A class of simple proper Bol loops

Gábor P. Nagy

March 30, 2022

The existence of finite simple non-Moufang Bol loops was considered as one of the main open problems in the theory of loops and quasigroups. In this paper, we present a class of proper simple Bol loops. This class also contains finite and new infinite simple proper Bol loops.

1 Preliminaries

For a loop $Q$, we call the maps $L_a(x) = ax, R_a(x) = xa$ left and right translations, respectively. These are permutations of $Q$, generating the left and right multiplication groups $\text{LMlt}(Q), \text{RMlt}(Q)$ of $Q$, respectively. The group closure $\text{Mlt}(Q)$ of $\text{LMlt}(Q)$ and $\text{RMlt}(Q)$ is the full multiplication group of $Q$. Just like for groups, normal subloops are kernels of homomorphisms of loops. The loop $Q$ is simple if it has no proper normal subloop. The commutator-associator subloop $Q'$ is the smallest normal subloop of $Q$ such that $Q/Q'$ is an Abelian group. For basic introductory reference on loops see [11].

The loop $Q$ is a left (right) Bol loop if the identity $x(y(xz)) = (x(yx))z (((xy)z)y = x((yz)y))$ holds in $Q$. Loops which satisfy both identities are called Moufang loops.

For any field $F$, L. J. Paige [10] constructed a simple nonassociative Moufang loop $M(F)$. Using the classification of finite simple groups, M. Liebeck [5] showed that the only finite simple nonassociative Moufang loops are $M(\mathbb{F}_q)$. The existence of finite simple non-Moufang Bol loops was considered as the one of the main open problems in the theory of loops and quasigroups, cf. [12] and [1, Question 4].

In this paper, Bol loops are left Bol loops and with proper Bol loops we mean left Bol loops which are not Moufang.

2 Bol loops as sections in groups

Let $Q$ be a Bol loop, $G$ the group generated by the left translations of $Q$, $H$ the stabilizer of 1 in $G$ and $S$ the set of left translations. ($S$ is called the left section of the loop.) It is widely known that the triple $(G, H, S)$ satisfies the following properties:

*This paper was written during the author’s Marie Curie Fellowship MEIF-CT-2006-041105.
Therefore, $N = \text{structure of the Bol loop}$.

Proof. Let $\phi = \text{Lemma 2.1.}$ Let $\phi$ be a surjective homomorphism: $\text{then the map } \tilde{\phi} = \text{Lemma 2.2.}$ Let $\sigma$ be an Abelian group and assume $\phi : Q \rightarrow A$ is a surjective homomorphism. Then the map $\tilde{\phi} : L_x \mapsto \varphi(x)$ extends to a surjective homomorphism $G \rightarrow A$. Indeed, if $L_{x_1} \cdots L_{x_n} = 1$ then $x_1(x_2(\cdots x_n)) = 1$ and

$$\varphi : \hat{G} = \langle S \rangle \rightarrow \text{LMlt}(S, \circ), \quad s \mapsto L_s = \alpha^{-1}s\alpha.$$  

The kernel of $\varphi$ is the largest normal subgroup of $\hat{G}$ contained in $H \cap \hat{G}$. If the permutation representation of $\hat{G}$ on the left cosets of $H$ is faithful, that is, if $H$ contains no proper normal subgroup of $G$, then $\varphi$ is a bijection.

In the remaining of this section, we show some folklore results which connect the structure of the Bol loop $Q$ and its left multiplication group.

**Lemma 2.1.** Let $Q$ be a loop with left multiplication group $G = \text{LMlt}(Q)$. Then $Q = Q'$ if and only if $G'$ acts transitively on $Q$.

**Proof.** Let $A$ be an Abelian group and assume $\varphi : Q \rightarrow A$ is a surjective homomorphism. Then the map $\tilde{\varphi} : L_x \mapsto \varphi(x)$ extends to a surjective homomorphism $G \rightarrow A$. Indeed, if $L_{x_1} \cdots L_{x_n} = 1$ then $x_1(x_2(\cdots x_n)) = 1$ and

$$\tilde{\varphi}(L_{x_1}) \cdots \tilde{\varphi}(L_{x_n}) = \varphi(x_1) \cdots \varphi(x_n) = \varphi(x_1(x_2(\cdots x_n))) = \varphi(1) = 1.$$  

Moreover, $N = \ker \tilde{\varphi}$ contains the stabilizer $G_1$ of the unit element of $Q$ in $G$:

$$\tilde{\varphi}(L_x^{-1}L_xL_y) = \varphi(xy)^{-1}\varphi(x)\varphi(y) = 1.$$  

Therefore, $N$ and $G' \leq N$ are not transitive. Conversely, if $G'$ is not transitive then $N = G'G_1$ is a proper normal subgroup of $G$. Then the map $\varphi : Q \rightarrow G/N$, $\varphi(x) = L_xN$ is a surjective homomorphism:

$$\varphi(x)\varphi(y) = L_xNL_yN = L_{xy}L_{xy}^{-1}L_xL_yN = L_{xy}N = \varphi(xy).$$  

**Lemma 2.2.** Let $Q$ be a Bol loop and let $\sigma$ be an automorphism of $\text{LMlt}(Q)$ such that $L_x^\sigma = L_x^{-1}$ for all $x \in Q$. Let $K$ be proper normal subloop of $Q$. Then, $K = N(1)$ for some $\sigma$-invariant normal subgroup $N$ of $\text{LMlt}(Q)$. In particular, $Q$ is simple if all $\sigma$-invariant normal subgroups of $\text{LMlt}(Q)$ act transitively on $Q$. 

\[2\]
Proof. Put $G = \text{LMlt}(Q)$ and define the subset

$$M = \{ g \in G \mid g(yK) = yK \text{ for all } y \in Q \}.$$  

of $G$. Clearly, $M \triangleleft G$ and $L_x \in M \cap M^\sigma$ for all $x \in K$. For the $\sigma$-invariant normal subgroup $N = M \cap M^\sigma$, $K = N(1)$ holds.

We notice that for any simple proper Bol loop $Q$, the left multiplication group possesses an involutorial automorphism $\sigma$ with $L_x^\sigma = L_x^{-1}$ for all $x \in Q$.

The bijection $u : Q \to Q$ is a left pseudo-automorphism of the loop $Q$ with companion element $c \in Q$ if

$$cu(x) = (cu(x))u(y)$$

holds for all $x, y \in Q$. Equivalently, $u(1) = 1$ and $L_c u L_x = L_{cu(x)} u$ for all $x \in Q$.

Two loops $(Q, \cdot)$ and $(K, \circ)$ are isotopes if bijections $\alpha, \beta, \gamma : Q \to K$ exist such that $\alpha(x) \circ \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q$. The loop $Q$ is a $G$-loop if it is isomorphic to all its isotopes.

Lemma 2.3. Let $Q$ be a left Bol loop and let us denote by $S$ the set of left translations of $Q$. The loop $Q$ is a $G$-loop if and only if for all $c \in Q$ there is a permutation $u$ of $Q$ such that $u(1) = 1$ and $uSu^{-1} = L_c^{-1}S$ hold.

Proof. Combining Theorem III.6.1 and IV.6.16 of [11], we see that a left Bol loop is a $G$-loop if and only if every element of $Q$ occurs as a companion of some left pseudo-automorphism. Let $c \in Q$ be given and let $u : Q \to Q$ be a bijection such that $u(1) = 1$ and for all $x \in Q$ holds $uL_xu^{-1} = L_{c^{-1}L_x}$, where $x' \in Q$ depends on $x, c$ and $u$. Then, $x' = cu(x)$ and $u$ is a left pseudo-automorphism with companion $c$.

We close this section with a lemma on the left multiplication groups of nonproper Bol loops.

Lemma 2.4. Let $Q$ be a simple Moufang loop. Then $\text{LMlt}(Q)$ is a simple group.

Proof. If $Q$ is a simple group, then $\text{LMlt}(Q_T) \cong Q_T$ is simple. The left and right Bol identities can be written in the form

$$R_{xz}R_z^{-1} = L_x^{-1}R_zL_x, \quad L_{xy}L_y^{-1} = R_y^{-1}L_xR_y.$$  

This means that for Moufang loops, the left and right multiplication groups are normal in the full multiplication group. Theorem 4.3 of [8] says that for an arbitrary nonassociative simple Moufang loop $Q$, the multiplication group is simple. Hence, $\text{LMlt}(Q) = \text{RMlt}(Q) = \text{Mlt}(Q)$ is a simple group.

3 Construction of left Bol loops using exact factorizations of groups

Definition 3.1. The triple $(X, Y_0, Y_1)$ is called an exact factorization triple if $X$ is a group, $Y_0, Y_1$ are subgroups of $X$ satisfying $Y_0 \cap Y_1 = 1$ and $Y_0Y_1 = X$. The exact factorization triple $(X, Y_0, Y_1)$ is faithful if $Y_0, Y_1$ do not contain proper normal subgroups of $X$.
If \( Y_1 \) does not contain any proper normal subgroup of \( X \), then an equivalent definition of exact factorization triples is that \( Y_0 \) is a regular subgroup in the permutation representation of \( X \) on the cosets of \( Y_1 \). In the mathematical literature, the group \( X \) is also called the \textit{Zappa-Szép product} of the subgroups \( Y_0, Y_1 \).

**Proposition 3.2.** Let \( \mathcal{T} = (X, Y_0, Y_1) \) be a faithful exact factorization triple. Let us define the triple \((G, H, S)\) by

\[
G = X \times X, \quad H = Y_0 \times Y_1 \leq G, \quad S = \{(x, x^{-1}) \mid x \in X\}.
\]

Then \((G, H, S)\) is a Bol loop folder. The associated left Bol loop \((S, \circ)\) is a \(G\)-loop.

**Proof.** We first show that \( S \) is a left transversal for all conjugates of \( H \). Let \( a, b \in X \) be arbitrary elements; we can write \( a^{-1} = a_0a_1 \) and \( b = b_0b_1 \) in a unique way with \( a_0, b_0 \in Y_0 \) and \( a_1, b_1 \in Y_1 \). We have

\[
\exists x \in X : (x, x^{-1}) \in (a, b)H \iff \exists y_0 \in Y_0, y_1 \in Y_1 : ay_0 = y_1^{-1}b^{-1} = \iff \exists y_0 \in Y_0, y_1 \in Y_1 : a^{-1}a_0^{-1}y_0 = y_1^{-1}b_1^{-1}b_0^{-1} = \iff \exists y_0 \in Y_0, y_1 \in Y_1 : a_0^{-1}y_0b_0 = a_1y_1^{-1}b_1^{-1} \in Y_0 \cap Y_1.
\]

Since \( Y_0 \cap Y_1 = 1 \), we obtain \( y_0 = a_0b_0^{-1}, y_1 = b_1^{-1}a_1 \) and the unique element of \((a, b)H \cap S\) is \((a_1b_0^{-1}, b_0a_1)\). This shows that \( S \) is a left transversal to \( H \) in \( G \). In order to prove the same fact for the conjugates of \( H \), let us take an arbitrary \( g \in G \) and write \( g = sh \); we have \( H^g = H^s \). For \( a \in G \) let us define \( t \in S \) as the unique element of \( S \cap aH^s \). This proves \((F1)\) and \((F2)\).

Let \( b \in X \) and write \( b = y_0y_1^{-1} \) with \( y_0 \in Y_0, y_1 \in Y_1 \). Then

\[
(y_0, y_1)(a, a^{-1})(y_0, y_1)^{-1} = (b, b^{-1})(y_1a_0^{-1}, y_0a^{-1}y_1^{-1}) \in (b, b^{-1})S.
\]

Since \( b \in X \) is arbitrary and \((y_0, y_1) \in H \), Lemma 2.3 implies that \((S, \circ)\) is a \(G\)-loop. \(\square\)

**Definition 3.3.** Let \( \mathcal{T} = (X, Y_0, Y_1) \) be a faithful exact factorization triple and let us define \( G, H, S \) as in Proposition 3.2. The Bol loop corresponding to the Bol loop folder \((G, H, S)\) will be denoted by \(Q_\mathcal{T}\).

**Lemma 3.4.** Let \( \mathcal{T} = (X, Y_0, Y_1) \) be a faithful exact factorization triple and let us define \( G, H, S \) as in Proposition 3.2. Then \( \operatorname{LMIt}(Q_\mathcal{T}) \) is isomorphic to \( \bar{G} = \langle S \rangle \cong X.X' \triangleleft G \).

**Proof.** We claim that \( H \) contains no normal subgroup of \( G \). Indeed, the projections of \( H \) to the direct factors of \( G = X \times X \) are \( Y_0, Y_1 \) which contain no normal subgroup of \( X \). Thus a normal subgroup of \( H \) must have trivial projections, hence it must be trivial. Therefore, the permutation action of \( G \) on the left cosets of \( H \) is faithful and we can consider \( G \) as a permutation group. Moreover, by the definition of \( Q = Q_\mathcal{T} \), the left translations are precisely the permutations induced by the elements of \( S \). This proves the lemma. \(\square\)

**Proposition 3.5.** Let \( \mathcal{T} = (X, Y_0, Y_1) \) be a faithful exact factorization triple such that \( X'Y_0 = X'Y_1 = X \) and let us define \( G, H, S \) as in Proposition 3.2. Then
(i) $\hat{G}H = G$ with $\hat{G} = \langle S \rangle$.

(ii) $Q_T^r = Q_T$. In particular, $Q_T$ is not solvable.

Proof. Since $X' \times X' \leq \hat{G}$, we have $X'' \times X'' \leq \hat{G}'$. By $1 \times Y_1 \leq H$ and $X''Y_1 = X$, we obtain $1 \times X \leq \hat{G}'H$. Clearly, for any $a, b \in X$, $([a, b], [a^{-1}, b^{-1}]) \in \hat{G}'$, thus $([a, b], 1) \in \hat{G}'H$. This implies $X' \times 1 \leq \hat{G}'H$, hence $X \times 1 \leq \hat{G}'H$ by $Y_0 \times 1 \leq H$ and $X'Y_0 = X$. This proves (i). Lemma 3.4 says that $\hat{G}$ is isomorphic to the left multiplication group of $Q$ and the commutator subgroup of $\hat{G}$ acts transitively on the left cosets of $H$ in $G$. Therefore, (ii) follows from Lemma 2.1.

We call the group $X$ almost simple if $T \leq X \leq \text{Aut}(T)$ for some nonabelian simple group $T$. The group $T$ is the socle of $X$.

**Theorem 3.6.** Let $X$ be an almost simple group with socle $T$. Let $T = (X,Y_0,Y_1)$ be a faithful exact factorization triple and assume $X = TY_0 = TY_1$. Then $Q_T$ is a simple proper left Bol loop.

Proof. Let $\sigma$ be the automorphism of $G$ mapping $(a, b) \mapsto (b, a)$. Since $S^\sigma = S$, we have $\hat{G}^\sigma = \hat{G}$ and $\text{LMlt}(Q_T)$ has an automorphism which inverts the left translations. Clearly, $T \times T \leq X' \times X' \leq \hat{G}$ and every $\sigma$-invariant normal subgroup of $\hat{G}$ contains $T \times T$. However, $T \times T$ is transitive by assumption, thus, $Q_T$ is simple by Lemma 2.2. Moreover, $Q$ is proper Bol by Lemma 2.4.

**4 Some classes of simple proper Bol loops**

In this section we present some finite and infinite simple proper Bol loops by applying the construction of Proposition 3.2.

**Example I:** Put $X = \text{PSL}(n, 2)$, let $Y_0$ be a Singer cycle and $Y_1$ be the stabilizer of a projective point. Then $Q_{(X,Y_0,Y_1)}$ is a finite simple proper Bol loop by Theorem 3.6. We notice that many other finite simple groups have exact factorizations. The factorizations of finite groups are intensively studied, cf. [6], [4] and the references therein.

**Example II:** Let $n$ be an even integer and put $X = S_n$, $Y_0 = \langle (1,2,\ldots,n) \rangle$ and $Y_1 = S_{n-1}$ with $n \geq 4$. Define the loop $Q_n = Q_{(X,Y_0,Y_1)}$. If $n \geq 6$ then $Q_n$ is simple by Theorem 3.6. If $n = 4$ then by Proposition 3.5 $Q_4$ is a nonsolvable Bol loop of order 24. It is known that all Bol loops of order at most 12 are solvable, thus, $Q_4$ is simple. We emphasize the fact that the left multiplication group of $Q_4$ is a solvable group of order 288. The computer result [7] of G. E. Moorhouse shows that all Bol loops of order less than 24 are solvable, hence $Q_4$ is a simple Bol loop of least possible order.

**Example III:** Put $X = \text{PSL}_2(\mathbb{R})$ and define the subgroups

$$Y_0 = \left\{ \pm \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix} \mid t \in \mathbb{R} \right\}, \quad Y_1 = \left\{ \pm \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right\} \quad a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}$$
of $X$. By Theorem 3.6, $Q_{(X,Y_0,Y_1)}(X,Y_0,Y_1)$ is a proper simple proper Bol loop which is isomorphic to all its isotopes. In particular, $Q_{(X,Y_0,Y_1)}(X,Y_0,Y_1)$ is not isotopic to a Bruck loop. Moreover, the left translation group is $PSL_2(\mathbb{R}) \times PSL_2(\mathbb{R})$.

In [2], the author classifies all differentiable Bol loops having a semi-simple left multiplications group of dimension at most 9. Our construction shows that the classification cannot be complete. (The author seems not to consider the case when the group $G$ topologically generated by the left translations is a proper direct product of simple Lie groups $G_1, G_2$ and the stabilizer of $1 \in Q$ in $G$ is a direct product $H = H_1 \times H_2$ with $1 \neq H_i \leq G_i, i = 1, 2$.)

Example IV: Let $\Sigma$ be the set of non-zero squares in $\mathbb{F}_{27}$, $|\Sigma| = 13$. Let $X$ be the set of transformations

$$X = \{ f(z) = az^t + b \mid a \in \Sigma, b \in \mathbb{F}_{27}, \tau \in \text{Aut}(\mathbb{F}_{27}) \}$$

of $\mathbb{F}_{27}$. Then $X$ has order $1053 = 3^4 \cdot 13$ and it acts primitively on $\mathbb{F}_{27}$. Moreover,

$$X' = \{ f(z) = az + b \mid a \in \Sigma, b \in \mathbb{F}_{27} \}, \quad X'' = \{ f(z) = z + b \mid b \in \mathbb{F}_{27} \}.$$

We define $Y_1$ as the stabilizer of 0 in $X$. Since $X''$ acts regularly, we have $X''Y_1 = X$. Let $U$ be the 3-Sylow subgroup of $X$, $|U| = 81$. Clearly, $U/X'' \cong C_3$, thus $U' \cap U_0 = 1$ where $U_0$ is the stabilizer of 0 in $U$. Therefore, $U$ has a subgroup $Y_0$ of order 27 such that $Y_0 \neq X''$ and $Y_0 \cap U_0 = 1$; in other words, $Y_0$ acts regularly on $\mathbb{F}_{27}$. Since $X''$ is the unique 3-Sylow subgroup of $X'$, $Y_0$ cannot be contained in $X'$. This implies $X'Y_0 = X$ because $X'$ has index 3 in $X$.

We define now the Bol loop $Q = Q_{(X,Y_0,Y_1)}$. Let $K$ be a maximal proper normal subgroup of $Q$, that is, $Q/K$ be a simple loop. If $Q/K$ were associative then by the Odd Order Theorem, it would be a cyclic group and we had a surjective homomorphism from $Q$ to an Abelian group. By Proposition 3.5 this is not possible. Hence, $Q/K$ is a proper simple Bol loop of odd order. (It can be shown by computer that $Q$ itself is a simple Bol loop.) This last construction shows that the Odd Order Theorem does not hold for finite Bol loops. (Cf. [3].)

Acknowledgement I would like to thank Peter Müller (Uni. Würzburg) for his help in finding the group $X$ in Example IV. I also thank Petr Vojtěchovský and Michael Kinyon (Uni. Denver) for many stimulating conversations and helpful comments.

References

[1] M. Aschbacher. On Bol loops of exponent 2. J. Algebra 288, No. 1, 99-136 (2005).

[2] A. Figula. Bol loops as sections in semi-simple Lie groups of small dimension. Manuscr. Math. 121, No. 3, 367-384 (2006).

[3] T. Foguel, M. K. Kinyon and J. D. Phillips. On twisted subgroups and Bol loops of odd order. http://arxiv.org/abs/math/0208231 (2004).
[4] M. GIUDICI. Factorisations of sporadic simple groups. *J. Algebra* **304**, No. 1, 311-323 (2006).

[5] M. W. LIEBECK. The classification of finite simple Moufang loops. *Math. Proc. Cambridge Philos. Soc.* **102**, 33-47 (1987).

[6] M. W. LIEBECK, C. E. PRAEGER and J. SAXL. Transitive subgroups of primitive permutation groups. *J. Algebra* **234**, No. 2, 291-361 (2000).

[7] G. E. MOORHOUSE. Bol loops of small order. http://www.uwyo.edu/moorhouse/pub/bol/ (2007).

[8] G. P. NAGY and M. VALSECCHI. Splitting automorphisms and Moufang loops. *Glasgow Math. J.* **46**, 305-310 (2004).

[9] P. T. NAGY and K. STRAMBACH. *Loops in Group Theory and Lie Theory*. W. de Gruyter, Berlin, New York (2002).

[10] L. J. PAIGE. A class of simple Moufang loops. *Proc. Amer. Math. Soc.* **7**, 471-482 (1956).

[11] H. O. PFLUGFELDER. *Quasigroups and loops*. Heldermann-Verlag, Berlin (1990).

[12] *Problems in Loop Theory and Quasigroup Theory*. http://www.math.du.edu/plq/ (2005).