b)\equiv 2^{t-1}(mod\ 2^t)\}$.

If we continue in similar manner, for every nontrivial $F(\varepsilon^{2^s})$ we get

$$\sum_{i\in A_0} k_i^2+2\sum_{j=1}^{s}\sum_{(a,b)\in A_j} k_ak_b-2\sum_{(a,b)\in A_{s+1}} k_ak_b=u^2. \tag{5}$$

□

There is also one simple question that should be covered. Sometimes, we need to know how many different powers we have such that $\varepsilon^{2^s(i-j)}$ is an involution. Next lemma gives the answer.

Lemma 1. *Let $(i,j)\in A_0^2$, where $i<j$ and $A_0=[2^t-1]_0$. Then there is unique $s\in\{1,2,\dots,t\}$ such that $2^{s-1}(i-j)\equiv 2^{t-1}(mod\ 2^t)$.*

Proof. Take $s_1\neq s_2$ from set $[t]$. Let as assume that $2^{s_1-1}(i-j)\equiv 2^{t-1}(mod\ 2^t)$ and $2^{s_2-1}(i-j)\equiv 2^{t-1}(mod\ 2^t)$. Then, there are $K_1,K_2\in\mathbb{Z}$ such that $2^{s_1-1}(i-j)=2^{t-1}+K_1\cdot 2^t$ and $2^{s_2-1}(i-j)=2^{t-1}+K_2\cdot 2^t$. We may assume that $s_1>s_2$, thus

$$\left(2^{s_1-s_2}-1\right)2^{s_2-1}(i-j)=(K_1-K_2)2^t.$$

Now we get $(i-j)\equiv 0(mod\ 2^{t+1-s_2})$, hence $2^{s_2-1}(i-j)\equiv 0(mod\ 2^t)$. But, using first assumption we would have $2^{t-1}\equiv 0(mod\ 2^{t+1-s_2})$, which is obvious contradiction. Therefore $K_1=K_2$, but then we get $s_1=s_2$, again contradiction. Thereby, we have proved the assertion. □

Next assertion rise from norm invariance analysis.

Lemma 2. *Let $\Omega_0,\dots,\Omega_t \in \mathbb{N}_0$ such that where $t \in \mathbb{N}$*

(i) $\Omega_0 + 2\sum_{i=1}^{s}\Omega_i - 2\Omega_{s+1} = u^2$, $s \in [t-1]$,

(ii) $\Omega_0 + 2\sum_{i=1}^{t}\Omega_i = (2u^2-u)^2$,

If u_1 is maximal odd divisor of u, then $\Omega_i \equiv 0(mod\ u_1^2)$ for every $i \in [t]_0$.
Additionally: if $u \in \mathbb{N}$ is odd, then $\Omega_i \equiv 0(mod\ u^2)$ for every $i \in [t]_0$, and also there is some integer K such that $u = 1 + 2^{t-1}K$.

Proof. Solving system of linear equations we get $\Omega_i = 2^{i-2}(\Omega_0 - u^2)$, $i \in [t]$. Now, using this and second assumption in our statement, we get $(2u^2-u)^2 = \Omega_0 + (\Omega_0 - u^2)(2^t - 1)$, hence

$$2^{t-2}(\Omega_0 - u^2) = u^3(u-1). \tag{6}$$

Firstly, let assume that u is odd. Therefore $u-1$ is divisible by 2^{t-2}. So, there is some integer K_1 such that $u = 1 + K_1 \cdot 2^{t-2}$. Therefore, $\Omega_0 - u^2 = K_1 \cdot u^3$ and $\Omega_0 = u^2(1 + K_1 \cdot u)$. This gives us $\Omega_0 \equiv 0(mod\ u^2)$. Since $\Omega_1 = \frac{1}{2}(\Omega_0 - u^2) = \frac{1}{2}K_1u^3 \in \mathbb{N}_0$ and u odd, we get $K_1 = 2K$ for some integer K. Finally, $u = 1 + K \cdot 2^{t-1}$ and $\Omega_1 \equiv 0(mod\ u^2)$. We already proved that $\Omega_{i+1} = 2\Omega_i$, $i \geq 1$. This gives us $\Omega_i \equiv 0(mod\ u^2)$.

Now, if $u = 2^R u_1$ where u_1 is odd, using (6) we get $\Omega_0 \equiv 0(mod\ u_1^2)$, hence $\Omega_1 \equiv 0(mod\ u_1^2)$. Therefore, $\Omega_i \equiv 0(mod\ u_1^2)$, $i \in [t]$. □

Now, we are going to need one classical result (for example see [4]).

Lemma 3. *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-conjugated modulo w, i.e. $p^j \equiv -1(mod\ w')$ for some $j \in \mathbb{N}$ where $m = p^a w'$, w' not divisible by p. If $\chi(A)\overline{\chi(A)} \equiv 0(mod\ p^{2i})$, then $\chi(A) \equiv 0(mod\ p^i)$.*

We present helpful algebraic claim that is most critical for proving main results of this paper.

Theorem 5. *Let ε be a root of unity of order 2^t. Let $F(\varepsilon) \in \mathbb{Z}[\varepsilon]$ with nonnegative coefficients whose sum is $2u^2 - u$, for some $u \in \mathbb{N}$. If $F(\varepsilon)$ is norm invariant of the norm u, then for every nontrivial $F(\varepsilon^{2^s})$ there is some $r_s \in \mathbb{Z}$ such that $F(\varepsilon^{2^s}) = u\varepsilon^{r_s}$.*

Proof. Let $F(\varepsilon) = \sum_{i\in A_0} k_i\varepsilon^i$, where $A_0 = [2^t - 1]_0$. Motivated by previous results, we introduce notation $\Omega_0 = \sum_{i\in A_0} k_i^2$, $\Omega_j = \sum_{(a,b)\in A_j} k_a k_b$, where

$$A_j = \{(a,b) \in A_0^2 \mid a < b,\ 2^{j-1}(a-b) \equiv 2^{t-1}(mod\ 2^t)\}.$$

If we compare coefficients next to 1 in $|F(\varepsilon^{2^s})|^2$ and use pairwise abbreviation theorem, we get $\Omega_0 + 2\sum_{i=1}^{s}\Omega_i - 2\Omega_{s+1} = u^2$. Assumption from theorem claim gives us $|F(\varepsilon^{2^t})|^2 = \Omega_0 + 2\sum_{i=1}^{t}\Omega_t$. Therefore, we are within conditions of Lemma 2.

In the first case we will assume that u is odd. Then $\Omega_i \equiv 0(mod\ u^2)$. Therefore, we can define $F'(\varepsilon) = \frac{1}{u}F(\varepsilon)$, $\Omega_i' = \frac{1}{u^2}\Omega_i$. Notice that for every $s \in [t-1]$ we get the system $\Omega_0' + 2\sum_{i=1}^{s}\Omega_i' - 2\Omega_{s+1}' = 1$, or in other words $|F'(\varepsilon)| = 1$.

Second case deals with even u. In this one we will need more severe tools. Put $u = 2^R u_1$, where u_1 is odd. Then $\Omega_i \equiv 0(mod\ u_1^2)$. We will use Lemma 3. Let us introduce $A = \sum_{i=0}^{2^t-1} k_i x^i \in \mathbb{Z}[x]$, where $\langle x\rangle \cong \langle\varepsilon\rangle \cong C_{2^t}$. Take character $\chi : A \to \mathbb{C}$ given by $\chi(x) = \varepsilon$. Now we have $\chi(A)\overline{\chi(A)} = |F(\varepsilon)|^2 = F(\varepsilon)\overline{F(\varepsilon)} = 2^{2R}u_1^2 \equiv 0(\ mod\ 2^{2R})$. Using the notation from Lemma 3, we may write $w = 2^t$, $p = 2$. Furthermore $w = 2^t w'$, where $w' = 1$. It is obvious that $2^j \equiv -1(mod\ w')$. By Lemma 3, we have $F(\varepsilon) = \chi(A) \equiv 0(mod\ 2^R)$. Therefore, $|F(\varepsilon)|^2 \equiv 0(mod\ u^2)$. Therefore, we can define F' and Ω_i' as in previous case.

So, both cases lead us to $|F(\varepsilon)'| = 1$. It is clear that F' has coefficients from $\mathbb{Q}$. Let us write $F(\varepsilon)' = (\varepsilon')^{i_1} + \ldots + (\varepsilon')^{i_q}$, where $(\varepsilon')^{i_j} = \frac{1}{u}\varepsilon^{i_j}$. Let us assume that some two $(\varepsilon')^{i_j}$ can be abbreviated in pairs. Additionally, we may assume that we have done all possible abbreviations in $F(\varepsilon)'$. Therefore, for roots that 'survived' abbreviations we may write $F(\varepsilon)' = (\varepsilon')^{s_1} + \ldots + (\varepsilon')^{s_{q_1}}$. Hence, $\sum_{i,j=1}^{q_1}(\varepsilon')^{s_i - s_j} = 1$. By pairwise abbreviation we get

$$1 = |F(\varepsilon)'| = |\sum_{i=1}^{q_1}(\varepsilon')^{s_i}| \leq \sum_{i=1}^{q_1}|(\varepsilon')^{s_i}| = \frac{q_1}{u}.$$

Thus $q_1 \geq u$. Also, we get $\sum_{i\neq j}^{q_1}(\varepsilon')^{s_i - s_j} + q_1 - 1 = 0$. The consequence is that, in previous sum, we must have at least one term equal to (-1). For example $(\varepsilon')^{s_1 - s_2} = -1$. It is clear that we would get $(\varepsilon')^{s_1} + (\varepsilon')^{s_1} = 0$, contrary to our assumption about maximal abbreviation. Therefore, the only option is that for every $j_i, j_2 \in [q_1]$ equation $(\varepsilon')^{s_{j_1} - s_{j_2}} = 1$ holds. Now, it is straight forward $q_1 = u$. Thus $F(\varepsilon)' = \frac{q_1}{u}\varepsilon^{r_0}$ for some $r_0 \in \mathbb{Z}$. Finally, this gives us $F(\varepsilon) = uF(\varepsilon)' = u\varepsilon^{r_0}$. □

3. Modular Case

This section deals with groups of order $4u^2$ with maximal 2-group of modular type. By that we mean that generators of such 2-group look like those in 2-generated modular 2-group. We will use $o(g)$ for order of element g.

Theorem 6. *Let $G = H \times L$ be a group of $4u^2$ where $|L| = u_1^2$. Let $H = \langle x, y_1, \ldots, y_s\rangle$ is of order 2^{2d+2} and $o(x) = 2^t$ where $x^{y_i} \in \{x, x^{2^{t-1}+1}\}$. If $H' \cap \langle x\rangle \leq \langle x^{2^{t-p}}\rangle$ and $o(x) \geq 2^{p+3}u$, then G is not a Hadamard group.*

Proof. Let us assume that G is a Hadamard group. Then G posses a difference set D with parameters $(4u^2, 2u^2 - u, u^2 - u)$. Now we will construct a 1-dimensional representations on H, which is also a representation on G.

Notice that $u = 2^d u_1$. Condition $H' \leq \langle x^{2^{t-p}}\rangle$ is needed, since for any homomorphism $\varphi : G \to \mathbb{C}$ we also have $G' \leq Ker(\varphi)$.

Now, we take difference set and divide it over classes modulo $\langle x\rangle$. Then we get

$$D = \sum_{i=1}^{a} x^{n_i} + \sum_{j=1}^{r}\left(\sum_{s=1}^{t_j} x^{m_{j_s}}\right) g_j.$$

Every $g \in G$ can be written in a form $g = x^i y_{i_1} y_{i_2} \dots y_{i_n}$, where $y_{i_j} \in \langle y_1, \dots, y_s \rangle$. Now, for $w = 1, 2, \dots, 2^{t-p}$ we define $\varphi_w : G \to \mathbb{C}$ by $\varphi_w(x^i y_{i_1} y_{i_2} \dots y_{i_n}) = \varepsilon^{2^p wi}$, where ε is a root of unity of order 2^t. Also, $G' = H' \times L'$. We notice that φ_w is well defined, since $G' \cap \big(\langle x \rangle \times \{1_L\}\big) \leq \langle x^{2^{t-p}} \rangle$ and $\langle \varphi_w(x^{2^{t-p}}) \rangle = \langle 1 \rangle$. Now it is clear that $G' \leq Ker(\varphi_w)$ is fulfilled. By Theorem 1 we have $\varphi_w(D)\varphi_w(D^{-1}) = |\varphi_w(D)|^2 = u^2$, for every nontrivial φ_w, i.e. for $w = 1, 2, \dots, 2^{t-p} - 1$. Hence $\varphi_w(D) = \sum_{i=1}^{a} \varepsilon^{2^p w n_i} + \sum_{j=1}^{r} \left(\sum_{s=1}^{t_j} \varepsilon^{2^p w m_j} \right)$ is norm invariant polynomial of norm u. Therefore, by Theorem 5, for every $w = 1, 2, \dots, 2^{t-p} - 1$ there is some $r_w \in \mathbb{Z}$ such that $\varphi_w(D) = \sum_{i=1}^{a} \varepsilon^{2^p w n_i} + \sum_{j=1}^{r} \left(\sum_{s=1}^{t_j} \varepsilon^{2^p w m_j} \right) = u\varepsilon^{2^p r_w}$. Then, by Theorem 2, in a sum $\varphi_1(D) = \sum_{j=0}^{r} \varphi_1(D \cap \langle x \rangle g_j)$ we must have u addends $\varepsilon^{2^p r_1}$ distributed over $r+1$ classes. This could be interpreted is of u copies (items or objects) of $\varepsilon^{2^p r_1}$ are distributed over $r+1$ boxes. Then we can use Dirichlet's principle. Number of boxes should be $[G : \langle x \rangle] = 2^{2d+2-t} u_1^2$. By Dirichlet's principle, there is some $j' \in \{0, 1, \dots, r\}$ such that $\varphi_1(D \cap \langle x \rangle g_{j'})$ has Ω copies of $\varepsilon^{2^p r_1}$. We estimate value for Ω as follows:

$$\begin{aligned}
\Omega &= \left\lfloor \frac{u-1}{2^{2d+2-t} u_1^2} \right\rfloor + 1 = \left\lfloor \frac{2^d u_1 - 1}{2^{2d+2-t} u_1^2} \right\rfloor + 1 \geq \left\lfloor \frac{2^d u_1}{2^{2d+2-t} u_1^2} \right\rfloor - 1 + 1 \\
&= \left\lfloor \frac{2^{t-d-2}}{u_1} \right\rfloor = \{\text{since } 2^t \geq 2^{p+3} u = 2^{p+3} 2^d u_1\} = \left\lfloor \frac{2^t \cdot 2^{-d-2}}{u_1} \right\rfloor \\
&\geq \left\lfloor \frac{2^{p+3} 2^d u_1 2^{-d-2}}{u_1} \right\rfloor = 2^{p+1}.
\end{aligned}$$

Therefore, $\Omega \geq 2^{p+1}$. Before we get a final contradiction, additional observation is necessary. We have

$$\begin{aligned}
(\varphi_1|_{\langle x \rangle})^{-1}(\varepsilon^{2^p r_1}) &= \{x^i \mid \varphi_1(x^i) = \varepsilon^{2^p r_1}\} = \{x^i \mid \varepsilon^{2^p i} = \varepsilon^{2^p r_1}\} \\
&= \{x^i \mid \varepsilon^{2^p (i - r_1)} = 1\} = \{x^i \mid \varphi_1(x^{i-r_1}) = 1\} = x^{r_1} Ker(\varphi_1).
\end{aligned}$$

Hence,

$$\begin{aligned}
2^{p+1} &\leq |\{i \mid 0 \leq i < 2^t,\ \varphi_1(x^i g_{j'}) = \varepsilon^{2^p r_1}\}| \\
&= |\{i \mid 0 \leq i < 2^t,\ \varphi_1(x^i) = \varepsilon^{2^p r_1}\}| \\
&= |(\varphi_1|_{\langle x \rangle})^{-1}(\varepsilon^{2^p r_1})| \\
&= |\mathrm{Ker}(\varphi_1|_{\langle x \rangle})| \\
&= 2^p,
\end{aligned}$$

which is an obvious contradiction. □

4. One Infinite Series of Groups for Modular Case

We construct one example of infinite series of groups that can be covered by previous result. Take $G = H \times L$, where

$$H = \langle x, y_1, y_2 \mid x^{2^{2t_1}} = y^{2^3} = y_2^{2^3} = 1,\ x^{y_1} = x^{y_2} = x^{2^{2t_1-1}+1},\ [y_1, y_2] = x^{2^{2t_1-4}} \rangle.$$

L could be any group of order u_1^2. Then $|H| = 2^{2t_1+6} = 2^{2d+2}$, where $t_1 = d-2$. Put $|G| = 4u^2$, where $u = 2^d u_1$. Let's take $p = 4$. Then we have $[x, y_i] = x^{-1}x^{y_i} = x^{2^{2t_1-1}} \in \langle x^{2^{2t_1-4}} \rangle$. Therefore $H' \leq \langle x^{2^{2t_1-4}} \rangle = \langle x^{2^{2t_1-p}} \rangle$. Additionally, if we put $2^{t_1} \geq 2^9 u_1$, using $t_1 = d-2$, we get $2^{2d-4} \geq 2^d \cdot 2^7 u_1 = 2^{p+3}u$. Therefore, we are within conditions of Theorem 6.

For example, $u_1 = 36$, $t_1 = 15$, $p = 4$ and $d = 17$. Then

$$2^{t_1} = 2^{15} = 32768 > 2^9 u_1 = 18432.$$

In that case group order would be $|G| = 2^{2d+2}u_1^2 = 2^{36} \cdot 36^2$.

5. Dihedral Case

This section covers types of groups of order $4u^2$ which also contain a 2-subgroup of dihedral type. This means that 2-subgroup has a normal cyclic subgroup, while outer elements either commute or invert generator of that normal subgroup.

Theorem 7. *Let $G = H \times L$ be a group of order $4u^2$ and $|L| = u_1^2$. Let $H = \langle x, y_1, \ldots, y_s \rangle$ has order 2^{2d+2} and $o(x) = 2^t$ where $x^{y_i} \in \{x, x^{-1}\}$. If $C_H(x)' \cap \langle x \rangle \leq \langle x^{2^{t-p}} \rangle$ and $o(x) \geq 2^{p+3}u$, then G is not a Hadamard group.*

Proof. We will use the same approach as in proof of Theorem 6. Let us assume that G posses a difference set D with parameters $(4u^2, 2u^2 - u, u^2 - u)$. This time, we will have to develop a 2-dimensional representations. Like before $u = 2^d u_1$. Since $[H : C_H(x)] = 2$, every $h \in H$ can be written as $h = cy^m$, where $c \in C_H(x)$ and $m \in \{0, 1\}$. So, every $g \in G$ can be written as $g = x^i c_1 y^m l$, where $c_1 \in C_H(x) \setminus \langle x \rangle$ and $l \in L$.

Then, for every $w = 1, 2, \ldots, 2^{t-p}$ we define $\Phi_w : G \to GL(2, \mathbb{C})$ by

$$\Phi_w(x^i c_1 y^m l) = \begin{pmatrix} \varepsilon^{2^p wi} & 0 \\ 0 & \varepsilon^{-2^p wi} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^m.$$

Because of $C_H(x)' \cap \langle x \rangle \leq \langle x^{2^{t-p}} \rangle$, map Φ_w is well defined 2-dimensional representation. Difference set D, after been taken modulo $\langle x \rangle$, becomes $D = \sum_{i=1}^{a} x^{n_i} + \sum_{j=1}^{r} \left(\sum_{s=1}^{t_j} x^{m_{j_s}} \right) g_j$. This time, we need to separate indices. Let's use j_1 if $x^{g_{j_1}} = x$, and j_2 when $g^{j_2} = x^{-1}$. Thus, from $\Phi_w(D)\Phi_w(D^{(-1)}) = u^2 I_2$, where I_2 is a 2×2 identity matrix, we get

$$\left| \sum_i \varepsilon^{2^p wn_1} + \sum_{j_1} \varepsilon^{2^p wm_{j_1}} + \sum_{j_2} \varepsilon^{2^p wm_{j_2}} \right| = u$$

where $w = 1, 2, \ldots, 2^{t-p} - 1$. Therefore, polynomial $\sum_i \varepsilon^{2^p n_1} + \sum_{j_1} \varepsilon^{2^p m_{j_1}} + \sum_{j_2} \varepsilon^{2^p m_{j_2}}$ is a norm invariant of norm u. Now, proof continues as for Theorem 6. □

6. One Infinite Series of Groups for Dihedral Case

This section offers one construction of infinite series of groups that are within conditions of Theorem 7. We start by taking a group $H = \langle x, y_1, y_2 \rangle$, where $o(x) = 2^{2t_1}$, $o(y_i) = 2^{s_i}$ and $x^{y_i} = x^{-1}$. It is easy to see that $[H : C_H(x)] = 2$. Firstly, let us show that assumption $[y_1, y_2] \in \langle x \rangle$ forces that $\langle y_1^2, y_2^2 \rangle \leq Z(H)$. From assumption we get that there is some α such that $[y_1, y_2] = x^\alpha$. Then $y_1 y_2 = y_2 y_1 x^\alpha$ and $y_2 y_1 = y_1 y_2 x^{-\alpha}$. Using this we get,

$$y_2^2 y_1 = y_2 y_2 y_1 = y_2 y_1 y_2 x^{-\alpha} = y_1 y_2 x^{-\alpha} y_2 x^{-\alpha} = y_1 y_2 y_2 x^\alpha x^{-\alpha} = y_1 y_2^2.$$

It is clear that $[y_2^2, y_2] = [y_2^2, x] = 1$, therefore $y_2^2 \in Z(H)$. Due to symmetry, similar works for y_1^2. Thus, $\langle y_1^2, y_2^2 \rangle \leq Z(H)$.

Now, let us show that $C_H(x) = \langle x, y_1^2, y_2^2, y_1 y_2 \rangle \leq H$ is abelian subgroup of index 2. By previous argument and because of $x^{y_1 y_2} = x$, it is clear that $C_1 := \langle x, y_1^2, y_2^2, y_1 y_2 \rangle \leq C_H(x)$. We obtain $|H| = 2^{2t_1 + s_1 + s_2}$ and $|C_1| = 2^{2t_1 + s_1 + s_2 - 2}$. Take $C_2 = \langle C_1, y_1 y_2 \rangle$. Since $(y_1 y_2)^2 = y_1^2 y_2^2 x^\alpha \in C_1$, we conclude that $[C_2 : C_1] = 2$, thus $[H : C_2] = 2$. Hence $C_2 = C_H(x)$. It is clear that $C_H(x)$ is abelian. Then $C_H(x)' \cap \langle x \rangle = \{1\}$.

After this, let us take concrete numbers. Put $s_1 = s_2 = 3$ and $[y_1, y_2] = x^{2t_1 - 1}$ (although, by previously proven facts, it is sufficient to assume $[y_1, y_2] \in \langle x \rangle$). Let L_1 be a group of order u_1^2 and $G = H \times L$ of order $4u^2 = 2^{2t_1 + 6} u_1^2$. Define $d = t_1 + 2$. Then $|H| = 2^{2d+2}$ and, as proved, $C_H(x) = \langle x, y_1^2, y_2^2, y_1 y_2 \rangle$. As shown, $C_H(x)' \cap \langle x \rangle \leq \langle x^{2t_1 - p} \rangle$ for any p. If $o(x) \geq 2^{p+3} u$ then we would be within conditions of Theorem 7. Because of $u = 2^{t_1 + 2} u_1$, we need $o(x) = 2^{2t_1} \geq 2^{p+3} \cdot 2^{t_1 + 2} u_1$. This gives us a conditions that chosen group parameters should fulfil: $2^{t_1 - p - 5} \geq u_1 \geq 1$. So, let us, for example choose $u_1 = 10$, $p = 2$, $t_1 = 11$. Then $2^{t_1 - p - 5} = 2^4 = 16 \geq 10 = u_1$. Then $o(x) = 2^{2t_1} = 2^{22}$. Thus, the group

$$G = \langle x, y_1, y_2 \mid x^{2^{22}} = y_1^8 = y_2^8 = 1,\ x^{y_i} = x^{-1},\ [y_1, y_2] = x^{2^{21}} \rangle \times L,$$

where $|L_1| = u_1^2 = 10^2$ is one concrete example. Group order is $|G| = 2^{28} \cdot 10^2$.

References

[1] T. Beth, D. Jungnickel and H. Lenz. *Design Theory*, Bibliographisches Institut, Manheim-Wien-Zürich, 1985.

[2] D. Jungnickel, A. Pott and K.W. Smith. *Difference Sets*, In C. J. Colburn, J.H. Dinitz, editors, The Handbook of Combinatorial Designs, Second Edition, 419-435. CRC Press, 2007.

[3] J. Mandić, M. O. Pavčević and K.Tabak. *On difference sets in high exponent 2-groups*, Journal of Algebraic Combinatorics, 38, 785-795. 2013

[4] A. Pott. *Finite Geometry and Character Theory*, Springer-Verlag, Berlin-Heidelberg, 1995.

[5] B. Schmidt. *Characters and Cyclotomic Fields in Finite Geometry*, Springer, Berlin-Heidelberg, 2002.

[6] R. J. Turyn. *Character sums and difference sets*, Pacific Journal of Mathematics, 15, 319-346. 1965.