Commentationes Mathematicae Universitatis Carolinae

Tomáš Kepka

A note on the number of associative triples in finite commutative Moufang loops

Commentationes Mathematicae Universitatis Carolinae, Vol. 22 (1981), No. 4, 745--753

Persistent URL: http://dml.cz/dmlcz/106116

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

22,4 (1981)

A NOTE ON THE NUMBER OF ASSOCIATIVE TRIPLES IN FINITE COMMUTATIVE MOUFANG LOOPS

Tomáš KEPKA

Abstract: Let G be a finite non-associative commutative Moufang loop. Then G has at most $313n^3/729$ associative triples of elements.

Key words: Associative triple of elements, commutative Moufang loop.

Classification: 20N05

In the present time, a considerable attention is paid to the theory of commutative Moufang loops (see [1] - [14]). It is well known that these loops are diassociative and locally nilpotent. Moreover, if A is an associative subset of a commutative Moufang loop then the subloop generated by A is a subgroup. Now, it is natural to ask about the maximal possible number of associative triples of elements, a finite non-associative commutative Moufang loop can possess. In this note, we show that $a(G) \le 313n^3/729$ (and hence $a(G) < 43n^3/100$), where a(G) is the number of associative triples in a finite non-associative commutative Moufang loop G of order n. This result is somewhat surprising, especially in connection with the following easy fact: For every even $n \ge 40$, there exists a non-associative commutative loop G of order n such that

$a(G) > 99n^3/100$.

1. Introduction. Let G be a groupoid. We put $A(G) = \{(x,y,z);\ x,y,z \in G,\ x.yz = z\}$ and $a(G) = \text{card } A(G)$.

Let G be a loop, i.e., a groupoid with unique division and a unit element. If G satisfies the identity $xx.yz = xy.xz$ then G is commutative and it is called a commutative Moufang loop (the reader is referred to [5] for details concerning these loops).

For every positive integer n, we shall define a number b(n) as follows: If there exists at least one non-associative commutative Moufang loop of order n then $b(n) = \max a(G)$ where G runs through all non-associative commutative Moufang loops of order n; $b(n) = n^3$ in the remaining cases.

2. Auxiliary results. Let $p \geq 2$ be a prime and $F_p = \{0,1,\dots,p-1\}$ the finite field of integers modulo p. Consider a finitely generated vector space V over F_p and an antisymmetric bilinear form $f: V^2 \to F_p$. Put $n = \dim V$, $\text{Ker } f = \{x \in V;\ f(x,y) = 0 \text{ for all } y \in V\}$ and $z(f) = \text{card } \{(x,y);\ x,y \in V,\ f(x,y) = 0\}$.

2.1. Lemma. (i) If $n = 0$ then $f = 0$.

(ii) If $p \neq 2$ and $n \leq 1$ then $f = 0$.

Proof. Obvious.

2.2. Lemma. Suppose that $p \neq 2$ and $f \neq 0$. Then $2 \leq n$ and $z(f) \leq (p^2 + p - 1).p^{2n-3}$.

Proof. We shall proceed by induction on n. For $n \leq 1$, $f = 0$ and there is nothing to prove. Let $2 \leq n$. Assume first that Ker $f = 0$. For all $0 \neq y \in V$, the mapping $x \to f(x,y)$ is a non-zero linear form. Therefore, $z(f) \leq (p^n - 1)p^{n-1} + p^n = p^{2n-3}.(p^2 + p^{3-n} - p^{2-n})$ and the rest is clear. Now, let Ker $f \neq 0$. There is a subspace W of V such that $V = W +$ Ker f and $W \cap$ Ker $f = 0$. Put $m = \dim W$, $k = \dim$ Ker f and $g = f|W^3$. Then $1 \leq k$, $m < n$, $n = m + k$. For all $x,y \in W$ and $u,v \in$ Ker f, we have $f(x+u,y+v) = f(x,y) = g(x,y)$. Hence $z(f) = z(g).p^{2k}$. Since $f \neq 0$, $g \neq 0$ and $z(g) \leq (p^2 + p - 1).p^{2m-3}$. Consequently, $z(f) \leq (p^2 + p - 1).p^{2n-3}$.

2.3. Lemma. Suppose that $p = 2$ and $f \neq 0$. Then $1 \leq n$ and $z(f) \leq 3.2^{2n-2}$.

Proof. Similar to that of 2.2.

2.4. Lemma. (i) If $p = 2$, $n = 1$ and $f \neq 0$ then $z(f) = 3$.
(ii) If $p \neq 2$, $n = 2$ and $f \neq 0$ then $z(f) = p^3 + p^2 - p$.

Proof. (i) This is clear.

(ii) Let $\{x,y\}$ be a basis of V. For all $a,b,c,d \in F_p$, $f(ax+by,cx+dy) = (ad-bc)f(x,y)$. Since $f \neq 0$, $f(x,y) \neq 0$ and $z(f) = \mathrm{card}\,\{(a,b,c,d);\ ad = bc\}$.

3. Auxiliary results. Let V be a finitely generated vector space over F_p and $f: V^3 \to F_p$ an antisymmetric trilinear form (i.e., $f(x,y,z) = -f(y,x,z) = -f(x,z,y)$). Put $n = \dim V$, Ker $f = \{x \in V;\ f(x,y,z) = 0$ for all $y,z \in V\}$ and $z(f) = \mathrm{card}\,\{(x,y,z);\ f(x,y,z) = 0\}$.

3.1. Lemma. (i) If $n = 0$ then $f = 0$.
(ii) If $p \neq 2$ and $n \leq 2$ then $f = 0$.

Proof. Obvious.

3.2. Lemma. Suppose that $p \neq 2$ and $f \neq 0$. Then $3 \leq n$ and $z(f) \leq (p^5 + p^4 - p^2 - p + 1).p^{3n-6}$.

Proof. We shall proceed by induction on n. For $n \leq 2$, $f = 0$ and there is nothing to prove. Let $3 \leq n$. Assume first that Ker $f = 0$. For every $0 \neq z \in V$, the mapping $(x,y) \longrightarrow$ $\longrightarrow f(x,y,z)$ is a non-zero antisymmetric bilinear form. Hence, by 2.2, $z(f) \leq (p^n - 1)p^{2n-3}.(p^2 + p - 1) + p^{2n} =$ $= p^{3n-6}.(p^5 + p^4 - p^3 - p^{5-n} - p^{4-n} + p^{3-n} + p^{6-n})$ and the rest is clear. Now, let Ker $f \neq 0$. Then we can proceed similarly as in the proof of 2.2.

3.3. Lemma. Suppose that $p = 2$ and $f \neq 0$. Then $1 \leq n$ and $z(f) \leq 7.2^{3n-3}$.

Proof. Similar to that of 3.2.

3.4. Lemma. (i) If $p = 2$, $n = 1$ and $f \neq 0$ then $z(f) = 7$.

(ii) If $p \neq 2$, $n = 3$ and $f \neq 0$ then $z(f) = p^8 + p^7 - p^5 - p^4 + p^3$.

Proof. (i) This is clear.

(ii) Let $\{x,y,z\}$ be a basis of V. For all $a,b,c,d,e,q,r,s,t \in F_p$, $f(ax+by+cz,dx+ey+qz,rx+sy+tz) =$ $= (aet - aqs - bdt + bqr + cds - cer)f(x,y,z)$. Since $f \neq 0$, $f(x,y,z) \neq 0$ and $z(f) = \text{card}\,\{(a,b,c,d,e,q,r,s,t);$ $a(et-qs) + b(qr-dt) + c(ds-er) = 0\}$. Put $A = \{(d,e,q,r,s,t);$ $et \neq qs\}$, $B = \{(d,e,q,r,s,t);\ et = qs,\ qr \neq dt\}$, $C =$ $= \{(d,e,q,r,s,t);\ et = qs,\ qr = dt,\ ds \neq er\}$ and $D =$ $= \{(d,e,q,r,s,t);\ et = qs,\ qr = dt,\ ds = er\}$. Then these sets are pair-wise disjoint and $z(f) = p^2(\text{card}\,A + \text{card}\,B + \text{card}\,C +$ $+ p.\text{card}\,D)$. However, card $A = p^6 - p^5 - p^4 + p^3$, card $B =$ $= p^5 - p^4 - p^3 + p^2$, card $C = p^4 - p^3 - p^2 + p$ and card $D =$

$= p^4 + p^3 - p$.

3.5. Lemma. (i) If $p = 3$, $n = 3$ and $f \neq 0$ then $z(f) =$ $= 8451$.

(ii) If $p = 3$ and $f \neq 0$ then $z(f) \leq 313.3^{3n-6}$.

Proof. Use 3.2 and 3.4.

4. Auxiliary results. Let $p \geq 2$ be a prime. Consider a finite abelian p-group $G(+)$ of order n and an antisymmetric triadditive mapping $f:G(+)^3 \longrightarrow G(+)$ such that $pf(x,y,z) = 0$ and $f(f(x,y,z),u,v) = 0$ for all $x,y,z,u,v \in G$. Put Ker $f =$ $= \{x \in G;\ f(x,y,z) = 0$ for all $y,z \in G\}$ and $z(f) = \operatorname{card}\{(x,y,z);\ x,y,z \in G,\ f(x,y,z) = 0\}$.

The group $G(+)$ is a direct sum of non-zero cyclic groups, say $G(+) = G_1(+) + \ldots + G_m(+)$, $0 \leq m$.

4.1. Lemma. Suppose that $p \neq 2$ and $f \neq 0$. Then $3 \leq m$ and $z(f) \leq (p^5 + p^4 - p^2 - p + 1)p^{-6}.n^3$.

Proof. Obviously, $3 \leq m$. Further, we shall proceed by induction on n.

(i) Suppose that Ker f contains a non-zero subgroup $H(+)$ such that $f(G^3) \nsubseteq H$. Put $K(+) = G(+)/H(+)$, $r = \operatorname{card} K$, $s = \operatorname{card} H$. Then $n = rs$, $r < n$ and there are $x_1, \ldots, x_r \in G$ such that $G = (x_1 + H) \cup \ldots \cup (x_r + H)$. Since $H \subseteq$ Ker f, f induces in a natural way an antisymmetric triadditive mapping $g:$ $:K(+)^3 \longrightarrow K(+)$. We have $g \neq 0$, since $f(G^3) \nsubseteq H$, and so $z(g) \leq$ $\leq (p^5 + p^4 - p^2 - p + 1)p^{-6}.r^3$ by the induction hypothesis. On the other hand, $f(x_i+u, x_j+v, x_k+w) = f(x_i, x_j, x_k)$ for all $1 \leq i,j,k \leq r$ and $u,v,w \in H$. Hence $z(f) \leq z(g)s^3$.

(ii) Suppose that $f(G^3)$ is contained in every non-zero subgroup of Ker f. Then $f(G^3)$ is a p-element group. Put $K(+) = G(+)/pG$. Since $pG \subseteq \mathrm{Ker}\, f$, f induces in a natural way an antisymmetric triadditive mapping $g: K(+)^3 \longrightarrow f(G^3)$. Moreover, $g \neq 0$ and $z(g) \leq (p^5 + p^4 - p^2 - p + 1)p^{-6} \cdot r^3$ where r = card K (use 3.2). The rest is clear.

4.2. Lemma. Suppose that p = 2 and $f \neq 0$. Then $1 \leq m$ and $z(f) \leq 7n^3/8$.

Proof. Similar to that of 4.1.

4.3. Lemma. Suppose that p = 3 and $f \neq 0$. Then $z(f) \leq 313n^3/729$.

Proof. Use 4.1.

5. <u>Main results</u>. Let G be a commutative Moufang loop. We denote by C(G) the centre of G and put $[a,b,c] = (ab.c)(a.bc)^{-1}$ for all $a,b,c \in G$.

5.1. Proposition. Let G be a finite commutative Moufang loop of order n. Then:

(i) G is centrally nilpotent.

(ii) G is a group, provided n is not divisible by 81.

(iii) G is a direct sum of p-loops for some primes p.

Proof. See [5].

5.2. Lemma. Let G be a finite commutative Moufang loop of order n and K a subloop of C(G). Put H = G/K, m = card H and r = card K. Then mr = n and $a(G) \leq r^3.a(H)$.

Proof. There are $x_1, \ldots, x_m \in G$ such that $x_1K \cup \ldots \cup x_mK = G$. Let $(x_iu, x_jv, x_kw) \in A(G)$, $1 \leq i,j,k \leq m$, $u,v,w \in K$. Since $K \subseteq C(G)$, $(x_i, x_j, x_k) \in A(G)$ and $(x_iK, x_jK, x_kK) \in A(H)$. The inequality $a(G) \leq r^3 . a(H)$ is now clear.

5.3. Lemma. Let G be a finite non-associative commutative Moufang loop of order n. Then n is divisible by 81 and $a(G) \leq 313n^3/729$.

Proof. We shall proceed by induction on n. By 5.1(ii), n is divisible by 81. By 5.1(iii), there are $m \geq 1$, prime numbers $p_1,\dots,p_m$ and non-trivial subloops $G_1,\dots,G_m$ of G such that $p_1 = 3$, G_i is a p_i-loop for every i and G is the direct sum of these subloops. Then G_1 is not associative, $G_2,\dots,G_m$ are groups and $a(G) = a(G_1).n_2^3 \dots n_m^3$, n_i = card G_i. If $2 \leq m$, then $n_1 < n$, $a(G_1) \leq 313n_1^3/729$ and $a(G) \leq 313n^3/729$. Hence, we can assume that m = 1 and G is a 3-loop. If G/C(G) is not associative then $3 \leq r$ = card C(G), card $G/C(G) < n$, $a(G/C(G)) \leq$ $\leq 313n^3/729r^3$ and $a(G) \leq 313n^3/729$ by 5.2. Consequently, we can assume that G is a 3-loop nilpotent of class 2. By [9], there are an abelian 3-group G(+) and a triadditive mapping $f:G(+)^3 \to G(+)$ such that $3f(x,y,z) = 0$, $f(x,y,z) = -f(y,x,z)$, $f(f(x,y,z),u,v) = 0 = f(u,v,f(x,y,z))$ and $xy = x + y +$ $+ f(x,y,x-y)$ for all $x,y,z,u,v \in G$. It is easy to check that $[a,b,c] = g(a,b,c) = f(a,b,c) + f(b,c,a) + f(c,a,b)$ for all $a,b,c \in G$. The mapping g is an antisymmetric triadditive mapping and $3g(x,y,z) = g(g(x,y,z),u,v) = 0$ for all $x,y,z,u,v \in G$. Since G is not associative, $g \neq 0$. By 4.3, $z(g) \leq 313n^3/729$. However, $z(g) = a(G)$.

5.4. Lemma. Let n be a positive integer divisible by 81. Then there exists a commutative Moufang loop G of order n such that G is nilpotent of class 2 and $a(G) = 313n^3/729$.

Proof. Put $H(+) = F_3^4$, $f(x,y,z) = (0,0,0,(x_1y_2-x_2y_1)z_3)$,

$g(x,y,z) = f(x,y,z) + f(y,z,x) + f(z,y,x)$ and $x * y = x + y + f(x,y,x-y)$ for all $x = (x_i)$, $y = (y_i)$ and $z = (z_i)$ from H. Then $H(*)$ is a commutative Moufang loop of order 81 and $a(H(*)) = z(g)$. But $z(g) = 313.81^3/729$ by 3.5. Now, let $K(+)$ be an abelian group of order $n/81$ and $G = H(*) \times K(+)$. Then G is a commutative Moufang loop of order n and $a(G) = 313n^3/729$.

5.5. Theorem. (i) $b(n) = n^3$ for every positive integer n not divisible by 81.

(ii) $b(n) = 313n^3/729$ for every integer $n \geq 81$ divisible by 81.

Proof. Apply 5.1(ii), 5.3 and 5.4.

R e f e r e n c e s

[1] L. BENETEAU: Une classe particulière de matroides parfaits, Ann. Discr. Math. 8(1980), 229- 232.

[2] L. BENETEAU: Free commutative Moufang loops and anticommutative gradede rings, J. Alg. 67(1980), 1-35.

[3] L. BENETEAU, J. LACARE: Groupes d´automorphismes des boucles de Moufang commutatives, Europ. J. Comb. 1 (1980), 299-309.

[4] G. BOL: Gewebe und Gruppen, Math. Ann. 114(1937), 414-431.

[5] R.H. BRUCK: A survey of binary systems, Springer Verlag 1971.

[6] R.H. BRUCK: An open question concerning Moufang loops, Arch. Math. 10(1959), 419-421.

[7] M. DEZA: Finite commutative Moufang loops, related matroids and association schemes, Proc. Conf. Comb., Arcata, California 1979, 3-15.

[8] T. EVANS: Identities and relations in commutative Moufang

loops, J. Alg. 31(1974), 508-513.

[9] T. KEPKA, P. NĚMEC: Commutative Moufang loops and distributive groupoids of small orders (to appear).

[10] K. KOZIOL: The extensions of commutative Moufang loops of period 3, Pr. Nauk. Uniw. Slask. Pr. Mat. 10(1979), 86-93.

[11] R. ROTH, D.K. RAY-CHAUDHURI: Commutative Moufang 3-loops, Not. Amer. Math. Soc. 84(1978).

[12] A.F. RUSSU: O mnogoobrazijach porožděnych konečnoj komutativnoj lupoj Mufang, Mat. Issled. 51(1979), 120-129.

[13] I.I. SANDU: O složnych associatorach komutativnoj lupy Mufang, Mat. Issled. 51(1979), 130-144.

[14] J.D.H. SMITH: Exterior algebra representations of commutative Moufang loops, Arch. Math. 34(1980), 393-398.

Matematicko-fyzikální fakulta, Universita Karlova, Sokolovská 83, 18600 Praha 8, Československo

(Oblatum 29.1. 1981)