Proceedings of the 2^{nd} IMT-GT Regional Conference on Mathematics, Statistics and Applications
Universiti Sains Malaysia

AN ALTERNATIVE CONSTRUCTION OF THE MOUFANG LOOP $M(G, 2)$

Andrew Rajah and Chong Kam Yoon
School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

Abstract. In [3], Orin Chein defined and constructed a class of Moufang loops called the $M(G, 2)$ with a product rule which is rather complicated. We provide an alternative definition of $M(G, 2)$ with a much simpler product rule.

1. Introduction & motivation

A Moufang loop $\langle L, \cdot\rangle$ is a loop which satisfies the identity $xy \cdot zx = (x \cdot yz)x$. $\langle L, \cdot\rangle$ is not necessarily associative, i.e., it may not satisfy the identity $xy \cdot z = x \cdot yz$. In fact, there exists a smallest nonassociative Moufang loop of order 12 [4]. In [3], Chein showed various methods of constructing nonassociative Moufang loops. In fact in this memoir, he constructed all the nonassociative Moufang loops of order less than 64. Among the most well used and probably the simplest was a Moufang loop called $M(G, 2)$, the definition of which was given in [3, p.5, Theorem 0] as we quote below:

"If L is a finite nonassociative Moufang loop for which every minimal set of generators contains an element of order 2, then L contains a nonabelian subgroup G and an element *u* of order 2 in L such that each element of L may be uniquely expressed in the form gu^{α}, where $g \in G$, and $\alpha = 0$ or 1. Furthermore, the product of two elements of L is given by

$$(g_1 u^{\delta})(g_2 u^{\epsilon}) = (g_1^{v} g_2^{\mu})^{v} u^{\delta+\epsilon}$$

where $v = (-1)^{\epsilon}$ and $\mu = (-1)^{\epsilon+\delta}$.

Conversely, given any nonabelian group $\langle G, \cdot\rangle$, the loop L constructed as indicated above is a nonassociative Moufang loop. It will be denoted by $M(G, 2)$."

So in order to use the product rule above, we would first need to calculate the values of v and μ before evaluating $(g_1^{v} g_2^{\mu})^{v} u^{\delta+\epsilon}$.

The primary goal of this paper is to simplify the product rule given by Chein. We notice that δ and ϵ are the values which mainly determine the value of $(g_1^{v} g_2^{\mu})^{v} u^{\delta+\epsilon}$. Since the values of δ and ϵ are either 0 or 1, we should look at the four possible combinations of choices for both δ and ϵ in order to find our own simplified product rule. This is what we do in Lemma 3.1.

Thus by looking at the 4 cases mentioned, we have come up with a much simpler product rule. Next, we have shown that the loop that we construct is indeed a Moufang loop, and that it is nonassociative if G is a nonabelian group.

Finally, we show that our loop is isomorphic to $M(G, 2)$.

Although there is nothing lacking in Chein's presentation of $M(G, 2)$, we wish to mention that our presentation is more similar to previously well known presentations or constructions of nonassociative Moufang loops. (See [2], [5] and [6].)

2. Definitions

1. A binary system $\langle L, \cdot\rangle$ in which specification of any two of the elements *x*, *y*, *z* in the equation $x \cdot y = z$ uniquely determines the third element is called a quasigroup. If further, it contains an identity element, then it is called a loop.
2. A loop $\langle L, \cdot\rangle$ is a Moufang loop if it satisfies any of the 3 (equivalent) Moufang identities:
   i) $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$,
   ii) $x \cdot [y \cdot (z \cdot y)] = [(x \cdot y) \cdot z] \cdot y$,
   iii) $x \cdot [y \cdot (x \cdot z)] = [(x \cdot y) \cdot x] \cdot z$.
   (See [1, Lemma 3.1, p.115]. Note that when there is no danger of misinterpretation, we can write xy to mean $x \cdot y$. So we will write $xy \cdot z$ instead of $(x \cdot y) \cdot z$, $xy \cdot zx$ instead of $(x \cdot y) \cdot (z \cdot x)$, etc., in order to simplify our presentation.)

3. A loop $\langle L,\ \cdot\rangle$ is a group if it satisfies the associative property $xy \cdot z = x \cdot yz$.
4. A loop $\langle L,\ \cdot\rangle$ is isomorphic to $\langle M,\ *\rangle$ if there exists a function $\phi : L \rightarrow M$ such that ϕ is one-to-one and onto with $(l_1 \cdot l_2)\phi = (l_1\phi) * (l_2\phi), \quad \forall l_i \in L$.
5. Other definitions follow those in [1].

3. Main results

Lemma 3.1. *In $M(G, 2)$,*

(i) $(g_1u^0)(g_2u^0) = (g_1g_2)u^0$,
(ii) $(g_1u^1)(g_2u^0) = (g_1g_2^{-1})u^1$,
(iii) $(g_1u^0)(g_2u^1) = (g_2g_1)u^1$,
(iv) $(g_1u^1)(g_2u^1) = (g_2^{-1}g_1)u^0$, $\forall g_1, g_2 \in G$.

Proof. From the definition of $M(G, 2)$, $(g_1u^\delta)(g_2u^\epsilon) = (g_1^v g_2^\mu)^v u^{\delta+\epsilon}$ where $v = (-1)^\epsilon$ and $\mu = (-1)^{\epsilon+\delta}$. So

(i) $(g_1u^0)(g_2u^0) = (g_1^1g_2^1)^1u^{(0+0)} = (g_1g_2)u^0$, because $v = (-1)^0 = 1, \mu = (-1)^{0+0} = 1$,
(ii) $(g_1u^1)(g_2u^0) = (g_1^1g_2^{-1})^1u^{(1+0)} = (g_1g_2^{-1})u^1$, because $v = (-1)^0 = 1, \mu = (-1)^{0+1} = -1$,
(iii) $(g_1u^0)(g_2u^1) = (g_1^{-1}g_2^{-1})^{-1}u^{(1+0)} = (g_2g_1)u^1$, because $v = (-1)^1 = -1, \mu = (-1)^{0+1} = -1$,
(iv) $(g_1u^1)(g_2u^1) = (g_1^{-1}g_2^1)^{-1}u^{(1+1)} = (g_2^{-1}g_1)u^0$, because $v = (-1)^1 = -1, \mu = (-1)^{1+1} = 1$.

□

We note that the power of g_2 in each of the four possible combinations of values for δ and ϵ is always 1 or -1, solely depending on the value of δ. If $\delta = 1$, the power of g_2 is -1, but if $\delta = 0$, the power of g_2 is 1. So we can write the power of g_2 as $(-1)^\delta$. On the other hand, the power of g_1 is always 1, but g_1 may appear on the left or right of $g_2^{(-1)^\delta}$, solely depending on the value of ϵ. Hence, we obtain the following lemma.

Lemma 3.2. *In $M(G, 2)$, $(g_1u^\delta)(g_2u^\epsilon) = (g_1^{1-\epsilon}g_2^{(-1)^\delta}g_1^\epsilon)u^{\delta+\epsilon}$.*

Proof. From Lemma 1, if $\delta = 1$, the power of g_2 is -1, but if $\delta = 0$, the power of g_2 is 1. So we can write the power of g_2 as $(-1)^\delta$. The power of g_1 is always 1, and if $\beta = 0$, g_1 will be multiplied on the left of $g_2^{(-1)^\alpha}$, whereas if $\epsilon = 1$, g_1 will be multiplied on the right of $g_2^{(-1)^\alpha}$. So in any case, we can write this observation as $g_1^{1-\epsilon}g_2^{(-1)^\delta}g_1^\epsilon$. Therefore, $(g_1u^\delta) \cdot (g_2u^\epsilon) = (g_1^{1-\epsilon}g_2^{(-1)^\delta}g_1^\epsilon)u^{\delta+\epsilon}$. □

Theorem 3.1. *Let $\langle G,\ \circ\rangle$ be a group and $M = \{(g, \alpha)\ |\ g \in G,\ \alpha \in Z_2\}$. Define $*$ on M as $(g_1, \alpha_1)*(g_2, \alpha_2) = (g_1^{1-\alpha_2} \circ g_2^{(-1)^{\alpha_1}} \circ g_1^{\alpha_2}, \quad \alpha_1 + \alpha_2)$. Then*

i) *$\langle M,\ *\rangle$ is a Moufang loop,*
ii) *$|M|\ = 2|G|$ if $|G|$ is finite,*
iii) *$\langle M,\ *\rangle$ is a not associative iff G is not commutative,*
iv) *$\langle M,\ *\rangle$ is isomorphic to $M(G, 2)$.*

Note 3.1. It is necessary to note that the power of g_1 should be either 0 or 1. We can observe that when finding the product of 3 or more elements of M, there may be cases where we would have to obtain $g_1^{1-\alpha-\beta}$ where $\alpha = \beta = 1$. Since the operations $1 - \alpha - \beta$ and $\alpha + \beta$ are in Z_2, i.e., the addition and subtraction are congruent modulo 2, we must take $g_1^{1-\alpha-\beta} = g_1^1$, rather than g_1^{-1}, and $g_1^{\alpha+\beta} = g_1^0 = 1$, rather than g_1^2 etc., so that the powers of g_1 remain as either 0 or 1 only, whereas the powers of g_2 are either 1 or -1.

Proof. Clearly M is closed under the operation $*$. Also $*$ is well defined. So $\langle M,\ *\rangle$ is a binary system. Obviously $(1, 0) \in M$, where 1 is the identity element of G, and $(1, 0) * (g, \alpha) = (g, \alpha) * (1,\ 0) = (g, \alpha), \quad \forall g \in G,\ \alpha \in Z_2$. Thus (1,0) is the identity element of $\langle M,\ *\rangle$.

For the rest of the proof we have chosen to omit writing the product rule '$\circ$' between elements in G since this results in no confusion but rather simplifies the presentation of our proof.

Take $(g, \alpha) \in M$. Define $(g, \alpha)' = (g^{(-1)^{\alpha+1}}, \alpha)$. Clearly $(g, \alpha)' \in M$. Now

$$(g, \alpha) * (g, \alpha)' = (g, \alpha) * (g^{(-1)^{\alpha+1}}, \alpha) = (g^{1-\alpha}\ \left[g^{(-1)^{\alpha+1}}\right]^{(-1)^\alpha} g^\alpha,\ \alpha + \alpha) = (1, 0), \forall \alpha \in Z_2.$$

Similarly, it can be seen that $(g,\ \alpha)' * (g,\ \alpha) = (1,0), \quad \forall\alpha \in Z_2$. So $(g,\alpha)' = (g,\alpha)^{-1}$, i.e., the inverse element of $(g,\ \alpha)$. Thus, for every element in M, there exists an inverse in M. Take $l_1 = (g,\alpha), \quad l_2 = (h,\beta), \quad l_3 = (k,\gamma) \in M$. By definition, $\langle M,\ *\rangle$ is a Moufang loop iff

$$(l_1 * l_2) * (l_3 * l_1) = [l_1 * (l_2 * l_3)] * l_1 \quad , \forall l_i \in M.$$

Now

$$l_1 * l_2 = (g,\alpha) * (h,\beta) = (g^{1-\beta} h^{(-1)^\alpha} g^\beta,\ \alpha+\beta),$$

and

$$l_3 * l_1 = (k,\gamma) * (g,\alpha) = (k^{1-\alpha} g^{(-1)^\gamma} k^\alpha,\ \alpha+\gamma).$$

So,

$$(l_1 * l_2) * (l_3 * l_1) = (g^{1-\beta} h^{(-1)^\alpha} g^\beta,\ \alpha+\beta) * (k^{1-\alpha} g^{(-1)^\gamma} k^\alpha,\ \alpha+\gamma) =$$
$$\left(\left[g^{1-\beta} h^{(-1)^\alpha} g^\beta\right]^{1-(\alpha+\gamma)} \left[k^{1-\alpha} g^{(-1)^\gamma} k^\alpha\right]^{(-1)^{\alpha+\beta}} \left[g^{1-\beta} h^{(-1)^\alpha} g^\beta\right]^{\alpha+\gamma},\ 2\alpha+\beta+\gamma \right).$$

We write

$$u = \left[g^{1-\beta} h^{(-1)^\alpha} g^\beta\right]^{1-(\alpha+\gamma)} \left[k^{1-\alpha} g^{(-1)^\gamma} k^\alpha\right]^{(-1)^{\alpha+\beta}} \left[g^{1-\beta} h^{(-1)^\alpha} g^\beta\right]^{\alpha+\gamma}.$$

Therefore

$$(l_1 * l_2) * (l_3 * l_1) = (u,\ 2\alpha+\beta+\gamma).$$

On the other hand,

$$l_2 * l_3 = (h,\ \beta) * (k,\ \gamma) = (h^{1-\gamma} k^{(-1)^\beta} h^\gamma, \beta+\gamma),$$

and

$$l_1 * (l_2 * l_3) = (g,\ \alpha) * (h^{1-\gamma} k^{(-1)^\beta} h^\gamma, \beta+\gamma) = (g^{1-(\beta+\gamma)} \left[h^{1-\gamma} k^{(-1)^\beta} h^\gamma\right]^{(-1)^\alpha} g^{\beta+\gamma}, \alpha+\beta+\gamma).$$

Then,

$$\begin{aligned}
[\,l_1 * (l_2 * l_3)\,] * l_1 &= (g^{1-(\beta+\gamma)} \left[h^{1-\gamma} k^{(-1)^\beta} h^\gamma\right]^{(-1)^\alpha} g^{\beta+\gamma},\ \alpha+\beta+\gamma) * (g,\alpha) \\
&= (\left[g^{1-(\beta+\gamma)} (h^{1-\gamma} k^{(-1)^\beta} h^\gamma)^{(-1)^\alpha} g^{\beta+\gamma}\right]^{1-\alpha} g^{(-1)^{\alpha+\beta+\gamma}} \\
&\qquad \left[g^{1-(\beta+\gamma)} (h^{1-\gamma} k^{(-1)^\beta} h^\gamma)^{(-1)^\alpha} g^{\beta+\gamma}\right]^{\alpha}, 2\alpha+\beta+\gamma).
\end{aligned}$$

Write

$$\begin{aligned}
v = &\left[g^{1-(\beta+\gamma)} (h^{1-\gamma} k^{(-1)^\beta} h^\gamma)^{(-1)^\alpha} g^{\beta+\gamma}\right]^{1-\alpha} g^{(-1)^{\alpha+\beta+\gamma}} \\
&\left[g^{1-(\beta+\gamma)} (h^{1-\gamma} k^{(-1)^\beta} h^\gamma)^{(-1)^\alpha} g^{\beta+\gamma}\right]^{\alpha}.
\end{aligned}$$

Therefore

$$[l_1 * (l_2 * l_3)] * l_1 = (v,\ 2\alpha+\beta+\gamma).$$

We see that

$$(l_1 * l_2) * (l_3 * l_1) = [\,l_1 * (l_2 * l_3)] * l_1 \quad , \forall l_i \in M,$$

iff $u = v$.

Case 1: $\alpha = 0$. So

$$u = (g^{1-\beta} h g^\beta)^{1-\gamma} \left[k g^{(-1)^\gamma}\right]^{(-1)^\beta} (g^{1-\beta} h g^\beta)^\gamma,$$

and

$$v = g^{1-(\beta+\gamma)} h^{1-\gamma} k^{(-1)^\beta} h^\gamma g^{1-(\beta+\gamma)}.$$

Case 1.1: $\gamma = 0$. Then $u = g^{1-\beta} h g^\beta (kg)^{(-1)^\beta}$, and $v = g^{1-\beta} h k^{(-1)^\beta} g^{1-\beta}$. Therefore $u = v$ for $\beta \in Z_2$.

Case 1.2: $\gamma = 1$. Then $u = (kg^{-1})^{(-1)^\beta} g^{1-\beta} h g^\beta$, and $v = g^{-\beta} k^{(-1)^\beta} h g^{-\beta}$ $= g^\beta k^{(-1)^\beta} h g^\beta \quad (-\beta = \beta,$ because $\beta \in Z_2)$. Therefore, $u = v$ for $\beta \in Z_2$.

Case 2: $\alpha = 1$. So

$$u = (g^{1-\beta} h^{-1} g^\beta)^{-\gamma} (g^{(-1)^\gamma} k)^{(-1)^{1+\beta}} (g^{1-\beta} h^{-1} g^\beta)^{1+\gamma},$$

and

$$v = g^{(-1)^{1+\beta+\gamma}} g^{1-(\beta+\gamma)} (h^{1-\gamma} k^{(-1)^\beta} h^\gamma)^{-1} g^{\beta+\gamma}.$$

Case 2.1: $\beta = 0$. Thus,

$$u = (gh^{-1})^{-\gamma} (g^{(-1)^\gamma} k)^{-1} (gh^{-1})^{1+\gamma} = (gh^{-1})^{\gamma} (g^{(-1)^\gamma} k)^{-1} (gh^{-1})^{1+\gamma} \quad (-\gamma = \gamma, \quad \because \gamma \in Z_2),$$

and

$$v = g^{(-1)^{1+\gamma}} g^{1-\gamma} (h^{1-\gamma} k h^\gamma)^{-1} g^\gamma.$$

Therefore $u = v$ for $\gamma \in Z_2$.

Case 2.2: $\beta = 1$. So $u = (h^{-1}g)^{-\gamma} g^{(-1)^\gamma} k (h^{-1}g)^{1+\gamma}$, and $v = g^{(-1)^\gamma} g^{-\gamma} (h^{1-\gamma} k^{-1} h^\gamma)^{-1} g^{1+\gamma}$. therefore $u = v$ for $\gamma \in Z_2$. Since $u = v$ for every case, it follows that $(l_1 * l_2) * (l_3 * l_1) = [l_1 * (l_2 * l_3)] * l_1,\ \forall l_i \in M$.

Therefore, $\langle M,\ *\rangle$ is a Moufang loop. This proves part (i) of this theorem.

Obviously, (ii) is true, i.e., $|M| = 2|G|$ if $|G|$ is finite since $|Z_2| = 2$.

Suppose G is a nonabelian group. Then there exists $g_1, g_2 \in G$ such that $g_1 g_2 \neq g_2 g_1$. Take $(1,\ 1)$, $(g_1^{-1},\ 0)$, $(g_2^{-1},\ 0) \in M$. Using the product rule *, we get $[(1,\ 1) * (g_1^{-1}, 0)] * (g_2^{-1},\ 0) = (g_1,\ 1) * (g_2^{-1}, 0) = (g_1 g_2,\ 1)$, and $(1,\ 1) * [(g_1^{-1}, 0) * (g_2^{-1}, 0)] = (1,\ 1) * (g_1^{-1} g_2^{-1}, 0) = (g_2 g_1,\ 1)$.

Since $g_1 g_2 \neq g_2 g_1$, $[(1,\ 1) * (g_1^{-1}, 0)] * (g_2^{-1},\ 0) \neq (1,\ 1) * [(g_1^{-1}, 0) * (g_2^{-1}, 0)]$. Now, suppose G is an abelian group, that is $g_1 g_2 = g_2 g_1, \forall g_1, g_2 \in G$. Therefore

$$(g_1, \alpha) * (g_2, \beta) = (g_1^{1-\beta} g_2^{(-1)^\alpha} g_1^\beta, \alpha + \beta) = (g_1^{1-\beta+\beta} g_2^{(-1)^\alpha}, \alpha + \beta) = (g_1 g_2^{(-1)^\alpha}, \alpha + \beta).$$

That is $(g_1, \alpha) * (g_2, \beta) = (g_1 g_2^{(-1)^\alpha}, \alpha + \beta)$ if G is abelian. Take $l_1 = (g, \alpha), \quad l_2 = (h, \beta), \quad l_3 = (k, \gamma) \in M$. So

$$(l_1 * l_2) * l_3 = [(g, \alpha) * (h, \beta)] * (k, \gamma) = (gh^{(-1)^\alpha}, \alpha + \beta) * (k, \gamma) = (gh^{(-1)^\alpha} k^{(-1)^{\alpha+\beta}}, \alpha + \beta + \gamma).$$

Now,

$$\begin{aligned} l_1 * (l_2 * l_3) &= (g, \alpha) * [(h, \beta) * (k, \gamma)] = (g, \alpha) * (hk^{(-1)^\beta}, \beta + \gamma) \\ &= (g(hk^{(-1)^\beta})^{(-1)^\alpha}, \alpha + \beta + \gamma) = (gh^{(-1)^\alpha} k^{(-1)^{\alpha+\beta}}, \alpha + \beta + \gamma) \end{aligned}$$

because G is abelian. Thus, if G is abelian, $\forall l_1, l_2, l_3 \in M$, $(l_1 * l_2) * l_3 = l_1 * (l_2 * l_3)$, that is, M is associative.

So M is not associative iff G is not commutative. Define $\phi : \langle M, *\rangle \to M(G, 2)$ as $\phi\,(g, \alpha) = gu^\alpha$. Now $\phi\ [\,(g, \alpha) * (h, \beta)\,] = \phi\,(g^{1-\beta} h^{(-1)^\alpha} g^\beta, \alpha + \beta) = (g^{1-\beta} h^{(-1)^\alpha} g^\beta)\ u^{\alpha+\beta} = (gu^\alpha) * (hu^\beta)$ (by Lemma 2) $= \phi\,(g, \alpha) * \phi\,(h, \beta)$. Thus, ϕ is a homomorphism. Clearly ϕ is one-to-one and onto. So it is also an isomorphism. This completes the proof of our theorem. □

Remark 3.1. Note that for the product rule that we have presented in our theorem above: $(g_1, \alpha_1) * (g_2, \alpha_2) = (g_1^{1-\alpha_2} \circ g_2^{(-1)^{\alpha 1}} \circ g_1^{\alpha_2}, \quad \alpha_1 + \alpha_2)$. Since

$$g_1^{1-\alpha_2} = \begin{cases} g_1, & \alpha_2 = 0 \\ 1, & \alpha_2 = 1 \end{cases} \quad \text{and} \quad g_1^{\alpha_2} = \begin{cases} 1, & \alpha_2 = 0 \\ g_1 & \alpha_2 = 1 \end{cases},$$

we can suggest an alternative way of writing it, i.e.,

$$g_1^{1-\alpha_2} = g_1^{\frac{1+(-1)^{\alpha 2}}{2}}, \quad \text{and} \quad g_1^{\alpha_2} = g_1^{\frac{1-(-1)^{\alpha 2}}{2}}$$

to avoid the confusion brought by the power of g_1 especially when the product involves 3 or more elements of M. For the reader who wishes to be more careful, we can rewrite the product rule as

$$(g_1, \alpha_1) * (g_2, \alpha_2) = (g_1^{\frac{1+(-1)^{\alpha 2}}{2}} \circ g_2^{(-1)^{\alpha 1}} \circ g_1^{\frac{1-(-1)^{\alpha 2}}{2}}, \quad \alpha_1 + \alpha_2).$$

However, since our main intention is to simplify the construction and product rule of $M(G, 2)$, we prefer to leave it in the form presented in our (main) theorem.

Remark 3.2. Actually, the statement (iv) in our theorem is essentially equivalent to parts (ii) and (iii) of this theorem. We have purposely proven (ii) and (iii) by themselves (before proving part (iv)) so that our paper would be as self-contained as possible.

4. Conclusion

Since the smallest nonabelian group is the symmetric group S_3, the smallest nonassociative Moufang loop that we could construct using our theorem would be the $\langle M, *\rangle$, with the set $M = S_3 \times Z_2$.

We know that we can write $S_3 = \{1, (12), (13), (23), (123), (321)\}$. In order to make the presentation of our table neater, we shall write *a* = (12), *b* = (13), *c* = (23), *d* = (123), *e* = (321). So M = { (1,0), (*a*,0), (*b*,0), (*c*,0), (*d*,0), (*e*,0), (1,1), (*a*,1), (*b*,1), (*c*,1), (*d*,1), (*e*,1) }. We provide below the multiplication table of this $\langle M, *\rangle$.

$*$	(1,0)	(*a*,0)	(*b*,0)	(*c*,0)	(*d*,0)	(*e*,0)	(1,1)	(*a*,1)	(*b*,1)	(*c*,1)	(*d*,1)	(*e*,1)
(1,0)	(1,0)	(*a*,0)	(*b*,0)	(*c*,0)	(*d*,0)	(*e*,0)	(1,1)	(*a*,1)	(*b*,1)	(*c*,1)	(*d*,1)	(*e*,1)
(*a*,0)	(*a*,0)	(1,0)	(*d*,0)	(*e*,0)	(*b*,0)	(*c*,0)	(*a*,1)	(1,1)	(*e*,1)	(*d*,1)	(*c*,1)	(*b*,1)
(*b*,0)	(*b*,0)	(*e*,0)	(1,0)	(*d*,0)	(*c*,0)	(*a*,0)	(*b*,1)	(*d*,1)	(1,1)	(*e*,1)	(*a*,1)	(*c*,1)
(*c*,0)	(*c*,0)	(*d*,0)	(*e*,0)	(1,0)	(*a*,0)	(*b*,0)	(*c*,1)	(*e*,1)	(*d*,1)	(1,1)	(*b*,1)	(*a*,1)
(*d*,0)	(*d*,0)	(*c*,0)	(*a*,0)	(*b*,0)	(*e*,0)	(1,0)	(*d*,1)	(*b*,1)	(*c*,1)	(*a*,1)	(*e*,1)	(1,1)
(*e*,0)	(*e*,0)	(*b*,0)	(*c*,0)	(*a*,0)	(1,0)	(*d*,0)	(*e*,1)	(*c*,1)	(*a*,1)	(*b*,1)	(1,1)	(*d*,1)
(1,1)	(1,1)	(*a*,1)	(*b*,1)	(*c*,1)	(*e*,1)	(*d*,1)	(1,0)	(*a*,0)	(*b*,0)	(*c*,0)	(*e*,0)	(*d*,0)
(*a*,1)	(*a*,1)	(1,1)	(*d*,1)	(*e*,1)	(*c*,1)	(*b*,1)	(*a*,0)	(1,0)	(*e*,0)	(*d*,0)	(*b*,0)	(*c*,0)
(*b*,1)	(*b*,1)	(*e*,1)	(1,1)	(*d*,1)	(*a*,1)	(*c*,1)	(*b*,0)	(*d*,0)	(1,0)	(*e*,0)	(*c*,0)	(*a*,0)
(*c*,1)	(*c*,1)	(*d*,1)	(*e*,1)	(1,1)	(*b*,1)	(*a*,1)	(*c*,0)	(*e*,0)	(*d*,0)	(1,0)	(*a*,0)	(*b*,0)
(*d*,1)	(*d*,1)	(*c*,1)	(*a*,1)	(*b*,1)	(1,1)	(*e*,1)	(*d*,0)	(*b*,0)	(*c*,0)	(*a*,0)	(1,0)	(*e*,0)
(*e*,1)	(*e*,1)	(*b*,1)	(*c*,1)	(*a*,1)	(*d*,1)	(1,1)	(*e*,0)	(*c*,0)	(*a*,0)	(*b*,0)	(*d*,0)	(1,0)

It is easy to see that [((13),0) * ((123),1)] * (1,1) = ((12),0), but ((13),0) *[((123),1)* (1,1)] = ((23),0).

So $\langle M, *\rangle$ is nonassociative. However, we have no desire to prove that $\langle M, *\rangle$ fulfills the Moufang identity for this case since it would be too tedious. Also it is unnecessary as we have already shown it for the general case in our theorem.

References

[1] R.H. Bruck, *A Survey of Binary Systems,* Springer-Verlag, New York, 1971.

[2] R.H. Bruck, Contributions to the theory of loops, *Trans. Amer. Math. Soc*. **60** (1946), 245–354.

[3] O. Chein, *Moufang Loops of Small Order,* Mem. Amer. Math. Soc. **13** (1978), no. 197, iv+131 pp.

[4] O. Chein and H. O. Pflugfelder, The smallest Moufang loop, *Archiv der Mathematik* ***22*** (1971), 573–576.

[5] A. Rajah, Moufang loops of odd order pq^3, *J. Algebra* **235** (2001), 66–93.

[6] C. R. B. Wright, Nilpotency conditions for finite loops, *Illinois J. Math*. **9** (1965), 399–409.