The Moufang Loops of Order 64 and 81

Gábor P. Nagy

Bolyai Institute, University of Szeged, Aradi vertanuk tere 1, 6720 Szeged, Hungary

Petr Vojtěchovský

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

Abstract

We classify Moufang loops of order 64 and 81 up to isomorphism, using a linear algebraic approach to central loop extensions. In addition to the 267 groups of order 64, there are 4262 nonassociative Moufang loops of order 64. In addition to the 15 groups of order 81, there are 5 nonassociative Moufang loops of order 81, 2 of which are commutative.

Key words: Moufang loop, code loop, 2-loop, classification of Moufang loops, GAP.

1. Introduction

1.1. Mathematical background

Let Q be a set with one binary operation, denoted by juxtaposition. For $x \in Q$, define the *left translation* L_x and the *right translation* R_x by $L_x(y) = xy$, $R_x(y) = yx$. Then Q is a *loop* if all translations are bijections of Q, and if Q possesses a *neutral element* 1 satisfying $1x = x = x1$ for every $x \in Q$.

A loop Q is *Moufang* if it satisfies the Moufang identity $(xy)(zx) = x((yz)x)$. Although Moufang loops are not associative in general, they have many properties we are familiar with from the theory of groups. For instance, every element x of a Moufang loop is paired with its inverse x^{-1} satisfying $x^{-1}(xy) = y = (yx)x^{-1}$, any two elements generate a subgroup (this property is called *diassociativity*), and any three elements that associate generate a subgroup (the famous Moufang theorem).

Indeed, the fact that the methods used in this paper work for Moufang loops can be seen as another confirmation of their proximity to groups.

⋆ Petr Vojtěchovský supported by the PROF 2006 grant of the University of Denver.

Email addresses: nagyg@math.u-szeged.hu (Gábor P. Nagy), petr@math.du.edu (Petr Vojtěchovský).

The *center* $Z(Q)$ of a loop Q consist of all elements that commute and associate with all other elements of Q. A subloop S of a loop Q is a nonempty subset of Q that happens to be a loop with respect to the multiplication inherited from Q. To see whether a subset $S \neq \emptyset$ of a Moufang loop Q is a subloop of Q, it suffices to check that S is closed under multiplication and inverses.

A subloop S of a loop Q is *normal* in Q if S is invariant under all inner maps $R_{xy}^{-1}R_yR_x$, $L_{yx}^{-1}L_yL_x$ and $L_x^{-1}R_x$. The center $Z(Q)$ is a normal subloop of Q.

A loop Q is *centrally nilpotent* if the sequence

$$Q,\ Q/Z(Q),\ (Q/Z(Q))/Z(Q/Z(Q)),\ \ldots$$

eventually yields the trivial loop.

Loops of order p^k, p a prime, are known as p-loops. A finite Moufang loop Q is a p-loop if and only if every element of Q has order that is a power of p.

Let Q be a centrally nilpotent p-loop. The *Frattini subloop* $\Phi(Q)$ of Q is the intersection of all maximal subloops of Q, or, equivalently, the subloop consisting of all non-generators of Q. Then $Q/\Phi(Q)$ is an elementary abelian p-group and $|Q/\Phi(Q)| = p^d$, where d is the size of a smallest generating set of Q, by (Bruck, 1971, Theorem 2.3).

An *isotopism* of loops Q_1, Q_2 is a triple (α, β, γ) of bijections $Q_1 \to Q_2$ such that $\alpha(x)\beta(y) = \gamma(xy)$ holds for every x, $y \in Q_1$. Then Q_2 is an *isotope* of Q_1.

Clearly, when two loops are isomorphic, they are also isotopic. The converse is not true in general. If all isotopes of a loop Q are already isomorphic to Q, we call Q a *G-loop* (since groups have this property). Moufang 2-loops are G-loops, and that is why a classification of such loops up to isomorphism is also a classification up to isotopism.

We refer the reader to (Bruck, 1971) and (Pflugfelder, 1990) for a systematic introduction to the theory of loops.

1.2. Historical background

The classification of Moufang loops started in earnest with the work of Chein. In (Chein, 1978), he described all Moufang loops of order less than 64. Chein's results are conveniently summarized in (Goodaire, May and Raman, 1999), and the respective loops are accessible in electronic form in (Nagy and Vojtěchovský, 2007). Table 1 gives the number of pairwise nonisomorphic nonassociative Moufang loops of order n for every $1 \leq n \leq 63$ for which at least one nonassociative Moufang loop exists.

Table 1. The number $M(n)$ of nonassociative Moufang loops of order n less than 64.

n	12	16	20	24	28	32	36	40	42	44	48	52	54	56	60
$M(n)$	1	5	1	5	1	71	4	5	1	1	51	1	2	4	5

Certain extensions that proved useful in group theory, see (Drápal, 2003), were used by the second author in (Vojtěchovský, 2006) to construct 4262 nonassociative Moufang loops of order 64. It was also conjectured in (Vojtěchovský, 2006) that no additional nonassociative Moufang loops of order 64 exist.

The related question "*For which integers n there exists a nonassociative Moufang loop of order n?*" has been studied extensively but is not fully resolved.

By (Chein and Rajah, 2003), a nonassociative Moufang loop of order $2m$ exists if and only if a nonabelian group of order m exists. Hence, a nonassociative Moufang loop of

order 2^k exists if and only if $k > 3$, and for every odd $m > 1$ there is a nonassociative Moufang loop of order $4m$. Here is the case $2m$, m odd:

Theorem 1 (Chein and Rajah, 2003, Corollary 2.4)**.** *Every Moufang loop of order $2m$, $m > 1$ odd, is associative if and only if $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1 < \cdots < p_k$ are odd primes and where*

(i) $\alpha_i \leq 2$, *for all* $i = 1, \ldots, k$,
(ii) $p_j \not\equiv 1 \pmod{p_i}$, *for any* i *and* j,
(iii) $p_j^2 \not\equiv 1 \pmod{p_i}$, *for any* i *and any* j *with* $\alpha_j = 2$.

Concerning odd orders, we have:

Theorem 2 (Leong and Rajah, 1997)**.** *Every Moufang loop of order $p^\alpha q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ is associative if $p < q_1 < \cdots < q_k$ are odd primes, and if one of the following conditions holds:*

(i) $\alpha \leq 3$ *and* $\alpha_i \leq 2$,
(ii) $p \geq 5$, $\alpha \leq 4$, *and* $\alpha_i \leq 2$.

In (Rajah, 2001), Rajah showed that for odd primes $p < q$ a nonassociative Moufang loop of order pq^3 exists if and only if $q \equiv 1 \pmod{p}$. It is well-known that there are nonassociative Moufang loops of order 3^4. Indeed, smallest nonassociative commutative Moufang loops are of order 3^4—see (Bol, 1937) for the first example attributed to Zassenhaus, and (Kepka and Němec, 1981) for the second nonassociative commutative Moufang loop of order 3^4. Wright (Wright, 1965) constructed a nonassociative Moufang loop of order p^5 for every prime p. Coming back to the classification results, it is shown in (Nagy and Valsecchi, 2007) that there are precisely 4 nonassociative Moufang loops of order p^5 for every prime $p \geq 5$.

1.3. Main result

In this paper we verify computationally:

Theorem 3. *There are* 4262 *pairwise nonisomorphic nonassociative Moufang loops of order* 64.

Theorem 4. *There are* 5 *pairwise nonisomorphic nonassociative Moufang loops of order* 81, 2 *of which are commutative. All* 5 *of these loops are isotopes of the* 2 *commutative ones.*

Here is our strategy, completely different from that of (Vojtěchovský, 2006):

Every Moufang loop Q of order p^{k+1}, p a prime, is a central extension of a Moufang loop K of order p^k by the p-element field $\mathbb{F}_p$, by Corollary 13. Moreover, if K is at most two-generated, then Q is associative, by Proposition 8. Therefore, in order to determine all nonassociative Moufang loops of order p^{k+1} one only needs to consider all central extensions of at least three-generated Moufang loops K of order p^k by $\mathbb{F}_p$.

Each such extension is determined by a Moufang cocycle, a map $K \times K \to \mathbb{F}_p$ satisfying certain cocycle identities (2.1), (2.2). All cocycles $K \times K \to \mathbb{F}_p$ form a vector space $\mathcal{C}(K)$ of dimension $p^{2k} - 2p^k + 1$, and the Moufang cocycles form a subspace $\mathcal{M}(K)$ of $\mathcal{C}(K)$.

Let $\mathcal{B}(K)$ be the subspace of coboundaries $K \times K \to \mathbb{F}_p$, as defined in (2.3). Every coboundary is a Moufang cocycle, by Lemma 10, so $\mathcal{M}(K)$ decomposes as $\mathcal{B}(K) \oplus \mathcal{D}(K)$

for some $\mathcal{D}(K)$. The system of linear equations whose solution determines $\mathcal{M}(K)$ has about p^{3k} equations in p^{2k} variables. The subspace $\mathcal{B}(K)$ can be constructed directly, and its dimension can be determined by means of generators of K, cf. Lemma 11.

Since two cocycles that differ by a coboundary give rise to isomorphic loops, by Lemma 9, the study of central Moufang extensions of K by $\mathbb{F}_p$ reduces to the study of the vector space $\mathcal{D}(K)$.

When the dimension of $\mathcal{D}(K)$ is small, it is possible to calculate all cocycles of $\mathcal{D}(K)$, to construct the corresponding extensions, and to test the resulting Moufang loops for isomorphism. (The isomorphism test is a nontrivial problem, but the *ad hoc* invariants used in the LOOPS package prove sufficient here. See (Vojtěchovský, 2006) for a brief description of the invariants used in the isomorphism test.)

Fortunately—and somewhat unexpectedly—the dimension of $\mathcal{D}(K)$ happens to be low for every Moufang loop K of order 32 and 27, with the exception of the elementary abelian 2-group of order 32. We do not know how to estimate the dimension of $\mathcal{D}(K)$ (and hence of $\mathcal{M}(K)$) theoretically. See Section 3 for more.

To speed up the search, we can further reduce the number of cocycles from $\mathcal{D}(K)$ that need to be considered by taking advantage of the action of the automorphism group of K on $\mathcal{M}(K)$, as described in Section 4.

The troublesome case where K is the elementary abelian group of order 32 has to be handled separately. Central extensions of elementary abelian 2-groups by $\mathbb{F}_2$ are known as *code loops*—a well-studied variety of Moufang loops with a rich interplay between the associator map, the commutator map, and the squaring map. We take advantage of this interplay (combinatorial polarization), and finish the search, as explained in Section 5.

2. Central extensions

Let K, A be loops. Then a loop Q is an *extension* of K by A if A is a normal subloop of Q such that Q/A is isomorphic to K. An extension Q of K by A is *central* if A is a subloop of $Z(Q)$.

Let us call a map $f : K \times K \to A$ satisfying

$$f(1, x) = f(x, 1) = 1 \tag{2.1}$$

a (*loop*) *cocycle*.

Proposition 5. *Let K be a loop, A an abelian group, and $f : K \times K \to A$ a cocycle. Define multiplication $*$ on $K \times A$ by*

$$(x, a) * (y, b) = (xy,\ abf(x, y)).$$

Then $Q = (K \times A, *)$ is a loop, in fact a central extension of K by A.

Proof. It is easy to see that Q is a quasigroup. The cocycle condition (2.1) guarantees that Q has a neutral element, namely $(1, 1)$, and that $1 \times A \leq Z(Q)$. □

We denote the resulting central extension by $E(K, A, f)$.

The following result belongs to loop-theoretical folklore:

Theorem 6 (Central extensions for loops.)**.** *Let Q, K and A be loops such that $A \leq Z(Q)$. Then Q is a central extension of A by K if and only if there is a cocycle $f : K \times K \to A$ such that Q is isomorphic to $E(K, A, f)$.*

Proof. Note that A is an abelian group because $A \leq Z(Q)$. If Q is isomorphic to $E(K, A, f)$, then Proposition 5 shows that Q is a central extension of K by A.

Assume that Q is a central extension of K by A. Let $\psi : K \to Q/A$ be an isomorphism, and let $\sigma : K \to Q$ be any map such that $\sigma(x) \in \psi(x)$ and $\sigma(1) = 1$. Then every element of Q can be written uniquely as $\sigma(x)a$ for some $x \in K$ and $a \in A$. Since A is a central subloop, we have $(\sigma(x)a)(\sigma(y)b) = (\sigma(x)\sigma(y))(ab)$. As $\sigma(x)\sigma(y) \in \psi(x)\psi(y) = \psi(xy)$ and $\sigma(xy) \in \psi(xy)$, we have $(\sigma(x)\sigma(y))(ab) = \sigma(xy)abf(x, y)$ for some unique $f(x, y) \in A$. It is now easy to check that the map $f : K \times K \to A$ so defined is a cocycle. □

Using the Moufang identity $(xy)(zx) = x((yz)x)$, we obtain by straightforward calculation:

Proposition 7. *Let K be a loop, A an abelian group, and $f : K \times K \to A$ a cocycle. Then $E(K, A, f)$ is a Moufang loop if and only if K is a Moufang loop and f satisfies*

$$f(xy, zx)f(x, y)f(z, x) = f(x, (yz)x)f(yz, x)f(y, z) \tag{2.2}$$

for all x, y, $z \in K$.

We call a cocycle $f : K \times K \to A$ satisfying (2.2) a *Moufang cocycle*.

It is not necessary to consider all groups while looking for nonassociative Moufang central extensions:

Proposition 8. *Let Q be a diassociative loop, and let $A \leq Z(Q)$ be such that Q/A has a generating subset of size at most 2. Then Q is a group.*

Proof. Let x, $y \in Q$ be such that Q/A is generated by $\{xA, yA\}$. Let H be the subloop of Q generated by $\{x, y\}$. Since Q is diassociative, H is a group. Moreover, HA/A is a subloop of Q/A containing $\{xA, yA\}$, thus $HA/A = Q/A$ and $HA = Q$. For h_1, h_2, $h_3 \in H$ and a_1, a_2, $a_3 \in A$, we have $(h_1a_1)((h_2a_2)(h_3a_3)) = (h_1(h_2h_3))(a_1a_2a_3) = ((h_1h_2)h_3)(a_1a_2a_3) = ((h_1a_1)(h_2a_2))(h_3a_3)$ because A is central and H is a group. Thus Q is a group. □

Let K be a loop and A an abelian group. Given a map $\tau : K \to A$, denote by $\delta\tau : K \times K \to A$ the map defined by

$$\delta\tau(x, y) = \tau(xy)\tau(x)^{-1}\tau(y)^{-1}. \tag{2.3}$$

Observe that $\delta\tau$ is a cocycle if and only if $\tau(1) = 1$. We call a cocycle of the form $\delta\tau$ (necessarily with $\tau(1) = 1$) a *coboundary*.

From now on we denote the operation in the abelian group A additively and let 0 be the neutral element of A.

Lemma 9. *Let K be a loop, A an abelian group, and f, $g : K \times K \to A$ cocycles. If $g - f$ is a coboundary then $E(K, A, f)$ is isomorphic to $E(K, A, g)$.*

Proof. Denote the multiplication in $E(K, A, f)$ by $*$, and the multiplication in $E(K, A, g)$ by $\circ$. Let $g - f = \delta\tau$ for some $\tau : K \to A$. Define $\psi : E(K, A, f) \to E(K, A, g)$ by

$\psi(x,a) = (x, a+\tau(x))$. Then ψ is clearly one-to-one, and $\psi(x, a-\tau(x)) = (x,a)$ shows that ψ is also onto. Now,

$$\begin{aligned}\psi((x,a)*(y,b)) &= \psi(xy, a+b+f(x,y)) \\ &= (xy, a+b+f(x,y)+\tau(xy)) = (xy, a+b+g(x,y)+\tau(x)+\tau(y)) \\ &= (x, a+\tau(x)) \circ (y, b+\tau(y)) = \psi(x,a)\circ\psi(y,b),\end{aligned}$$

and we are through. □

The converse of Lemma 9 is not true in general. We have:

Lemma 10. *Let K be a Moufang loop, A an abelian group, and $\delta\tau : K\times K \to A$ a coboundary. Then $\delta\tau$ is a Moufang cocycle.*

Proof. We need to show that (2.2) holds for $\delta\tau$, that is

$$\delta\tau(xy, zx) + \delta\tau(x,y) + \delta\tau(z,x) = \delta\tau(x,(yz)x) + \delta\tau(yz,x) + \delta\tau(y,z).$$

This is equivalent to

$$\begin{aligned}&\tau((xy)(zx)) - \tau(xy) - \tau(zx) + \tau(xy) - \tau(x) - \tau(y) + \tau(zx) - \tau(z) - \tau(x) \\ &= \tau(x((yz)x)) - \tau(x) - \tau((yz)x) + \tau((yz)x) - \tau(yz) - \tau(x) + \tau(yz) - \tau(y) - \tau(z),\end{aligned}$$

which holds because K is Moufang. □

3. Nonequivalent cocycles

Let $\mathbb{F}_p = \{0, \dots, p-1\}$ be the p-element field and K a Moufang loop. The cocycles $K\times K \to \mathbb{F}_p$ form a vector space $\mathcal{C}(K)$ over $\mathbb{F}_p$, Moufang cocycles form a subspace $\mathcal{M}(K)$ of $\mathcal{C}(K)$, and coboundaries form a subspace $\mathcal{B}(K)$ of $\mathcal{M}(K)$, by Lemma 10.

We say that two cocycles $f, g : K\times K \to \mathbb{F}_p$ are *equivalent* if $f-g$ is a coboundary.

Let $n = |K|^2$, and let $b : K\times K \to \{1,\dots,n\}$ be a fixed bijection. Let $v_1, \dots, v_n$ be variables. Identify the cocycle $f : K\times K \to \mathbb{F}_p$ with a vector $(f_1, \dots, f_n)$ of $\mathbb{F}_p^n$ by letting $f_{b(x,y)} = f(x,y)$. An identity for f, such as (2.2), can then be translated into a set of equations in $\mathbb{F}_p[v_1,\dots,v_n]$.

For instance, the cocycle identities $f(1,x) = 0$, $f(x,1) = 0$ give rise to the $2|K|-1$ linear equations

$$v_{b(1,x)} = 0, \quad v_{b(x,1)} = 0, \quad \text{for } x \in K. \tag{3.1}$$

Since the equations of (3.1) are linearly independent, we have $\dim(\mathcal{C}(K)) = |K|^2 - 2|K| + 1$.

The subspace $\mathcal{B}(K)$ of coboundaries can be described directly. For $1 \neq x \in K$ let $\tau_x : K \to \mathbb{F}_p$ be the map

$$\tau_x(y) = \begin{cases} 1, \text{ if } y = x, \\ 0, \text{ otherwise.}\end{cases}$$

Then $\{\tau_x;\ 1 \neq x \in K\}$ is a basis of the vector space of all maps $K \to \mathbb{F}_p$. Since the operator $\delta : \tau \mapsto \delta\tau$ is linear, $\mathcal{B}(K)$ is generated by $\{\delta\tau_x;\ 1 \neq x \in K\}$, and thus $\dim(\mathcal{B}(K)) \leq |K| - 1$. In fact:

Lemma 11. *Let Q be a Moufang p-loop of order p^k, and let d be the size of a minimal generating set of Q. Let $\mathcal{B}(Q) = \{\delta\tau;\ \tau : Q \to \mathbb{F}_p,\ \tau(1) = 0\}$ be the vector space of coboundaries. Then $\dim(\mathcal{B}(Q)) = p^k - 1 - d$. Equivalently, $|Q/\Phi(Q)| = p^{p^k-1-\dim(\mathcal{B}(Q))}$, where $\Phi(Q)$ is the Frattini subloop of Q.*

Proof. We know that $|Q/\Phi(Q)| = p^d$. Note that $\delta : \tau \mapsto \delta\tau$ is a homomorphism onto $\mathcal{B}(Q)$ with $\ker\delta = \mathrm{Hom}(Q, \mathbb{F}_p)$.

Consider the map $\psi : \mathrm{Hom}(Q/\Phi(Q), \mathbb{F}_p) \to \mathrm{Hom}(Q, \mathbb{F}_p)$ defined by

$$\psi(f)(x) = f(x\Phi(Q)).$$

Then ψ is a monomorphism, and we claim that it is onto. Consider $f \in \mathrm{Hom}(Q, \mathbb{F}_p)$. Since $\dim(\mathbb{F}_p) = 1$, $\ker f$ is either all of Q or it is a maximal subloop of Q. In any case, $\Phi(Q) \le \ker f$. Then $\overline{f} : Q/\Phi(Q) \to \mathbb{F}_p$, $x\Phi(Q) \mapsto f(x)$ is a well-defined homomorphism, and $\psi(\overline{f})(x) = \overline{f}(x\Phi(Q)) = f(x)$, so $\psi(\overline{f}) = f$.

$Q/\Phi(Q)$ is a vector space of dimension d, and thus its dual $\mathrm{Hom}(Q/\Phi(Q), \mathbb{F}_p)$ has also dimension d. Hence $\mathrm{Hom}(Q, \mathbb{F}_p)$ has dimension d, by the above paragraph. Altogether, $\dim(\mathrm{im}\,\delta) = \dim(\mathbb{F}_p^Q) - \dim(\mathrm{Hom}(Q, \mathbb{F}_p)) = p^k - d$. We have $\dim(\mathcal{B}(Q)) = \dim(\mathrm{im}\,\delta) - 1$ due to the requirement that every coboundary is of the form $\delta\tau$ for some τ satisfying $\tau(1) = 0$. □

We now determine $\mathcal{M}(K)$. The Moufang cocycle identity (2.2) gives rise to the $|K|^3$ linear equations

$$v_{b(xy,zx)} + v_{b(x,y)} + v_{b(z,x)} - v_{b(x,(yz)x)} - v_{b(yz,x)} - v_{b(y,z)} = 0, \quad \text{for } x,\ y,\ z \in K, \quad (3.2)$$

necessarily linearly dependent. The subspace $\mathcal{M}(K)$ of Moufang cocycles is obtained by solving the system of linear equations (3.1) combined with (3.2).

The main reason why Moufang p-loops are somewhat amenable to enumeration is the following result, cf. (Glauberman, 1968) and (Glauberman and Wright, 1968):

Theorem 12. *Moufang p-loops are centrally nilpotent.*

In particular:

Corollary 13. *A nontrivial Moufang p-loop contains a central subgroup of order p.*

Proof. Let Q be a Moufang p-loop of order at least p. Since Q is centrally nilpotent, its center $Z(Q)$ is nontrivial. Then $Z(Q)$ is a p-group of order at least p, and so it contains an element of order p. This element generates a central subgroup (hence normal subgroup) of order p. □

Given a Moufang p-loop K, choose $\mathcal{D}(K)$ so that $\mathcal{M}(K) = \mathcal{B}(K) \oplus \mathcal{D}(K)$.

Among the 51 groups of order 32, 20 are two-generated, including the cyclic group. No nonassociative Moufang loop is two-generated, thanks to diassociativity. Thus, in order to obtain all Moufang loops of order 64 up to isomorphism, it suffices to construct all extensions $E(K, \mathbb{F}_2, f)$, where K is one of the $71 + 51 - 20 = 102$ Moufang loops of order 32 that are not two-generated, and where f is chosen from $\mathcal{D}(K)$.

It is not clear how to estimate the dimension of $\mathcal{M}(K)$ (and hence of $\mathcal{D}(K)$) theoretically. Table 2 gives the dimensions of $\mathcal{M}(K)$ and $\mathcal{B}(K)$ for every Moufang loop of order 32 that is not two-generated. The ith Moufang loop of order 32 in the table corresponds

Table 2. Dimensions of Moufang cocycles $\mathcal{M}(K)$ and coboundaries $\mathcal{B}(K)$ for all Moufang loops K of order 32 that are not two-generated.

loop K	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\dim(\mathcal{M}(K))$	41	40	40	36	35	34	35	34	34	40	40	40	40	40	40	40
$\dim(\mathcal{B}(K))$	27	27	27	28	28	28	28	28	28	27	27	27	27	27	27	27
loop K	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\dim(\mathcal{M}(K))$	40	40	40	40	40	40	34	34	34	34	34	34	34	34	34	34
$\dim(\mathcal{B}(K))$	27	27	27	27	27	27	28	28	28	28	28	28	28	28	28	28
loop K	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$\dim(\mathcal{M}(K))$	34	34	34	34	34	34	34	34	34	33	33	33	33	33	34	34
$\dim(\mathcal{B}(K))$	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28
loop K	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
$\dim(\mathcal{M}(K))$	33	34	34	33	33	34	34	34	34	33	33	35	34	34	34	34
$\dim(\mathcal{B}(K))$	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28
loop K	65	66	67	68	69	70	71									
$\dim(\mathcal{M}(K))$	34	33	34	34	35	35	34									
$\dim(\mathcal{B}(K))$	28	28	28	28	28	28	28									
group K	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\dim(\mathcal{M}(K))$	35	36	35	34	35	34	36	35	34	34	34	33	33	35	34	35
$\dim(\mathcal{B}(K))$	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28
group K	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	
$\dim(\mathcal{M}(K))$	34	34	35	34	34	34	34	34	41	41	40	40	40	40	51	
$\dim(\mathcal{B}(K))$	28	28	28	28	28	28	28	28	27	27	27	27	27	27	26	

to the ith Moufang loop of order 32 in (Goodaire, May and Raman, 1999) and to the ith Moufang loop of order 32 in LOOPS, where it can be retrieved as `MoufangLoop(32,i)`. The ith group of order 32 in the table corresponds to the ith group of order 32 in (GAP, 2006), where it can be retrieved as `SmallGroup(32,i)`.

Note that for every Moufang loop K listed in Table 2 we have $\dim(\mathcal{D}(K)) \leq 14$, with the exception of the elementary abelian group of order 32 (the last group in the table).

As for the Moufang loops of order 81, the only group K of order 27 that is not two-generated is the elementary abelian group. We have $\dim(\mathcal{B}(K)) = 23$ by Lemma 11, and a short computer calculation yields $\dim(\mathcal{M}(K)) = 30$. This means that the classification of nonassociative Moufang loops of order 81 is an easy task, indeed, for a computer.

4. Cocycles and the automorphism group

Let K be a loop and A an abelian group. The automorphism group $\mathrm{Aut}(K)$ acts on $\mathcal{C}(K)$ by $f \mapsto f^\alpha$, where $f^\alpha(x, y) = f(\alpha(x), \alpha(y))$.

Lemma 14. *Let K be a loop, A an abelian group, $f : K \times K \to A$ a cocycle, and $\alpha \in \mathrm{Aut}(K)$. Then $E(K, A, f)$ is isomorphic to $E(K, A, f^\alpha)$.*

Proof. Define $\psi : E(K, A, f^\alpha) \to E(K, A, f)$ by $(x, a) \mapsto (\alpha(x), a)$. Denote the product in $E(K, A, f^\alpha)$ by $*$ and the product in $E(K, A, f)$ by $\circ$. Then

$$\begin{aligned}\psi((x,a) * (y,b)) &= \psi(xy, a + b + f^\alpha(x,y)) = (\alpha(xy), a + b + f^\alpha(x,y)) \\ &= (\alpha(x)\alpha(y), a + b + f(\alpha(x), \alpha(y))) = (\alpha(x), a) \circ (\alpha(y), b) = \psi(x,a) \circ \psi(y,b).\end{aligned}$$

Since ψ is clearly a bijection, we are done. □

We can therefore use the action of the automorphism group to reduce the number of nonequivalent cocycles that need to be taken into consideration. Let us return to the Moufang case, extending a Moufang loop K by $\mathbb{F}_p$.

Set $X = \emptyset$ and $Y = \mathcal{D}(K)$. Until Y is empty, repeat the following: Pick $f \in Y$ and insert it into X. For every $\alpha \in \mathrm{Aut(K)}$, calculate f^α. Decompose $f^\alpha = g_\alpha + h_\alpha$, where $g_\alpha \in \mathcal{B}(K)$ and $h_\alpha \in \mathcal{D}(K)$. Remove h_α from Y, if possible.

We claim that all extensions of K by $\mathbb{F}_p$ are obtained if only cocycles from X are considered. To see this, note that $E(K, A, f)$ is isomorphic to $E(K, A, f^\alpha)$ by Lemma 14, and that $E(K, A, f^\alpha)$ is in turn isomorphic to $E(K, A, h_\alpha)$, because $f^\alpha - h_\alpha = g_\alpha$ is a coboundary.

The size of X is often much smaller than the size of $\mathcal{D}(K)$. For instance, for $K =$ `MoufangLoop(32,1)` we have $|X| = 246$ (or about 1.5 percent of $|\mathcal{D}(K)| = 2^{14}$), for $K =$ `MoufangLoop(32,71)` we have $|X| = 20$ (31.3 percent), for $K = \mathbb{Z}_{32}$ we have $|X| = 2$ (100 percent), for $K =$ `SmallGroup(32,50)` we have $|X| = 138$ (1.7 percent), and for K the elementary abelian group of order 27 we have $|X| = 11$ (0.5 percent).

5. The elementary abelian case in characteristic two

When K is the elementary abelian group of order 32, the dimension of $\mathcal{D}(K)$ is prohibitively large, equal to 25. In this section we describe how this case was handled in the search.

As we have already mentioned, Moufang 2-loops Q with a central subloop Z of order 2 such that $V = Q/Z$ is an elementary abelian group are known as code loops. The first code loop is due to Parker, as discussed in (Conway, 1985), and the first systematic exposition of code loops can be found in (Griess, 1986).

Let Q be a code loop, $Z \leq Z(Q)$, $|Z| = 2$, $V = Q/Z$ elementary abelian. For $x, y \in Q$, denote by $[x, y]$ the *commutator* of x, y, that is, the unique element u of Q such that $xy = (yx)u$. For x, y, $z \in Q$, denote by $[x, y, z]$ the *associator* of x, y, z, that is, the unique element v of Q such that $(xy)z = (x(yz))v$.

The three maps

$$\begin{aligned}&P : Q \to Q,\ x \mapsto x^2 \text{ (power map)},\\ &C : Q \times Q \to Q,\ (x, y) \mapsto [x, y] \text{ (commutator map)},\\ &A : Q \times Q \times Q \to Q,\ (x, y, z) \mapsto [x, y, z] \text{ (associator map)}\end{aligned}$$

can in fact be considered as maps

$$P : V \to Z, \quad C : V \times V \to Z, \quad A : V \times V \times V \to Z,$$

and therefore identified with forms from the vector space V to the field $\mathbb{F}_2$.

The three forms are related by combinatorial polarization: A is a trilinear alternating form,

$$C(x,y) = P(x+y) - P(x) - P(y),$$

and

$$\begin{aligned} A(x,y,z) &= C(x+y,z) - C(x,z) - C(y,z) \\ &= P(x+y+z) - P(x+y) - P(x+z) - P(y+z) + P(x) + P(y) + P(z). \end{aligned}$$

We digress for a while to give more details on combinatorial polarization. The material of Subsection 5.1 is taken from (Drápal and Vojtěchovský, 2007). See (Ward, 1979) for an introduction to combinatorial polarization.

5.1. Combinatorial polarization

Let V be a vector space over the p-element field $\mathbb{F}_p$, p a prime. For a map $\alpha : V \to \mathbb{F}_p$ and $n > 1$ define $\alpha_n : V^n \to \mathbb{F}_p$ by

$$\alpha_n(u_1, \ldots, u_n) = \sum_{\{i_1,\ldots,i_m\} \subseteq \{1,\ldots,n\}} (-1)^{n-m} \alpha(u_{i_1} + \cdots + u_{i_m}), \tag{5.1}$$

where $\alpha(\emptyset) = 0$. Then α_n is clearly a symmetric form, called the *nth derived form of* α. We say that $\alpha = \alpha_1, \alpha_2, \alpha_3, \ldots$ are *related by polarization*.

The *combinatorial degree* of $\alpha : V \to \mathbb{F}_p$ is the largest integer n such that $\alpha_n \neq 0$ and $\alpha_m = 0$ for every $m > n$, if it exists.

The defining identity (5.1) is equivalent to the recurrence relation

$$\begin{aligned} &\alpha_n(u, v, w_3, \ldots, w_n) \\ &\quad = \alpha_{n-1}(u+v, w_3, \ldots, w_n) - \alpha_{n-1}(u, w_3, \ldots, w_n) - \alpha_{n-1}(v, w_3, \ldots, w_n). \end{aligned} \tag{5.2}$$

We see from (5.2) that the combinatorial degree of α is equal to n if and only if $\alpha_n \neq 0$ is a symmetric n-linear form (since $\mathbb{F}_p$ is a prime field). Moreover, an easy induction proves:

Lemma 15. *Let V be a vector space over $\mathbb{F}_p$ and $\alpha : V \to \mathbb{F}_p$ a map satisfying $\alpha(0) = 0$. Then $\alpha_n(0, u_2, \ldots, u_n) = 0$ for every $u_2, \ldots, u_n \in V$.*

Proposition 16. *Let V be a vector space over $\mathbb{F}_p$ with basis $B = \{e_1, \ldots, e_d\}$. Let $\alpha : V \to \mathbb{F}_p$ be a map of combinatorial degree n. Then the following conditions are equivalent:*

(i) $\alpha(u_1)$, $\alpha_2(u_1, u_2)$, $\ldots$, $\alpha_n(u_1, \ldots, u_n)$ are known for every $u_1, \ldots, u_n \in V$,

(ii) $\alpha(u_1)$, $\alpha_2(u_1, u_2)$, $\ldots$, $\alpha_n(u_1, \ldots, u_n)$ are known for every $u_1, \ldots, u_n \in B$.

Proof. Clearly, (i) implies (ii). Assume that (ii) holds. Then $\alpha_n(u_1, \ldots, u_n)$ is known for every $u_1, \ldots, u_n \in V$ since α_n is n-linear and by Lemma 15.

Assume that $k > 0$ and $\alpha_{k+1}(u_1, \ldots, u_{k+1})$ is known for every $u_1, \ldots, u_{k+1} \in V$. Write $u_i = \sum_{j=1}^{d} u_{ij} e_j$, and let $||u_i|| = \sum_{j=1}^{n} u_{ij}$, where the *norm* is calculated in $\mathbb{Z}$, not in $\mathbb{F}_p$. We show that $\alpha_k(u_1, \ldots, u_k)$ is known for every $u_1, \ldots, u_k \in V$ by induction on $\sum_{i=1}^{k} ||u_i||$.

If for every $1 \leq i \leq k$ we have $||u_i|| \leq 1$, then $\alpha_k(u_1, \ldots, u_k)$ is known by (ii) and by Lemma 15. Otherwise we can assume that either u_1 has two nonzero coefficients, or that

u_1 has a nonzero coefficient larger than 1. In any case, upon writing u_1 as a sum of two vectors of smaller norm, we are done by the induction hypothesis and by the recurrence relation (5.2) for α_{k+1} and α_k. $\square$

5.2. Code loops up to isomorphism

Let us return to code loops of order 64. In the notation of derived forms, we have $C = P_2$ and $A = P_3$. The code loop Q is determined by the three forms P, C, A, and hence, by Proposition 16, by the values

$$P(e_i), \quad C(e_i, e_j), \quad A(e_i, e_j, e_k), \tag{5.3}$$

where $\{e_1, \dots, e_5\}$ is a basis of V, and where $i < j < k$.

Moreover, Aschbacher shows in (Aschbacher, 1994) that two code loops Q, Q' with associated triples (P, C, A) and (P', C', A') are isomorphic if and only if (P, C, A) and (P', C', A') are *equivalent*, i.e., there is $\psi \in \mathrm{GL}(V)$ such that

$$P(u) = P'(\psi(u)), \quad C(u, v) = C'(\psi(u), \psi(v)), \quad A(u, v, w) = A'(\psi(u), \psi(v), \psi(w))$$

for every u, v, $w \in V$.

In order to construct all nonassociative code loops of order 64, we must first find all triples (P, C, A) up to equivalence, where P has combinatorial degree 3. (If the combinatorial degree of P is less than 3 then the associator map $A = P_3$ is trivial and hence the resulting loop is a group.) For the convenience of the reader, we give formulae for evaluating A, C and P on V based only on (5.3) and on the symmetry of the three forms:

$$A(\sum_i x_i e_i, \sum_j y_j e_j, \sum_k z_k e_k) = \sum_{i,j,k} x_i y_j z_j A(e_i, e_j, e_k),$$

$$C(\sum_i x_i e_i, \sum_j y_j e_j) = \sum_{i,j} x_i y_j C(e_i, e_j) + \sum_k \sum_{i<j} x_i x_j y_k A(e_i, e_j, e_k) + \sum_i \sum_{j<k} x_i y_j y_k A(e_i, e_j, e_k),$$

and

$$P(\sum_i x_i e_i) = \sum_i x_i P(e_i) + \sum_{i<j} x_i x_j C(e_i, e_j) + \sum_{i<j<k} x_i x_j x_k A(e_i, e_j, e_k),$$

where all running indices range from 1 to 5.

A linear transformation $M = (m_{ij}) \in \mathrm{GL}(V)$ turns the triple (P, C, A) into a triple (P^M, C^M, A^M) according to

$$A^M(e_i, e_j, e_k) = \sum_{u,v,w} m_{iu} m_{jv} m_{kw} A(e_u, e_v, e_w),$$

$$C^M(e_i, e_j) = \sum_{u,v} m_{iu} m_{jv} C(e_u, e_v) + \sum_w \sum_{u<v} m_{iu} m_{iv} m_{jw} A(e_u, e_v, e_w) + \sum_u \sum_{v<w} m_{iu} m_{jv} m_{jw} A(e_u, e_v, e_w),$$

and

$$P^M(e_i) = \sum_u m_{iu} P(e_u) + \sum_{u<v} m_{iu} m_{iv} C(e_u, e_v) + \sum_{u<v<w} m_{iu} m_{iv} m_{iw} A(e_u, e_v, e_w).$$

A computer search based on the above formulae produced 80 nonequivalent triples (P, C, A). However, it is conceivable (and, in fact, it does happen) that some of the associated code loops were already obtained earlier in the search as extensions $E(K, \mathbb{F}_2, f)$ for some Moufang loop K of order 32 that is not elementary abelian. It is therefore necessary to construct the 80 code loops explicitly and test them for isomorphism against the previously found loops.

There are several ways in which the code loop Q can be recovered from the triple (P, C, A). The first, iterative construction is due to (Griess, 1986), another construction (also iterative) using twisted products was given in (Hsu, 2000), and the most recent construction is due to the first author (Nagy, 2007). In the latter paper, Nagy shows that there is a one-to-one correspondence between nonequivalent triples (P, C, A), a certain class of non-S-isomorphic groups with triality, and code loops. The correspondence of (Nagy, 2007) is constructive, and we used it to obtain a concrete description of the 80 code loops.

6. Conclusion of the search

We have by now obtained all Moufang loops of order 64 (resp. 81) by producing all central extensions $E(K, \mathbb{F}_2, f)$ (resp. $E(K, \mathbb{F}_3, f)$), where K is an at least three-generated Moufang loop of order 32 (resp. 27) and $f : K \times K \to \mathbb{F}_2$ (resp. $f : K \times K \to \mathbb{F}_3$) is a Moufang cocycle modulo coboundaries modulo the action of $\mathrm{Aut}(K)$.

Upon sorting the loops up to isomorphism and discarding groups (which arise when K is associative and f is a group cocycle, see Remark 18), we have found 4262 nonassociative Moufang loops of order 64 and 5 nonassociative Moufang loops of order 81. This finishes the proof of Theorem 3 and the enumerative part of Theorem 4. One can then check, for instance in the LOOPS package, that 2 of the 5 nonassociative Moufang loops of order 81 are commutative, and that the remaining 3 loops are isotopes of the commutative ones. We have proved Theorem 4.

The 4262 nonassociative Moufang loops of order 64 and the 5 nonassociative Moufang loops of order 81 are available electronically in the latest version of LOOPS. The command `MoufangLoop(n,m)` retrieves the mth Moufang loop of order n from the database.

Remark 17. Based on the discussion in Subsection 1.2, we see that the classification of nonassociative Moufang loops of order p^4 is now complete. Moreover, by (Nagy and Valsecchi, 2007), the only case missing in the classification of nonassociative Moufang loops of order p^5 is $3^5 = 243$. The tools used here fall just short of covering this case. (The associated systems of linear equations can be solved but the isomorphism problem is too difficult for the methods present in the LOOPS package. We believe it could be solved using a specialized algorithm for Moufang 3-loops.)

Remark 18. Given a loop K and an abelian group A we say that $f : K \times K \to A$ is a *group cocycle* if

$$f(xy, z) + f(x, y) = f(x, yz) + f(y, z)$$

holds for every x, y, $z \in K$. When K is a group and f is a group cocycle, $E(K, A, f)$ is a group. Group cocycles form a subspace of $\mathcal{M}(K)$ containing $\mathcal{B}(K)$.

The reader might wonder why we did not take advantage of group cocycles in the search to further cut the dimension of the complement $\mathcal{D}(K)$. (For illustration, when K is the elementary abelian group of order 32, the subspace of group cocycles has dimension 41, compared to $\dim(\mathcal{B}(K)) = 26$.) The difficulty is that two (Moufang) cocycles that differ by a group cocycle do not necessarily yield isomorphic loops.

6.1. Technical information

We conclude the paper with some technical information concerning the search.

The calculations have been carried twice, on two different computers, and with slightly different algorithms. We worked within the GAP (GAP, 2006) package LOOPS (Nagy and Vojtěchovský, 2007). The GAP code for all algorithms specific to this paper can be downloaded at http://www.math.du.edu/~petr in section "Publications". The code is well commented and contains additional details about the search not provided here.

The total running time of the program on a 2 gigahertz PC with Windows XP operating system was about 3 hours, out of which about 1 minute was devoted to the case $n = 81$, and about 15 minutes to the elementary abelian case for $n = 64$.

For each Moufang loop K of order 32 that is not two-generated the program returned a list of IDs of pairwise nonisomorphic nonassociative Moufang loops of order 64 that are central extensions of K by $\mathbb{F}_2$. These 102 lists contained 11434 IDs, with 4262 unique IDs, and with maximal multiplicity of an ID equal to 7. Precisely 64 out of the 80 code loops of order 64 cannot be obtained as central extensions of any other Moufang loop of order 32 than the elementary abelian group.

References

Aschbacher, M., 1994. *Sporadic groups*, Cambridge Tracts in Mathematics **104**, Cambridge University Press, Cambridge.

Bol, G., 1937. *Gewebe und Gruppen*, Math. Ann. **114**, 414–431.

Bruck, R. H., 1971. A Survey of Binary Systems, third printing, corrected, *Ergebnisse der Mathematik und Ihrer Grenzgebiete*, New series, Volume **20**, Springer-Verlag, New York-Heidelberg-Berlin.

Chein, O., 1978. *Moufang loops of small order*, Memoirs of the American Mathematical Society, Volume **13**, Issue 1, Number **197**.

Chein, O., Rajah, A., 2003. *Possible orders of nonassociative Moufang loops*, Comment. Math. Univ. Carolin. **41**, **2** (April 2003), 237–244.

Conway, J. H., 1985. *A simple construction for the Fisher-Griess monster group*, Invent. Math. **79**, no. **3**, 513–540.

Drápal, A., 2003. *Cyclic and dihedral constructions of even order*, Comment. Math. Univ. Carolin. **44**, **4**, 593–614.

Drápal, A., Vojtěchovský, P., 2007. *Symmetric multilinear forms and polarization of polynomials*, submitted.

Hsu, T., 2000. *Moufang loops of class* 2 *and cubic forms*, Math. Proc. Cambridge Philos. Soc. **128**, 197–222.

The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4; Aachen, St Andrews (2006). (Visit http://www-gap.dcs.st-and.ac.uk/~gap).

Glauberman, G., 1968. *On loops of odd order II*, J. Algebra **8**, 393–414.
Glauberman, G., Wright, C. R. B., 1968. *Nilpotence of finite Moufang* 2*-loops*, J. Algebra **8**, 415–417.
Goodaire, E. G., May, S., Raman, M., 1999. The Moufang Loops of Order less than 64, Nova Science Publishers.
Griess, Jr., R. L., 1986. *Code Loops*, J. Algebra **100**, 224–234.
Kepka, T., Němec, P., *Commutative Moufang loops and distributive groupoids of small orders*, Czechoslovak Math. J. **31** (**106**) (1981), no. **4**, 633–669.
Leong, F., Rajah, A., 1997. *Moufang loops of odd order* $p^\alpha q_1^2 \cdots q_n^2 r_1 \cdots r_m$, J. Algebra **190**, 474–486.
Nagy, G. P., 2007. *Direct construction of code loops*, to appear in Discrete Mathematics.
Nagy G. P., Valsecchi, M., 2007. *On nilpotent Moufang loops with central associators*, J. Algebra **307** (2007), 547–564.
Nagy G. P., Vojtěchovský, P., 2007. LOOPS: *Computing with quasigroups and loops in* GAP, download at `http://www.math.du.edu/loops`.
Pflugfelder, H. O., 1990. Quasigroups and Loops: Introduction, *Sigma series in pure mathematics* **7**, Heldermann Verlag Berlin.
Rajah, A., 2001. *Moufang loops of odd order* pq^3, J. Algebra **235**, no. **1**, 66–93.
Vojtěchovský, P., 2006. *Toward the classification of Moufang loops of order* 64, European J. Combin. **27**, issue **3** (April 2006), 444–460.
Ward, H. N., 1979. *Combinatorial Polarization*, Discrete Mathematics **26**, 186–197.
Wright, C. R. B., 1965. *Nilpotency conditions for finite loops*, Illinois J. Math. **9**, 399–409.