THE SMALLEST MOUFANG LOOP REVISITED

PETR VOJTĚCHOVSKÝ

Abstract. We derive presentations for Moufang loops of type $M_{2n}(G,\,2)$, defined by Chein, with G finite, two-generated. We then use $G = S_3$ to visualize the smallest non-associative Moufang loop.

Math. Subject Classification: Primary: 20N05, Secondary: 20F05
Keywords: Moufang loop, presentations of loops, loops $M_{2n}(G,\,2)$.

1. Introduction

In order to derive a presentation for a groupoid $A = (A,\,\cdot)$, one usually needs to introduce a normal form for elements of A written in terms of some generators. Such a normal form is not easy to find when A is not commutative, and even more so when A is not associative. Once a normal form is found, it might be still difficult to come up with presenting relations. Indeed, it is often the case that the only known presentation for a non-associative groupoid is the *table presentation*, i.e., the presentation consisting of all relations $x \cdot y = z$ such that $x \cdot y$ equals z in A, and where x, y run over all elements of A. Table presentations are extremely useful when one constructs a multiplication table for A, however, they are of little use when one needs to identify A as a subgroupoid of another groupoid. To do the latter, it is necessary, in principle, to evaluate all products $x \cdot y$ with $x,\, y \in A$. It is therefore desirable to have access to presentations with a few presenting relations.

The infinite class of Moufang loops $M_{2n}(G,\,2)$, defined below, represents a significant portion of non-associative Moufang loops of small order. We derive compact presentations for $M_{2n}(G,\,2)$ for every finite, two-generated group G.

Thirty years ago, Chein and Pflugfelder [3] proved that the smallest non-associative Moufang loop is of order 12 and is unique up to isomorphism. It coincides with $M = M_{12}(S_3,\,2)$. Guided by our presentation for M, we give a new, visual description of M in the last section.

2. The Loops $M_{2n}(G,\,2)$

A loop $L = (L,\,\cdot)$ is *Moufang* if it satisfies one of the three equivalent *Moufang identities*

$$xy \cdot zx = x(yz \cdot x), \quad x(y \cdot xz) = (xy \cdot x)z, \quad x(y \cdot zy) = (xy \cdot z)y. \tag{1}$$

In fact, it is not necessary to assume that L possesses a neutral element. By a result of Kunen [4], every quasigroup satisfying one of the Moufang identities is necessarily a (Moufang) loop. Every element x of a Moufang loop has a two-sided inverse x^{-1}. Also, Moufang loops are *diassociative*, i.e, every two-generated subloop is a group. We will use these well-known properties of Moufang loops without warning throughout the paper.

The following construction is due to O. Chein [2]. Let G be a finite group of order n. Pick a new element u, and define

$$M_{2n}(G,\,2) = \{gu^\alpha;\ g \in G,\ \alpha = 0,\,1\},$$

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

where

$$gu^\alpha \cdot hu^\beta = (g^{(-1)^\beta} h^{(-1)^{\alpha+\beta}})^{(-1)^\beta} u^{\alpha+\beta} \quad (g,\, h \in G,\ \alpha,\, \beta = 0,\, 1). \tag{2}$$

Then $M_{2n}(G,\, 2)$ is a Moufang loop of order $2n$. It is associative if and only if G is commutative.

Let $\pi(m)$ be the number of isomorphism types of non-associative Moufang loops of order at most m, and let $\sigma(m)$ be the number of non-associative loops of the form $M_{2n}(G,\, 2)$ of order at most m. Then, according to Chein's classification [2], $\pi(31) = 13$, $\sigma(31) = 8$, $\pi(63) = 158$, $\sigma(63) = 50$. (As Orin Chein kindly notified me, Edgar Goodaire noticed that the loop $M_{12}(S_3,\, 2) \times C_3$ is missing in [2]. He also observed that $M_{48}(5,\, 5,\, 5,\, 3,\, 3,\, 0)$ is isomorphic to $M_{48}(5,\, 5,\, 5,\, 3,\, 6,\, 0)$, and $M_{48}(5,\, 5,\, 5,\, 3,\, 3,\, 6)$ to $M_{48}(5,\, 5,\, 5,\, 3,\, 6,\, 6)$. That is why $\pi(63)$ equals 158, rather than 159.) This demonstrates eloquently the abundance of loops of type $M_{2n}(G,\, 2)$ among Moufang loops of small order.

3. The Presentations

We start with the table presentation (2) for $M_{2n}(G,\, 2)$ and prove

Theorem 3.1. *Let $G = \langle x,\, y;\ R\rangle$ be a presentation for a finite group G, where R is a set of relations in generators x, y. Then $M_{2n}(G,\, 2)$ is presented by*

$$\langle x,\, y,\, u;\ R,\, u^2 = (xu)^2 = (yu)^2 = (xy \cdot u)^2 = e\rangle, \tag{3}$$

where e is the neutral element of G.

Let us emphasize that (3) is a presentation in the *variety of Moufang loops*, not groups.

The complicated multiplication formula (2) merely describes the four cases

$$g \cdot h = gh, \tag{4}$$

$$gu \cdot h = gh^{-1} \cdot u, \tag{5}$$

$$g \cdot hu = hg \cdot u, \tag{6}$$

$$gu \cdot hu = h^{-1}g \tag{7}$$

in a compact way. In particular, identities (7) and (5) imply

$$u^2 = e, \quad gu = ug^{-1}\ (g \in G). \tag{8}$$

We claim that (8) is equivalent to (2). An element $g \in G$ will be called *good* if $gu = ug^{-1}$ can be derived from (3).

Lemma 3.2. *If $h \in G$ is good, then (5) holds. If g, h, $hg \in G$ are good, then (6) holds. If g, $g^{-1}h$ are good, then (7) holds.*

Proof. We have $gu \cdot h = (gu \cdot h)u \cdot u = (g \cdot uhu)u = (g \cdot h^{-1}uu)u = gh^{-1} \cdot u$ if h is good. Assume that g, h, hg are good. Then $g \cdot hu = g \cdot uh^{-1} = u \cdot u(g \cdot uh^{-1}) = u(ugu \cdot h^{-1}) = u \cdot g^{-1}h^{-1} = hg \cdot u$. Finally, when g and $g^{-1}h$ are good, we derive $gu \cdot hu = ug^{-1} \cdot hu = u \cdot g^{-1}h \cdot u = h^{-1}g$. □

Thus (8) is equivalent to (2). Moreover, in order to prove Theorem 3.1, it suffices to show that every $g \in G$ is good.

Thanks to diassociativity, g^s (s positive integer) is good whenever g is. Since G is finite, g^{-1} is good whenever g is.

Lemma 3.3. *Assume that g, $h \in G$ are good. Then gh is good if and only if hg is.*

Proof. Because of the symmetry, it is enough to prove only one implication. Assume that hg is good. By Lemma 3.2, $g \cdot hu = hg \cdot u$. Using this identity, we obtain $gh \cdot ug = g(hu \cdot g) = (g \cdot hu)g = (hg \cdot u)g = h \cdot gug = hu$, thus $gh = hu \cdot g^{-1}u = uh^{-1} \cdot g^{-1}u = u \cdot h^{-1}g^{-1} \cdot u$, and so $gh \cdot u = u \cdot h^{-1}g^{-1}$. ☐

Lemma 3.4. *Assume that* $g,\, h \in G$ *are good. Then so is* ghg.

Proof. Since g^{-1}, h are good, Lemma 3.2 yields $ug \cdot h = g^{-1}u \cdot h = g^{-1}h^{-1} \cdot u$. Then $u \cdot ghg \cdot u = (ug \cdot h)g \cdot u = (g^{-1}h^{-1} \cdot u)g \cdot u = g^{-1}h^{-1} \cdot ugu = g^{-1}h^{-1}g^{-1}$, and we are done. ☐

We continue by induction on the *complexity*, or *length*, if you will, of the elements of G, defined below.

For $\varepsilon = 1,\, -1$, let X_ε be the set of symbols $\{x_1^\varepsilon,\, \cdots,\, x_m^\varepsilon\}$, and write $X = X_1 \cup X_{-1}$. Every word w of the free group $F = \langle X \rangle$ can be written uniquely in the form $x_{i_1}^{\varepsilon_1} \cdots x_{i_r}^{\varepsilon_r}$, where $i_j \neq i_{j+1}$, and ε_j is a non-zero integer. Define the *complexity* of w as the ordered pair $c(w) = (r,\, \sum_{j=1}^{r} |\varepsilon_r|)$, and order the complexities lexicographically.

From now on, assume that G is two-generated, and write $x = x_1$, $y = x_2$.

Since $xu = ux^{-1}$ and $yu = uy^{-1}$ are presenting relations, both x, y are good, and hence both x^s, y^s are good for every integer s. The last presenting relation $xy \cdot u = u \cdot y^{-1}x^{-1}$ shows that both xy and $y^{-1}x^{-1} = (xy)^{-1}$ are good. Then yx and $x^{-1}y^{-1} = (yx)^{-1}$ are good, by Lemma 3.3. Also, Lemma 3.4 implies that $x^{-1} \cdot xy \cdot x^{-1} = yx^{-1}$ is good. Then $x^{-1}y$, $xy^{-1} = (yx^{-1})^{-1}$ and $y^{-1}x = (x^{-1}y)^{-1}$ are good, by Lemma 3.3. This means that every $g \in G$ with $c(g) < (2,\, 3)$ is good.

Lemma 3.5. *Every* $g \in G$ *with* $c(g) < (3,\, 0)$ *is good.*

Proof. Suppose there is g that is not good, and let $c(g) = (r,\, s)$ be as small as possible. We can assume that $g = a^u b^v$, where $\{a,\, b\} = \{x,\, y\}$, $s = |u| + |v| > 2$, and $u \neq 0 \neq v$.

Either $|u| > 1$ or $|v| > 1$. Without loss of generality, $u > 1$. (By Lemma 3.3, we can assume that $|u| > 1$. When u is negative, consider the inverse $b^{-v}a^{-u}$ instead, and apply Lemma 3.3 again.) Since $c(a^{u-2}b^v) < (2,\, s)$, the element $a^{u-2}b^v$ is good, and so is $a^{u-1}b^v a = a \cdot a^{u-2}b^v \cdot a$. As $a^{u-1}b^v$ is good by the induction hypothesis, $a^u b^v a = a \cdot a^{u-1}b^v \cdot a$ is good as well, by Lemma 3.4. Then the decomposition of $a^{u-1}b^v a$ into $a^{-1} \cdot a^u b^v a$ demonstrates that $a^u b^v a \cdot a^{-1} = a^u b^v$ is good, by Lemma 3.3. We have reached a contradiction. ☐

To finish the proof, assume there is $g \in G$ that is not good, and let $c(g) = (r,\, s)$ be as small as possible. By Lemma 3.5, $r \geq 3$. When r is odd, we can write $g = a^{\varepsilon_1}b^{\varepsilon_2}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-1}}a^{\varepsilon_r} = khk$, where $k = a^{\varepsilon_r}$, $h = a^{\varepsilon_1 - \varepsilon_r}b^{\varepsilon_2}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-1}}$, and $\{a,\, b\} = \{x,\, y\}$. Since $c(k)$, $c(h) < (r,\, s)$, both k, h are good, and then g is good by Lemma 3.4.

Assume that r is even. Then $g = a^{\varepsilon_1}b^{\varepsilon_2} \cdots a^{\varepsilon_{r-1}}b^{\varepsilon_r} = khk$, where $k = a^{\varepsilon_1}b^{\varepsilon_r}$ and $h = b^{\varepsilon_2 - \varepsilon_r}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-2}}a^{\varepsilon_{r-1} - \varepsilon_1}$. Again, $c(k)$, $c(h) < (r,\, s)$, thus both k and h are good, and so is g, by Lemma 3.4.

Theorem 3.1 is proved.

4. VISUALIZATION OF THE SMALLEST MOUFANG LOOP

The multiplication formula (2) for $M = M_{12}(S_3,\, 2)$ is certainly difficult to memorize, and so is the one in [5, Example IV.1.2]. We present a visual description of M.

Note that there are 9 involutions and 2 elements of order 3 in M (cf. [1, Table 3]). We are going to define a 12-element groupoid L and show that it is isomorphic to M.

Look at the four diagrams in Figure 1. Think of the vertices $x_0, \ldots, x_8$ as involutions. Let L consists of $e, x_0, \ldots, x_8, y, y^{-1}$, where y is of order 3. Interpret the edges of diagrams I–IV as multiplication rules in the following way. If x_i and x_j are connected by a solid line, let $x_i x_j$ be the third vertex of the (unique) triangle containing both x_i and x_j. If x_i and x_j are not connected by a solid line, we must have $j = i \pm 3$, and then x_i and x_j are connected by a dotted line (in diagram III). Define $x_i x_{i+3} = y$ and $x_i x_{i-3} = y^{-1}$.

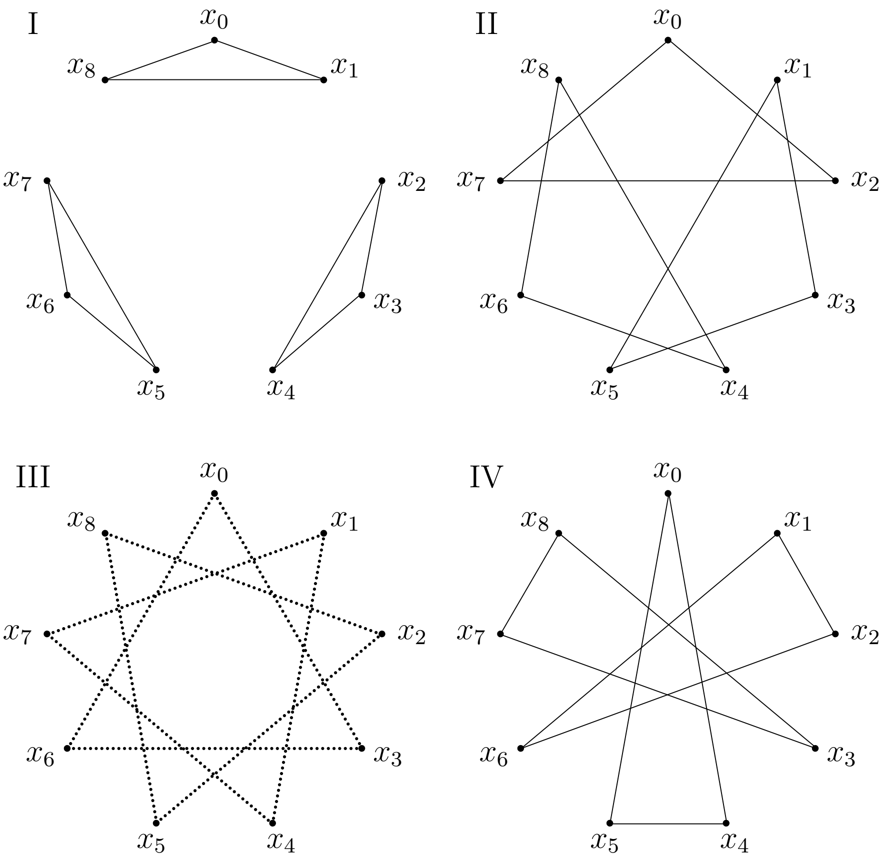

FIGURE 1. Multiplication in $M_{12}(S_3, 2)$

This partial multiplication can be extended by properties of Moufang loops. To avoid ambiguity, we postulate that $x_i y = y^{-1} x_i = x_{i+3}$ and $y x_i = x_i y^{-1} = x_{i-3}$.

Obviously, L is closed under multiplication and has a neutral element. It is non-associative, since $x_0 x_1 \cdot x_3 = x_8 x_3 = x_7 \neq x_4 = x_0 x_5 = x_0 \cdot x_1 x_3$. Is L isomorphic to M? There is a unique Moufang loop of order 12 [3], so it suffices to check the Moufang identities for L. However, this is not so easy! Instead, we verify directly that L satisfies the multiplication formula (2) with some choice of G and u.

Remark 4.1. It does not suffice to verify (8) for some choice of G and u because (8) is equivalent to (2) only when it is assumed that L is Moufang.

Put $x = x_0$, and observe that $G = \langle x, y \rangle = \{e, x_0, y, x_3, x_6, y^{-1}\}$ is isomorphic to S_3. Let $u = x_1 \notin G$. We show that (4)–(7) are satisfied for every $g, h \in G$. Thanks to the symmetry of Figure 1, it is enough to consider only $\{g, h\} = \{x_0, x_3\}, \{x_0, y\}$.

Identity (4) is trivial. Let us prove (5). We have $x_0x_1 \cdot x_3 = x_8x_3 = x_7 = yx_1 = x_0x_3^{-1} \cdot x_1$, $x_0x_1 \cdot y = x_8y = x_2 = x_6x_1 = x_0y^{-1} \cdot x_1$, $x_3x_1 \cdot x_0 = x_5x_0 = x_4 = y^{-1}x_1 = x_3x_0^{-1} \cdot x_1$, and $yx_1 \cdot x_0 = x_7x_0 = x_2 = x_6x_1 = yx_0^{-1} \cdot x_1$. Similarly for (6), (7).

Hence L is isomorphic to M. The subloop structure of L is apparent from the visual rules, too. If $j \equiv i \pmod 3$ then $\langle x_i, x_j\rangle \cong S_3$; otherwise, $\langle x_i, x_j\rangle \cong V_4$, for $i \neq j$.

REFERENCES

[1] O. Chein, *Moufang Loops of Small Order I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.

[2] O. Chein, *Moufang Loops of Small Order*, Memoirs of the American Mathematical Society, Volume **13**, Issue 1, Number **197** (1978).

[3] O. Chein, H. O. Pflugfelder, *The smallest Moufang loop*, Arch. Math. **22** (1971), 573–576.

[4] K. Kunen, *Moufang Quasigroups*, J. Algebra **183** (1996), no 1, 231–234.

[5] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, (Sigma series in pure mathematics; **7**), Heldermann Verlag Berlin (1990).

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

E-mail address: `petr@math.du.edu`

Eingegangen am 13. März 2003