On Hadamard 2-groups

Noboru Ito
Department of Mathematics, Meijo University
Nagoya, Tenpaku, 468 Japan

Abstract

For any given 2-group H there exists an Hadamard 2-group G containing a subgroup isomorphic to H.

§1. **Introduction.** Let G be a finite group of order $4n$ containing a central involution e^*, and T a transversal of G with respect to $\langle e^* \rangle$. If T and Tr, where r is any element of G outside $\langle e^* \rangle$, intersect in n elements, then T and G are called an Hadamard subset and an Hadamard group (with respect to $\langle e^* \rangle$) respectively. A cyclic group of order 4 is an Hadamard group, and n is even for other Hadamard groups. See [**3**]. In this paper we are interested in Hadamard 2-groups.

§2. **One-stepped 2-groups.** Let G be a 2-group of order 2^n. Then G is called one-stepped if there exist n involutions $r_1, r_2, \dots, r_n$ of G such that $\langle r_1 \rangle \langle r_2 \rangle \dots \langle r_i \rangle$ is a subgroup of order 2^i for $i = 1, 2, \dots, n$.

Lemma 1. *A 2-group G is one-stepped if and only if G is generated by involutions.*

Proof. It is obvious that if G is one-stepped, then G is generated by involutions. Now assume that G is generated by involutions and let H be a maximal one-stepped subgroup of G. If $G = H$, then we are done. Otherwise, let M be a maximal subgroup of G containing H. If M is generated by involutions, then, by using induction on the order, we have that $M = H$. Since G is generated by involutions, there exists an involution r of G outside H. Since $G = H\langle r \rangle$, this contradicts the maximality of H. If M is not generated by involutions, then the subgroup of M generated by all the involutions of M equals H. Then clearly H is normal in G. Take an involution r of G outside H and consider the subgroup $H\langle r \rangle$ which is one-stepped. This contradicts the maximality of H.

Lemma 2. *A Sylow 2-subgroup $S(n)$ of the symmetric group $Sym(2^n)$ of degree 2^n has order 2^{2^n-1} and it is generated by involutions.*

Proof. See [**2**], *p*.378.

Lemma 3. *A 2-group G of order 2^n is isomorphic to a subgroup of $S(n)$.*

Proof. Consider a regular permutation representation of G and use Sylow's theorem. See [**2**], $p.29$ and $p.34$.

By Lemmas 1, 2 and 3 we see that any 2-group can be a subgroup of a one-stepped 2-group.

§3. Construction of Hadamard 2-groups.

Lemma 4. *Let a 2-group G of order $8n$ contain an Hadamard maximal subgroup H with respect to a central involution e^*. If G contains an element r outside H such that $r^2 = e^*$, then G is also Hadamard.*

Proof. Clearly, e^* is central in G. Let E be an Hadamard subset of H and put $D = Ee^* + Er$. We show that D is an Hadamard subset of G. Let s be an element of H outside $\langle e^* \rangle$. Then $rs = rsr^{-1}r$ and rsr^{-1} is an element of H outside $\langle e^* \rangle$. So we have that $|Ee^* \cap Es| + |Ersr^{-1} \cap Er| = 2n$. Now any element of G outside H is of the form tr, where t is an element of H. If $t = e$, where e denotes the identity element of G, then $Dtr = Dr = Ee^* + Ee^*r$. Since Ee^*r and Er are disjoint, we have that $|D \cap Dr| = |Ee^*| = 2n$. If $t = e^*$, then $Dtr = De^*r = E + Er$. Obviously we have that $|D \cap De^*r| = |Ee^*| = 2n$. If t is outside $\langle e^* \rangle$, then $rtr = rtr^{-1}e^*$ and rtr^{-1} is an element of H outside $\langle e^* \rangle$. So we have that $Dtr = Ertr^{-1}e^* + Ete^*r$ and that

$$|D \cap Dtr| = |Ee^* \cap Ertr^{-1}e^*| + |Er \cap Ete^*r| = n + n = 2n.$$

See also [**1**] and [**6**].

Lemma 5. *Let G be an Hadamard 2-group with respect to $\langle e^* \rangle$ such that $e^* = r^2$ for some element r of G and H a one-stepped 2-group. Then their direct product is Hadamard with respect to $\langle e^* \rangle$.*

Proof. Let H be of order 2^n and $r_1, r_2, \ldots, r_n$ n involutions which define H. Then we have that $(rr_i)^2 = e^*$ for each $i = 1, 2, \ldots, n$. So using Lemma 4 we may adjoin $rr_1, rr_2, \ldots, rr_n$ successively to G.

Now by Lemmas 3 and 5 we have the following proposition.

Proposition 1. *Every 2-group is a subgroup of an Hadamard 2-group.*

§4. Remarks about Proposition 1. Let G be a 2-group of order 2^n, and H a one-stepped 2-group of the least order containing G. Then the index $[H : G]$ will be called the **1**-index of G and be denoted by $\mathbf{1}(G)$. Moreover let K be an Hadamard 2-group of the least order containing G. Then the index $[K : G]$ will be called the h-index of G and be denoted by $h(G)$. Now by Lemma 2 and 3 we have that $\mathbf{1}(G) \leq 2^{2^n-1-n}$ and since a cyclic group of order 4 is Hadamard, by Lemma 5 we have that $h(G) \leq 2^{2^n+1-n}$. These bounds for $\mathbf{1}(G)$ and $h(G)$ will be too crude. However, if G is Abelian, things are easy.

Lemma 6. *If G is an Abelian but not elementary Abelian 2-group, then we have that $\mathbf{1}(G) \le 2$ and hence that $h(G) \le 2^3$.*

Proof. Since G is Abelian, there exists an automorphism τ of G which inverts every element of G. τ has order two. So consider the holomorph $H = G\langle\tau\rangle$ of G by τ. Since $(r\tau)^2 = e$ for any element r of G, H is one-stepped.

Further, in the case of the h-index we realize that if a central involution is prescribed, the situation is much more complicated.

§5. **Two infinite families of non-Hadamard 2-groups.** It is known that there exist five non-isomorphic 2-groups of order 2^{n+1} and exponent 2^n, where $n \geqq 3$. See [**2**], $p.91$: 1) the Abelian group of type $(n, 1)$, 2) the dihedral group, 3) the generalized quaternion group, 4) the group G presented by

$$G(n) = \langle r, s \mid r^{2^n} = s^2 = e,\ \ srs = r^{1+2^{n-1}}\rangle$$

and 5) the group G presented by

$$G(n) = \langle r, s \mid r^{2^n} = s^2 = e,\ \ srs = r^{-1+2^{n-1}}\rangle.$$

The Hadamard property of groups of types 1, 2 and 3 has been investigated in [**3**], [**4**] and [**7**].

Proposition 2. *Groups of type 4 are not Hadamard.*

Proof. Assume that a group G of type 4 is Hadamard and that D is an Hadamard subset of G. Let α be a primitive 2^n-th root of unity and put $m = 2^{n-1}$. Then we have that $r^m = e^*$. Further $x^m + 1 = 0$ is the defining equation for α. Now we consider an irreducible representation F of G of degree two defined by

$$F(r) = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$$

and

$$F(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then we have that

$$F(sr) = \begin{pmatrix} 0 & -\alpha \\ \alpha & 0 \end{pmatrix}$$

and we may put

$$F(D) = \begin{pmatrix} \sum c_i\alpha^i & \sum(-1)^i d_i\alpha^i \\ \sum d_i\alpha^i & \sum(-1)^i c_i\alpha^i \end{pmatrix},$$

where $c_i = 1$ or -1 according as r^i or $r^i e^*$ belongs to D, $d_i = 1$ or -1 according as sr^i or $sr^i e^*$ belongs to D, and in each summation i runs from 0 to $m-1$. Then we have that

$$F(D)^* = \begin{pmatrix} \sum c_i\alpha^{-i} & \sum d_i\alpha^{-i} \\ \sum(-1)^i d_i\alpha^{-i} & \sum(-1)^i c_i\alpha^{-i} \end{pmatrix},$$

where the matrix operation $*$ is the composition of complex-conjugation and transposition. Now it is known that $F(D)^*F(D) = F(D)F(D)^* = 2mI$, where I denotes the identity matrix of degree two. For this see [5]. Equating $(1,1)$-entries of $F(D)^*F(D)$ and $F(D)F(D)^*$ we have that

$$(\sum c_i\alpha^{-i})(\sum c_i\alpha^{i}) + (\sum d_i\alpha^{-i})(\sum d_i\alpha^{i})$$

$$= (\sum c_i\alpha^{i})(\sum c_i\alpha^{-i}) + (\sum(-1)^i d_i\alpha^{i})(\sum(-1)^i d_i\alpha^{-i}).$$

Thus we obtain that

$$(\sum d_i\alpha^{-i})(\sum d_i\alpha^{i}) = (\sum(-1)^i d_i\alpha^{i})(\sum(-1)^i d_i\alpha^{-i}). \tag{1}$$

We multiply out both sides of (1). Then, using the defining equation $x^m + 1 = 0$ we reduce both sides to polynomials in α of degree at most $m-1$. Now equating the coefficients of α on either side we obtain that

$$d_0d_1 + d_1d_2 + \cdots + d_{m-3}d_{m-2} + d_{m-2}d_{m-1} - d_{m-1}d_0 = 0. \tag{2}$$

(2) says that the vector $d = (d_0, d_1, \ldots, d_{m-1})$ is orthogonal to its nega-cyclic shift $(-d_{m-1}, d_0, \ldots, d_{m-2})$. On the other hand, in order to estimate the inner product of a vector with its nega-cyclic shift, we may asume that $d_0 = d_{m-1} = 1$. Then we rewrite d as follows: $d = (e_1, -e_2, e_3, -e_4, \ldots, e_u)$, where each subvector e_i is an all-one vector ($i = 1, 2, \ldots, u$). Here we notice that u is odd. Now we see that the inner product of d with its nega-cyclic shift is equal to $m - 2u$. Since u is odd and m is a multiple of 4, $m - 2u$ is congruent to 2 mod 4. This contradicts (2).

Proposition 3. *Groups of type* 5 *are not Hadamard.*

Proof. Assume that a group G of type 5 is Hadamard and that D is an Hadamard subset of G. α and m are the same as in the proof of Proposition 2. Now we consider an irreducible representation F of G of degree two defined by

$$F(r) = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha^{-1} \end{pmatrix}$$

and

$$F(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then we have that

$$F(sr) = \begin{pmatrix} 0 & -\alpha^{-1} \\ \alpha & 0 \end{pmatrix}$$

and we may put

$$F(D) = \begin{pmatrix} \sum c_i\alpha^i & \sum(-1)^i d_i\alpha^{-i} \\ \sum d_i\alpha^i & \sum(-1)^i c_i\alpha^{-i} \end{pmatrix},$$

where c_i, d_i and the summation are the same as in Proposition 2. Then we have that

$$F(D)^* = \begin{pmatrix} \sum c_i \alpha^{-i} & \sum d_i \alpha^{-i} \\ \sum (-1)^i d_i \alpha^i & \sum (-1)^i c_i \alpha^i \end{pmatrix}.$$

Now equating $(1,1)$-entries of $F(D)^* F(D)$ and $F(D)F(D)^*$ we have that

$$(\sum c_i \alpha^{-i})(\sum c_i \alpha^i) + (\sum d_i \alpha^{-i})(\sum d_i \alpha^i)$$

$$= (\sum c_i \alpha^i)(\sum c_i \alpha^{-i}) + (\sum (-1)^i d_i \alpha^{-i})(\sum (-1)^i d_i \alpha^i).$$

Thus we obtain that

$$(\sum d_i \alpha^{-i})(\sum d_i \alpha^i) = (\sum (-1)^i d_i \alpha^{-i})(\sum (-1)^i d_i \alpha^i). \tag{3}$$

Comparing (3) with (1) we see that we may proceed in the same way as in the proof of Proposition 2.

REFERENCES

1. J.R. Cho, N. Ito, P.S. Kim and H.S. Sim, *Hadamard 2-groups with arbitarily large derived length*, Australas. J. Combin. **16** (1997), 83–86.
2. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.
3. N. Ito, *On Hadamard groups*, Journal of Algebra **168** (1994), 981-987.
4. N. Ito, *Some results on Hadamard groups*, Proc. Groups-Korea '94, de Gruyter, 1995, pp. 149-155..
5. N. Ito, *Note on Hadamard groups and difference sets*, Australas. J. Combin. **11** (1995), 135-138.
6. N. Ito, *Remarks on Hadamard groups*, Kyushu J. Math. **50** (1996), 83-91.
7. N. Ito, *On Hadamard groups III*, Kyushu J. Math. **51** (1997), 1-11.

(Received 26/8/97)