TOWARD THE CLASSIFICATION OF MOUFANG LOOPS OF ORDER 64

PETR VOJTĚCHOVSKÝ

Abstract. We show how to obtain all nonassociative Moufang loops of order less than 64 and 4262 nonassociative Moufang loops of order 64 in a unified way. We conjecture that there are no other nonassociative Moufang loops of order 64. The main idea of the computer search is to modify precisely one quarter of the multiplication table in a certain way, previously applied to small 2-groups.

1. Introduction

A set Q with one binary operation is a *quasigroup* if the equation $xy = z$ has a unique solution in Q whenever two of the three elements x, y, $z \in Q$ are specified. *Loop* is a quasigroup with a neutral element 1 satisfying $1x = x1 = x$ for every x. *Moufang loops* are loops in which any of the (equivalent) *Moufang identities*

$$(xy)x)z = x(y(xz)), \tag{M1}$$

$$x(y(zy)) = ((xy)z)y, \tag{M2}$$

$$(xy)(zx) = x((yz)x), \tag{M3}$$

$$(xy)(zx) = (x(yz))x \tag{M4}$$

holds. It was shown recently [23] that, in an analogy to groups, any set with one binary operation, neutral element and two-sided inverses satisfying either (M1) or (M2) is already a Moufang loop.

Moufang loops are certainly the most studied loops. They arise naturally in algebra (as the multiplicative loop of octonions [24], [7]), and in projective geometry (Moufang planes [25]), for example.

Although Moufang loops are generally nonassociative, they retain many properties of groups that—borrowing a phrase from [6, p. 7]—we know and love. For instance: (i) every x is accompanied by its two-sided inverse x^{-1} such that $xx^{-1} = x^{-1}x = 1$, (ii) any two elements generate a subgroup (this property is called *diassociativity*), (iii) in finite Moufang loops, the order of an element divides the order of the loop, and, as is believed to be shown recently in [17], the order of a subloop divides the order of the loop.

On the other hand, many essential tools of group theory are not available for Moufang loops. The lack of associativity makes presentations very awkward and hard to calculate, and permutation representations in the usual sense impossible.

1991 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Moufang loops, loops $M(G, 2)$, extra loops, classification of Moufang loops, computer search.

It is therefore no surprise that the classification of Moufang loops of order n is completed only up to and including $n = 63$ [2], [16]. Several ingenious constructions, described in detail in [16], are needed to obtain all the loops.

In this paper, we introduce a class of Moufang loops that includes all nonassociative Moufang loops of order less than 64, and 4262 nonassociative Moufang loops of order 64 (compare this with the 267 groups of order 64). We conjecture that there are no other nonassociative Moufang loops of order 64.

The class is obtained by a computer program based on an idea of Drápal. It takes only a few minutes to obtain the Moufang loops of order less than 64, and about 2 weeks to obtain 4262 Moufang loops of order 64 (using a PC with 2 GHz processor).

Thanks to this algorithm, small Moufang loops can now be stored in a uniform and very efficient way (about 4 bytes of data are needed for a Moufang loop of order 64). They are available via the GAP [13] package LOOPS [20] written by G. Nagy and the present author. Great care was taken to comply with the naming conventions introduced in [16].

Unfortunately, there is no guarantee that the algorithm found all nonassociative Moufang loops of order 64, and, in fact, it is not clear how this question could be answered easily. Nevertheless, it appears to be a definite step toward the classification of small Moufang loops, especially small Moufang 2-loops.

1.1. **Organization of this paper.** It is known that a finite Moufang loop has order p^n if and only if it has exponent p^m, for some prime p and integers n, m. This fact is recalled and newly proved in Section 2.

Drápal's cyclic and dihedral constructions are described in Section 3, where we also summarize some results of these constructions obtained in an earlier paper [11].

The computer search always starts with a single Moufang loop, referred to as a *seed*. We use the so-called loops $M(G, 2)$ (due to Chein) as seeds. The definition and properties of the loops $M(G, 2)$ can be found in Section 4.

The computer search is outlined in Section 5, where we also present the results in a tabular form. The reader who is only interested in the outcome of the search will understand it fully at that point and does not have to read further.

The algorithm is discussed in detail in Section 6.

Several nontrivial theoretical results were needed to make the algorithm sufficiently fast. These are collected and proved in Section 7. We pay attention especially to the isomorphism problem for (Moufang) loops.

Section 8 contains detailed instructions on how to obtain and use the GAP package LOOPS.

The paper closes with a section devoted to conjectures and open problems.

2. Moufang 2-loops

A loop is said to be *power associative* if the power x^n is well-defined for every element x and a positive integer n. Moufang loops are power associative, by diassociativity.

Let p be a prime. We say that a power associative loop has *exponent* p^r if the order of every element of L divides p^r. Finite power associative loops of exponent p^r, for some r, are called *p-loops*.

One of the fundamental facts of group theory is that a finite group has exponent p^r if and only if it is of order p^s. This certainly does not generalize to p-loops.

It is easy to construct by hand a loop of order 5 and exponent 2, for instance. Another well-known example is the smallest nonassociative Steiner loop of order 10 and exponent 2 [5].

This has the unfortunate consequence that the two natural definitions of a p-loop are not equivalent, yet they appear side by side in the literature. Since we deal predominantly with Moufang loops of order $64 = 2^6$ here, let us first make sure that all is well for Moufang loops. The following proposition was first proved by Glauberman [14] for odd p, and by Glauberman and Wright [15] for $p = 2$. We offer a short proof that relies on the classification of finite simple Moufang loops, and hence on the classification of finite simple groups. The original proofs of Glauberman and Wright do not require the classification.

Recall that a subloop H of a loop L is *normal* in L if $aH = Ha$, $a(bH) = (ab)H$, and $(aH)b = a(Hb)$ holds for every $a, b \in L$. Given elements x, y, z of a loop L, the *associator* $[x, y, z] \in L$ is defined by $(xy)z = (x(yz))[x, y, z]$. The *associator subloop* $A(L)$ of L is the subloop of L generated by all associators $[x, y, z]$. The *nucleus* $N(L)$ of L consists of all elements $x \in L$ such that $[x, y, z] = [y, x, z] = [y, z, x] = 1$ for every y, $z \in L$. Finally, the *center* $Z(L)$ is the subloop $\{x \in N(L);\ xy = yx$ for every $y \in L\}$.

Proposition 2.1. *Let M be a finite Moufang loop and p a prime. Then M is of exponent p^r for some r if and only if M has order p^s for some s.*

Proof. Let $|M| = p^s$ and let $x \in M$. As is well-known (cf. [22, p. 13]), the order of x divides the order of M. In particular, M is of exponent p^s.

Conversely, suppose that M is of exponent p^s. Assume, for a contradiction, that $|M|$ is not a power of p, and that s is as small as possible.

If M is not simple, it possesses a nontrivial normal subloop L. Then $|M| = |L| \cdot |M/L|$. Both L, M/L are Moufang loops of exponent a power of p. Since $|L| < |M|$ and $|M/L| < |M|$, the orders of L and M/L are powers of p, by the induction hypothesis. Then $|M|$ is a power of p, too.

We complete the proof by showing that there is no nonassociative finite simple Moufang loop of exponent p^s.

Liebeck classified all nonassociative finite simple Moufang loops in [19]. It turns out that there is exactly one nonassociative finite simple Moufang loop $M^*(q)$ for every finite field $GF(q)$. The loops $M^*(q)$ are obtained as follows (see [21], [28] for more details):

Let $F = GF(q)$. Consider the *Zorn vector matrices*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}, \tag{1}$$

where a, $b \in F$, and α, $\beta \in F^3$. The matrices are multiplied according to the Zorn multiplication formula

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix},$$

where $\alpha \cdot \beta$ (resp. $\alpha \times \beta$) is the dot product (resp. cross product) of α and β.

Let $M(q)$ consist of all matrices (1) with $ab - \alpha \cdot \beta = 1$. Then $M^*(q) = M(q)/Z(M(q))$. Note that the group $PSL(2, q)$ embeds into $M^*(q)$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & (b, 0, 0) \\ (c, 0, 0) & d \end{pmatrix},$$

since all cross products vanish when two such vector matrices are multiplied. Since no $PSL(2,q)$ is a p-group, we are done. □

3. The Cyclic and Dihedral Constructions

While working on the problem of Hamming distances of groups [8], Drápal discovered two constructions that modify exactly one quarter of the multiplication table of a group and yield another group, often with a different center and thus not isomorphic to the original group. It is known [9] that two 2-groups whose multiplication tables (with rows and columns labelled in the same way) coincide in more than three quarters of the cells must be isomorphic. Hence, the two constructions exemplify a minimal change in a 2-group (in the sense of multiplication tables) that yields a nonisomorphic group.

Let us first give a brief description of the constructions and then talk about their power. Note that the constructions work for Moufang loops, too. The generalization from groups to Moufang loops was carried through in [11].

3.1. **Modular arithmetic.** For a positive integer m, let $M = \{-m+1, \ldots, m\}$. Define $\sigma : \mathbb{Z} \to \{-1, 0, 1\}$ by

$$\sigma(i) = \begin{cases} 0, & i \in M, \\ 1, & i > m, \\ -1, & i < -m+1. \end{cases}$$

Then σ can be used to describe addition $\oplus$ and subtraction $\ominus$ modulo M. Namely, for i, $j \in M$, we have $i \oplus j = i + j - 2m\sigma(i+j)$, $i \ominus j = i - j - 2m\sigma(i-j)$.

3.2. **The cyclic construction.** Let G be a Moufang loop with normal subloop S such that G/S is a cyclic group of order $2m$. Let α be a generator of G/S. Then for every $x \in G$ there is a unique $i \in M = \{-m+1, \ldots, m\}$ such that $x \in \alpha^i \subseteq G$. Let $h \in Z(G) \cap S$. Define a new multiplication $*$ on G by

$$x * y = xyh^{\sigma(i+j)},$$

where $x \in \alpha^i$, $y \in \alpha^j$, $i \in M$, $j \in M$. Note that no parentheses are needed in the expression $xyh^{\sigma(i+j)}$ because $h \in N(G)$.

As is shown in [11], the resulting loop $(G, *)$ is a Moufang loop. Adopting the notation of [10], the loop $(G, *)$ will also be denoted by $G[S, \alpha, h]$ or $G[\alpha, h]$.

3.3. **The dihedral construction.** Let G be a Moufang loop with normal subloop S such that G/S is a dihedral group of order $4m$, $m \geq 1$. Let β, γ be involutions of G/S such that $\alpha = \beta\gamma$ is of order $2m$. Pick $e \in \beta$, $f \in \gamma$. Then for every element $x \in G$ there are uniquely determined integers i, $j \in M$ such that $x \in \alpha^i \cup e\alpha^i$ and $x \in \alpha^j \cup \alpha^j f$. Let $G_0 = \bigcup_{i \in M} \alpha_i \leq G$. Let $h \in N(G) \cap Z(G_0) \cap S$. Define a new multiplication $*$ on G by

$$x * y = xyh^{(-1)^r \sigma(i+j)},$$

where $x \in \alpha^i \cup e\alpha^i$, $y \in \alpha^j \cup \alpha^j f$, $i \in M$, $j \in M$, and $r \in \{0, 1\}$ is equal to 0 if and only if $y \in G_0$.

As is shown in [11], the resulting loop $(G, *)$ is a Moufang loop, and will also be denoted by $G[S, \beta, \gamma, h]$ or $G[\beta, \gamma, h]$.

$*$	α^0	α^1	α^2	α^3	α^4	α^{-3}	α^{-2}	α^{-1}
α^0								
α^1					+			
α^2				+	+			
α^3			+	+	+			
α^4		+	+	+	+			
α^{-3}						−	−	−
α^{-2}						−	−	
α^{-1}						−		

$*$	α^0	$\alpha^0 f$	α^1	$\alpha^1 f$	α^2	$\alpha^2 f$	α^{-1}	$\alpha^{-1} f$
α^0								
$e\alpha^0$								
α^1					+	−		
$e\alpha^1$					+	−		
α^2			+	−	+	−		
$e\alpha^2$			+	−	+	−		
α^{-1}							−	+
$e\alpha^{-1}$							−	+

FIGURE 1. Pictorial representation of the constructions.

3.4. **Pictorial representation of the constructions.** The reader might get a better feel for the constructions when considering the effect of the constructions on the multiplication table of G. The diagrams in Figure 1 indicate the changes to the multiplication table caused by the cyclic construction for $m = 4$ (left) and by the dihedral construction for $m = 2$ (right). Each square represents $(n/|S|)^2$ elements of G. The multiplication table of $(G, *)$ differs from the multiplication table of $(G, \cdot)$ according to the symbol in the square: no symbol $\Rightarrow$ no change, "+" $\Rightarrow$ multiply every entry by h, "−" $\Rightarrow$ multiply every entry by h^{-1}. Viewed in this way, the constructions get a more combinatorial flavor.

3.5. **Invariants of the constructions.** The essential properties of the constructions are summarized in the following theorem:

Theorem 3.1 (Theorem 6.3, Theorem 6.4 [11])**.** *Let $(G, \cdot)$ be a Moufang loop and let $(G, *)$ be obtained from $(G, \cdot)$ by the cyclic or the dihedral construction. Then:*

(i) *$(G, *)$ is a Moufang loop,*
(ii) *$(G, *)$ is a group if and only if $(G, \cdot)$ is,*
(iii) *the associators of $(G, \cdot)$, $(G, *)$ are in S, and thus the associator subloops of $(G, \cdot)$ and $(G, *)$ coincide as loops,*
(iv) *the nuclei of $(G, \cdot)$ and $(G, *)$ coincide as sets,*
(v) *the constructions are reversible, i.e., $(G, \cdot)$ is obtained from $(G, *)$ by the cyclic or the dihedral construction with some parameters.*

Extra loops are loops satisfying the identity $x(y(zx)) = ((xy)z)x$. Extra loops are precisely Moufang loops with all squares in the nucleus [4, Corollary 2]. The constructions preserve this property of Moufang loops:

Lemma 3.2. *Let $(G, \cdot)$ be an extra loop and let $(G, *)$ be obtained from $(G, \cdot)$ by the cyclic or the dihedral construction. Then $(G, *)$ is an extra loop.*

Proof. It suffices to show that $x * x \in N(G, *)$ for every $x \in G$. This follows immediately from Theorem 3.1(iv), since $x * x = x^2 h^\varepsilon$ for some ε, and $x^2 \in N(G, \cdot)$, $h \in N(G, \cdot)$. □

3.6. **Using the constructions.** A good question is whether the constructions are powerful enough to produce many 2-groups from a single group. Given two groups G, H, let us call H a *modification* of G if there is an integer n and groups $G = K_0$, K_1, ..., K_{n-1}, $K_n \cong H$ such that K_{i+1} is obtained from K_i by one of the two constructions, for $0 \leq i < n$. For a group G, let $\mathcal{M}(G)$ denote the set of all modifications of G. We will call G the *seed* of $\mathcal{M}(G)$.

Since the constructions are reversible, every element of $\mathcal{M}(G)$ is in fact a seed of $\mathcal{M}(G)$. The most optimistic plan is therefore to show that given any group G of order 2^m, $\mathcal{M}(G)$ comprises all groups of order 2^m. This indeed happens for $n = 2^m \leq 32$. (This was noticed by the present author for $n = 8$ in [26], and by Drápal and Zhukavets for $n = 16$, 32 in [12].)

There are, of course, other, much faster means of generating 2-groups (cf. the manual of GAP [13] or the survey paper [1]), however, none of the group-theoretical methods applies to Moufang loops.

Theorem 3.1 claims that the nuclei and associator subloops are invariant under the constructions. A quick glance into the classification of small Moufang loops [16] reveals that some Moufang loops of order 32 have nucleus of size 2, others of size 4. Hence no single nonassociative Moufang loop of order 32 can possible yield all other Moufang loops of that order by a repeated application of the two constructions, shattering our most optimistic plan outlined above. We need more seeds.

4. Seeds for the computer search

There is a class of nonassociative Moufang loops, first defined by Chein [2], that is well understood. Let G be a group of order n, and let u be a new element. Define multiplication $\circ$ on $G \cup Gu$ by

$$g \circ h = gh, \quad g \circ hu = (gh^{-1})u, \quad gu \circ h = (hg)u, \quad gu \circ hu = hg^{-1},$$

where g, $h \in G$. The resulting loop $(G \cup Gu, \circ) = M(G, 2)$ is a Moufang loop. It is nonassociative if and only if G is nonabelian.

We are going to show that $M(G, 2)$ is isomorphic to $M(H, 2)$ if and only if G is isomorphic to H. Thus, we will obtain as many nonassociative Moufang loops of order $2n$ as there are nonabelian groups of order n. Proposition 4.2 is probably well known, but since we were unable to find a reference, we give a proof here.

For a finite power-associative loop L and a positive integer i, let

$$s_i(L) = |\{x \in L;\ |x| = i\}|.$$

We call $s(L) = (s_1(L),\ s_2(L),\ \dots)$ the *order statistic* of L. The following Lemma shows why black-box recognition of finite abelian groups is not hard in principle.

Lemma 4.1. *A finite abelian group is determined uniquely by its order statistic.*

Proof. Let A be a finite abelian group. For a prime p, let $A_{(p)} = \{x \in A; x^{(p^i)} = 1$ for some $i\}$ be the p-primary component of A. Then $s_{p^k}(A_{(p)}) = s_{p^k}(A)$. Thus, $s(A)$ determines $s(A_{(p)})$, and it suffices to prove the lemma for all finite abelian p-groups A.

Let m be the largest integer with $s_{p^m}(A) > 0$. Then $A = B \times C$, where C is a cyclic group of order p^m, and B is a finite abelian p-group. As $A = B \times C$ is a direct product, we have

$$s_{p^u}(A) = s_{p^u}(B) \cdot \Big(|C| - \sum_{v>u} s_{p^v}(C)\Big) + \Big(|B| - \sum_{v>u} s_{p^v}(B)\Big) \cdot s_{p^u}(C) - s_{p^u}(B) s_{p^u}(C).$$

Since the order statistics of A and C are known, the order statistic of B can be calculated, starting with $s_{p^m}(B)$. We are done by induction on $|A|$. □

Proposition 4.2. *Assume that G, H are two finite groups. Then $G \cong H$ if and only if $M(G, 2) \cong M(H, 2)$.*

Proof. Only one implication is nontrivial. Assume that $M(G,2) \cong M(H,2)$. Then we can consider H to be a subgroup of $M(G,2)$. By [3, Lemma 3.11] or by [27, Subsection 4.2], either $H = G$ (and we are done), or there is a subgroup A of G such that $H = M(A,2)$. Since H is associative, A is abelian. Similarly, either $G = H$ (and we are done), or there is an abelian group B such that $G \cong M(B,2)$.

The order statistic of a group K and the order statistic of the associated loop $M(K,2)$ can be reconstructed from each other, because the coset Ku consists of involutions. Being isomorphic, the loops $M(G,2) = M(M(B,2),2)$ and $M(H,2) = M(M(A,2),2)$ have identical order statistics. Thus the abelian groups B, A have identical order statistics, and are isomorphic by Lemma 4.1. Then $G = M(B,2)$, $H = M(A,2)$ are isomorphic, too. □

5. Notation and results of the computer search

From now on, whenever we say *Moufang loop* we mean a *nonassociative Moufang loop*.

Given a seed (Moufang loop) M, we can calculate the class of Moufang loops $\mathcal{M}(M)$, collecting only one loop of each isomorphism type.

Thanks to Section 4, we have plenty of seeds with which to start the computer search. It turns out that all Moufang 2-loops of order less than 64 are obtained from the seeds $M(G,2)$, and only four more seeds (see below) are needed in addition to the loops $M(G,2)$ to obtain all Moufang loops of order less than 64.

The results of the search can be found in Table 1. Here is how to read Table 1.

Under `class`, we give the name of the class $\mathcal{M}(M)$ of Moufang loops. The names are systematic if the seed is of the form $M(G,2)$, and *ad hoc* in the 4 remaining cases.

When the seed of order $2n$ is of the form $M(G,2)$, then G is a nonabelian group of order n. (Table 2 gives the number of nonabelian groups of order $1 \leq n \leq 32$ with orders for which no nonabelian group exists omitted.) Each such group is identified uniquely in GAP (version 4.3). If it is cataloged as the mth nonabelian group of order n in GAP, it can be obtained by the GAP command `AllGroups(n, IsCommutative, false)[m]`, for instance. Accordingly, we use the name $2n : m$ for the corresponding class of Moufang loops. (Warning: Since we cannot guarantee that the GAP libraries of groups will not change in the future, the reader should note the version of GAP carefully.)

When the seed of order $2n$ is not of the form $M(G,2)$, we denote the class by $2n : xm$, as in $36 : x1$.

Under `|nucleus|`, we give the size of the nucleus of all loops in the class.

Under `assoc. subloop`, we give the isomorphism type of the associator subloop of all loops in the class, using standard group-theoretical notation. Hence, C_m denotes the cyclic group of order m, Q_8 denotes the quaternion group of order 8, and A_4 denotes the alternating group of order 12.

Under `seed(s)`, we list the seed that was used to generate the class. When an integer m is listed, the seed is the loop $M(G,2)$ where G is the mth nonabelian group of order n. When several integers are listed, then all corresponding loops $M(G,2)$ can be used as seeds, but only the first one was actually used in the search. In the remaining cases $2n : xm$, we give the seed explicitly by referring to smaller Moufang loops. Here, `MoufangLoop(n,m)` denotes the mth Moufang loop of order n, as cataloged in [16] and in the package LOOPS.

Under `extra?` we specify if all loops in the class are extra loops (yes), or if all loops in the class are not extra loops (no). No other scenarios can occur by Lemma 3.2.

Under `|class|` we specify the number of nonisomorphic loops forming the class.

5.1. **What the results indicate.** As we have already mentioned, both constructions preserve the nucleus (as a set) and the associator subloop (as a loop). Let us therefore say that the *parameter* of a seed M is the triple ($|M|$, $|N(M)|$, isomorphism class of $A(M)$).

With one exception (classes $54:01$, $54:02$), two seeds $M(G,2)$ are in the same class of loops if and only if their parameters coincide.

More importantly, the seeds $M(G,2)$ generate all Moufang 2-loops of order less than 64, and all but 4 classes of Moufang loops of order less than 64. The four exceptional cases are all generated by seeds of the form $M \times C_{2k+1}$, where M is a Moufang loop of smaller order.

Table 1 accounts for all Moufang loops of order less than 63, according to the classification [16].

Remark 5.1. *It is known that the* 267 *groups of order* 64 *split into two classes* (*of size* 261 *and* 6) *with respect to the modifications. We have checked that none of the* 6 *groups in the second class is of the form* $M(G,2)$*, where* G *is a group of order* 32*.*

6. The Algorithm

This section describes the main steps of the algorithm used to calculate the class $\mathcal{M}(M)$ from a seed M.

6.1. **Platform.** All calculations were implemented in GAP version 4.3 for Windows, using the package LOOPS. The search ran for about 2 weeks on a PC with a 2GHz processor.

6.2. **Input.** A Moufang loop M (seed), flagged as unexplored.

6.3. **Output.** The class of Moufang loops $\mathcal{M}(M)$ (with one Moufang loop for every isomorphism type) together with data that describes how to build all loops of $\mathcal{M}(M)$ from the seed M.

6.4. **Main cycle.** Let L be the first unexplored loop. If there is none, the search is over. Otherwise:

(i) determine all normal subloops S of L such that L/S is cyclic of even order or dihedral of doubly even order,
(ii) for every normal subloop S of L, determine all admissible parameters of the constructions of Section 3 (e.g., in the cyclic case, find all pairs (α, h) where α is a generator of L/S and $h \in S \cap Z(L)$),
(iii) using the parameters found in step (ii), construct the modifications $(L, *)$ from L,
(iv) store those newly found loops $(L, *)$ that are not isomorphic to any of the previously found loops; flag them as unexplored,
(v) flag L as explored.

TABLE 1. Classes of nonassociative Moufang loops obtained by the cyclic and dihedral constructions from the indicated seeds. All nonassociative Moufang loops of order less than 64 are accounted for in this table.

class	|nucleus|	assoc. subloop	seed(s)	extra?	|class|
12 : 01	1	C_3	1	no	1
16 : 01	2	C_2	1, 2	yes	5
20 : 01	1	C_5	1	no	1
24 : 01	2	C_3	1, 3	no	4
24 : 02	1	$C_2 \times C_2$	2	no	1
28 : 01	1	C_7	1	no	1
32 : 01	4	C_2	1–3, 7–9	yes	60
32 : 04	2	C_4	4-6	no	11
36 : 01	1	C_9	1	no	1
36 : 02	3	C_3	2	no	1
36 : 03	1	$C_3 \times C_3$	3	no	1
36 : $x1$	3	C_3	MoufangLoop$(12, 1) \times C_3$	no	1
40 : 01	2	C_5	1, 3	no	4
40 : 02	1	C_5	2	no	1
42 : 01	1	C_7	1	no	1
44 : 01	1	C_{11}	1	no	1
48 : 01	4	C_3	1, 4, 5, 12	no	19
48 : 02	2	Q_8	2	no	2
48 : 03	2	C_6	3, 5, 7	no	11
48 : 08	6	C_2	8, 9	yes	11
48 : 10	1	A_4	10	no	1
48 : 11	2	$C_2 \times C_2$	11	no	2
48 : $x1$	6	C_2	MoufangLoop$(16, 4) \times C_3$	yes	5
52 : 01	1	C_{13}	1	no	1
54 : 01	3	C_3	1	no	1
54 : 02	3	C_3	2	no	1
56 : 01	2	C_7	1, 2	no	4
60 : 01	5	C_3	1	no	1
60 : 02	3	C_5	2	no	1
60 : 03	1	C_{15}	3	no	1
60 : $x1$	3	C_5	MoufangLoop$(20, 1) \times C_3$	no	1
60 : $x2$	5	C_3	MoufangLoop$(12, 1) \times C_5$	no	1
64 : 01	8	C_2	1–3, 10, 14, 18–22, 32, 33	yes	1316
64 : 04	2	$C_2 \times C_2$	4–6	no	18
64 : 07	4	C_4	7–9, 11–13, 34–37	no	214
64 : 15	2	C_8	15–17	no	11
64 : 23	4	$C_2 \times C_2$	23–31	yes	2612
64 : 38	2	C_4	38, 39	no	44
64 : 43	2	C_2	43, 44	yes	47

TABLE 2. Number of isomorphism classes of nonabelian groups of order $1 \leq n \leq 32$.

order	6	8	10	12	14	16	18	20	21	22	24	26	27	28	30	32
nonab. groups	1	2	1	3	1	9	3	3	1	1	12	1	2	2	3	44

7. Speeding up the algorithm

The steps (i), (ii) and (iv) are expensive, especially step (iv). We describe in this section how to speed up (ii) and (iv). Many additional improvements of programming character were incorporated into the algorithm but we do not mention them here.

7.1. **Speeding up step (ii).** The problem with step (ii) is that there are typically very many parameters S, α, β, γ, h that can be used to modify the loop L into $(L, *)$. Since we are only interested in the isomorphism type of the resulting loop $(L, *)$, we would like to know which parameters yield isomorphic loops. This topic has been studied for groups in [10]. For example, it is proved in [10] that the cyclic modification $G[S, \alpha, h]$ is independent of the generator α of S, in the sense that for two generators α, α' of S and $h \in S \cap Z(L)$ there is $h' \in S \cap Z(L)$ such that $G[S, \alpha, h]$ is isomorphic to $G[S, \alpha', h']$. Such an observation speeds up the search substantially, since a cyclic group of order n contains $\varphi(n)$ generators, where φ (the Euler function) counts the number of positive integers relatively prime to n.

Unfortunately, it is by no means easy to generalize the results of [10] into the nonassociative case. (In fact, it is often impossible, for we have found counterexamples to some generalizations of [10].) What follows is a generalization of the above result (independence of α in the cyclic construction) for a class of Moufang loops with the associator subloop contained in the center. By [18], all extra 2-loops L of order less than 512 satisfy $A(L) \subseteq Z(L)$. Table 1 shows that the two largest classes of Moufang loops of order 64 consist of extra loops.

We follow the reasoning of [10], often word for word. The proofs had to be expanded substantially when diassociativity did not apply.

Lemma 7.1. *Let σ be as in Section 3. For every i, $j \in M = \{-m+1, \dots, m\}$, we have:*

(i) $\sigma(i + j) + \sigma((i \oplus j) - i) = 0$,
(ii) $\sigma(m + j) + \sigma((m \oplus j) + m) = 1$.

Proof. We have $(i \oplus j) - i = j - 2m\sigma(i + j)$. Therefore $\sigma((i \oplus j) - i)$ is opposite to $\sigma(i + j)$. This shows (i).

Let us prove (ii). If $j \leq 0$, we have $\sigma(m+j) = 0$ and $\sigma((m \oplus j)+m) = \sigma(2m+j)$. Since $2m + j > 2m - m = m$, we are done. If $j > 0$, we have $\sigma(m + j) = 1$, and $\sigma((m \oplus j) + m) = \sigma(j) = 0$. □

When $(G, *)$ is a obtained from G by the cyclic or the dihedral construction, denote by x^* the inverse of x in $(G, *)$, and by x_i the ith power of x in $(G, *)$.

Lemma 7.2. *Let $G(*) = G[S, \alpha, h]$ be a cyclic modification of G such that $|G/S| = 2m$. Then for $x \in G$ we have*

$$x^* = \begin{cases} x^{-1}, & x \notin \alpha^m, \\ x^{-1}h^{-1}, & x \in \alpha^m. \end{cases}$$

Proof. Assume that $x \in \alpha^i$, $i \in M \setminus \{m\}$. Then $x^{-1} \in \alpha^{-i}$, and therefore $x * x^{-1} = xx^{-1}h^{\sigma(0)} = xx^{-1} = 1$. Assume that $x \in \alpha^m$. Then $x^{-1} \in \alpha^{-m} = \alpha^m$. Therefore $x^{-1}h^{-1} \in \alpha^m$, too, and we have $x * (x^{-1}h^{-1}) = xx^{-1}h^{-1}h^{\sigma(m+m)} = 1$. □

Lemma 7.3. *Under the assumptions of Lemma 7.2, we have $x * y * x^* = xyx^{-1}$, $x^* * y * x = x^{-1}yx$ for every x, $y \in G$.*

Proof. We only prove $x*y*x^* = xyx^{-1}$. The other equality is proved along similar lines. Let $x \in \alpha^i$, $y \in \alpha^j$, $i \in M$, $j \in M$.

First assume that $i \neq m$. Then, by Lemma 7.2, $x^* = x^{-1} \in \alpha^{-i}$, and we have $x * y * x^* = xyh^{\sigma(i+j)} * x^{-1} = xyx^{-1}h^{\sigma(i+j)+\sigma((i\oplus j)-i)}$. We are done by Lemma 7.1(i).

Now assume that $i = m$. Then, by Lemma 7.2, $x^* = x^{-1}h^{-1} \in \alpha^m$, and we have $x * y * x^* = xyh^{\sigma(m+j)} * (x^{-1}h^{-1}) = xyx^{-1}h^{\sigma(m+j)+\sigma((m\oplus j)+m)-1}$. We are done by Lemma 7.1(ii). □

Lemma 7.4. *Assume that $(G, *) = G[S, \alpha, h]$, $|G/S| = 2m$, and $x \in \alpha$. Then*

$$x_i = \begin{cases} x^i, & i \in M, \\ x^i h, & m < i \leq 2m. \end{cases}$$

Furthermore, if $x \in \alpha^j$ and $j \in M$, we have $x_{2m} = x^{2m}h^j$.

Proof. First note that $x^i \in \alpha^i$ for every i. Therefore $x_i * x = x_i x$ for every $i \in \{0, \dots, m-1\}$. This means that $x_i = x^i$ for every $i \in \{0, \dots, m\}$.

Consider x_i for $i \in \{-m+1, \dots, -1\}$. We have $(x_i)^* = x_{-i}$. By the previous paragraph, $x_{-i} = x^{-i} = (x^i)^{-1}$. By Lemma 7.2, $(x^i)^{-1} = (x^i)^*$. Altogether, we have $(x_i)^* = (x^i)^*$, and thus $x_i = x^i$.

We have $x_m * x = x_m xh = x^m xh \in \alpha^{-m+1}$. It then follows that $x_i = x^i h$ for every $i \in \{m+1, \dots, 2m\}$.

Let $x \in \alpha^j$, $j \in M$. Given x, $x' \in \alpha^k$, we have $x_n = x^n h^\varepsilon$ and $x'_n = (x')^n h^\varepsilon$ for the same ε, because the value of the exponent ε depends only on n and k. We can therefore assume that $x = y^j$ for some $y \in \alpha$. Using the above results, we have $x_{2m} = (y^j)_{2m} = (y_j)_{2m} = y_{2mj} = (y_{2m})_j = (y_{2m})^j = (y^{2m}h)^j = (y^j)^{2m}h^j = x^{2m}h^j$. □

When L is a Moufang loop, the associator subloop $A(L)$ can be defined equivalently as the smallest normal subloop H of L such that L/H is associative. Therefore $A(L) \leq S$ anytime S is among the parameters of a cyclic modification of L.

Proposition 7.5. *Let $G_1 = (G, \cdot)$, $G_2 = (G, \circ)$ be two Moufang loops with common normal subloop S, and let $x \in G$ be such that:*

(i) *$G_1/S \cong G_2/S$ are cyclic of order $2m$,*
(ii) *both G_1, G_2 are generated by $S \cup \{x\}$,*
(iii) *the $2m$-th powers of x coincide in G_1, G_2,*
(iv) *the conjugates s^x for $s \in S$ coincide in G_1 and G_2,*
(v) *the multiplication in S is the same in G_1, G_2,*
(vi) *the associators coincide in G_1, G_2,*

(vii) $A(G_i) \leq Z(G_i) \cap S$, *for* $i = 1, 2$,
(viii) $[a, b, cd] = [a, b, c \circ d]$ *for every* $a, b, c \in G$.
Then G_1 *is isomorphic to* G_2.

Proof. Any element of G_1 decomposes uniquely as $x^i s$, where $i \in M = \{-m + 1, \ldots, m\}$, $s \in S$. Similarly, any element of G_2 decomposes uniquely as $x_i \circ s$, where we use x_i to denote the ith power of x in G_2. Then the map $\varphi : G_2 \to G_1$, $x_i \circ s \mapsto x^i s$ is a bijection.

We now show that $\varphi(x_k \circ s) = x^k s$ for every $k \in \{-2m + 2, \ldots, 2m\}$. When $k \in M$, we are done by the definition of φ. Assume that $k > m$. Since $k - 2m \in M$ and x_{2m} is an element of S, we have $\varphi(x_k \circ s) = \varphi(x_{k-2m} \circ x_{2m} \circ s) = x^{k-2m}(x_{2m} \circ s)$. By (v), $x_{2m} \circ s = x_{2m} s$. Thus, by (iii), $\varphi(x_k \circ s) = x^{k-2m} x^{2m} s = s$. Similarly, when $k < -m + 1$, we have $\varphi(x_k \circ s) = \varphi(x_{k+2m} \circ x_{-2m} \circ s) = x^{k+2m}(x_{-2m} \circ s) = x^{k+2m} x_{-2m} s = x^{k+2m} x^{-2m} s = s$.

We also claim that $\varphi(s \circ x_k) = s x^k$ for $s \in S$, $k \in \{-2m + 2, \ldots, 2m\}$. Since $x_{-k} \circ s \circ x_k \in S$, we have $\varphi(s \circ x_k) = \varphi(x_k \circ x_{-k} \circ s \circ x_k) = x^k(x_{-k} \circ s \circ x_k)$. By (iv), the last expression is equal to $x^k s$.

Define a new multiplication $*$ on G by $x * y = \varphi(\varphi^{-1}(x) \circ \varphi^{-1}(y))$. Then $(G, *)$ is isomorphic to G_2. We are going to show that the multiplication $*$ coincides with the multiplication in G_1.

Now, for $i, j \in M$ and $s, t \in S$ we have $(x^i s) * (t x^j) = \varphi((x_i \circ s) \circ (t \circ x_j))$. By (vi) and (vii), $(x_i \circ s) \circ (t \circ x_j) = x_i \circ (s \circ (t \circ x_j)) \circ [x_i, s, t \circ x_j] = x_i \circ (s \circ t) \circ x_j \circ [s, t, x_j]_{-1} \circ [x_i, s, t \circ x_j] = x_i \circ (s \circ t) \circ [s, t, x_j]_{-1} \circ [x_i, s, t \circ x_j] \circ x_{-i} \circ x_{i+j}$. By (v), (vii) and (viii), we can simplify this further to $x_i((st)[s, t, x_j]^{-1}[x_i, s, t x_j]) x_{-i} \circ x_{i+j}$. Therefore, by the preceding paragraphs and (iv), $(x^i s) * (t x^j) = x^i (st)[s, t, x_j]^{-1}[x_i, s, t x_j] x^{-i} x^{i+j}$.

On the other hand, $(x^i s) \cdot (t x^j) = x^i (st)[s, t, x_j]^{-1}[x_i, s, t x_j] x^{-i} x^{i+j}$, and we are through. □

Proposition 7.6. *Suppose that* G *is a Moufang 2-loop such that* $A(G) \leq Z(G)$. *Suppose that* S *is a normal subloop of* G *such that* G/S *is cyclic of order* $2m$, $G/S = \langle \alpha \rangle$. *Let* j *be relatively prime to* $2m$, *and let* $k \in M = \{-m + 1, \ldots, m\}$ *be such that* $jk \equiv 1 \pmod{2m}$. *Then* $G[S, \alpha^j, h] \cong G[S, \alpha, h^k]$.

Proof. Set $G_1 = G[S, \alpha, h^k]$, $G_2 = G[S, \alpha^j, h]$. Pick $x \in \alpha$. We are going to check all assumptions of Proposition 7.5. By Lemma 7.4, both G_1 and G_2 are generated by $S \cup \{x\}$, and the $2m$-th power of x in G_1 is equal to $x^{2m} h^k$. Since $\alpha = (\alpha^j)^k$, the Lemma also implies that the $2m$-th power of x in G_2 is equal to $x^{2m} h^k$. By Lemma 7.3, the conjugates s^x are the same in G_1 and G_2. The multiplication in S is the same in G_1, G_2 (and G) by definition. By Theorem 3.1, the associators of G_i and G are the same for $i = 1, 2$. Thus the associators of G_1 and G_2 are the same. By the same theorem, $A(G_i) \subseteq S$ for $i = 1, 2$. Consider the associators $[a, b, cd]$, $[a, b, c \circ d]$, where $\cdot$ is the multiplication in G, and $\circ$ is the multiplication in G_1. Note that $c \circ d$ differs from cd by a central element (namely a power of h). Therefore $[a, b, cd] = [a, b, c \circ d]$. Similarly for G and G_2. Thus all assumptions of Proposition 7.5 are satisfied, and $G_1 \cong G_2$ follows. □

Corollary 7.7. *Let* G *be a Moufang loop with normal subloop* S *such that* G/S *is cyclic of order* $2m$. *Let* α, α' *be two generators of* G/S. *Then for every* $h \in S \cap Z(G)$ *there is* $h' \in S \cap Z(G)$ *such that* $G[S, \alpha, h] \cong G[S, \alpha', h']$.

Proof. The generators of G/S are exactly the powers α^j, where $(j, 2m) = 1$. □

TABLE 3. The importance of discriminators in the search.

class	|class|	discrim. types	max. with same discrim.	max. modifications
16 : 01	5	5	1	3
32 : 01	60	58	2	14
32 : 04	11	11	1	5
64 : 01	1316	1104	6	38
64 : 04	18	18	1	6
64 : 07	214	174	5	29
64 : 15	11	11	1	5
64 : 23	2612	2331	6	103
64 : 38	44	44	1	19
64 : 43	47	47	1	11

7.2. **Speeding up step (iv).** The main bottleneck of the search is to decide if the newly found loops $(L, *)$ are isomorphic to any of the previously found loops. We are going to describe here how this problem was overcome. In fact, it appears that the following algorithm performs very well for all (power associative) loops, and 2-loops in particular. Its idea is natural and simple, but the details, based on theory and some heuristic, are not so trivial.

Our task is to determine if two loops L, M of order n are isomorphic. The main problem is that the space of possible isomorphisms is huge, consisting of $n!$ bijections. Naturally, given an element x of L, it cannot be mapped onto an arbitrary element of M if the mapping is supposed to be an isomorphism. Certain invariants, such as the order of x, must be preserved. The trick is to find invariants that are cheap yet powerful, in the sense that the set of possible images of x is small. Here are the invariants actually used in the search:

For $x \in L$, let $I(x) = (|x|, s, f, (c_1, c_2, \ldots, c_n))$, where

$$s = |\{y \in L; x = y^2\}|,$$
$$f = |\{y \in L; x = y^4\}|,$$
$$c_i = |\{y \in L; |y| = i,\ xy = yx\}.$$

For a loop L and an invariant I, let

$$d_I = |\{x \in L;\ I(x) = I\}|,$$
$$D(L) = \{(I(x), d_{I(x)});\ x \in L\}.$$

The distinguishing power of the *discriminator* $D(L)$ is tremendous. Table 3 illustrates this eloquently for Moufang 2-loops. For instance, the table shows that the 2612 loops forming the class 64 : 23 give rise to 2331 different discriminators in such a way that there are no more than 6 loops with the same discriminator. Hence, by precalculating the discriminator once, at most 6 instead of 2612 loops have to be actually tested for isomorphism at any given time in the search through the class 64 : 23.

Table 3 also lists the maximum number of nonisomorphic modifications $(L, *)$ of a loop L in the given class. This shows that the constructions of Section 3 often produce a large amount of nonisomorphic loops in one step.

8. The LOOPS package for GAP

The purpose of the GAP [13] package LOOPS [20] is to implement calculation with loops and quasigroups in GAP. The package exists only in a beta version and has not yet been accepted as a GAP shared package. It is available online [20], together with installation instructions.

All Moufang loops found in this paper have now been included in the libraries of LOOPS. Then mth nonassociative Moufang loop of order n can be retrieved by the command `MoufangLoop(n,m)`.

Since [16] already contains all nonassociative Moufang loops of order less than 64, LOOPS catalog numbers correspond to those of [16]. Hence, for $n < 64$, the Moufang loop called n/m in [16] is indeed isomorphic to `MoufangLoop(n,m)` of LOOPS. The numbering of Moufang loops of order 64 of LOOPS is based on our search. For instance, the first 1316 Moufang loops of order 64 are those of class $64 : 01$.

Moreover, for a Moufang loop L of order at most 64, the LOOPS command `IsomorphismTypeOfMoufangLoop(L)` returns the catalog number of L and the corresponding isomorphism, if possible. This command will be handy in the search for additional Moufang loops of order 64, should they exist.

9. Conjectures

Conjecture 9.1. *There are* 4262 *nonassociative Moufang loops of order* 64*, as listed in this paper.*

The above conjecture holds if the following statement is true for $2^n = 64$: *Every nonassociative Moufang* 2*-loop of order* 2^n *is a modification of a loop* $M(G, 2)$*, where* G *is a nonabelian group of order* 2^{n-1}. In view of Remark 5.1, the word "nonassociative" is essential in the statement. Is the statement true for 64? Is it true for 128?

Finally, it is customary to classify loops with respect to isotopism in addition to isomorphism. Recall that two loops L, H are *isotopic* if there are bijections α, β, $\gamma : L \to H$ such that $\alpha(x)\beta(y) = \gamma(xy)$ for every x, $y \in L$. We ask: *How do the modifications behave with respect to isotopism? How many isotopism classes of nonassociative Moufang loops of order* 64 *are there?*

10. Acknowledgement

I would like to thank Edgar G. Goodaire for providing me with electronic multiplication tables of Moufang loops of order at most 32. I also thank anonymous referees for several useful comments, and for an improvement of the proof of Proposition 7.5.

References

[1] Hans Ulrich Besche, Bettina Eick and E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. **5**, 623–644.

[2] Orin Chein, Moufang loops of small order, *Mem. Amer. Math. Soc.* **13** (1978), 31–51.

[3] Orin Chein and Edgar G. Goodaire, *Minimally nonassociative nilpotent Moufang loops*, J. Algebra **268** (2003), 327–342.

[4] Orin Chein and D. A. Robinson, *An "extra" law for characterizing Moufang loops*, Proc. Amer. Math. Soc. **33**, no. **1** (May, 1972), 29–32.
[5] Charles J. Colbourn and Alexander Rosa, Triple systems, *Oxford Mathematical Monographs*, The Clarendon Press, Oxford University Press, New York, 1999.
[6] John H. Conway, On Numbers and Games, second edition, A K Peters, Natick, Massachusetts, 2001.
[7] John H. Conway and Derek A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A K Peters, 2003.
[8] Aleš Drápal, *How far apart can the group multiplication tables be?*, European J. Combin. **13** (1992), no. **5**, 335–343.
[9] Aleš Drápal, *Non-isomorphic 2-groups coincide at most in three quarters of their multiplication tables*, European J. Combin. **21** (2000), no. **3**, 301–321.
[10] Aleš Drápal, *Cyclic and dihedral constructions of even order*, Comment. Math. Univ. Carolinae **44**, **4** (2003), 593–614.
[11] Aleš Drápal and Petr Vojtěchovský, *Moufang loops that share associator and three quarters of their multiplication tables*, to appear in Rocky Mountain Journal of Mathematics.
[12] Aleš Drápal annd Natalia Zhukavets, *On multiplication tables of groups that agree on half of the columns and half of the rows*, Glasg. Math. J. **45** (2003), no. **2**, 293–308.
[13] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews (1999). (Visit http://www-gap.dcs.st-and.ac.uk/~gap).
[14] G. Glauberman, *On loops of odd order. II.*, J. Algebra **8** (1968), 393–414.
[15] G. Glauberman and C. R. B. Wright, *Nilpotence of finite Moufang 2-loops*, J. Algebra **8** (1968), 415–417.
[16] Edgar G. Goodaire, Sean May and Maitreyi Raman, The Moufang Loops of Order less than 64, Nova Science Publishers, 1999.
[17] Alexandr N. Grishkov and Andrei V. Zavarnitsine, Lagrange's theorem for Moufang loops, submitted.
[18] Michael Kinyon and Kenneth Kunen, *The structure of extra loops*, to appear in Quasigroups and Related Systems.
[19] M. W. Liebeck, *The classification of finite simple Moufang loops.* Math. Proc. Cambridge Philos. Soc. **102** (1987), no. 1, 33–47.
[20] LOOPS version 0.997, package for GAP 4, by Gábor P. Nagy and Petr Vojtěchovský. (Available at http://www.math.du.edu/loops)
[21] L. Paige, *A Class of Simple Moufang Loops*, Proceedings of the American Mathematical Society **7**, Issue **3** (June 1956), 471–482.
[22] Hala O. Pflugfelder, Quasigroups and Loops: Introduction, *Sigma Series in Pure Mathematics* **7**, Heldermann Verlag Berlin, 1990.
[23] J. D. Phillips and Petr Vojtěchovský, *A scoop from groups: new equational foundations for loops*, submitted.
[24] Tonny A. Springer and Ferdinand D. Veldkamp, Octonions, Jordan Algebras and Exceptional Groups, *Springer Monographs in Mathematics*, Springer Verlag, 2000.
[25] Jacques Tits and Richard M. Weiss, Moufang polygons, *Springer Monographs in Mathematics*, Springer Verlag, 2003.
[26] Petr Vojtěchovský, *On Hamming distances of groups (O Hammingově vzdálenosti grup)*, M.S. thesis, Department of Algebra, Charles University,

Prague, June 1998, in Czech.

[27] Petr Vojtěchovský, *Finite simple Moufang loops*, Ph.D. dissertation, Department of Mathematics, Iowa State University, Ames, Iowa, 2001.

[28] Petr Vojtěchovský, *Generators for finite simple Moufang loops*, Journal of Group Theory **6** (2003), 169–174.

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, 80208, Colorado, U.S.A.

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