<table>
<thead>
<tr>
<th>Title</th>
<th>On the Higman-Sims Simple Group of Order $44,352,000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11 = 176 \cdot 175 \cdot 10 \cdot 9 \cdot 8 \cdot 2$ (有限群論)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>KIMURA, HIROSHI</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 1976, 277: 58-66</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1976-08</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/106005">http://hdl.handle.net/2433/106005</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
On the Higman-Sims simple group of order $44,352,000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$

$= 176 \cdot 175 \cdot 10 \cdot 9 \cdot 8 \cdot 2$

Let $y$ be a field automorphism of $\PGL(2,q^2)$ of order 2, where $q$ is a power of an odd prime number.

**Theorem.** Let $G$ be a 2-transitive group on $\Omega = \{1,2,\ldots,n\}$, $n$ is even. If $G_{1,2}$ is $\PGL(2,q^2)\langle y \rangle$, then either

(1) $G$ has a RNS, or

(2) $q = 3$, $n = 176$ and $G$ is the Higman-Sims simple group.

I gave an outline of a proof of this theorem.

**Notation:** Let $X$ be a subset of a permutation group $Y$.

Let $F(X)$ denote the set of all fixed points of $X$ and $\alpha(X)$ be the number of points in $F(X)$. $N_Y(X)$ acts on $F(X)$.

Let $\chi_1(X)$ and $\chi(X)$ be the kernel of this representation and its image, respectively.

1. Properties of $\PGL(2,q^2)\langle y \rangle$.

Let $t'$ be an element of $\PGL(2,q^2)$ of order $q^2 - 1$ and $x$ be an involution of $\PSL(2,q^2)$ which normalizes $\langle t' \rangle$. Set $<s> = O_2(<t'>)$ and $<t> = 0(<t'>)$. We may assume $<t'>^Y = <t'>$ and $[x,y] = 1$. Let $\tau$ be a unique involution of $<s>$.

1.1 $<y,s>$ is quasi-dihedral if $4 | q - 1$ and

$<yx,s>$ is quasi-dihedral if $4 | q - 1$
(1.2) $\text{PGL}(2,q^2)<y>$ has 3 classes of involutions.

$\tau$, $y$ and $xs$ are representatives of these classes.

2. Let $I$ be an involution of $G$ with the cycle structure $(1,2)\cdots$.

Then $I$ normalizes $G_{1,2}$ and we may assume $[I,G_{1,2}] = 1$. By $(1.2)$ every involution of $G$ is conjugate to $I$, $I\tau$, $Ixs$ or $Iy$.

3. Conjugation of involutions.

Lemma 3.1. $\tau \sim y$, $xs$.

Lemma 3.2. $y \sim xs$

By Lemma 3.1 and a theorem of Witt $\chi(\tau)$ is 2-transitive on $F(\tau)$.

4. Structure of $\chi(\tau)$.

Let $\bar{g}$ denote the image in $\chi(\tau)$ of an element $g$ of $G_{g}(\tau)$.

Lemma 4.1. $\chi(\bar{x})$ is 2-transitive on $F(\bar{x})$.

Let $T$ be a Sylow 2-subgroup of $\chi_{1}(\tau)$ contained in $S = <x,s,y>$.

By the structure of $\chi(\tau)_{1,2}$ we have the following cases.

(I) $s^2 \notin T \triangleleft <s>$

(II) $s^2 \in T \triangleleft <s>$

(III) $T \subseteq <s>$.

Lemma 4.5. $\chi(\tau) \supset RNS \Rightarrow T \sim \tau$.

Lemma 4.6. $\chi(\tau) \supset RNS \Rightarrow q = 3$

$Iy \sim \tau$

Lemma 4.7. $\alpha(\tau)$ is a power of 2 $\Rightarrow IXS \sim \tau$.

Lemma 4.12. $q = 3$ or $F \neq 1$.

Lemma 4.4. In the case (I) $T = <xys^j>$ or $<ys^j>$

\[ [s^j,xy] = 1 \quad [y,s^j] = 1 \]
where \(|s^j| = 4\), and \(\chi(\tau) \not\subset RNS\).

5. The case (I)

Lemma 5.1. \(q = 3 \Rightarrow G \text{ is H-S}\)

Lemma 5.2. \(q \neq 3 \Rightarrow G \not\supset RNS\).

6. The case (II)

There is no group satisfying the conditions in Theorem.

7. The case (III).

Lemma 7.10. \(T = \langle \tau \rangle\).

Lemma 7.11. \(\chi(\tau) \not\subset RNS \Rightarrow q \neq 3\).

Lemma 7.12. \(\chi(\overline{x}) \not\subset RNS\).

From these lemmas we have that \(G\) has a RNS.

8. By the proof of Theorem we have the following.

Corollary. Let \(G\) be as in Theorem. If \(G\) has a RNS, the following conditions are satisfied.

(1) \(n = \alpha(\tau)^2 = \alpha(y)^2\).

(2) \(\overline{x} \neq 1\), and

(3) \(\chi_1(\tau) = \langle xys'\rangle\) if \(<y,s>\) is quasi-dihedral,

\(\chi_1(\tau) = \langle ys'\rangle\) if \(<xy,s>\) is quasi-dihedral

or

\(\chi_1(\tau) = \langle \tau \rangle\), where \(s'\) is an element of \(<s>\) of order 4.

Important theorems for the proof of Theorem are the following:

1. Theorems of Aschbacher.

(1) Doubly transitive groups in which the stabilizer of two points is abelian, J. Alg. 18 (1971).
(11) 2-transitive groups whose 2-point stabilizer has 2-rank 1, J. Alg. 36 (1975).

2. A theorem of Baer.

3. A Theorem of Bender.


5. Degree formula (Ito-Nagao-Kimura).
Let $G$ be a 2-transitive group on $\Omega = \{1, \cdots, n\}$. Let $\xi$ be an involution of $G_{1,2}$. Let $B(\xi)$ be the number of involutions of $G$ with cycle structures $(1,2) \cdots$ which are conjugate to $\xi$ and $\gamma(\xi)$ be the number of involutions of $G_{1,2}$ which are conjugate to $\xi$. Then

$$n = \frac{B(\xi)}{\gamma(\xi)} \alpha(\xi)(\alpha(\xi)-1) + \alpha(\xi),$$

and

$$|C_G(\xi)| = \alpha(\xi)(\alpha(\xi)-1) \frac{|G_{1,2}|}{\gamma(\xi)}.$$ 

Degree formula is useful in a proof of Theorem.

As an example we shall prove Lemma 3.1. and the case (I).

Proof of Lemma 3.1.

| $|G_{1,2}:C_{G_{1,2}}(\xi)|$ | $\tau$ | $\gamma$ | $\chi_s$ |
|-----------------|-------|--------|--------|
| $q^2(q^2+1)$    | $\frac{q^2(q^2+1)}{2}$ | $q(q^2+1)$ | $\frac{q^2(q^2-1)}{2}$ |
| ($q = 3$)       | 45    | 30     | 36     |

- 4 -
(1) Assume $\tau \sim y \sim x$. Since $\gamma(\tau) = |G_{1,2}|(1/4(q^2 - 1)
+ 1/2q(q^2 - 1)) = |G_{1,2}|(q + 2)/4q(q^2 - 1)$,

$|C_{G}(\tau)| = 4i(1 - 1)q(q^2 - 1)/(q + 2)$ by the degree formula.

We next prove $\chi(\tau)$ is a rank 3 permutation group on $F(\tau)$ with subdegrees $1$, $q(1 - 1)/q + 2$ and $2(1 - 1)/q + 2$. Consider the length of the $C_{G_{1}}(\tau)$-orbit containing the point 2.

$|2^{G_{1}}| = |C_{G_{1}}(\tau) : C_{G_{1,2}}(\tau)|$.

$= |C_{G}(\tau) : C_{G_{1,2}}(\tau)|/|C_{G}(\tau) : C_{G_{1}}(\tau)|$.

$= i(1 - 1)q/i'(q + 2)$, where $i' = |C_{G}(\tau) : C_{G_{1}}(\tau)|$. Similarly

$|2^{G_{1}}| = 2i(1 - 1)/i''(q + 2)$, where $i'' = |C_{G}(y) : C_{G_{1}}(y)|$.

Set $y^g = \tau$ with $g$ in $G$. If $1^G(\tau)$ and $(1^G(y))^g$ are different $C_{G}(\tau)$-orbits, then $1 - 1 \leq 1(1 - 1)q/i'(q + 2)
+ 2i(1 - 1)/i''(q + 2) \leq 1 - 2$, a contradiction. Thus

$C_{G_{1}}(\tau) = (1^G(y))^g = 1^{G_{1}}(\tau)$ and $i' = i''$. Since $|2^{G_{1}}|$

$C_{G_{1}}(y)^g$,

$|2^{G_{1}}|$, $C_{G_{1}}(\tau)$ has at least three orbits of length 1,

$C_{G_{1}}(\tau)$ and $|2^{G_{1}}|$. Thus $1 - 1 \leq 1(1 - 1)q/i'(q + 2)
+ 2i(1 - 1)/i'(q + 2) \leq 1 - 1$. Hence $i = i'$ and $\chi(\tau)$ is of rank 3. $C_{G_{1,2}}(y)$ is conjugate to a subgroup of $C_{G_{1}}(\tau)$. Since
<s, x, y> is a Sylow 2-subgroup of $\text{C}_{G_1}(\tau)$ and $u^2 = \tau$ for every element $u$ in $<s, x, y>$ of order 4, a square of every element in $\text{C}_{G_{1,2}}(y)$ of order 4 is $y$. On the other hand $\text{C}_{G_{1,2}}(y)$ is isomorphic to $\text{PGL}(2, q) \times <y>$, a contradiction.

(2). Assume $\tau \sim xs \sim y$. As in the case (1), $\chi(\tau)$ is also of rank 3. Thus $\text{C}_{G_{1,2}}(xs)$ is conjugate to a subgroup of $\text{C}_{G_1}(\tau)$. A Sylow 2-subgroup of $\text{C}_{G_{1,2}}(xs)$ is $<xs> \times Z_4$, which is a contradiction.

(3). Assume $\tau \sim y \sim xs$. As in the case (1), $\chi(\tau)$ is of rank 4 and we have also a contradiction. This proves the lemma.
The case I

Lemma 5.1. In the case I G is the Higman-Sims simple group if $\bar{e} = 1$.

Proof. By Lemma 4.12 $q = 3$. By Lemma 4.4 $T$ is $\langle x, y^2 \rangle$, $\langle \bar{x}, \bar{e} \rangle$ is dihedral of order 8 and $\chi(\tau)$ has a RNS. Since $\chi(\tau)_{1,2}$ is non-abelian, $\chi(\tau)$ is not solvable by [7]. By Lemma 4.1 $\chi(\tau)_{1}$ has two classes of involutions. By [5. Theorem 7.7.3] $\chi(\tau)_{1}$ has a subgroup $X$ of index 2 and $X_{1,2}$ is a four-group. By [1] $\chi(\tau)$ is a semi-direct product of $V$ by $\text{PSL}(2, 4)$, where $V$ is a 2-dimensional vector space over the field $GF(4)$ of 4 elements, and $i = 16$. By Lemma 4.5 and Lemma 4.7 $\tau$ is not conjugate to $I$ or $I_\alpha$.

By Lemma 3.3 $\chi(y)$ is a rank 3 group on $F(y)$ with subdegrees 1, 5(\(\alpha(y) - 1)/11\) and 6(\(\alpha(y) - 1)/11\). Set $\alpha(y) = 11m + 1$.

If $\tau \sim I \tau \sim I y$, $\gamma(\tau) = \beta(\tau)$ and $n = 16^2$. Since $\gamma(y) = 66$, by the degree formula $11m(11m + 1) \beta(y)/66 + 11m + 1 = 16^2$, where $\beta(y)$ is a sum of elements in a subset of $\{1, 30, 36\}$. A calculation yields that there exists no integer $m$ satisfying the above condition. Similarly we have a contradiction in the case $\tau \sim I \tau \sim I y$. Thus $\tau \sim I y \sim I \tau$, $y \sim I \tau \sim I \bar{x}$, $\chi(y) = 12$ and $n = 30 \cdot 16 \cdot 15/45 + 16 = 176$.

Finally we shall prove the simplicity of $G$. Let $N$ be a minimal normal subgroup. If $N$ is Frobenius group, $G$ has
a RNS and n must be a power of 2. Therefore $N_{1,2}$ contains $\text{PSL}(2, 9)$. If $N_{1,2} = \text{PSL}(2, 9)$, the image in $\chi(\tau)_{1,2}$ of $C_N(\tau)_{1,2}$ is $<\bar{x}, \bar{s}^2>$ since $\chi_1(\tau) = <xs^2>$. We have $\bar{x} \sim \bar{s}^2$ since $\chi(\tau)_1 = \text{PGL}(2, 4)$. This contradicts Lemma 4.1. If $N_{1,2} = \text{PSL}(2, 9)<ys>$, the image in $\chi(\tau)_{1,2}$ of $C_N(\tau)_{1,2}$ is isomorphic to $<\bar{x}, s^2, ys>/<\tau>$, a contradiction. Thus $N_{1,2}$ contains $y$.

Since $y \sim x_s$, $N_{1,2} = G_{1,2}$. Since $\chi(\tau)$ is generated by $\bar{x}$ and $\bar{s}x(\tau)$, the image in $\chi(\tau)$ of $C_N(\tau)$ is $\chi(\tau)$, that is, $C_N(\tau) = C_G(\tau)$. Since $Z(<x, s, y>) = <\tau>$, $N_{G_1}(<x, s, y>)$ is contained in $C_{G_1}(\tau)$. By the Frattini argument $G_1 = N_1 N_{G_1}(<x, s, y>) = N_1$.

Thus $G = N$. By Parrott-Wong, $G$ is the Higman-Sims simple group. This completes a proof of Lemma 5.1.

Lemma 5.2. In the case I G has a RNS if $\bar{t} \neq 1$.

Proof. By Lemma 4.4 $\chi(\tau)$ has a RNS. Therefore by Lemma 4.5-Lemma 4.7 $\tau$ is not conjugate to $I$, $Iy$ or $Ixs$ and $\tau \sim _{Ix}$. By the degree formula $n = 1^2$. By Lemma 3.2 $\gamma(y) =$ even. Since $\alpha(y)$ is even, $\beta(y)$ must be even by the degree formula.

Thus $y \sim I$ and $\alpha(I) = 0$. Assume $<y, s>$ is quasidihedral. $I$ is contained in a RNS of $\chi(\tau)$. By Lemma 4.1 $\bar{x}$ is not conjugate to $\bar{s}^J$. If $\bar{s}^J \sim \bar{x}$, $\chi(\tau)_1$ has three classes of involutions, it is solvable by [5, Theorem 7.7.3] and so is $\chi(\tau)$. This contradicts [8]. Thus $\bar{s}^J \sim \bar{xs}$. Since $[\chi(\tau)_{1,2} : C_{\chi(\tau)_{1,2}}(\bar{u})]$ is
even, where \( \bar{u} \) is \( \bar{x} \) or \( \bar{xs} \) and it is 1 for \( \bar{u} = \bar{s}^j \), \( \gamma(\bar{s}^j) \) is odd and \( \gamma(\bar{x}) \) is even. By the degree formula \( \beta(\bar{s}^j) \) is odd and \( \beta(\bar{x}) \) is even, that is, \( I\bar{s}^j \sim \bar{s}^j \). Since \( Is^j_T = \{Is^j, Is^j, Ixy, Ixy\} \) and \( s^j_T = \{s^j, s^j, xy, xy\} \), \( Ixy \sim xy \) and hence \( Iy \sim y \). Since \( x_T = \{x, x, ys^j, ys^j\} \) and \( Ix_T = \{Ix, Ix, Iys^1J, Iys^1J\} \), \( x \sim Ix \). Therefore \( IxS \sim Is^j \) since \( a(IxS) > 0 \), that is, \( Iy \sim Ix \).

This proves that \( IG_{1,2} \) contains a unique fixed point free involution \( I \) and \( n \) is a power of 2. By Lemma 2.2 \( G \) has a RNS. This completes a proof of the lemma.