A characterization of the full wreath product

J.I. Hall
Department of Mathematics
Michigan State University
East Lansing, Michigan 48824, U.S.A.
jhall@math.msu.edu

Version of: 22 December 2005

1 Introduction

A groupoid [3, 17] is a set Q endowed with a binary product, that is, a map from $Q \times Q$ to Q. In his 1964 paper [7], Bernd Fischer studied distributive quasigroups, which by definition are groupoids Q for which right multiplication by any fixed element gives an automorphism of Q as does left multiplication. Fischer proved that the right multiplication group $R(Q)$ of a finite distributive quasigroup Q is solvable. He did this by showing that, for a minimal counterexample, the right multiplications $T = \{ \mu_a \colon g \mapsto ga \mid a \in Q \}$ are a generating conjugacy class of involutions in $R(Q) \leq \mathrm{Aut}(Q)$ with the additional property that $|tr| = 3$ for distinct t and r from T. He then proved that this property forces finite $R(Q)$ to have a normal 3-group of index 2.

This led Fischer to consider [8, 9, 10] the extent to which finite symmetric groups can be characterized through being generated by a conjugacy class of involutions with all products of order 1, 2, or 3—a class of 3-*transpositions*, since the model is the transposition (2-cycle) class of $\mathrm{Sym}(\Omega)$, the symmetric group on the set Ω. In a landmark theorem [10], Fischer found all finite 3-transposition groups with no nontrivial solvable normal subgroups, discovering three new sporadic simple groups along the way.

At the same time that Fischer was considering distributive quasigroups, George Glauberman was working on certain special groupoids, called Bruck loops. Glauberman [13] proved that finite Bruck and finite Moufang loops of odd order are solvable. His approach was similar to Fischer's. He constructed a canonical conjugacy class T of involutory loop permutations with the additional property that $|tr|$ was always odd for t and r from T. In his famous Z^*-theorem [14], Glauberman then proved that a finite group generated by such a class T has a normal subgroup of odd order and index 2 (a result also proved by Fischer [7] in the special case where all orders $|tr|$ are powers of some fixed odd prime).

Fischer's and Glauberman's work on finite quasigroups and loops had a profound effect on the theory of finite simple groups. For a normal set of involutions

T in the group G, let the *order spectrum* of T be the set $\mathrm{Spec}(T) = \{\, |tr| \mid t, r \in G \,\}$. Fischer's questions concerned groups generated by a class T with spectrum contained in $\{1, 2, 3\}$, and Glauberman's work dealt with a class whose spectrum was entirely odd.

If $G = \langle T \rangle$, then by convention G is called an *S-transposition* group, where $S = \mathrm{Spec}(T) \setminus \{1, 2\}$ (since 1 is always in the spectrum and Glauberman's Z^*-theorem largely handles the case when 2 is not in the spectrum). Fischer's ideas motivated a great deal of work characterizing finite groups in terms of the spectrum of an involution class. Notable early examples were Timmesfeld's results [19] on finite $\{3, 4\}$-transposition groups and Aschbacher's classification [1] of finite odd-transposition groups (order spectrum in $\{1, 2, 3, 5, 7, 9, \ldots\}$) with no nontrivial solvable normal subgroup.

Much later Cuypers and the present author [5] classified all 3-transposition groups with trivial center and having order spectrum $\{1, 2, 3\}$. In contrast to Fischer's theorem where the groups that occur are nearly simple, there are conclusions with relatively complicated normal structure. In particular, the following construction due to Zara and, in part, Doro becomes relevant. (Here $\mathrm{FSym}(\Omega)$ is the subgroup of $\mathrm{Sym}(\Omega)$ generated by transpositions; see Section 2.2 below.)

(1.1) THEOREM. **(Zara [21], Doro [6])** *Let T be the transposition class of the full wreath product $K \wr_\Omega \mathrm{FSym}(\Omega)$ with $|\Omega| \geq 2$. Let the associated projection homomorphism be $\pi\colon K \wr_\Omega \mathrm{FSym}(\Omega) \longrightarrow \mathrm{FSym}(\Omega)$. Then, for all $t, r \in T$, we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,.$$

The order spectrum $\mathrm{Spec}(T) = \{\, |tr| \mid t, r \in T \,\}$ is equal to $\{\, |k| \mid k \in K \,\}$ when $|\Omega| = 2$, equal to $\{3\} \cup \{\, |k| \mid k \in K \,\}$ when $|\Omega| = 3$, and equal to $\{2, 3\} \cup \{\, |k| \mid k \in K \,\}$ when $|\Omega| > 3$.

Therefore, in considering general 3-transposition groups in [15, Theorem 8.2], the author needed to characterize full wreath products in which the wreathed group K had all elements of order 1, 2, or 3. Similarly, in Aschbacher's work on odd-transpositions, he had to characterize [1, Lemma 3.11] wreath products with K isomorphic to $\mathrm{PSL}_2(2^a)$, for $a \geq 2$, as these are simple groups each of whose elements has order 2 or odd order.

Let $\mathrm{Wr}(K, \Omega)$ be the subgroup of $K \wr_\Omega \mathrm{FSym}(\Omega)$ that is generated by the transposition class. The next theorem is the main result of this paper and provides a nearly complete converse to Theorem 1.1.

(1.2) THEOREM. *Let T be a conjugacy class of involutions in the group $G = \langle T \rangle$; and let $\pi\colon G \longrightarrow \mathrm{FSym}(\Omega)$, with $|\Omega| \geq 4$, be a homomorphism in which $\pi(T)$ is the transposition class of $\mathrm{FSym}(\Omega)$. Further assume that, for all $t, r \in T$, we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,.$$

Then there is a group K with

$$G/Z(G) \simeq \mathrm{Wr}(K,\Omega)/Z(\mathrm{Wr}(K,\Omega))\,.$$

For $\pi(t) \neq \pi(r)$ the only possible orders $|\pi(t)\pi(r)|$ are 2 and 3. A version of the theorem holds even if we only assume, for all $t, r \in T$, that we have

$$(\dagger) \qquad \textit{if } |\pi(t)\pi(r)| = 2, \textit{ then } |tr| = 2\,.$$

Section 2 provides various properties of wreath products, in particular a proof of the Zara-Doro Theorem 1.1. Section 3 then proves Theorem 1.2 in a more precise form and presents some related results, such as that on (†) mentioned in the previous paragraph. Section 4 deals with symmetric quotients $\mathrm{Sym}(\Omega)$ for which we only assume

$$(\ddagger) \qquad \textit{if } |\pi(t)\pi(r)| = 3, \textit{ then } |tr| = 3\,,$$

the focus and critical case being $|\Omega| = 3$. We see that such groups are intimately connected with Moufang loops; so we have come full circle, arriving back at quasigroups and loops—Fischer's and Glauberman's original motivations. We use Theorem 1.2 to characterize and illuminate certain Moufang loops first discussed by Chein [4][1]. We close Section 4 and the paper by noting that a counterpart to Theorem 1.2 assuming only (‡) would have a much longer list of conclusions.

Our general references for quasigroups and loops are [3, 17]. For group theory, see [2].

2 Wreath products

2.1 Relative universal central extensions

Let G be a group generated by the normal subset T of involutions. Consider the group $\mathrm{U}(G,T)$ given by the presentation

$$\mathrm{U}(G,T) = \langle\, \tilde{t},\, t \in T \,|\, \tilde{t}\tilde{r}\tilde{t} = \widetilde{trt},\, t,r \in T \,\rangle\,.$$

The group $\mathrm{U}(G,T)$ is the *universal central extension of G relative to T*. We also write $\mathrm{UT}(G,T) = \{\, \tilde{t} \,|\, t \in T \,\}$. The terminology is justified by

(2.1) Proposition. *The map $\tilde{t} \mapsto t$ extends to a homomorphism from $\mathrm{U}(G,T)$ onto G with kernel Z central in $\mathrm{U}(G,T)$. Indeed let G_0 be a group generated by a normal set of involutions T_0 for which there exists a bijection $\phi\colon T \longrightarrow T_0$ with $\phi(t)\phi(r)\phi(t) = \phi(trt)$, for all $t,r \in T$. Then there is a central subgroup Z_0 of $\mathrm{U}(G,T)$ with $G_0 \simeq \mathrm{U}(G,T)/Z_0$ and $\mathrm{UT}(G,T)Z_0/Z_0 = T_0$.*

Furthermore, for all $t,r \in T$, we have $|tr| = |\phi(t)\phi(r)| = |\tilde{t}\tilde{r}|$.

[1] After this paper was submitted, the author learned that R.T. Curtis had, in a Rayleigh Prize essay submitted to the University of Cambridge in early 1970, given a Moufang loop construction essentially the same as that of Chein.

PROOF. There is a canonical isomorphism between $\mathrm{U}(G,T)$ and $\mathrm{U}(G_0,T_0)$, so we need only verify the remarks relating $\tilde{G} = \mathrm{U}(G,T)$ and G. Set $\tilde{T} = \mathrm{UT}(G,T)$. By design G is a homomorphic image of $\tilde{G}$. In particular, each $\tilde{t}$ has even order and each $|\tilde{t}\tilde{r}|$ is a multiple of $|tr|$.

The elements $\tilde{t}$ of even order are indeed involutions, since $\tilde{t} = \widetilde{ttt} = \tilde{t}\tilde{t}\tilde{t}$ for all $t \in T$. Therefore $\tilde{t}\tilde{r}\tilde{t} = \tilde{t}^{-1}\tilde{r}\tilde{t}$, and the set $\tilde{T}$ is a normal generating set for $\tilde{G}$. Considering the image $\tilde{G}/Z \simeq G$, we find $\tilde{T} \cap \tilde{t}Z = \{\tilde{t}\}$ for each $\tilde{t} \in \tilde{T}$. Thus Z fixes each $\tilde{t}$ and so is central in $\tilde{G} = \langle \tilde{T} \rangle$, as claimed.

Let $|tr| = k$, so that k divides $|\tilde{t}\tilde{r}|$. The relation $(tr)^k = 1$ is equivalent to the relation $trt \cdots trt = r$, which says that two elements from T are equal. This leads in $\tilde{G}$ to the corresponding relation in $\tilde{t}$ and $\tilde{r}$ and thus to $(\tilde{t}\tilde{r})^k = 1$. Therefore $\tilde{t}\tilde{r}$ has order k. For instance, if tr has order 3, then $\tilde{t}(\tilde{r}\tilde{t}\tilde{r})\tilde{t} = \tilde{t}\,\widetilde{rtr}\,\tilde{t} = (t(rtr)t)^{\sim} = \tilde{r}$; so $(\tilde{t}\tilde{r})^3 = 1$, and $\tilde{t}\tilde{r}$ has order 3.

REMARKS. (1) Start from the free group with a generator $\hat{g}$ for each element g of the group G. The multiplication table for G then gives a natural set of relations $\hat{g}\hat{h} = \widehat{gh}$ that defines G. Similarly here, the transform table for the generating normal set T defines G up to a central subgroup (not visible in the transform data).

(2) An equivalent set of relations would consist of all $\tilde{t}^2 = 1$ and $\tilde{t}^{\tilde{r}} = \widetilde{t^r}$. For a normal generating subset with elements of arbitrary order, the orders and transform table can again be used to define a relative universal central extension, although orders of products do not behave in general. For instance, if $T = \{t_1, \ldots, t_4\}$ is a conjugacy class of elements of order 3 in $\mathrm{Sym}(4)$, then the corresponding universal group

$$\langle\, \tilde{t}_i,\ 1 \le i \le 4 \,|\, \tilde{t}_i^3 = 1,\ \tilde{t}_i^{-1}\tilde{t}_j\tilde{t}_i = \widetilde{t_i^{-1}t_jt_i},\ 1 \le i,j \le 4 \,\rangle$$

is $\mathrm{SL}_2(3)$, where $|\tilde{t}_i\tilde{t}_j| = 6$ whenever $|t_it_j| = 3$.

2.2 Some properties of wreath products

If Ω is a set, then the finitary symmetric group $\mathrm{FSym}(\Omega)$ is the group of all permutations of Ω that only move a finite number of letters. Thus when Ω is finite $\mathrm{FSym}(\Omega) = \mathrm{Sym}(\Omega)$, but when Ω is infinite $\mathrm{FSym}(\Omega)$ is a proper normal subgroup of $\mathrm{Sym}(\Omega)$. Here $\mathrm{FSym}(\Omega)$ might best be thought of as the normal subgroup generated by the conjugacy class $(a,b)^{\mathrm{Sym}(\Omega)} = (a,b)^{\mathrm{FSym}(\Omega)}$ of all 2-cycles or *transpositions*.

Any automorphism of $\mathrm{FSym}(\Omega)$ that takes transpositions to transpositions actually belongs to $\mathrm{Sym}(\Omega)$. In particular, since we always will identify the transposition class, we will not need to worry about the distinction between $\mathrm{FSym}(\Omega)$ as permutation group and as abstract group. A subgroup H of $\mathrm{FSym}(\Omega)$ that is generated by transpositions must be the subgroup $\bigoplus \mathrm{FSym}(\Delta)$, where Δ runs through the nontrivial orbits of H on Ω.

Let G be a group that acts permuting the G-space Ω. Given a group K, the *wreath product* $K \wr_\Omega G$ is the split extension of $B = K^\Omega$ by G. The base group

B is the group of all functions from Ω to K with pointwise multiplication, the action of G on B being given by $f^g(x^g) = f(x)$, for $f \in B$, $x \in \Omega$, and $g \in G$. In the special case $G = \mathrm{Sym}(\Omega)$, we call $K \wr_\Omega \mathrm{Sym}(\Omega)$ the *(unrestricted) full wreath product*.

For each $x \in \Omega$, there is an injection of K into B written $k \mapsto k_x$ with image K_x, where the function k_x has values $k_x(x) = k$ and $k_x(y) = 1$ for $y \in \Omega$ with $y \neq x$. The subgroup $B_0 \simeq \bigoplus_{x\in\Omega} K_x$ spanned by the various K_x is invariant under G, and the subgroup $B_0 : \mathrm{Sym}(\Omega)$ is the *restricted full wreath product*. The action simplifies to $k_x^g = k_{x.g}$.

We shall be interested in normal subgroups $B : \mathrm{FSym}(\Omega)$ $(= K \wr_\Omega \mathrm{FSym}(\Omega))$ and $B_0 : \mathrm{FSym}(\Omega)$, the *finitary full wreath products*. Of course for finite Ω we have

$$K \wr_\Omega \mathrm{Sym}(\Omega) = B_0 : \mathrm{Sym}(\Omega) = B_0 : \mathrm{FSym}(\Omega) = B : \mathrm{FSym}(\Omega)\,.$$

Indeed, essentially all our calculations will be done within the group

$$\mathrm{Wr}(K, \Omega) = [B, \mathrm{FSym}(\Omega)]\,\mathrm{FSym}(\Omega) \leq B_0 : \mathrm{FSym}(\Omega)\,,$$

which we call the *augmented full wreath product*. The group $\mathrm{Wr}(K, \Omega)$ is again best thought of as the normal subgroup of the wreath product generated by the conjugacy class $T = (a, b)^{K\wr_\Omega \mathrm{FSym}(\Omega)}$ containing the 2-cycle class of $\mathrm{FSym}(\Omega)$ (see Lemma 2.2 below). We call $T = \mathrm{T}(K, \Omega)$ the set of *transpositions* of $K \wr_\Omega \mathrm{FSym}(\Omega)$.

For each of the various versions of the wreath product, the intersection with B is the corresponding *base* subgroup. The homomorphism π with the base subgroup as kernel is *projection* onto the corresponding version of the symmetric group. We write $\mathrm{B}(K, \Omega)$ for $B \cap \mathrm{Wr}(K, \Omega) = [B, \mathrm{FSym}(\Omega)]$.

Throughout we will write $\mathrm{Sym}(n)$ for the group $\mathrm{Sym}(\{1, 2, \ldots, n\})$, $\mathrm{Wr}(K, n)$ for $\mathrm{Wr}(K, \{1, 2, \ldots, n\})$, and so forth.

(2.2) Lemma. *Let (a, b) be a transposition of $\mathrm{FSym}(\Omega) \leq K \wr_\Omega \mathrm{Sym}(\Omega)$. Then $T \cap (a, b)B = (a, b)^B = \{\, k_a k_b^{-1}(a, b) \mid k \in K \,\}$. In particular, $\mathrm{Wr}(K, \Omega) = \langle \mathrm{T}(K, \Omega) \rangle$. If $|\Omega| \geq 3$ then $(a, b)^B = (a, b)^{[B,(b,c)]}$.*

Proof. The normalizer of the coset $(a, b)B$ is generated by $(a, b)B$ and $\mathrm{Sym}(\Omega \setminus \{a, b\})$, which centralizes (a, b). Therefore $T \cap (a, b)B = (a, b)^{(a,b)B} = (a, b)^B$, giving the first equality.

For $f \in B$ we have $(a, b)^f = [f, (a, b)](a, b)$, so we calculate $[f, (a, b)] = f^{-1} f^{(a,b)}$. If $x \in \Omega \setminus \{a, b\}$, then $f^{-1} f^{(a,b)}(x) = f^{-1}(x) f^{(a,b)}(x) = f(x)^{-1} f(x) = 1$. On the other hand $f^{-1} f^{(a,b)}(a) = f(a)^{-1} f(b) = k$, say, and $f^{-1} f^{(a,b)}(b) = f(b)^{-1} f(a) = k^{-1}$. Therefore $[f, (a, b)] = f^{-1} f^{(a,b)} = k_a k_b^{-1}$, as claimed. All possible k do occur, as seen by taking $f = k_b$ or indeed any function with $f(a) = 1$ and $f(b) = k$, for instance $f(c) = k^{-1}$.

(2.3) Corollary. *Assume $|\Omega| \geq 3$. Then*

$$[\mathrm{B}(K, \Omega), (a, b)] = [B, (a, b)] = (K'_a \times K'_b)\{\, k_a k_b^{-1} \mid k \in K \,\}\,.$$

In particular $[\mathrm{B}(K,\Omega),(a,b)] \cap [\mathrm{B}(K,\Omega),(b,c)] = K'_b$ *and*

$$K \simeq [\mathrm{B}(K,\Omega),(a,b)]/[\mathrm{B}(K,\Omega),(a,b)] \cap [\mathrm{B}(K,\Omega),(b,c)]\,.$$

PROOF. Clearly $[\mathrm{B}(K,\Omega),(a,b)] \leq [B,(a,b)] \leq (K'_a \times K'_b)\{\, k_a k_b^{-1} \mid k \in K \,\}$, so it is enough to show $K'_a \leq [\mathrm{B}(K,\Omega),(a,b)]$. But $[k_a k_c^{-1}, [h_b h_c^{-1}, (a,b)]] = [k,h]_a$.

(2.4) PROPOSITION. *For arbitrary $k,h \in K$ and distinct $a,b,c,d \in \Omega$ (as possible), we have:*

(1) $\big(k_a k_b^{-1}(a,b)\big)^{h_a h_b^{-1}(a,b)} = (hk^{-1}h)_a (hk^{-1}h)_b^{-1}(a,b)$;
(2) $\big(k_a k_b^{-1}(a,b)\big)^{h_b h_c^{-1}(b,c)} = (kh)_a (kh)_b^{-1}(a,c)$;
(3) $\big(k_a k_b^{-1}(a,b)\big)^{h_a h_b^{-1}(c,d)} = k_a k_b^{-1}(a,b)$.

PROOF. These are routine and direct calculations.

PROOF OF ZARA AND DORO'S THEOREM 1.1:

For $t,r \in T$, if $|\pi(t)\pi(r)| = 2$, then $\pi(t) = (a,b)$ and $\pi(r) = (c,d)$ for distinct $a,b,c,d \in \Omega$. Therefore $t^r = t$ by Proposition 2.4.3, so $|tr| = 2$.

If $|\pi(t)\pi(r)| = 3$, then there are $h,k \in K$ and distinct $a,b,c \in \Omega$ with $t = k_a k_b^{-1}(a,b)$ and $r = h_b h_c^{-1}(b,c)$. By Proposition 2.4.2, $t^r = (kh)_a (kh)_c^{-1}(a,c)$. Also by Proposition 2.4.2

$$r^t = \big((h^{-1})_c (h^{-1})_b^{-1}(c,b)\big)^{(k^{-1})_b (k^{-1})_a^{-1}(b,a)} = (h^{-1}k^{-1})_c (h^{-1}k^{-1})_a^{-1}(c,a)\,.$$

Therefore $r^t = (kh)_a (kh)_c^{-1}(a,c) = t^r$, so that $(tr)^3 = (trt)(rtr) = (r^t)(t^r) = 1$.

To find the order spectrum of T, it remains to calculate $|tr|$ when $\pi(t) = \pi(r)$. Suppose $t,r \in (a,b)^B$, say $t = (a,b)^f$ and $r = (a,b)^g$. Thus $|tr| = |(a,b)^f (a,b)^g| = |(a,b)^{fg^{-1}}(a,b)| = |(a,b)^h (a,b)|$ with $h = fg^{-1}$. If $(a,b)^h = m_a m_b^{-1}(a,b)$ then $|tr| = |m_a m_b^{-1}| = |m|$. Therefore the order spectrum is contained in the given set. On the other hand, for arbitrary $k \in K$, if we take $t = k_a k_b^{-1}(a,b)$ and $r = (a,b)$ then $|tr| = |k|$; and the order spectrum is equal to the given set.

For a group K and set Ω of size at least 2, consider the following

(2.5) PRESENTATION. *Let* $\mathrm{UWr}(K,\Omega)$ *be the group with presentation:*

Generators:

$\langle\!\langle k\,;\, a\,, b \rangle\!\rangle$ *for arbitrary $k \in K$ and distinct $a,b \in \Omega$;*

Relations:

for arbitrary $k,h \in K$ and distinct $a,b,c,d \in \Omega$ (as possible)

(1) $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle^2 = 1$;
(2) $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle = \langle\!\langle k^{-1}\,;\, b\,, a \rangle\!\rangle$;
(3) $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle^{\langle\!\langle h\,;\, a\,, b \rangle\!\rangle} = \langle\!\langle hk^{-1}h\,;\, a\,, b \rangle\!\rangle$;
(4) $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle^{\langle\!\langle h\,;\, b\,, c \rangle\!\rangle} = \langle\!\langle kh\,;\, a\,, c \rangle\!\rangle$;
(5) $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle^{\langle\!\langle h\,;\, c\,, d \rangle\!\rangle} = \langle\!\langle k\,;\, a\,, b \rangle\!\rangle$.

(2.6) THEOREM. *Let K be a group and Ω a set with $|\Omega| \geq 2$. The group $\mathrm{UWr}(K,\Omega)$ of Presentation 2.5 is isomorphic to the universal central extension $\mathrm{U}(\mathrm{Wr}(K,\Omega),T)$ of the augmented wreath product $\mathrm{Wr}(K,\Omega)$ relative to its set $T = \mathrm{T}(K,\Omega)$ of transpositions. In particular, we have $\langle\langle k\,;\,a\,,b\rangle\rangle = \langle\langle h\,;\,c\,,d\rangle\rangle$ in $\mathrm{UWr}(K,\Omega)$ if and only if either $h = k$, $c = a$, and $d = b$ or $h = k^{-1}$, $c = b$, and $d = a$.*

PROOF. For

$$t = k_a k_b^{-1}(a,b) = (k^{-1})_b (k^{-1})_a^{-1}(b,a) \in T$$

set

$$\tilde{t} = \langle\langle k\,;\,a\,,b\rangle\rangle = \langle\langle k^{-1}\,;\,b\,,a\rangle\rangle \in \mathrm{UT}(K,\Omega)$$

in accordance with relation (2.5.2). The elements $\tilde{t}$ have square 1 by relation (2.5.1), so by Proposition 2.4 the relations (2.5.3-5) are the transform table relations $\tilde{t}\tilde{r}\tilde{t} = \widetilde{trt}$ for the normal generating set T of $\mathrm{Wr}(K,\Omega)$, giving the theorem.

Because of the natural bijection with $\mathrm{T}(K,\Omega)$, we call the elements of the set $\mathrm{UT}(K,\Omega) = \{\, \langle\langle k\,;\,a\,,b\rangle\rangle \mid k \in K, a, b \in \Omega \,\}$ the *transpositions* of $\mathrm{UWr}(K,\Omega)$. This normal generating set is in bijection with $\mathrm{T}(K,\Omega)$. The map $\langle\langle k\,;\,a\,,b\rangle\rangle \mapsto (a,b)$ extends to the *projection* homomorphism $\pi^U\colon \mathrm{UWr}(K,\Omega) \longrightarrow \mathrm{FSym}(\Omega)$. The kernel $\mathrm{UB}(K,\Omega)$ of π^U is called the *base* subgroup of $\mathrm{UWr}(K,\Omega)$. If we let Z be the central kernel of the natural map from $\mathrm{UWr}(K,\Omega)$ to $\mathrm{Wr}(K,\Omega)$, then the natural projection $\pi\colon \mathrm{Wr}(B,\Omega) \longrightarrow \mathrm{FSym}(\Omega)$ factors through π^U since $Z \leq \mathrm{UB}(K,\Omega)$ and $\mathrm{UB}(K,\Omega)/Z = \mathrm{B}(K,\Omega)$.

(2.7) REMARK. For $|\Omega| \geq 3$, the relations (2.5.3) are redundant, being consequences of the relations (2.5.1), (2.5.2), and (2.5.4). Specifically, we have

$$\begin{aligned}
\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,a\,,b\rangle\rangle} &= \langle\langle k^{-1}\,;\,b\,,a\rangle\rangle^{\langle\langle h\,;\,a\,,b\rangle\rangle} \\
&= \big(\langle\langle k^{-1}\,;\,c\,,a\rangle\rangle\langle\langle 1\,;\,b\,,c\rangle\rangle\langle\langle k^{-1}\,;\,c\,,a\rangle\rangle\big)^{\langle\langle h\,;\,a\,,b\rangle\rangle} \\
&= \langle\langle k^{-1}\,;\,c\,,a\rangle\rangle^{\langle\langle h;\,a\,,b\rangle\rangle}\langle\langle 1\,;\,c\,,b\rangle\rangle^{\langle\langle h^{-1};\,b\,,a\rangle\rangle}\langle\langle k^{-1}\,;\,c\,,a\rangle\rangle^{\langle\langle h;\,a,b\rangle\rangle} \\
&= \langle\langle k^{-1}h\,;\,c\,,b\rangle\rangle\langle\langle h^{-1}\,;\,c\,,a\rangle\rangle\langle\langle k^{-1}h\,;\,c\,,b\rangle\rangle \\
&= \langle\langle k^{-1}h\,;\,c\,,b\rangle\rangle\langle\langle h\,;\,a\,,c\rangle\rangle\langle\langle k^{-1}h\,;\,c\,,b\rangle\rangle \\
&= \langle\langle h(k^{-1}h)\,;\,a\,,b\rangle\rangle\,.
\end{aligned}$$

3 A characterization of the full wreath product

We now look for sensible converses to Zara and Doro's Theorem 1.1. Thus throughout this section we will be concerned with the various forms of the

(3.1) HYPOTHESIS. *Let T be a normal set of involutions in the group $G = \langle T\rangle$; and let $\pi\colon G \longrightarrow \mathrm{FSym}(\Omega)$ be a homomorphism in which $\pi(T)$ is the transposition class of $\mathrm{FSym}(\Omega)$ with $|\Omega| \geq 3$. Assume additionally one of:*

(1) *T is a conjugacy class of G and, for all $t, r \in T$, if $\pi(t) \neq \pi(r)$, then $|\pi(t)\pi(r)| = |tr|$;*

(2) *for all $t, r \in T$, if $\pi(t) \neq \pi(r)$, then $|\pi(t)\pi(r)| = |tr|$;*

(3) *T is a conjugacy class of G and, for all $t, r \in T$, if $|\pi(t)\pi(r)| = 2$, then $|tr| = 2$;*

(4) *for all $t, r \in T$, if $|\pi(t)\pi(r)| = 2$, then $|tr| = 2$;*

(5) *T is a conjugacy class of G and, for all $t, r \in T$, if $|\pi(t)\pi(r)| = 3$, then $|tr| = 3$;*

(6) *for all $t, r \in T$, if $|\pi(t)\pi(r)| = 3$, then $|tr| = 3$.*

For $|\Omega| = 2$ the hypothesis would only say that G is an imperfect group generated by involutions (from a single class in 3.1.1, 3.1.3, and 3.1.5). There is little to be added in this case.

Under any version of the hypothesis and for Δ a subset of Ω, we let $G^\Delta = \langle\, t \in T \,|\, \pi(t) = (a, b), a, b \in \Delta \,\rangle$ and $G_\Delta = \langle\, t \in T \,|\, \pi(t) = (a, b), a, b \notin \Delta \,\rangle$. We shall frequently write $G^{a,b}$ for $G^{\{a,b\}} = \langle\, t \in T \,|\, \pi(t) = (a, b) \,\rangle$, G_a for $G_{\{a\}}$, and so forth.

(3.2) Lemma. *Under any version of Hypothesis 3.1, suppose $G^{a,b} \leq H = \langle T \cap H \rangle$ with $\pi(H)$ transitive on Ω. Then $H = G$.*

Proof. The image $\pi(H)$ is a transitive subgroup generated by transpositions and so is all $\mathrm{FSym}(\Omega)$. Thus H contains every $G^{x,y}$ and so all T.

The six hypotheses are not all distinct.

(3.3) Lemma. *Assume Hypothesis 3.1.2 or 3.1.6. Then the normal set T is in fact a conjugacy class, so we have Hypothesis 3.1.1 or 3.1.5 (respectively). We also have, for $t \in T$, that $tZ(G) \cap T = \{t\}$.*

Proof. For distinct $t, r \in T$, there is an s with $|\pi(t)\pi(s)| = |\pi(r)\pi(s)| = 3$. Therefore $|ts| = |rs| = 3$; so $\langle t, s\rangle \simeq \langle r, s\rangle \simeq \mathrm{Sym}(3)$, and t and r are conjugate to s and each other in $\langle t, r, s\rangle$. If $tr \in Z(G)$, then $\langle t, r, s\rangle = \langle tr\rangle \times \langle r, s\rangle = 2 \times \mathrm{Sym}(3)$, within which r and t are not conjugate.

By Theorem 1.1 and Proposition 2.1, the groups $\mathrm{Wr}(K, \Omega)$ and $\mathrm{UWr}(K, \Omega)$, for $|\Omega| \geq 3$, enjoy all versions of Hypothesis 3.1 and so any of the properties verified in this section. In particular we have:

(3.4) Corollary. *Let K be a group and Ω a set with $|\Omega| \geq 3$.*

(1) *The transposition class $T = \mathrm{T}(K, \Omega)$ of $K \wr_\Omega \mathrm{FSym}(\Omega)$ remains a conjugacy class in $\mathrm{Wr}(K, \Omega)$. For each $t \in T$ we have $T \cap tZ(\mathrm{Wr}(K, \Omega)) = \{t\}$.*

(2) *In the group $\mathrm{UWr}(K, \Omega)$ with Presentation 2.5 the set of transpositions $\mathrm{UT}(K, \Omega)$ is a conjugacy class. For each $t \in \mathrm{UT}(K, \Omega)$ we have $\mathrm{UT}(K, \Omega) \cap tZ(\mathrm{UWr}(K, \Omega)) = \{t\}$.*

(3) *For $Z \leq Z(\mathrm{UWr}(K, \Omega))$, we have $Z(\mathrm{UWr}(K, \Omega)/Z) = Z(\mathrm{UWr}(K, \Omega))/Z$.*

PROOF. Only (3) needs discussion. Let W be the preimage of the center $Z(\mathrm{UWr}(K,\Omega)/Z)$ in $\mathrm{UWr}(K,\Omega)$. Certainly $Z \leq Z(\mathrm{UWr}(K,\Omega)) \leq W$. Suppose for $t, r \in \mathrm{UT}(K,\Omega)$ that $tW = rW$. Then by Lemma 3.3 applied to $\mathrm{UWr}(K,\Omega)/Z$ we have $tZ = rZ$. Next by (2) we have $t = r$. That is, $\mathrm{UT}(K,\Omega) \cap tW = \{t\}$. The subgroup W therefore fixes each transposition of $\mathrm{UT}(K,\Omega)$ and so is central in $\langle \mathrm{UT}(K,\Omega) \rangle = \mathrm{UWr}(K,\Omega)$, as claimed.

REMARKS. (1) Parts (1) and (2) of the corollary can be false when $|\Omega| = 2$. For instance with $|K| = 2$ the group $2 \wr 2$ is dihedral of order 8, so $\mathrm{Wr}(2,2)$ is 2×2.

(2) We already know from Proposition 2.1 that there is a "largest" group generated by a class with the same transform table as $\mathrm{T}(K,\Omega)$, namely $\mathrm{UWr}(K,\Omega)$. The lemma and corollary tell us, for $|\Omega| \geq 3$, that $\mathrm{UWr}(K,\Omega)/Z(\mathrm{UWr}(K,\Omega))$ is the "smallest" such group. That is, for any G generated by a class of involutions having the same transform table as $\mathrm{T}(K,\Omega)$, we must have $G/Z(G)$ isomorphic to $\mathrm{UWr}(K,\Omega)/Z(\mathrm{UWr}(K,\Omega))$. This smallest group $\mathrm{UWr}(K,\Omega)/Z(\mathrm{UWr}(K,\Omega))$ is uniquely determined up to isomorphism as a group with trivial center and generated by a class of involutions with the same transform table as $\mathrm{T}(K,\Omega)$.

We leave Hypothesis 3.1.5 and the equivalent 3.1.6 for now and concentrate on the four Hypotheses 3.1.1-4, those under which products of order two are respected.

(3.5) LEMMA. *Assume that we have Hypothesis 3.1.4. For $\Delta \subseteq \Omega$, we have $[G_\Delta, G^\Delta] = 1$.*

PROOF. This is immediate.

We saw in Lemma 3.3 that Hypotheses 3.1.1 and 3.1.2 are equivalent to each other as are Hypotheses 3.1.5 and 3.1.6. Hypotheses 3.1.3 and 3.1.4 are not equivalent, as the following example demonstrates:

> Let E be a nontrivial elementary abelian 2-group generated by S. Then $E \times \mathrm{Wr}(K,\Omega)$ (for $|\Omega| \geq 3$) has generating set $S \times T = \{\, st \mid s \in S, t \in T \,\}$, where T is the transposition class of $\mathrm{Wr}(K,\Omega)$. The set $S \times T$ is a union of $|S|$ conjugacy classes (determined by the projection onto central S) and satisfies Hypothesis 3.1.4 (with $\pi(st) = \pi(t)$). Indeed, if $u, v \in S \times T$ with $|\pi(u)\pi(v)| = 3$, then $|uv|$ is 3 or 6 and $(uv)^3 \in E$.

For Hypotheses 3.1.3 and 3.1.4 to have teeth, we must additionally assume that $|\Omega| \geq 4$. The next result shows that in this case the example above is essentially all that separates Hypothesis 3.1.4, the weakest of Hypotheses 3.1.1-4, from the strongest, Hypothesis 3.1.1.

(3.6) PROPOSITION. *Assume we have Hypothesis 3.1.4 and $|\Omega| \geq 4$. Then G has a central elementary abelian 2-subgroup*

$$E = \{\, (tr)^3 \mid t, r \in T, |\pi(t)\pi(r)| = 3 \,\} = \{\, tr \mid t, r \in T, tr \in Z(G) \,\}$$

contained in $\ker\pi$ *and such that* G/E *satisfies Hypothesis 3.1.1 with respect to the conjugacy class* TE/E *and the induced homomorphism* $\pi_E\colon G/E \longrightarrow \mathrm{FSym}(\Omega)$.

PROOF. Let $a,b,c,d \in \Omega$ be distinct, and let $s,u \in T$ with $\pi(s) = (a,c)$ and $\pi(u) = (b,c)$. Then 3 divides $|su|$; and $e = (su)^3 = (sus)(usu) = xy$, where $x = sus$ and $y = usu$ are both in T with $\pi(x) = \pi(y) = (a,b)$. The element $e = xy$ is therefore in $G^{a,b}$ and is centralized by $G_{a,b}$ by Lemma 3.5. Also $e = (su)^3$ is in $\langle s,u\rangle$, a dihedral group, and so is inverted by s and u. Therefore $\langle e\rangle$ is normalized by $\langle s,u,G_{a,b}\rangle$. As $G_{a,b} \geq G^{c,d}$, this is G by Lemma 3.2. Indeed, since the normal subgroup $\langle e\rangle$ is centralized by $G^{c,d}$, whose normal closure is G, $\langle e\rangle$ is centralized by G. As e is now both inverted and centralized by s and u, it is a central element of order 1 or 2.

Let $E = \{\, (tr)^3 \mid t,r \in T, |\pi(t)\pi(r)| = 3 \,\}$. By the previous paragraph, E is a central elementary abelian 2-subgroup. As $|\Omega| \neq 2$, central E is contained in $\ker\pi$; and by construction G/E satisfies Hypothesis 3.1.2 with respect to TE/E and the induced homomorphism $\pi_E\colon G/E \longrightarrow \mathrm{FSym}(\Omega)$. By Lemma 3.3 the normal set TE/E is a single conjugacy class, and G/E satisfies Hypothesis 3.1.1.

We saw above that the central element e is xy with $x,y \in T$. Therefore $E \leq \{\, tr \mid t,r \in T, tr \in Z(G) \,\}$. On the other hand, suppose $t,r \in T$ with $tr = z \in Z(G)$. As $|\Omega| \neq 2$, $\pi(t)$ and $\pi(r)$ must be equal, say (a,c). Choose a $v \in T$ with $\pi(v) = (b,c)$. Replacing v by r^{vr} if necessary, we may assume that $|rv| = 3$. Then $z = (tv)^3 \in E$, so $E \geq \{\, tr \mid t,r \in T, tr \in Z(G) \,\}$.

(3.7) THEOREM. *Assume we have Hypothesis 3.1.1 and* $|\Omega| \geq 4$. *Then there is a group* K, *unique up to isomorphism, and a central subgroup* Z *of the group* $\mathrm{UWr}(K,\Omega)$ *with Presentation 2.5 such that*

(*i*) G *is isomorphic to* $\mathrm{UWr}(K,\Omega)/Z$;

(*ii*) *the isomorphism induces a bijection between the transposition class* $\mathrm{UT}(K,\Omega)$ *of* $\mathrm{UWr}(K,\Omega)$ *and the class* T *of* G;

(*iii*) $\ker\pi = \mathrm{UB}(K,\Omega)/Z$.

Before embarking upon our proof of the theorem, we observe that Theorem 1.2 is a direct consequence.

PROOF OF THEOREM 1.2:

By assumption we have a group G satisfying Hypothesis 3.1.1 with $|\Omega| \geq 4$. By Theorem 3.7 there is a group K and a central subgroup Z of $\mathrm{UWr}(K,\Omega)$ with G isomorphic to $\mathrm{UWr}(K,\Omega)/Z$, so by Corollary 3.4.3 the central quotient $G/Z(G)$ is isomorphic to $\mathrm{UWr}(K,\Omega)/Z(\mathrm{UWr}(K,\Omega))$. On the other hand, by Theorem 2.6 and Corollary 3.4.3 again we also have $\mathrm{Wr}(K,\Omega)/Z(\mathrm{Wr}(K,\Omega))$ isomorphic to $\mathrm{UWr}(K,\Omega)/Z(\mathrm{UWr}(K,\Omega))$. In particular the groups $G/Z(G)$ and $\mathrm{Wr}(K,\Omega)/Z(\mathrm{Wr}(K,\Omega))$ are isomorphic, which is the conclusion of Theorem 1.2.

We now pursue Theorem 3.7. For the balance of this section assume that we have a group G as in Hypothesis 3.1.1, with all the attendant assumptions and notation, and additionally that $|\Omega| \geq 4$. Set $B = \ker \pi$.

(3.8) LEMMA. *There is a subgroup $F \simeq \mathrm{FSym}(\Omega)$ with $G = B.F$, $F \cap B = 1$, and $T \cap F$ the transposition class of F.*

PROOF. Compare [15, Lemma 8.4]. Choose $\infty \in \Omega$ and for each transposition (∞, i) of $\pi(G) \simeq \mathrm{FSym}(\Omega)$ select an element $t_{i,\infty} \in T$ with $\pi(t_{\infty,i}) = (\infty, i)$. For all distinct $i, j \in \Omega$, set $t_{i,j} = t_{j,i} = t_{i,\infty}t_{j,\infty}t_{i,\infty} = t_{j,\infty}t_{i,\infty}t_{j,\infty}$, the last equality true by hypothesis as $(t_{i,\infty}t_{j,\infty})^3 = 1$.

The set $T_0 = \{\, t_{i,j} \mid i, j \in \Omega \,\}$ contains a unique element t_0 of each coset tB for $t \in T$, so $F = \langle T_0 \rangle$ supplements B in G.

For distinct $a, b, c \in \Omega \setminus \{\infty\}$, we have $\langle t_{\infty,a}, t_{\infty,b}, t_{\infty,c} \rangle = \langle t_{\infty,a}, t_{a,b}, t_{b,c} \rangle \simeq \mathrm{Sym}(4)$, since the second generating set satisfies the relations of the Weyl group $\mathrm{W}(A_3)$. If $|\Omega| = 4$, then this subgroup is F and splits the extension, as claimed.

For distinct $a, b, c, d \in \Omega \setminus \{\infty\}$, similarly we find $\langle t_{\infty,a}, t_{\infty,b}, t_{\infty,c}, t_{\infty,d} \rangle = \langle t_{\infty,a}, t_{a,b}, t_{b,c}, t_{c,d} \rangle \simeq \mathrm{W}(A_4) \simeq \mathrm{Sym}(5)$. This implies that T_0 is closed under conjugation and that the F-class $T_0 = T \cap F$ meets each coset tB, for $t \in T$, exactly once. In particular $F \cap B$, the kernel of the map $F \longrightarrow \mathrm{FSym}(\Omega)$, is central in F. Let z be an element of $F \cap B$. As T_0 generates F, there is a finite subset Δ of size $m \geq 3$ with $z \in F_1 = \langle\, t_{i,j} \mid i, j \in \Delta \,\rangle$. Arguing as before we see that F_1 has a generating set with the relations of $\mathrm{W}(A_{m-1}) \simeq \mathrm{Sym}(m)$ and so has trivial center. Therefore $z = 1$ and $F \cap B = 1$, completing the lemma.

The following is immediate for $|\Omega| \leq 3$ and otherwise comes from the lemma.

(3.9) COROLLARY. *The group $\mathrm{UWr}(1, \Omega)$ of Presentation 2.5 is isomorphic to $\mathrm{FSym}(\Omega)$ and is isomorphic to the subgroup $\langle\, \langle\!\langle 1\,;\, a\,, b \rangle\!\rangle \mid a, b \in \Omega \,\rangle$ of each group $\mathrm{UWr}(K, \Omega)$, giving a complement to the corresponding base subgroup.*

By the lemma we can and do identify F with $\mathrm{FSym}(\Omega)$. For distinct $a, b \in \Omega$, set $B^{a,b} = [B, (a, b)] \leq B \cap G^{a,b}$ and $B^a = \bigcap_{x \neq a} B^{a,x}$.

(3.10) LEMMA. *Let $a, b, c \in \Omega$ be distinct.*
(1) *$B^a = B^{a,b} \cap B^{a,c} = C_{B^{a,b}}(G_a)$.*
(2) *$T \cap (a, c)B = (a, c)^B = (a, c)^{B^{a,b}}$, and $B \cap G^{a,c} = B^{a,c}$.*
(3) *$\{\, t(a, b) \mid t \in T \cap (a, b)B \,\}$ is a set of coset representatives for B^b in $B^{a,b}$.*
(4) *$B^{a,b} \cap Z(G) = B^a \cap Z(G)$.*

PROOF. We have

$$\begin{aligned} B^a &\leq B^{a,b} \cap B^{a,c} \\ &\leq C_{B^{a,b}}(\langle G_{a,b}, G_{a,c} \rangle) = C_{B^{a,b}}(G_a) \\ &\leq \bigcap_{g \in G_a} (C_{B^{a,b}}(G_a))^g \leq \bigcap_{g \in G_a} (B^{a,b})^g = B^a\,, \end{aligned}$$

since $G_a = \langle G_{a,b}, G_{a,c}\rangle$ is transitive on $\Omega \setminus \{a\}$ (by Lemma 3.2 and $|\Omega| \geq 4$!). This gives (1).

For (2) and (3), we let $\Sigma = T \cap (a,c)B$ and consider the action of $B^{a,b}$ on Σ. For $r \in \Sigma$, $C_{B^{a,b}}(r) = C_{B^{a,b}}(\langle r, G_{a,b}\rangle) = C_{B^{a,b}}(G_b) = B^b$ by (1). So $B^{a,b}$ induces semiregular action on Σ with all stabilizers equal to B^b.

Let $r_1, r_2 \in \Sigma$. Set $u = r_1^{(a,b)} \in T \cap (b,c)B$ and $t = u^{r_2} \in T \cap (a,b)B$. Then $r_2^t = t^{r_2} = u = r_1^{(a,b)}$, hence $r_2^{t(a,b)} = r_1$ with $t(a,b) \in B \cap G^{a,b}$. In particular, $\Sigma = (a,c)^B$ and

$$B^{a,c}\langle(a,c)\rangle \leq (B \cap G^{a,c})\langle(a,c)\rangle = G^{a,c} = \langle\Sigma\rangle = [B,(a,c)]\langle(a,c)\rangle = B^{a,c}\langle(a,c)\rangle\,;$$

so $B \cap G^{a,c} = B^{a,c}$ and $B \cap G^{a,b} = B^{a,b}$ as well, giving (2).

We also know that $\{\, t(a,b) \mid t \in T \cap (a,b)B \,\}$ contains a set of coset representatives for B^b in $B^{a,b}$. Suppose $s(a,b)$ and $t(a,b)$ represent the same coset. Then st is in the stabilizer B^b and so is centralized by G_b. The subgroup $\langle st\rangle$ is also inverted by s and t. Therefore $\langle st\rangle$ is normal in $G = \langle t, G_b\rangle$. Since it is centralized by G_b, whose normal closure is all G, the element st is central in G. By Lemma 3.3 we have $t = s$. We conclude that $\{\, t(a,b) \mid t \in T \cap (a,b)B \,\}$ is a set of coset representatives for B^b in $B^{a,b}$ as in (3).

For (4) we have $B^a \leq B^{a,b}$, so certainly $B^a \cap Z(G) \leq B^{a,b} \cap Z(G)$. On the other hand $B^{a,b} \cap Z(G) \leq \bigcap_{g \in G_a} (B^{a,b})^g = B^a$.

(3.11) Corollary. *$B = [B, \mathrm{FSym}(\Omega)]$ and $G = [B, \mathrm{FSym}(\Omega)]\,\mathrm{FSym}(\Omega)$.*

Proof. The group $G/[B, \mathrm{FSym}(\Omega)]$ is a central quotient of $\mathrm{UWr}(1,\Omega)$ and so is $\mathrm{FSym}(\Omega)$ by Corollary 3.9. Thus $G = \langle T\rangle \leq [B, \mathrm{FSym}(\Omega)]\,\mathrm{FSym}(\Omega) \leq G$.

Set $K^{a,b} = B^{a,b}/B^b$. As $[B^{a,b}, G_{a,b}] = 1$, we have, for all $g \in \mathrm{FSym}(\Omega)$, that $(K^{a,b})^g = K^{ag,bg}$. Indeed, if we let K be an abstract group isomorphic to each $K^{a,b}$, then we can choose isomorphisms $K \longrightarrow K^{a,b}$ given by $k \mapsto k^{a,b}$ so that $(k^{a,b})^g = k^{ag,bg}$ for all $g \in \mathrm{FSym}(\Omega)$. The inverse isomorphism $K^{a,b} \longrightarrow K$ will be given by $h \mapsto h_{a,b}$. That is, $k = (k^{a,b})_{a,b}$ for $k \in K$.

We wish to show that the map

$$\mu\colon\ \mathrm{UT}(K,\Omega) \longrightarrow T \text{ given by } \mu\left(\langle\!\langle k\,;\, a\,, b\rangle\!\rangle\right) = t\,,$$

where

$$\pi(t) = (a,b) \text{ and } k = (t(a,b)B^b)_{a,b}\,,$$

is a well-defined bijection and extends to a homomorphism from $\mathrm{UWr}(K,\Omega)$ onto G with central kernel.

(3.12) Lemma. *The map μ is a well-defined bijection between the conjugacy class $\mathrm{UT}(K,\Omega)$ of $\mathrm{UWr}(K,\Omega)$ and the class T of G. Furthermore the map respects the relation (2.5.2); that is, $\mu(\langle\!\langle k\,;\, a\,, b\rangle\!\rangle) = \mu(\langle\!\langle k^{-1}\,;\, b\,, a\rangle\!\rangle)$ for all $k \in K$ and distinct $a, b \in \Omega$.*

PROOF. If $t \in T$ with $\pi(t) = (a, b)$, then $t(a, b)B^b$ is a coset of B^b in $B^{a,b}$ by Lemma 3.10.2 and so an element of $K^{a,b}$. Hence $(t(a, b)B^b)_{a,b}$ is an element of K as claimed. Therefore if the map μ is a well-defined injection, it is also a surjection and hence a bijection.

By Lemma 3.10.3, for each $k \in K$ and distinct $a, b \in \Omega$, there is a unique $t \in T$ with $\pi(t) = (a, b)$ and $(t(a, b)B^b)_{a,b} = k$. Therefore μ is well-defined at least as a map from the set of ordered triples $\{ (k, a, b) \in K \times \Omega \times \Omega \mid a \neq b \}$ to T. By Theorem 2.6 different triples (k, a, b) and (h, c, d) correspond to equal transpositions $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle = \langle\!\langle h\,;\, c\,, d \rangle\!\rangle$ if and only if $h = k^{-1}$, $c = b$, and $d = a$. Suppose $\mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle) = t$. Then $\pi(t) = (a, b) = (b, a)$ and

$$\begin{aligned} k &= (t(a, b)B^b)_{a,b} \\ k^{a,b} &= t(a, b)B^b \\ (k^{-1})^{a,b} &= (a, b)tB^b \\ (k^{-1})^{b,a} &= (a, b)\left((a, b)tB^b\right)(a, b) = t(b, a)B^a \\ k^{-1} &= (t(b, a)B^a)_{b,a}\,. \end{aligned}$$

Therefore $t = \mu(\langle\!\langle k^{-1}\,;\, b\,, a \rangle\!\rangle)$ as well, and μ is indeed well-defined on $\mathrm{UT}(K, \Omega)$. Additionally, we see that relation (2.5.2) is respected: $\mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle) = t = \mu(\langle\!\langle k^{-1}\,;\, b\,, a \rangle\!\rangle)$ for all appropriate k, a, b.

Finally, suppose that $\mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle) = \mu(\langle\!\langle h\,;\, c\,, d \rangle\!\rangle) = t$, say. Then $(a, b) = \pi(t) = (c, d)$. Hence either $a = c$ and $b = d$ or $a = d$ and $b = c$. In the first case we have $h = (t(c, d)B^d)_{c,d} = (t(a, b)B^b)_{a,b} = k$ and in the second case $h = (t(c, d)B^d)_{c,d} = (t(b, a)B^a)_{b,a} = k^{-1}$, as above. In either case $\langle\!\langle k\,;\, a\,, b \rangle\!\rangle = \langle\!\langle h\,;\, c\,, d \rangle\!\rangle$; so μ is injective, as desired.

(3.13) LEMMA. *The map μ respects the relations (2.5.1) and (2.5.5).*

PROOF. The members of $\mathrm{UT}(K, \Omega)$ and T are all involutions, so (2.5.1) is respected.

Suppose $\mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle) = t$ and $\mu(\langle\!\langle h\,;\, c\,, d \rangle\!\rangle) = r$ with a, b, c, d distinct. Then $|\pi(t)\pi(r)| = |(a, b)(c, d)| = 2 = |tr|$ by Hypothesis 3.1.1. That is,

$$\mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle)^{\mu(\langle\!\langle h\,;\, c\,, d \rangle\!\rangle)} = t^r = t = \mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle)\,,$$

as required for relation (2.5.5).

(3.14) LEMMA. *The map μ respects the relation (2.5.4).*

PROOF. For distinct $a, b, c \in \Omega$, let $t = \mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle)$ and $r = \mu(\langle\!\langle h\,;\, b\,, c \rangle\!\rangle)$ so that $t^r = \mu(\langle\!\langle g\,;\, a\,, c \rangle\!\rangle)$ To prove the lemma we must verify

$$\mu(\langle\!\langle k\,;\, a\,, b \rangle\!\rangle)^{\mu(\langle\!\langle h\,;\, b\,, c \rangle\!\rangle)} = \mu(\langle\!\langle kh\,;\, a\,, c \rangle\!\rangle)\,.$$

That is, we must prove $kh = g$, where $k = (t(a, b)B^b)_{a,b}$, $h = (r(b, c)B^c)_{b,c}$, and $g = (rtr(a, c)B^c)_{a,c}$.

We have $k^{a,b} = t(a,b)B^b$ and $h^{b,c} = r(b,c)B^c$, so

$$\begin{aligned}(kh)^{a,c} &= k^{a,c}h^{a,c} = (k^{a,b})^{(b,c)}(h^{b,c})^{(a,b)} \\ &= (b,c)t(a,b)B^b(b,c)(a,b)r(b,c)B^c(a,b) \\ &= (b,c)t(a,b)(b,c)(a,b)r(b,c)(a,b)B^c \\ &= (b,c)t(a,c)r(a,b)(a,c)B^c\,.\end{aligned}$$

What needs to be verified is then

$$(b,c)t(a,c)r(a,b)(a,c)B^c = rtr(a,c)B^c$$

or equivalently

$$rtr(b,c)t(a,c)r(a,b) \in B^a\,.$$

Although this could be checked directly, it seems easier (and perhaps more enlightening) to take a different approach. (Compare [15, Lemma 8.6].)

Set $H = G^{a,b,c} = (B \cap H).\mathrm{Sym}(\{a,b,c\})$. As $B^{a,b} = [B,(a,b)]$, the element (a,b) of G normalizes $B^{a,b}B^{b,c} = B^{a,b}B^{b,c}B^{a,c}$. Therefore by Lemma 3.10.2 we have $B \cap H = B^{a,b}B^{b,c}$. Let

$$K_a = (B \cap H)/B^{b,c}, \quad K_b = (B \cap H)/B^{a,c}, \quad K_c = (B \cap H)/B^{a,b}\,.$$

Then, for $\{x,y,z\} = \{a,b,c\}$,

$$K_x = (B \cap H)/B^{y,z} = B^{x,y}B^{y,z}/B^{y,z} \simeq B^{x,y}/B^{x,y} \cap B^{y,z} = B^{x,y}/B^y \simeq K\,.$$

By design (x,y) is trivial on K_z and switches K_x and K_y, so

$$(K_a \times K_b \times K_c).\mathrm{Sym}(\{a,b,c\}) = K \wr_{\{a,b,c\}} \mathrm{Sym}(\{a,b,c\})\,.$$

Consider the map $H \longrightarrow K \wr_{\{a,b,c\}} \mathrm{Sym}(\{a,b,c\})$ given by $h = v\sigma \mapsto \bar{h} = \bar{v}\sigma$, where $\sigma \in \mathrm{Sym}(\{a,b,c\})$ and $v \in B \cap H$ has image $\bar{v} = (vB^{b,c})_a(vB^{a,c})_b(vB^{a,b})_c$. By the Chinese Remainder Theorem, this map is a homomorphism with kernel $B^{b,c} \cap B^{a,c} \cap B^{a,b} \leq B^a$. So what remains is to check that the image of the element $rtr(b,c)t(a,c)r(a,b)$ is in the image of B^a.

By Lemma 2.2 there are $m,n \in K$ with $\bar{t} = m_a m_b^{-1}(a,b)$ and $\bar{r} = n_b n_c^{-1}(b,c)$. We now easily calculate

$$\bar{r}\bar{t}\bar{r}(b,c)\bar{t}(a,c)\bar{r}(a,b) = (mnm^{-1}n^{-1})_a\,.$$

Therefore $rtr(b,c)t(a,c)r(a,b) \in B^{a,c} \cap B^{a,b} = B^a$, as desired.

(3.15) Lemma. *The map μ respects the relation (2.5.3).*

Proof. This can be calculated directly as in Lemma 3.12, verified within the wreath product subgroup H of Lemma 3.14, or deduced from relations (2.5.1), (2.5.2), and (2.5.4) as in Remark 2.7.

Proof of Theorem 3.7:

The group $\mathrm{UWr}(K,\Omega)$ is its own universal central extension relative to the class $\mathrm{UT}(K,\Omega)$. Therefore, by Proposition 2.1 and Lemmas 3.12 through 3.15, the bijection μ between $\mathrm{UT}(K,\Omega)$ and T extends to a homomorphism (also μ) from $\mathrm{UWr}(K,\Omega)$ to G whose kernel Z is central in $\mathrm{UWr}(K,\Omega)$.

By Lemma 3.10 and Corollary 3.11,

$$\begin{aligned}\ker\pi &= B = \langle\, B^{a,b} \mid a,b \in \Omega \,\rangle \\ &= \langle\, tr \mid t,r \in (a,b)^B, a,b \in \Omega \,\rangle \\ &= \langle\, \mu(\langle\!\langle k\,;\, a\,, b\rangle\!\rangle)\mu(\langle\!\langle h\,;\, a\,, b\rangle\!\rangle) \mid k,h \in K, a,b \in \Omega \,\rangle \\ &= \mu(\mathrm{UB}(K,\Omega))\,.\end{aligned}$$

Suppose K_0 is a group and Z_0 a central subgroup of $\mathrm{UWr}(K_0,\Omega)$ for which we have (i)-(iii) of the theorem. By Lemma 3.10.1 our group K was chosen to be isomorphic to

$$B^{a,b}/B^b = [\ker\pi,(a,b)]/[\ker\pi,(a,b)] \cap [\ker\pi,(b,c)]\,,$$

and by Lemma 3.10.4 this calculation is not affected by central elements. This observation and Corollary 2.3 give

$$\begin{aligned}K &\simeq [\mathrm{B}(K,\Omega),(a,b)]/[\mathrm{B}(K,\Omega),(a,b)] \cap [\mathrm{B}(K,\Omega),(b,c)] \\ &\simeq [\mathrm{UB}(K,\Omega),(a,b)]/[\mathrm{UB}(K,\Omega),(a,b)] \cap [\mathrm{UB}(K,\Omega),(b,c)] \\ &\simeq B^{a,b}/B^b \\ &\simeq [\mathrm{UB}(K_0,\Omega),(a,b)]/[\mathrm{UB}(K_0,\Omega),(a,b)] \cap [\mathrm{UB}(K_0,\Omega),(b,c)] \\ &\simeq [\mathrm{B}(K_0,\Omega),(a,b)]/[\mathrm{B}(K_0,\Omega),(a,b)] \cap [\mathrm{B}(K_0,\Omega),(b,c)] \\ &\simeq K_0\,.\end{aligned}$$

Therefore K is uniquely determined up to isomorphism, and the proof of the theorem is complete.

4 Respecting three

We return to Hypothesis 3.1.5 and the equivalent 3.1.6, those hypotheses under which products of order three are respected. Although we can no longer force things to commute, Hypothesis 3.1.5 is still strong, as we have seen in Remark 2.7. If t and r are distinct involutions, then the following three statements are equivalent

(i) $|tr| = 3$;

(ii) $\langle t,r\rangle \simeq \mathrm{Sym}(3)$;

(iii) $t^r = r^t$.

Which form is most helpful will depend upon the situation.

4.1 Moufang loops

Most of our discussion has focused on situations described by the data (G, T, π_Ω), where T is a conjugacy class of involutions in the group $G = \langle T \rangle$ and $\pi_\Omega = \pi$ is a homomorphism $\pi\colon G \longrightarrow \mathrm{FSym}(\Omega)$ for which $\pi(T)$ is the transposition class of $\mathrm{FSym}(\Omega)$. Theorem 3.7 can then be thought of as saying that, provided $|\Omega| \geq 4$, the following two statements are equivalent:

> $(*)$ *For all* $t, r \in T$, *if* $\pi(t) \neq \pi(r)$, *then* $|\pi(t)\pi(r)| = |tr|$.
>
> $(**)$ *There is a group* K *(unique up to isomorphism) and a central subgroup* Z *of the group* $\mathrm{UWr}(K, \Omega)$ *with Presentation 2.5 such that*
>
> > (i) G *is isomorphic to* $\mathrm{UWr}(K, \Omega)/Z$;
> > (ii) *the isomorphism induces a bijection between the transposition class* $\mathrm{UT}(K, \Omega)$ *of* $\mathrm{UWr}(K, \Omega)$ *and the class* T *of* G, *both of cardinality* $3|K|$;
> > (iii) $\ker \pi = \mathrm{UB}(K, \Omega)/Z$.

We have already remarked that $(*)$ is nearly useless for $|\Omega| = 2$. For $|\Omega| = 3$, the groups and triples (G, T, π_3) satisfying $(*)$ have in fact been studied extensively, starting with Glauberman [13] and Doro [6], under the name of *groups with triality* (or *triality groups*); see [11, 12, 16, 20], for instance. Such groups need not arise from wreath products, Cartan's triality groups $\mathrm{P}\Omega_8^+(\mathbb{F})\colon \mathrm{Sym}(3)$, for $\mathbb{F}$ a field, furnishing the canonical examples (and the name) of groups with triality. This makes it all the more surprising that something very close to Theorem 3.7 remains true.

(4.1) Theorem. *Let* T *be a conjugacy class of involutions in the group* $G = \langle T \rangle$. *Furthermore let* $\pi_3\colon G \longrightarrow \mathrm{Sym}(3)$ *be a homomorphism in which* $\pi_3(T)$ *is the transposition class of* $\mathrm{Sym}(3)$. *Then the following two statements are equivalent:*

> $(*)$ *For all* $t, r \in T$, *if* $\pi_3(t) \neq \pi_3(r)$, *then* $|\pi_3(t)\pi_3(r)| = |tr|$.
>
> $(***)$ *There is a loop* L *(unique up to isotopy) with the Moufang Property and a central subgroup* Z *of the group* $\mathrm{UWr}(L, 3)$ *with Presentation 2.5 such that*
>
> > (i) G *is isomorphic to* $\mathrm{UWr}(L, 3)/Z$;
> > (ii) *the isomorphism induces a bijection between the transposition class* $\mathrm{UT}(L, 3)$ *of* $\mathrm{UWr}(L, 3)$ *and the class* T *of* G, *both of cardinality* $3|L|$;
> > (iii) $\ker \pi_3 = \mathrm{UB}(L, 3)/Z$.

Results near or equivalent to this can be found in all the above references (for instance, [16, Theorem 3.6]), so we do not give a proof. A few remarks are appropriate.

A loop is a "not necessarily associative group." That is, L is a loop if it has a binary multiplication with an identity element and furthermore right

multiplication by any fixed element is a permutation of L as is left multiplication by that element. A *Moufang loop* is a loop that satisfies a weak form of the associative law called the *Moufang Property*: $(a(bc))a = (ab)(ca)$, for all $a, b, c \in L$. In particular a group is a Moufang loop, and it was in this context that Doro [6, p. 385] noted that wreath products of groups with Sym(3) produce groups with triality. (Equivalently, wreath products respect transposition products of order 3—Doro's contribution to the Zara-Doro Theorem 1.1.)

Two loops L and M are *isotopic* if there are bijections α, β, γ from L to M with $a^\alpha b^\beta = (ab)^\gamma$, for all $a, b \in L$. Few results on loops are needed for our arguments. One is this pleasant exercise: a loop isotopic to the group G is, in fact, a group isomorphic to G (which explains why isotopy is not a concept discussed in group theory; see [3, (i), p. 57] and [17, Corollary III.2.3]). Also we need to know that in Moufang loops right inverses and left inverses are equal: $xy = 1$ if and only if $yx = 1$, in which case we write $y = x^{-1}$. This is part of Theorem 4.1, or see [3, Lemma VII.3.1] and [17, I.4.2, IV.1.4].

As before $\mathrm{UWr}(L, 3)$ is a universal central extension relative to the involution class $\mathrm{UT}(L, 3)$. The above remarks about inverses show that (2.5.2) is unambiguous. Since $|\Omega| = 3$, relation (2.5.5) is not relevant for Theorem 4.1. The loop L might not be associative, so relation (2.5.3) needs discussion. For the purposes of Theorem 4.1, this relation should be written

$$\langle\!\langle k\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle h\,;\, a\,, b\rangle\!\rangle} = \langle\!\langle h(k^{-1}h)\,;\, a\,, b\rangle\!\rangle$$

and remains, as in Remark 2.7, a consequence of relations (2.5.1), (2.5.2), and (2.5.4).

We view Theorem 4.1 as saying the any group G with triality can be "coordinatized" by the Moufang loop L via the bijection $\mu(\langle\!\langle k\,;\, a\,, b\rangle\!\rangle) = t$ of (ii). Furthermore, any loop L that coordinatizes G as in Presentation 2.5 must be a Moufang loop and isotopic to L. Conversely, any Moufang loop coordinatizes a group with triality, and all triality groups that it coordinatizes are central quotients of a fixed relative universal central extension.

There are many Moufang loops that are not groups, but easily described families of examples are hard to come by. All octonian algebras satisfy the Moufang Property [18, 1.4.1], so their loops of units are Moufang loops. In particular, the norm 1 split octonians over $\mathbb{F}$ give rise to the triality group $\mathrm{P}\Omega_8^+(\mathbb{F}) : \mathrm{Sym}(3)$.

Another easily described class of Moufang loops was given by Chein.

(4.2) THEOREM. **(Chein [4, Theorem 1])** *Let L be a Moufang loop in which the subloop L_0 generated by all elements of order not 2 is a proper subloop. Then there is a subgroup H containing L_0 and an element x of order 2 in $L \setminus H$ such that each element of L may be uniquely expressed in the form hx^a, where $h \in H$, $a = 0, 1$; and the product of elements of L is given by*

$$(h_1 x^d)(h_2 x^e) = (h_1^n h_2^m)^n x^{d+e}$$

where $n = (-1)^e$ and $m = (-1)^{d+e}$.

Conversely, given any group H, the loop L constructed as above is a Moufang loop. The loop L is a group if and only if the group H is abelian.

Chein's proof is short and elementary (but somewhat messy). For the characterization of the first paragraph he uses a hypothesis that is slightly stronger than $L_0 < L$. The two hypotheses are equivalent for finite loops, the case of interest to Chein.

Chein's loops can be thought of as "generalized dihedral" loops, since every element outside the subgroup H is an element of order 2 that inverts each element of h by conjugation. The group case is very elementary (and versions can be found as exercises in various texts).

(4.3) LEMMA. (1) *Let H be a group and $L = H \cup Hx$ a loop with multiplication given by*

$$(h_1 x^d)(h_2 x^e) = (h_1^n h_2^m)^n x^{(d+e \bmod 2)}$$

where $d = 0, 1$, $n = (-1)^e$ and $m = (-1)^{d+e}$. Then the loop L is a group if and only if the group H is abelian and conjugation by x inverts each element of H.

(2) *Let L be a group in which the subgroup L_0 generated by all elements of order not 2 is proper. Then there is an abelian subgroup H containing L_0 and an element x of order 2 in $L \setminus H$ such that L is the semidirect product of H by $\langle x \rangle$ with x inverting each element of H by conjugacy.*

PROOF. (1) Assume L is a group. Then $h_1 = 1$ and $d = e = 1$ gives $x^2 = 1$ when $h_2 = 1$ and in general gives $x^{-1} h_2 x = x h_2 x = h_2^{-1}$. Thus x inverts abelian H, as claimed.

Conversely, if H is an abelian group and x an element of order 2 that inverts H, then in the semidirect product $H \rtimes \langle x \rangle$ we find $(h_1 x^d)(h_2 x^e) = (h_1^n h_2^m)^n x^{d+e}$ (as is easily checked). Thus the loop L is isomorphic to the semidirect product group $H \rtimes \langle x \rangle$.

(2) Let H_0 be any subgroup with $L > H_0 \geq L_0$. Then, for arbitrary $h \in H_0$ and $x \in L \setminus H$, the element h is the product of the two involutions x and xh and so is inverted by x in the dihedral subgroup they generate. Therefore if $H = L_0 C_L(L_0)$ is proper in L, then any choice of x in $L \setminus H$ works. On the other hand if $L = L_0 C_L(L_0)$, then with $H_0 = L_0$ any choice of $x \in C_L(L_0) \setminus L_0$ reveals L to be an elementary abelian 2-group, and H can be chosen as maximal subject to $x \notin H$.

We wish to put Chein's construction and result into the context of the present paper. Aside from Theorem 4.1, almost everything in this section comes from the trivial but crucial observation that

> *there is a homomorphism from* $\mathrm{Sym}(4)$ *onto* $\mathrm{Sym}(3)$ *that takes transpositions to transpositions. Therefore, for any group H, the augmented wreath product* $\mathrm{Wr}(H, 4)$ *has* $\mathrm{Sym}(3)$ *as an image, and so* $\mathrm{Wr}(H, 4)$ *is a group with triality.*

To make this precise, choose the homomorphism $\rho\colon \mathrm{Sym}(4) \longrightarrow \mathrm{Sym}(3)$ so that $\rho((a,b)) = \rho((c,4)) = (a,b)$, for $\{a,b,c\} = \{1,2,3\}$. Let $\mathrm{Wr}(H,4)$ have transposition class T and projection π_4 from $\mathrm{Wr}(H,4)$ to $\mathrm{Sym}(4)$. Then $\pi_3 = \rho\pi_4$ maps $\mathrm{Wr}(H,4)$ onto $\mathrm{Sym}(3)$ taking T to transpositions. By the Zara-Doro Theorem 1.1 all transposition products of order 3 in $\mathrm{Sym}(4)$ are respected by $\mathrm{Wr}(H,4)$ and π_4, and this carries over to π_3 and its image $\mathrm{Sym}(3)$. That is, $(\mathrm{Wr}(H,4), T, \pi_3)$ is a group with triality.

By Theorem 4.1 the triality group $(\mathrm{Wr}(H,4), T, \pi_3)$ is coordinatized by some Moufang loop L. As we see next, this is precisely Chein's generalized dihedral loop from Theorem 4.2.

(4.4) THEOREM. *Let H be a group, and let $T = \mathrm{UT}(H,4)$ be the transposition class of the group $\mathrm{UWr}(H,4)$ whose projection map onto $\mathrm{Sym}(4)$ is π_4^U.*

For x a new symbol, set $Hx = \{\, hx \mid h \in H \,\}$ and $L = H \cup Hx$. We give new names to the members of the transposition class T:

$$\text{for } \{a,b,c\} = \{1,2,3\} \text{ set } \quad \begin{cases} [h\,;\,a\,,b\,] = \langle\!\langle h\,;\,a\,,b\rangle\!\rangle \\ [hx\,;\,a\,,b\,] = \langle\!\langle h\,;\,4\,,c\rangle\!\rangle \end{cases} .$$

Define the multiplication $\circ\colon L \times L \longrightarrow L$ by

$$[k\,;\,1\,,2\,]^{[j\,;\,2\,,3\,]} = [\,k \circ j\,;\,1\,,3\,]$$

for all $k, j \in L$.

Then $L = (L, \circ)$ is a Moufang loop that coordinatizes the triality group $(\mathrm{UWr}(H,4), T, \pi_3^U)$ (where $\pi_3^U = \rho\pi_4^U$) in the sense that $\langle\!\langle k\,;\,a\,,b\rangle\!\rangle \mapsto [\,k\,;\,a\,,b\,]$ is an isomorphism of the group $\mathrm{UWr}(L,3)$ of Theorem 4.1 with $\mathrm{UWr}(H,4)$.

Furthermore, H is naturally embedded as a subgroup of L; all the elements of the coset Hx have order 2; and the multiplication is that of the Chein generalized dihedral loop:

$$(h_1 x^d) \circ (h_2 x^e) = (h_1^n h_2^m)^n x^{(d+e \bmod 2)}$$

where $d = 0, 1$, $n = (-1)^e$ and $m = (-1)^{d+e}$.

PROOF. We always have $\pi_4([\,k\,;\,a\,,b\,])$ equal to (a,b) or $(4,c)$ (for $\{a,b,c\} = \{1,2,3\}$). Thus $\pi_4\left([\,k\,;\,a\,,b\,]^{[j\,;\,b\,,c\,]}\right)$ is (a,c) or $(4,b)$, and $\pi_3\left([\,k\,;\,a\,,b\,]^{[j\,;\,b\,,c\,]}\right)$ is (a,c). We conclude that $[\,k\,;\,a\,,b\,]^{[j\,;\,b\,,c\,]} = [\,m\,;\,a\,,c\,]$, for some $m \in L$. Especially, $\circ$ is well-defined.

Since, for $h \in H$,

$$\begin{aligned} [1\,;\,1\,,2\,]^{[hx\,;\,2\,,3\,]} &= \langle\!\langle 1\,;\,1\,,2\rangle\!\rangle^{\langle\!\langle h\,;\,4\,,1\rangle\!\rangle} = \langle\!\langle 1\,;\,2\,,1\rangle\!\rangle^{\langle\!\langle h^{-1}\,;\,1\,,4\rangle\!\rangle} \\ &= \langle\!\langle h^{-1}\,;\,2\,,4\rangle\!\rangle = \langle\!\langle h\,;\,4\,,2\rangle\!\rangle = [hx\,;\,1\,,3\,], \end{aligned}$$

always $1 \circ hx = hx$; and the identity element 1 of H is a left identity element for $(L, \circ)$. Similarly 1 is a right identity and so an identity element.

We have $[\,k\,;\,1\,,2\,]^{[j\,;\,2\,,3\,]} = [kj\,;\,1\,,3\,] = [kj\,;\,1\,,2\,]^{[1\,;\,2\,,3\,]}$, whence

$$[\,k\,;\,1\,,2\,]^{[j\,;\,2\,,3\,][1\,;\,2\,,3\,]} = [kj\,;\,1\,,2\,];$$

so right multiplication by the element j is a permutation of L and similarly for left multiplication. We conclude that the operation $\circ$ gives the set L the structure of a loop.

We now must show that the symbols $[*\,;*\,,*\,]$ admit the relations (2.5.1), (2.5.2), and (2.5.4). (Relation (2.5.5) is empty since $|\Omega| = 3$, and again (2.5.3) is a consequence of the other relations as in Remark 2.7.)

All the elements of T have order 2, so (2.5.1) holds. Also, for $h \in H$, we have $[h\,;a\,,b\,] = \langle\!\langle h\,;a\,,b\rangle\!\rangle = \langle\!\langle h^{-1}\,;b\,,a\rangle\!\rangle = [h^{-1}\,;b\,,a\,]$; so at least in this case we have (2.5.2). By definition $[hx\,;a\,,b\,] = [hx\,;b\,,a\,] = \langle\!\langle h\,;4\,,c\rangle\!\rangle$, so to complete (2.5.2) we need to show that $hx \circ hx = 1$ always (as claimed). But

$$\begin{aligned}[hx \circ hx\,;1\,,3\,] &= [hx\,;1\,,2\,]^{[hx\,;2\,,3\,]} \\ &= \langle\!\langle h\,;4\,,3\rangle\!\rangle^{\langle\!\langle h\,;4\,,1\rangle\!\rangle} = \langle\!\langle h^{-1}\,;3\,,4\rangle\!\rangle^{\langle\!\langle h\,;4\,,1\rangle\!\rangle} \\ &= \langle\!\langle 1\,;3\,,1\rangle\!\rangle = \langle\!\langle 1\,;1\,,3\rangle\!\rangle = [1\,;1\,,3\,]\,,\end{aligned}$$

as desired. This also shows that right inverses are left inverses in $(L, \circ)$.

For relation (2.5.3), we have already shown that $[k\,;a\,,b\,]^{[j\,;b\,,c\,]} = [m\,;a\,,c\,]$, for some $m \in L$; so it remains to prove $k \circ j = m$. We have the special case

$$[hx\,;a\,,b\,]^{[1\,;b\,,c\,]} = [hx\,;a\,,b\,]^{(b,c)} = \langle\!\langle h\,;4\,,c\rangle\!\rangle^{(b,c)} = \langle\!\langle h\,;4\,,b\rangle\!\rangle = [hx\,;a\,,c\,]\,,$$

for $h \in H$, and similarly $[hx\,;a\,,b\,]^{[1\,;a\,,c\,]} = [hx\,;c\,,b\,]$. Therefore in general $[k\,;a\,,b\,]^{(b,c)} = [k\,;a\,,c\,]$ and $[k\,;a\,,b\,]^{(a,c)} = [k\,;c\,,b\,]$. We conclude that, for arbitrary $\sigma \in \mathrm{Sym}(3) = \langle (a,c), (b,c)\rangle$, always $[k\,;a\,,b\,]^{\sigma} = [k\,;a^{\sigma}\,,b^{\sigma}\,]$.

Let σ be the element of $\mathrm{Sym}(3)$ given by $a \mapsto 1$, $b \mapsto 2$, and $c \mapsto 3$. Then by the previous paragraph

$$\begin{aligned}[k\,;1\,,2\,]^{[j\,;2\,,3\,]} &= ([k\,;a\,,b\,]^{\sigma})^{[j\,;b\,,c\,]^{\sigma}} \\ &= \Big([k\,;a\,,b\,]^{[j\,;b\,,c\,]}\Big)^{\sigma} = [m\,;a\,,c\,]^{\sigma} = [m\,;1\,,3\,]\,,\end{aligned}$$

By the definition of $\circ$, we thus have $k \circ j = m$ and have finished our check of relation (2.5.3).

We therefore have found a bijection $\langle\!\langle k\,;a\,,b\rangle\!\rangle \mapsto [k\,;a\,,b\,]$ from the class $\mathrm{UT}(L,3)$ of $\mathrm{UWr}(L,3)$ to the class $T = \mathrm{UT}(H,4)$ of $\mathrm{UWr}(H,4)$ and have verified that, via this bijection, the two classes have the same transform table. Since each group is the universal central extension relative to its chosen class, we conclude that this bijection extends to an isomorphism of the two groups $\mathrm{UWr}(L,3)$ and $\mathrm{UWr}(H,4)$. Additionally we see that this isomorphism relates the two projections maps by $\pi_3^U = \rho\pi_4^U$. Also note that by Theorem 4.1 the loop L is a Moufang loop. (The Moufang property could also be checked directly thus rendering the present theorem independent of Theorem 4.1.)

For $h \in H$, we always have $[h\,;a\,,b\,] = \langle\!\langle h\,;a\,,b\rangle\!\rangle$; so $h_1 \circ h_2 = h_1 h_2$, and the group H is naturally embedded in the loop L, as claimed. We have already seen that the coset Hx consists of elements of order 2 in L. It remains to check

Chein's multiplication, which is summerized in the following table:

$\circ$	h_2	h_2x
h_1	h_1h_2	$(h_2h_1)x$
h_1x	$(h_1h_2^{-1})x$	$h_2^{-1}h_1$

.

We have already observed $h_1 \circ h_2 = h_1h_2$. We have $h_1 \circ h_2x = (h_2h_1)x$ since

$$\begin{aligned}
[h_1\,;\,1\,,2\,]^{[h_2x\,;\,2\,,3\,]} &= \langle\!\langle h_1\,;\,1\,,2\rangle\!\rangle^{\langle\!\langle h_2\,;\,4\,,1\rangle\!\rangle} = \langle\!\langle h_1^{-1}\,;\,2\,,1\rangle\!\rangle^{\langle\!\langle h_2^{-1}\,;\,1\,,4\rangle\!\rangle} \\
&= \langle\!\langle h_1^{-1}h_2^{-1}\,;\,2\,,4\rangle\!\rangle = \langle\!\langle h_2h_1\,;\,4\,,2\rangle\!\rangle \\
&= [(h_2h_1)x\,;\,1\,,3\,]\,,
\end{aligned}$$

and the other entries in the table are easily verified in the same way.

When H is a subloop of L, we write $\langle\!\langle h\,;\,a\,,b\rangle\!\rangle_H$ and $\langle\!\langle h\,;\,a\,,b\rangle\!\rangle_L$ to distinguish between $\langle\!\langle h\,;\,a\,,b\rangle\!\rangle$ as an element of $\mathrm{UWr}(H,3)$ and of $\mathrm{UWr}(L,3)$.

(4.5) Lemma. (1) *Let H be a subloop of L. Then the natural injection $\mathrm{UT}(H,3) \longrightarrow \mathrm{UT}(L,3)$ given by $\langle\!\langle h\,;\,a\,,b\rangle\!\rangle_H \mapsto \langle\!\langle h\,;\,a\,,b\rangle\!\rangle_L$ extends to a homomorphism from $\mathrm{UWr}(H,3)$ onto $\langle\, \langle\!\langle h\,;\,a\,,b\rangle\!\rangle_L \,|\, h \in H \,\rangle \leq \mathrm{UWr}(L,3)$ with central kernel.*

(2) *If the subgroup $G = \langle G \cap \mathrm{UT}(L,3)\rangle$ of $\mathrm{UWr}(L,3)$ contains $\mathrm{Sym}(3) = \langle \langle\!\langle 1\,;\,1\,,2\rangle\!\rangle, \langle\!\langle 1\,;\,2\,,3\rangle\!\rangle \rangle$, then there is a subloop H of L such that $G \cap \mathrm{UT}(L,3) = \{\, \langle\!\langle h\,;\,a\,,b\rangle\!\rangle_L \,|\, h \in H \,\}$.*

Proof. The first part is immediate by Proposition 2.1. For (2) let H be the set of all $h \in L$ for which there is a pair a, b with $\langle\!\langle h\,;\,a\,,b\rangle\!\rangle \in G$. As $\mathrm{Sym}(3) \leq G$, once this happens for one pair a, b, then it happens for all pairs by relation (2.5.4). By assumption $1 \in H$, and by relation (2.5.3) the set H is closed under inverses. Finally it is closed under multiplication by (2.5.4) again.

We now complete our recasting of Chein's Theorem 4.2 in the present context.

(4.6) Theorem. *Let L be a Moufang loop in which the subloop L_0 generated by all elements of order not 2 is a proper subloop. Then there is a subgroup H containing L_0 and an element x of order 2 in $L \setminus H$ such that each element of L may be uniquely expressed in the form hx^a, where $h \in H$, $a = 0, 1$. Furthermore the triality group $\mathrm{UWr}(L,3)$ is isomorphic to $\mathrm{UWr}(H,4)$ with $\pi_3^U = \rho\pi_4^U$.*

Proof. We actually prove something a little stronger:

(a) There is a subloop H containing L_0 and an element $x \in L \setminus H$ with $L = \langle H, x\rangle$.

(b) Suppose H is a subloop containing L_0 and that $x \in L \setminus H$ with $L = \langle H, x\rangle$. Then H is a subgroup, and the triality group $\mathrm{UWr}(L,3)$ is isomorphic to $\mathrm{UWr}(H,4)$ with $\pi_3^U = \rho\pi_4^U$.

We first claim that (a) is a consequence of (b). In proving this we may assume (b) and also, in view of Lemma 4.3.2, that L is not associative. On the other hand, (b) applied to any subloop $\langle x, L_0\rangle$ (for $x \notin L_0$) shows that L_0 is associative. Choose $x_1, x_2, x_3 \in L$ with $(x_1x_2)x_3 \neq x_1(x_2x_3)$. Then $L = \langle x_1, x_2, x_3, L_0\rangle$, as otherwise we could apply (b) to $\langle x, x_1, x_2, x_3, L_0\rangle$, for any $x \notin \langle x_1, x_2, x_3, L_0\rangle$, to reveal $\langle x_1, x_2, x_3, L_0\rangle$ as associative. Let i be the smallest index with $x = x_i \notin \langle\, L_0, x_j \,|\, j > i \,\rangle = H$. Then $L = \langle x, H\rangle$, as desired.

Our proof of (b) proceeds in a series of steps, the first of which is the main point since it shows that, using H, we can partition the involutions of $\mathrm{UT}(L, 3)$ in a way compatible with the involutions of $\mathrm{Sym}(4)$.

Step (1). *Let $h \in H$ and $l \in L \setminus H$. Then $\langle\!\langle h\,;\, a\,, b\rangle\!\rangle$ and $\langle\!\langle l\,;\, a\,, b\rangle\!\rangle$ have product of order 2.*

Proof. Set $t = \langle\!\langle h\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle h^{-1}\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle 1\,;\, a\,, c\rangle\!\rangle$, $r = \langle\!\langle l\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle h^{-1}\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle lh^{-1}\,;\, a\,, c\rangle\!\rangle$. Then by relation (2.5.3)

$$t^r = \langle\!\langle 1\,;\, a\,, c\rangle\!\rangle^{\langle\!\langle lh^{-1}\,;\, a\,, c\rangle\!\rangle} = \langle\!\langle (lh^{-1})^2\,;\, a\,, c\rangle\!\rangle = \langle\!\langle 1\,;\, a\,, c\rangle\!\rangle = t\,,$$

since $lh^{-1} \in L \setminus H$ has order 2. Therefore $2 = |tr| = |\langle\!\langle h\,;\, a\,, b\rangle\!\rangle\langle\!\langle l\,;\, a\,, b\rangle\!\rangle|$.

Step (2). *For $\{a, b, c\} = \{1, 2, 3\}$, set*

$$P^{a,b} = P^{b,a} = \{\, \langle\!\langle h\,;\, a\,, b\rangle\!\rangle \,|\, h \in H \,\} \text{ and } P^{c,4} = P^{4,c} = \{\, \langle\!\langle hx\,;\, a\,, b\rangle\!\rangle \,|\, h \in H \,\}\,.$$

Then, for $\sigma \in \mathrm{Sym}(3) = \langle \langle\!\langle 1\,;\, 1\,, 2\rangle\!\rangle, \langle\!\langle 1\,;\, 2\,, 3\rangle\!\rangle \rangle$, we have $(P^{d,e})^\sigma = P^{d^\sigma, e^\sigma}$.

Proof. Immediate.

Step (3). *For $h, k \in H$, we have $\langle\!\langle hk^{-1}\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle k\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle h\,;\, a\,, c\rangle\!\rangle$ and $\langle\!\langle hx\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle x\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle h\,;\, a\,, c\rangle\!\rangle$.*

Proof. These are the special cases $(u, v) = (h, k^{-1})$ and $(u, v) = (h, x)$ of the Right Inverse Property: $(uv)v^{-1} = u$, valid in any Moufang loop. To verify the property, conjugate $\langle\!\langle u\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle v\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle uv\,;\, a\,, c\rangle\!\rangle$ by (b, c) to find

$$\langle\!\langle u\,;\, a\,, c\rangle\!\rangle = \langle\!\langle uv\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle v\,;\, c\,, b\rangle\!\rangle} = \langle\!\langle uv\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle v^{-1}\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle (uv)v^{-1}\,;\, a\,, c\rangle\!\rangle\,,$$

as desired.

Step (4). *For $h, k \in H$ and $\{a, b, c\} = \{1, 2, 3\}$, we have $\langle\!\langle hx\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle k\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle (hk^{-1})x\,;\, a\,, c\rangle\!\rangle$.*

Proof. Set $t = \langle\!\langle h\,;\, a\,, c\rangle\!\rangle$. We have by Step (3) that $\langle\!\langle hk^{-1}\,;\, a\,, b\rangle\!\rangle^t = \langle\!\langle k\,;\, b\,, c\rangle\!\rangle$ and $\langle\!\langle hx\,;\, a\,, b\rangle\!\rangle^t = \langle\!\langle x\,;\, b\,, c\rangle\!\rangle$. Thus

$$\begin{aligned} \left(\langle\!\langle hk^{-1}\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle x\,;\, b\,, c\rangle\!\rangle}\right)^t &= \langle\!\langle k\,;\, b\,, c\rangle\!\rangle^{\langle\!\langle hx\,;\, a\,, b\rangle\!\rangle} = \langle\!\langle hx\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle k\,;\, b\,, c\rangle\!\rangle} \\ \langle\!\langle (hk^{-1})x\,;\, a\,, c\rangle\!\rangle^t &= \langle\!\langle (hx)k\,;\, a\,, c\rangle\!\rangle\,. \end{aligned}$$

However, $t = \langle\langle h\,;\,a\,,c\rangle\rangle$ with $h \in H$, while $(hk^{-1})x$ is in $L \setminus H$. Therefore by Step (1) the element t commutes with $\langle\langle (hk^{-1})x\,;\,a\,,c\rangle\rangle$, giving

$$\langle\langle (hk^{-1})x\,;\,a\,,c\rangle\rangle = \langle\langle (hk^{-1})x\,;\,a\,,c\rangle\rangle^t = \langle\langle (hx)k\,;\,a\,,c\rangle\rangle\,.$$

Step (5). *For $t \in P^{d,e}$ and $r \in P^{f,g}$, we have $r^t \in P^{f^{(d,e)},g^{(d,e)}}$.*

Proof. If $|\{d,e,f,g\}| = 4$, then this follows from Step (1).

If $|\{d,e,f,g\}| = 3$, then there are four separate cases. For $h,k \in H$ and $\{a,b,c\} = \{1,2,3\}$ we must show

(i) $\langle\langle h\,;\,a\,,b\rangle\rangle^{\langle\langle k\,;\,b\,,c\rangle\rangle} \in P^{a,c}$;
(ii) $\langle\langle hx\,;\,a\,,b\rangle\rangle^{\langle\langle k\,;\,b\,,c\rangle\rangle} \in P^{b,4}$;
(iii) $\langle\langle h\,;\,a\,,b\rangle\rangle^{\langle\langle kx\,;\,b\,,c\rangle\rangle} \in P^{b,4}$;
(iv) $\langle\langle hx\,;\,a\,,b\rangle\rangle^{\langle\langle kx\,;\,b\,,c\rangle\rangle} \in P^{a,c}$.

Part (i) is immediate, and part (ii) comes directly from Step (4). For (iii),

$$\langle\langle h\,;\,a\,,b\rangle\rangle^{\langle\langle kx\,;\,b\,,c\rangle\rangle} = \langle\langle kx\,;\,b\,,c\rangle\rangle^{\langle\langle h\,;\,a\,,b\rangle\rangle} = \langle\langle kx\,;\,c\,,b\rangle\rangle^{\langle\langle h^{-1}\,;\,b\,,a\rangle\rangle} \in P^{b,4}$$

by (ii).

Using Step (4), we have for all $n,k \in H$

$$\langle\langle n\,;\,c\,,a\rangle\rangle^{\langle\langle kx\,;\,b\,,c\rangle\rangle} = \langle\langle kx\,;\,b\,,c\rangle\rangle^{\langle\langle n\,;\,c\,,a\rangle\rangle} = \langle\langle (kn^{-1})x\,;\,b\,,a\rangle\rangle\,,$$

hence

$$\langle\langle (kn^{-1})x\,;\,a\,,b\rangle\rangle^{\langle\langle kx\,;\,b\,,c\rangle\rangle} = \langle\langle (kn^{-1})x\,;\,b\,,a\rangle\rangle^{\langle\langle kx\,;\,b\,,c\rangle\rangle} = \langle\langle n\,;\,c\,,a\rangle\rangle \in P^{a,c}\,.$$

Since inversion and left multiplication by k are permutations of H, we can replace kn^{-1} by h and find (iv) to be valid for all $h,k \in$H.

We are left with the case $|\{d,e,f,g\}| = 2$. If $\{d,e\} = \{f,g\} = \{a,b\} \subset \{1,2,3\}$, then $\langle\langle h\,;\,a\,,b\rangle\rangle^{\langle\langle k\,;\,a\,,b\rangle\rangle} = \langle\langle k(h^{-1}k)\,;\,a\,,b\rangle\rangle \in P^{a,b}$ by relation (2.5.3). If instead $\{d,e\} = \{f,g\} = \{c,4\}$ with $\{a,b,c\} = \{1,2,3\}$, then an argument similar to that of Remark 2.7 applies. Specifically

$$\begin{aligned}\langle\langle hx\,;\,a\,,b\rangle\rangle^{\langle\langle kx\,;\,a\,,b\rangle\rangle} &= (\langle\langle 1\,;\,c\,,a\rangle\rangle\langle\langle hx\,;\,c\,,b\rangle\rangle\langle\langle 1\,;\,c\,,a\rangle\rangle)^{\langle\langle kx\,;\,a\,,b\rangle\rangle}\\ &= \langle\langle kx\,;\,c\,,b\rangle\rangle\langle\langle hx\,;\,c\,,b\rangle\rangle^{\langle\langle kx\,;\,a\,,b\rangle\rangle}\langle\langle kx\,;\,c\,,b\rangle\rangle\\ &\in (P^{a,c})^{\langle\langle kx\,;\,c\,,b\rangle\rangle} = P^{c,4}\,.\end{aligned}$$

Step (6). $L = H \cup Hx$ *and* $\mathrm{UT}(L,3) = \bigcup_{d,e} P^{d,e}$.

Proof. The subset $P = \bigcup_{d,e} P^{d,e}$ of $\mathrm{UT}(L,3)$ is closed under conjugation by the previous step. Therefore by Lemma 4.5 if $G = \langle P\rangle$, then $P = G \cap \mathrm{UT}(L,3)$ and there is a subloop H_1 of L with $P = \{\,\langle\langle h\,;\,a\,,b\rangle\rangle \,|\, h \in H_1\,\}$. But $L = \langle H,x\rangle \leq H_1$, so $L = H_1$ and $P = \mathrm{UT}(L,3)$.

Step (7). *The subloop H of the Moufang loop L is a subgroup. There is an isomorphism* $\mathrm{UWr}(H,4) \longrightarrow \mathrm{UWr}(L,3)$ *with* $\rho\pi_4^U = \pi_3^U$.

Proof. By Step (5), the map taking each member of $P^{d,e}$ to $(d,e) \in \mathrm{Sym}(4)$ extends to a homomorphism π_4^U from $G = \langle \mathrm{UT}(L,3) \rangle = \mathrm{UWr}(L,3)$ (by Step (6)) onto $\mathrm{Sym}(4)$ in which each element g of $\mathrm{UWr}(L,3)$ permutes the six $P^{d,e}$ according to $\pi_4^U(g)$. By construction $\pi_3^U = \rho\pi_4^U$.

Furthermore, for $t, r \in \mathrm{UT}(L,3)$, if $\pi_4^U(t) \neq \pi_4^U(r)$, then $|\pi_4^U(t)\pi_4^U(r)| = |tr|$ by $(*)$ if $\pi_3^U(t) \neq \pi_3^U(r)$ and by Step (1) if $\pi_3^U(t) = \pi_3^U(r)$. Therefore, by Theorem 3.7 there is a group K with $\mathrm{UT}(L,3)$ isomorphic to a central quotient of $\mathrm{UWr}(K,4)$, the homomorphism inducing a bijection between $\mathrm{UT}(K,4)$ and $\mathrm{UT}(L,3)$. Thus $\mathrm{UWr}(K,4)$ and $\mathrm{UWr}(L,3)$ have isomorphic transform tables relative to these two classes. Since each group has been defined as the corresponding relative universal central extension, the central kernel is trivial and the homomorphism is an isomorphism.

Again by Theorem 3.7, this isomorphism takes the base group of $\mathrm{UWr}(K,4)$ to that of $\mathrm{UWr}(L,3)$, which is to say that the projection map of $\mathrm{UWr}(K,4)$ onto $\mathrm{Sym}(4)$ factors through π_4^U. In particular, if we look at the subgroup of of $\mathrm{UWr}(K,4)$ that projects onto $\mathrm{Sym}(3)$, then by Lemma 4.5 it is a central quotient of $\mathrm{UWr}(K,3)$ that the isomorphism carries to a central quotient of $\mathrm{UWr}(H,3)$. This group with triality is therefore coordinatized both by the group K and by the Moufang loop H. By Theorem 4.1, a coordinatizing Moufang loop is unique up to isotopy. Since, as noted above, a loop isotopic to a group is in fact an isomorphic group, we conclude that H is a group isomorphic to K. This concludes this step and so our proof of (b) and Theorem 4.6.

Remark. We are not claiming that our arguments are easier than those of Chein, only that the construction and treatment via wreath products reveal how naturally the generalized dihedral loops arise: the wreath products $\mathrm{Wr}(H,4)$ are groups with triality, so they are coordinatized by an interesting class of Moufang loops.

4.2 A cautionary tale

The question arises: can we classify all groups with symmetric quotient of degree at least 4 subject only to Hypothesis 3.1.5, that is, respecting transposition products of order 3?

While a solution is conceivable, there are many examples that are somewhat removed from the full wreath product.

(4.7) Theorem. *Let finite $|\Omega| \geq 3$, and further let K be a group with $\{ k^3 \mid k \in K \} \neq 1$. Then, for a faithful transitive* $\mathrm{Sym}(\Omega)$*-space Δ, the wreath product $K \wr_\Delta \mathrm{Sym}(\Omega)$ satisfies Hypothesis 3.1.5 if and only if Δ is isomorphic to the* $\mathrm{Sym}(\Omega)$*-space of i-subsets, $\binom{\Omega}{i}$, for some $0 < i \leq |\Omega|/2$.*

Here we should more properly speak of that subgroup of $K \wr_\Delta \mathrm{Sym}(\Omega)$ normally generated by the transpositions of $\mathrm{Sym}(\Omega)$.

We only sketch a proof of Theorem 4.7. Let Σ be an orbit for the subgroup S, a "transposition Sym(3)" of $\mathrm{Sym}(\Omega)$, in the action on Δ. Then results of [6] imply that, with K as described, the transpositions of $K \wr_\Sigma S$ generate a group with triality with base in K^3 if and only if $|\Sigma|$ is 1 or 3. Therefore all orbits of S on Δ have length 1 or 3. However, the faithful and transitive permutation representations of $\mathrm{Sym}(\Omega)$ with this property are exactly those isomorphic to $\binom{\Omega}{i}$, for some $0 < i \leq |\Omega|/2$.

The usual full wreath product, as in Theorem 1.2, corresponds to the case $i = 1$. The Sym(4)-space $\binom{\Omega}{2}$ leads once again to triality groups. The first new example is thus $|\Omega| = 5$, $i = 2$, and $|K| = 2$. The transposition class of the corresponding group $2^{10}{:}\,\mathrm{Sym}(5)$ generates a subgroup $2^9{:}\,\mathrm{Sym}(5)$. As $\mathbb{F}_2\,\mathrm{Sym}(5)$-module, the base 2^9 has a submodule 2^5 that is the usual permutation module. The quotient 2^4 is the natural module $\mathbb{F}_4^2$ for $\Sigma\mathrm{L}_2(4) \simeq \mathrm{Sym}(5)$, and so $\mathbb{F}_4^2{:}\,\Sigma\mathrm{L}_2(4)$ satisfies Hypothesis 3.1.5.

References

[1] M. Aschbacher, On finite groups generated by odd transpositions, I, Math. Z., **127** (1972), 45–56, II, III, IV, J. Algebra, **26** (1973), 451–459, 460–478, 479–491.

[2] M. Aschbacher, "Finite Group Theory," Second edition, Cambridge Studies in Advanced Mathematics, **10**, Cambridge University Press, Cambridge, 2000.

[3] R.H. Bruck, "A Survey of Binary Systems," Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[4] O. Chein, Moufang loops of small order. I, Trans. Amer. Math. Soc., **188** (1974), 31–51.

[5] H. Cuypers and J.I. Hall, The 3-transposition groups with trivial center, J. Algebra, **178** (1995), 149–193.

[6] S. Doro, Simple Moufang loops, Math. Proc. Cambridge Philos. Soc., **83** (1978), 377–392.

[7] B. Fischer, Distributive Quasigruppen endlicher Ordnung, Math. Z., **83** (1964), 267–303.

[8] B. Fischer, A characterization of the symmetric groups on 4 and 5 letters, J. Algebra, **3** (1966), 88–98.

[9] B. Fischer, Eine Kennzeichnung der symmetrischen Gruppen vom Grade 6 und 7, Math. Z., **95** (1967), 288–298.

[10] B. Fischer, Finite groups generated by 3-transpositions, I, Invent. Math., **13** (1971), 232–246.

[11] M. Funk and P.T. Nagy, On collineation groups generated by Bol reflections, J. Geom., **48** (1993), 63–78.

[12] S.M. Gagola III, "Subloops of the unit octonians," Ph.D. thesis, Michigan State University, 2005.

[13] G. Glauberman, On loops of odd order, I, J. Algebra, **1** (1964), 374–396, II, J. Algebra, **8** (1968), 393–414.

[14] G. Glauberman, Central elements in core-free groups, J. Algebra, **4** (1966), 403–420.

[15] J.I. Hall, General theory of 3-tranposition groups, Math. Proc. Cambridge Philos. Soc., **114** (1993), 269–294.

[16] J.I. Hall and G.P. Nagy, On Moufang 3-nets and groups with triality, Acta Sci. Math. (Szeged), **67** (2001), 675–685.

[17] H.O. Pflugfelder, "Quasigroups and Loops: Introduction," Sigma Series in Pure Mathematics, **7**, Heldermann Verlag, Berlin, 1990.

[18] T.A. Springer and F.D. Veldkamp, "Octonions, Jordan algebras and exceptional groups," Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[19] F.G. Timmesfeld, A characterization of the Chevalley- and Steinberg-groups over $\mathbf{F}_2$, Geom. Ded., **1** (1973), 269–321.

[20] J. Tits, Sur la trialité et les algèbres d'octaves, Acad. Roy. Belg. Bull. Cl. Sci., **44** (1958), 332–350.

[21] F. Zara, "Classification des couples fischeriens," Thése, Amiens, 1985.