# MOUFANG LOOPS THAT SHARE ASSOCIATOR AND THREE QUARTERS OF THEIR MULTIPLICATION TABLES

ALEŠ DRÁPAL AND PETR VOJTĚCHOVSKÝ

Abstract. Two constructions due to Drápal produce a group by modifying exactly one quarter of the Cayley table of another group. We present these constructions in a compact way, and generalize them to Moufang loops, using loop extensions. Both constructions preserve associators, the associator subloop, and the nucleus. We conjecture that two Moufang 2-loops of finite order $n$ with equivalent associator can be connected by a series of constructions similar to ours, and offer empirical evidence that this is so for $n = 16$, 24, 32; the only interesting cases with $n \leq 32$. We further investigate the way the constructions affect code loops and loops of type $M(G, 2)$. The paper closes with several conjectures and research questions concerning the distance of Moufang loops, classification of small Moufang loops, and generalizations of the two constructions.

MSC2000: Primary: 20N05. Secondary: 20D60, 05B15.

## 1. Introduction

Moufang loops, i.e., loops satisfying the *Moufang identity* $((xy)x)z = x(y(xz))$, are surely the most extensively studied loops. Despite this fact, the classification of Moufang loops is finished only for orders less than 64, and several ingenious constructions are needed to obtain all these loops. The purpose of this paper is to initiate a new approach to finite Moufang 2-loops. Namely, we intend to decide whether all Moufang 2-loops of given order with equivalent associator can be obtained from just one of them, using only group-theoretical constructions. (See below for details). We prove that this is the case for $n = 16$, 24, and 32, which are the only orders $n \leq 32$ for which there are at least two non-isomorphic nonassociative Moufang loops (5, 5, and 71, respectively). We also show that for every $m \geq 6$ there exist classes of loops of order $2^m$ that satisfy our hypothesis. Each of these classes consists of code loops whose nucleus has exactly two elements (cf. Theorem 8.8).

As it turns out, we will only need two constructions that were introduced in [7], and that we call *cyclic* and *dihedral*. They are recalled in Sections 3 and 4, and generalized to Moufang loops in Sections 6 and 7. The main feature of both constructions is that, given a Moufang loop $(G, \cdot)$, they produce a generally non-isomorphic Moufang loop $(G, *)$ that has the same associator and nucleus as $(G, \cdot)$, and whose multiplication table agrees with the multiplication table of $(G, \cdot)$ in 3/4 of positions.

The constructions allow a very compact description with the help of simple modular arithmetic, developed in Section 2. Nevertheless, in order to prove that the constructions are meaningful for Moufang loops (Theorems 6.3, 7.3), one benefits from knowing some loop extension theory (Section 5). (An alternative proof using only identities is available as well [17], but is much longer.)

Work supported by Grant Agency of Charles University, grant number 269/2001/B-MAT/MFF. The first author supported also by institutional grant MSM 113200007.

We then turn our attention to two classes of Moufang loops: code loops (Section 8), and loops of type $M(G, 2)$ (Section 9).

Up to isomorphism, code loops can be identified with maps $P : V \longrightarrow F$ whose 3rd derived form is trilinear, where $F = GF(2)$ and $V$ is a finite vector space over $F$. Section 8 explains how $P$ is modified under our constructions. These modification can be described in terms of linear and quadratic forms, and it is not difficult to see how one can gradually transform a code loop to any other code loop with equivalent associator (cf. Proposition 8.7).

The loops of type $M(G, 2)$ play a prominent role in the classification of Moufang loops, chiefly thanks to their abundance among small loops. In Section 9, we describe how the loops $M(G, 2)$ behave under both constructions.

It has been conjectured [6] that from each finite 2-group one can obtain all other 2-groups of the same order by repeatedly applying a construction that preserves exactly 3/4 of the corresponding multiplication tables. For $n \leq 32$, this conjecture is known to be true, and for such $n$ it suffices to use only the cyclic and dihedral constructions [20]. For $n = 64$, these constructions yield two blocks of groups and it is not known at this moment if there exists a similar construction that would connect these two blocks [2].

In view of these results about 2-groups, it was natural to ask how universal the cyclic and dihedral constructions remain for Moufang loops of small order. A computer search (cf. Section 10) has shown that for orders $n = 16, 24, 32$ the blocks induced by cyclic and dihedral constructions coincide with blocks of Moufang loops with equivalent associator. This is the best possible result since none of the constructions changes the associator, and since the two constructions are not sufficient even for groups when $n = 64$.

The search for pairs of 2-groups that can be placed at quarter distance (a phrase expressing that 3/4 of the multiplication tables coincide) stems from the discovery that two 2-groups which differ in less than a quarter of their multiplication tables are isomorphic [6]. We conjecture that this property remains true for Moufang 2-loops. Additional conjectures, together with suggestions for future work, can be found at the end of the paper.

We assume basic familiarity with calculations in nonassociative loops and in Moufang loops in particular. The inexperienced reader should consult [14].

A word about the notation. The dihedral group $\langle a, b;\ a^n = b^2 = 1,\ aba = b\rangle$ of order $2n$ will be denoted by $D_{2n}$, although some of the authors we cite use $D_n$; for instance [11]. We count the Klein 4-group among dihedral groups, and denote it also by $V_4$. The generalized quaternion group $\langle a, b;\ a^{2^{n-1}} = 1,\ a^{2^{n-2}} = b^2,\ bab^{-1} = a^{-1}\rangle$ of order $2^n$ will be denoted by $Q_{2^n}$. We often write $ab$ instead of $a \cdot b$. In fact, following the custom, we use "$\cdot$" to indicate the order in which elements are multiplied. For example, $a \cdot bc$ stands for $a(bc) = a \cdot (b \cdot c)$.

## 2. Modular Arithmetic and the Function $\sigma$

Let $m$ be a positive integer and $M$ the set $\{-m+1, -m+2, \dots, m-1, m\}$. Denote by $\oplus$ and $\ominus$ the addition and subtraction modulo $2m$ in $M$, respectively. More precisely, define $\sigma : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ by

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

and let

$$i \oplus j = i + j - 2m\sigma(i + j), \quad i \ominus j = i - j - 2m\sigma(i - j),$$

for any $i, j \in M$. In order to eliminate parentheses, we postulate that $\oplus$ and $\ominus$ are more binding than $+$ and $-$. Observe that $1-i$ belongs to $M$ whenever $i$ does, and that $\sigma(1-i) = -\sigma(i)$.

We will need the following identities for $\sigma$ in Sections 3 and 4:

$$\sigma(i+j) + \sigma(i \oplus j + k) = \sigma(j+k) + \sigma(i + j \oplus k), \tag{1}$$

$$-\sigma(i+j) + \sigma(1 - i \oplus j + k) = \sigma(1 - j + k) - \sigma(i + j \ominus k). \tag{2}$$

The identity (1) follows immediately from $(i \oplus j) \oplus k = i \oplus (j \oplus k)$. To establish (2), consider $(i \oplus j) \ominus k = i \oplus (j \ominus k)$. This yields $-\sigma(i+j) - \sigma(i \oplus j - k) = -\sigma(j-k) - \sigma(i + j \ominus k)$. Since $-\sigma(i \oplus j - k) = \sigma(1 - i \oplus j + k)$ and $-\sigma(j-k) = \sigma(1-j+k)$, we are done.

## 3. The Cyclic Construction

Let us start with the less technical of the two constructions—the cyclic one. We will work in the more general setting of Moufang loops, and take full advantage of the function $\sigma$ defined in Section 2.

Let $G$ be a Moufang loop. Recall that $Z(G)$, the *center* of $G$, consists of all elements that commute and associate with all elements of $G$. In more detail, given $x, y, z \in G$, the *commutator* $[x, y]$ of $x, y$ (resp. the *associator* $[x, y, z]$ of $x, y, z$) is the unique element $w \in G$ satisfying $xy = yx \cdot w$ (resp. $(xy)z = x(yz) \cdot w$). When three elements of a Moufang loop associate in some order, they associate in any order. Hence $Z(G) = \{x \in G;\ [x, y] = [x, y, z] = 1 \text{ for every } y, z \in G\}$.

We say that $(G, S, \alpha, h)$ satisfies condition $(\mathcal{C})$ if

- $G$ is a Moufang loop,
- $S \trianglelefteq G$, and $G/S = \langle \alpha \rangle$ is a cyclic group of order $2m$,
- $1 \neq h \in S \cap Z(G)$.

Then we can view $G$ as the disjoint union $\bigcup_{i \in M} \alpha^i$, and define a new multiplication $*$ on $G$ by

$$x * y = xyh^{\sigma(i+j)}, \tag{3}$$

where $x \in \alpha^i$, $y \in \alpha^j$, and $i, j \in M$.

The resulting loop (that is Moufang, as we shall see) will be denoted by $(G, *)$. Whenever we say that $(G, S, \alpha, h)$ satisfies $(\mathcal{C})$, we assume that $(G, *)$ is defined by (3).

The following Proposition is a special case of Theorem 6.3. We present it here because the associative case is much simpler than the Moufang case.

**Proposition 3.1.** *When $G$ is a group and $(G, S, \alpha, h)$ satisfies $(\mathcal{C})$ then $(G, *)$ is a group.*

*Proof.* Let $x \in \alpha^i$, $y \in \alpha^j$, $z \in \alpha^k$, for some $i, j, k \in M$. Since $h \in Z(G)$, we have

$$\begin{aligned} (x*y)*z &= (xy)z \cdot h^{\sigma(i+j)+\sigma(i\oplus j+k)}, \\ x*(y*z) &= x(yz) \cdot h^{\sigma(j+k)+\sigma(i+j\oplus k)}. \end{aligned} \tag{4}$$

This follows from (3) and from the fact that $xy \in \alpha^{i \oplus j}$, $yz \in \alpha^{j \oplus k}$. By (1), $(G, *)$ is associative. □

## 4. The Dihedral Construction

We proceed to the dihedral construction. Let $G$ be a Moufang loop, and let $N(G)$ be the nucleus of $G$. Recall that $N(G) = \{x \in G;\ [x, y, z] = 1 \text{ for every } y, z \in G\}$, and that $[x, y, z] = 1$ implies $[y, x, z] = [x, z, y] = 1$ for every $x, y, z \in G$.

We say that $(G, S, \beta, \gamma, h)$ satisfies condition $(\mathcal{D})$ if

- $G$ is a Moufang loop,
- $S \trianglelefteq G$ and $G/S$ is a dihedral group of order $4m$ (where we allow $m = 1$),
- $\beta$, $\gamma$ are involutions of $G/S$ such that $\alpha = \beta\gamma$ is of order $2m$,
- $1 \neq h \in S \cap Z(G_0) \cap N(G)$ and $hxh = x$ for some (and hence every) $x \in G_1$, where $G_0 = \bigcup_{i\in M} \alpha^i$, $G_1 = G \setminus G_0$.

We can then choose $e \in \beta$ and $f \in \gamma$, view $G$ as the disjoint union $\bigcup_{i\in M}(\alpha^i \cup e\alpha^i)$ or $\bigcup_{j\in M}(\alpha^j \cup \alpha^j f)$, and define a new multiplication $*$ on $G$ by

$$x * y = xyh^{(-1)^r\sigma(i+j)}, \tag{5}$$

where $x \in \alpha^i \cup e\alpha^i$, $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, $i, j \in M$, and $r \in \{0, 1\}$.

The resulting loop (again always Moufang) will be denoted by $(G, *)$. As in the cyclic case, whenever we say that $(G, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$, we assume that $(G, *)$ is defined by (5).

Note that $*$ does not depend on the choice of $e \in \beta$ and $f \in \gamma$. Also note that when $(G, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$, then $(G_0, S, \alpha = \beta\gamma, h)$ satisfies $(\mathcal{C})$.

Since $G/S$ is dihedral, $\alpha$, $\beta$ and $\gamma$ satisfy

$$\beta\alpha^i = \alpha^{\ominus i}\beta,\ \gamma\alpha^i = \alpha^{\ominus i}\gamma,\ \beta\alpha^i = \alpha^{1-i}\gamma,\ \alpha^i\gamma = \beta\alpha^{1-i},$$

for any $i \in M$, where we write $\ominus i$ rather than $-i$ to make sure that the exponents remain in $M$.

**Remark 4.1.** Although $\alpha$, $G_0$, $G_1$, $e$ and $f$ are not explicitly mentioned in condition $(\mathcal{D})$, we will often refer to them. Strictly speaking, we did not need to include $S$ among the parameters of any of the constructions, as it can always be calculated from the remaining parameters. Finally, we will sometimes find ourselves in a situation when we do not want to treat $(\mathcal{C})$ and $(\mathcal{D})$ separately. Let us therefore agree that $G_0 = G_1 = G$, $e = f = 1$, and that $\beta$, $\gamma$ are meaningless when $(\mathcal{C})$ applies.

**Lemma 4.2.** *Assume that $(G, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$. Then $(ex) * y = e(x * y)$ and $(x * y)f = x * (yf)$ whenever $y \in N(G)$.*

*Proof.* Choose $x \in \alpha^i \cup e\alpha^i$, $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, and note that $ex$ belongs to $\alpha^i \cup e\alpha^i$, while $yf$ belongs to $(\alpha^j \cup \alpha^j f) \cap G_{r+1}$. For the sake of brevity, set $t = h^{(-1)^r\sigma(i+j)}$. Then $(ex) * y = (ex)y \cdot t = e(xy) \cdot t = e(xy \cdot t) = e(x * y)$, and $(x * y)f = (xy \cdot t)f = xy \cdot tf = xy \cdot ft^{-1} = (xy)f \cdot t^{-1} = x(yf) \cdot t^{-1} = x * (yf)$, where we used $y \in N(G)$ and $h \in N(G)$ several times. □

Similarly as in the cyclic case, Proposition 4.3 is a special case of Theorem 7.3:

**Proposition 4.3.** *When $G$ is a group and $(G, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$ then $(G, *)$ is a group.*

*Proof.* If $(x * y) * z = x * (y * z)$, Lemma 4.2 implies that $((ex) * y) * z = (ex) * (y * z)$ and $(x * y) * (zf) = x * (y * (zf))$. We can therefore assume that $x \in \alpha^i$, $z \in \alpha^k$, and $y \in \alpha^j \cup \alpha^j f$, for some $i, j, k \in M$.

When $y \in \alpha^j$, the definition (5) of $*$ coincides with the cyclic case (3), and $x$, $y$, $z$ associate in $(G, *)$ by Proposition 3.1. Assume that $y \in \alpha^j f \subseteq G_1$, and recall the coset relations $\alpha^j\gamma = \beta\alpha^{1-j}$. Then

$$\begin{aligned} (x * y) * z &= (xy)z \cdot h^{-\sigma(i+j)+\sigma(1-i\oplus j+k)}, \\ x * (y * z) &= x(yz) \cdot h^{\sigma(1-j+k)-\sigma(i+j\ominus k)}, \end{aligned} \tag{6}$$

because $xy \in \alpha^i\alpha^j\gamma = \alpha^{i\oplus j}\gamma = \beta\alpha^{1-i\oplus j}$, and $yz \in \alpha^j\gamma\alpha^k = \alpha^{j\ominus k}\gamma$. By (2), $(G, *)$ is associative. □

## 5. Factor Sets

Before we prove that $(G, *)$ is a Moufang loop if $(\mathcal{C})$ or $(\mathcal{D})$ is satisfied, let us briefly review extensions of abelian groups by Moufang loops. We follow closely the group-theoretical approach, cf. [15, Ch. 11].

Let $Q$ be a Moufang loop and $A$ a $Q$-module. Since, later on, we will deal with two extensions at the same time, we shall give a name to the action of $Q$ on $A$, say $\varphi : Q \longrightarrow \operatorname{Aut} A$. Consider a map $\eta : Q \times Q \longrightarrow A$, and define a new multiplication on the set product $Q \times A$ by

$$(x, a)(y, b) = (xy, a^{\varphi(y)} + b + \eta(x, y)),$$

where we use additive notation for the abelian group $A$. The resulting quasigroup will be denoted by $E = (Q, A, \varphi, \eta)$.

It is easy to see that $E$ is a loop if and only if there exists $c \in A$ such that

$$\eta(x, 1) = c, \quad \eta(1, x) = c^{\varphi(x)}, \tag{7}$$

for every $x \in Q$. The neutral element of $E$ is then $(1, -c)$.

From now on, we will assume that $E$ satisfies (7) with $c = 0$, and speak of $E$ as an *extension* of $A$ by $Q$. Verify that $E$ is a group if and only if $Q$ is a group and

$$\eta(x, y)^{\varphi(z)} + \eta(xy, z) = \eta(y, z) + \eta(x, yz) \tag{8}$$

holds for every $x, y, z \in Q$. Moreover, using the Moufang identity $(xy \cdot x)z = x(y \cdot xz)$, one can check by straightforward calculation that $E$ is a Moufang loop if and only if

$$\eta(x, y)^{\varphi(xz)} + \eta(xy, x)^{\varphi(z)} + \eta(xy \cdot x, z) = \eta(x, z) + \eta(y, xz) + \eta(x, y \cdot xz) \tag{9}$$

holds for every $x, y, z \in Q$. (Note that $\varphi(y \cdot xz) = \varphi(yx \cdot z)$ even if $x, y, z$ do not associate.)

Every pair $(\varphi, \eta)$ satisfying (7) with $c = 0$ is called a *factor set*. If it also satisfies (8), resp. (9), we call it *associative factor set*, resp. *Moufang factor set*.

Given two factor sets $(\varphi, \eta)$ and $(\varphi, \mu)$, we can obtain another factor set, their *sum* $(\varphi, \eta + \mu)$, by letting $(\eta + \mu)(x, y) = \eta(x, y) + \mu(x, y)$ for every $x, y \in Q$. Since $A$ is an abelian group, the sum of two associative factor sets (resp. Moufang factor sets) is associative (resp. Moufang). As every group is a Moufang loop, it must be the case that every associative factor set is Moufang. Here is a proof that only refers to factor sets:

**Lemma 5.1.** *Every associative factor set is Moufang.*

*Proof.* Let $(\varphi, \eta)$ be an associative factor set. Substituting $xz$ for $z$ in (8) yields

$$\eta(x, y)^{\varphi(xz)} + \eta(xy, xz) = \eta(y, xz) + \eta(x, y \cdot xz), \tag{10}$$

while substituting $xy$ for $x$, and simultaneously $x$ for $y$ in (8) yields

$$\eta(xy, x)^{\varphi(z)} + \eta(xy \cdot x, z) = \eta(x, z) + \eta(xy, xz). \tag{11}$$

The identity (9) is obtained by adding (10) to (11) and subtracting $\eta(xy, xz)$ from both sides. □

Assume that $(\varphi, \eta)$ is a Moufang factor set. Then the right inverse of $(x, a)$ in $(Q, A, \varphi, \eta)$ is $(x^{-1}, -a^{\varphi(x^{-1})} - \eta(x, x^{-1}))$, as a short calculation reveals. Similarly, the left inverse of $(x, a)$ is $(x^{-1}, -a^{\varphi(x^{-1})} - \eta(x^{-1}, x)^{\varphi(x^{-1})})$. Since $(Q, A, \varphi, \eta)$ is a Moufang loop, the two inverses coincide, and we have

$$\eta(x, x^{-1}) = \eta(x^{-1}, x)^{\varphi(x^{-1})}, \tag{12}$$

for any Moufang factor set $(\varphi, \eta)$ and $x \in Q$. (Alternatively—and more naturally—the identity (12) follows immediately from (9) when we substitute $x^{-1}$ for $x$, $x$ for $y$, and 1 for $z$.)

**Lemma 5.2.** *Assume that $(\varphi, \eta)$ is a Moufang factor set and $(\varphi, \mu)$ is an associative factor set. Then the associators in $(Q, A, \varphi, \eta)$ and $(Q, A, \varphi, \eta+\mu)$ coincide if and only if*

$$\mu((x \cdot yz)^{-1}, xy \cdot z) = \mu(x \cdot yz, (x \cdot yz)^{-1})^{\varphi(xy\cdot z)} \tag{13}$$

*for every $x, y, z \in Q$. This happens if and only if*

$$\mu(x \cdot yz, [x, y, z]) = 0 \tag{14}$$

*for every $x, y, z \in Q$. In particular, the associators coincide if $Q$ is a group.*

*Proof.* Let $(x, a), (y, b), (z, c) \in (Q, A, \varphi, \eta)$. Then

$$\begin{aligned} u = (x, a)(y, b) \cdot (z, c) &= (xy \cdot z, s+t), \\ v = (x, a) \cdot (y, b)(z, c) &= (x \cdot yz, s), \end{aligned}$$

where

$$\begin{aligned} s &= a^{\varphi(yz)} + b^{\varphi(z)} + c + \eta(y, z) + \eta(x, yz), \\ t &= \eta(x, y)^{\varphi(z)} + \eta(xy, z) - \eta(y, z) - \eta(x, yz). \end{aligned}$$

The associator $[(x, a), (y, b), (z, c)]$ in $(Q, A, \varphi, \eta)$ is therefore equal to $v^{-1}u = ([x, y, z], d)$, where

$$d = t + \eta((x \cdot yz)^{-1}, xy \cdot z) - \eta(x \cdot yz, (x \cdot yz)^{-1})^{\varphi(xy\cdot z)}.$$

Similarly, the same associator in $(Q, A, \varphi, \eta+\mu)$ is $([x, y, z], d+e+f)$, where

$$\begin{aligned} e &= \mu(x, y)^{\varphi(z)} + \mu(xy, z) - \mu(y, z) - \mu(x, yz), \\ f &= \mu((x \cdot yz)^{-1}, xy \cdot z) - \mu(x \cdot yz, (x \cdot yz)^{-1})^{\varphi(xy\cdot z)}. \end{aligned}$$

Since $(\varphi, \mu)$ satisfies (8), $e$ vanishes. Therefore the two associators coincide for all $x$, $y$, $z \in Q$ if and only if (13) is satisfied for every $x, y, z \in Q$.

Substituting $x \cdot yz$ for $x$, $(x \cdot yz)^{-1}$ for $y$, and $xy \cdot z$ for $z$ into (8) yields

$$\mu(x \cdot yz, (x \cdot yz)^{-1})^{\varphi(xy\cdot z)} = \mu((x \cdot yz)^{-1}, xy \cdot z) + \mu(x \cdot yz, [x, y, z]).$$

Hence (13) is satisfied if and only if (14) holds. The latter condition is of course satisfied when $Q$ is a group. □

## 6. The Cyclic Construction for Moufang loops

Throughout this section, assume that $(G, S, \alpha, h)$ satisfies $(\mathcal{C})$, and that $A$ is the subloop of $S$ generated by $h$. Using loop extensions, we prove that $(G, *)$ is a Moufang loop with the same associators, associator subloop, and nucleus as $(G, \cdot)$. Recall that the *associator subloop* of a loop $L$ is the subloop $A(L)$ generated by all associators $[x, y, z]$, where $x, y, z \in L$.

**Lemma 6.1.** *$A$ is a normal subloop of both $(G, \cdot)$ and $(G, *)$. Moreover, $(G, \cdot)/A = (G, *)/A$.*

*Proof.* Since $h \in Z(G, \cdot)$, the subgroup $A = \langle h\rangle \subseteq Z(G, \cdot)$ is normal in $(G, \cdot)$. In fact, $x * h = xh$, $h * x = hx$ for every $x \in G$ (since $h \in S = \alpha^0$), and thus $A$ is normal in $(G, *)$ as well.

Write the elements of $G/A$ as cosets $xA$. Since, for some $t$, we have $xA \cdot yA = (xy)A$ and $xA * yA = (x * y)A = (xyh^t)A = (xy)A$, the loops $(G, \cdot)/A$ and $(G, *)/A$ coincide. □

Let $Q$ be the Moufang loop $(G, \cdot)/A = (G, *)/A$. Let $\iota$ be the trivial homomorphism $Q \longrightarrow \operatorname{Aut} A$, $\iota(q) = id_A$, for every $q \in Q$. We want to construct two factor sets $(\iota, \eta)$, $(\iota, \eta^*)$ such that $(Q, A, \iota, \eta) \simeq (G, \cdot)$ and $(Q, A, \iota, \eta^*) \simeq (G, *)$. In order to save space, we keep writing the operation in $A$ multiplicatively.

Let $\pi : Q = G/A \longrightarrow G$ be a transversal, i.e., a map satisfying $\pi(xA) \in xA$ for every $x \in G$. Then, for every $xA$, $yA$, there is an integer $\tau(xA, yA)$ such that $\pi((xy)A) = \pi(xA)\pi(yA)h^{\tau(xA, yA)}$.

**Proposition 6.2.** *Assume that $(G, S, \alpha, h)$ satisfies $(\mathcal{C})$, and that $A$ is the subloop of $S$ generated by $h$. With $Q = (G, \cdot)/A = (G, *)/A$ and $\tau$ as above, define $\eta$, $\eta^* : Q \times Q \longrightarrow A$ by*

$$\begin{aligned} \eta(xA, yA) &= h^{-\tau(xA, yA)}, \\ \eta^*(xA, yA) &= \eta(xA, yA)h^{\sigma(i+j)}, \end{aligned}$$

*where $x \in \alpha^i$, $y \in \alpha^j$, and $i$, $j \in M$. Then $(Q, A, \iota, \eta) \simeq (G, \cdot)$ and $(Q, A, \iota, \eta^*) \simeq (G, *)$.*

*Proof.* First of all, when $x$ belongs to $\alpha^i$ then every element of $xA$ belongs to $\alpha^i$, and so $\eta^*$ is well-defined.

Let $\theta : (Q, A, \iota, \eta) \longrightarrow (G, \cdot)$ be defined by $\theta(xA, h^a) = \pi(xA)h^a$. Note that $\theta$ is well-defined, and that it is clearly a bijection. Since

$$\begin{aligned} &\theta((xA, h^a)(yA, h^b)) = \theta((xy)A, h^{a+b}\eta(xA, yA)) = \pi((xy)A)h^{a+b}\eta(xA, yA) \\ &= \pi(xA)\pi(yA)h^{\tau(xA, yA)}h^{a+b}h^{-\tau(xA, yA)} = \pi(xA)h^a\pi(yA)h^b = \theta(xA, h^a)\theta(yA, h^b), \end{aligned}$$

$\theta$ is an isomorphism.

Similarly, let $\theta^* : (Q, A, \iota, \eta^*) \longrightarrow (G, *)$ be defined by $\theta^*(xA, h^a) = \pi(xA)h^a$. This is again a bijection. Pick $x \in \alpha^i$, $y \in \alpha^j$. Since

$$\begin{aligned} \theta^*((xA, h^a)(yA, h^b)) &= \theta^*((xy)A, h^{a+b}\eta^*(xA, yA)) = \pi((xy)A)h^{a+b}\eta^*(xA, yA) \\ &= \pi(xA)\pi(yA)h^{\tau(xA, yA)}h^{a+b}h^{-\tau(xA, yA)}h^{\sigma(i+j)} = \pi(xA)\pi(yA)h^{a+b}h^{\sigma(i+j)} \\ &= \pi(xA)h^a * \pi(yA)h^b = \theta^*(xA, h^a) * \theta^*(yA, h^b), \end{aligned}$$

$\theta^*$ is an isomorphism. □

We are now ready to prove the main theorem for the cyclic construction:

**Theorem 6.3.** *The Moufang factor sets $(\iota, \eta)$ and $(\iota, \eta^*)$ introduced in Proposition 6.2 differ by an associative factor set $(\iota, \mu)$ that satisfies (13). Consequently, $(G, *)$ is a Moufang loop, the associators in $(G, \cdot)$ and $(G, *)$ coincide, $A(G, \cdot) = A(G, *)$ coincide as loops, and $N(G, \cdot) = N(G, *)$ coincide as sets.*

*Proof.* With $\mu = \eta^* - \eta$ and $x \in \alpha^i$, $y \in \alpha^j$, we have $\mu(xA, yA) = h^{\sigma(i+j)}$. Since $\mu(xA, A) = \mu(A, xA) = h^{\sigma(i)} = h^0 = 1$, $(\iota, \mu)$ is a factor set. Pick further $z \in \alpha^k$. We must verify that $(\iota, \mu)$ is associative, i.e., that

$$\mu(xA, yA)\mu(xA, yAzA) = \mu(yA, zA)\mu(xA, yAzA).$$

But this follows immediately from (1), as $xAyA \in \alpha^{i\oplus j}$ and $yAzA \in \alpha^{j\oplus k}$. Thus $(\iota,\, \mu)$ is associative, in particular Moufang. Then $(\iota,\, \eta^*) = (\iota,\, \eta) + (\iota,\, \mu)$ is a Moufang factor set.

It is easy to verify that all associators of $(G,\, \cdot)$ belong to $\alpha^0$. This means that $\mu(xAyA \cdot zA,\, [xA,\, yA,\, zA])$ vanishes, and hence the associators in $(G,\, \cdot)$ and $(G,\, *)$ coincide by Lemma 5.2. The associator subloops $A(G,\, \cdot)$ and $A(G,\, *)$ are therefore generated by the same elements. In fact, the multiplication in $A(G,\, \cdot)$ coincides with the multiplication in $A(G,\, *)$ because, once again, every associator belongs to $\alpha^0$. Finally, since an element belongs to the nucleus if and only if it associates with all other elements, we must have $N(G,\, \cdot) = N(G,\, *)$. □

## 7. The Dihedral Construction for Moufang Loops

We are now going to prove that the dihedral construction works for Moufang loops, too. The reasoning is essentially that of Section 6, however, we decided that it deserves a separate treatment since it differs in several details. The confident reader can proceed directly to the next section.

Throughout this section, we assume that $(G,\, S,\, \beta,\, \gamma,\, h)$ satisfies $(\mathcal{D})$, and that $A$ is the subloop of $S$ generated by $h$.

**Lemma 7.1.** *$A$ is a normal subloop of both $(G,\, \cdot)$ and $(G,\, *)$. Moreover, $(G,\, \cdot)/A = (G,\, *)/A$.*

*Proof.* We claim that $A$ is a normal subloop of $(G,\, \cdot)$. It suffices to prove that $xA = Ax$, $x(Ay) = (xA)y$ and $x(yA) = (xy)A$ for every $x,\, y \in G$. Since $A \le N(G)$, we only have to show that $xA = Ax$ for every $x \in G$. When $x \in G_0$, there is nothing to prove as $h \in Z(G_0)$. When $x \in G_1$, we have $xA = \{xh^a;\ 0 \le a < 2m\} = \{h^{-a}x;\ 0 \le a < 2m\} = Ax$, because $hxh = x$. Thus $A$ is normal in $(G,\, \cdot)$. In fact, $x * h = xh$, $h * x = hx$ for every $x \in G$ (since $h \in S = \alpha^0$), and thus $A$ is normal in $(G,\, *)$ as well.

Write the elements of $G/A$ as cosets $xA$. Since, for some $t$, we have $xA \cdot yA = (xy)A$ and $xA * yA = (x * y)A = (xyh^t)A = (xy)A$, the loops $(G,\, \cdot)/A$ and $(G,\, *)/A$ coincide. □

We let $Q$ be the Moufang loop $(G,\, \cdot)/A = (G,\, *)/A$, and continue to construct two factor sets $(\varphi,\, \eta)$, $(\varphi,\, \eta^*)$ such that $(Q,\, A,\, \varphi,\, \eta) \simeq (G,\, \cdot)$ and $(Q,\, A,\, \varphi,\, \eta^*) \simeq (G,\, *)$.

Fix a transversal $\pi : Q = G/A \longrightarrow G$. Then, for every $xA$, $yA$, there is an integer $\tau(xA,\, yA)$ such that $\pi((xy)A) = \pi(xA)\pi(yA)h^{\tau(xA,\, yA)}$.

**Proposition 7.2.** *Assume that $(G,\, S,\, \beta,\, \gamma,\, h)$ satisfies $(\mathcal{D})$, and that $A$ is the subloop of $S$ generated by $h$. With $Q = (G,\, \cdot)/A = (G,\, *)/A$ and $\tau$ as above, define $\varphi : Q \longrightarrow \mathrm{Aut}\, A$ by $a^{\varphi(y)} = a^{(-1)^r}$, where $y \in G_r$, $r \in \{0,\, 1\}$. Furthermore, define $\eta,\, \eta^* : Q \times Q \longrightarrow A$ by*

$$\begin{aligned} \eta(xA,\, yA) &= h^{-\tau(xA,\, yA)}, \\ \eta^*(xA,\, yA) &= \eta(xA,\, yA)h^{(-1)^r\sigma(i+j)}, \end{aligned}$$

*where $x \in \alpha^i \cup e\alpha^i$, $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, $i,\, j \in M$, $r \in \{0,\, 1\}$. Then $(Q,\, A,\, \varphi,\, \eta) \simeq (G,\, \cdot)$ and $(Q,\, A,\, \varphi,\, \eta^*) \simeq (G,\, *)$.*

*Proof.* Since $G_rG_s = G_{r+s \pmod 2}$ for every $r,\, s \in \{0,\, 1\}$, $\varphi$ is a homomorphism.

When $x$ belongs to $\alpha^i \cup e\alpha^i$, then every element of $xA$ belongs to $\alpha^i \cup e\alpha^i$. When $y$ belongs to $(\alpha^j \cup \alpha^j f) \cap G_r$, then every element of $yA$ belongs to $(\alpha^j \cup \alpha^j f) \cap G_r$. Hence $\eta^*$ is well-defined.

Let $\theta : (Q, A, \varphi, \eta) \longrightarrow (G, \cdot)$ be defined by $\theta(xA, h^a) = \pi(xA)h^a$. This is clearly a well-defined bijection. When $y \in G_r$, we have

$$\begin{aligned}&\theta((xA, h^a)(yA, h^b)) = \theta((xy)A, h^{(-1)^r a}h^b\eta(xA, yA))\\ &= \pi((xy)A)h^{(-1)^r a}h^b\eta(xA, yA) = \pi(xA)\pi(yA)h^{\tau(xA, yA)}h^{(-1)^r a}h^b h^{-\tau(xA, yA)}\\ &= \pi(xA)\pi(yA)h^{(-1)^r a}h^b = \pi(xA)h^a\pi(yA)h^b = \theta(xA, h^a)\theta(yA, h^b),\end{aligned}$$

and $\theta$ is an isomorphism.

Similarly, let $\theta^* : (Q, A, \varphi, \eta^*) \longrightarrow (G, *)$ be defined by $\theta^*(xA, h^a) = \pi(xA)h^a$. This is again a bijection. With $x \in \alpha^i \cup e\alpha^i$, $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, we have

$$\begin{aligned}&\theta^*((xA, h^a)(yA, h^b)) = \theta^*((xy)A, h^{(-1)^r a}h^b\eta^*(xA, yA))\\ &= \pi((xy)A)h^{(-1)^r a}h^b\eta^*(xA, yA)\\ &= \pi(xA)\pi(yA)h^{\tau(xA, yA)}h^{(-1)^r a}h^b h^{-\tau(xA, yA)}h^{(-1)^r\sigma(i+j)}\\ &= \pi(xA)h^a\pi(yA)h^b h^{(-1)^r\sigma(i+j)} = \pi(xA)h^a * \pi(yA)h^b = \theta^*(xA, h^a) * \theta^*(yA, h^b),\end{aligned}$$

and $\theta^*$ is an isomorphism. □

**Theorem 7.3.** *The Moufang factor sets* $(\varphi, \eta)$ *and* $(\varphi, \eta^*)$ *introduced in Proposition* 7.2 *differ by an associative factor set* $(\varphi, \mu)$ *that satisfies* (13). *Consequently,* $(G, *)$ *is a Moufang loop, the associators in* $(G, \cdot)$ *and* $(G, *)$ *coincide,* $A(G, \cdot) = A(G, *)$ *coincide as loops, and* $N(G, \cdot) = N(G, *)$ *coincide as sets.*

*Proof.* Let $\mu = \eta^* - \eta$. For $x \in \alpha^i \cup e\alpha^i$, $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, we have $\mu(xA, yA) = h^{(-1)^r\sigma(i+j)}$.

Since $\mu(xA, A) = \mu(A, xA) = h^0 = 1$, $(\varphi, \mu)$ is a factor set. By the first 2 paragraphs of the proof of Proposition 4.3, $(\varphi, \mu)$ is associative, hence Moufang. Then $(\varphi, \eta^*) = (\varphi, \eta) + (\varphi, \mu)$ is a Moufang factor set.

It is easy to verify that every associator of $(G, \cdot)$ belongs to $\alpha^0$. We can therefore reach the same conclusion as in Theorem 6.3. □

## 8. Code Loops

Now when we know that $(G, *)$ is a Moufang loop for both constructions, we will focus on the effect the constructions have on two important classes of Moufang loops: code loops and loops of type $M(G, 2)$. These loops are abundant among small Moufang loops, as we will see in Section 10. The results of Sections 8 and 9 are not needed elsewhere in this paper. Let us get started with code loops.

A loop $G$ is called *symplectic* if it possesses a central subloop $Z$ of order 2 such that $G/Z$ is an elementary abelian 2-group. When $G$ is symplectic, we can define $P : G/Z \longrightarrow Z$, $C : G/Z \times G/Z \longrightarrow Z$, $A : G/Z \times G/Z \times G/Z \longrightarrow Z$ by $P(aZ) = a^2$, $C(aZ, bZ) = [a, b]$, $A(aZ, bZ, cZ) = [a, b, c]$, for every $a, b, c \in G$. Note that the three maps are well defined. For obvious reasons, we will often call $P$ the *power map*, $C$ the *commutator map*, and $A$ the *associator map*.

Every symplectic loop $G$ is an extension $(V, F, \iota, \eta)$ of the 2-element field $F = \{0, 1\}$ by a finite vector space $V$ over $F$, where $\eta : V \times V \longrightarrow F$ satisfies $\eta(u, 0) = \eta(0, u) = 0$ for every $u \in V$ (i.e., $(\iota, \eta)$ is a factor set as defined in Section 5). We can then identify $F$ with $Z$, $V$ with $G/Z$, and consider $P$, $C$, $A$ as maps $P : V \longrightarrow F$, $C : V \times V \longrightarrow F$, $A : V \times V \times V \longrightarrow F$.

It is known that the triple $(P, C, A)$ determines the isomorphism type of $G$ (cf. [1, Theorem 12.13]).

Before we introduce code loops, we must define derived forms and combinatorial degree. We will restrict the definitions to the two-element field $F$; more general definitions can be found in [1] and [19].

Let $f : V \longrightarrow F$ be a map satisfying $f(0) = 0$. Then the *nth derived form* $f_n : V^n \longrightarrow F$ of $f$ is defined by

$$f_n(v_1, \dots, v_n) = \sum_{\{i_1, \dots, i_m\} \subseteq \{1, \dots, n\}} f(v_{i_1} + \cdots + v_{i_m}),$$

where the summation runs over all nonempty subsets of $\{1, \dots, n\}$. Although it is not immediately obvious, $f_n(v_1, \dots, v_n)$ vanishes whenever $v_1, \dots, v_n$ are linearly dependant, and it makes sense to define the *combinatorial degree* of $f$, $\operatorname{cdeg} f$, as the smallest nonnegative integer $n$ such that $f_{n+1} = 0$.

Every form $f_n$ is symmetric, and two consecutive derived forms are related by *polarization*, i.e.,

$$f_{n+1}(v_1, \dots, v_{n+1}) = f_n(v_1, v_3, \dots, v_{n+1}) + f_n(v_2, \dots, v_{n+1}) + f_n(v_1 + v_2, v_3, \dots, v_{n+1}),$$

for every $v_1, \dots, v_{n+1} \in V$. Thus $f_n$ is $n$-linear if and only if $\operatorname{cdeg} f \leq n$. Since $f(0) = 0$, the form $f_2$ is alternating. Recall that every alternating bilinear form over the two-element field is symmetric. When $f$ is a quadratic form, $f_2$ is an alternating (thus symmetric) bilinear form. Therefore the subspace of all forms $f : V \longrightarrow F$ with $\operatorname{cdeg} f \leq 2$ coincides with the subspace of all quadratic forms.

A symplectic loop $G$ defined on $V \times F$ is called a *code loop* if the power map $P : V \longrightarrow F$ has $\operatorname{cdeg} P \leq 3$, the commutator map $C$ coincides with $P_2$, and the associator map $A$ coincides with $P_3$. The power map therefore determines a code loop up to an isomorphism, and we will use the notation $G = (V, F, P)$.

**Remark 8.1.** Code loops were discovered by Griess [12], who used them to elucidate the construction of the Parker loop, that is in turn involved in the construction of the Monster group. We completely ignore the code aspect of code loops here, and model our approach on [1] and [13].

Of course, not every symplectic loop is a code loop, however, as Aschbacher proved in [1, Lemma 13.1], Chein and Goodaire in [4], and Hsu in [13]:

**Theorem 8.2.** *Code loops are exactly symplectic Moufang loops.*

Thus our two constructions apply to code loops and we proceed to have a closer look at them. Recall that the *radical* $\operatorname{Rad} f$ of an $n$-linear form $f : V^n \longrightarrow F$ is the subspace consisting of all vectors $v_1 \in V$ such that $f(v_1, \dots, v_n) = 0$ for every $v_2, \dots, v_n \in V$.

The radical of $P_3$ determines the nucleus of the associated code loop, and vice versa. We offer a complete description of the situation when $P_3$ has trivial radical (i.e., $\operatorname{Rad} P_3 = F$). Then there is only one choice of $h$ for $(\mathcal{C})$ and $(\mathcal{D})$ (see below). We expect to return to code loops with nontrivial radical in a future paper.

**Remark 8.3.** Code loops with nontrivial radical are not closed under the two constructions. (cf. Example 10.2). In fact, all code loops of order 32 have this property.

**Lemma 8.4.** *Let $G = (V, F, P)$ be a code loop. Assume that $(\mathcal{C})$ or $(\mathcal{D})$ is satisfied with some $h$, $S$. Then:*

(i) *If $G$ is not a group or if $h \in F$, then $S \supseteq F$, and $G/S \simeq C_2$ or $G/S \simeq V_4$.*
(ii) *If $h \in F$ then the resulting loop $(G, *)$ is a code loop with the same radical as $G$.*
(iii) *If $\operatorname{Rad} P_3 = F$ then $h \in N(G) = Z(G) = F$.*

*Proof.* Since $G = (V, F, P)$ is a code loop, we have $A(G) \subseteq F$. Let us prove (i). First assume that $G$ is not a group. Since $|F| = 2$, we must have $A(G) = F$. As $G/S$ is associative, the subloop $S$ contains $A(G) = F$. Now assume that $1 \neq h \in F$. Since $h$ belongs to $S$, we immediately obtain $S \supseteq F$. Hence, in any case, $G/S \leq G/F$, and $G/S$ is an elementary abelian 2-group. The only two elementary abelian 2-groups satisfying $(\mathcal{C})$ or $(\mathcal{D})$ are $C_2$ and $V_4$, respectively.

To prove (ii), assume that $h \in F$. Then $(F, *)$ is a subloop of $(G, *)$, by (3) and (5). Now, $x * a = xa$ and $a * x = ax$ for every $x \in G$, $a \in F$. Since $F$ is central in $G$, $(F, *)$ is also central in $(G, *)$. Finally, $x * x$ belongs to $F$ for every $x \in G$, thus $(G, *)/(F, *)$ is an elementary abelian 2-group. By Theorems 6.3 and 7.3, $(G, *)$ is a Moufang loop. Then Theorem 8.2 implies that $(G, *)$ is a code loop. Another consequence of Theorems 6.3 and 7.3 is that $N(G) = N(G, *)$. Hence the radical of the associator map $P_3$ in $G$ coincides with the radical of the associator map $P_3^*$, where $P^*$ is the power map in $(G, *)$.

To prove (iii), suppose that $\operatorname{Rad} P_3 = F$. Then $h \in N(G) \subseteq F \subseteq Z(G) \subseteq N(G)$, where the only nontrivial inclusion $N(G) \subseteq F$ follows from the fact that $\operatorname{Rad} P_3$ is trivial. □

Consider this general result about Moufang loops and code loops with trivial radical.

**Lemma 8.5.** *Suppose that $L$ is a Moufang loop whose associator is equivalent to the associator of a code loop $G$ with trivial radical. Then $L$ is a code loop with trivial radical.*

*Proof.* By the assumptions, $A(G) \leq N(G) = Z(G)$, therefore $A(L) \leq N(L) = Z(L)$, and $L/N(L)$ is a group. Let $R$ be the associator map in $L$, and let $x, y, z \in L$. Then $R(x, y, z) = 0$ if and only if $R(x^{-1}, y, z) = 0$, by the Moufang theorem. Since $|A(L)| \leq 2$, we obtain

$$R(x, y, z) = R(x^{-1}, y, z) \tag{15}$$

for every $x, y, z \in L$. Because $R$ is equivalent to the associator map of the code loop $G$, it is trilinear and $\operatorname{Rad} R = N(L)$. Then (15) implies $xN(L) = x^{-1}N(L)$ in $L/N(L)$, and $L/N(L)$ is an elementary abelian 2-group. □

**Lemma 8.6.** *Assume that $h \in F$, and that $(G, *)$ is constructed from a code loop $G = (V, F, P)$ as in Lemma* 8.4*. Let $P^*$ be the power map of $(G, *)$. When $G/S \simeq C_2$ then*

$$P^*(xF) = \begin{cases} P(xF), & x \in S, \\ P(xF) + h, & x \in G \setminus S, \end{cases} \tag{16}$$

*and $P^* - P$ is linear.*

*Else $G/S \simeq V_4$,*

$$P^*(xF) = \begin{cases} P(xF), & x \notin \alpha, \\ P(xF) + h, & x \in \alpha, \end{cases} \tag{17}$$

(*where $\alpha = \beta\gamma$ is as usual*), *and $P^* - P$ is a quadratic form.*

*Proof.* Since $x * y \in \{xy, xyh\}$, the addition in $G/F$ coincides with the addition in $(G, *)/F$, and we can let $G/F = (G, *)/F = V$. By Lemma 8.4(i), $G/S \simeq C_2$ or $G/S \simeq V_4$. If $G/S \simeq C_2$, we have (16). Thus $P^* - P$ is linear.

If $G/S \simeq V_4$, we have (17). We claim that $R = P^* - P$ is a quadratic form. First of all, $R_2(xF, yF) = R(xF) + R(yF) + R(xF + yF)$ does not vanish if and only if $x, y$ belong to $\alpha \cup \beta \cup \gamma$ but not to the same coset at the same time. Then $R_3(xF, yF, zF) = R_2(xF, zF) + R_2(yF, zF) + R_2(xF + yF, zF)$ always vanishes, as one easily checks. □

We are ready to characterize all loops obtainable from code loops with trivial radical via both of the constructions. We will also show how to connect all code loops with the same associator maps.

**Proposition 8.7.** *Let $G = (V, F, P)$ be a code loop with power map $P$. Let $H_0 = G$, $H_1, \dots, H_s$ be a sequence of loops, where $H_{i+1}$ is obtained from $H_i$ by the cyclic or the dihedral construction, for $i = 0, \dots, s-1$. If $\mathrm{Rad}\, P_3$ is trivial, then $H_s$ is a code loop with power map $R$ satisfying $\mathrm{cdeg}\,(R - P) \le 2$. Whether $\mathrm{Rad}\, P_3$ is trivial or not, every code loop $H_s$ with power map $R$ satisfying $\mathrm{cdeg}\,(R-P) \le 2$ can be obtained from $H_0$ in this way.*

*Proof.* Denote by $P^*$ the power map in $H_1$. For the rest of this paragraph, assume that $P_3$ has trivial radical. By Lemma 8.4, $H_1$ is a code loop with trivial radical, and, by Lemma 8.6, $\mathrm{cdeg}\,(P^* - P) \le 2$. By induction, $H_s$ is a code loop and $\mathrm{cdeg}\,(R-P) \le 2$.

In fact, the two maps $P^* - P$ from (16) and (17) are available as long as $h \in F$, no matter what $\mathrm{Rad}\, P_3$ is.

In order to obtain all code loops with $\mathrm{cdeg}\,(R-P) \le 2$ from $H_0$, we must show that the forms $P^* - P$ from (16) and (17) generate all forms with cdeg $\le 2$, i.e., all quadratic forms. Every quadratic form $Q$ determines an alternating bilinear form $Q_2$, and when $Q_2 = T_2$ for two quadratic forms $Q$, $T$, their difference $Q - T$ is a linear form. We must therefore show how to obtain all linear forms, and also all alternating bilinear forms as second derived forms of maps stemming from (16) and (17).

Note that the difference $P^* - P$ in (16) determines a hyperplane $S \cap V$ of $V$. Conversely, if $W \le V$ is a hyperplane, then $W + F$ is a normal subloop of $V + F$. In this way, we obtain all linear forms.

In (17), $Q = P^* - P$ is a quadratic form such that $\mathrm{Rad}\, Q_2 = S$ has codimension 2 (since $|G/S| = 4$). Moreover, $Q_2(\gamma, \gamma) = Q_2(\beta, \beta) = 0$, $Q_2(\beta, \gamma) \ne 0$, so that $Q = U \oplus S$ for a hyperbolic plane $U = \langle x, y\rangle$, $x \in \beta$, $y \in \gamma$. In this way, we can obtain all hyperbolic planes. Every alternating bilinear form $f$ can be expressed as $U_1 \oplus \cdots \oplus U_k \oplus \mathrm{Rad}\, f$, where every $U_i$ is a hyperbolic plane. Thus, by summing up the differences $Q$ from repeated applications of the dihedral construction, we can obtain any alternating bilinear form. □

Let us summarize the results about code loops obtained in this section:

**Theorem 8.8.** *If $G$ is a code loop with trivial radical and $(\mathcal{C})$ or $(\mathcal{D})$ is satisfied for some $S \le G$, then $G/S$ is isomorphic to $C_2$ or $V_4$. The resulting loop $(G, *)$ is a code loop with trivial radical, and the associators of $G$ and $(G, *)$ are equivalent. Every Moufang loop whose associator is equivalent to the associator of a code loop with trivial radical is itself a code loop with trivial radical. Finally, any two code loops with equivalent associators can be connected by the cyclic and dihedral constructions, possibly repeated.*

**Remark 8.9.** It is not hard to check that trilinear alternating forms with trivial radical exist in dimension $n$ if and only if $n = 3$ or $n \ge 5$. (There are many nonequivalent trilinear alternating forms with trivial radical when $n \ge 9$.) Consequently, there are code loops with trivial radical (i.e., with two-element nucleus) of order $2^n$ if and only if $n = 4$ or $n \ge 6$.

## 9. Loops of Type $M(G, 2)$

Chein [3] discovered the following way of building up nonassociative Moufang loops from nonabelian groups: Let $G$ be a finite group, and denote by $\overline{G}$ the set of new elements

$\{\overline{x};\ x \in G\}$. Then $M(G,\,2) = (G \cup \overline{G},\,\circ)$ with multiplication $\circ$ defined by

$$x \circ y = xy, \quad x \circ \overline{y} = \overline{yx}, \quad \overline{x} \circ y = \overline{xy^{-1}}, \quad \overline{x} \circ \overline{y} = y^{-1}x \tag{18}$$

is a Moufang loop that is associative if and only if $G$ is abelian. As the restriction of the multiplication $\circ$ on $G$ coincides with the multiplication in $G$, we will usually denote the multiplication in $M(G,\,2)$ by $\cdot$, too.

Many small Moufang loops are of this type; for instance $16/k$ for $k \le 2$, and $32/k$ for $k \le 9$, where $n/k$ is the $k$th nonassociative Moufang loop of order $n$. (See Section 10 for details. Table 1 in [11, p. A-3] lists all loops $M(G,\,2)$ of order at most 63.)

In this Section we are going to explore the effects of our constructions on loops $M(G,\,2)$. The results are summarized in Corollary 9.3 for the cyclic construction, and in Proposition 9.4 for the dihedral construction.

The following Lemma gives some basic properties of loops $M(G,\,2)$:

**Lemma 9.1.** *Let $G$ be a group and let $L = M(G,\,2)$ be the Moufang loop defined above. Then:*

(i) *If $G$ is an abelian group then $N(L) = L$, else $N(L) = Z(G)$.*
(ii) *If $G$ is an elementary abelian 2-group then $Z(L) = L$, else $Z(L) = Z(G) \cap \{x \in G;\ x^2 = 1\}$.*
(iii) *If $S \le L$ then $S \le G$ or $|S \cap G| = |S \cap \overline{G}|$.*
(iv) *If $S \trianglelefteq G$ then $S \trianglelefteq L$.*
(v) *If $S \trianglelefteq L$ then $S \trianglelefteq G$, or both $G/(S \cap G)$ and $L/S$ are elementary abelian 2-groups.*

*Proof.* We know that $N(L) = L$ if and only if $G$ is abelian. Assume that $G$ is not abelian. Then there are $x,\,y,\,z \in G$ such that $\overline{x} \cdot yz = \overline{x(yz)^{-1}} \ne \overline{xy^{-1}z^{-1}} = \overline{x}y \cdot z$, and thus no element of $\overline{G}$ belongs to $N(L)$. We have $x \cdot y\overline{z} = \overline{zyx}$, while $xy \cdot \overline{z} = \overline{zxy}$. Also, $x(\overline{y} \cdot \overline{z}) = xz^{-1}y$, while $x\overline{y} \cdot \overline{z} = z^{-1}yx$. Hence $x \in G$ belongs to $N(L)$ if and only if $x \in Z(G)$. This proves (i).

When $G$ is an elementary abelian 2-group, we have $L \simeq G \times C_2$. As $x\overline{y} = \overline{yx}$ and $\overline{y}x = \overline{yx^{-1}}$, an element $x \in G$ commutes with all elements of $L$ if and only if $x \in Z(G)$ and $x^2 = 1$. This proves (ii).

Part (iii) is an easy exercise (or see [16, Proposition 4.5]).

Let $S \trianglelefteq G$, and let $\varphi : G \longrightarrow H$ be a group homomorphism with kernel $S$. It is then easy to see that $\psi : M(G,\,2) \longrightarrow M(H,\,2)$ defined by $\psi(g) = \varphi(g)$, $\psi(\overline{g}) = \overline{\varphi(g)}$, for $g \in G$, is a homomorphism of Moufang loops with kernel $S$. Thus $S \trianglelefteq M(G,\,2)$, and (iv) is proved.

Finally, assume that $S \trianglelefteq L$ and $S \not\le G$. Then there is $y \in G$ such that $\overline{y} \in S$. For every $x \in G$, the element $x\overline{y}x^{-1} \cdot \overline{y}$ belongs to $S$, since $S \trianglelefteq L$. However, $x\overline{y}x^{-1} \cdot \overline{y} = \overline{yxx} \cdot \overline{y} = y^{-1}yxx = xx$. That is why $S \cap G$ contains all squares $x^2$, for $x \in G$, and the group $G/(S \cap G)$ must be an elementary abelian 2-group. Also, $\overline{x} \cdot \overline{x} = 1$ for every $x \in G$. Hence $L/S$ is an elementary abelian 2-group. □

We now investigate the two constructions for loops $M(G,\,2)$.

**Lemma 9.2.** *Let $G$ be a group and let $L = M(G,\,2)$ be the Moufang loop defined above. Then:*

(i) *If $(G,\,S,\,\alpha,\,h)$ satisfies $(\mathcal{C})$ then $L/S$ is dihedral, $h \in N(L)$, and $hxh = x$ for every $x \in L \setminus G$.*
(ii) *If $L/S$ is cyclic then $L/S \simeq C_2$ and either $S = G$ or $G/S \cap G \simeq C_2$.*

*Proof.* Assume that $S \trianglelefteq G$ and $G/S = \langle\alpha\rangle$ is cyclic of order $m$. Set $a = \alpha$, $b = \overline{S} = \overline{\alpha^0}$. Then $\langle a,\,b\rangle = L/S$ and, thanks to diassociativity, $L/S$ is a group. Moreover, $a^m = S$,

$b^2 = \overline{S} \cdot \overline{S} = S$, and $aba = \alpha\overline{\alpha^0}\alpha = \overline{\alpha}\alpha = \overline{\alpha^0} = b$. We know from Lemma 9.1(i) that $h \in S \cap Z(G)$ belongs to $N(L)$. Pick $\overline{g} \in \overline{G}$. Then $h\overline{g}h = \overline{gh}h = \overline{ghh^{-1}} = \overline{g}$. This proves (i).

We proceed to prove (ii). Assume that $L/S = \langle \alpha \rangle$ is cyclic. There must be some $x \in G$ such that $\overline{x} \in \alpha$, else $\alpha \subseteq G$, which is impossible. As $\overline{x} \cdot \overline{x} = 1$, we have $\alpha^2 = S$, and $L/S \simeq C_2$ follows. The rest is obvious. □

Consider this generalization of loops $M(G, 2)$, also found in [3, Theorem 2']: Let $G$ be a group, $\theta$ an antiautomorphism of $G$, and $1 \neq h \in Z(G)$ such that $\theta$ is an involution, $\theta(h) = h$, and $x\theta(x) \in Z(G)$ for every $x \in G$. Then the loop $M(G, \theta, h) = (G \cup \overline{G}, \circ)$ with multiplication $\circ$ defined by

$$x \circ y = xy, \quad x \circ \overline{y} = \overline{yx}, \quad \overline{x} \circ y = \overline{x\theta(y)}, \quad \overline{x} \circ \overline{y} = \theta(y)xh, \tag{19}$$

is a Moufang loop that is associative if and only if $G$ is abelian.

Notice how the multiplication in $M(G, {}^{-1}, h)$ differs from that of $M(G, 2)$ only at $\overline{G} \times \overline{G}$.

We claim that $M(G, {}^{-1}, h)$ is never isomorphic to $M(H, 2)$, for any groups $G$, $H$: Every element of $\overline{H}$ in $M(H, 2)$ is an involution. Calculating in $M(G, {}^{-1}, h)$, we get $\overline{x} * \overline{x} = h$ for every $x \in G$. Thus every element of $\overline{G}$ in $M(G, {}^{-1}, h)$ is of order $2|h|$, where $|h|$ is the order of $h$. Then there are simply not enough elements of order $2|h|$ in $M(H, 2)$ for $M(H, 2)$ to be isomorphic to $M(G, {}^{-1}, h)$.

Using Lemma 9.2 and the definitions (18) and (19), we get:

**Corollary 9.3.** *Let $G$ be a group and let $L = M(G, 2)$ be the Moufang loop defined above. Assume that $(L, S, \alpha, h)$ satisfies $(\mathcal{C})$. Then $S = G$ or $G/(S \cap G) \simeq C_2$. When $S = G$, the Moufang loop $(L, *)$ is isomorphic to $M(G, {}^{-1}, h)$. Every loop $M(G, {}^{-1}, h)$ with $h^2 = 1$ can be obtained in this way. When $G/(S \cap G) \simeq C_2$, then the multiplication in $(L, *)$ is given by*

$$x * y = \begin{cases} x \cdot y, & \text{if } x \in S \text{ or } y \in S, \\ (x \cdot y)h, & \text{otherwise}, \end{cases} \tag{20}$$

*where $x$, $y \in L$, and where $\cdot$ is the multiplication in $L$.*

With the classification [11] available, one can often determine the isomorphism type of $(L, *)$ from Corollary 9.3. To illustrate this point, assume that $(L = M(G, 2), S, \alpha, h)$ satisfies $(\mathcal{C})$ and that $S = G$. When $G = D_8$, the loop $L = M(D_8, 2)$ contains 2 elements of order 4. Hence $(L, *)$ must contain $2 + 8 = 10$ elements of order 4, and it turns out that the only such nonassociative Moufang loop of order 16 is 16/5, according to [11]. Similarly, $16/2 = M(Q_8, 2)$ always yields 16/2—the octonion loop of order 16. If $L = 24/1 = M(D_{12}, 2)$, $(L, *)$ is isomorphic to 24/4; if $L = 32/9 = M(Q_{16}, 2)$, $(L, *)$ is 32/38, etc.

Now for the dihedral construction:

**Proposition 9.4.** *Let $G$ be a group and let $L = M(G, 2)$ be the Moufang loop defined above. Assume that $(L, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$. Then $(L, *)$ is isomorphic to $M(H, 2)$ for some group $H$. Moreover, $S \trianglelefteq G$, or $L/S \simeq G/(S \cap G) \simeq V_4$. When $S \trianglelefteq G$, then $(G, S, G \setminus S, h)$ satisfies $(\mathcal{C})$, and the loop $(L, *)$ is equal to $M((G, *), 2)$.*

*Proof.* Assume that $(L, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$. Since the only elementary abelian 2-group that is also dihedral is $V_4$, Lemma 9.1(v) implies that $S \trianglelefteq G$, or $L/S \simeq G/S \cap G \simeq V_4$. When $S \trianglelefteq G$, the group $G/S$ is obviously cyclic.

Suppose that $S \trianglelefteq G$ and $\alpha = G \setminus S$. Then $(G, S, \alpha, h)$ satisfies $(\mathcal{C})$, and we can construct the group $(G, *)$. We are going to show that the loop $(L, *)$ obtained from $L$ by the dihedral construction is equal to $(L, \circ) = M((G, *), 2)$, where we have denoted the operation by $\circ$ to avoid confusion.

Write $G = \bigcup_{i \in M} \alpha^i$. Without loss of generality, suppose that $\overline{\alpha^i} = \alpha^i\gamma = \beta\alpha^{1-i}$ for every $i \in M$. Let $x \in \alpha^i$ and $y \in \alpha^j$. We must show carefully that $x * y = x \circ y$, $x * \overline{y} = x \circ \overline{y}$, $\overline{x} * y = \overline{x} \circ y$, and $\overline{x} * \overline{y} = \overline{x} \circ \overline{y}$. Clearly, $x * y = x \circ y$. Also, $x * \overline{y} = (x \cdot \overline{y}) \cdot h^{-\sigma(i+j)} = \overline{yx} \cdot h^{-\sigma(i+j)} = \overline{yxh^{\sigma(i+j)}} = \overline{y * x} = x \circ \overline{y}$. Similarly, $\overline{x} * y = (\overline{x} \cdot y) \cdot h^{\sigma(1-i+j)} = \overline{xy^{-1}} \cdot h^{\sigma(1-i+j)} = \overline{xy^{-1}h^{-\sigma(1-i+j)}} = \overline{xy^{-1}h^{\sigma(i-j)}} = \overline{x * y^{-1}} = \overline{x} \circ y$, where we have used the coset relation $\alpha^i\gamma = \beta\alpha^{1-i}$, and $-\sigma(t) = \sigma(1-t)$. Finally, $\overline{x} * \overline{y} = (\overline{x} \cdot \overline{y}) \cdot h^{-\sigma(1-i+j)} = y^{-1}xh^{-\sigma(1-i+j)} = y^{-1}xh^{\sigma(i-j)} = y^{-1} * x = \overline{x} \circ \overline{y}$.

It remains to show that $(L, *) = M(H, 2)$ for some $H$ whenever $L/S$ is dihedral. We take advantage of [3, Theorem 0]: If $Q$ is a nonassociative Moufang loop such that every minimal generating set of $Q$ contains an involution, then $Q = M(H, 2)$ for some group $H$.

Pick $x \in e\alpha^{1-i} = \alpha^i f$. If $x \in G$ then $\alpha^2 = S$, and $x * x = x \cdot x = 1$. If $x \notin G$ then $x * x = x \cdot x \cdot h^{\sigma(1-i+i)} = 1$. Because $\langle \alpha \rangle$ is a subloop of $(L, *)$, we have just shown that every (minimal) generating set of $(L, *)$ contains an involution. □

We conclude this section with an example generalizing [5].

**Example 9.5.** It is demonstrated in [5] that $D_{2^n}$ can be obtained from $Q_{2^n}$ via the cyclic construction, for $n > 2$. Indeed, if $G = D_{2^n} = \langle a, b \rangle$, then $\langle a \rangle = S \trianglelefteq G$, $G/S \simeq C_2$, $h = a^{2^{n-2}} \in Z(G)$, and $(G, S, a, h)$ satisfies $(\mathcal{C})$. The inverse of $b$ in $(G, *)$ is $hb$, as $b * hb = bhbh = 1$. Thus $a^{2^{n-1}} = 1$, $b * b = bbh = a^{2^{n-2}}$, $(b * a) * (a^{2^{n-2}}b) = ba * a^{2^{n-2}}b = baa^{2^{n-2}}ba^{2^{n-2}} = bab = a^{-1}$, and $(G, *) \simeq Q_{2^n}$ follows. Then, by Lemma 9.2(ii), $L/S = M(D_{2^n}, 2)/S$ is dihedral of order 4, and $(L, S, \beta, \gamma, h)$ satisfies $(\mathcal{D})$, where we can choose $\beta, \gamma$ so that $\alpha = \beta\gamma = G \setminus S$. Proposition 9.4 then yields $(L, *) = M((G, *), 2) \simeq M(Q_{2^n}, 2)$.

## 10. Small Moufang Loops

Both the cyclic and dihedral constructions were studied for small 2-groups. In particular, using computers, the following question was answered positively for groups of order 8, 16 and 32 in [20]: *Given two groups $G$, $H$ of order $n$, is it possible to construct a sequence of groups $G_0 \simeq G$, $G_1, \ldots, G_s \simeq H$ so that $G_{i+1}$ is obtained from $G_i$ by means of the cyclic or the dihedral construction?* The purpose of this section is to study an analogous question for small Moufang loops, not necessarily of order $2^n$.

We will rely heavily on [11], where one finds multiplication tables of all nonassociative Moufang loops of order less than 64; one for each isomorphism type. The book [11] is based on Chein's classification [3].

Following the notational conventions of [11] closely, the $k$th Moufang loop of order $n$ will be denoted by $n/k$. Whenever we refer to a multiplication table of $n/k$, we always mean the one given in [11].

As we have mentioned in the Introduction, the only orders $n \leq 32$ for which there are at least two non-isomorphic nonassociative Moufang loops are $n = 16$, 24, and 32, with 5, 5, and 71 loops, respectively.

For $n = 24$ and $n = 32$, all nonassociative Moufang loops of order $n$ can be split into two subsets according to the size of their associator subloop (or nucleus). Namely,

$$\begin{aligned} A_{24} &= \{24/1,\ 24/3,\ 24/4,\ 24/5\},\\ B_{24} &= \{24/2\},\\ A_{32} &= \{32/1,\ \dots,\ 32/6,\ 32/10,\ \dots, 32/26,\ 32/29,\ 32/30,\\ &\quad\ 32/35,\ 32/36,\ 32/39,\ \dots,\ 32/71\},\\ B_{32} &= \{32/7,\ \dots,\ 32/9,\ 32/27,\ 32/28,\ 32/31,\ \dots,\ 32/34,\ 32/37,\ 32/38\}. \end{aligned}$$

The size of the nucleus and the size of the associator subloop for loops in the subsets $A_i$, $B_i$ are as follows:

| class | size of nucleus | size of associator subloop |
|---|---|---|
| $A_{24}$ | 2 | 3 |
| $B_{24}$ | 1 | 4 |
| $A_{32}$ | 4 | 2 |
| $B_{32}$ | 2 | 4 |

All loops $16/k$, for $1 \le k \le 5$, have associator subloop and nucleus of cardinality 2. Since the associator subloops do not change under our constructions (cf. Theorems 6.3 and 7.3), a loop from set $A_i$ cannot be transformed to a loop from set $B_i$ via any of the two constructions. The striking result is that the converse is also true:

**Theorem 10.1.** *For $n = 16$, 24, 32, let $\mathcal{G}(n)$ be a graph whose vertices are all isomorphism types of nonassociative Moufang loops of order $n$, and where two vertices form an edge if a representative of the second type can be obtained from a representative of the first type by one of the two constructions.* (*Lemmas* 6.1 *and* 7.1 *guarantee that $\mathcal{G}(n)$ is not directed.*) *Then:*

(i) *The graph $\mathcal{G}(16)$ is connected.*
(ii) *There are two connected components in $\mathcal{G}(24)$, namely $A_{24}$ and $B_{24}$.*
(iii) *There are two connected components in $\mathcal{G}(32)$, namely $A_{32}$ and $B_{32}$.*

*In all cases, the connected components correspond to blocks of loops with equivalent associator, and also to blocks of loops that have nucleus of the same size.*

*Proof.* The proof depends on machine computation that, together with detailed information about exhaustive search for edges in $\mathcal{G}(n)$, will be presented elsewhere. Our GAP libraries are available online [10]. □

It is possible to select representatives of each connected component so that they can be described in a uniform way. For instance, select representatives $16/1 = M(D_8, 2)$, $24/1 = M(D_{12}, 2)$, $24/2 = M(A_4, 2)$, $32/1 = M(D_8 \times C_2, 2)$, and $32/7 = M(D_{16}, 2)$. See Section 9 for the definition of loops $M(G, 2)$.

It is certainly of interest that, although the groups $D_{16}$ and $D_8 \times C_2$ are connected, the loops $M(D_{16}, 2) = 32/7$ and $M(D_8 \times C_2, 2) = 32/1$ are not. This, in view of Proposition 9.4, means that the groups $D_{16}$ and $D_8 \times C_2$ cannot be connected via the cyclic construction.

**Example 10.2.** Let us return to code loops. Their multiplication tables are easy to spot thanks to this result of Chein and Goodaire [4, Theorem 5]: *A loop $L$ is a code loop if and only if it is a Moufang loop with $|L^2| \le 2$.* Here, $L^2$ denotes the set of all squares in $L$.

Table 1. Multiplication table of $32/1 = M(D_8 \times C_2,\, 2)$.

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 3 | 4 | 1 | 6 | 7 | 8 | 5 | 10 | 11 | 12 | 9 | 14 | 15 | 16 | 13 | 18 | 19 | 20 | 17 | 24 | 21 | 22 | 23 | 26 | 27 | 28 | 25 | 32 | 29 | 30 | 31 |
| 3 | 4 | 1 | 2 | 7 | 8 | 5 | 6 | 11 | 12 | 9 | 10 | 15 | 16 | 13 | 14 | 19 | 20 | 17 | 18 | 23 | 24 | 21 | 22 | 27 | 28 | 25 | 26 | 31 | 32 | 29 | 30 |
| 4 | 1 | 2 | 3 | 8 | 5 | 6 | 7 | 12 | 9 | 10 | 11 | 16 | 13 | 14 | 15 | 20 | 17 | 18 | 19 | 22 | 23 | 24 | 21 | 28 | 25 | 26 | 27 | 30 | 31 | 32 | 29 |
| 5 | 8 | 7 | 6 | 1 | 4 | 3 | 2 | 13 | 16 | 15 | 14 | 9 | 12 | 11 | 10 | 21 | 22 | 23 | 24 | 17 | 18 | 19 | 20 | 29 | 30 | 31 | 32 | 25 | 26 | 27 | 28 |
| 6 | 5 | 8 | 7 | 2 | 1 | 4 | 3 | 14 | 13 | 16 | 15 | 10 | 9 | 12 | 11 | 22 | 23 | 24 | 21 | 20 | 17 | 18 | 19 | 30 | 31 | 32 | 29 | 28 | 25 | 26 | 27 |
| 7 | 6 | 5 | 8 | 3 | 2 | 1 | 4 | 15 | 14 | 13 | 16 | 11 | 10 | 9 | 12 | 23 | 24 | 21 | 22 | 19 | 20 | 17 | 18 | 31 | 32 | 29 | 30 | 27 | 28 | 25 | 26 |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 24 | 21 | 22 | 23 | 18 | 19 | 20 | 17 | 32 | 29 | 30 | 31 | 26 | 27 | 28 | 25 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 10 | 11 | 12 | 9 | 14 | 15 | 16 | 13 | 2 | 3 | 4 | 1 | 6 | 7 | 8 | 5 | 26 | 27 | 28 | 25 | 32 | 29 | 30 | 31 | 18 | 19 | 20 | 17 | 24 | 21 | 22 | 23 |
| 11 | 12 | 9 | 10 | 15 | 16 | 13 | 14 | 3 | 4 | 1 | 2 | 7 | 8 | 5 | 6 | 27 | 28 | 25 | 26 | 31 | 32 | 29 | 30 | 19 | 20 | 17 | 18 | 23 | 24 | 21 | 22 |
| 12 | 9 | 10 | 11 | 16 | 13 | 14 | 15 | 4 | 1 | 2 | 3 | 8 | 5 | 6 | 7 | 28 | 25 | 26 | 27 | 30 | 31 | 32 | 29 | 20 | 17 | 18 | 19 | 22 | 23 | 24 | 21 |
| 13 | 16 | 15 | 14 | 9 | 12 | 11 | 10 | 5 | 8 | 7 | 6 | 1 | 4 | 3 | 2 | 29 | 30 | 31 | 32 | 25 | 26 | 27 | 28 | 21 | 22 | 23 | 24 | 17 | 18 | 19 | 20 |
| 14 | 13 | 16 | 15 | 10 | 9 | 12 | 11 | 6 | 5 | 8 | 7 | 2 | 1 | 4 | 3 | 30 | 31 | 32 | 29 | 28 | 25 | 26 | 27 | 22 | 23 | 24 | 21 | 20 | 17 | 18 | 19 |
| 15 | 14 | 13 | 16 | 11 | 10 | 9 | 12 | 7 | 6 | 5 | 8 | 3 | 2 | 1 | 4 | 31 | 32 | 29 | 30 | 27 | 28 | 25 | 26 | 23 | 24 | 21 | 22 | 19 | 20 | 17 | 18 |
| 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 32 | 29 | 30 | 31 | 26 | 27 | 28 | 25 | 24 | 21 | 22 | 23 | 18 | 19 | 20 | 17 |
| 17 | 20 | 19 | 18 | 21 | 22 | 23 | 24 | 25 | 28 | 27 | 26 | 29 | 30 | 31 | 32 | 1 | 4 | 3 | 2 | 5 | 6 | 7 | 8 | 9 | 12 | 11 | 10 | 13 | 14 | 15 | 16 |
| 18 | 17 | 20 | 19 | 22 | 23 | 24 | 21 | 26 | 25 | 28 | 27 | 30 | 31 | 32 | 29 | 2 | 1 | 4 | 3 | 8 | 5 | 6 | 7 | 10 | 9 | 12 | 11 | 16 | 13 | 14 | 15 |
| 19 | 18 | 17 | 20 | 23 | 24 | 21 | 22 | 27 | 26 | 25 | 28 | 31 | 32 | 29 | 30 | 3 | 2 | 1 | 4 | 7 | 8 | 5 | 6 | 11 | 10 | 9 | 12 | 15 | 16 | 13 | 14 |
| 20 | 19 | 18 | 17 | 24 | 21 | 22 | 23 | 28 | 27 | 26 | 25 | 32 | 29 | 30 | 31 | 4 | 3 | 2 | 1 | 6 | 7 | 8 | 5 | 12 | 11 | 10 | 9 | 14 | 15 | 16 | 13 |
| 21 | 22 | 23 | 24 | 17 | 20 | 19 | 18 | 29 | 30 | 31 | 32 | 25 | 28 | 27 | 26 | 5 | 8 | 7 | 6 | 1 | 2 | 3 | 4 | 13 | 16 | 15 | 14 | 9 | 10 | 11 | 12 |
| 22 | 23 | 24 | 21 | 18 | 17 | 20 | 19 | 30 | 31 | 32 | 29 | 26 | 25 | 28 | 27 | 6 | 5 | 8 | 7 | 4 | 1 | 2 | 3 | 14 | 13 | 16 | 15 | 12 | 9 | 10 | 11 |
| 23 | 24 | 21 | 22 | 19 | 18 | 17 | 20 | 31 | 32 | 29 | 30 | 27 | 26 | 25 | 28 | 7 | 6 | 5 | 8 | 3 | 4 | 1 | 2 | 15 | 14 | 13 | 16 | 11 | 12 | 9 | 10 |
| 24 | 21 | 22 | 23 | 20 | 19 | 18 | 17 | 32 | 29 | 30 | 31 | 28 | 27 | 26 | 25 | 8 | 7 | 6 | 5 | 2 | 3 | 4 | 1 | 16 | 15 | 14 | 13 | 10 | 11 | 12 | 9 |
| 25 | 28 | 27 | 26 | 29 | 30 | 31 | 32 | 17 | 20 | 19 | 18 | 21 | 22 | 23 | 24 | 9 | 12 | 11 | 10 | 13 | 14 | 15 | 16 | 1 | 4 | 3 | 2 | 5 | 6 | 7 | 8 |
| 26 | 25 | 28 | 27 | 30 | 31 | 32 | 29 | 18 | 17 | 20 | 19 | 22 | 23 | 24 | 21 | 10 | 9 | 12 | 11 | 16 | 13 | 14 | 15 | 2 | 1 | 4 | 3 | 8 | 5 | 6 | 7 |
| 27 | 26 | 25 | 28 | 31 | 32 | 29 | 30 | 19 | 18 | 17 | 20 | 23 | 24 | 21 | 22 | 11 | 10 | 9 | 12 | 15 | 16 | 13 | 14 | 3 | 2 | 1 | 4 | 7 | 8 | 5 | 6 |
| 28 | 27 | 26 | 25 | 32 | 29 | 30 | 31 | 20 | 19 | 18 | 17 | 24 | 21 | 22 | 23 | 12 | 11 | 10 | 9 | 14 | 15 | 16 | 13 | 4 | 3 | 2 | 1 | 6 | 7 | 8 | 5 |
| 29 | 30 | 31 | 32 | 25 | 28 | 27 | 26 | 21 | 22 | 23 | 24 | 17 | 20 | 19 | 18 | 13 | 16 | 15 | 14 | 9 | 10 | 11 | 12 | 5 | 8 | 7 | 6 | 1 | 2 | 3 | 4 |
| 30 | 31 | 32 | 29 | 26 | 25 | 28 | 27 | 22 | 23 | 24 | 21 | 18 | 17 | 20 | 19 | 14 | 13 | 16 | 15 | 12 | 9 | 10 | 11 | 6 | 5 | 8 | 7 | 4 | 1 | 2 | 3 |
| 31 | 32 | 29 | 30 | 27 | 26 | 25 | 28 | 23 | 24 | 21 | 22 | 19 | 18 | 17 | 20 | 15 | 14 | 13 | 16 | 11 | 12 | 9 | 10 | 7 | 6 | 5 | 8 | 3 | 4 | 1 | 2 |
| 32 | 29 | 30 | 31 | 28 | 27 | 26 | 25 | 24 | 21 | 22 | 23 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 10 | 11 | 12 | 9 | 8 | 7 | 6 | 5 | 2 | 3 | 4 | 1 |

All loops $16/k$, $1 \leq k \leq 5$, are code loops with trivial radical (i.e., with nucleus of cardinality 2). In view of Proposition 8.7 and Theorem 10.1, it suffices to establish this just for one loop $16/k$; for example, the octonion loop of order 16 is a code loop.

The loops $32/k$ are code loops for $k \in \{1, \ldots, 3, 10, \ldots, 22\}$, all with nontrivial radical. Markedly, it is possible to obtain a code loop from a loop that is not code. Consider the loops $32/1 = M(D_8 \times C_2, 2)$ (its multiplication table is given in Table 1), and the loop $32/4 = M(16\Gamma_2 c_1, 2)$ (its multiplication table is given in Table 2). The group $16\Gamma_2 c_1$ has presentation $\langle a, b;\ a^4 = b^4 = (ab)^2 = [a^2, b] = 1\rangle$. The loop 32/1 is a code loop, while the loop 32/4 is not, by the result of Chein and Goodaire. They are connected, however, by Theorem 10.1.

## 11. Conjectures and Prospects

Recall that given two Moufang loops (or groupoids) $(G, \circ)$, $(G, *)$ defined on the same set $G$, their *distance* $d(\circ, *)$ is the cardinality of the set $\{(a, b) \in G \times G;\ a \circ b \neq a * b\}$.

Assume that $(G, *)$ is constructed from the Moufang loop $(G, \circ)$ via one of the constructions. Then, as we hinted on in the title, $d(\circ, *) = n^2/4$, where $n = |G|$. We conjecture that, similarly as for groups, this is the smallest possible distance:

**Conjecture 11.1.** *Every two Moufang 2-loops of order $n$ in distance less than $n^2/4$ are isomorphic.*

Since $A(G, *) = A(G, \circ)$ if $(\mathcal{C})$ or $(\mathcal{D})$ is satisfied, we wonder what is the minimum distance of two Moufang loops with nonequivalent associator.

**Conjecture 11.2.** *Two Moufang loops of order $n$ with nonequivalent associator are in distance at least $3n^2/8$.*

TABLE 2. Multiplication tables of $32/4 = M(16\Gamma_2 c_1,\, 2)$ and $32/7 = M(D_{16},\, 2)$.

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 3 | 4 | [1] | 6 | 7 | 8 | [5] | 10 | 11 | 12 | [9] | 14 | 15 | 16 | [13] | 18 | 19 | 20 | [17] | 22 | 23 | 24 | [21] | [32] | 29 | 30 | 31 | [28] | 25 | 26 | 27 |
| 3 | 4 | [1] | [2] | 7 | 8 | [5] | [6] | 11 | 12 | [9] | [10] | 15 | 16 | [13] | [14] | 19 | 20 | [17] | [18] | 23 | 24 | [21] | [22] | [27] | [28] | 25 | 26 | [31] | [32] | 29 | 30 |
| 4 | [1] | [2] | [3] | 8 | [5] | [6] | [7] | 12 | [9] | [10] | [11] | 16 | [13] | [14] | [15] | 20 | [17] | [18] | [19] | 24 | [21] | [22] | [23] | [30] | [31] | [32] | 29 | [26] | [27] | [28] | 25 |
| 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 13 | 14 | 15 | 16 | 9 | 10 | 11 | 12 | 21 | 22 | 23 | 24 | 17 | 18 | 19 | 20 | 29 | 30 | 31 | 32 | 25 | 26 | 27 | 28 |
| 6 | 7 | 8 | [5] | 2 | 3 | 4 | [1] | 14 | 15 | 16 | [13] | 10 | 11 | 12 | [9] | 22 | 23 | 24 | [21] | 18 | 19 | 20 | [17] | [28] | 25 | 26 | 27 | [32] | 29 | 30 | 31 |
| 7 | 8 | [5] | [6] | 3 | 4 | [1] | [2] | 15 | 16 | [13] | [14] | 11 | 12 | [9] | [10] | 23 | 24 | [21] | [22] | 19 | 20 | [17] | [18] | [31] | [32] | 29 | 30 | [27] | [28] | 25 | 26 |
| 8 | [5] | [6] | [7] | 4 | [1] | [2] | [3] | 16 | [13] | [14] | [15] | 12 | [9] | [10] | [11] | 24 | [21] | [22] | [23] | 20 | [17] | [18] | [19] | [26] | [27] | [28] | 25 | [30] | [31] | [32] | 29 |
| 9 | [16] | [11] | [14] | 13 | [12] | [15] | [10] | 1 | [8] | [3] | [6] | 5 | [4] | [7] | [2] | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 10 | 13 | [12] | [15] | 14 | 9 | [16] | [11] | 2 | 5 | [4] | [7] | 6 | 1 | [8] | [3] | 26 | 27 | 28 | [25] | 30 | 31 | 32 | [29] | [24] | 21 | 22 | 23 | [20] | 17 | 18 | 19 |
| 11 | 14 | 9 | [16] | 15 | 10 | 13 | [12] | 3 | 6 | 1 | [8] | 7 | 2 | 5 | [4] | 27 | 28 | [25] | [26] | 31 | 32 | [29] | [30] | [19] | [20] | 17 | 18 | [23] | [24] | 21 | 22 |
| 12 | 15 | 10 | 13 | 16 | 11 | 14 | 9 | 4 | 7 | 2 | 5 | 8 | 3 | 6 | 1 | 28 | [25] | [26] | [27] | 32 | [29] | [30] | [31] | [22] | [23] | [24] | 21 | [18] | [19] | [20] | 17 |
| 13 | [12] | [15] | [10] | 9 | [16] | [11] | [14] | 5 | [4] | [7] | [2] | 1 | [8] | [3] | [6] | 29 | 30 | 31 | 32 | 25 | 26 | 27 | 28 | 21 | 22 | 23 | 24 | 17 | 18 | 19 | 20 |
| 14 | 9 | [16] | [11] | 10 | 13 | [12] | [15] | 6 | 1 | [8] | [3] | 2 | 5 | [4] | [7] | 30 | 31 | 32 | [29] | 26 | 27 | 28 | [25] | [20] | 17 | 18 | 19 | [24] | 21 | 22 | 23 |
| 15 | 10 | 13 | [12] | 11 | 14 | 9 | [16] | 7 | 2 | 5 | [4] | 3 | 6 | 1 | [8] | 31 | 32 | [29] | [30] | 27 | 28 | [25] | [26] | [23] | [24] | 21 | 22 | [19] | [20] | 17 | 18 |
| 16 | 11 | 14 | 9 | 12 | 15 | 10 | 13 | 8 | 3 | 6 | 1 | 4 | 7 | 2 | 5 | 32 | [29] | [30] | [31] | 28 | [25] | [26] | [27] | [18] | [19] | [20] | 17 | [22] | [23] | [24] | 21 |
| 17 | [20] | [19] | [18] | 21 | [24] | [23] | [22] | 25 | 30 | 27 | 32 | 29 | 26 | 31 | 28 | 1 | [4] | [3] | [2] | 5 | [8] | [7] | [6] | 9 | 14 | 11 | 16 | 13 | 10 | 15 | 12 |
| 18 | 17 | [20] | [19] | 22 | 21 | [24] | [23] | 26 | 31 | 28 | [29] | 30 | 27 | 32 | [25] | 2 | 1 | [4] | [3] | 6 | 5 | [8] | [7] | [16] | 9 | 14 | 11 | [12] | 13 | 10 | 15 |
| 19 | 18 | 17 | [20] | 23 | 22 | 21 | [24] | 27 | 32 | [25] | [30] | 31 | 28 | [29] | [26] | 3 | 2 | 1 | [4] | 7 | 6 | 5 | [8] | [11] | [16] | 9 | 14 | [15] | [12] | 13 | 10 |
| 20 | 19 | 18 | 17 | 24 | 23 | 22 | 21 | 28 | [29] | [26] | [31] | 32 | [25] | [30] | [27] | 4 | 3 | 2 | 1 | 8 | 7 | 6 | 5 | [14] | [11] | [16] | 9 | [10] | [15] | [12] | 13 |
| 21 | [24] | [23] | [22] | 17 | [20] | [19] | [18] | 29 | 26 | 31 | 28 | 25 | 30 | 27 | 32 | 5 | [8] | [7] | [6] | 1 | [4] | [3] | [2] | 13 | 10 | 15 | 12 | 9 | 14 | 11 | 16 |
| 22 | 21 | [24] | [23] | 18 | 17 | [20] | [19] | 30 | 27 | 32 | [25] | 26 | 31 | 28 | [29] | 6 | 5 | [8] | [7] | 2 | 1 | [4] | [3] | [12] | 13 | 10 | 15 | [16] | 9 | 14 | 11 |
| 23 | 22 | 21 | [24] | 19 | 18 | 17 | [20] | 31 | 28 | [29] | [26] | 27 | 32 | [25] | [30] | 7 | 6 | 5 | [8] | 3 | 2 | 1 | [4] | [15] | [12] | 13 | 10 | [11] | [16] | 9 | 14 |
| 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 32 | [25] | [30] | [27] | 28 | [29] | [26] | [31] | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | [10] | [15] | [12] | 13 | [14] | [11] | [16] | 9 |
| 25 | 30 | 27 | 32 | 29 | 26 | 31 | 28 | 17 | [20] | [19] | [18] | 21 | [24] | [23] | [22] | 9 | [12] | [11] | [10] | 13 | [16] | [15] | [14] | 1 | 6 | 3 | 8 | 5 | 2 | 7 | 4 |
| 26 | 31 | 28 | [29] | 30 | 27 | 32 | [25] | 18 | 17 | [20] | [19] | 22 | 21 | [24] | [23] | 10 | 9 | [12] | [11] | 14 | 13 | [16] | [15] | [8] | 1 | 6 | 3 | [4] | 5 | 2 | 7 |
| 27 | 32 | [25] | [30] | 31 | 28 | [29] | [26] | 19 | 18 | 17 | [20] | 23 | 22 | 21 | [24] | 11 | 10 | 9 | [12] | 15 | 14 | 13 | [16] | [3] | [8] | 1 | 6 | [7] | [4] | 5 | 2 |
| 28 | [29] | [26] | [31] | 32 | [25] | [30] | [27] | 20 | 19 | 18 | 17 | 24 | 23 | 22 | 21 | 12 | 11 | 10 | 9 | 16 | 15 | 14 | 13 | [6] | [3] | [8] | 1 | [2] | [7] | [4] | 5 |
| 29 | 26 | 31 | 28 | 25 | 30 | 27 | 32 | 21 | [24] | [23] | [22] | 17 | [20] | [19] | [18] | 13 | [16] | [15] | [14] | 9 | [12] | [11] | [10] | 5 | 2 | 7 | 4 | 1 | 6 | 3 | 8 |
| 30 | 27 | 32 | [25] | 26 | 31 | 28 | [29] | 22 | 21 | [24] | [23] | 18 | 17 | [20] | [19] | 14 | 13 | [16] | [15] | 10 | 9 | [12] | [11] | [4] | 5 | 2 | 7 | [8] | 1 | 6 | 3 |
| 31 | 28 | [29] | [26] | 27 | 32 | [25] | [30] | 23 | 22 | 21 | [24] | 19 | 18 | 17 | [20] | 15 | 14 | 13 | [16] | 11 | 10 | 9 | [12] | [7] | [4] | 5 | 2 | [3] | [8] | 1 | 6 |
| 32 | [25] | [30] | [27] | 28 | [29] | [26] | [31] | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | [2] | [7] | [4] | 5 | [6] | [3] | [8] | 1 |

This is illustrated in Table 2 for $n = 32$, where one can find multiplication tables of $32/4 = M(16\Gamma_2 c_1,\, 2)$ and $32/7 = M(D_{16},\, 2)$ the way they are listed in [11]. To obtain the multiplication table for 32/7, permute the $8 \cdot 8 = 64$ framed triangular regions by switching region $(2k, j)$ with region $(2k+1, j)$, for $k = 0, \ldots, 3$, $j = 0, \ldots, 7$.

This does not mean that two loops with nonequivalent associator cannot be closer. In fact, if a group multiplication table contains a subsquare

$$\begin{matrix} a & b \\ b & a \end{matrix} \tag{21}$$

and if the group is sufficiently large ($n \geq 6$), then the loop obtained by switching $a$ and $b$ in (21) cannot be associative.

We conclude the paper with a few suggestions for future research:

1. Decide whether two Moufang loops $M_0$, $M_s$ of order $n$ with equivalent associator can be connected by a series of Moufang loops $M_0, M_1, \ldots, M_s$ so that the distance of $M_{i+1}$ from $M_i$ is $n^2/4$, for $i = 0, \ldots, s-1$. (Note that additional constructions are needed already for $n = 64$.)
2. The main result of [9] says that when the parameters of any of the constructions are varied in a certain way, the isomorphism type of the resulting group will not be affected. Can this be generalized to Moufang loops? (See [18] for a step in this direction.)
3. Is there a general construction that preserves three quarters of the multiplication table yet yields a Moufang loop with nonequivalent associator?
4. This paper attempts to launch a new approach to Moufang 2-loops, by obtaining them using group-theoretical constructions. One can envision a similar programme for Bol loops modulo Moufang loops, for instance.

5. While this paper was under review, one of the authors has determined by computer search that there are 4262 nonassociative Moufang loops of order 64 that can be obtained from loops $M(G, 2)$ by the two constructions, where $G$ is a nonabelian group of order 32. See [18] for more details. Are there other nonassociative Moufang loops of order 64?

## 12. Acknowledgement

We would like to thank Edgar G. Goodaire for providing us with electronic files containing multiplication tables of all nonassociative Moufang loops of order at most 32. We also thank the referee for many useful comments that resulted in an improved exposition of the material.

## References

[1] Michael Aschbacher, *Sporadic groups*, Cambridge Tracts in Mathematics **104**. Cambridge University Press, Cambridge, 1994.
[2] M. Bálek, A. Drápal, and N. Zhukavets, *The neighbourhood of dihedral 2-groups*, submitted.
[3] Orin Chein, *Moufang loops of small order*, Memoirs of the American Mathematical Society, Volume **13**, Issue 1, Number **197** (1978).
[4] Orin Chein and Edgar G. Goodaire, *Moufang loops with a Unique Nonidentity Commutator (Associator, Square)*, J. Algebra **130** (1990), 369–384.
[5] Diane Donovan, Sheila Oates-Williams, Cheryl Praeger, *On the distance between distinct group Latin squares*, J. Combin. Des. 5 (1997), no. 4, 235–248.
[6] Aleš Drápal, *Non-isomorphic 2-groups coincide at most in three quarters of their multiplication tables*, European J. Combin. **21** (2000), 301–321.
[7] Aleš Drápal, *On groups that differ in one of four squares*, European J. Combin. **23** (2002), 899–918.
[8] Aleš Drápal, *Cyclic and dihedral constructions of even order*, Comment. Math. Univ. Carolinae **44**, **4** (2003), 593–614.
[9] Aleš Drápal and Natalia Zhukavets, *On multiplication tables of groups that agree on half of columns and half of rows*, Glasgow Mathematical Journal **45** (2003), 293–308.
[10] 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). The GAP libraries specific to this paper are available at http://www.math.du.edu/~petr in section research | computing.
[11] Edgar G. Goodaire, Sean May, Maitreyi Raman, *The Moufang Loops of Order less than 64*, Nova Science Publishers, 1999.
[12] Robert L. Griess, Jr., *Code Loops*, J. Algebra **100** (1986), 224–234.
[13] Tim Hsu, *Moufang loops of class 2 and cubic forms*, Math. Proc. Cambridge Philos. Soc. **128** (2000), 197–222.
[14] Hala O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.
[15] Derek J. S. Robinson, A course in the Theory of Groups, second edition, *Graduate Texts in Mathematics* **80**, Springer, 1996.
[16] Petr Vojtěchovský, *Finite Simple Moufang Loops*, Ph.D. thesis, Iowa State University, 2001.

[17] Petr Vojtěchovský, *Term formulas for the cyclic and dihedral constructions*, an alternative proof, available at http://www.math.du.edu/~petr in section research | publications.
[18] Petr Vojtěchovský, *Toward the classification of Moufang loops of order* 64, submitted.
[19] Harold N. Ward, *Combinatorial Polarization*, Discrete Mathematics **26** (1979), 186–197.
[20] Natalia Zhukavets, *On small distances between small* 2*-groups*, Comment. Math. Univ. Carolinae **42** (2001), no. 2, 247–257.

*E-mail address*: drapal@karlin.mff.cuni.cz

Department of Algebra, Charles University, Sokolovská 83, 186 75 Prague, Czech Republic

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

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO 80208, USA