Hokkaido Mathematical Journal Vol. 22(1993) p. 373-378

Note on Hadamard groups of quadratic residue type

To Tosiro Tsuzuku on the occasion of his retirement

Noboru ITO
(Received January 26, 1993)

1. Introduction

In a previous paper (3) we introduced an Hadamard design and an Hadamard group as follows. An Hadamard design $D=(P, B)$ is a block design, where P and B are the sets of points and blocks respectively, satisfying the following conditions;

(1) $|P|=|B|=2n$, where $|X|$ denotes the number of elements in a finite set X. For $\alpha\in B$ we have that $|\alpha|=n$ and $P-\alpha\in B$;

(2) For α, $\beta\in B$ we have that $|\alpha\cap\beta|=n/2$, provided that $\beta\neq\alpha$ and $P-\alpha$, and

(3) We may put $P=\{a_1, \cdots, a_n, b_1, \cdots, b_n\}$ so that $|\alpha\cap\{a_i, b_i)|=1$ for any $\alpha\in B$ and $1\leq i\leq n$.

Then we consider an Hadamard design whose automorphism group contains a regular subgroup. An Hadamard group is a group theoretical formulation of such a subgroup. A group G of order $2n$ is called an Hadamard group if G contains a subset D and an element e^* satisfying the following conditions:

(4) $|D\cap Da|=n$ if $a=e$, where e denotes the identity element of G; $=0$ if $a=e^*$ and $=n/2$ for any other element a of G, and

(5) $|Da\cap\{b, be^*\}|=1$ for any elements a and b of G.

Furthermore, in (3) we gave a constrution of an Hadamard design and an Hadamard group of quadratic residue type. Let $\mathsf{GF(q)}$ be a finite field of q elements where q is a prime power such that $q\equiv 3 \pmod 4$. Further let Q and N denote the sets of quadratic residues and non-residues of $\mathsf{GF(q)}$-$\{0\}$ respectively. Now an Hadamard design $D(q)=(P(q)$, $B(q))$ of quadratic residue type is defined in the following way. $P(q)$ is the set of projective half-points. In the notation of (3) projective half-points are $\infty=\{(0, a), a\in Q\}$, $\infty^*=\{(0, a), a\in N\}$, $a=\{(b, ba), b\in Q\}$ and $a^*=\{(b, ba), b\in N\}$, where $a\in GF(q)$. Let us consider $*$ as a natural isomorphism from $GF(q)$ to its disjoint copy $GF(q)^*$. So we have that $Q^*=\{a^*, a\in Q\}$ and $N^*=\{a^*, a\in N\}$. Then $B(q)$ consists of $GF(q)\cup\{\infty\}$, Q

$+a\cup\{\infty\}\cup N^*+a^*\cup(a^*)$ and their complements, where $a\in GF(q)$.

Now an Hadamard group **G(q)** of quadratic residue type is a group of order $2(q+1)$ defined by $a^{q+1}=b^4=e$ and $b^{-1}ab=a^{-1}$. To show that **G(q)** is an Hadamard group it is natural to present **G(q)** as a subgroup of **SL(2, q)**;

$$a=\begin{pmatrix} a & b \\ b & d \end{pmatrix} \quad \text{and} \quad b=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ with } a+d=y,\ y=x+x^q$$

where x in an element of $\mathbf{GF(q^2)}$ of order $q+1$.
Then **G(q)** acts on $D(q)$ regularly and D is the set of elements of **G(q)** which transfers ∞ into $\mathbf{GF(q)}^*\cup\{\infty^*\}$.

It is well known that tetrahedral, octahedral and icosahedral subgroups of orders 12, 24 and 60 respectively are distinguished amog subgroups of **PSL(2, q)**. For this see (**1**, **2**). We keep the same names for the corresponding subgroups of orders 24, 48 and 120 of **SL(2, q)**. Moreover we call a group G tetrahedral, octahedral or icosahedral if G is isomorphic to a tetrahedral, octahedral or icosahedral subgroup of **SL(2, q)** respectively.

Now the purpose of this note is to prove the following proposition.

PROPOSITION. *Tetrahedral, octahedral and icosahedral groups are skew Hadamard groups.*

In each of these three groups there exists a unique involution. Hence it should be e^*. So it is suficient to determine D in each of these three groups which will be done separately.

2. Tetrahedral case

Let G_4 be a tetrahedral group. Then in order to show that G_4 is an Hadamard group it is natural to present G_4 as a subgroup of SL(2,11).

$$\text{Let } a=\begin{pmatrix} 0 & 10 \\ 1 & 0 \end{pmatrix},\ b=\begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix} \text{ and } c=\begin{pmatrix} 4 & 7 \\ 8 & 6 \end{pmatrix}.$$

Then we have that $a^2=b^2=e^*$, $b^{-1}ab=ae^*$, $c^3=e$, $c^{-1}ac=b$ and $c^{-1}bc=ab$. Hence $\langle a, b, c\rangle$ is a presentation of G_4. Now D is determined in the same way as $G(11)$:

$$D=\{e^*, ae^*, be^*, abe^*, c, ace^*, bce^*, abc, c^2e^*, ac^2, bc^2e^*, abc^2e^*\}.$$

In order to inspect the intersection property of D it is convenient to use the following relations; $ba=abe^*$, $ca=abc$, $c^2a=bc^2$, $cb=ac$, $bcb=$

$abce^*$ and $c^2b=abc^2$. We omit to give the details of the inspection. Instead we give the resulting Hadamard matrix. We use elements of D neglecting e^* in the order listed above as the label of row and column of the matrix. Then the matrix obtained is the following, where $+$ and $-$ denote 1 and -1 respectively:

$$\begin{pmatrix}
- & - & - & - & + & - & - & + & - & + & - & - \\
+ & - & - & + & - & - & + & + & + & + & - & + \\
+ & + & - & - & + & + & + & + & + & - & - & - \\
+ & - & + & - & + & - & + & - & - & - & - & + \\
- & + & - & - & - & - & - & - & + & - & - & + \\
+ & + & - & + & + & - & - & + & - & - & + & + \\
+ & - & - & - & + & + & - & - & + & + & + & + \\
- & - & - & + & + & - & + & - & + & - & + & - \\
+ & - & - & + & - & + & - & - & - & - & - & - \\
- & - & + & + & + & + & - & + & + & - & - & + \\
+ & + & + & + & + & - & - & - & + & + & - & - \\
+ & - & + & - & - & - & - & + & + & - & + & -
\end{pmatrix}.$$

3. Octahedral case

Let G_8 be an octahedral group. Then in order to show that G_8 is an Hadamard group it is natural to present G_8 as a subgroup of $\mathbf{SL}(2,23)$.

Let $a=\begin{pmatrix} 7 & 19 \\ 4 & 11 \end{pmatrix}$, $b=\begin{pmatrix} 10 & 9 \\ 22 & 13 \end{pmatrix}$ and $c=\begin{pmatrix} 18 & 11 \\ 19 & 4 \end{pmatrix}$.

Then we have that $a^4=b^2=e^*$, $b^{-1}ab=a^3e^*$, $c^3=e$, $c^{-1}a^2c=b$, $c^{-1}bc=a^2be^*$ and $(ab)^{-1}cab=c^{-1}$. Hence $\langle a, b, c\rangle$ is a presentation of G_8. Now D is determined in the same way as $G(23)$:

$$D=\{e^*, ae^*, a^2e^*, a^3e^*, b, abe^*, a^2b, a^3be^*, c, ac, a^2ce^*, a^3ce^*, bc, abce^*, a^2bc, a^3bce^*, c^{-1}e^*, ac^{-1}, a^2c^{-1}e^*, a^3c^{-1}, bc^{-1}e^*, abc^{-1}e^*, a^2bc^{-1}e^*, a^3bc^{-1}\}.$$

In order to inspect the intersection property of D it is convenient to use the following relations; $ba=a^3be^*$, $ca=a^3c^{-1}$, $bca=abc^{-1}e^*$, $c^{-1}a=a^3bc$, $bc^{-1}a=ac$, $cd=a^2c$, $bcb=a^2bce^*$, $c^{-1}b=a^2bc^{-1}e^*$ and $bc^{-1}b=a^2c^{-1}e^*$. We omit to give the details of the inspection. Instead we give the resulting Hadamard matrix as in the case of G_4:

```
----+-+-++--+-+--+-+---+
+----+-------+---+++--+-
++--+--++--+----+++--+-+
+++---+---+---++++-+-+++
-+-+----+++++--+-+++-++-
+-+++---++----+-+-+++++-
-++-++--+-+---++-++-+---
++-++++--+--+++++++--+--
-+-+---+----+-+-++--+-+-
-+++--+-+----+-------+--
+++--+-+++--+--++--+----
++-+-++++++---+---+---++
-+++-++--+-+----+++++--+
+-+++++-+-+++---++----+-
-++-+----++-++--+-+---++
+++--+--++-++++--+--++++
++--+-+--+-+---+----+-+-
-----+---+++--+-+----+--
+--+----+++--+-+++--+--+
--+---++++-+-++++++---+-
+++++--+-+++-++--+-+----
++----+-+-+++++-+-+++---
+-+---++-++-+----++-++--
-+--+++++++--+--++-++++-
```
.

4. Icosahedral case

Let G_{20} be an icosahedral group. Then in order to show that G_{20} is an Hadamard group it is natural to present G_{20} as a subgroup **SL(2,59)**.

Let $a=\begin{pmatrix} 6 & 47 \\ 8 & 53 \end{pmatrix}$, $b=\begin{pmatrix} 17 & 51 \\ 51 & 42 \end{pmatrix}$, $c=\begin{pmatrix} 51 & 9 \\ 33 & 7 \end{pmatrix}$ and $d=\begin{pmatrix} 46 & 3 \\ 56 & 46 \end{pmatrix}$. Then we have that $a^2=b^2=e^*$, $c^3=e$, $d^5=e$, $(da)^3=e^*$, $d^2a=cde^*$ and $c^{-1}ac=b$. Hence $\langle a, d\rangle=\langle a, b, c, d\rangle$ is a presentation of G_{20}. Now D is determined in the same way as $G(59)$:

$D=\{e^*, a, be^*, abe^*, c, ac, bc, abc, c^2e^*, ac^2, bc^2, abc^2, d, ad, bd, abd, cde^*, acde^*, bcd, abcd, c^2d, ac^2de^*, bc^2de,^*, abc^2d, d^2e^*, ad^2e^*, bd^2e^*, abd^2, cd^2, acd^2e^*, bcd^2e^*, abcd^2e^*, c^2d^2, ac^2d^2e^*, bc^2d^2e^*, abc^2d^2e^*, d^3, ad^3, bd^3e^*, abd^3, cd^3, acd^3e^*, bcd^3, abcd^3e^*, c^2d^3e^*, ac^2d^3, bc^2d^3, abc^2d^3, d^4e^*, ad^4, bd^4e^*, abd^4, cd^4e^*, acd^4e^*, bcd^4, abcd^4e^*, c^2d^4e^*, ac^2d^4e^*, bc^2d^4, abc^2d^4\}$.

In order to inspect the intersection properoy of D it is convenient to use the following relations; $ba=abe^*$, $ca=abc$, $c^2a=bc^2$, $da=c^2d^2$, $cda=d^2$, $c^2da=cd^2$, $d^2a=cde^*$, $cd^2a=c^2de^*$, $c^2d^2a=de^*$, $d^3a=abcd^4$, $cd^3a=bc^2d^4$, $c^2d^3a=ad^4$, $d^4a=ac^2d^3$, $cd^4a=abd^3$, $c^2d^4a=bcd^3$, $cb=ac$, $c^2b=abc^2$, $db=bd^4$, $cdb=acd^4$, $c^2db=abc^2d^4$, $d^2b=bd^3$, $cd^2b=acd^3$, $c^2d^2b=abc^2d^3$, $d^3b=bd^2$, $cd^3b=acd^2$ $c^2d^3b=abc^2d^2$, $d^4b=bd$, $cd^4b=acd$, $c^2d^4b=abc^2d$, $dc=abcd^3e^*$, $d^2c=ac^2d^2e^*$, $d^3c=ad^4e^*$ and $d^4c=c^2de^*$. We omit to give the details of the inspection. Instead we give the resulting Hadamard matrix as in the case of G_8:

```
−+−−++++−+++++++−−+++−−+−−−++−−−+−−−++−++−+−−+++−+−+−−+−−−++
−−−+−+−+−−−+−++++++−−+++−−+++−−++++++++−−−−−−−++−−+−−−−+−++−
++−+−++−−+−−+−−++−−−−++−+−++++−−−+−−+−−−++−++−++−−+++−+−−−++
+−−−−−++−−+−−+−−+−++++−−−++++−−+−++−−−−−++++−+−+−−−+−+−−−+−−
−+++−+−−++++++−+++−−+−+−−+−−−−−+−+−−−−−−+−+−+++++−−−−−−−+++−
−−−+−−−+−+−++++−+−−+++−+++−−++−−−+−+++−++−+++−−−+−++−+−+++++
−+−−++−+−++−−+−+++−−++−−−++−−−+−−−−+++++++−−−−−+−−+−+++−++−+
−−+−+−−−−−+++−+++−+++++−++−−+−+−++−++−+−−+++++−+−++−+−+−−++−
++++−+++−+−−++++−−−+−+++++−+−−+−+++−−−+++++−−−−−−++−−−−−++−−
−+−+−−−+−−−++−+−−−−−−+−−−++−−++−+−+−+−−−−−+−−+−++−−−+−−−−−−+
−++−−+−−++−+−−−+−−+−++−+−−−+−++++++++−+−++++−−−−+−−+−++−−+++
−−++−−+−+−−−−+−++−−++−−+−−−−−+−−+−+−+−+++−−−++−+−−+++−++−+−−
−+−+−−+−−−++−+−−++++−+++++++−−+++−−+−−−++−−−+−−−++−++−+−−+++
−−+−−−−+−++−−−−+−+−+−−−+−++++++−−+++−−+++−−++++++++−−−−−−−++
−−+++−+−−−++++−+−++−−+−−+−−++−−−−++−+−++++−−−+−−+−−−++−++−++
−−−+−+−−−+−−+−−−−−++−−+−−+−−+−++++−−−++++−−+−++−−−−−++++−+−+
+−−−−−−−+++−−+++−+−−++++++−+++−−+−+−−+−−−−−+−+−−−−−−+−+−++++
+−++−+−+++++−−−+−−−+−+−++++−+−−+++−+++−−++−−−+−+++−++−+++−−−
−−+−+++−++−+−+−−++−+−++−−+−+++−−++−−−++−−−+−−−−+++++++−−−−−+
−++−+−+−−++−−−+−+−−−−−+++−+++−+++++−++−−+−+−++−++−+−−++++−−+
−++−−−−−++−−++++−+++−+−−++++−−−+−+++++−+−−+−+++−−−+++++−−−−−
+−−−+−−−−−−+−+−+−−−+−−−++−+−−−−−−+−−−++−−++−+−+−+−−−−−+−−+−+
+−−+−++−−+++−++−−+−−++−+−−−+−−+−++−+−−−+−++++++++−+−++++−−−−
−−+++−++−+−−−−++−−+−+−−−−+−++−−++−−+−−−−−+−−+−+−+−+++−−−++−+
++−++−+−−+++−+−+−−+−−−++−+−−++++−+++++++−−+++−−+−−−++−−−+−−−
+++−−−−−−−++−−+−−−−+−++−−−−+−+−+−−−+−++++++−−+++−−+++−−+++++
+−−−++−++−++−−+++−+−−−++++−+−++−−+−−+−−++−−−−++−+−++++−−−+−−
−−−−++++−+−+−−−+−+−−−+−−+−−−−−++−−+−−+−−+−++++−−−++++−−+−++−
−−−−+−+−+++++−−−−−−−+++−−+++−+−−++++++−+++−−+−+−−+−−−−−+−+−−
++−++−+++−−−+−++−+−+++++−−−+−−−+−+−++++−+−−+++−+++−−++−−−+−+
++++++−−−−−+−−+−+++−++−+−+−−++−+−++−−+−+++−−++−−−++−−−+−−−−+
+−+−−+++++−+−++−+−+−−++−−−+−+−−−−−+++−+++−+++++−++−−+−+−++−+
−−+++++−−−−−−++−−−−−++−−++++−+++−+−−++++−−−+−+++++−+−−+−+++−
+−−−−−+−−+−++−−−+−−−−−−+−+−+−−−+−−−++−+−−−−−−+−−−++−−++−+−+−
+−+−++++−−−−+−−+−++−−+++−++−−+−−++−+−−−+−−+−++−+−−−+−+++++++
+−+++−−−++−+−−+++−++−+−−−−++−−+−+−−−−+−++−−++−−+−−−−−+−−+−+−
−−−++−−−+−−−++−++−+−−+++−+−+−−+−−−++−+−−++++−+++++++−−+++−−+
−−+++−−++++++++−−−−−−−+−−−+−−−−+−++−−−−+−+−+−−−+−++++++−−+++
+−++++−−−+−−+−−−++−++−++−−+++−+−−−++++−+−++−−+−−+−−++−−−−++−
−++++−−+−++−−−−−++++−+−+−−−+−+−−−+−−+−−−−−++−−+−−+−−+−++++−−
−+−−−−−+−+−−−−−−+−+−+++++−−−−−−−+++−−+++−+−−++++++−+++−−+−+−
++−−++−−−+−+++−++−+++−−−+−++−+−+++++−−−+−−−+−+−++++−+−−+++−+
−++−−−+−−−−+++++++−−−−−+−−+−+++−++−+−+−−++−+−++−−+−+++−−+−−−
++−−+−+−++−++−+−−+++++−+−++−+−+−−++−−−+−+−−−−−+++−+++−+++++−
++−+−−+−+++−−−+++++−−−−−−++−−−−−++−−++++−+++−+−−+++++−−+−+++
−++−−++−+−+−+−−−−−+−−+−++−−−+−−−−−−+−+−+−−−+−−−++−+−−−−−−+−−
−−−+−++++++++−+−++++−−−−+−−+−++−−+++−++−−+−−++−+−−−+−−+−++−+
−−−−−+−−+−+−+−+++−−−++−+−−+++−++−+−−−−++−−+−+−−−−+−++−−++−−+
++++−−+++−−+−−−++−−−+−−−++−++−+−−+++−+−+−−+−−−++−+−−++++−+++
−++++++−−+++−−+++−−++++++++−−−−−−−++−−+−−−−+−++−−−−+−+−+−−−+
+−−++−−−−++−+−++++−−−+−−+−−−++−++−++−−+++−+−−−++++−+−++−−+−−
−+−−+−++++−−−++++−−+−++−−−−−++++−+−+−−−+−+−−−+−−+−−−−−++−−+−
++−+++−−+−+−−+−−−−−+−+−−−−−−+−+−+++++−−−−−−−+++−−+++−+−−++++
+++−+−−+++−+++−−++−−−+−+++−++−+++−−−+−++−+−+++++−−−+−−−+−+−+
−+−+++−−++−−−++−−−+−−−−+++++++−−−−−+−−+−+++−++−+−+−−++−+−++−
+−+++−+++++−++−−+−+−++−++−+−−+++++−+−++−+−+−−++−−−+−+−−−−−++
++++−−−+−++++++−+−−+−+++−−−+++++−−−−−++−−−−−++−−++++−+++−+−−
+−+−−−−−−+−−−++−−++−+−+−+−−−−−+−−+−++−−−+−−−−−−+−+−+−−−+−−−+
−−−+−−+−++−+−−−+−++++++++−+−++++−−−−+−−+−++−−+++−++−−+−−++−+
−+−++−−++−−+−−−−−+−−+−+−+−+++−−−++−+−−+++−++−+−−−−++−−+−+−−−
```
.

5. Remarks

We collect here group theoretical facts of Hadamard groups so far constructed.

(i) All Hadamard groups constructed in (**3**) are 2-nilpotent and metabelian. G_4 and G_8 are neither 2-nilpotent nor metabelian. G_4 and G_8 have derived lengths 3 and 4 respectively.

(ii) Using Dirichlet's theorem we see that any prime p divides the order of some Hadamard group of quadratic residue type. For $p>5$ a Sylow p-subgroup is normal in every Hadamard group so far constructed.

(iii) G_{20} is non-solvable and isomorphic to $SL(2,5)$. So far $PSL(2, 5)$ is an only non-Abelian composition factor appearing in Hadamard groups.

References

[1] L. E. DICKSON, Linear groups with an exposition of the Galois field thory. Dover, 1958.
[2] B. HUPPERT, Endliche Gruppen I. Springer, 1967.
[3] N. ITO, On Hadamard groups. To appear in Journal of Algebra.

Department of Mathematics
Meijo University
Nagoya, Tenpaku 468, Japan