Nonsplitting F-quasigroups

Stephen Gagola III

Abstract. T. Kepka, M.K. Kinyon and J.D. Phillips [*The structure of F-quasigroups*, J. Algebra **317** (2007), no. 2, 435–461] developed a connection between F-quasigroups and NK-loops. Since NK-loops are contained in the variety generated by groups and commutative Moufang loops, a question that arises is whether or not there exists a nonsplit NK-loop and likewise a nonsplit F-quasigroup. Here we prove that there do indeed exist nonsplit F-quasigroups and show that there are exactly four corresponding nonsplit NK-loops of minimal order 3^6.

Keywords: F-quasigroup, NK-loop, Moufang loop

Classification: Primary 20E10; Secondary 20N05

1. Introduction

A quasigroup $(Q,\cdot)$ is a nonempty set Q together with a binary operation such that the equation $x\cdot y=z$ has a unique solution in Q whenever two of the three elements $x,y,z\in Q$ are given. An element e_x of a quasigroup Q is called the right local identity for $x\in Q$ if $xe_x=x$. Similarly, if $f_x x=x$ for $f_x\in Q$ then f_x is called the left local identity for $x\in Q$.

A quasigroup Q is called an *F-quasigroup* if

$$x(yz)=(xy)(e_x z)$$
$$(yz)x=(yf_x)(zx)$$

are satisfied for all $x,y,z\in Q$ where e_x and f_x are the right and left local identities of x respectively. F-quasigroups were first studied by D.C. Murdoch [10] back in 1939. It was then V.D. Belousov [1] who first called these quasigroups 'F-quasigroups' as he showed that a distributive quasigroup is isotopic to a commutative Moufang loop. V.D. Belousov also noted that an F-quasigroup is a quasigroup in which the solutions x and y of the equations

$$a(bx)=(ab)c$$
$$(yb)a=c(ba)$$

depend only on the elements a and b. In this way, F-quasigroups form a nontrivial generalization of groups.

A quasigroup Q is called a *loop* if there exists an identity element $1\in Q$ with $1x=x=x1$ for every $x\in Q$. A *Moufang loop* is a loop that satisfies the following (equivalent) Moufang identities:

$$((xy)x)z = x(y(xz)),$$
$$((zx)y)x = z(x(yx)),$$
$$x((yz)x) = (xy)(zx),$$
$$(x(yz))x = (xy)(zx).$$

Such loops were first introduced by R. Moufang back in 1934. By Moufang's Theorem, if L is a Moufang loop such that $x, y, z \in L$ associate in some order then they associate in any order.

The *nucleus* of a loop L is defined by

$$\mathrm{Nuc}\,(L) = \left\{ a \in L \;\middle|\; \begin{array}{l} a(xy) = (ax)y,\ x(ay) = (xa)y, \\ \text{and } x(ya) = (xy)a \text{ for all } x, y \in L \end{array} \right\}.$$

By Moufang's Theorem, if L is a Moufang loop then

$$\mathrm{Nuc}\,(L) = \{a \in L \mid a(xy) = (ax)y \text{ for all } x, y \in L\}.$$

The *commutant* of a loop L, sometimes called the Moufang center, is the set

$$\mathbf{C}(L) = \{a \in L \mid ax = xa \text{ for all } x \in L\}.$$

In any Moufang loop, both the nucleus and the commutant are normal subloops [4]. The *center* of a loop L, denoted by $Z(L)$, is defined to be the intersection between the nucleus and the commutant.

An *NK-loop* is a loop L such that $L = NK$ where $N = \mathrm{Nuc}\,(L)$ and $K = \mathbf{C}(L)$. It was proven in [8] that every NK-loop is a Moufang loop. Thus any minimal nonassociative NK-loop would be a commutative Moufang loop of order 81. There are exactly two such Moufang loops. The nonassociative commutative Moufang loop of order 81 and exponent 3 was constructed by H. Zassenhaus [2] and the other nonassociative commutative Moufang loop of order 81 with exponent 9 was constructed by T. Kepka and P. Němec [9].

It was T. Kepka, M.K. Kinyon and J.D. Phillips [8] who solved an open problem, proposed by V.D. Belousov in 1967, by developing the following connection between F-quasigroups and NK-loops.

Theorem 1. *A quasigroup $(Q, \cdot)$ is an F-quasigroup if and only if there exists an NK-loop $(Q, +)$ with automorphisms $f, g \in Aut\,(Q, +)$ and an element $e \in Q$ such that the following conditions are satisfied:*

(i) $x + f(x) \in Nuc\,(Q, +)$ *for all* $x \in Q$;
(ii) $-x + f(x) \in \mathbf{C}(Q, +)$ *for all* $x \in Q$;
(iii) $x + g(x) \in Nuc\,(Q, +)$ *for all* $x \in Q$;
(iv) $-x + g(x) \in \mathbf{C}(Q, +)$ *for all* $x \in Q$;
(v) $fg = gf$;
(vi) $x \cdot y = f(x) + e + g(y)$ *for all* $x, y \in Q$.

So from Theorem 1, the class of Moufang loops that can occur as loop isotopes of F-quasigroups are characterized as NK-loops. In [7], Theorem 1 was also used to establish an equivalence between the equational class of (pointed) F-quasigroups and the equational class corresponding to a certain notion of generalized module (with noncommutative, nonassociative addition) for an associative ring.

We say that an F-quasigroup $(Q,\cdot)$ is *split* if its corresponding NK-loop $(Q,+)$ is split and can be written as the direct product between a group and a commutative Moufang loop. Here we not only use Theorem 1 to prove the existence of nonsplit F-quasigroups but also show that there are exactly four NK-loops that can occur as loop isotopes of such F-quasigroups of minimal order. By better understanding NK-loops we reveal more about the structure of F-quasigroups which include distributive Steiner quasigroups and medial quasigroups.

2. Splitting NK-loops

In this section we show that an F-quasigroup is split if and only if it is isotopic to an NK-loop that can be written as the direct product between a group and a loop-isotope of a commutative Moufang loop.

Two quasigroups $(Q_1,\cdot)$ and $(Q_2,\circ)$ are *isotopic* if there are bijections α, β, and γ from Q_1 to Q_2 such that $\alpha(x)\circ\beta(y)=\gamma(x\cdot y)$ for any $x,y\in Q_1$. Here Q_2 is called an *isotope* of Q_1.

If a loop is isotopic to a group then it is actually isomorphic to that group [11]. It should also be noted that every loop-isotope of a Moufang loop is again a Moufang loop.

Let L be a Moufang loop with a fixed element $\kappa\in L$. The *κ-isotope* of L, denoted by $(L,\circ_\kappa)$, is a loop isotopic to L where

$$a\circ_\kappa b=(a\kappa)(\kappa^{-1}b)$$

for any $a,b\in L$. The following is a useful proposition which was originally proven by H.O. Pflugfelder [11].

Proposition 2. *A loop-isotope of a Moufang loop L is isomorphic to a κ-isotope of L.*

Corollary 3. *If L is a Moufang loop then the nucleus of any loop-isotope of L is just $Nuc(L)$.*

Theorem 4. *An NK-loop is splitting and therefore the direct product between a group and a commutative Moufang loop if and only if it is a loop-isotope of a splitting NK-loop.*

Proof: Suppose that L is an NK-loop that can be written as the direct product between a group and a loop-isotope, say $(K,\circ_x)$, of a commutative Moufang loop K. In order for L to be an NK-loop, $(K,\circ_x)$ itself must be an NK-loop.

Let C be the commutant of $(K, \circ_x)$. If a is in C then

$$\begin{aligned}(x^{-1}b)(ax) &= (ax)(x^{-1}b)\\ &= a \circ_x b\\ &= b \circ_x a\\ &= (bx)(x^{-1}a)\\ &= (ax^{-1})(xx^{-1}bx)\\ &= (a(x^{-1}b))x\\ &= ((x^{-1}b)a)x\end{aligned}$$

for any $b \in K$. Thus if $a \in C$ then for any $b \in K$ the elements x, a, and b associate in K.

Now let (n_1a_1) and (n_2a_2) be arbitrary elements of K where $n_1, n_2 \in \mathrm{Nuc}\,(K)$ and $a_1, a_2 \in C$. Since

$$\begin{aligned}(x(n_1a_1))(n_2a_2) &= ((x(n_1a_1))n_2)a_2\\ &= (x(n_1a_1n_2))a_2\\ &= x((n_1a_1n_2)a_2)\\ &= x((n_1a_1)(n_2a_2))\end{aligned}$$

x lies in the nucleus of K. Hence, $(K, \circ_x)$ is commutative and L is the direct product between a group and a commutative Moufang loop. □

3. Minimal nonsplit NK-loops

To classify the minimal nonsplit NK-loops we first note that every NK-loop is contained in the variety, say V, generated by all groups and commutative Moufang loops. One can see this from the fact that an NK-loop Q with a nucleus $N = \mathrm{Nuc}\,(Q)$ and a commutant $K = \mathbf{C}(Q)$ would be isomorphic to the quotient $N \oplus K / \ker(\varphi)$ where φ is the usual map

$$\begin{aligned}\varphi : N \oplus K &\longrightarrow Q,\\ (g, x) &\longmapsto gx.\end{aligned}$$

Theorem 5. *There exist nonsplit NK-loops with an order equal to* 3^6.

Proof: Let K be a nonassociative commutative Moufang loop of order 81 and let $Z(K) = \langle c \rangle$ be its center of order three. Now define L to be the following set:

$$L = \{(x, n, m) \mid x \in K,\ n, m \in \mathbb{Z}_3\}\,.$$

It follows that L together with the binary operation

$$(x, n, m) \cdot (y, k, l) = (c^{nl}xy, n + k, m + l)$$

forms a Moufang loop of order 3^6. Here the nucleus of L is

$$\mathrm{Nuc}\,(L) = \{(a, n, m) \in L \mid a \in Z(K)\}$$

and the commutant of L is

$$\mathbf{C}(L) = \{(x, 0, 0) \in L\}.$$

By definition, L is an NK-loop. Furthermore, L is nonsplit since the nontrivial commutator subgroup of $\mathrm{Nuc}\,(L)$ coincides with the associator subloop of $\mathbf{C}(L)$. □

Let N be a noncommutative group of order 27 with $Z(N) = \langle b \rangle$ and K be a nonassociative commutative Moufang loop of order 81 with $Z(K) = \langle c \rangle$. To picture nonsplit NK-loops of order 3^6 as quotients in the variety V let Q be the quotient $N \oplus K/H$ where $H = \langle (b, c) \rangle \trianglelefteq N \oplus K$. Since there are exactly two noncommutative groups of order 27, one of exponent 3 and one of exponent 9, there are exactly four such Moufang loops, Q. These are in fact the only nonsplit NK-loops of order 3^6 since the commutant must have an order of 81 in order to be nonassociative and the nucleus must have an order of 27 in order to be nonabelian.

Corollary 6. *There exist nonsplit F-quasigroups that have an order equal to* 3^6.

Proof: From Theorem 1, there exists a nonsplit F-quasigroup $(Q, \cdot)$ if there exist automorphisms f and g of a nonsplit NK-loop $(Q, +)$ that satisfy conditions (i)–(v). Here it is enough to show that there exists an automorphism f of the loop $(Q, +)$ that satisfies conditions (i) and (ii) since f commutes with itself. In each of the four nonsplit NK-loops of order 3^6 the commutant, say K, is a commutative nonassociative Moufang loop of order 81 and the nucleus, say N, is a nonabelian group of order 27. Furthermore, $Z(K) = \langle c \rangle = Z(N)$ and is of order three.

From conditions (i) and (ii), f must stabilize both N and K. Note that for any $x \in K$, $x + f(x) \in N \cap K = Z(Q, +)$. Likewise, for any $g \in N$, $-g + f(g) \in N \cap K = Z(Q, +)$. Since $Z(Q, +) = [N, N]$, f must fix all of the elements of $Z(Q, +)$. Hence, if $x, y, z \in K$ are generators of K and $g, h \in N$ are generators of N then the map $f : Q \longrightarrow Q$ defined by

$$\begin{aligned} f(nc + (m_1x + m_2y) &+ m_3z + k_1g + k_2h) \\ &= nc + (m_1x + m_1a_x + m_2y + m_2a_y) + m_3z + m_3a_z \\ &\quad + k_1g + k_1a_g + k_2h + k_2a_h \\ &= m_1a_x + m_2a_y + m_3a_z + k_1a_g + k_2a_h \\ &\quad + nc + (m_1x + m_2y) + m_3z + k_1g + k_2h \end{aligned}$$

forms an automorphism of $(Q, +)$ satisfying conditions (i) and (ii) where a_x, a_y, a_z, a_g, and a_h are any fixed elements of $Z(Q, +)$. □

Lemma 7. *Every finite nonassociative commutative Moufang loop has a nontrivial center with an order divisible by three.*

Proof: Let L be a finite nonassociative commutative Moufang loop. From [3] there exists a group N and a commutative 3-loop K such that $L \cong N \oplus K$. Since L is nonassociative, K is nontrivial. Let $G(K)$ be a minimal triality group corresponding to K. By [5], $G(K)$ is a 3-group. Thus $G(K)$ has a nontrivial center which is also a triality group. By minimality of $G(K)$, the center of $G(K)$ contains nontrivial elements of K otherwise $G(K)/Z(G(K))$ would be a smaller triality group corresponding to K. The elements of $K \cap Z(G(K))$ both commute and associate with all of the elements in K. Hence K, and therefore L, has a nontrivial center with an order divisible by three. □

Theorem 8. *There does not exist a nonsplit NK-loop with an order less than* 3^6.

Proof: Suppose L is a nonsplit NK-loop with an order less than 3^6. Since L is nonsplit, L is both nonabelian and nonassociative. Thus $K = \mathbf{C}(L)$ contains a nonassociative subloop with an order divisible by 81. Thus, if N is the nucleus of L then N has an order less than 27. By Lemma 7, the loop K, and therefore the loop L, has a nontrivial center with an order divisible by three. Thus $N/Z(N)$ has an order less than nine. The only possible nonabelian groups that satisfy these conditions are isomorphic to $S_3 \oplus \mathbb{Z}_3$ or $H \oplus \mathbb{Z}_3$ where H is a nonabelian group of order 8. In each of these cases the associator subloop of K intersects the commutator subgroup of N trivially. Hence, L is isomorphic to either $S_3 \oplus Q$ or $H \oplus Q$ where Q is a nonassociative commutative Moufang loop of order 81. This contradicts the fact that L is a nonsplit NK-loop. □

Corollary 9. *Minimal nonsplit F-quasigroups have an order of* 3^6.

It was shown in [6] that non-medial trimedial quasigroups have a minimal order of 81 with exactly 35 such isomorphism classes. So from Corollary 9 it follows that if $(Q, \cdot)$ is a minimal F-quasigroup that is not trimedial and not isotopic to a group then $(Q, +)$ would have to split into N and K where K is not isotopic to a group and therefore of order 81 and $N \cong S_3$. Thus minimal F-quasigroups that are not trimedial and not isotopic to a group have an order of $2 \cdot 3^5$.

References

[1] Belousov V.D., *About one quasigroup class*, Uchenye Zapiski Beltskogo Gospedinstituta im. A. Russo, **5** (1960), 29–44 (in Russian).

[2] Bol G., *Gewebe und Gruppen*, Math. Ann. **114** (1937), no. 1, 414–431.

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

[4] Gagola S.M. III, *A Moufang loop's commutant*, Proc. Cambridge Phil. Soc. **152** (2012), no. 2, 193–206.

[5] Gagola S.M. III, *The number of Sylow p-subloops in finite Moufang loops*, Comm. Algebra **38** (2010), no. 4, 1436–1448.

[6] Kepka T., Bénéteau L., Lacaze J., *Small finite trimedial quasigroups*, Comm. Algebra **14** (1986), no. 6, 1067–1090.

[7] Kepka T., Kinyon M.K., Phillips J.D., *F-quasigroups and generalized modules*, Comment. Math. Univ. Carolin. **49** (2008), no. 2, 249–257.

[8] Kepka T., Kinyon M.K., Phillips J.D., *The structure of F-quasigroups*, J. Algebra **317** (2007), no. 2, 435–461.
[9] Kepka T., Němec P., *Commutative Moufang loops and distributive groupoids of small orders*, Czechoslovak Math. J. **31 (106)** (1981), no. 4, 633–669.
[10] Murdoch D.C., *Quasi-groups which satisfy certain generalized associative laws*, Amer. J. Math. **61** (1939), 509–522.
[11] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics, 7, Heldermann, Berlin, 1990.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: gagola@karlin.mff.cuni.cz

(*Received* January 25, 2012, *revised* May 10, 2012)