I.Korchagina
Nagoya Math. J.
Vol. 171 (2003), 197–206

ON A THEOREM OF P. FONG

INNA KORCHAGINA

Abstract. This paper is a contribution to the "revision" project of Gorenstein, Lyons and Solomon, whose goal is to produce a unified proof of the Classification of Finite Simple Groups.

§1.

This paper is a contribution to the "revision" project of Gorenstein, Lyons and Solomon, whose goal is to produce a unified proof of the Classification Theorem of Finite Simple Groups [GLS]. Theorem $\mathcal{C}_2$ [GLS2] is the part of the proof of the Classification Theorem which deals with the "small odd cases". One case of this theorem is the following result:

Theorem. *If G is a finite simple group of odd type and of 2-rank 3 (where the 2-rank of G is a 2-rank of a Sylow 2-subgroup of G), then one of the following holds*:

(1) $G \cong {}^2G_2(q)$ *for some* $q = 3^{2n+1}$, $n \geq 1$;

(2) $G \cong G_2(q)$ *for some odd* q *with* $q > 3$;

(3) $G \cong {}^3D_4(q)$ *for some odd* q; *or*

(4) $G \cong M_{12}$, J_1 *or* ON.

In order to prove this theorem, one begins by showing that $G \approx G^*$ for some $G^* \in \{{}^2G_2(q), G_2(q), {}^3D_4(q), M_{12}, J_1, ON\}$ with q odd, which means that the following conditions hold:

(1) G and G^* have isomorphic Sylow 2-subgroups;

(2) G has exactly one class of involutions z^G; and

(3) If $C = C_G(z)$, then $C \cong C_{G^*}(z^*)$ for z^* an involution of G^*.

Received February 25, 2002.
2000 Mathematics Subject Classification: 20E32.

At this time the proof splits into two major cases. The first one deals with the situation $G^* = {}^2G_2(q)$. In the second case, $C_G(z)$ has a subgroup K of index 2 with $K = K_1 \circ K_2$ and $K_i \cong SL_2(r_i)$ (i.e., $[K_1, K_2] = 1$, $K_1 \cap K_2 = Z(K) = Z(K_i) = \langle z \rangle$), where $r_2 = q$ and $r_1 = q$ or q^3. The analysis depends on the values of the parameters r_1 and r_2. If $r_1 > r_2$ or $r_1 = r_2 \neq 3^n$, then local analysis shows that $G \cong {}^3D_4(q)$ or $G_2(q)$. Finally, suppose that $q = r_1 = r_2 = 3^n$ with $n \geq 2$. The crucial point of the analysis is to show that the centralizer of the central involution does not contain a Sylow 3-subgroup of G. If $q > 9$, this is a fairly easy application of an order formula obtained by Brauer using modular character theory. This was proved by Fong and Wong [FW]. Unfortunately for the case $q = 9$, this proof does not work. One has to try to come up with a different trick. This is achieved in the theorem which we state:

THEOREM 1.1. *There is no finite group G satisfying the following conditions:*

(1) *G has a unique conjugacy class of involutions*;

(2) *If z is an involution of G, then $C_G(z) = (L_1 \circ L_2)T$, where $L_i \cong SL_2(9)$, $T \cong \mathbb{Z}_2$ (i.e., $[L_1, L_2] = 1$ and $L_1 \cap L_2 = \langle z \rangle$) and $C_G(z)/L_i \cong PGL_2(9)$ for $i = 1, 2$;*

(3) *For every nontrivial 3-subgroup $P \leq C_G(z)$, we have $N_G(P) \leq C_G(z)$;*

(4) *Every nontrivial 5-element of G is conjugate to some nontrivial 5-element of $L_1 \cup L_2$ and $C_G(s) \leq C_G(z)$ for all nontrivial 5-elements $s \in L_1 \cup L_2$; and*

(5) *7 divides the order of G.*

We remark that (3), (4) and (5) follow by local group theory method from (1), (2) and the hypothesis that $C_G(z)$ contains a Sylow 3-subgroup of G [GLS2]. Thus Theorem 1.1 leads one to the desired goal: $G \cong G_2(9)$. This result was first announced by P. Fong in [F1]. If $G \approx G_2(9)$, then his proof, an elaborate exercise in exceptional character theory, occupies 25 pages of unpublished notes [F2]. In this paper we give a considerably shorter proof of this result. We begin in the same way as Fong by establishing a group order formula (equation (5) below) using the work of M. Suzuki, but then we apply a theorem of Frobenius in the manner of Lyons [L]. Combining those two results with the Chinese Remainder Theorem and Sylow's Theorem, we obtain an easy contradiction, proving the result. We refer the reader to [Co] for the basic terminology and results of exceptional character theory.

We now begin the proof. We assume the contrary and proceed to a contradiction in a sequence of lemmas. Fix a nontrivial involution $z \in G$ and let $C = C_G(z)$.

Consider the set $S \subseteq C$ which consists of the following elements:

($\mathcal{S}1$) roots of z;

($\mathcal{S}2$) 3-singular elements; and

($\mathcal{S}3$) non-trivial 5-elements of $L_1 \cup L_2$.

For $s \in S$, we let $C^*_G(s) = \{g \in G | s^g = s\} \cup \{g \in G | s^g = s^{-1}\}$.

LEMMA 1.2. *If $s \in S$, then $C^*_G(s) \leq C$.*

Proof. There are three types of elements in S. Let us deal with them one by one. If s is a root of z, then clearly $C^*_G(s) \leq C$. If s is a 3-element, then the result follows from the hypothesis of the theorem. But this immediately implies the result for all 3-singular elements. Finally if $s \in S$ is a 5-element, we have the following:

$$C^*_G(s) \geq C^*_C(s) \geq C_C(s) = C_G(s).$$

But $|C^*_G(s) : C_G(s)| \leq 2$, while $|C^*_C(s) : C_C(s)| = 2$. Thus $C^*_G(s) \leq C$.

LEMMA 1.3. *S is a closed set of special classes.*

Proof. There are four things that we must check:
(1) S is a normal subset of C;
(2) Whenever $s \in S$, every generator of $\langle s \rangle$ also lies in S;
(3) Whenever s_1 and s_2 are elements of S which are conjugate in G, then s_1 and s_2 are conjugate in C; and
(4) If $s \in S$, then $C_G(s) \leq C$.

Clearly conditions (1) and (2) follow immediately from the definition of S. Condition (4) follows from Lemma 1.2. Finally let us deal with the condition (3). If s_1, s_2 are the roots of z and $h \in G$ is such that $s_1 = s_2^h$, then $z^h = z$, and so $h \in C$.

Finally suppose that either s_1, s_2 are nontrivial G-conjugate 3-singular elements of S, or s_1 and s_2 are nontrivial G-conjugate 5-elements of S.

Then there exists $h \in G$ with $s_1 = s_2^h$ and so $C_G(s_1) = C_G(s_2^h) = C_G(s_2)^h$. In both cases $\langle z \rangle$ is the unique Sylow 2-subgroup of $Z(C_G(s_i))$. Hence $\langle z \rangle$ is a characteristic subgroup of $C_G(s_i)$ for $i = 1, 2$. Therefore $\langle z \rangle^h = \langle z \rangle$, and so $h \in C$.

Corollary 1.4. *Induction is an isometry from the set $\mathcal{M}_C(S)$ of class functions of C which vanish outside of S to the character ring $\mathcal{C}h(G)$ of G.*

Proof. Since S is a closed set of special classes of C, the result follows immediately from Theorem 9 in [Co].

Lemma 1.5. *There exists a class function θ of C such that $\theta \in \mathcal{M}_C(S)$ and the following conditions hold*:

(1) $(\theta, \theta)_C = 3$;
(2) $(\theta, \theta)_C = (\theta^G, \theta^G)_G$; *and*
(3) $(\theta^G, 1_G) = 1$.

Proof. Let us simply construct such a class function. Consider $X_1 \times X_2$ with $X_i \cong PGL_2(9)$, $i = 1, 2$. Let χ_i be a Steinberg character of X_i, $i = 1, 2$. Then $\chi_1 \times \chi_2$ is an irreducible character of a group isomorphic to $PGL_2(9) \times PGL_2(9)$ (4.21 [Is]). Take the lift of $\chi_1 \times \chi_2$ to the double cover C^* of $PGL_2(9) \times PGL_2(9)$, which contains C as a subgroup of index 2. Now define α to be the restriction of this lift to C, i.e., α is an irreducible character of C of degree 81 with $\ker(\alpha) = \langle z \rangle$.

Let ρ be an irreducible character of $L_1 \circ L_2$ of degree 8 with $\ker(\rho) = L_2$ and λ be one of the two irreducible characters of $L_1 \circ L_2$ of degree 5 with $\ker(\lambda) = L_1$. Denote $\beta = (\rho \cdot \lambda)^C$. Then β is an irreducible character of C of degree 80 such that $\ker(\beta) = \langle z \rangle$ and $\beta|_{L_1 \circ L_2} = \rho \cdot (\lambda + \lambda')$ where λ' is the other character of $L_1 \circ L_2$ of degree 5 with L_1 in its kernel.

Finally consider the following class function: $\theta = 1_C + \beta - \alpha$. By direct calculations, we see that θ vanishes outside of S. Let us study some properties of θ. Clearly $(\theta, \theta)_C = (1_C + \beta - \alpha, 1_C + \beta - \alpha)_C = 3$. Also by Corollary 1.4, $(\theta, \theta)_C = (\theta^G, \theta^G)_G$. Finally, by Frobenius Reciprocity (p.62, [Is]), $(\theta^G, 1_G) = (\theta, 1_H) = 1$.

This lemma has very important consequences:

Corollary 1.6. *There exist irreducible complex characters Ψ, Φ of G such that $\theta^G = 1_G + \Psi - \Phi$, and the following conditions hold*:

(1) $\Phi(1) = 1 + \Psi(1)$ *and* $\Phi(z) = 1 + \Psi(z)$; *and*
(2) $|\Psi(z)| \leq 509$.

Proof. Since $\theta^G(1) = 0$, Lemma 1.5 implies the existence of irreducible complex characters Ψ, Φ of G such that $\theta^G = 1_G + \Psi - \Phi$. Moreover since $\theta^G(z) = 0$, condition (1) of the corollary obviously holds.

Finally, $1 + \Psi(z)^2 + \Phi(z)^2 \leq \sum_\chi \chi(z)^2$, where the summation is taken over all the irreducible characters of G. But $\sum_\chi \chi(z)^2 = |C|$ by Orthogonality Relations (p.21, [Is]). Applying condition (1), we obtain that $1 + \Psi(z)^2 + (\Psi(z) + 1)^2 \leq |C|$ which implies that $|\Psi(z)| \leq 509$.

Next define a complex-valued class function ξ of G by

$$\xi(h) = \sum_\chi \frac{\chi(z)^2}{\chi(1)} \chi(h) \tag{1.1}$$

where the summation is taken over all the irreducible characters of G. Let us use a simple manipulation to present ξ in a slightly different way:

$$\xi(h) = \frac{|G|}{|C|^2} \sum_\chi \frac{\chi(z)^2}{\chi(1)} \chi(h) \frac{|C|^2}{|G|} = a_{zzh} \frac{|C|^2}{|G|} = a_{zz}(h) \frac{|C|^2}{|G|} \tag{1.2}$$

where $a_{zz} : G \to \mathbf{C}$ is the class function defined for all $h \in G$ by

$$a_{zz}(h) = a_{zzh} = |\{(h_1, h_2) \in z^G \times z^G : \ h_1 h_2 = h\}|$$

Since ξ is a complex-valued class function on G, we may calculate $(\theta^G, \xi)_G$:

$$(\theta^G, \xi)_G = \left(1_G + \Psi - \Phi, \sum_\chi \frac{\chi(z)^2}{\chi(1)} \chi\right)_G = 1 + \frac{\Psi(z)^2}{\Psi(1)} - \frac{\Phi(z)^2}{\Phi(1)}$$

Using Corollary 1.6(1), we obtain the following formula:

$$(\theta^G, \xi)_G = 1 + \frac{\Psi(z)^2}{\Psi(1)} - \frac{(\Psi(z) + 1)^2}{\Psi(1) + 1} = \frac{(\Psi(1) - \Psi(z))^2}{\Psi(1) \cdot (\Psi(1) + 1)} \tag{1.3}$$

On the other hand using Frobenius Reciprocity and formula (1.2), we have:

$$(\theta^G, \xi)_G = (\theta, \xi|_C)_C = \left(\theta, \frac{|C|^2}{|G|} a_{zz}|_C\right)_C = \frac{|C|^2}{|G|} (\theta, a_{zz}|_C)_C$$

Since θ vanishes outside of S, we basically are dealing with $a_{zz}|_S$. Since $h_i s h_i = s^{-1}$ for $i = 1, 2$, we have that $h_i \in C^*_G(s)$. But by Lemma 1.2, if

$s \in S$, then $C^*_G(s) \leq C$ and so for every $s \in S$ we have that a_{zzs} can be written as

$$a_{zzs} = a'_{zzs} + a'_{zts} + a'_{zls} + a'_{tts} + a'_{tzs} + a'_{tls} + a'_{lls} + a'_{lzs} + a'_{lts}$$

where $a'_{zzs}, \ldots, a'_{lts}$ are algebra constants of C with z, t, l being the representatives of all the conjugacy classes of involutions in C, for $z^G|_C = \{z\} \cup t^C \cup l^C$. Notice that the only element of S inverted by z is z itself. Clearly $a'_{zhz} = 0$ for all $h \in C - \{1\}$. So we must have $a'_{zzs} = a'_{zts} = a'_{zls} = a'_{tzs} = a'_{lzs} = 0$. Therefore

$$a_{zzs} = a'_{tts} + a'_{tls} + a'_{lls} + a'_{lts}.$$

All this allows us to reduce the situation to the calculations inside C. So we obtain the following result:

$$(\theta^G, \xi)_G = \frac{2^{14} \cdot 3^8 \cdot 5^3 \cdot 41^2}{|G|} \tag{1.4}$$

Finally combining (1.3) and (1.4) we obtain:

$$|G| = 2^{14} \cdot 3^8 \cdot 5^3 \cdot 41^2 \cdot \frac{\Psi(1) \cdot (\Psi(1) + 1)}{(\Psi(1) - \Psi(z))^2}$$

Set $x = \Psi(1)$ and $a = \Psi(z)$. Let us recall all that we know about $|G|$:

LEMMA 1.7. *The following conditions hold*:
(1) $|G|_2 = 2^8$;
(2) $|G|_3 = 3^4$;
(3) $|G|_5 = 5^2$; *and*
(4) $|G|$ *is divisible by* 7.

Let $g = \frac{|G|}{2^8 \cdot 3^4 \cdot 5^2}$. Thus g is an integer which is coprime to $2 \cdot 3 \cdot 5$, divisible by 7 and most importantly, g can be written in the following form:

$$g = 2^6 \cdot 3^4 \cdot 5 \cdot 41^2 \cdot \frac{x \cdot (x+1)}{(x-a)^2} \tag{1.5}$$

COROLLARY 1.8. *The following inequality is correct*:

$$2^6 \cdot 3^4 \cdot 5 \cdot 41^2 \cdot \frac{x(x+1)}{(x+509)^2} < g < 2^6 \cdot 3^4 \cdot 5 \cdot 41^2 \cdot \frac{x(x+1)}{(x-509)^2}$$

Proof. Since $|a| \le 509$, we have the following inequality:

$$x - 509 \le x - a \le x + 509$$

Using this together with definition of g, we immediately obtain the desired result.

Let $f_1(x) = 2^6 \cdot 3^4 \cdot 5 \cdot 41^2 \cdot \frac{x(x+1)}{(x+509)^2}$ and $f_2(x) = 2^6 \cdot 3^4 \cdot 5 \cdot 41^2 \cdot \frac{x(x+1)}{(x-509)^2}$. Then Corollary 1.8 can be rewritten as:

$$f_1(x) < g < f_2(x) \tag{1.6}$$

Since g is not divisible by either 2, 3 or 5, their powers must cancel out in (1.5). Also 2 must divide $x(x+1)$. Therefore $2^4 \cdot 3^2 \cdot 5$ divides $x - a$. So the natural question is: what about 41? Does it at all influence the picture?

Lemma 1.9. *Suppose that* 41 *divides* $x-a$. *Then the following inequality holds*:

$$81|C| < g < 88|C|$$

Proof. If 41 divides $x-a$, then $2^4 \cdot 3^2 \cdot 5 \cdot 41$ divides $x-a$. In particular $2^4 \cdot 3^2 \cdot 5 \cdot 41 \le x - a$. But $x - a \le x + 509$ and so $x \ge 29011$.

Consider the functions $f_1(x)$ and $f_2(x)$ for $x \ge 29011$. Since $f_1(x)$ increases on this interval, we have $f_1(x) \ge f_1(29011) > 42083356$. Since $f_2(x)$ decreases on this interval, $f_2(x) \le f_2(29011) < 45143207$. These estimates together with (1.6) show that $42083356 < g < 45143207$, i.e., $81|C| < g < 88|C|$.

Lemma 1.10. *Suppose that* 41 *does not divide* $x-a$. *Then* 41^2 *divides* $|G|$ *and* $g < 981|C|$.

Proof. Clearly, if $(41, x-a) = 1$, then 41^2 must divide $|G|$. So let us prove the inequality. Recall that $|a| \le 509$. Suppose that $a \ge 0$. Then $2^4 \cdot 3^2 \cdot 5 \le x - a \le x$, i.e., $x \ge 720$. Consider the function $f_2(x)$ when $x \ge 720$. Since $f_2(x)$ decreases on this interval, $f_2(x) \le f_2(720)$. This estimate together with (1.6) implies that $g < 508048954$, i.e., $g < 981|C|$.

If $a < 0$, then from the formula (1.5) it follows that $g \le 2^6 \cdot 3^4 \cdot 5 \cdot 41^2 \cdot \frac{x\cdot(x+1)}{(x+1)^2}$ and so $g < 2^6 \cdot 3^4 \cdot 5 \cdot 41^2$, i.e., $g < 85|C|$ and the result follows.

LEMMA 1.11. $g \equiv 45523 \pmod{|C|}$.

Proof. For every prime divisor p of $|G|$, let $g_p = |G|_p$. Then the Theorem of Frobenius asserts that

$$|\{h \in G | h^{g_p} = 1\}| \equiv 0 \pmod{g_p}. \tag{1.7}$$

The left side of the congruence is nothing else but $1 + \sum_i \frac{|G|}{|C_G(h_i)|}$, where the sum ranges over the representatives h_i's of conjugacy classes of non-identity p-elements. Let $p \in \{2, 3, 5\}$. Since $|G| = g \cdot |C|$, Formula (1.7) can be rewritten in the following way:

$$1 + g \cdot \sum_i \frac{|C|}{|C_G(h_i)|} \equiv 0 \pmod{g_p} \tag{1.8}$$

In order to continue the calculations, we will need the following table:

The Orders of the Centralizers of p-elements

p	Class	Order of the Centralizer
$p = 2$	2_1	$2^8 \cdot 3^4 \cdot 5^2$
	$4_1, 4_2$	$2^7 \cdot 3^2 \cdot 5$
	$8_1, 8_2, 8_3, 8_4$	$2^7 \cdot 3^2 \cdot 5$
	$8_5, 8_6$	2^6
	$16_1, 16_2, 16_3, 16_4$	$2^4 \cdot 5$
$p = 3$	$3_1, 3_2$	$2^4 \cdot 3^4 \cdot 5$
	$3_3, 3_4$	$2 \cdot 3^4$
$p = 5$	$5_1, 5_2, 5_3, 5_4$	$2^5 \cdot 3^2 \cdot 5^2$

Substituting the data from the table into the Formula (1.8) for $p \in \{2, 3, 5\}$, we obtain the following congruences:

$$g \equiv 211 \pmod{2^8},\ g \equiv 1 \pmod{3^4},\ g \equiv 23 \pmod{5^2}$$

Finally applying the Chinese Remainder Theorem, we obtain that

$$g \equiv 45523 \pmod{2^8 \cdot 3^4 \cdot 5^2}$$

which is precisely what we wanted to show.

LEMMA 1.12. *If* 41 *divides* $x - a$, *then* $g = 7 \cdot 1039 \cdot 5851$.

Proof. Since 41 divides $x-a$, Lemma 1.9 gives that $81|C| < g < 88|C|$. On the other hand $g \equiv 45523 \pmod{|C|}$. Recall that 7 divides g. Putting together all this information, we obtain the unique solution: $g = 7 \cdot 1039 \cdot 5851$.

Corollary 1.13. 41 *does not divide* $x - a$.

Proof. Assume the contrary. Then as we just proved, $g = 7 \cdot 1039 \cdot 5851$ and so $|G| = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 1039 \cdot 5851$. Let $Q \in Syl_{1039}(G)$ and $N = N_G(Q)$. By Sylow Theorem, $|G : Q| \equiv |N : Q| \pmod{1039}$. Thus $|N : Q| \equiv 418 \pmod{1039}$. Since the centralizer of Q is a $\{2,3,5\}'$-group and $1038 = 2 \cdot 3 \cdot 173$, we obtain that $|N : Q|$ divides $2 \cdot 3 \cdot 7 \cdot 5851$. Therefore there exist integers $t \geq 1, r \geq 1$ such that

$$(1039t + 418)r = 2 \cdot 3 \cdot 7 \cdot 5851 \tag{1.9}$$

Solving it modulo 1039, we obtain that $r \equiv 51 \pmod{1039}$. If $r > 51$, then the left side of (1.9) becomes strictly larger than the right side. Therefore $r = 51$, which is a contradiction.

Therefore we are now in the conditions of Lemma 1.10. So let us summarize all that we know about g:

$$g < 981|C|,\ g \equiv 45523 \pmod{|C|} \text{ and } g \equiv 0 \pmod{7 \cdot 41^2}$$

Putting the last two together with the help of the Chinese Remainder Theorem, we obtain that $g \equiv 4651130323 \pmod{7 \cdot 41^2 \cdot |C|}$. But this means that $g > 8972|C|$, which is an obvious contradiction proving the result.

References

[Co] M.J. Collins, *Representations and characters of finite groups*, Cambridge University Press (1990).

[GLS] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number* 1, Amer. Math. Soc. Surveys and Monographs, **40, # 1** (1995).

[GLS2] ———, *The Classification of the Finite Simple Groups, Number* 1, Amer. Math. Soc. Surveys and Monographs, **40, # 6** (to be published).

[F1] P. Fong, *A Characterization of the finite simple groups* $PSp(4,q)$*,* $G_2(q)$*,* ${}^2D_4(q)$*. Part* 2, Nagoya Math. J., **39** (1970), 37–79.

[F2] P. Fong, *Unpublished Notes.*

[FW] P. Fong and W.J. Wong, *A Characterization of the finite simple groups* $PSp(4,q)$*,* $G_2(q)$*,* ${}^2D_4(q)$*. Part* 1, Nagoya Math. J., **36** (1969), 143–184.

[Is] I. Martin Isaacs, Character Theory of Finite Simple Groups, Academic Press, New York, 1976.

[L] R. Lyons, *Evidence for a new simple group*, J. Algebra, **20** (1972), 540–569.

Department of Mathematics
Hill Center-Busch Campus
Rutgers, The State University of New Jersey
110 Frelinghuysen Rd
Piscataway, NJ 08854-8019
U.S.A.
innako@math.rutgers.edu