Tomáš Kepka

Notes on associative triples of elements in commutative groupoids

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 22 (1981), No. 2, 39--47

Persistent URL: `http://dml.cz/dmlcz/142472`

1981 ACTA UNIVERSITATIS CAROLINAE - MATHEMATICA ET PHYSICA VOL. 22. NO. 2. Pag. 39—47

Notes On Associative Triples Of Elements In Commutative Groupoids

T. KEPKA
Department of Mathematics, Charles University, Prague*)

Received 5 March 1981

The numbers of associative triples of elements in some finite commutative groupoids are investigated.

V článku se vyšetřují počty asociativních trojic prvků v některých konečných komutativních grupoidech.

В статье исследуются числа ассоциативных троек в некоторых классах конечных коммутативных группоидов.

1. Introduction

For a groupoid G, let $A(G) = \{(x, y, z) \mid x, y, z \in G,\ x \,.\, yz = xy \,.\, z\}$, $B(G) = G^3 \setminus A(G)$, $a(G) = \operatorname{card} A(G)$ and $b(G) = \operatorname{card} B(G)$. Let C be a class of groupoids. Then, for every positive integer n, we define two numbers $a(C, n)$ and $b(C, n)$ as follows: $a(C, n) = \min a(G)$, $G \in C$, $\operatorname{card} G = n$; $a(C, n) = -1$ if C contains no groupoid of order n; $b(C, n) = \max a(G)$, $G \in C$, G is not associative, $\operatorname{card} G = n$; $b(C, n) = n^3$ if C contains at least one groupoid of order n and every groupoid of order n contained in C is associative; $b(C, n) = -1$ in C contains no groupoid of order n.

1.1 Lemma. Let G be a finite commutative groupoid of order n. Then $n^2 \leqq a(G)$.

Proof. We have $a \,.\, ba = ab \,.\, a$ for all $a, b \in G$.

1.2 Lemma. Let G be a non-associative commutative groupoid. Then $2 \leqq b(G)$.

Proof. Since $B(G)$ is non-empty, $(a, b, c) \in B(G)$ for some $a, b, c \in G$. Then $(c, b, a) \in B(G)$. If $(a, b, c) = (c, b, a)$ then $a = c$ and $(a, b, c) \in A(G)$, a contradiction.

1.3 Lemma. Let G be a non-associative commutative groupoid such that $B(G)$ contains a triple (a, b, c) with $a \neq b \neq c$. Then $4 \leqq b(G)$.

*) 186 00 Praha 8, Sokolovská 83, Czechoslovakia.

Proof. We have $(a, b, c), (c, b, a) \in B(G)$. If $(a, c, b), (b, c, a), (b, a, c), (c, a, b) \in \in A(G)$, then $a \cdot bc = a \cdot cb = ac \cdot b = ca \cdot b = c \cdot ab = ab \cdot c$, a contradiction.

1.4 Lemma. Let $3 \leqq n$ be an integer. Then there exists a commutative groupoid G of order n such that $a(G) = n^3 - 2$.

Proof. We shall proceed by induction on n. First, let $n = 3$. Consider the following three-element groupoid $K = \{a, b, c\}$: $ab = b = ba$, $aa = ac = ca = bb = bc = cb = cc = c$. It is easy to check that K is commutative and $b(K) = 2$. Now, let $4 \leqq n$ and let H be a commutative groupoid of order $n - 1$ such that $b(H) = 2$. Take an element w not belonging to H, put $G = H \cup \{w\}$ and define $wx = w = xw$ for every $x \in G$. Then G is a commutative groupoid, card $G = n$ and $b(G) = 2$.

1.5 Lemma. Let n be an odd positive integer. Then there exists a commutative medial quasigroup Q such that $a(Q) = n^2$.

Proof. Let $Q(+) = \{0, 1, \ldots, n - 1\}$ be the cyclic group of integers modulo n. Put $x * y = -x - y$ for all $x, y \in Q$. The rest is clear.

1.6 Lemma. Let $4 \leqq n$ be an integer divisible by 4. Then there exists a commutative medial quasigroup Q of order n such that $a(Q) = n^2$.

Proof. We have $n = 2^k m$, where $2 \leqq k$ and $1 \leqq m$ is odd. Let F be a finite field of order 2^k, $0, 1 \neq a \in F$ and $x * y = ax + ay$ for all $x, y \in F$. Then $F(*)$ is a commutative medial quasigroup and $a(F(*)) = 2^{2k}$. By 1.5, there exists a commutative medial quasigroup $P(*)$ of order m such that $a(P(*)) = m^2$. Now, it suffices to put $Q = F(*) \times P(*)$.

1.7 Lemma. Let n be a positive integer. Then there exists a commutative groupoid G of order n such that $a(G) = n^2$.

Proof. With respect to 1.5 and 1.6, we can assume that $n = 2m$ where $1 \leqq m$ is odd. Consider the following two-element groupoid $K = \{a, b\} : aa = b$, $ab = ba = bb = a$. Then $a(K) = 4$ and we can put $G = K \times H$, where H is a groupoid of order m such that $a(H) = m^2$.

In the following proposition, let $a(n) = a(C, n)$ and $b(n) = b(C, n)$, where C is the class of commutative groupoids.

1.8 Proposition. (i) $a(n) = n^2$ for every $1 \leqq n$. (ii) $b(1) = 1$, $b(2) = 4$ and $b(n) = n^3 - 2$ for every $3 \leqq n$.

Proof. Apply 1.1, 1.2, 1.4 and 1.7.

1.9 Remark. Let C denote the class of commutative quasigroups. By 1.1, 1.5 and 1.6, $a(C, n) = n^2$ for every $3 \leqq n$ such that n is either odd or divisible by 4. Further, by [1], $b(C, n) = n^3 - 16n + 64$ for every even $168 \leqq n$.

Let f be a permutation of an abelian group $G(+)$. Put $f'(x) = f(x) - x$ and $p(f) = \operatorname{card}\{(x, y) \mid x, y \in G, f'(x) = f'(y)\}$.

2.1 Lemma. Let $G(+)$ be a finite abelian group of order n and f a permutation of G. Put $x * y = f(x) + f(y)$ for all $x, y \in G$. Then $G(*)$ is a commutative quasigroup and $a(G(*)) = n\, p(f)$.

Proof. $(x, y, z) \in A(G(*))$ iff $f(x) + f(f(y) + f(z)) = f(f(x) + f(y)) + f(z)$. Hence $a(G(*)) = \operatorname{card} T$, T being the set of ordered triples (x, y, z) such that $x, y, z \in G$ and $x + f(y + z) = f(x + y) + z$. Now, let $x, y, z \in G$ and $u = y + z$, $v = x + y$. Then $(x, y, z) \in T$ iff $f'(u) = f'(v)$ and the rest is clear.

2.2 Lemma. Let $2 \leqq k$ and $1 \leqq p_1, \ldots, p_k$ be such that $3 \leqq n = \Sigma p_i$ and $p_1, p_2 \notin \{1, 2\}$ if $k = 2$. Then $\Sigma p_i^2 \leqq n^2 - 4n + 6$.

Proof. We shall proceed by induction on k. Let us distinguish the following cases:

(i) $k = 2$. Then $p_2 = n - p$, $p = p_1$, and $\Sigma p_i^2 = n^2 + 2p^2 - 2np$. Further, $2n - 3 \leqq np - p^2$, since $3 \leqq p$, $p - n$ and $6 \leqq n$. Hence $2p^2 - 2np \leqq$ $\leqq -4n + 6$ and $2p^2 + n^2 - 2np \leqq n^2 - 4n + 6$.

(ii) $k = 3$. Put $p = p_1$, $q = p_2$ and $t = p_3$ and assume that $p \leqq q \leqq t$. It suffices to show that $0 \leqq pq + ht + qt - 2p - 2q - 2t + 3 = w$. If $p = 1$ then $w = qt - q - t + 1 = q(t - 1) - (t - 1)$ and $0 \leqq w$, since $t - 1 \leqq q(t - 1)$. If $2 \leqq p$ then $0 \leqq (p - 2)\, q + (q - 2)\, t + (t - 2)\, p + 3 = w$.

(iii) $4 \leqq k$. Put $q = p_1 + \ldots + p_{k-1}$ and $p = p_k$. We have $3 \leqq q$ and $\Sigma p_i^2 \leqq q^2 -$ $- 4q + 6 + p^2$. However, $q^2 - 4q + 6 + p^2 = q^2 - 4q + 6 + (n - q)^2 =$ $= n^2 + 2q^2 - 4q - 2nq + 6$ and it suffices to show that $2n \leqq (2 + n)\, q -$ $- q^2$. But this is clear, since $3 \leqq q \leqq n - 1$.

2.3 Lemma. Let $G(+)$ be a finite abelian group of odd order n and f a permutation of G such that $f \neq L_a^+$ for every $a \in G$. Then $p(f) \leqq n^2 - 4n + 6$.

Proof. Since $f \neq L_a^+$ for every $a \in G$, the equivalence $\ker f'$ has $2 \leqq k$ blocks; say $A_1, \ldots, A_k$. Put $p_i = \operatorname{card} A_i$. Obviously, $\Sigma p_i = n$ and $\Sigma p_i^2 = p(f)$. With respect to 2.2, it is enough to show that $p_1, p_2 \notin \{1, 2\}$, provided $k = 2$. Assume first that $k = 2$ and $p_1 = 1$. Then $A_1 = \{a\}$ for some $a \in G$. Since $f'(x) = f'(y) = b$ for all $x, y \in A_2 = G \setminus \{a\}$, $f(z) = z + b$ for each $z \in A_2$. Consequently, $f(a) \neq a + b$, $f(a) = c + b$, $c \in A_2$, $f(c) = c + b$, $f(a) = f(c)$, $a = c$, a contradiction. Now, let $k = 2$, $p_1 = 2$ and $A_1 = \{a, b\}$. Again, $f(x) = x + c$ and $f(y) = y + d$ for all $x \in A_1$, $y \in A_2$ and some $c, d \in G$, $c \neq d$. But $a + c = e + d$, $e \notin A_2$, and so $e = b$ and $a + c = b + d$. Similarly, $b + c = a + d$, $a + 2c = b + c + d = a + 2d$, $2(c - d) = 0$ and $c = d$, a contradiction.

2.4 Lemma. Let $2 \leqq k$ and $1 \leqq p_1, \ldots, p_k$ be such that $3 \leqq n = \Sigma p_i$ and $p_1 \neq 1 \neq p_2$ if $k = 2$. Then $\Sigma p_i^2 \leqq n^2 - 4n + 8$.

Proof. With regard to 2.2, we can assume that $k = 2 = p_1$ and $p = p_2$. Then $n = p + 2$, $\Sigma p_i^2 = 4 + p^2$ and $n^2 - 4n + 8 = p^2 + 4$.

2.5 Lemma. Let $G(+)$ be a finite abelian group of order n and f a permutation of G such that $f \neq L_a^+$ for every $a \in G$. Then $p(f) \leqq n^2 - 4n + 8$.

Proof. Using 2.4, we can proceed in the same way as in the proof of 2.3.

2.6 Lemma. Let $3 \leqq n$ be an odd integer. Then there exists a commutative quasigroup Q of order n such that Q is isotopic to a group and $a(Q) = n^3 - 4n^2 + 6n$.

Proof. Let $Q(+) = \{0, 1, \ldots, n - 1\}$ be the cyclic group of integers modulo n. Define a permutation f by $f(0) = 1$, $f(1) = 0$ and $f(i) = i$ for $2 \leqq i \leqq n - 1$. It is easy to verify that $p(f) = (n - 2)^2 + 2 = n^2 - 4n + 6$. The rest is clear by 2.1.

2.7 Lemma. Let $2 \leqq n$ be an even integer. Then there exists a commutative quasigroup of order n such that Q is isotopic to a group and $a(Q) = n^3 - 4n^2 + 8n$.

Proof. Let $Q(+)$ be the cyclic group of integers modulo n. Put $m = n/2$ and define f by $f(0) = m$, $f(m) = 0$ and $f(i) = i$ for $0 < i \leqq n - 1$, $i \neq m$. The rest is clear.

2.8 Lemma. Let $G(+)$ be a finite abelian group of order n. Put $s = \Sigma x$, $x \in G$, and $H = \{y \in G \mid 2y = 0\}$. Then $s \in H$. Moreover, $s \neq 0$ iff card $H = 2$; in this case, $H = \{0, s\}$.

Proof. Obvious.

2.9 Lemma. Let $G(+)$ be a finite abelian group of order $n = 2m$, where $1 \leqq m$ is odd. Let f be a permutation of G. Then $n + 2 \leqq p(f)$.

Proof. It suffices to show that f' is not a permutation. Suppose that f' is a permutation and put $s = \Sigma x$, $x \in G$. Then $\Sigma f(x) = s = \Sigma f'(x) = \Sigma f(x) - \Sigma x = s - s = 0$, a contradiction with 2.8.

2.10 Lemma. Let $1 \leqq m$ be odd and $n = 2m$. Then there exists a commutative quasigroup Q of order n such that Q is isotopic to a group and $a(Q) = n^2 + 2n$.

Proof. Let $Q(+)$ be the cyclic group of integers modulo n. Define a permutation f by $f(0) = m - 1$, $f(1) = 0$, $f(2) = 1, \ldots, f(m - 2) = m - 3$, $f(m - 1) = m - 2$, $f(m) = m$, $f(m + 1) = m + 1, \ldots, f(n - 2) = n - 2$, $f(n - 1) = n - 1$ and put $g(x) = f(-x)$ for every $x \in G$. Then $\ker g' = \{((m + 1)/2, 0), (0, (m + 1)/2)\} \cup \mathrm{id}_Q$ and the rest follows from 2.1.

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

2.11 Theorem. (i) $a(n) = n^2$ for every $1 \leqq n$ such that n is either odd or divisible by 4.

(ii) $a(n) = n^2 + 2n$ for every $n = 2m$, where $1 \leqq m$ is odd.

(iii) $b(1) = 1$ and $b(n) = n^3 - 4n^2 + 6n$ for every odd $3 \leqq n$.

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

Proof. (i) This follows from 1.1, 1.5 and 1.6.

(ii) Let Q be a commutative quasigroup of order $n = 2m$, $1 \leqq m$ odd, such that Q is isotopic to a group. Then there are an abelian group $Q(+)$ and a permutation f of Q such that $xy = f(x) + f(y)$ for all $x, y \in Q$. By 2.1 and 2.9, $n^2 + 2n \leqq \leqq a(Q)$. The equality $a(n) = n^2 + 2n$ follows now from 2.10.

(iii) Let $3 \leqq n$ be odd and let Q be a non-associative commutative quasigroup of order n such that Q is isotopic to a group. There are an abelian group $Q(+)$ and a permutation f of Q such that $xy = f(x) + f(y)$ for all $x, y \in Q$. Since Q is not a group, $f \neq L_a^+$ for every $a \in Q$. By 2.1 and 2.3, $a(Q) \leqq n^3 - 4n^2 + 6n$. The result follows now from 2.6.

(iv) Using 2.5 and 2.7, we can proceed similarly as in the proof of (iii).

3. Commutative Medial Quasigroups

Let f be an automorphism of an abelian group $G(+)$. Put $q(f) = \operatorname{card} \{x \mid x \in G, f(x) = x\}$.

3.1 Lemma. Let $G(+)$ be a finite abelian group of order n, f an automorphism of $G(+)$ and $w \in G$. Put $x * y = f(x + y) + w$ for all $x, y \in G$. Then $G(*)$ is a commutative medial quasigroup and $a(G(*)) = n^2 \,.\, q(f)$.

Proof. Easy.

3.2 Lemma. Let $G(+)$ be a finite abelian group of order $n = 2m$, where $3 \leqq m$ is odd. Let f be an automorphism of $G(+)$. Then $2 \leqq q(f)$. Moreover, if $f \neq \mathrm{id}_G$ then $q(f) \leqq 2m/p$, p being the least prime dividing m.

Proof. Put $K = \{x \mid f(x) = x\}$ and $s = \Sigma x$, $x \in G$. By 2.8, $0 \neq s$ and $s \in K$. Consequently, $2 \leqq q(f)$. Suppose $f \neq \mathrm{id}$. Then K is a proper subgroup of $G(+)$ and $\operatorname{card} K = 2k$, where k divides m and $k \neq m$. Obviously, $k \leqq m/p$.

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

3.3 Theorem. (i) $a(n) = n^2$ for every $1 \leqq n$ such that n is either odd or divisible by 4.

(ii) $a(n) = 2n^2$ for every $n = 2m$, where $1 \leqq m$ is odd.

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

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

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

Proof. (i) See 1.1, 1.5 and 1.6.

(ii) Let Q be a commutative medial quasigroup of order $n = 2m$. There exist an abelian group $Q(+)$, an automorphism f of $Q(+)$ and $w \in Q$ such that $xy = f(x + y) + w$ for all $x, y \in Q$. By 3.1 and 3.2, $a(Q) = n^2 . q(f)$, $2 \leqq q(f)$ and $2n^2 \leqq a(Q)$. Further, let $G(+)$ be the cyclic group of integers modulo n, $f(x) = -x$ and $x * y = -x - y$ for all $x, y \in G$. Then $G(*)$ is a commutative medial quasigroup, $f(x) = x$ iff $x \in \{0, m\}$, $q(f) = 2$ and $a(G(*)) = 2n^2$.

(iii) Let $3 \leqq n$ be an odd number and let p be the least prime divisor of n. Consider a non-associative commutative medial quasigroup of order n. There are an abelian group $Q(+)$, an automorphism f of $Q(+)$ and $w \in Q$ such that $xy = f(x + y) + w$ for all $x, y \in Q$. Put $H = \{x \mid f(x) = x\}$. Since Q is not associative, $f \neq \mathrm{id}$ and H is a proper subgroup of $Q(+)$. Hence $q(f) = \operatorname{card} H \leqq n/p$ and $a(Q) \leqq n^3/p$ by 3.1. On the other hand, let $A(+)$ and $B(+)$ be cyclic groups of orders p and n/p, resp. Put $G(+) = A(+) \times B(+)$ and $f(x, y) = (-x, y)$ for all $x \in A$ and $y \in B$. Then f is an automorphism of $G(+)$ and $q(f) = n/p$.

(iv) Using similar arguments as in the proof of (iii), we can show that $b(n) = n^3/2$. Further, $n = 2^k m$, where $2 \leqq k$ and $1 \leqq m$ is odd. Consider cyclic groups $A(+)$ and $B(+)$ of orders 2^k and m, resp., and put $G(+) = A(+) \times B(+)$ and $f(x, y) = ((2^{k-1} + 1)\, x, y)$ for all $x \in A$ and $y \in B$. The rest is clear.

(v) Let $3 \leqq m$ be an odd integer, p the least prime dividing m and $n = 2m$. Further, let $G(+)$ be a finite abelian group of order n and $f \neq \mathrm{id}$ an automorphism of $G(+)$. Put $H = \{x \mid f(x) = x\}$. Then $\operatorname{card} H = q(f)$ is an even number. On the other hand, $q(f)$ divides n. Consequently, $q(f) \leqq 2m/p$ and $b(n) \leqq n^3/p$. Finally, by (iii), there is a commutative medial quasigroup P of order m such that $a(P) = m^3/p$. Put $Q = K \times P$, where K is a two-element group. Then $a(Q) = n^3/p$.

4. Commutative Quasitrivial Groupoids

A groupoid G is said to be quasitrivial if $xy \in \{x, y\}$ for all $x, y \in G$. A relation r defined on a set M is called complete if for all $x, y \in M$, either $(x, y) \in r$ or $(y, x) \in r$.

4.1 Lemma. There is a one-to-one correspondence between commutative quasitrivial groupoids and non-empty complete antisymmetric reflexive relations.

Proof. Let G be a quasitrivial commutative groupoid. Define a relation r on G by $(x, y) \in r$ iff $xy = y$. The rest is clear.

Consider the following three-element groupoid $T = \{a, b, c\} : aa = ab = ba = = a$, $bb = bc = cb = b$, $cc = ac = ca = c$. Then T is a commutative quasitrivial groupoid, $a(T) = 21$ and $b(T) = 6$.

4.2 Lemma. Let G be a commutative quasitrivial groupoid, $x, y, z \in G$ and $P = \{x, y, z\}$. Then P is a subgroupoid of G and $x \,.\, yz \neq xy \,.\, z$ iff P is isomorphic to T.

Proof. First, let $x \,.\, yz \neq xy \,.\, z$. Then $x \neq y \neq z$ and $x \neq z$. If $xy = x$ then $x \,.\, yz \neq xz$, and hence $yz = y$, $x \neq xz$ and $xz = z$. If $xy = y$ then $x \,.\, yz \neq yz$, and hence $yz = z$ and $xz = x$. In both cases, P is isomorphic to T. The converse is clear.

4.3 Lemma. Let G be a finite commutative quasitrivial groupoid of order n. Denote by m the number of all three-element subsets $S = \{x, y, z\}$ of G such that the subgroupoid S is isomorphic to T. Then $b(G) = 6m$ and $a(G) = n^3 - 6m$.

Proof. This is an easy consequence of 4.2.

4.4 Lemma. Let G be a commutative quasitrivial groupoid, r the corresponding relation and $S = \{x, y, z\}$ a three-element subset of G. Then S is isomorphic to T iff at least one of the following conditions is satisfied:

(i) $(y, x), (z, y), (x, z) \in r$.
ii) $(x, y), (y, z), (z, x) \in r$.

Proof. Easy.

In the following theorem, let $a(n) = a(C, n)$ and $b(n) = b(C, n)$, where C is the class of commutative quasitrivial groupoids.

4.5 Theorem. (i) $a(n) = (3n^3 + n)/4$ for every odd $n \geqq 1$.
(ii) $a(n) = (3n^3 + 4n)/4$ for every even $n \geqq 2$.
(iii) $b(1) = 1$, $b(2) = 8$ and $b(n) = n^3 - 6$ for every $n \geqq 3$.
Proof. (i) and (ii). See 4.3, 4.4 and [2].

(iii) Let $n \geqq 3$. Starting with T and proceeding simılarly as in the proof of 1.4, we can show that there exists a commutative quasitrivial groupoid G of order n such that $a(G) = n^3 - 6$. The rest is clear from 4.2 and 4.3.

5. Commutative Distributive Groupoids

For a groupoid G, let $C(G) = \{(x, y, z) \in A(G) \mid x \neq z\}$ and $c(G) = \text{card}\, C(G)$.
A groupoid satisfying the identities $x \,.\, yz = xy \,.\, xz$ and $yz \,.\, x = yx \,.\, zx$ is said to be distributive.

5.1 Lemma. Let G be a CD-groupoid containing a subquasigroup Q and an element a such that $G = Q \cup \{a\}$ and $aQ \subseteq Q$. Then there is an element $b \in Q$ such that $ax = bx$ for every $x \in Q$. Moreover, either $aa = a$ or $aa = b$.

Proof. Take $c \in Q$. There is $b \in Q$ such that $ac = bc$. Then $c . ax = ca . cx = = cb . cx = c . bx$ and $ax = bx$. Moreover, $b = b . bb = a . ab = aa . ab = = aa . b$.

5.2 Lemma. Let G be a finite CD-groupoid of order n containing a subquasigroup Q and an element a such that $a \notin Q$, $G = Q \cup \{a\}$ and $aQ \subseteq Q$. Then $c(G) \geqq 2n$.

Proof. By 5.1, there is an element $b \in Q$ such that (a, x, b), (b, x, a), (a, a, b), $(b, a, a) \in A(G)$ for every $x \in Q$.

Let G be a CDI-groupoid (i.e., a commutative distributive idempotent groupoid). Define a relation r on G by $(x, y) \in r$ iff the elements x, y generate the same ideal of G. Then r is a congruence of G, G/r is a semigroup and every block of r is a cancellation groupoid.

5.3 Lemma. Let G be a finite CDI-groupoid of order n such that G is not a quasigroup. Then $c(G) \geqq 2n$.

Proof. Since G is not a quasigroup, $q = \operatorname{card} G/r \geqq 2$. We shall proceed by induction on q. First, let $q = 2$. Then $G/r = \{K, H\}$, where $KH \subseteq H$. Put $k = \operatorname{card} K$ and $m = \operatorname{card} H$. By 5.2, $c(G) \geqq 2km + 2k \geqq 2n$. Now, let $q \geqq 3$, f be the natural homomorphism of G onto G/r and let K be a block of r such that $f(K)$ is a maximal element in the semilattice G/r. Put $H = G \setminus K$, $k = \operatorname{card} K$ and $m = \operatorname{card} H$. Then H is a subgroupoid of G and $c(G) \geqq 2m + 4k \geqq 2n$ (take into account that $KL \subseteq L$ for a block $L \neq K$ of r).

5.4 Lemma. Let G be a finite CD-groupoid of order n such that G is not a quasigroup. Then $c(G) \geqq 2n$.

Proof. We can assume that G is not idempotent. Denote by I the set of all idempotents of G. Then I is a proper ideal of G and $k, m \geqq 1$, $k = \operatorname{card} G \setminus I$ and $m = \operatorname{card} I$. If I is a quasigroup then $c(G) \geqq 2km + 2k \geqq 2n$ by 5.2. If I is not a quasigroup then $c(G) \geqq 2m + 4k \geqq 2n$ (take into account that $GH \subseteq H$, H being the intersection of all ideals of G).

5.5 Lemma. Let Q be a finite CD-quasigroup of order n. Then n is odd, $c(Q) = 0$ and $a(Q) = n^2$.

Proof. Easy.

5.6 Lemma. For every odd $n \geqq 1$, there exists at least one CIM-quasigroup (i.e., a commutative idempotent medial quasigroup) of order n.

Proof. Easy.

5.7 Lemma. Let $n \geqq 4$ be even. Then there exists a CIM-groupoid G of order n such that $c(G) = 2n$.

Proof. Let Q be a CIM-quasigroup of order $n - 1$ and let $b \in Q$ and $a \notin Q$. Put $G = Q \cup \{a\}$ and $aa = a$, $ax = xa = bx$ for every $x \in Q$. The rest is clear.

5.8 Lemma. Let G be a non-associative CD-groupoid. Then $b(G) \geqq 18$.

Proof. We can assume that G is a non-trivial quasigroup and the result follows then from 5.5.

5.9 Lemma. For every $n \geqq 3$, there exists a CIM-groupoid G of order n such that $b(G) = 18$.

Proof. Put $G = \{0, 1, \ldots, n - 1\}$ and define $0 * 0 = 1 * 2 = 2 * 1 = 0$, $1 * 1 = 0 * 2 = 2 * 0 = 1$, $2 * 2 = 0 * 1 = 1 * 0 = 2$, $i * j = \max(i, j)$ for all $0 \leqq i, j \leqq n - 1$ such that either $3 \leqq i$ or $3 \leqq j$.

In the following theorem, let $a(n) = a(C, n)$ and $b(n) = b(C, n)$, where C is the class of CD-groupoids.

5.10 Theorem. (i) $a(n) = n^2$ for every odd $n \geqq 1$.
(ii) $a(n) = n^2 + 2n$ for every even $n \geqq 2$.
(iii) $b(1) = 1$, $b(2) = 8$ and $b(n) = n^3 - 18$ for every $n \geqq 3$.

Proof. See 5.1, …, 5.9.

5.11 Remark. The same result is true for the classes of CDI-groupoids and CIM-groupoids.

References

[1] DRÁPAL, A.: On quasigroups rich in associative triples (to appear).
[2] ERDÖS, P., SPENCER, J.: Probabilistic methods in combinatorics. Akadémiai kiadó, Budapest 1974.
[3] KEPKA, T.: Commutative distributive groupoids. Acta Univ. Carolinae Math. Phys. *19/2* (1978), 45—58.