Commentationes Mathematicae Universitatis Carolinae

Aleš Drápal; Tomáš Kepka

A note on the number of associative triples in quasigroups isotopic to groups

Commentationes Mathematicae Universitatis Carolinae, Vol. 22 (1981), No. 4, 735--743

Persistent URL: http://dml.cz/dmlcz/106115

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

22,4 (1981)

A NOTE ON THE NUMBER OF ASSOCIATIVE TRIPLES IN QUASIGROUPS ISOTOPIC TO GROUPS

Aleš DRÁPAL, Tomáš KEPKA

Abstract: Let G be a finite non-associative quasigroup of order n isotopic to a group. Denote by a(G) the number of associative triples of elements of G. Then $a(G) \leq n^3 - 4n^2 + 6n$, provided $n \geq 3$ is odd, and $a(G) \leq n^3 - 4n^2 + 8n$, provided n is even.

Key words: Associative triple, quasigroup, isotopy.

Classification: 20N05

In the past, some problems concerning associative triples of elements in finite groupoids were studied from time to time (see [1],[3],[4] and [5]). Such questions and investigations (especially those concerning enumerations) belong to a certain branch of combinatorial algebra, and therefore they are of interest in the present time, too. In [2], the upper and the lower bounds for a(G), G being a finite non-associative commutative quasigroup isotopic to a group, were found. The purpose of this short note is to investigate the same problem in the non-commutative case.

1. <u>Introduction</u>. For a groupoid G, let $A(G) = \{(a,b,c); a,b,c \in G, a.bc = ab.c\}$ and $a(G) = \text{card } A(G)$. Let C be a class of groupoids. Then, for every positive integer n, we define numbers $a(C,n)$ and $b(C,n)$ as follows: $a(C,n) = -1 = b(C,n)$ if C contains no groupoid of order n; $a(C,n) = \min a(G)$, $G \in C$, card $G = n$, if C contains at least one groupoid of order n; $b(C,n) = n^3$ if C contains at least one groupoid of order n and every such groupoid is associative; $b(C,n) = \max a(G)$, $G \in C$, G not associative, card $G = n$, if C contains at least one non-associative groupoid of order n.

Let G be a groupoid and $a \in G$. Define two transformations L_a and R_a of G by $L_a(b) = ab$ and $R_a(b) = ba$.

2. <u>Auxiliary results</u>. In this section, let G(+) be a finite group (possibly non-commutative) of order n and f a permutation of G. Put $f'(x) = f(x) - x$ and $f''(x) = -x + f(x)$ for every $x \in G$. Let $p(f) = \text{card } \{(x,y); x,y \in G, f'(x) = f'(y)\}$ and $q(f) = \text{card } \{(x,y); x,y \in G, f''(x) = f''(y)\}$. For every $a \in \text{Im } f'$ ($a \in \text{Im } f''$), let $p(a,f) = \text{card } A$ ($q(a,f) = \text{card } A$) where A is the block of ker f' (ker f'') with $f'(A) = a$ ($f''(A) = a$). If $a \notin \text{Im } f'$ ($a \notin \text{Im } f''$) then $p(a,f) = 0$ ($q(a,f) = 0$).

2.1. Lemma. $p(f) = \sum_{a} p(a,f)^2$ and $q(f) = \sum_{a} q(a,f)^2$.

Proof. Obvious.

2.2. Lemma. $p(f) = p(L_a^+ f)$ and $q(f) = q(R_a^+ f)$ for every $a \in G$.

Proof. Obvious.

2.3. Lemma. Suppose that n is odd and $f \neq L_a^+$ ($f \neq R_a^+$)

for every $a \in G$. Then $p(f) \leq n^2 - 4n + 6$ $(q(f) \leq n^2 - 4n + 6)$.

Proof. The proof is in fact the same as that of [2, Lemma 2.3].

2.4. Lemma. Suppose that $f \neq L_a^+$ $(f \neq R_a^+)$ for every $a \in G$. Then $p(f) \leq n^2 - 4n + 8$ $(q(f) \leq n^2 - 4n + 8)$.

Proof. The same as that of [2, Lemma 2.5].

3. Auxiliary results. In this section, let $G(+)$ be a finite group of order n and f, g permutations of G. Put $r(f,g) = \operatorname{card}\{(a,b);\ a,b \in G,\ f''(a) = g''(b)\}$, $B(f,g) = \{(a,b,c);\ -a + f(a) - f(b) = -g(b) + g(c) - c\}$, $s(f,g) = \operatorname{card} B(f,g)$ and $t(f,g) = \operatorname{card}\{(a,b);\ g^{-1}(-f''(a)) = f^{-1}(-g'(b))\} - \operatorname{card}\{(a,b);\ f(b) + g(b) = b,\ f''(a) = f''(b)\} - \operatorname{card}\{(a,b);\ a \neq b,\ f(a) + g(a) = a,\ g'(a) = g'(b)\}$.

3.1. Lemma. $r(f,g) = \sum_a p(a,g)q(a,f)$.

Proof. Obvious.

3.2. Lemma. Let $n \geq 1$ and let $a_1,\dots,a_n,b_1,\dots,b_n$ be real numbers. Then $\sum a_i b_i \leq \max(\sum a_i^2, \sum b_i^2)$.

Proof. Obvious.

3.3. Lemma. $r(f,g) \leq \max(q(f),p(g))$.

Proof. Use 3.1, 3.2 and 2.1.

3.4. Lemma. $t(f,g) + p(g) + q(f) - n \leq s(f,g)$.

Proof. Put $A = \{(a,a,a);\ a \in G\}$, $B = \{(a,b,b);\ a \neq b,\ f''(a) = f''(b)\}$, $C = \{(a,a,b);\ a \neq b,\ g'(a) = g'(b)\}$ and $D = \{(a,c,b);\ c = g^{-1}(-f''(a)) = f^{-1}(-g'(b))\}$. Then $A \cup B \cup C \cup D \subseteq B(f,g)$, $A \cap B = A \cap C = B \cap C = \emptyset$, $\operatorname{card} A = n$, card $B = q(f) - n$, card $C = p(g) - n$. Finally, $D \cap (A \cup B \cup C) = \{(a,b,b);\ f(b) + g(b) = b,\ f''(a) = f''(b)\} \cup \{(a,a,b);\ f(a) + g(a) = a,\ a \neq b,\ g'(a) = g'(b)\}$.

3.5. Lemma. Suppose that neither f'' nor g' is a permutation. Then $n + 4 \leq s(f,g)$.

Proof. $q(f) \leq n + 2$ and $p(g) \leq n + 2$.

3.6. Lemma. Suppose that either f'' or g' is a permutation. Then $n^2 \leq s(f,g)$.

Proof. Let f'' be a permutation. Then, for all $b,c \in G$, there is an $a \in G$ with $-a + f(a) = -g(b) + g(c) - c + f(b)$.

3.7. Lemma. $s(f,g) = \sum_{b} r(R^{+}_{-f(b)}f,\ L^{+}_{-g(b)}g) = \sum_{a,b} q(a,R^{+}_{-f(b)}f)p(a,L^{+}_{-g(b)}g)$.

Proof. Easy.

3.8. Lemma. $s(f,g) \leq n.\max(q(f),p(g))$.

Proof. By 3.3 and 2.2, $r(R^{+}_{-f(b)}f,\ L^{+}_{-g(b)}g) \leq \max(q(f),p(g))$ and we can use 3.7.

3.9. Lemma. If $f = id$ ($g = id$) then $s(f,g) = np(g)$ ($s(f,g) = nq(f)$).

Proof. Easy.

4. Auxiliary results. In this section, let $G(+)$ be a finite group of order n and f, g permutations of G. Define a multiplication on G by $ab = f(a) + g(b)$. In this way, we obtain a quasigroup G.

4.1. Lemma. (i) G contains a left unit iff $g = L^{+}_{a}$ for some $a \in G$.

(ii) G contains a right unit iff $f = R_a^+$ for some $a \in G$.

(iii) G is a group iff $f = R_a^+$ and $g = L_b^+$ for some $a, b \in G$.

Proof. Easy.

4.2. Lemma. $a(G) = s(f,g)$.

Proof. $(x,y,z) \in A(G)$ iff $f(x) + g(f(y) + g(z)) = f(f(x) + g(y)) + g(z)$. Since f, g are permutations, $a(G) = \text{card } A$, where $A = \{(x,y,z);\ x + g(f(y) + z) = f(x + g(y)) + z\}$. Define a mapping h of A into $B(f,g)$ by $h(x,y,z) = (x + g(y), y, f(y) + z)$. Then h is bijective.

5. Quasigroups isotopic to groups. In the following result, let $a(n) = a(C,n)$ and $b(n) = b(C,n)$ where C is the class of left loops isotopic to groups.

5.1. Theorem. (i) $a(1) = 1 = b(1)$, $a(2) = 8 = b(2)$.

(ii) $a(n) = n^2$ for every n such that either n is odd or n is divisible by 4.

(iii) $a(n) = n^2 + 2n$ for every even n not divisible by 4.

(iv) $b(n) = n^3 - 4n^2 + 6n$ for every odd $n \geq 3$.

(v) $b(n) = n^3 - 4n^2 + 8n$ for every even n.

Proof. (i) These equalities are clear.

(ii) and (iii). Let G be a finite quasigroup of order n such that G contains a left unit e and G is isotopic to a group. Put $x + y = R_e^{-1}(x)y$ for all $x, y \in G$. Then $G(+)$ is a group and $xy = f(x) + y$, $f = R_e$. By 4.2, and 3.9, $a(G) = nq(f)$. Since $n \leq q(f)$, $n^2 \leq a(G)$ and we have proved that $n^2 \leq a(n)$. If $n = 2m$ for an odd m then f'' cannot be a permutation (this fact is easy and well known - see e.g.[1]), and so $n + 2 \leq q(f)$,

$n^2 = 2n \leq a(G)$ and $n^2 + 2n \leq a(n)$. In the rest, we can proceed similarly as in [2, Lemmas 1.5, 1.6, 2.10].

(iv) and (v). Suppose that $n \geq 3$. Let G be a non-associative finite quasigroup of order n such that G contains a left unit and G is isotopic to a group. Then there are a group G(+) and a permutation f of G such that $xy = f(x) + y$ for all $x,y \in G$. Since G is not associative, $f \neq R_a^+$ for every $a \in G$. By 4.2, 3.9 and 2.4 (resp. 2.3), $a(G) \leq n^3 - 4n^2 + 8n$ (resp. $a(G) \leq n^3 - 4n^2 + 6n$ provided n is odd). In the rest, we can proceed similarly as in [2, Lemmas 2.6, 2.7].

In the following result, let $a(n) = a(C,n)$ and $b(n) = b(C,n)$ where C is the class of quasigroups isotopic to groups.

5.2. <u>Theorem</u>. (i) $a(1) = 1 = b(1)$, $a(2) = 8 = b(2)$.

(ii) $n + 4 \leq a(n) \leq n^2$ for every $n \geq 2$ such that n is either odd or divisible by 4.

(iii) $n + 4 \leq a(n) \leq n^2 + 2n$ for every even n which is not divisible by 4.

(iv) $b(n) = n^3 - 4n^2 + 6n$ for every odd $n \geq 3$.

(v) $b(n) = n^3 - 4n^2 + 8n$ for every even n.

Proof. (i) These equalities are clear.

(ii) and (iii). We can assume that $3 \leq n$. Then $n + 4 \leq n^2$ and the result follows from 3.5, 4.2 and 5.1.

(iv) Let G be a non-associative quasigroup of order n such that G is isotopic to a group. With respect to 5.1, we can assume that G is neither a left nor a right loop. Then there are a group G(+) and permutations f, g of G such that $ab = f(a) + g(b)$ and $f \neq R_a^+$, $g \neq L_a^+$ for all $a,b \in G$ (use 4.1). By 4,2, 3.8 and 2.3, $a(G) \leq n^3 - 4n^2 + 6n$. Thus $a(n) \leq n^3 - 4n^2 + 6n$.

The converse inequality follows from 5.1(iv).

(v) We can proceed similarly as in (iv).

6. <u>Auxiliary results</u>. In this section, let $G(+)$ be a finite abelian group of order n and f, g endomorphisms of $G(+)$. Put $C(f,g) = \{(a,b);\ a,b \in G,\ f(a) = g(b)\}$ and $u(f,g) = \text{card}\ C(f,g)$.

6.1. Lemma. $n \leq u(f,g)$.

Proof. Define a mapping $h: G \times G \to G$ by $h(a,b) = f(a) - g(b)$. Then h is a homomorphism of the abelian group $G(+) \times G(+)$ into $G(+)$ and $\text{Ker}\ h = C(f,g)$. Hence $(\text{card Ker}\ h) \cdot (\text{card Im}\ h) = n^2$ and $\text{card Im}\ h \leq n$. Consequently, $n \leq u(f,g)$.

6.2. Lemma. Suppose that $n = 2m$ where $m \geq 1$ is odd and that $f = h'$, $g = k'$ for some automorphisms h and k of $G(+)$. Then $2n \leq u(f,g)$.

Proof. We can assume that $G(+) = H(+) \times K(+)$, $h = h_1 \times h_2$, $k = k_1 \times k_2$ where $H(+)$ is a group of order m, $K(+) = \{0,1\}$ is a two-element group, h_1, k_1 are automorphisms of $H(+)$ and h_2, k_2 of $K(+)$. Then $h_2 = \text{id} = k_2$, $h_2' = 0 = k_2'$, $f = h_1' \times 0$, $g = k_1' \times 0$ and the result follows easily from 6.1.

Put $r = \text{card Ker}\ f$ and $s = \text{card Ker}\ g$.

6.3. Lemma. $u(f,g) \leq \max(rn, sn)$.

Proof. For every $a \in G$, let $r(a) = \text{card}\{b;\ f(b) = a\}$ and $s(a) = \text{card}\{b;\ g(b) = a\}$. Then $u(f,g) = \sum_a r(a)s(a)$. By 3.2, $u(f,g) \leq \max(\sum r(a)^2, \sum s(a)^2)$. However, $rn = \sum r(a)^2$ and $sn = \sum s(a)^2$.

6.4. Lemma. Let $f = 0$ ($g = 0$). Then $u(f,g) = sn$

$(u(f,g) = rn)$.

Proof. Easy.

7. Auxiliary results. In this section, let $G(+)$ be a finite abelian group of order n, f, g commuting automorphisms of $G(+)$ and $w \in G$. Put $ab = f(a) + g(b) + w$ for all $a, b \in G$. We obtain thus a medial quasigroup G.

7.1. Lemma. (i) $f = id$ iff G contains a right unit.

(ii) $g = id$ iff G contains a left unit.

(iii) G is a group iff $f = id = g$.

Proof. Easy.

7.2. Lemma. $a(G) = nu(f', g')$.

Proof. $(x,y,z) \in A(G)$ iff $f^2(x) + g(z) + f(w) = f(x) + g^2(z) + g(w)$. Thus $a(G) = n.\mathrm{card}\, A$ where $A = \{(x,y);\ f(x + w) - x - w = g(y + w) - y - w\}$. The rest is clear.

8. Medial quasigroups. In the following result, let $a(n) = a(C,n)$ and $b(n) = b(C,n)$ where C is the class of medial quasigroups.

8.1. Theorem. (i) $a(n) = n^2$ for every n such that n is either odd or divisible by 4.

(ii) $a(n) = 2n^2$ for every even n not divisible by 4.

(iii) $b(1) = 1$ and $b(n) = n^3/p$ for every odd $n \geq 3$, p being the least prime dividing n.

(iv) $b(2) = 8$ and $b(n) = n^3/p$ for every $n = 2m$ where $m \geq 3$ is odd and p is the least prime dividing m.

(v) $b(n) = n^3/2$ for every $n \geq 4$ divisible by 4.

Proof. Using 6.1, 6.2, 6.3, 6.4, 7.1 and 7.2, we can proceed similarly as in the proofs of 5.1, 5.2 and [2, Theorem 3.3].

R e f e r e n c e s

[1] A.C. CLIMESCU: Etudes sur la théorie des systèmes multiplicatifs uniformes I. L´indice de non associativité, Bull. de l´Ecole Polytech. de Jassy 2(1947), 97-121.

[2] T. KEPKA: Notes on associative triples of elements in commutative groupoids (to appear).

[3] D.A. NORTON: A note on associativity, Pacific J. Math. 10 (1960), 591-596.

[4] G. SZÁSZ: Die Unabhängigkeit der Assoziativitätsbedingungen, Acta Sci. Math. Szeged 15(1953), 20-28.

[5] A. WAGNER: On the associative law of groups, Rend. Math. e Appl. 21(1962), 60-76.

Výzkumný ústav matematických strojů, Lužná 2, 16000 Praha 6
Československo

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

(Oblatum 29.1. 1981)