Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 51 (2010), No. 1, 117-135.

Self-invariant 1-Factorizations of Complete Graphs and Finite Bol Loops of Exponent 2

Barbara Baumeister **Alexander Stein** *

Technische Universität Dortmund, Fakultät für Mathematik
44221 Dortmund, Germany
e-mail: baumeist@mi.fu-berlin.de

Fachbereich Mathematik und Informatik, FU Berlin
Arnimallee 3, 14195 Berlin, Germany

1. Introduction

Let Ω be a complete graph on an even number $n = 2m$ of vertices $\mathcal{V} = \mathcal{V}(\Omega) = \{\omega_1, \ldots, \omega_n\}$ and assume that $\mathcal{K} = \{k_1, \ldots, k_{n-1}\}$ is a 1-factorization of Ω. Identify every $k \in \mathcal{K}$ with the fixed point free involution of $\mathrm{Sym}(\mathcal{V})$ which interchanges the ends of every edge in k and set $G_{\mathcal{K}} = \langle \mathcal{K} \rangle$. Then $\mathcal{K}$ is said to be *self-invariant* if $\mathcal{K}^k = \mathcal{K}$ for all $k \in \mathcal{K}$. Heiss [13] studied self-invariant 1-factorizations and conjectured

Conjecture 1.1. [13] *If $\mathcal{K}$ is a self-invariant 1-factorization, then $G_{\mathcal{K}}$ is a 2-group.*

This conjecture holds if and only if some long standing conjecture on Bol loops is true. We follow the notation and terminology of [2]. A *loop* is a magma $(X, \circ)$, that is a set X together with a binary operation $\circ$ on X, with an identity 1 such that for every x in X the maps

$$R(x) : y \mapsto y \circ x \quad \text{and} \quad L(x) : y \mapsto x \circ y,$$

*This research is part of the project "Transversals in groups with an application to loops" (GZ: BA 2200/2-2), funded by the DFG.

called *right* and *left translations*, are permutations of X. Thus in a loop for every pair of elements $s, t \in X$ there exist unique elements x, y in X such that $s \circ x = t$ and $y \circ s = t$. Hence one may think of a loop as a group without associative axiom.

Loops play a role in physics – in particular those which satisfy a weak associative axiom, see for instance [23]. A loop X is a *right Bol loop* if it satisfies the *right Bol Identity* (BOL) for all x, y, z in X:

$$((x \circ y) \circ z) \circ y = x \circ (((y \circ z) \circ y).$$

This is equivalent to the condition:

$$R(y)R(z)R(y) = R((y \circ z) \circ y) \qquad \text{for all } y, z \in X.$$

Notice, that it makes no difference whether left or right Bol loops are studied. We obtain a left Bol loop out of a right one by dualizing it and vice versa, see [14, p. 2]. In this paper, we consider right Bol loops and call them simply Bol loops to shorten the notation. For several years Bol loops have been studied by numerous people, see for instance [7], [9], [10], [22], [19], [20], [13], [2]. A Bol loop X is said to be of *exponent* 2 if $x \circ x = 1$ for all $x \in X$. If the loop of exponent 2 is a group, then it is an elementary abelian 2-group. It was a widely accepted opinion, that there is an analogous statement for loops. A *normal subloop* is the kernel of a loop homomorphism, and a *section* of a loop X is the homomorphic image of a subloop of X. The loop is *soluble* if there is a series of subloops

$$X = X_0 \geq X_1 \geq X_2 \geq \cdots \geq 1$$

such that X_{i+1} is normal in X_i and such that the respective sections are abelian groups. This determines the loop, as the Jordan-Hölder theorem for loops holds [1]. If X does not possess a non-trivial normal subloop, then X is *simple*.

Conjecture 1.2. [21] *Every finite Bol loop of exponent* 2 *is soluble.*

This implies the following conjecture, in particular.

Conjecture 1.3. [21] *If X is a finite simple Bol loop of exponent* 2*, then X is a* 2*-group.*

Every Bol loop of exponent 2 is a Bruck loop. In a Bol loop, every element x has an inverse element x^{-1}, for instance see [14]. A *Bruck loop* (in loop theory also called K-Loop [16], [14] or in physics gyrocommutative gyrogroup [23], see also [15, p. 5]), is a Bol loop X which satisfies the automorphic inverse property AIP

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \text{ in } X.$$

Bruck loops of odd order were studied by Glauberman [9], [10]. He generalized Feit-Thompson's theorem to Bruck loops of odd order – as well as the group theoretic theorems such as Cauchy's, Sylow's, Lagrange's and Hall's theorems.

Bol loops of exponent 2 behave differently. In this paper we present a counterexample to the second conjecture, see Theorem 1. We call this example the *Aschbacher loop* $\mathcal{A}$ and prove that the Aschbacher loop is the smallest counterexample which exists, see Theorem 3. Notice, in particular, that $\mathcal{A}$ is not a group. In the next section we recall the equivalence of the Conjectures 1.1 and 1.2. It is an easy exercise to construct a counterexample to Conjecture 1.1 out of the Aschbacher loop.

Let X be a counterexample to Conjecture 1.2 which is of minimal size. Then X is a simple loop. A Bol loop M which also satisfies the identity

$$x \circ (y \circ (x \circ z)) = ((x \circ y) \circ x) \circ z \text{ for all } x, y, z \in M$$

is called *Moufang loop*. Moufang showed that every Moufang loop is di-associative, meaning every two elements of the loop generate a subgroup. This implies that a Moufang loop of exponent 2 is abelian. It has been shown by Bruck that every Moufang loop of exponent 2 is an elementary abelian 2-group [5, VIII (11.1)].

Hence, every finite minimal counterexample is a finite simple Bol loop which is not a simple Moufang loop. Therefore, the loop $\mathcal{A}$ is also an example answering positively the

Question 1.4. [2, Question 4] Does there exist a finite simple Bol loop which is not a simple Moufang loop?

Notice that this question has also already been answered by Nagy in [20].

We show the following.

Theorem 1. *The Aschbacher loop $\mathcal{A}$ constructed in Section 3 is a finite simple insoluble Bol loop of exponent 2 and the following hold.*

(a) $|\mathcal{A}| = 96$.

(b) $G := \langle R(x) \mid x \in X \rangle$ *is a non-split extension* $2^{5\cdot} PGL_2(5)$.

(c) $Aut(\mathcal{A}) \cong \mathbb{Z}_5 : Mod_{16}$.

This theorem implies

Theorem 2. *There exists a self-invariant factorization of the complete graph on 96 vertices such that $G_{\mathcal{K}}$ is a non-split extension $2^{5\cdot} PGL_2(5)$.*

An immediate question is whether $\mathcal{A}$ is the smallest example. Our answer is as follows:

Theorem 3. *If $\mathcal{B}$ is a finite Bol loop of exponent 2 which is not isomorphic to $\mathcal{A}$ and which is not soluble, then $|\mathcal{A}| < |\mathcal{B}|$.*

The starting point of the construction of our example was the main theorem of [2], while the starting point of the work by Aschbacher is what he calls the *Baer correspondence*. This is a correspondence between loops and certain triples of group theoretic data and is as follows [2], [4]:

Let X be a Bol loop; let

$$K = \{R(x) \mid x \in X\}$$

be the set of right translations of X and let $G = \langle K \rangle$ be the subgroup of $\mathrm{Sym}(X)$ generated by K. Then K is a right transversal to the stabilizer H of 1 in G, see [2, p. 100]. In [2] this triple (G, H, K) is called *the envelope* of the loop X, and G the *enveloping group* of X. In particular, as G acts faithfully on the set of cosets of H in G, the subgroup H does not contain a non-trivial normal subgroup of G (i.e. $\mathrm{core}_G(H) = 1$), see also [2, 1.3].

If G is a group, H a subgroup of G and K a transversal to H^g in G for every g in G which contains the identity $1 \in K$, then the triple (G, H, K) is called *loop folder* [2]. Baer observed that given a loop folder we can construct a loop out of it by defining a multiplication on K as follows:

$$k \circ l = m \;\text{ if }\; Hkl = Hm \;\text{ for all } k, l, m \text{ in } K,$$

see [4] or [2]. The loop folder (G, H, K) is called a *loop envelope* if $G = \langle K \rangle$ and *faithful* if $\mathrm{core}_G(H) = 1$. The loop folder constructed above using the right translations is by definition a faithful loop envelope. The loop to a loop folder is a Bol loop if and only if K is a twisted subgroup of G, that is if for all the elements x, y in K also x^{-1} and xyx are contained in K [2, 6.1 (1)].

Aschbacher denotes by an *N-loop*, a finite Bol loop of exponent 2 such that the enveloping group is not a 2-group, but it is a 2-group for every proper subloop. Heiss showed that the enveloping group of an N-loop is neither soluble nor simple [13]. This result has been strengthened by Aschbacher considerably:

Theorem 4. [2, Main theorem] *Let X be a finite Bol loop of exponent* 2 *which is an N-loop. Let (G, H, K) be the envelope of X, $J = O_2(G)$ and $G^\star = G/J$. Then*

(a) *$G^\star \cong PGL_2(q)$, with $q = 2^n + 1 \geq 5$, $H^\star$ a Borel subgroup of $G^\star$, and $K^\star$ consists of the involutions in $G^\star - F^\star(G^\star)$.*

(b) *$F^\star(G) = J$.*

(c) *$|K \cap J| = n_0$, $|K \cap aJ| = n_1$ for a in $K - J$, where $n_0 = n_1 2^{n-1}$ is a* 2*-power and $|K| = (q+1)n_0 = n_1 2^n(2^{n-1}+1)$.*

Notice that the Aschbacher loop is an N-loop with $q = 5$. It is possible to construct infinite series of examples out of the Aschbacher loop with $q = 5$, see [6] or [19]. It is an open (and difficult) question as to whether there are examples with $q > 5$.

Preciseley the same example as ours has also been found by Nagy [19]. Our construction presented here is completely different from the one given in [19].

Finally notice that as in group theory many interesting questions on loops can be reduced to questions on simple loops. An example is Lagrange's theorem, see Bruck [5]. Recently Lagrange's theorem was proven for Moufang loops independently by various groups of people (see Theorem 5.5 in [12] and the references therein), based on the classification of simple Moufang loops by Liebeck [17].

The existence of simple insoluble Bruck loops raises therefore a new challenging problem:

Is it possible to classify the enveloping groups of the finite simple Bruck loops?

This classification became more feasible as in recent years Aschbacher, Kinyon and Phillips [3] studied Bruck loops of even order. They showed, that in Bruck loops elements of odd order commute with elements of 2-power order. Therefore, the problem of simple Bruck loops reduces to simple Bruck loops with all elements of 2-power order. The special case of Bol loops of exponent 2 seems to be a natural starting point for questions on finite simple Bruck loops.

In the next section we provide further notation on loops and recall the equivalence of the Conjectures 1.1 and 1.2. Then in the third section we construct the Aschbacher Loop $\mathcal{A}$ in the wreath product $\mathbb{Z}_4 \wr \mathrm{Sym}(5) \leq \mathbb{Z}_4 \wr \mathrm{Sym}(15)$. Moreover, we present a simple Bruck loop of exponent 4, which lives in the enveloping group G of $\mathcal{A}$, see 3.5. In the fourth section we determine the subloops and the automorphism group of $\mathcal{A}$ and state some further properties of this loop. Theorem 3 is proven in the last section.

Acknowledgement. We like to thank the referee for many helpful comments.

2. Graphs, Groups and Loops

In this section we recall the notion of a $(\star)$-group which was introduced by Heiss [13].

Definition 2.1. *A finite group G is called a $(\star)$-group with respect to a subgroup H and a set of involutions $I \subseteq G$ if and only if the following hold.*

($\star$a) $G = \langle I \rangle$.

($\star$b) *I is invariant under conjugation.*

($\star$c) $G = \bigcup_{k \in K} Hk$ *where* $K = I \cup \{1\}$.

Remark 2.2. Note that in the definition of a $(\star)$-group, the condition ($\star$c) may be replaced by the equivalent condition

($\star$d) $KK \cap H = 1$ and $|G| = |K||H|$,

or equivalently by

($\star$e) $KK \cap H = 1$ and $G = KH$.

We show that self-invariant 1-factorizations as well as finite Bol loops of exponent 2 are related to $(\star)$-groups.

Lemma 2.3. *Let $\mathcal{I}$ be a self-invariant 1-factorization of the complete undirected graph $\Omega = (\mathcal{V}, \mathcal{E})$. Identify $\mathcal{I}$ with a set of involutions in $\mathrm{Sym}(\mathcal{V})$ as described in the introduction. Then $G_{\mathcal{I}} \leq \mathrm{Sym}(\mathcal{V})$ is a $(\star)$-group with respect to the stabilizer H of the vertex $\omega_1 \in \mathcal{V}$ in $G_{\mathcal{I}}$ and the set $\mathcal{I}$ of involutions.*

Proof. By definition $\mathcal{I}$ is a set of involutions of $G_{\mathcal{I}}$ which generate the latter group. As $G_{\mathcal{I}}$ is a subgroup of $\mathrm{Sym}(\mathcal{V})$, it is finite. Also ($\star$b) follows immediately from the definition of a self-invariant 1-factorization.

As $\mathcal{I}$ comes from a 1-factorization, the orbit of ω under the action of $\mathcal{I}$ is the whole set $\mathcal{V}$. This implies ($\star$c). □

On the other hand if G is a ($\star$)-group with respect to the subgroup H and the set of involutions $I \subseteq G$, then every element $k \in I$ corresponds to a 1-factor in the complete graph Ω with set of vertices the set of cosets of H in G [13]. Therefore, I corresponds to a self-invariant 1-factorization of Ω and the permutation group generated by I is $G/\operatorname{core}_G(H)$.

Heiss [13] showed

Lemma 2.4. *Conjecture* 1.1 *holds if and only if every* ($\star$)*-group is a* 2*-group.*

Now we prove the respective lemma for finite Bol loops of exponent 2.

Lemma 2.5. *Let X be a finite Bol loop of exponent* 2 *and let (G, H, K) be the envelope of the loop X. Then G is a* ($\star$)*-group with respect to the subgroup H and the set $I = K - \{1\}$.*

Proof. By the definition of G it satisfies condition ($\star$a). As K is a transversal to H in G, ($\star$c) holds as well.

It remains to show that $K - \{1\}$ is the union of conjugacy classes of involutions. As X is a Bol loop, K is a twisted subgroup of G, that is for all the elements x, y in K also x^{-1} and xyx are contained in K [2, 6.1 (1)]. Moreover, $R(x^n) = R(x)^n$ for all $x \in X$ and $n \in \mathbb{N}$, see [2, 6.8 (1)]. As X is of exponent 2, for all x in X we have $x \circ x = 1$. Thus $R(x)^2 = R(x^2) = 1$ for all x in X which shows that $K - \{1\}$ consists of elements of order 2. As xyx is contained in K for all x, y in K, the latter is closed under conjugation with elements in G. □

The Baer correspondence and 2.5 yield the following characterization of Bol loops.

Proposition 2.6. *A loop folder (G, H, K) is the envelope of a Bol loop of exponent* 2 *if and only if* $\operatorname{core}_G(H) = 1$ *and G is a* ($\star$)*-group with respect to the subgroup H and the set $K - \{1\}$.*

Proof. Let G be a ($\star$)-group with respect to the subgroup H and the set $K - \{1\}$. We need showing that K is a twisted subgroup of G. Let x and y be elements in K. As they are involutions by the definition of a ($\star$)-group, $x^{-1} = x$ is in K and moreover, $xyx = x^{-1}yx$. By conditions ($\star$a) and ($\star$b) $x^{-1}yx$ is in K. □

3. The Aschbacher loop $\mathcal{A}$

Let L be a group isomorphic to the symmetric group $\mathrm{Sym}(5) \cong PGL_2(5)$ and let $N = M^{15}$, $M \cong \mathbb{Z}_4$, be a homocyclic group of rank 15 and exponent 4. Label the 15 generators of N with the 15 involutions of $L' \cong \mathrm{Alt}(5)$. This gives a natural module action of L on N. We consider N as a $\mathbb{Z}L$-module and write $\cdot$ for the module action and $+$ for the sum in $\mathbb{Z}L$.

Denote the semidirect product of N with L by W, i.e. W is the wreath product $W = M \wr L$ and L is acting as a subgroup of $\mathrm{Sym}(15)$ on $N = M^{15}$.

Consider the Steinberg presentation for $L \cong PGL_2(5)$, see [8],

$$L = \langle w, y, n \mid 1 = w^5 = y^4 = n^2, w^y = w^2, y^n = y^{-1}, n = ww^n w\rangle.$$

For instance $w = (1,2,3,4,5), y = (1,3,2,5), n = (1,5)(2,3)$ satisfy these relations.

Notice, that $B := \langle w, y\rangle \cong \mathbb{Z}_5 : \mathbb{Z}_4$ is a Borel subgroup of L.
Let v be the generator in N corresponding to the involution y^2 and

$$b_1 := v \cdot (1 + w + w^2 + w^3 + w^4),$$
$$b_2 := v \cdot (w^4 n(1 + w + w^2 + w^3 + w^4))$$

and

$$b_3 := v \cdot (w^3 n(1 + w + w^2 + w^3 + w^4)).$$

Note that b_1, b_2, b_3 are centralized by w. Moreover, b_1 is centralized by y, while b_2 and b_3 are interchanged by y.

(1) Next we define an L-submodule J in $\Omega_1(N)$ (the subgroup of N which is generated by the involutions of N). Set

$$v_1 := (b_2 b_3)^2.$$

Then v_1 is the product of the squares of all generators corresponding to $\mathrm{Alt}(5)$-involutions outside the Borel $\langle w, y\rangle$. Therefore v_1 is centralized by w and y and

$$|L : C_L(v_1)| = 6 = |L : B|.$$

This yields that the normal closure J of $\langle v_1\rangle$ in W is an L-module, which is an image of the permutation module for $L \cong PGL_2(5)$ of degree 6.

As every $\mathrm{Alt}(5)$-involution fixes two of the 6 points, the sum of all conjugates of v_1 is zero, thus J is at most 5-dimensional. Since there is an orbit of length 6, the module is the unique 5-dimensional image of the 6-dimensional permutation module. Therefore, L has three orbits on $J^{\#}$, which are of size $15, 10$ and 6.

We introduce some new elements by defining

$$v_2 := v_1^n,\ v_3 := v_2^w,\ v_4 := v_3^w,\ v_5 := v_4^w,\ v_6 := v_5^w.$$

The permutation action of w, y, n on $v_1, \ldots, v_6$ is

$$(v_2, v_3, v_4, v_5, v_6), \quad (v_3, v_4, v_6, v_5) \text{ and } (v_1, v_2)(v_3, v_6),$$

respectively. The orbit of length 15 consists of the $\binom{6}{2} = 15$ products of length 2 of the generators, the orbit of length 10 of the $\binom{6}{3} = 20$ products of length 3 (recall $v_1 v_2 v_3 v_4 v_5 v_6 = 1$).

(2) We define $y_* := b_1 b_3 y$. Then $y_*^4 = v_1$ and $|\langle w, y_*\rangle| = 40$ as w and $b_1 b_3$ commute.

(3) Let $n_* = (v \cdot (w^3(1 + n - nw) + w^4(1 - n + 2nw) + 1))n$. Then we can verify the following relations:

(3a) $n_*^2 = v_1v_2v_5$.
(3b) $(y_*n_*)^2 = v_1v_2$.
(3c) $n_*v_6v_2 = ww^{n_*}w$ (equivalently $(n_*w)^3 = 1$).
(4) Set

$$G := \langle w, y_*, n_* \rangle.$$

We claim that $O_2(G) = J = \langle v_1, v_2, v_3, v_4, v_5 \rangle$.
In (2) we saw that v_1 is an element in J. As G covers L, we get that J is contained in $O_2(G)$. By evaluating the defining relations for L, which was done in (3), we see that $J = O_2(G)$.

Notice, that (4) implies

(5) $|G| = 2^8 \cdot 3 \cdot 5$.

(6) $\langle y_*, n_* \rangle \in Syl_2(G)$:

In $\langle y_*, n_* \rangle$ are the elements $v_1(= y_*^4), v_2(= v_1^{n_*}),\ v_5(= n_*^2v_1v_2),\ v_6(= v_5^{n_*}), v_3(= v_5^{y_*}), v_4(= v_3^{y_*})$, so $J \le \Phi(\langle y_*, n_* \rangle)$. As $\langle y_*, n_* \rangle$ covers $\langle y, n \rangle \in Syl_2(L)$, $\langle y_*, n_* \rangle \in Syl_2(G)$.

(7) The Frattini subgroup $\Phi(G)$ of G equals $O_2(G)$:

Assume there is some supplement S to $O_2(G)$ and let $P \in Syl_2(S)$. Then $O_2(G)P \in Syl_2(G)$ and we may assume $O_2(G)P = \langle y_*, n_* \rangle$. As $P < O_2(G)P$, we have $O_2(G) \not\le \Phi(PO_2(G)) = \Phi(\langle y_*, n_* \rangle)$, contradicting the calculations in (6). Therefore there is no supplement to $O_2(G)$ in G, which implies (7).

(8) There are precisely 80 involutions in $G - O_2(G)$. They are all conjugate and map to transpositions in $L \cong$ Sym(5). A representative is $v_1y_*n_*$:

Let $u \in J = O_2(G)$ and consider $(un_*)^2 = uu^nn_*^2$. As $uu^n \in [J, n]$, but $n_*^2 = v_1v_2v_5$ is not in $[J, n]$, the coset Jn_* does not contain involutions. This yields that the involutions in G which are not in J map to transpositions in $G/J \cong L \cong$ Sym(5). According to (3b) $v_1y_*n_*$ is an involution in $G - J$. All the involutions in the coset Jy_*n_* are $uv_1y_*n_*$ with u in $C_J(yn) = \langle v_1v_2, v_3v_4, v_1v_3v_5 \rangle$. Hence there are exactly $2^3 \cdot 10$ involutions in $G - J$.

As y_*^2 does not commute with $v_1y_*n_*$ (although y^2 commutes with yn), $C_G(v_1 y_*n_*) \cong 2^3 \cdot \mathbb{Z}_6$. Thus the orbit $(v_1y_*n_*)^G$ is of length $2^4 \cdot 5$ and all the involutions in $G - O_2(G)$ are conjugate. Set

$$K := \{1\} \cup \{(v_1v_2)^x \mid x \in G\} \cup \{(v_1y_*n_*)^y \mid y \in G\}$$

and

$$H := \langle w, y_* \rangle.$$

Lemma 3.1. *G is a $(\star)$-group with respect to the subgroup H and the set $K - \{1\}$.*

Proof. $|G : H| = 96 = |K|$ and K is a normal subset of G which consists beside the identity of involutions. Clearly, G is generated by K. It remains to show that K is a transversal to H in G. Hence we need showing that $KK \cap H = \{1\}$. In the factor group Sym(5) $\cong G/J$ we see, that the only critical products are of the following two types:

A pair of involutions of K which map to the same transposition in $L \cong \mathrm{Sym}(5)$ and

a pair of involutions of K which map to different but in $L \cong \mathrm{Sym}(5)$ commuting transpositions.

The product of a pair of the first type is in the centralizer in J of that transposition, which does not intersect with $H \cap J = \langle v_1 \rangle$. This is true for the transposition $v_1 y_* n_*$, see the centralizer given in (8). As B acts transitively on the transpositions in L, this is then true in general.

By conjugation we may assume in the other case, that the transpositions map to yn and $y^3 n$ and that one of them is $t_1 := v_1 y_* n_*$ and the other is in $t_2 \langle v_1 v_2, v_3 v_5, v_1 v_3 v_4 \rangle$ with $t_2 := v_3 y_*^3 n_*$. A short calculation shows that

$$C_J(t_1) \cap C_J(t_2) = \langle v_1 v_2, v_1 v_4 v_5 \rangle.$$

Therefore, it is enough to consider the products $(t_1 t_2)^2 = v_1 v_3 v_6$ and $(t_1 v_3 v_5 t_2)^2 = v_1 v_4 v_5$: In the other cases we get the same squares. But this reveals, that the product of any two involutions, which map to different commuting transpositions, is an element of order 4, which squares into the G-orbit of length 10 in J. As the elements of order 4 in H square to v_1, we get the transversal property of K. $\square$

Remark 3.2. Notice, that Theorem 1.2 of Hall [11] implies that there are involutions t, r in $K - J$ such that $tJ \neq rJ$ and such that the order of tr is different from the order of trJ.

Corollary 3.3. $\mathcal{A} = (K, \circ)$ *where* $\circ$ *is as defined in the introduction is a Bol loop of exponent* 2.

Proof. Proposition 2.6 and Lemma 3.1 imply the assertion. $\square$

Lemma 3.4. $\mathcal{A}$ *is a simple loop.*

Proof. Let $\mathcal{B}$ be a normal subloop of $\mathcal{A}$. Then $G_0 := \langle R(x) \mid x \in \mathcal{B} \rangle$ is a normal subgroup of G and if $G_0 \neq G$, then G/G_0 is a group related to a Bol loop of exponent 2. If $G_0 \neq 1$, then $[J, G] \leq G_0$. Therefore, G/G_0 does not satisfy the condition (b) of Theorem 4, that is $F^*(G/G_0) \neq O_2(G/G_0)$. Thus it is therefore not related to a Bol loop of exponent 2. $\square$

Remark 3.5. If we replace K by

$$\tilde{K} := \{1\} \cup \{(v_1 v_2)^x \mid x \in G\} \cup \{(y_* n_*)^y \mid y \in O_2(G)H\}$$

then $(G, H, \tilde{K})$ is the envelope of a simple Bruck loop of exponent 4 as we checked on a computer with the help of MAGMA [18].

4. Further properties of the Aschbacher loop

In this section we continue the notation introduced in the previous sections.

4.1. The subloops of $\mathcal{A}$

Lemma 4.1. *$\mathcal{F} := \{x \mid x \in \mathcal{A}, R(x) \in J\}$ is a subloop isomorphic to the group $\mathbb{Z}_2^4$,*

Proof. From the definition of K and the structure of J it is clear, that $\mathcal{F}$ is a subloop isomorphic to $[J, G]$ with loop folder $(JH, H, K \cap J)$. □

Lemma 4.2. *Let $x, y \in \mathcal{A} - \mathcal{F}$ with $x \circ y \notin \mathcal{F}$. Then $\langle x, y\rangle$ is not a soluble loop.*

Proof. Let $t_1 := R(x)$ and $t_2 := R(y)$. The t_i map to transpositions in Sym(5). In case they map to the same transposition, $t_1t_2 \in J$ and therefore $R(x \circ y) \in J$, which implies $x \circ y \in \mathcal{F}$.

If t_1, t_2 map to noncommuting transpositions, the group generated by t_1, t_2 is not a 2-group, therefore the loop to $\langle x, y\rangle$ cannot be soluble.

If t_1, t_2 map to commuting transpositions, we have two cases. The product t_1t_2 maps to some involution in Alt(5) which is either in $B = \langle w, y\rangle$ or not.

Consider the first case. Then $t_1t_2 \in JH = \langle R(x) \mid x \in \mathcal{F}\rangle H$. As this is the enveloping group of $\mathcal{F}$, it follows that $x \circ y \in \mathcal{F}$.

In the other case, as $R(x)R(y)R(x \circ y) \in H$, the element $R(x \circ y)$ can not be in $K \cap J$. Thus $R(x \circ y)$ maps to some transposition. This implies that $R(x)R(y)R(x \circ y)$ maps to some element of odd sign in B and therefore to some element of order 4. Checking all the possibilities in Sym(5) when a product of three transpositions has order 4, we conclude, that $R(x), R(x\circ y)$ and $R(x\circ y), R(y)$ map to pairs of noncommuting transpositions. Therefore $\langle x, y\rangle$ is insoluble as in the previous case. □

Lemma 4.3. *Let $x \in \mathcal{A} - \mathcal{F}$. Then the following hold.*

(a) *$\mathcal{M}_x := \mathcal{F} \cup (x \circ \mathcal{F})$ is a subloop of $\mathcal{A}$ of order* 32.

(b) *$(S, H \cap S, K \cap S)$ is a loop folder to $\mathcal{M}_x$ with $S = N_G(P) \in Syl_2(G)$ where P is the unique Sylow 2-subgroup of JH which is invariant under $R(x)$ (the right translation to x).*

(c) *Let $y \in \mathcal{A} - \mathcal{F}$. Then $\mathcal{M}_x = \mathcal{M}_y$ if and only if $y \in \mathcal{M}_x$.*

(d) *$\mathcal{M}_x$ is non-associative.*

(e) *The subloops $\mathcal{M}_x$ are conjugate under the action of $H \leq Aut(\mathcal{A})$.*

Moreover, the 5 *different subloops $\mathcal{M}_x$ induce a partition of $\mathcal{A} - \mathcal{F}$, the blocks being the nontrivial cosets of $\mathcal{F}$ in $\mathcal{A}$.*

Proof. Let $t := R(x)$. Every transposition in L fixes a unique Sylow 2-subgroup of B, as B acts transitively on the set of transpositions of L with stabilizer of order 2. Therefore every element in $K - J$ is contained in the normalizer of a unique Sylow 2-subgroup of JH, which is a Sylow 2-subgroup of G.

As $\langle w\rangle$ acts transitively on these five Sylow 2-subgroups, we may assume $t \in N_G(\langle J, y_*\rangle)$. In this case $N_G(\langle J, y_*\rangle) = S := \langle y_*, n_*\rangle \in Syl_2(G)$.

We claim that $|K \cap S| = 32$: S maps to $S^\star \in Syl_2(G^\star)$, therefore S contains 16 involutions which map to two transpositions. Together with $K \cap J$ this gives 32 elements. As $KK \cap H = 1$ we have

$$(S \cap K)(S \cap K) \cap \langle y_* \rangle = 1.$$

Notice, that $Z(S) = \langle v_1 v_2 \rangle$, therefore $Z(S) \cap \langle y_* \rangle = 1$ and $\langle y_* \rangle$ is core free in S. We conclude, that $(S, \langle y_* \rangle, K \cap S)$ is a subloop folder to a soluble subloop. The involutions of $G - J$ act nontrivially on $[J, G]$, so the subloop cannot be associative.

As this subloop contains x and $\mathcal{F}$, it contains the subset $\mathcal{M}_x$, which is of size 32, thus closed under multiplication. In particular $\mathcal{F} \circ x = x \circ \mathcal{F}$ and $\mathcal{F}$ is normal in $\mathcal{M}_x$ as it is of index 2.

As H permutes the 2-Sylow-subgroups of JH, it permutes the subloops $\mathcal{M}_x$ too. □

Lemma 4.4. *Every proper subloop of $\mathcal{A}$ is contained in a subloop $\mathcal{M}_x$ for some $x \in \mathcal{A}$.*

Proof. Let $\mathcal{B}$ be a proper subloop of $\mathcal{A}$. If $\mathcal{B}$ is insoluble, it contains an N-loop, whose group of translations is subject to Theorem 4. From the subgroup structure of G it is clear, that there is no such subgroup which is proper. So $\mathcal{B}$ is soluble and $\mathcal{A}$ is an N-loop itself.

The product of every two elements x, y of $\mathcal{B}$, where x and y are not in $\mathcal{F}$, is in $\mathcal{F}$ by Lemma 4.2. This implies that y is contained in $x \circ \mathcal{F}$, see 4.3. Thus $\mathcal{B}$ is contained in $\mathcal{M}_x$. □

4.2. The automorphism group of $\mathcal{A}$

Lemma 4.5. *The element $\alpha := b_2^2$ induces a nontrivial automorphism on G, which centralizes v_1, v_2, v_3, v_4, v_5, v_6, w and G/J. Moreover we have $y_*^\alpha = y_*^5 = y_* v_1$ and $n_*^\alpha = n_* v_3 v_6$.*

Proof. This follows from calculation in the group W. □

Lemma 4.6. *The automorphism group of G is (isomorphic to) $G_1 := G : \langle \alpha \rangle$.*

Proof. Let β be some automorphism of G. Then β acts on the set v_1^G. As G induces on v_1^G the group $PGL_2(5)$ and as $PGL_2(5)$ is a self-normalizing subgroup of $\mathrm{Sym}(6)$, an element $g \in G$ exists, such that βi_g centralizes v_1^G where i_g denotes the inner automorphism of g. Therefore, without loss we may assume, that β centralizes $\langle v_1^G \rangle = J$.

As G/J acts faithfully on J, β acts trivially on G/J. Therefore there exist $v_w, v_y, v_n \in J$ with $\beta(w) = w v_w$, $\beta(y_*) = y_* v_y$ and $\beta(n_*) = n_* v_n$. Using the relations for w, y_*, n_* from the construction section, we get conditions on v_w, v_y, v_n. For instance $w^5 = 1$ gives

$$1 = \beta(w^5) = (w v_w)^5 = w^5 v_w^{w^4 + w^3 + w^2 + w + 1},$$

which is

$$1 = v_w^{w^4+w^3+w^2+w+1}.$$

The action of w, y_*, n_* on J provides us with a system of linear equations. Solving them we get that either $\beta = 1$ or $\beta = \alpha$. □

The next lemma is a general statement, which we will apply in the proof of 4.9.

Lemma 4.7. *If the Bol loop X of exponent 2 to a loop folder (G_X, H_X, K_X) is insoluble, then H_X is not a 2-group.*

Proof. As X is insoluble, it contains subloops Y and Z, such that Z/Y is an N-loop. Therefore there exists a section of H_X which is not a 2-group due to Theorem 4 (a). □

Lemma 4.8. *$(G_1, \langle H, \alpha\rangle, K)$ is a faithful loop folder but not a loop envelope.*

Proof. The action of α on G is such that $H_1 := H\langle\alpha\rangle = \langle H, \alpha\rangle$ and K gives a loop folder to a Bol loop of exponent 2. (The relation $KK \cap H_1 = 1$ is obvious.) It is $\langle K\rangle = G < G_1$. Therefore, (G_1, H_1, K) is not a loop envelope. As H_1 is core free in G_1, it is a faithful loop folder. □

Lemma 4.9. *If (G_1, H_*, K_*) is a loop folder to a Bol loop of exponent 2, then $H_* = H_1$ and $K_* = K$. In particular, the loop is the Aschbacher loop.*

Proof. Notice, that every involution in $G_1 - O_2(G_1)$ is already contained in $G - J$: For t a transposition $C_{O_2(G_1)}(t) = C_J(t)$, so the number of involutions with the same image in $G_1/O_2(G_1)$ is 8 as it is in G.

Further, G_1 still has no involutions, which map to involutions in $L' \cong \mathrm{Alt}(5)$, which can be seen from the structure of H_1: Such an involution would invert some element of order 5, thus normalizes some Sylow-5-subgroup of G_1, see [2, 8.1 (1)]. But H_1 is the normalizer of a Sylow-5-subgroup, containing no such involutions.

If $K_* \subseteq O_2(G_1)$, then H_* covers $G/O_2(G_1)$. The only proper such subgroup H_* is G, but then $|K_*| = 2$ is impossible. Therefore, all the involutions in $G_1 - O_2(G_1)$ are in K_* (see (8) of Section 3).

Hence, there are involutions in K_* whose product is of order divisible by 3. This implies that H_* is either a 2-group or a $\{2,5\}$-group, of order at most

$$\frac{2|G|}{1+80} < 94.$$

As there are 143 involutions in $G\langle\alpha\rangle$, we get

$$|H_*| > \frac{2|G|}{1+143} > 53.$$

In particular, $|G : H_*|$ is even, which yields that K_* contains beside the identity the unique conjugacy class of involutions of odd length (namely 15). Thus $|K_*| \geq 96$ and $|H_*| \leq 80$. If H_* is a $\{2,5\}$-group, it is either 5-closed, so without loss

$H_* = H_1$, or 2-closed. The latter case does not produce a loop folder as the unique subgroup H_* in question intersects already nontrivially with K_*.
The case of H_* being a 2-group is impossible by Lemma 4.7, but also by some easy inspection of G_1, as then $|K_*| = 120$ and no such union of G_1-conjugacy classes of involutions exists. □

Lemma 4.10. *The automorphism group of the loop $\mathcal{A}$ is of size 80 and it is induced by H_1.*

Proof. Let $a, b \in \mathcal{A}$ and $\alpha \in Aut(\mathcal{A})$. Then

$$a^{\alpha R(\alpha(b))} = \alpha(a)^{R(\alpha(b))} = \alpha(a) \circ \alpha(b) = \alpha(a \circ b) = \alpha(a^{R(b)}) = a^{R(b)\alpha},$$

which gives $\alpha^{-1}R(b)\alpha = R(\alpha(b))$.

Thus every automorphism of the loop induces an automorphism on the group $G = \langle R(a) \mid a \in \mathcal{A} \rangle$ and fixes H, the stabilizer in G of $1 \in \mathcal{A}$. In particular the subgroup of $\mathrm{Sym}(\mathcal{A})$ generated by G and $Aut(\mathcal{A})$ contains G as a normal subgroup, containing its own centralizer. Therefore $Aut(\mathcal{A})$ is a subgroup of $G : \langle \alpha \rangle$, which contains H_1.

In the previous lemma we just proved, that H_1 induces automorphisms on $\mathcal{A}$.

A subgroup of $G\langle \alpha \rangle$ which contains H_1 properly is a union of H_1-cosets. Therefore, it contains elements of $K - 1$. The elements of K are the right translations of $\mathcal{A}$ which do not fix the 1-element of $\mathcal{A}$, except in the trivial case. So translations are almost never automorphisms and H_1 is the group of automorphism of $\mathcal{A}$. □

Lemma 4.11. *Let X be a finite Bol loop containing a subloop Y isomorphic to $\mathcal{A}$. Then $G \cong \langle R(x) \mid x \in Y \rangle \leq \langle R(x) \mid x \in X \rangle$.*

Proof. The group generated by $\{R(x) \mid x \in Y\}$ is a homomorphic image of the abstract group G_0, which is generated by free generators $R_x, x \in \mathcal{A}$ subject to the relations $R_x^2 = 1, R_1 = 1, R_{(x \circ y) \circ x} = R_x R_y R_x$ for $x, y \in \mathcal{A}$.

The latter relation expresses the Bol identity. In fact they describe the conjugacy action of the elements in K on themselves. Therefore, G_0 is a central extension of G.

We verified using the Todd-Coxeter algorithm on the trivial group, that in our case $G_0 \cong G$ and it is clear, that no proper homomorphic image of G can be the enveloping group of a subloop of size $|\mathcal{A}| = 96$. □

4.3. The embedding of G into some almost simple groups

First of all we present an embedding of G into $GL_8(2)$ by writing down $(8 \times 8)GF(2)$-matrices for w, y_* and n_*. Let

$$W := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \qquad Y := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$N_1 := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \qquad N_2 := \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$
$$E_1 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ and } E_2 := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $w := \begin{pmatrix} W & 0 \\ 0 & W \end{pmatrix}$, $y_* := \begin{pmatrix} Y & 0 \\ E_1 & Y \end{pmatrix}$ and $n_* := \begin{pmatrix} N_1 & 0 \\ E_2 & N_2 \end{pmatrix}$ defines a faithful embedding of $G = \langle w, y_*, n_* \rangle$ into $GL_8(2)$.
Notice, that the two 4-dimensional $GF(2)$-modules for $P\Gamma L_2(4) \cong \mathrm{Sym}(5) = \langle w, y, n \rangle$ defined by W, Y, N_1 and W, Y, N_2, respectively, are not isomorphic. This yields that G is a subgroup of $\tilde{G}$ as defined in 4.12(g).

The following is known about embeddings of G into almost simple groups and stated without proof:

Lemma 4.12. (a) *The smallest faithful linear $GF(2)$-representations are of degree 8, and fix no form.*

(b) *The smallest faithful semilinear $GF(4)$-representations have degree 6.*

(c) *The smallest faithful linear k-representations where k is a field of odd or zero characteristic are of degree 15.*

(d) *The minimal permutation degree of G is 40.*

(e) *G embeds into $2^{12\cdot}M_{24} \leq Fi_{24}$ and therefore also into the Monster M. It does not embed into the simple group Fi_{24}'. The embedding into the BabyMonster BM is open. The group does not embed into the other sporadic almost simple groups.*

(f) *G is not a subgroup of the Dempwolf group.*

(g) *G embeds into $\tilde{G} := 2^{16} : \mathrm{Sym}(5)$ where $O_2(\tilde{G})$ is the tensor product of the two non-isomorphic $GF(2)\mathrm{Sym}(5)$-modules.*

5. Proof of Theorem 2

Let $\mathcal{B}$ be a loop which is a simple Bol loop of exponent 2 with at most 96 elements and which is not soluble. We may assume that $\mathcal{B}$ is minimal with that condition, i.e. an N-loop in the language of [2]. Let (G, H, K) be a faithful loop envelope of $\mathcal{B}$. Then according to Theorem 4 (1) as stated below holds.

(1) $G^\star := G/O_2(G) \cong PGL_2(q)$ and $|\mathcal{B}| = |K| = n_1 2^n(2^{n-1}+1)$ where $n_1 = |K \cap aO_2(G)|$ with $a \in K - O_2(G)$ and $q = 2^n + 1$. Moreover, $H^\star$ is a Borel subgroup of $G^\star$ and $K^\star$ consists of all the involutions in $G^\star$ which are not in $G^{\star\prime}$.

(2) $q = 5$ and $n = 2$:
There are $(q-1)q/2$ involutions in $PGL_2(q) - PSL_2(q)$. Therefore $q \leq 14$, so $q = 5$ or $q = 9$. In case $q = 9$ there are 36 involutions in $G^\star$ which are not in

$(G^\star)' \cong PSL_2(9)$. Hence, there is an orbit of G on the set of involutions in $G-G'$ which is a multiple of 36. As the size of the loop is at most 96, it follows that this number is 36 or 72. Then these involutions centralize $O_2(G)$ or a subgroup of index 2 in $O_2(G)$. The first case is not possible, as $C_G(O_2(G))$ is contained in $O_2(G)$ (Theorem 4 (b)). Hence there are 72 involutions and the index of the centralizer in $O_2(G)$ of such an involution in $O_2(G)$ is 2. In particular, the product of every two of these involutions centralize a subgroup of index 4, so its centralizer has index 4 or less. As $PGL_2(9)$ has outer involutions whose product is of order 5, these elements can not act non-trivially on $O_2(G)$. Hence, $q = 5$ and $n = 2$.

(3) $|K| \in \{24, 48, 96\}$:
As $n = 2$, we have $|K| = n_1 \cdot 12$. On the other hand $|K| = |G : H| = 2^m \cdot 3$ for some $m \in \mathbb{N}$.

(4) G acts transitively, but imprimitivily on the set of cosets of H in G with blocks of imprimitivety $\{Hk\ |k \in K$ and $Hk \subseteq O_2(G)Ha\}$, $a \in G$. There are 6 blocks, say $B_1 \subseteq O_2(G)H, B_2, \ldots, B_6$, each of size $2n_1$ and $G^\star \cong PGL_2(5)$ acts on the set of blocks in its action of degree 6:
This follows immediately from the fact that $H \leq O_2(G)H$ and that the latter is a maximal subgroup of G of index 6.

(5) $|O_2(G) \cap K| = |K \cap (O_2(G)H)| = |B_1|$:
According to Theorem 4(c) $|O_2(G) \cap K| = n_0 = 2n_1$, which equals the size of B_1

$$2n_1 = |B_1| = |K \cap (O_2(G)H)|$$

by (4).

(6) Let $i \in \{1, \ldots, 6\}$ and n and m be elements in B_i. Then there is precisely one element t in $O_2(G) \cap K$ such that n^t equals m:
If $o \in O_2(G)$, we can write $o = hk$ with $h \in H, k \in K$ as (G, H, K) is a loop folder. Then $ok = h$. Using the homomorphism of G onto $G/O_2(G) \cong \mathrm{Sym}(5)$ we see, that this implies $k, h \in O_2(G)$. Therefore, $O_2(G) \cap K$ is a transversal to $H \cap O_2(G)$ in $O_2(G)$ and to H in $O_2(G)H$. As $O_2(G) \cap K$ is a G-normal subset, it is a transversal to H^g in $O_2(G)H^g$ for every $g \in G$. In particular it is a transversal to a point stabilizer in a block stabilizer to that point.

(7) Let w be an element of order 5 in H. Then w acts non-trivially on B_1:
Assume that w is in the kernel M_1 of the action of H on B_1.

(7.1) $[w, O_2(G) \cap K] = 1$:
Let t be an element in $O_2(G) \cap K$. Then $w^{-1}twt$ is in M_1. Therefore, the product $t^w t$ of the two elements t^w and t of K lies in H. This implies that $t^w = t$. Hence, $[w, O_2(G) \cap K] = 1$.

(7.2) This implies that $[\langle w^G \rangle, O_2(G) \cap K] = 1$. Set $L := \langle w^G \rangle$. Then, as $G/O_2(G) \cong PGL_2(5) \cong Sym(5)$, the group $L^\star$ is isomorphic to $\mathrm{Alt}(5)$.

Let y be an element in L which inverts w. Then according to [2, 12.9 (4)] y is not an involution. We may assume that y is an element whose order is a power of 2. Then $v := y^2$ is a non-trivial 2-element in $O_2(G) \cap L$. As $G^\star$ acts on the set of blocks as the group $PGL_2(5)$, the element y fixes the block B_1, as well as a further block, say B_2.

(7.3) $v \in M_1$:
If v fixes a point in B_1, then, as $[v, O_2(G) \cap K] = 1$ by choice of y, the statement (6) implies that v fixes every point in B_1 and that $v \in M_1$. If v does not fix a point in B_1, then the cycle decomposition of y on B_1 contains a cycle of length at least 4, which contradicts $[y, O_2(G) \cap K] = 1$ and (6). Thus v is in M_1.

(7.4) The contradiction. Precisely the same argument as in the last paragraph yields that $v \in M_2$. As w permutes the 5 blocks, $B_2, \ldots, B_6$, and as $[w, v] = 1$, it follows that v is in M_i, for $1 \leq i \leq 6$. Thus v fixes every element in $B_1 \cup \cdots \cup B_6$, which contradicts the fact that (G, H, K) is a faithful loop envelope, see the introduction.

(8) $H^\star \cong \mathbb{Z}_5 : \mathbb{Z}_4$ acts faithfully on B_1 and on $K \cap O_2(G)$:
This is an immediate consequence of the nontrivial action of elements of order 5 by (7).

(9) $|K| = 96$, $|B_1| = 16$ and G induces on B_1 a group of type $\mathbb{Z}_2^4 : (\mathbb{Z}_5 : \mathbb{Z}_4)$, acting transitively on 16 points:
By (6) $(O_2(G)H, H, K \cap O_2(G))$ is a loop folder to a subloop $\mathcal{C}$ of $\mathcal{B}$ of size $|B_1|$. As H is core free in G, it acts as group of automorphisms on $\mathcal{B}$. By (8) H has an element which induces on B_1 a nontrivial automorphism of order 5. As $\mathcal{C}$ is proper, it is soluble, thus has a chain of derived subloops with quotients being elementary abelian.
Nontrivial action of an automorphism of order 5 can only happen in case that this loop has size 16 and is elementary abelian: If an automorphism is trivial on both a normal subloop and its quotient and fixes an element outside the normal subloop, it fixes the entire coset of this element by the automorphism property. In particular, every non trivial automorphism of order 5 acts on some elementary abelian section of the loop of order at least 16. From (3) we get $|K| = 96$ and $|B_1| = 16$.

Hence $O_2(G)H$ induces on B_1 at least a group $\mathbb{Z}_2^4 : (\mathbb{Z}_5 : \mathbb{Z}_4)$, where the subgroup isomorphic to $\mathbb{Z}_2^4$ is induced from $\langle K \cap O_2(G) \rangle$, which is the enveloping group of $\mathcal{C}$. (6) implies that $\langle K \cap O_2(G) \rangle$ acts as a transitive normal subgroup of $O_2(G)H$ on B_1. Thus the structure of $A_8 = L_4(2) = Aut(\mathbb{Z}_2^4)$ and that of $O_2(G)H$ yields the second part of claim (9).

(10) G is either isomorphic to the group of the Aschbacher loop or to its automorphism group:
This result is based on heavy computer calculations. We describe here, which calculations the computer did and what our conclusions were.

As shown in (9) we can embed G into the full wreath product W of the action of $O_2(G)H$ on a block with $G/O_2(G) \cong$ Sym(5) acting transitively on the 6 blocks. This group is a transitive subgroup of Sym(96) and in this permutation representation the computer calculated.

By (9) we know, that an element $w \in G$ of order 5 fixes exactly one point in the loop. Calculation inside a Sylow-5-subgroup of W and additional conjugacy tests in W show, that all such elements are conjugate in W. So we pick one of them.

We can calculate $C_W(w)$, which is of shape $\mathbb{Z}_5^2 \times (\mathbb{Z}_2^4 : (\mathbb{Z}_5 : \mathbb{Z}_4))$, and $N_W(\langle w \rangle)$, which gets by factor 4 bigger. We determine the conjugacy classes of the cyclic subgroups $\langle y \rangle$ of $N_W(\langle w \rangle)$, which are of 2-power order at least 8 and induce on $\langle w \rangle$ a group of order 4. There exist two classes of these subgroups, both of order 8. So we found subgroups of G which are isomorphic to $\mathbb{Z}_5 : \mathbb{Z}_8$.

In the next step we calculate all the candidates for $N_G(\langle w \rangle)$ up to conjugacy in $N := N_W(\langle w \rangle)$. This is done by the following trick:

We have already a candidate N_{i-1}, which may be a subgroup of even index in our candidate. So we pick $T \in Syl_2(N_{i-1})$ and calculate a transversal to T in $N_N(T)$. For each element x in this transversal we consider $\langle N_{i-1}, x \rangle$ as a new candidate, provided this group does not contain involutions, which map to involutions in A_5, as by [2, 12.9 (4)] G does not contain such involutions.

From the two initial cyclic candidates for a 2-Sylow of $N_G(\langle w \rangle)$ one gets only two more candidates for $N_G(\langle w \rangle)$, which are isomorphic to each other, one new candidate to each cyclic candidate. The Sylow-2-subgroup of these candidates is the modular group of size 16.

We have now 4 subgroups of W, which are candidates for subgroups of G and contain $N_G(\langle w \rangle)$. We use the normalizer-transversal-trick as before to look in the lattice of overgroups in W for candidates of G: In fact we determine all overgroups Y of our 4 candidates N_1, N_2, N_3, N_4 with the following properties:

- $N_Y(\langle w \rangle) = N_{N_i}(\langle w \rangle)$ and
- $O_2(Y)$ is of index 20 or 120, and either $Y = O_2(Y)N_i$ or $Y/O_2(Y) \cong \mathrm{Sym}(5)$.

Given a candidate Y, we pick $T \in Syl_2(Y)$, calculate $N_W(T)$ and a transversal to T in it. For each x in this transversal, we calculate $Y_x := \langle Y, x \rangle$. Next we check whether Y_x satisfies the conditions above, in which case we keep it as a new candidate.

In a final step we drop the groups with $O_2(Y)$ of index 20 and keep only those subgroups Y, which contain a core free subgroup of shape $\mathbb{Z}_5 : \mathbb{Z}_8$ and a conjugacy class of transpositions of length less or equal to 80. Here we use the fact, that if Y is the group to a Bol loop folder (Y, H_Y, K_Y), H_Y contains such a core free subgroup and K_Y contains such a conjugacy class of transpositions.

Computer calculations show that there are only the two isomorphism types, the group to the Aschbacher loop and its automorphism group: Two of the candidates, one of shape $5 : 8$, the other of shape $5 : Mod_{16}$ (containing the first) did not have any overgroups Y with $N_Y(\langle w \rangle) = N_{N_i}(\langle w \rangle)$ and $|Y : O_2(Y)| = 120$.

The third candidate of shape $5 : 8$ produced 4 conjugate subgroups isomorphic to the group to the Aschbacher loop, and the final one (of shape $5 : Mod_{16}$) produced 12 conjugate subgroups isomorphic to the automorphism group of the group to the Aschbacher loop.

(11) The loop is the Aschbacher loop:
This follows from Lemma 4.9 and the structure of the groups in question.

References

[1] Albert, A. A.: *Quasigroups II.* Trans. Am. Math. Soc **55** (1944), 401–419. Zbl 0063.00042

[2] Aschbacher, M.: *On Bol loops of exponent* 2. J. Algebra **288** (2005), 99–136. Zbl 1090.20037

[3] Aschbacher, M.; Kinyon, M.; Phillips, J. D.: *Finite Bruck loops*. Trans. Am. Math. Soc. **358**(7), 3061–3075. Zbl 1102.20046

[4] Baer, R.: *Nets and groups*. Trans. Am. Math. Soc. **46** (1939), 110–141. Zbl 0022.01105

[5] Bruck, R. H.: *A survey of binary systems*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge **20**. Reihe: Gruppentheorie, Springer Verlag, Berlin etc. 1958. Zbl 0081.01704

[6] Baumeister, B.; Stein, A.: *On simple Bol loops of exponent* 2. Preprint 2007, 25 pages.

[7] Burn, R. P.: *Finite Bol loops*. Math. Proc. Camb. Philos. Soc. **84** (1978), 377–385. Zbl 0385.20043

[8] Carter, R.: *Simple Groups of Lie Type*. Pure and Applied Mathematics. **28**, John Wiley and Sons, London 1972. Zbl 0248.20015

[9] Glauberman, G.: *On loops of odd order*. J. Algebra **1** (1964), 374–396. Zbl 0123.01502

[10] Glauberman, G.: *On Loops of odd order II.* J. Algebra **8** (1968), 393–414. Zbl 0155.03901

[11] Hall, J. I.: *A characterization of the full wreath product*. J. Algebra **300** (2006), 529–554. Zbl 1163.20019

[12] Hall, J. I.: *Central automorphisms of latin square designs and loops*. Quasigroups Relat. Syst. **15**(1) (2007), 19–47. Zbl 1137.20052

[13] Heiss, S.: *Self-invariant* 1*-factorizations of complete graphs*. Preprint 1998.

[14] Kiechle, H.: *The Theory of K-Loops*. Lecture Notes in Mathematics **1778**, Springer, Berlin, Heidelberg, New-York 2002.

[15] Kinyon, M. K.: *Global left loop structures on spheres*. arXiv:math/9910111v2 2000.

[16] Kreuzer, A.: *Inner mappings of Bruck loops*. Math. Proc. Camb. Philos. Soc. **123** (1998), 53–57. Zbl 0895.20052

[17] Liebeck, M. W.: *The classification of finite Moufang loops*. Math. Proc. Camb. Philos. Soc. **102** (1987), 33–47. Zbl 0622.20061

[18] MAGMA Computational Algebra System, Version V2.14-14. http://magma.maths.usyd.edu.au/magma/ (2007).

[19] Nagy, G.: *A class of simple proper Bol loops*. Preprint 2007.

[20] Nagy, G.: *Finite simple left Bol loops*. http://www.math.u-szeged.hu/ nagyg/pub/simple_bol_loops.html

[21] Personal communication with many, 1998–2007.

[22] Robinson, D. A.: *Bol loops*. Trans. Am. Math. Soc. **123** (1966), 341–354. Zbl 0163.02001

[23] Ungar, A. A.: *Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession: The Theory of Gyrogroups and Gyrovectors Spaces*. Kluwer Academic Publishers, Dordrecht-Boston-London 2001. Zbl 0972.83002

Received December 8, 2008