

On the uniqueness of loops $M(G, 2)$

PETR VOJTĚCHOVSKÝ

Abstract. Let G be a finite group and C_2 the cyclic group of order 2. Consider the 8 multiplicative operations $(x, y) \mapsto (x^i y^j)^k$, where $i, j, k \in \{-1, 1\}$. Define a new multiplication on $G \times C_2$ by assigning one of the above 8 multiplications to each quarter $(G \times \{i\}) \times (G \times \{j\})$, for $i, j \in C_2$. If the resulting quasigroup is a Bol loop, it is Moufang. When G is nonabelian then exactly four assignments yield Moufang loops that are not associative; all (anti)isomorphic, known as loops $M(G, 2)$.

Keywords: Moufang loops, loops $M(G, 2)$, inverse property loops, Bol loops

Classification: 20N05

1. Introduction

Because of the specialized topic of this paper, we assume that the reader is familiar with the theory of Bol and Moufang loops (cf. [6]).

Chein introduced the following construction in [1] to obtain Moufang loops from groups: Let G be a finite group and let $\overline{G} = \{\overline{x}; x \in G\}$ be a set of new elements. Define multiplication $*$ on $G \cup \overline{G}$ by

$$(1) \quad x * y = xy, \quad x * \overline{y} = \overline{yx}, \quad \overline{x} * y = \overline{xy^{-1}}, \quad \overline{x} * \overline{y} = y^{-1}x,$$

where $x, y \in G$. The resulting Moufang loop $M(G, 2)$ is associative if and only if G is abelian, according to [1].

Loops $M(G, 2)$ play an important role among Moufang loops of small order (cf. [1], [5]). Recently, it was found that all Moufang loops of order $n \in \{16, 24, 32\}$ can be obtained by modifying one quarter of the multiplication tables of loops $M(G, 2)$ in a certain way [4]. The smallest nonassociative Moufang loop is isomorphic to $M(S_3, 2)$, where S_3 is the symmetric group on 3 points (cf. [3], [7]).

We are going to study a generalization of Chein’s construction (1). Given a group G , consider the 8 multiplicative operations on G : $(x, y) \mapsto (x^i y^j)^k$, where $i, j, k \in \{-1, 1\}$. Let C_2 be the cyclic group of order 2. Define a new multiplication on $G \times C_2$ by assigning one of the above 8 multiplications to each quarter $(G \times \{i\}) \times (G \times \{j\})$, for $i, j \in C_2$. Let M be the resulting quasigroup.

Work partially supported by Grant Agency of Charles University, grant number 269/2001/B-MAT/MFF.

In this note, we characterize when M is a loop (Lemma 1); we show that if M is a Bol loop, it is Moufang (Lemma 2); and we prove that when G is nonabelian then there are exactly 4 assignments that yield nonassociative Moufang loops, all (anti)isomorphic to the loop $M(G, 2)$. See Theorem 6 for details.

Chein’s construction (1) is therefore unique, in a sense.

2. Notation

Let us introduce a notation that will better serve our purposes. Consider the permutations ι, σ, τ of $G \times G$ defined by $(x, y)\iota = (x, y)$, $(x, y)\sigma = (y, x)$, and $(x, y)\tau = (y^{-1}, x)$. Since $\sigma^2 = \tau^4 = \iota$ and $\sigma\tau\sigma = \tau^{-1}$, the group A generated by σ and τ is isomorphic to Q_8 , the quaternion group of order 8. The elements ψ of A are described by

$$(x,y)\psi \left| \begin{array}{cccccccc} \iota & \sigma & \tau & \tau^2 & \tau^3 & \sigma\tau & \sigma\tau^2 & \sigma\tau^3 \\ \hline (x,y) & (y,x) & (y^{-1},x) & (x^{-1},y^{-1}) & (y,x^{-1}) & (x^{-1},y) & (y^{-1},x^{-1}) & (x,y^{-1}) \end{array} \right. .$$

We like to think of these elements as multiplications in G , and often identify $\psi \in A$ with the map $\psi\Delta : G \times G \rightarrow G$, where $(x, y)\Delta = xy$. For instance, the permutation $\sigma\tau$ determines the multiplication $x * y = x^{-1}y$. Note that $\sigma\Delta = \iota\Delta$ when G is abelian, and that $A\Delta = \iota\Delta$ when G is an elementary abelian 2-group.

To avoid trivialities, we assume throughout the paper that G is not an elementary abelian 2-group, and that $|G| > 1$.

It is natural to split the multiplication table of $M(G, 2)$ into four quarters $G \times G, G \times \overline{G}, \overline{G} \times G$ and $\overline{G} \times \overline{G}$, as in

$$\begin{array}{c|c} * & G \overline{G} \\ \hline \overline{G} & \\ \hline \overline{G} & \end{array} .$$

Then Chein’s construction (1) can be represented by the matrix

$$(2) \quad M_c = \begin{pmatrix} \iota & \sigma \\ \sigma\tau^3 & \tau \end{pmatrix} .$$

For example, we can see from M_c that $\overline{x} * y = \overline{(x, y)\sigma\tau^3} = \overline{xy^{-1}}$, for $x, y \in G$.

3. Main result

When we look at Chein’s construction (1) via (2), it appears to be somewhat arbitrary. Let us therefore investigate all multiplications

$$(3) \quad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} ,$$

where $\alpha, \beta, \gamma, \delta \in A$. We will no more distinguish between the matrix M and the groupoid it defines.

We note in passing that every M is a quasigroup. The next lemma characterizes all loops M . In the course of the proof we encounter several identities of the form $w_1 = w_2$, where w_i is a word in some symbols $x_1, \dots, x_m \in G$. When w_1, w_2 reduce to the same word in the free group on x_1, \dots, x_m , then $w_1 = w_2$ surely holds in G . Conversely, since we assumed that G is not an elementary abelian 2-group and $|G| > 1$, there are many identities that do not hold in G , no matter what G is. For instance, $x \neq x^{-1}$, $y \neq xy^{-1}x^{-1}$ (set $x = y$), and so on.

Lemma 1. *M is a loop if and only if $\alpha \in \{\iota, \sigma\}$, $\beta \in \{\iota, \sigma, \tau^3, \sigma\tau\}$ and $\gamma \in \{\iota, \sigma, \tau, \sigma\tau^3\}$. When M is a loop, its neutral element coincides with the neutral element of G .*

PROOF: We first show that if M is a loop, its neutral element e coincides with the neutral element 1 of G . This is clear, as for some $\varepsilon \in A$ we have $1 = 1 * e = (1, e)\varepsilon \in \{e, e^{-1}\}$, and thus $1 = e$.

The equation $y = 1 * y$ holds for every $y \in G$ if and only if $y = (1, y)\alpha$, which happens if and only if $\alpha \in \{\iota, \sigma, \tau^3, \sigma\tau\}$. Similarly, the equation $y = y * 1$ holds for every $y \in G$ if and only if $\alpha \in \{\iota, \sigma, \tau, \sigma\tau^3\}$. Altogether, $y = y * 1 = 1 * y$ holds for every $y \in G$ if and only if $\alpha \in \{\iota, \sigma\}$.

Following the same strategy, $\bar{y} = 1 * \bar{y}$ holds for every $y \in G$ if and only if $\beta \in \{\iota, \sigma, \tau^3, \sigma\tau\}$, and $\bar{y} = \bar{y} * 1$ holds for every $y \in G$ if and only if $\gamma \in \{\iota, \sigma, \tau, \sigma\tau^3\}$. □

Once M is a loop, it must have two-sided inverses:

Lemma 2. *If M is a loop then it is an inverse property loop. In particular, if M happens to be a Bol loop, it must be Moufang.*

PROOF: Assume that $x * y = 1$ for some $x, y \in G \cup \bar{G}$. Then both x, y belong to G , or both belong to \bar{G} , by Lemma 1. We therefore want to show that $(x, y)\varepsilon = 1$ implies $(y, x)\varepsilon = 1$ for every $\varepsilon \in A$ and $x, y \in G$.

Pick $\varepsilon \in A$. Then $(x, y)\varepsilon = (x^i y^j)^k$ for some $i, j, k \in \{-1, 1\}$. Assume that $(x, y)\varepsilon = 1$. Then $x^i y^j = 1$ and $y^j x^i = 1$. If $i = j$, we conclude from the latter equality that $y^i x^j = 1$, and thus $(y, x)\varepsilon = 1$. The inverse of the former equality yields $y^{-j} x^{-i} = 1$. If $i = -j$, we immediately have $y^i x^j = 1$, and thus $(y, x)\varepsilon = 1$.

Hence M is an inverse property loop. It is well-known that a Bol loop is Moufang if and only if it is an inverse property loop (cf. [2]). □

Given M as in (3), let

$$M^{\text{op}} = \begin{pmatrix} \sigma\alpha & \sigma\gamma \\ \sigma\beta & \sigma\delta \end{pmatrix}.$$

Lemma 3. *The quasigroup M^{op} is opposite to M .*

PROOF: Denote by \circ the multiplication in M^{op} . Then

$$\begin{aligned} x \circ y &= (x, y)\sigma\alpha = (y, x)\alpha = y * x, \\ x \circ \bar{y} &= \overline{(x, y)\sigma\gamma} = \overline{(y, x)\gamma} = \bar{y} * x, \\ \bar{x} \circ y &= \overline{(x, y)\sigma\beta} = \overline{(y, x)\beta} = y * \bar{x}, \\ \bar{x} \circ \bar{y} &= (x, y)\sigma\delta = (y, x)\delta = \bar{y} * \bar{x}, \end{aligned}$$

for every $x, y \in G$. □

Let us assume from now on that G is nonabelian. Then the identity $xy = yx$ and any other identity that reduces to $xy = yx$ do not hold in G , of course. We will come across the identity $xxxy = yxx$. Note that this identity holds in G if and only if the center of G is of index 2 in G .

We would like to know when M is a Bol (and hence Moufang) loop. Assume from now on that M is a loop.

Recall that the opposite of a Moufang loop is again Moufang. We can therefore combine Lemmas 1, 3 and assume that the loop M satisfies $\alpha = \iota$. Since every Moufang loop is diassociative, we are going to have a look at such loops:

Lemma 4. *If G is nonabelian and M is a diassociative loop with $\alpha = \iota$ then (β, γ, δ) is one of the eight triples*

$$(4) \quad (\iota, \iota, \iota), \quad (\tau^3, \iota, \sigma\tau), \quad (\sigma, \sigma, \sigma), \quad (\sigma\tau, \sigma, \tau^3), \\ (\tau^3, \tau, \tau^2), \quad (\iota, \tau, \sigma\tau^3), \quad (\sigma, \sigma\tau^3, \tau), \quad (\sigma\tau, \sigma\tau^3, \sigma\tau^2).$$

PROOF: The identities $(\bar{x} * \bar{x}) * y = \bar{x} * (\bar{x} * y)$, $\bar{x} * (y * \bar{x}) = (\bar{x} * y) * \bar{x}$ hold in M , for every $x, y \in G$. They translate into

$$(5) \quad (x, x)\delta y = (x, (x, y)\gamma)\delta,$$

$$(6) \quad (x, (y, x)\beta)\delta = ((x, y)\gamma, x)\delta,$$

respectively. We are first going to check which pairs (γ, δ) satisfy (5).

Assume that $\gamma = \iota$. Then (5) becomes $(x, x)\delta y = (x, xy)\delta$. Denote this identity by $I(\delta)$. Then $I(\iota)$ is $xxxy = xxy$ (true), $I(\sigma)$ is $xxxy = xyx$ (false), $I(\tau)$ is $y = y^{-1}$ (false), $I(\tau^2)$ is $x^{-2}y = x^{-1}y^{-1}x^{-1}$ (false), $I(\tau^3)$ is $y = xyx^{-1}$ (false), $I(\sigma\tau)$ is $y = y$ (true), $I(\sigma\tau^2)$ is $x^{-2}y = y^{-1}x^{-1}x^{-1}$ (false), and $I(\sigma\tau^3)$ is $y = xy^{-1}x^{-1}$ (false).

Assume that $\gamma = \sigma$. Then (5) becomes $(x, x)\delta y = (x, yx)\delta$. Verify that this identity holds only if $\delta = \sigma$ or $\delta = \tau^3$. (The case $\delta = \sigma$ leads to the identity $xxxy = yxx$ mentioned before this lemma.)

When $\gamma = \tau$, (5) holds only if $\delta = \tau^2$ or $\delta = \sigma\tau^3$.

When $\gamma = \sigma\tau^3$, (5) holds only if $\delta = \tau$ or $\delta = \sigma\tau^2$.

Altogether, (5) can be satisfied only when (γ, δ) is one of the 8 pairs (ι, ι) , $(\iota, \sigma\tau)$, (σ, σ) , (σ, τ^3) , (τ, τ^2) , $(\tau, \sigma\tau^3)$, $(\sigma\tau^3, \tau)$, $(\sigma\tau^3, \sigma\tau^2)$. All these pairs will now be tested on (6).

Straightforward calculation shows that (6) can be satisfied only when (β, γ, δ) is one of the 8 triples listed in (4). \square

The *Moufang identity* $((xy)x)z = x(y(xz))$ will help us eliminate 4 out of the 8 possibilities in (4). We have $((x * \bar{y}) * x) * z = x * (\bar{y} * (x * z))$ in M , and thus

$$(7) \quad (((x, y)\beta, x)\gamma, z)\gamma = (x, (y, xz)\gamma)\beta.$$

The pairs $(\beta, \gamma) = (\sigma, \sigma)$, (τ^3, ι) , (ι, τ) , $(\sigma\tau, \sigma\tau^3)$ do not satisfy (7). For instance, $(\beta, \gamma) = (\sigma, \sigma)$ turns (7) into $zxyx = xzyx$, i.e., $zx = xz$.

The four remaining triples from (4) yield Moufang loops, as we are going to show.

The quadruple $(\alpha, \beta, \gamma, \delta) = (\iota, \iota, \iota, \iota) = G_\iota$ corresponds to the direct product of G and the two-element cyclic group. The quadruple $(\iota, \sigma, \sigma\tau^3, \tau) = M_c$ is the Chein Moufang loop $M(G, 2)$ that is associative if and only if G is abelian, by [1]. (We can also verify this directly.)

Set $G_\tau = (\iota, \tau^3, \tau, \tau^2)$ and $M_\sigma = (\iota, \sigma\tau, \sigma, \tau^3)$. We claim that G_ι is isomorphic to G_τ , and M_c is isomorphic to M_σ .

Lemma 5. Define $T : A^4 \rightarrow A^4$ by

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \tau^3\beta \\ \gamma\tau & \tau^2\delta \end{pmatrix} = MT.$$

If $((x, y)\beta\Delta)^{-1} = (y^{-1}, x^{-1})\beta\Delta$ and $((x, y)\gamma\Delta)^{-1} = (x^{-1}, y)\gamma\tau\Delta$ then M is isomorphic to MT .

PROOF: Consider the permutation f of $G \cup \bar{G}$ defined by $f(x) = x$, $f(\bar{x}) = \overline{x^{-1}}$, for $x \in G$. Let $*$ be the multiplication in M and \circ the multiplication in MT . We show that $(x * y)f = xf \circ yf$ for every $x, y \in G \cup \bar{G}$. With $x, y \in G$, we have

$$\begin{aligned} (x * y)f &= (x, y)\alpha\Delta f = (x, y)\alpha\Delta = x \circ y = xf \circ yf, \\ (\bar{x} * \bar{y})f &= (x, y)\delta\Delta f = (x, y)\delta\Delta = (x^{-1}, y^{-1})\tau^2\delta\Delta = \bar{x}f \circ \bar{y}f. \end{aligned}$$

Using the assumption on β and γ , we also have

$$(x * \bar{y})f = \overline{(x, y)\beta\Delta}f = \overline{((x, y)\beta\Delta)^{-1}} = \overline{(y^{-1}, x^{-1})\beta\Delta} = \overline{(x, y^{-1})\tau^3\beta\Delta} = xf \circ \bar{y}f,$$

and

$$(\bar{x} * y)f = \overline{(x, y)\gamma\Delta}f = \overline{((x, y)\gamma\Delta)^{-1}} = \overline{(x^{-1}, y)\gamma\tau\Delta} = \bar{x}f \circ yf. \quad \square$$

Note that $G_\iota T = G_\tau$ and $M_c T = M_\sigma$. Now, $\beta \in \{\iota, \sigma\}$ satisfies $((x, y)\beta\Delta)^{-1} = (y^{-1}, x^{-1})\beta\Delta$, and $\gamma \in \{\iota, \sigma\tau^3\}$ satisfies $((x, y)\gamma\Delta)^{-1} = (x^{-1}, y)\gamma\tau\Delta$. By Lemma 5, G_ι is isomorphic to G_τ , and M_c is isomorphic to M_σ .

We have proved:

Theorem 6. *Let G with $|G| > 1$ be a finite group that is not an elementary abelian 2-group. With the above conventions, let*

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

specify the multiplication in $L = G \cup \overline{G}$, where $\alpha, \beta, \gamma, \delta \in A = \langle \sigma, \tau \rangle$, and $(x, y)\sigma = (y, x)$, $(x, y)\tau = (y^{-1}, x)$. If L is a Bol loop then it is Moufang.

When G is nonabelian, then L is a Bol loop if and only if M is equal to one of the following matrices:

$$\begin{aligned} G_\iota &= \begin{pmatrix} \iota & \iota \\ \iota & \iota \end{pmatrix}, & G_\iota^{\text{op}} &= \begin{pmatrix} \sigma & \sigma \\ \sigma & \sigma \end{pmatrix}, \\ G_\tau &= \begin{pmatrix} \iota & \tau^3 \\ \tau & \tau^2 \end{pmatrix}, & G_\tau^{\text{op}} &= \begin{pmatrix} \sigma & \sigma\tau \\ \sigma\tau^3 & \sigma\tau^2 \end{pmatrix}, \\ M_c &= \begin{pmatrix} \iota & \sigma \\ \sigma\tau^3 & \tau \end{pmatrix}, & M_c^{\text{op}} &= \begin{pmatrix} \sigma & \tau^3 \\ \iota & \sigma\tau \end{pmatrix}, \\ M_\sigma &= \begin{pmatrix} \iota & \sigma\tau \\ \sigma & \tau^3 \end{pmatrix}, & M_\sigma^{\text{op}} &= \begin{pmatrix} \sigma & \iota \\ \tau & \sigma\tau^3 \end{pmatrix}. \end{aligned}$$

The loops X^{op} are opposite to the loops X . The isomorphic loops G_ι , G_τ and their opposites are groups. The isomorphic loops M_c , M_σ and their opposites are Moufang loops that are not associative.

Even when G is abelian, it turns out there are no additional matrices M besides those listed in Theorem 6 that yield Bol loops. The proof of this observation is not long and can be found in [8].

REFERENCES

[1] Chein O., *Moufang loops of small order*, Memoirs of the American Mathematical Society, Volume **13**, Issue 1, Number **197** (1978).
 [2] Chein O., Pflugfelder H.O., Smith J.D.H., Eds., *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Mathematics **8**, Heldermann Verlag, Berlin, 1990.
 [3] Chein O., Pflugfelder H.O., *The smallest Moufang loop*, Arch. Math. **22** (1971), 573–576.

- [4] Drápal A., Vojtěchovský P., *Moufang loops that share associator and three quarters of their multiplication tables*, submitted.
- [5] Goodaire E.G., May S., Raman M., *The Moufang Loops of Order less than 64*, Nova Science Publishers, 1999.
- [6] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics **7**, Heldermann Verlag, Berlin, 1990.
- [7] Vojtěchovský P., *The smallest Moufang loop revisited*, to appear in Results Math.
- [8] Vojtěchovský P., *Connections between codes, groups and loops*, Ph.D. Thesis, Charles University, 2003.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DENVER, 2360 S GAYLORD ST., DENVER, CO 80208, USA

E-mail: petr@math.du.edu

(Received December 9, 2002, revised March 17, 2003)