Journal of Algebra 321 (2009) 1407–1428

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Reduction of the Hall–Paige conjecture to sporadic simple groups

Stewart Wilcox

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02318, USA

ARTICLE INFO

Article history:
Received 1 August 2007
Available online 7 January 2009
Communicated by Ronald Solomon

Keywords:
Hall–Paige conjecture

ABSTRACT

A complete mapping of a group G is a permutation $\phi : G \to G$ such that $g \mapsto g\phi(g)$ is also a permutation. Complete mappings of G are equivalent to transversals of the Cayley table of G, considered as a Latin square. In 1953, Hall and Paige proved that a finite group admits a complete mapping only if its Sylow-2 subgroup is trivial or noncyclic. They conjectured that this condition is also sufficient. We prove that it is sufficient to check the conjecture for the 26 sporadic simple groups and the Tits group.

1. Introduction

All groups will be assumed finite. Let G be a group. For the sake of brevity, we say G is *bad* if the Sylow-2 subgroup of G is nontrivial and cyclic, and otherwise we say G is *good*. A *complete mapping* of G consists of an indexing set I and bijections $a, b, c : I \to G$, such that

$$a(i)b(i) = c(i)$$

for all $i \in I$. Note that $\phi = ba^{-1}$ and $\psi = ca^{-1}$ are bijections, so G possesses a complete mapping if and only if there are permutations ϕ and ψ of G with $g\phi(g) = \psi(g)$. Complete mappings also have a combinatorial interpretation; a group possesses a complete mapping if and only if its Cayley table, which is a Latin square, possesses an orthogonal mate [16].

Hall and Paige [12] proved that if G possesses a complete mapping, then it is good; they also conjectured the converse (henceforth the "HP conjecture"), and proved it in many special cases. They also proved many useful results, including Propositions 1, 2 and 3 below.

Proposition 1. *(See [12, Theorem 6].) Any good soluble group possesses a complete mapping.*

E-mail address: swilcox@fas.harvard.edu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2008.11.033

In particular, any group of odd order is soluble [11] and therefore possesses a complete mapping (this can be easily shown directly by making ϕ the identity).

Recall that a left transversal of a subgroup $H \subseteq G$ is a set $X \subseteq G$ such that

$$G = \coprod_{x \in X} xH,$$

and similarly for a right transversal.

Proposition 2. *(See [12, Theorem 1].) Suppose H is a subgroup of G, and H possesses a complete mapping. Suppose X is both a left and right transversal for H, and ϕ and ψ are permutations of X such that*

$$x\phi(x)H = \psi(x)H$$

for $x \in X$. Then G possesses a complete mapping.

The following result is a direct corollary of Proposition 2.

Proposition 3. *(See [12, Corollary 2].) Suppose N is a normal subgroup of G such that both N and $H = G/N$ possess complete mappings. Then G possesses a complete mapping.*

Recently many groups have been shown to satisfy the conjecture. The Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24}, and some groups of Lie type, have been shown to possess complete mappings [5,7, 8,17]. Dalla Volta and Gavioli have shown that a minimal counterexample to the HP conjecture would have to be almost simple, or contain a central involution [6]. Continuing in this direction, we will show that a minimal counterexample must be one of the 26 sporadic simple groups or the Tits group. In a companion paper, Evans [9] deals with 26 of these groups (including an alternative treatment of the Mathieu groups), leaving the fourth Janko group as the only possible counterexample. John Bray reports that this group is also not a counterexample, thus completing the proof of the HP conjecture.

In Section 2 we give two versions of Proposition 3 in which N and H are replaced by $\mathbb{Z}_2$ (see Propositions 7 and 11 respectively). These are used, along with Proposition 1, to reduce the conjecture to simple groups.

In Section 3 we prove a version of Proposition 2 in which the assumption on the cosets of H is weakened (see Proposition 14). We also prove versions in which this assumption is replaced by an assumption on the double cosets of H, which is often easier to check in practice (see Corollaries 15 and 16).

Finally in Section 4, we use the results of Section 3 and results about (B, N)-pairs to prove that a minimal counterexample cannot be a finite simple group of Lie type.

2. Reduction to simple groups

We start with some well known results.

Lemma 4. *Suppose G is bad. Then there exists a characteristic subgroup of G of index* 2.

Corollary 5. *Suppose G is bad. Then G contains a characteristic subgroup N of odd order, such that the quotient G/N is a cyclic* 2*-group. In particular, G is soluble.*

The first result follows by considering the inverse image of the alternating group under the regular representation $G \to S_G$. The second follows from the first by induction on $|G|$.

To prove the first version of Proposition 3, we need the following well known combinatorial result, the proof of which is straightforward.

Lemma 6. *Suppose I is a finite set and S and T are involutions on I with no fixed points. Then we can write I as a disjoint union*

$$I = J \amalg K$$

such that $S(J) = T(J) = K$ (in particular $|K| = |J| = \frac{1}{2}|I|$).

Now we are ready to prove:

Proposition 7. *Suppose that G is a good finite group, and N is a normal subgroup of G isomorphic to $\mathbb{Z}_2$. Suppose $H = G/N$ possesses a complete mapping. Then G possesses a complete mapping.*

Proof. Let $N = \{1, x\}$, so that x is a central involution in G. Let $\pi : G \twoheadrightarrow H$ be the natural surjection. Clearly if $|H|$ is odd, then N is a Sylow-2 subgroup of G, contradicting the goodness of G. Thus $|H|$ is even. In particular, H contains an involution $\bar{y}$. Then right multiplication by $\bar{y}$ gives an involution r_y on H with no fixed points.

Now H admits a complete mapping, so choose an indexing set I and bijections $\bar{a}, \bar{b}, \bar{c} : I \to H$ such that $\bar{a}(i)\bar{b}(i) = \bar{c}(i)$ for $i \in I$. Then $S = \bar{b}^{-1} r_y \bar{b}$ and $T = \bar{c}^{-1} r_y \bar{c}$ are both involutions on I with no fixed points. By Lemma 6, we can write

$$I = J \amalg K$$

such that $S(J) = T(J) = K$. Now let y be one of the two elements in $\pi^{-1}(\bar{y})$. We lift $\bar{b}$ and $\bar{c}$ to G as follows. Let

$$b, c : J \to G$$

be any maps satisfying $\pi b = \bar{b}$ and $\pi c = \bar{c}$. Extend b and c to K by defining

$$b(Sj) = b(j)y \quad \text{and} \quad c(Tj) = c(j)y \quad \text{for } j \in J. \tag{1}$$

By definition of S, we have $\bar{b}(Si) = \bar{b}(i)\bar{y}$ for all $i \in I$. Thus

$$\pi\big(b(Sj)\big) = \pi\big(b(j)y\big) = \bar{b}(j)\bar{y} = \bar{b}(Sj)$$

for $j \in J$. With a similar calculation for c, we see that $\pi b = \bar{b}$ and $\pi c = \bar{c}$ on all of I. Finally define $a(i) = c(i)b(i)^{-1}$. Then

$$\pi\big(a(i)\big) = \pi\big(c(i)\big)\pi\big(b(i)\big)^{-1} = \bar{c}(i)\bar{b}(i)^{-1} = \bar{a}(i),$$

so that $\pi a = \bar{a}$. Now define maps $A, B, C : I \times N \to G$ by

$$\begin{aligned}
&A(j,1) = a(j), && B(j,1) = b(j), && C(j,1) = c(j),\\
&A(j,x) = a(j)x, && B(j,x) = b(j)yx, && C(j,x) = c(j)y,\\
&A(k,1) = a(k), && B(k,1) = b(k)y^{-1}x, && C(k,1) = c(k)y^{-1}x, \quad \text{and}\\
&A(k,x) = a(k)x, && B(k,x) = b(k), && C(k,x) = c(k)x
\end{aligned}$$

for $j \in J$ and $k \in K$. Because $a(i)b(i) = c(i)$ for all $i \in I$, and x is central, it is clear that $A(i,t)B(i,t) = C(i,t)$ for all $(i,t) \in I \times N$. It remains to show that A, B and C are bijective. Since $|I \times N| = |G|$, it is sufficient to prove surjectivity. Since $\pi b = \bar{b}$ is a bijection, $b(I)$ is a transversal for N in G, so that $G = b(I) \amalg b(I)x$. Also (1) shows that $b(K) = b(J)y$, so

$$\begin{aligned} B(I \times N) &= B\big(J \times \{1\}\big) \cup B\big(J \times \{x\}\big) \cup B\big(K \times \{1\}\big) \cup B\big(K \times \{x\}\big) \\ &= b(J) \cup b(J)yx \cup b(K)y^{-1}x \cup b(K) \\ &= b(J) \cup b(K)x \cup b(J)x \cup b(K) \\ &= b(I) \cup b(I)x \\ &= G, \end{aligned}$$

as required. The calculations for A and C are similar. □

Note that Hall and Paige prove Proposition 1 by proving the HP conjecture for 2 groups. The above result allows us to easily reproduce the conjecture for 2 groups by induction on the order of the group; indeed if G is a noncyclic 2 group and $G \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, one can always find a central involution $x \in G$ such that $G/\{1, x\}$ is noncyclic.

Our second version of Proposition 3, which deals with a subgroup N in G of index 2, was proven in [10] under the following technical assumption: that there exist elements $a, b \in G - N$ such that $xa^i x^{-1} \neq b^j$ for all $x \in N$ and odd integers i, j. We will show that, provided G is good, this assumption always holds.

A theorem of Frobenius states that if n divides the order of a finite group G, then the number of solutions of $x^n = 1$ in G is divisible by n (see [15] for an elementary proof). We will use the following special case. Recall that a 2-element in G is an element whose order is a power of 2.

Lemma 8. *Suppose G is a finite group and P is a Sylow-2 subgroup of G. Then the number of 2-elements in G is divisible by $|P|$.*

The following result is well known and can be found, for instance, in Theorem 4.2.1 of [14].

Lemma 9. *Suppose P is a finite 2-group and $H \subset P$ is a proper subgroup. Then the normaliser $N_P(H)$ is strictly larger than H.*

Lemma 10. *Suppose G is a good finite group and $N \subseteq G$ is a normal subgroup of index 2. Consider the cyclic subgroups generated by 2-elements in the set complement $G - N$. These subgroups are not all conjugate in G.*

Proof. Let X be the set of 2-elements in $G - N$. Let

$$Y = \big\{\langle x\rangle \bigm| x \in X\big\}$$

be the set of cyclic groups generated by elements of X. For any $x \in X$, we have

$$\langle x\rangle - N = \big\{x^k \bigm| k \in \mathbb{Z} \text{ odd}\big\}.$$

Since x is a 2-element, if k is odd then $x^{kl} = x$ for some $l \in \mathbb{Z}$. Thus $\langle x\rangle$ is generated by any element of $\langle x\rangle - N$. It follows that if $H, H' \in Y$ are distinct, then $(H - N) \cap (H' - N) = \emptyset$. Thus

$$X = \coprod_{H' \in Y} (H' - N).$$

Let $P \subseteq G$ be a Sylow-2 subgroup of G. Then P is not contained in N, so choose $x \in P - N \subseteq X$, and let $H = \langle x\rangle \in Y$. Suppose by way of contradiction that every $H' \in Y$ is conjugate to H. Then the orbit stabiliser theorem gives

$$|Y| = \frac{|G|}{|N_G(H)|}.$$

Also each $H' \in Y$ has the same order as H, so

$$|X| = \sum_{H' \in Y} |H' - N| = \sum_{H' \in Y} \frac{|H'|}{2} = \frac{1}{2}|H| \cdot |Y| = \frac{|H| \cdot |G|}{2|N_G(H)|}.$$

Now Lemma 8 shows that $|P|/2$ divides the number of 2-elements in N, and the number of 2-elements in G. Thus it divides $|X|$, so that

$$\frac{|G|}{|P| \cdot [N_P(H) : H]} = \frac{|H| \cdot |G|}{|N_G(H)|} \cdot \frac{1}{|P|} \cdot \frac{|N_G(H)|}{|N_P(H)|} = \frac{2|X|}{|P|} \cdot \left[N_G(H) : N_P(H)\right] \in \mathbb{Z}.$$

Now $|G|/|P|$ is odd and $[N_P(H) : H]$ is a power of 2, so $[N_P(H) : H] = 1$. That is, $H = N_P(H)$. By Lemma 9, we must have $P = H$. But H is cyclic, contradicting the goodness of G. □

We can now prove the second version of Proposition 3:

Proposition 11. *Suppose that G is a good finite group, and N is a normal subgroup of G such that N possesses a complete mapping and $G/N \cong \mathbb{Z}_2$. Then G possesses a complete mapping.*

Proof. By the previous lemma, we can find 2-elements a and b in $G - N$, such that $\langle a \rangle$ and $\langle b \rangle$ are not conjugate in G. For any odd integers i and j, we have $\langle a^i \rangle = \langle a \rangle$ and $\langle b^j \rangle = \langle b \rangle$. Therefore $\langle a^i \rangle$ is not conjugate to $\langle b^j \rangle$, so in particular, a^i and b^j are not conjugate in G. The result now follows by Theorem 11 of [10]. □

We can now reduce the Hall Paige conjecture to simple groups. The idea of taking a minimal counterexample to the conjecture and considering a minimal normal subgroup is due to Dalla Volta and Gavioli [6].

Theorem 12. *Suppose G is a minimal counterexample to the HP conjecture. That is, G is good but has no complete mapping, and any good group smaller than G has a complete mapping. Then G is simple.*

Proof. Suppose otherwise, and let N be a minimal nontrivial normal subgroup of G. There are four cases to consider. Suppose first that N and G/N are both good. By the minimality of G, they must satisfy the HP conjecture. Thus they both possess complete mappings. Proposition 3 now shows that G possesses a complete mapping.

Next suppose N and G/N are both bad. They are both soluble by Corollary 5. Thus G is soluble and good, so it possesses a complete mapping by Proposition 1.

Now suppose N is good and G/N is bad. If $|N|$ is odd, then N is soluble, and G possesses a complete mapping just as in the last case. Suppose $|N|$ is even. By Lemma 4, there is a characteristic subgroup $\bar{H}$ of G/N of index 2. The inverse image H of $\bar{H}$ is a normal subgroup of G of index 2 containing N. Because the Sylow-2 subgroup of N is noncyclic, the same is true of H. Thus H is good, so it possesses a complete mapping by minimality. It follows from Proposition 11 that G possesses a complete mapping.

Finally suppose N is bad and G/N is good. By Lemma 4, we have a characteristic subgroup H of N of index 2. Because H is characteristic in N, it is normal in G. But N is a minimal nontrivial normal subgroup of G, so H is trivial. That is, $N \cong \mathbb{Z}_2$. Again G/N possesses a complete mapping by minimality of G, so it follows from Proposition 7 that G possesses a complete mapping. □

3. Double coset results

In this section we prove some results similar to Proposition 2, in which a complete mapping of a subgroup is extended to a complete mapping of the group. We will use the following result about transversals, which is an immediate corollary of Theorem 5.1.6 of [13] (see the proof of [13, Theorem 5.1.7]).

Lemma 13. *Suppose H and K are subgroups of G with the same order. Then there exists a left transversal for H which is also a transversal for K (either left or right, as desired).*

In fact the proof of Proposition 2 given in [12] is valid under weaker hypotheses; namely, the elements x, $\phi(x)$ and $\psi(x)$ may run through three different left transversals of H as x varies, and only one need also be a right transversal. Using this observation and the previous lemma, we may now prove:

Proposition 14. *Suppose $H \subseteq G$ is a subgroup of G which admits a complete mapping. Suppose we have bijections $\tilde{x}$, $\tilde{y}$ and $\tilde{z}$ from an indexing set I to G/H (so that $|I| = [G : H]$), and suppose $\tilde{x}(i)\tilde{y}(i) \supseteq \tilde{z}(i)$ for all $i \in I$. Then G possesses a complete mapping.*

Proof. By Lemma 13, we can find a set $\{y_i \mid i \in I\}$ which is both a left and right transversal of H. We can label these elements so that $y_i \in \tilde{y}(i)$. For a given $i \in I$, we have

$$\tilde{z}(i) \subseteq \tilde{x}(i)\tilde{y}(i) = \bigcup_{x \in \tilde{x}(i)} x\tilde{y}(i).$$

Now each $x\tilde{y}(i)$ is a left coset of H, and we know distinct left cosets are disjoint, so $\tilde{z}(i) = x_i\tilde{y}(i)$ for some $x_i \in \tilde{x}(i)$. Define $z_i = x_i y_i \in x_i\tilde{y}(i) = \tilde{z}(i)$, so $\{x_i\}$ and $\{z_i\}$ are both left transversals of H.

As noted above, the remainder of the proof follows [12]. Since H possesses a complete mapping, we can choose an indexing set J and bijections a, b and c from J to H such that $a(j)b(j) = c(j)$ for $j \in J$. Because $\{y_i\}$ is a right transversal of H, for any $(i, j) \in I \times J$ we can write

$$y_i a(j) = d(i, j) y_{r(i,j)} \tag{2}$$

for some $d(i, j) \in H$ and $r(i, j) \in I$. Then

$$z_i c(j) = x_i y_i a(j) b(j) = x_i d(i, j) y_{r(i,j)} b(j).$$

Thus $C(i, j) = A(i, j)B(i, j)$, where the maps A, B and C from $I \times J$ to G are defined by

$$A(i, j) = x_i d(i, j), \qquad B(i, j) = y_{r(i,j)} b(j), \qquad C(i, j) = z_i a(j).$$

It remains to show that these maps are bijective. Since $|I \times J| = |G|$, it suffices to prove injectivity. Suppose $A(i, j) = A(i', j')$, so that $x_i d(i, j) = x_{i'} d(i', j')$. Now the x_i form a left transversal for H and $d(i, j)$, $d(i', j') \in H$, so $i = i'$ and $d(i, j) = d(i', j')$. Thus (2) gives

$$y_{r(i,j)} a(j)^{-1} = d(i, j)^{-1} y_i = d(i', j')^{-1} y_{i'} = y_{r(i',j')} a(j')^{-1}.$$

Now the y_i also from a left transversal for H, so $a(j)^{-1} = a(j')^{-1}$. Since a is a bijection, this gives $j = j'$, as required.

Now assume $B(i, j) = B(i', j')$, so that $y_{r(i,j)} b(j) = y_{r(i',j')} b(j')$. Since the y_i form a left transversal for H, we have $r(i, j) = r(i', j')$ and $b(j) = b(j')$. Hence $j = j'$. Now (2) gives

$$d(i, j)^{-1} y_i = y_{r(i,j)} a(j)^{-1} = y_{r(i',j')} a(j')^{-1} = d(i', j')^{-1} y_{i'}.$$

Since the y_i form a right transversal for H, we conclude that $i = i'$, as required. The injectivity of C is straightforward. □

The above result is similar to Proposition 3; although we are no longer considering a normal subgroup, we require a "complete mapping" of sorts on G/H. In fact we have more freedom when H is not normal, since the "product" of two left cosets aH and bH can be any left coset contained in $aHbH$; in general $|aHbH| > |H|$, so there will be more than one choice. The expression $aHbH$ motivates us to consider double cosets; recall that a double coset of $H \subseteq G$ is a set of the form HxH, for some $x \in G$. We denote the set of double cosets by $H\backslash G/H$.

Corollary 15. *Suppose $H \subseteq G$ is a subgroup of G which admits a complete mapping. Suppose ϕ and ψ are permutations of $H\backslash G/H$ such that for each $D \in H\backslash G/H$, we have $|D| = |\phi(D)| = |\psi(D)|$ and $D\phi(D) \supseteq \psi(D)$. Then G possesses a complete mapping.*

Proof. Fix $D \in H\backslash G/H$ and pick some $z_D \in \psi(D) \subseteq D\phi(D)$, so that $z_D = x_D y_D$ for some $x_D \in D$ and $y_D \in \phi(D)$. It is well known that

$$D = Hx_D H = \coprod_{h \in X} h x_D H$$

for any left transversal X of $H \cap x_D H x_D^{-1}$ in H. In particular,

$$|D| = \frac{|H|^2}{|H \cap x_D H x_D^{-1}|}.$$

Now $|D| = |\phi(D)| = |\psi(D)|$, so $|H \cap x_D H x_D^{-1}| = |H \cap y_D H y_D^{-1}| = |H \cap z_D H z_D^{-1}|$. By Lemma 13, we can find a subset $X_D \subseteq H$ which is simultaneously a left transversal for $H \cap x_D H x_D^{-1}$ and for $H \cap z_D H z_D^{-1}$ in H. Thus

$$D = \coprod_{h \in X_D} h x_D H \quad \text{and} \quad \psi(D) = \coprod_{h \in X_D} h z_D H.$$

Also let Y_D be a left transversal for $H \cap y_D H y_D^{-1}$ in H, so that

$$\phi(D) = \coprod_{h \in Y_D} h y_D H.$$

Now $|X_D| = |Y_D|$, so choose a bijection $\mu_D : X_D \to Y_D$. Let

$$I = \{(D, h) \mid D \in H\backslash G/H \text{ and } h \in X_D\}.$$

Define maps $\tilde{x}$, $\tilde{y}$ and $\tilde{z} : I \to G/H$ by

$$\tilde{x}(D, h) = h x_D H, \qquad \tilde{y}(D, h) = \mu_D(h) y_D H \quad \text{and} \quad \tilde{z}(D, h) = h z_D H.$$

Certainly since $\mu_D(h)^{-1} \in H$ for $h \in X_D$, we have

$$\tilde{z}(D, h) = h z_D H = h x_D y_D H \subseteq h x_D H \mu_D(h) y_D H = \tilde{x}(D, h)\tilde{y}(D, h).$$

Thus the statement will follow from Proposition 14, provided $\tilde{x}$, $\tilde{y}$ and $\tilde{z}$ are bijections. Equivalently, G should be a disjoint union of $\tilde{x}(D, h)$ for $(D, h) \in I$, and similarly for $\tilde{y}$ and $\tilde{z}$. Since ϕ and ψ are permutations, and μ_D is a bijection,

$$G = \coprod_{D \in H\backslash G/H} D = \coprod_{\substack{D \in H\backslash G/H \\ h \in X_D}} h x_D H = \coprod_{(D,h)\in I} \tilde{x}(D,h),$$

$$G = \coprod_{D \in H\backslash G/H} \phi(D) = \coprod_{\substack{D \in H\backslash G/H \\ h \in Y_D}} h y_D H$$

$$= \coprod_{\substack{D \in H\backslash G/H \\ h \in X_D}} \mu_D(h) y_D H = \coprod_{(D,h)\in I} \tilde{y}(D,h) \quad \text{and}$$

$$G = \coprod_{D \in H\backslash G/H} \psi(D) = \coprod_{\substack{D \in H\backslash G/H \\ h \in X_D}} h z_D H = \coprod_{(D,h)\in I} \tilde{z}(D,h). \qquad \square$$

We will use the special case in which ϕ and ψ are the identity:

Corollary 16. *Suppose $H \subseteq G$ is a subgroup of G which admits a complete mapping. Suppose $D^2 \supseteq D$ for all $D \in H\backslash G/H$. Then G possesses a complete mapping.*

4. The HP conjecture for groups of Lie type

In this section we suppose that G is a finite simple group of Lie type, excluding the Tits group. We begin by stating a number of properties of such groups, which can be found in [3]. First we recall in Table 1 the list of families of such groups.

Consider first the *untwisted groups*, namely those with no superscript on the left. Let $\Phi = \Phi^+ \cup \Phi^-$ denote the corresponding root system, and let K denote the field of q elements. The group G is generated by elements $x_r(t)$ for $r \in \Phi$ and $t \in K$, which satisfy $x_r(t)x_r(u) = x_r(t+u)$. If $r, s \in \Phi$ are linearly independent, then $x_s(u)$ and $x_r(t)$ satisfy Chevalley's commutator formula [3, Theorem 5.2.2]:

$$x_r(t)x_s(u) = x_s(u)\left[\prod_{\substack{i,j>0, \\ ir+js\in\Phi}} x_{ir+js}\big(C_{ijrs}t^i u^j\big)\right]x_r(t), \tag{3}$$

where the product is taken in order of increasing $i+j$, and the integer constants C_{ijrs} are determined by

Table 1
Families of groups of Lie type.

Group	Parameter values	Rank l
$A_k(q)$	$k \geqslant 1$ and q a prime power	k
$B_k(q)$	$k \geqslant 2$ and q a prime power	k
$C_k(q)$	$k \geqslant 3$ and q a prime power	k
$D_k(q)$	$k \geqslant 4$ and q a prime power	k
$E_6(q)$	q a prime power	6
$E_7(q)$	q a prime power	7
$E_8(q)$	q a prime power	8
$F_4(q)$	q a prime power	4
$G_2(q)$	q a prime power	2
${}^2A_k(q)$	$k \geqslant 2$ and q a prime power squared	$\lceil k/2 \rceil$
${}^2D_k(q)$	$k \geqslant 4$ and q a prime power squared	$k-1$
${}^3D_4(q)$	q a prime power cubed	2
${}^2E_6(q)$	q a prime power squared	4
${}^2B_2(q)$	$q = 2^{2k+1}$	1
${}^2F_4(q)$	$q = 2^{2k+1}$	2
${}^2G_2(q)$	$q = 3^{2k+1}$	1

$$C_{i1rs} = M_{rsi}; \qquad C_{1jrs} = (-1)^j M_{srj};$$
$$C_{32rs} = \frac{1}{3} M_{r+s,r,2}; \qquad C_{23rs} = -\frac{2}{3} M_{s+r,s,2};$$
$$M_{rsi} = \frac{1}{i!} \prod_{j=0}^{i-1} N_{r,\,jr+s}; \qquad N_{r,s} = \pm \max\{p+1 \mid s - pr \in \Phi\}.$$

The signs of $N_{r,s}$ are chosen to satisfy certain conditions that do not concern us here [3, Sections 4.2]. We will only use (3) for G_2, in which case we use the values for $N_{r,s}$ at the end of Section 12.4 of [3].

For $r \in \Phi$ we have a homomorphism $\rho_r : SL_2(K) \to G$ satisfying

$$\rho_r \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_r(t) \quad \text{and} \quad \rho_r \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-r}(t).$$

Let

$$h_r(t) = \rho_r \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \quad \text{and} \quad n_r = \rho_r \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

for $t \in K^*$. Clearly $n_r^2 = h_r(-1)$. Let H, U, V, B and N be the subgroups of G generated by:

$$H = \langle h_r(t) \mid r \in \Phi,\ t \in K^* \rangle \subseteq G,$$
$$U = \langle x_r(t) \mid r \in \Phi^+,\ t \in K \rangle \subseteq G,$$
$$V = \langle x_r(t) \mid r \in \Phi^-,\ t \in K \rangle \subseteq G,$$
$$B = \langle H, U \rangle \subseteq G,$$
$$N = \langle h_r(t),\ n_r \mid r \in \Phi,\ t \in K^* \rangle \subseteq G.$$

We will need an explicit description of the subgroup H. Let Λ denote the lattice spanned by Φ; this is a free abelian group whose rank is the rank l in Table 1. Let Λ^* denote the dual lattice to Λ. The Cartan matrix of Φ gives a bilinear form on Λ (not necessarily symmetric) which allows us to identify Λ with a subgroup of Λ^*. Then H can be identified with the image of $\mathrm{Hom}(\Lambda^*, K^*)$ in $\mathrm{Hom}(\Lambda, K^*)$ (see [3, Section 7.1]). Explicitly, $h_r(t)$ corresponds to the function

$$h_r(t)(v) = t^{\frac{2(r,v)}{(r,r)}} \quad \text{for } v \in \Lambda,$$

where $(\cdot,\cdot)$ is a symmetrised version of the above bilinear form. In particular, if $r, s, ir + js \in \Phi$ and $t \in K^*$, then

$$h_{ir+js}(t)^{(ir+js,ir+js)} = h_r(t)^{i(r,r)} h_s(t)^{j(s,s)}. \tag{4}$$

We have a left exact sequence

$$\mathrm{Hom}(\Lambda^*/\Lambda, K^*) \hookrightarrow \mathrm{Hom}(\Lambda^*, K^*) \to \mathrm{Hom}(\Lambda, K^*), \tag{5}$$

so $H \cong \hat{H}/H_1$, where $\hat{H} = \mathrm{Hom}(\Lambda^*, K^*) \cong (K^*)^{\oplus l}$ and $H_1 = \mathrm{Hom}(\Lambda^*/\Lambda, K^*)$. The group Λ^*/Λ is given by the following table (see Section 8.6 of [3]):

G	A_k	B_k	C_k	D_{2k+1}	D_{2k}	G_2	F_4	E_6	E_7	E_8
Λ^*/Λ	$\mathbb{Z}_{k+1}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_4$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	0	0	$\mathbb{Z}_3$	$\mathbb{Z}_2$	0

In particular, Λ^*/Λ is generated by at most two elements in the case of D_{2k}, and is cyclic otherwise. The same statement is true of H_1, since K^* is cyclic.

Now suppose G is a *twisted group*, that is, one with a superscript on the left. Let $\bar{G}$ be the corresponding untwisted group obtained by removing the superscript, with subgroups $\bar{H}$, $\bar{U}$, $\bar{V}$, $\bar{B}$ and $\bar{N}$ as constructed above. There is an automorphism σ of $\bar{G}$ (described in [3, Section 13.4]) fixing all of these subgroups. Let $U = \bar{U}^\sigma$ and $V = \bar{V}^\sigma$ be the groups of σ-invariant elements in $\bar{U}$ and $\bar{V}$. Then G is defined to be the subgroup of $\bar{G}$ generated by U and V. Let $H = \bar{H} \cap G$, and similarly for B and N. Again we will need to describe H more explicitly. First suppose that $\bar{G}$ is simply laced; that is, G is not ${}^2B_2(q)$, ${}^2F_4(q)$ or ${}^2G_2(q)$. Recall $\bar{H}$ is the image of the second map in (5). The action of σ on $\bar{H}$ can be extended to $\mathrm{Hom}(\Lambda, K^*)$ by

$$\sigma(\chi)(r) = \chi(\tau r)^\theta,$$

where τ is an isometry of Λ fixing the set of simple roots $\Pi \subseteq \Phi$, and θ is an automorphism of K (see [3, Lemma 13.7.1]). Similarly σ acts on $\mathrm{Hom}(\Lambda^*, K^*)$ and $\mathrm{Hom}(\Lambda^*/\Lambda, K^*)$, and we obtain a left exact sequence

$$\mathrm{Hom}\big(\Lambda^*/\Lambda, K^*\big)^\sigma \hookrightarrow \mathrm{Hom}\big(\Lambda^*, K^*\big)^\sigma \to \mathrm{Hom}\big(\Lambda, K^*\big)^\sigma.$$

In fact H is the image of the second map [3, Theorem 13.7.2], so we can again write H as a quotient

$$H \cong \hat{H}/H_1,$$

now with $\hat{H} = \mathrm{Hom}(\Lambda^*, K^*)^\sigma$ and $H_1 = \mathrm{Hom}(\Lambda^*/\Lambda, K^*)^\sigma$. Since τ permutes the set Π^*, which freely generates Λ^* as an abelian group, we have

$$\hat{H} \cong \bigoplus_{O \in \tau\backslash\Pi^*} \big(K^*\big)^{\theta^{|O|}},$$

where $\tau\backslash\Pi^*$ is the set of orbits of τ in Π^*, and $(K^*)^{\theta^{|O|}}$ is the subgroup of K^* fixed by $\theta^{|O|}$. The number of orbits $l = |\tau\backslash\Pi^*|$ is exactly the rank listed in Table 1. If $\bar{G}$ is not of type D_{2k}, then $\mathrm{Hom}(\Lambda^*/\Lambda, K^*)$ is cyclic as noted above, so the same is true of the subgroup H_1. In fact H_1 is trivial when G has type ${}^3D_4(q)$, and is trivial or $\mathbb{Z}_2$ when G has type ${}^2D_{2k}(q)$ (see the note after [3, Lemma 14.1.2]).

Finally suppose G is of type ${}^2B_2(q)$, ${}^2F_4(q)$ or ${}^2G_2(q)$. Let p be the characteristic of K. For ${}^2B_2(q)$ we have $\Lambda^*/\Lambda \cong \mathbb{Z}_2$ and $p = 2$, and otherwise $\Lambda^*/\Lambda = 0$, so

$$\mathrm{Hom}\big(\Lambda^*/\Lambda, K^*\big) = \mathrm{Ext}^1\big(\Lambda^*/\Lambda, K^*\big) = 0$$

in either case. Hence

$$\bar{H} = \mathrm{Hom}\big(\Lambda^*, K^*\big) = \mathrm{Hom}\big(\Lambda, K^*\big).$$

We again have a permutation τ of Π; this no longer induces an isometry as the roots of Π have different lengths. Nevertheless we have the following explicit description of H [3, Theorem 13.7.4]:

$$H = \big\{\chi \in \bar{H} \;\big|\; \chi(r) = \chi(\tau r)^{(r,r)\theta} \text{ for } r \in \Pi\big\}, \tag{6}$$

where $q = p\theta^2$ and $(\cdot,\cdot)$ is normalised to give short roots length 1. Also τ acts on Π as an involution switching long and short roots, and $l = |\tau\backslash\Pi|$ is the rank listed in Table 1. It follows that

$$H \cong \big(K^*\big)^{\oplus l}.$$

In this case we set $\hat{H} = H$ and $H_1 = 0$.

We now state some results applicable to every group G in Table 1. In each case we have written H as a quotient $\hat{H}/H_1$, where $\hat{H}$ is a product of l cyclic groups, each of order $p^s - 1$ for some s, where p is the characteristic of K. The subgroups U, V, B, H and N in G, constructed above, satisfy $H = B \cap N$ and $B = H \ltimes U$. It is shown in [3] Sections 8.6 and 14.1 that

$$|U| = p^M \quad \text{for some integer } M\text{, and } p \nmid [G : U]. \tag{7}$$

The subgroups B and N form a (B, N)-pair in G. The following results about (B, N)-pairs are proved in [2]. Firstly H is normal in N, and the quotient $W = N/H$ is a Coxeter group, generated by a set S of involutions. In fact $l = |S|$ is the rank listed in Table 1. Moreover if G is untwisted, we may take S to be the image of $\{n_r \mid r \in \Pi\}$, and W is the Coxeter group with the same Dynkin diagram as G. If G is twisted, W is either dihedral or of type A_1, B_l or F_4. The double cosets of B in G are indexed by W, so that

$$G = \coprod_{w \in W} BwB.$$

Here, by abuse of notation, we use BwB to denote $B\bar{w}B$ for any $\bar{w} \in N$ which maps to $w \in W = N/H$. In fact we can say more in the case of groups of Lie type. For each $w \in W$, choose $n_w \in N$ mapping to w. Then every element of G has a unique expression of the form

$$u' n_w h u, \tag{8}$$

where $w \in W$, $u \in U$, $h \in H$ and u' is in a subgroup U_w^- of U [3, Corollary 8.4.4 and Proposition 13.5.3]. We will not use any properties of U_w^-, except that U_1^- is trivial and $U_w^- = U$ when w is the longest element of W.

Let $\ell : W \to \mathbb{Z}_{\geqslant 0}$ denote the usual length function. The product of two double cosets of B in G is determined by the formula

$$(BsB)(BwB) = \begin{cases} BswB & \text{if } \ell(sw) > \ell(w), \\ BswB \cup BwB & \text{if } \ell(sw) < \ell(w), \end{cases} \quad \text{for } s \in S \text{ and } w \in W. \tag{9}$$

A subgroup W' of W is called a *parabolic subgroup* if it is generated by $W' \cap S$. In this case each double coset in $W' \backslash W / W'$ contains a unique element of minimal length; these elements are the *minimal double coset representatives* for W' in W. Also the subset

$$P = \coprod_{w \in W'} BwB$$

is a subgroup of G, also called a parabolic subgroup. There is a natural correspondence between $W' \backslash W / W'$ and $P \backslash G / P$. Explicitly, every double coset in $P \backslash G / P$ can be written as

$$PaP = \coprod_{w \in W' v W'} BwB \tag{10}$$

for some $W' v W' \in W' \backslash W / W'$.

Now suppose $r \in S$, and let $W' \subseteq W$ be the parabolic subgroup generated by $S - \{r\}$. Let P be the corresponding parabolic subgroup of G as above. Our aim is to apply Corollary 16 to $P \subseteq G$. We first prove:

Lemma 17. *We can choose r so that P is good, except when G has type ${}^2G_2$, ${}^2A_2$ or A_1, and q is odd and $|H|$ is even. Moreover any r will suffice, except for types B_2 and ${}^2A_3$.*

Proof. First suppose q is even. Then $|U|$ is a power of 2 and $[G : U]$ is odd, by (7). Hence U is a Sylow-2 subgroup of G. It is noncyclic since G is good. Since $U \subseteq B \subseteq P$, this shows that P is good.

Now suppose q is odd. Note that this excludes types ${}^2B_2$ and ${}^2F_4$. Suppose first that $l = 1$, so that G has type ${}^2G_2$, ${}^2A_2$ or A_1. In these cases, we are not required to prove the statement when $|H|$ is even, so suppose $|H|$ is odd (in fact this can only occur for type A_1). Since $l = 1$ for these groups, W' is trivial and $P = B$. But then $|P| = |H| \cdot |U|$ is odd by (7), so P is good.

Now suppose $l \geqslant 2$. It suffices to prove that P contains two nontrivial commuting involutions, as this would prevent the Sylow-2 subgroup of P from being cyclic. Since $H \subseteq B \subseteq P$ and H is abelian, it suffices to prove that H contains two nontrivial involutions. Let $\#(H)$ denote the number of involutions of H (including the identity).

Recall that H is a quotient $H = \hat{H}/H_1$. It is easy to see that $\#(\hat{H}) \leqslant \#(H)\#(H_1)$. Moreover since p is odd, $\hat{H}$ is a direct product of l cyclic groups of even order, so $\#(\hat{H}) = 2^l$. If G is of type D_k, then $l = k \geqslant 4$ and H_1 is generated by at most two elements, so

$$16 \leqslant \#(\hat{H}) \leqslant \#(H)\#(H_1) \leqslant 4 \times \#(H).$$

Hence $\#(H) \geqslant 4$, as required. In any other case, H_1 is cyclic, so $\#(H_1) \leqslant 2$, giving $\#(H) \geqslant 2^{l-1}$. If $l \geqslant 3$, we again obtain $\#(H) \geqslant 4$. We are left with the rank 2 cases, namely A_2, B_2, G_2, ${}^2A_3$, ${}^2A_4$ and ${}^3D_4$. For types A_2, G_2 and ${}^2A_4$, the group Λ^*/Λ has odd order, so the same is true of H_1. For type ${}^3D_4$, the group H_1 is trivial as noted above. In these cases, $\#(H_1) = 1$, so $\#(H) \geqslant \#(\hat{H}) = 4$, as required.

The remaining cases, B_2 and ${}^2A_3$, are dealt with most easily by realising the group G explicitly. First consider the B_2 case. Let

$$X = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

and consider the group

$$M = \{A \in SL_4(K) \mid A^t X A = X\},$$

where A^t denotes the transpose of A. Let $Z = \{\pm 1\}$ denote the subgroup of scalar matrices in M. There is an isomorphism $G \cong M/Z$ mapping H to the image of the diagonal matrices in M (see [3, Theorem 11.3.2(iii)]). Thus H contains the image of

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Unfortunately, H may not be good in this case. However, P must also contain the double coset of B corresponding to one of the elements of S. By choosing r appropriately, we may suppose P contains the image of

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

The images of these elements in M/Z are distinct commuting involutions, and we are done.

Now consider the ${}^2A_3$ case. Recall that $q = |K|$ is a prime power squared, so K is a degree 2 extension of a subfield L. Let $\bar{}$ be the unique nontrivial automorphism of K over L. Let

$$X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

and consider the group

$$M = \{A \in SL_4(K) \mid A^\dagger X A = X\},$$

where $A^\dagger$ denotes the conjugate transpose of A with respect to $\bar{}$. Again we have $G \cong M/Z$, where Z is the subgroup of scalar matrices in M, and H maps to the image of diagonal matrices (see [3, Theorem 14.5.1]). Now H contains the image of

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Again by choosing r appropriately, we may ensure that P contains the image of

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

As above, the images are distinct commuting involutions, and we are done. □

For the next proof, we require two easy consequences of (9). We say that the expression $u_1 u_2 \dots u_k \in W$ is *reduced* if

$$\ell(u_1 u_2 \dots u_k) = \ell(u_1) + \ell(u_2) + \dots + \ell(u_k).$$

It follows inductively from (9) that if $s_1 s_2 \dots s_k$ is a reduced expression, with $s_i \in S$, then

$$B s_1 s_2 \dots s_k B = (B s_1 B)(B s_2 B) \dots (B s_k B).$$

Hence

$$(BwB)(BuB) = BwuB \quad \text{whenever } wu \text{ is reduced.} \tag{11}$$

It follows that

$$(BwB)(BuB) = (BuB)(BwB) \quad \text{if } wu = uw \text{ is reduced.} \tag{12}$$

Lemma 18. *We can choose r so that every double coset $D \in P\backslash G/P$ satisfies $D^2 \supseteq D$. In the cases of B_2 and ${}^2A_3$, either choice of r will suffice.*

Proof. Because G is a disjoint union of double cosets of P, we need only show that D^2 intersects D for each $D \in P\backslash G/P$. By (10), it suffices to show that every double coset in $W'\backslash W/W'$ contains an element w satisfying

$$(BwB)^2 \supseteq BwB.$$

This will follow if w has a reduced expression of the form

$$w = u^{-1} s_1 s_2 \dots s_p u, \tag{13}$$

where $u \in W$ and the s_i are commuting elements of S (we allow p to be 0 and u to be the identity). Indeed,

$$\begin{aligned}(BwB)(BwB) &= \big(Bu^{-1}B\big)(Bs_1B)\dots(Bs_pB)(BuB)\\ &\quad\times \big(Bu^{-1}B\big)(Bs_1B)\dots(Bs_pB)(BuB) \quad \text{by (11)}\\ &\supseteq \big(Bu^{-1}B\big)(Bs_1B)\dots(Bs_pB)(Bs_1B)\dots(Bs_pB)(BuB)\\ &= \big(Bu^{-1}B\big)(Bs_1B)^2\dots(Bs_pB)^2(BuB) \quad \text{by (12)}\\ &\supseteq \big(Bu^{-1}B\big)(Bs_1B)\dots(Bs_pB)(BuB) \quad \text{by (9)}\\ &= BwB \quad \text{by (11).}\end{aligned}$$

We will consider each possibility for W and, for a particular choice of r, find a set of double coset representatives for W' in W, each with a reduced expression of the form (13); in fact it will be the set of minimal coset representatives in each case.

Case 1 – Dihedral group. Suppose that $l = 2$; that is, W is the dihedral group. Then $S = \{r, s\}$ and rs has order n, where $|W| = 2n$. Now $W' = \{1, s\}$, so the minimal double coset representatives are

$$1, r, rsr, rsrsr, \dots, rsrs\dots srsr,$$

where the length of the last word is n or $n-1$. All these words are of the form (13), as follows. For the identity we take $p = 0$ and $u = 1$. For the rest we take $p = 1$; either $s_1 = r$ and $u = (sr)^i$, or $s_1 = s$ and $u = r(sr)^i$.

Note that our argument did not depend on the choice of $r \in S$; indeed there is an automorphism of W switching the elements of S. In particular this applies in the cases B_2 and ${}^2A_3$, both of which have rank 2.

Case 2 – Type A_l. In this case W is the symmetric group S_{l+1}. Choose r to be the rightmost node, so W' is the natural copy of S_l in S_{l+1}. It is easy to see that there are just two double cosets of W' in W; the minimal coset representatives are 1 and r, both of which are of the form (13).

Case 3 – Type $B_l = C_l$. Now W is the wreath product

$$W = S_l \wr \mathbb{Z}_2 = \big\{(\sigma, \epsilon_1, \epsilon_2, \dots, \epsilon_l) \,\big|\, \sigma \in S_l,\ \epsilon_i = \pm 1\big\}.$$

Write $S = \{\tau, s_1, s_2, \dots, s_{l-1}\}$, where the s_i generate S_l, and

$$\tau = (1, -1, 1, 1, \dots, 1).$$

Let $r = s_{l-1}$. Consider the double coset of W' in W containing $u = (\sigma, \epsilon_1, \epsilon_2, \dots, \epsilon_l)$. As in Case 2, by multiplying u on the left and right by elements of S_{l-1}, we may suppose that $\sigma = 1$ or $\sigma = r$. Also for any $\nu_1, \nu_2, \dots, \nu_{l-1} \in \{\pm 1\}$, the element $(1, \nu_1, \nu_2, \dots, \nu_{l-1}, 1)$ is in W'. Hence if $\sigma = 1$, we may replace u by

$$u(1, \epsilon_1, \epsilon_2, \dots, \epsilon_{l-1}, 1) = (1, 1, \dots, 1, \epsilon_l).$$

If $\sigma = r$, we may replace u by

$$(1, 1, \dots, \epsilon_l, 1)u(1, \epsilon_1, \epsilon_2, \dots, \epsilon_{l-1}, 1) = (r, 1, \dots, 1, 1).$$

Therefore the elements $(1, 1, \dots, 1, \pm 1)$ and $(r, 1, \dots, 1)$ form a set of double coset representatives for W' in W. Written in terms of the generators, these elements are

$$1, r, s_{l-1}s_{l-2} \dots s_1 \tau s_1 s_2 \dots s_{l-1}.$$

Again each is of the form (13).

Case 3 – Type D_l. We may realise W as the subgroup

$$W = \left\{(\sigma, \epsilon_1, \epsilon_2, \dots, \epsilon_l) \in S_l \wr \mathbb{Z}_2 \;\middle|\; \epsilon_1\epsilon_2 \dots \epsilon_l = 1\right\}.$$

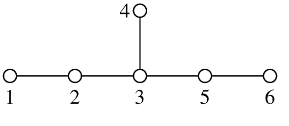
The generating involutions are $\{\rho, s_1, \dots, s_{l-1}\}$, where the s_i are as above, but ρ is now $(s_1, -1, -1, 1, \dots, 1)$. Again let $r = s_{l-1}$. Arguing as in the previous case, the double cosets of W' in W are represented by the elements

$$\begin{aligned}
(1, 1, 1, \dots, 1, 1) &= 1, \\
(1, -1, 1, \dots, 1, -1) &= s_{l-1}s_{l-2} \dots s_2 s_1 \rho s_2 s_3 \dots s_{l-1}, \\
(r, 1, 1, \dots, 1, 1) &= r.
\end{aligned}$$

As above, these expressions are of the form (13).

For a specific Coxeter group, a computer algebra package such as MAGMA [1] can be used to find the minimal double coset representatives for W' in W, and to determine when specified words are reduced. We do so in the remaining cases without further comment. Also for brevity, we simply denote elements of S by integers, and we use ε to denote the identity.

Case 4 – $W = E_6$. Label S as shown below.

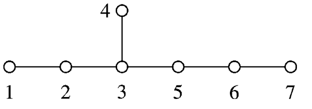


Let $r = 6$. The minimal double coset representatives are

$$\varepsilon, 6, 65324356.$$

The last representative can be written $u^{-1}24u$, with $u = 356$. Since 2 and 4 commute, each representative is of the form (13), and we are done.

Case 5 – $W = E_7$. Label S as shown below.



Let $r = 7$. The minimal double coset representatives are

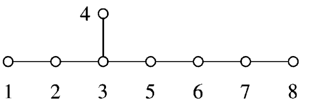
$$\varepsilon, 7, 7653243567, 765321432534653217653243567.$$

The last two words can be written $u_1^{-1} 24 u_1$ and $u_2^{-1} 457 u_2$ respectively, where

$$u_1 = 3567,$$
$$u_2 = 635234123567.$$

Since 2, 4, 5 and 7 all commute, again each word is of the form (13).

Case 6 – $W = E_8$. Label S as shown below.



Let $r = 8$. The minimal double coset representatives are

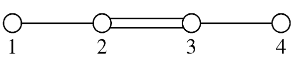
$$\varepsilon, 8, 876532435678, 8765321432534653217653243567 8,$$
$$87653214325346532176532435678765321432534653217653243 5678.$$

The last three words can be written $u_1^{-1} 24 u_1$, $u_2^{-1} 457 u_2$ and $u_3^{-1} 8 u_3$ respectively, where

$$u_1 = 35678,$$
$$u_2 = 6352341235678,$$
$$u_3 = 76534235671235643523412356 78.$$

Again since 2, 4, 5 and 7 all commute, each word is of the form (13).

Case 7 – $W = F_4$. Label S as shown below.



Let $r = 4$. The minimal double coset representatives are

$$\varepsilon, 4, 43234, 43213234, 432132343213234.$$

The last three words can be written $u_1^{-1} 2 u_1$, $u_2^{-1} 13 u_2$ and $u_3^{-1} 4 u_3$ respectively, where

$$u_1 = 34,$$

$$u_2 = 234,$$

$$u_3 = 3213234.$$

Since 1 and 3 commute, each word is of the form (13). □

The previous two lemmas allow us to apply Corollary 16, except when G has type A_1, ${}^2A_2$ or ${}^2G_2$, and q is odd and $|H|$ is even. From this point, suppose G is such a group. Then the Weyl group of G has rank 1; that is, $|W| = 2$. Unfortunately this implies that there is only one proper parabolic subgroup, namely B, and it is bad. We are forced to do some explicit calculations in these cases.

Lemma 19. *There is an involution $n \in N - H$, and $nUn = V$. Every element of G is uniquely expressible either as hu or $u'nhu$, where $h \in H$ and $u, u' \in U$.*

Proof. The second statement is true for any $n \in N - H$ by (8). For type A_1, the group G is $PSL_2(K)$ [3, Theorem 11.3.2], and we may take

$$n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

In the ${}^2A_2$ case, K is a degree 2 extension of a subfield L. Let $\bar{}$ denote the nontrivial automorphism of K over L. Let

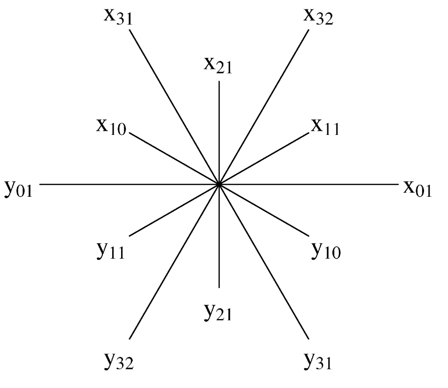
$$X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and $M = \{A \in SL_3(K) \mid A^\dagger X A = X\}$, where † denotes conjugate transpose with respect to $\bar{}$. Then G is M modulo scalar matrices [3, Theorem 14.5.1], and we may take n to be the image of X.

Finally suppose $G = {}^2G_2(q)$, where $q = 3^{2k+1} = 3\theta^2$. Recall that G is a subgroup of the group $\bar{G}$ of type $G_2(q)$. Let r and s denote, respectively, the short and long simple roots of the root system Φ of $\bar{G}$. For brevity we will denote

$$x_{ij}(t) = x_{ir+js}(t), \qquad y_{ij}(t) = x_{-ir-js}(t), \qquad h_{ij}(t) = h_{ir+js}(t), \qquad n_{ij} = n_{ir+js}$$

for $ir + js \in \Phi^+$ and $t \in K$. The root system Φ is depicted below.



Let $n = n_{11}n_{31}$. Then n_{11} and n_{31} commute by (3), so

$$n^2 = n_{11}^2 n_{31}^2 = h_{11}(-1)h_{31}(-1) = 1,$$

using (4). Also n maps to the longest element of the Weyl group of $\bar{G}$, so $n\bar{U}n = \bar{V}$ [3, Lemma 7.2.1]. We have an explicit description of the subgroups $U \subseteq \bar{U}$ and $V \subseteq \bar{V}$ [3, Propositions 13.6.1 and 13.6.3]:

$$U = \{x_{10}(t^\theta)x_{01}(t)x_{11}(t^{\theta+1} + u^\theta)x_{21}(t^{2\theta+1} + v^\theta)x_{31}(u)x_{32}(v) \mid t, u, v \in K\}, \tag{14}$$

$$V = \{y_{10}(t^\theta)y_{01}(t)y_{11}(t^{\theta+1} + u^\theta)y_{21}(t^{2\theta+1} + v^\theta)y_{31}(u)y_{32}(v) \mid t, u, v \in K\}. \tag{15}$$

In particular,

$$n = x_{11}(1)x_{31}(1)y_{11}(-1)y_{31}(-1)x_{11}(1)x_{31}(1) \in UVU \subseteq G.$$

Hence $n \in G \cap (\bar{N} - \bar{H}) = N - H$, and $nUn = G \cap n\bar{U}n = G \cap \bar{V} = V$, as required. □

Lemma 20. *There is a nontrivial element $a \in U$ such that $H \subseteq UVaV$.*

Proof. We give the calculation in the case ${}^2G_2(q)$. Let $a = x_{31}(1)x_{11}(1)$, which is in U by (14). We will show that any element $h \in H$ is in $UVaV$. By (4), we can write $h = h_{10}(\lambda)h_{01}(\mu)$ for some $\lambda, \mu \in K^*$. Recall that we have identified $\bar{H}$ with $\mathrm{Hom}(\Lambda, K^*)$ by defining

$$h_q(\lambda)(v) = \lambda^{\frac{2(q,v)}{(q,q)}}$$

for $q \in \Phi$. By (6),

$$\lambda^2\mu^{-1} = h(r) = h(s)^\theta = \lambda^{-3\theta}\mu^{2\theta}.$$

Putting both sides to the power $3\theta - 2$, and noting that $t^{3\theta^2} = t$ for $t \in K$, we obtain $\lambda = \mu^\theta$. Since $|K^*| = 3^{2k+1} - 1 \equiv 2 \pmod 4$, there are no elements of order 4 in K^*, so -1 is not a square. Thus we can either write $\mu^{-1} = \nu^2$ or $\mu^{-1} = -\nu^2 = \nu^2 + \nu^2$. In either case $\mu^{-1} = \nu^2 + \kappa^2$ for some $\nu \in K^*$ and $\kappa \in K$. Finally

$$(3\theta + 1, q - 1) = (3\theta + 1, 3\theta^2 - 1) = (3\theta + 1, \theta + 1) = (2, \theta + 1) = 2,$$

so we can choose $\iota \in K^*$ with $\iota^{3\theta+1} = \nu^2$. We can therefore write

$$h = h_{10}(\iota^{\theta+1} + \kappa^{2\theta})^{-1}h_{01}(\iota^{3\theta+1} + \kappa^2)^{-1} \tag{16}$$

with $\iota \neq 0$. Given $t, u \in K$ with $tu \neq -1$, we have

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u \\ t & 1 + tu \end{pmatrix} = \begin{pmatrix} 1 & u\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t\lambda^{-1} & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix},$$

where $\lambda = (1 + tu)^{-1}$. Applying the homomorphism $\rho_{ir+js} : SL_2(K) \to \bar{G}$ gives $y_{ij}(t)x_{ij}(u) = x_{ij}(u\lambda)y_{ij}(t\lambda^{-1})h_{ij}(\lambda)$. Using this and Chevalley's commutator formula (3), and noting that K has characteristic 3, we calculate

$$
\begin{aligned}
&\bar{U} y_{21}(t) y_{32}(u) x_{31}(v) x_{11}(w) \bar{V} \\
&\quad = \bar{U} y_{21}(t) x_{31}(v) y_{01}(-uv) y_{32}(u) x_{11}(w) \bar{V} \\
&\quad = \bar{U} x_{31}(v) x_{10}(-tv) y_{11}\big(t^2 v\big) y_{32}\big(t^3 v\big) y_{01}\big(t^3 v^2\big) y_{21}(t) y_{01}(-uv) y_{32}(u) x_{11}(w) \bar{V} \\
&\quad = \bar{U} y_{01}\big(t^3 v^2 - uv\big) y_{32}\big(t^3 v + u\big) y_{11}\big(t^2 v\big) y_{21}(t) x_{11}(w) \bar{V} \\
&\quad = \bar{U} y_{01}\big(t^3 v^2 - uv\big) y_{32}\big(t^3 v + u\big) y_{11}\big(t^2 v\big) x_{11}(w) y_{10}(2tw) y_{21}(t) \bar{V} \\
&\quad = \bar{U} y_{01}\big(t^3 v^2 - uv\big) y_{32}\big(t^3 v + u\big) y_{11}\big(t^2 v\big) x_{11}(w) \bar{V} \\
&\quad = \bar{U} y_{01}\big(t^3 v^2 - uv\big) y_{32}\big(t^3 v + u\big) x_{11}(w\mu) \bar{V} h_{11}(\mu) \quad \text{with } \mu = \big(1 + t^2 vw\big)^{-1} \\
&\quad = \bar{U} y_{01}\big(t^3 v^2 - uv\big) x_{11}(w\mu) x_{01}\big(-w^3 \mu^3 \big(t^3 v + u\big)\big) \bar{V} h_{11}(\mu) \\
&\quad = \bar{U} y_{01}\big(t^3 v^2 - uv\big) x_{01}\big(-w^3 \mu^3 \big(t^3 v + u\big)\big) \bar{V} h_{11}(\mu) \\
&\quad = \bar{U} \bar{V} h_{01}\big(1 - vw^3 \mu^3 \big(t^3 v + u\big)\big(t^3 v - u\big)\big)^{-1} h_{11}(\mu) \\
&\quad = \bar{U} \bar{V} h_{01}\big(1 - vw^3 \mu^3 \big(t^6 v^2 - u^2\big)\big)^{-1} h_{01}(\mu)^3 h_{10}(\mu) \quad \text{by (4)} \\
&\quad = \bar{U} \bar{V} h_{01}\big(\big(1 + t^2 vw\big)^3 - vw^3 \big(t^6 v^2 - u^2\big)\big)^{-1} h_{10}(\mu) \\
&\quad = \bar{U} \bar{V} h_{01}\big(1 + u^2 vw^3\big)^{-1} h_{10}\big(1 + t^2 vw\big)^{-1},
\end{aligned}
$$

assuming that $1 + t^2 vw$ and $1 + u^2 vw^3$ are nonzero. Thus with ι and κ as in (16),

$$
\begin{aligned}
&\bar{U} y_{21}\big(\kappa^\theta\big) y_{32}(\kappa) y_{31}(\iota - 1) y_{11}\big(\iota^\theta - 1\big) a \bar{V} \\
&\quad = \bar{U} y_{21}\big(\kappa^\theta\big) y_{32}(\kappa) y_{31}(\iota - 1) y_{11}\big(\iota^\theta - 1\big) x_{31}(1) x_{11}(1) \bar{V} \\
&\quad = \bar{U} y_{21}\big(\kappa^\theta\big) y_{32}(\kappa) x_{31}\big(\iota^{-1}\big) x_{11}\big(\iota^{-\theta}\big) \bar{V} h_{11}\big(\iota^{-\theta}\big) h_{31}\big(\iota^{-1}\big) \\
&\quad = \bar{U} \bar{V} h_{01}\big(1 + \kappa^2 \iota^{-3\theta-1}\big)^{-1} h_{10}\big(1 + \kappa^{2\theta} \iota^{-\theta-1}\big)^{-1} h_{11}\big(\iota^{-\theta}\big) h_{31}\big(\iota^{-1}\big) \\
&\quad = \bar{U} \bar{V} h_{10}\big(\iota^{\theta+1} + \kappa^{2\theta}\big)^{-1} h_{01}\big(\iota^{3\theta+1} + \kappa^2\big)^{-1} \quad \text{by (4)} \\
&\quad = \bar{U} \bar{V} h.
\end{aligned}
$$

Now $y_{21}(\kappa^\theta) y_{32}(\kappa) y_{31}(\iota - 1) y_{11}(\iota^\theta - 1) \in V$ by (15), so

$$h \in \bar{U} V a \bar{V} = \bar{U} n U n a n \bar{U} n.$$

Write $h = bncnandn$, where $b, d \in \bar{U}$ and $c \in U$. Rearranging,

$$dnh^{-1} b = na^{-1} nc^{-1} n.$$

Recall that U and V are the subgroups of $\bar{U}$ and $\bar{V}$ fixed by σ. The right hand side above is invariant under σ, so $dnh^{-1} b = \sigma(d) nh^{-1} \sigma(b)$. Now (8) implies $d = \sigma(d)$ and $b = \sigma(b)$; that is, $d, b \in U$. Hence $h \in UVaV$, as required.

In the notation of the previous proof, we may take

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

in the A_1 case, and

$$a = \begin{pmatrix} 1 & 0 & \epsilon \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

in the $^2A_2$ case, where $\epsilon \in K^*$ satisfies $\epsilon + \bar{\epsilon} = 0$. We omit these calculations as they are similar to, but much easier than, the $^2G_2$ calculation. □

Lemma 21. *The double cosets of U satisfy $(UnhU)(Unh'U) \supseteq (Unh''U)$ for all $h, h', h'' \in H$.*

Proof. Let $a \in U$ be the nontrivial element constructed in the previous lemma. Suppose $nan \in B$. Then $nan = hb$ for some $h \in H$ and $b \in U$, giving $an = nhb$. Expressions of the form $UnHU$ are unique, so $a = 1$, a contradiction. Hence $nan \notin B$, so $nan \in UnhU$ for some $h \in H$. Since H normalises U, we obtain

$$H \subseteq UnUnanUn \subseteq UnU(UnhU)Un = UnUnUnh^n.$$

But n normalises H, so $h^n \in H$. Hence $H \subseteq UnUnUn$. Now for arbitrary $h, h', h'' \in H$, we have

$$nh'' \in nHh^nh' = Hnh^nh' \subseteq UnUnUh^nh' = UnhUnh'U.$$

Thus $(UnhU)(Unh'U) \supseteq Unh''U$, as required. □

This lemma suggests that we should apply Corollary 15 to the subgroup U; indeed $|U|$ is odd by (7), so U possesses a complete mapping. However, the normaliser of U is B, and $B/U \cong H$. Since $l = 1$, the group $\hat{H}$ is cyclic, so H is a cyclic group of even order. This implies that no permutations of $U\backslash G/U$ can satisfy the conditions of Corollary 15. Nevertheless we can come close using the following lemma, which says that H falls one equation short of having a complete mapping.

Lemma 22. *If C is a cyclic group of even order, then there exist permutations α and β of C such that $c\alpha(c) = \beta(c)$ for $c \neq 1$. Moreover we can take $\beta(1) = 1$ and $\alpha(1) \neq 1$.*

Proof. Identify C with $\mathbb{Z}_{2k}$, written additively. Let $\alpha(0) = k$. For $1 \leqslant i < k$, let $\alpha(i) = i$, and for $k \leqslant i < 2k$, let $\alpha(i) = i + 1$. For $0 \leqslant i < k$, let $\beta(i) = 2i$, and for $k \leqslant i < 2k$, let $\beta(i) = 2i + 1$. It is clear that $i + \alpha(i) = \beta(i)$ for $i \neq 0$. Also $\beta(i)$ takes all the even values for $0 \leqslant i < k$, and all the odd values for $k \leqslant i < 2k$. Thus β is a permutation, and it is easy to see that α is a permutation also. □

The proof of Corollary 15 constructs permutations of the left cosets satisfying the conditions of Proposition 14. To prove the next result, we apply the same construction to permutations of $U\backslash G/U$ which do not quite satisfy the required conditions. After some tweaking, we can apply Proposition 14 directly.

Lemma 23. *Suppose G has type A_1, $^2A_2$ or $^2G_2$, q is odd and $|H|$ is even. Then G possesses a complete mapping.*

Proof. The left cosets of U in G are exactly hU and $unhU$ for $u \in U$ and $h \in H$. Let $I = H \amalg (U \times H)$. We will define bijections $\bar{x}$, $\bar{y}$ and $\bar{z}$ from I to G/U as follows. Firstly, for any $h \in H$, Lemma 21 gives

$$nhU \subseteq UnhUnhU.$$

Thus there exists $v_h \in U$ such that $nhU \subseteq v_h nhUnhU$. Let α and β be the permutations of H given by Lemma 22. Define

$$\begin{aligned} &\bar{x}(h) = hU, && \bar{y}(h) = \alpha(h)U, && \bar{z}(h) = \beta(h)U, \\ &\bar{x}(u,h) = uv_h nhU, && \bar{y}(u,h) = unhU, && \bar{z}(u,h) = unhU. \end{aligned}$$

Since α and β are permutations, $\bar{x}$, $\bar{y}$ and $\bar{z}$ are certainly bijections from I to G/U. Also

$$\bar{x}(u,h)\bar{y}(u,h) = uv_h nhUunhU = u(v_h nhUnhU) \supseteq unhU = \bar{z}(u,h)$$

for any $(u,h) \in U \times H$, and

$$\bar{x}(h)\bar{y}(h) = h\alpha(h)U = \beta(h)U = \bar{z}(h),$$

provided $h \neq 1$. Unfortunately this does not hold when $h = 1$. We therefore tweak a few values; put $\zeta = \alpha(1)^{-1} \neq 1$, and define

$$\begin{aligned} &\tilde{x}(1) = v_\zeta v_1 nU, && \tilde{y}(1) = v_\zeta nU, && \tilde{z}(1) = U, \\ &\tilde{x}(v_\zeta, 1) = v_\zeta n\zeta U, && \tilde{y}(v_\zeta, 1) = \alpha(1)U, && \tilde{z}(v_\zeta, 1) = v_\zeta nU, \\ &\tilde{x}(1,\zeta) = U, && \tilde{y}(1,\zeta) = n\zeta U, && \tilde{z}(1,\zeta) = n\zeta U. \end{aligned}$$

Define $\tilde{x}$, $\tilde{y}$ and $\tilde{z}$ to coincide with $\bar{x}$, $\bar{y}$ and $\bar{z}$ on $I - \{1, (v_\zeta, 1), (1,\zeta)\}$. Recalling that $\beta(1) = 1$, we have

$$\begin{aligned} \bar{x}\big(\{1, (v_\zeta, 1), (1,\zeta)\}\big) &= \{U, v_\zeta v_1 nU, v_\zeta n\zeta U\} = \tilde{x}\big(\{1, (v_\zeta, 1), (1,\zeta)\}\big), \\ \bar{y}\big(\{1, (v_\zeta, 1), (1,\zeta)\}\big) &= \{\alpha(1)U, v_\zeta nU, n\zeta U\} = \tilde{y}\big(\{1, (v_\zeta, 1), (1,\zeta)\}\big), \\ \bar{z}\big(\{1, (v_\zeta, 1), (1,\zeta)\}\big) &= \{U, v_\zeta nU, n\zeta U\} = \tilde{z}\big(\{1, (v_\zeta, 1), (1,\zeta)\}\big). \end{aligned}$$

Thus $\tilde{x}$, $\tilde{y}$ and $\tilde{z}$ are also bijections. Also

$$\begin{aligned} \tilde{x}(1)\tilde{y}(1) &= v_\zeta v_1 nUv_\zeta nU \supseteq v_\zeta v_1 n^2 U = U = \tilde{z}(1), \\ \tilde{x}(v_\zeta, 1)\tilde{y}(v_\zeta, 1) &= v_\zeta n\zeta U\alpha(1)U = v_\zeta n\alpha(1)^{-1}\alpha(1)U = v_\zeta nU = \tilde{z}(v_\zeta, 1), \\ \tilde{x}(1,\zeta)\tilde{y}(1,\zeta) &= Un\zeta U \supseteq n\zeta U = \tilde{z}(1,\zeta). \end{aligned}$$

Thus $\tilde{x}(i)\tilde{y}(i) \supseteq \tilde{z}(i)$ for all $i \in I$, so Proposition 14 gives the result. □

Summarising these results, we have:

Theorem 24. *Suppose G is a minimal counterexample to the HP conjecture. Then G is one of the* 26 *sporadic simple groups or the Tits group.*

Proof. By Theorem 12, the group G must be simple. Therefore G is either a cyclic group, an alternating group, a simple group of Lie type, the Tits group, or one of the 26 sporadic groups [4]. The HP conjecture holds for cyclic groups by Proposition 1. It holds for alternating groups by Theorem 3 of [12]. Suppose G is a simple group of Lie type. Suppose G is not covered by Lemma 23. Then Lemmas 17 and 18 show that G has a good proper subgroup P whose double cosets D satisfy $D^2 \supseteq D$. By the minimality assumption, P admits a complete mapping, so Corollary 16 shows that G admits a complete mapping. Therefore the only remaining groups are the sporadic groups and the Tits group. □

Acknowledgments

The author would like to thank Peter McNamara and Martin Isaacs for useful discussions concerning Lemma 8, and also Bob Howlett for explaining how to find minimal double coset representatives with MAGMA.

References

[1] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265, Computational Algebra and Number Theory, London, 1993, http://magma.maths.usyd.edu.au/magma/.
[2] N. Bourbaki, Éléments de mathématique, Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968.
[3] Roger W. Carter, Simple Groups of Lie Type, Wiley Classics Lib., John Wiley & Sons Ltd., New York, 1972.
[4] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups, Oxford University Press, Eynsham, 1985, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J.G. Thackray.
[5] F. Dalla Volta, N. Gavioli, Complete mappings in some linear and projective groups, Arch. Math. (Basel) 61 (2) (1993) 111–118.
[6] F. Dalla Volta, N. Gavioli, Minimal counterexamples to a conjecture of Hall and Paige, Arch. Math. (Basel) 77 (3) (2001) 209–214.
[7] Francesca Dalla Volta, Norberto Gavioli, On the admissibility of some linear and projective groups in odd characteristic, Geom. Dedicata 66 (3) (1997) 245–254.
[8] O.M. Di Vincenzo, On the existence of complete mappings of finite groups, Rend. Mat. Appl. (7) 9 (2) (1989) 189–198.
[9] Anthony B. Evans, The admissibility of sporadic simple groups, J. Algebra 321 (2009) 105–116.
[10] Anthony B. Evans, The existence of complete mappings of finite groups, in: Proceedings of the Twenty-third Southeastern International Conference on Combinatorics, Boca Raton, FL, 1992, in: Graph Theory Comput., vol. 90, 1992, pp. 65–75.
[11] Walter Feit, John G. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963) 775–1029.
[12] Marshall Hall, L.J. Paige, Complete mappings of finite groups, Pacific J. Math. 5 (1955) 541–549.
[13] Marshall Hall, Jr., Combinatorial Theory, Blaisdell Publishing Co. Ginn and Co., Waltham, MA/Toronto, ON/London, 1967.
[14] Marshall Hall, Jr., The Theory of Groups, Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition.
[15] I.M. Isaacs, G.R. Robinson, On a theorem of Frobenius: Solutions of $x^n = 1$ in finite groups, Amer. Math. Monthly 99 (4) (1992) 352–354.
[16] Henry B. Mann, The construction of orthogonal Latin squares, Ann. Math. Statist. 13 (1942) 418–423.
[17] Donato Saeli, Complete mappings and difference ratio in double loops, Riv. Mat. Univ. Parma (4) 15 (1989) 111–117.