Jaroslav Ježek; Tomáš Kepka
Notes on the number of associative triples

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 31 (1990), No. 1, 15--19

Persistent URL: `http://dml.cz/dmlcz/142611`

Notes on the Number of Associative Triples

JAROSLAV JEŽEK, TOMÁŠ KEPKA

Praha*)

Received 2 February 1989

Some questions concerning the number of associative triples in a quasigroup are discussed.

Diskutují se některé otázky, týkající se počtu asociativních trojic v kvazigrupě.

Дискутируются некоторые вопросы о числе ассоциативных троек в квазигруппе.

1. Introduction

For a quasigroup Q, let

$$\mathrm{A}(Q) = \{(x, y, z) \in Q^3;\ x \,.\, yz = xy \,.\, z\}\,, \quad \mathrm{a}(Q) = \mathrm{card}\,(\mathrm{A}(Q))\,,$$
$$\mathrm{B}(Q) = Q^3 - A(Q)\,, \quad \mathrm{b}(Q) = \mathrm{card}\,(\mathrm{B}(Q))\,.$$

Obviously, $\mathrm{b}(Q) = 0$ iff Q is a group. By [3], Q if Q is infinite and nonassociative then a $(Q) = \mathrm{b}(Q) = \mathrm{card}\,(Q)$. Now, let Q be finite and $n = \mathrm{card}\,(Q)$. Then $\mathrm{a}(Q) + \mathrm{b}(Q) = n^3$; for every $x \in Q$ we can define two elements $f(x), e(x) \in Q$ by $f(x)\, x = x = x\, e(x)$; since $f(x) \,.\, x\, e(x) = x = f(x)\, x \,.\, e(x)$, the set $\{(f(x), x, e(x));\ x \in Q\}$ is contained in $\mathrm{A}(Q)$ and we get $n \leqq \mathrm{a}(Q) \leqq n^3$.

Every quasigroup with at most two elements is a group. On the other hand, for every $n \geqq 3$ there are nonassociative quasigroups of order n. We denote by $\mathrm{a}_{\max}(n)$ the maximum and by $\mathrm{a}_{\min}(n)$ the minimum of the numbers $\mathrm{a}(Q)$, for Q running over all the nonassociative quasigroups of order $n \geqq 3$. The numbers $\mathrm{b}_{\max}(n)$ and $\mathrm{b}_{\min}(n)$ can be defined similarly, and we have $\mathrm{b}_{\max}(n) = n^3 - \mathrm{a}_{\min}(n)$ and $\mathrm{b}_{\min}(n) = n^3 - \mathrm{a}_{\max}(n)$.

For every $n \geqq 1$ denote by assspec (n) the set of the numbers $\mathrm{a}(Q)$, where Q runs over the quasigroups of order n. This set, called the associativity spectrum of n, is contained in $\{n, n + 1, \ldots, n^3\}$. We have

asspec $(1) = \{1\}$,

*) Department of Mathematics, Charles University, 186 00 Praha 8, Sokolovská 83, Czechoslovakia.

$\operatorname{assspec}(2) = \{8\}$,
$\operatorname{assspec}(3) = \{9, 27\}$,
$\operatorname{assspec}(4) = \{16, 24, 32, 64\}$,
$\operatorname{assspec}(5) = \{15, \ldots, 57, 59, 62, 63, 74, 79, 80, 89, 125\}$,
$\operatorname{assspec}(6) = \{16, 19, \ldots, 114, 116, 117, 118, 120, 121, 122, 124, \ldots, 128, 130, \ldots$
$\ldots, 137, 141, 142, 144, 148, 152, 160, 162, 168, 172, 184, 189, 216\}$.

Hence

$$\begin{aligned} a_{\min}(3) &= a_{\max}(3) = 9, \\ a_{\min}(4) &= 16, \quad a_{\max}(4) = 32, \\ a_{\min}(5) &= 15, \quad a_{\max}(5) = 89, \\ a_{\min}(6) &= 16, \quad a_{\max}(6) = 189. \end{aligned}$$

These values can be obtained on a computer. A standard backtracking program can be used to generate all n-element quasigroups with a fixed permutation for the top row of the multiplication table. For $n = 6$ there are 1 128 960 such quasigroups. Then for each quasigroup generated by the backtracking routine, each number of a certain set of permutations is applied to give an isotopic quasigroup. The number of associative triples in each such quasigroup is counted. For $n = 6$ only 12 permutations are needed to get all the nonindempotent quasigroups, and the idempotent case is handled separately. The program was written and the computation for $n = 6$ was done by J. Berman using the facilities of the Computer Center at the University of Illinois at Chicago.

The following are examples of a quasigroup H of order 6 with $a(H) = 16$ and of a quasigroup Q of order 6 with $a(Q) = 189$:

H	1	2	3	4	5	6
1	2	1	4	3	5	6
2	1	2	5	6	4	3
3	6	5	1	2	3	4
4	5	6	3	4	1	2
5	4	3	2	1	6	5
6	3	4	6	5	2	1

Q	1	2	3	4	5	6
1	2	3	1	5	6	4
2	3	1	2	6	4	5
3	1	2	3	4	5	6
4	6	5	4	1	3	2
5	4	6	5	2	1	3
6	5	4	6	3	2	1

2. Examples

2.1. Example. Let $n \geqq 4$ be an even number. Take an abelian group $Q(+)$ of order n and two distinct elements $a, b \in Q - \{0\}$ with $2a = 0$. Let us define a new binary operation, a multiplication, on Q as follows: put $xy = x + y$ for all $x, y \in Q$ such that either $x \notin \{b, a + b\}$ or $y \notin \{b, a + b\}$; put $bb = (a + b)(a + b) = 2b + a$ and $b(a + b) = (a + b)\,b = 2b$. It is easy to verify that Q is a commutative loop and that $(x, y, z) \in B(Q)$ iff either $x \in \{b, a + b\}$, $y \in \{b, a + b, b - z, a + b - z\}$

and $z \notin \{0, a, b, a + b\}$ or else $x \in \{0, a, b, a + b\}$, $y \in \{b, a + b, b - x, a + b - x\}$ and $z \in \{b, a + b\}$. Hence $\mathrm{b}(Q) = 16n - 64$.

As a consequence we get

$$n^3 - 16n + 64 \in \operatorname{assspec}(n),$$
$$\mathrm{b}_{\min}(n) \leqq 16n - 64,$$
$$\mathrm{a}_{\max}(n) \geqq n^3 - 16n + 64$$

for any even number $n \geqq 6$.

2.2. Example. Let $n \geqq 3$ be such that $n \neq 4k + 2$ for any k. Then there exist a commutative group $Q(+)$ and an automorphism f of $Q(+)$ such that $f(x) \neq x$ for all $x \in Q - \{0\}$. For example, we can express n as $n = 2^m d$ where $m \neq 1$ and d is an odd number, take $Q(+) = C_1(+) \times \ldots \times C_m(+) \times D(+)$ where C_i is the two-element group and D is the cyclic group of order d and put $f(x_1, \ldots, x_m, y) = (x_1 + x_2, x_3, \ldots, x_m, x_1, 2y)$. Define a multiplication on Q by $xy = f(x + y)$. In this way we obtain a quasigroup Q and it is easy to see that $\mathrm{A}(Q) = \{(x, y, x);\ x, y \in Q\}$.

As a consequence we get

$$n^2 \in \operatorname{assspec}(n),$$
$$\mathrm{a}_{\min}(n) \leqq n^2,$$
$$\mathrm{b}_{\max}(n) \geqq n^3 - n^2$$

for any number $n \geqq 3$ such that $n \neq 4k + 2$ for any k.

2.3. Example. Let $G(+)$ be an abelian group of an odd order $m \geqq 3$ and let $Q(+) = Z_2(+) \times G(+)$. Put $f(a, x) = (a, 2x)$ for any $(a, x) \in Q$. Then f is an automorphism of $Q(+)$ and we can define a multiplication on Q by $pq = f(p) + q$ for all $p, q \in Q$. Clearly, Q becomes a quasigroup and $\mathrm{A}(Q) = \{((a, 0), (b, y), (c, z));\ a, b, c \in Z_2, y, z \in G\}$.

As a consequence we get

$$2n^2 \in \operatorname{assspec}(n),$$
$$\mathrm{a}_{\min}(n) \leqq 2n^2,$$
$$\mathrm{b}_{\max}(n) \geqq n^3 - 2n^2$$

for every number $n \geqq 6$ such that $n = 4k + 2$ for some k.

3. The group distance and the numbers $\mathrm{b}_{\min}(n)$

Let $Q(*)$ and $Q(\circ)$ be two quasigroups with the same underlying set Q. We put $\operatorname{dist}(Q(*), Q(\circ)) = \operatorname{card}(\{(x, y) \in Q^2;\ x * y \neq x \circ y\})$. This cardinal number is called the distance of the two quasigroups; it is easy to see that it is not less than 4, provided that the two quasigroups are different.

For a quasigroup Q denote by gdist (Q) the minimum of the numbers dist $(Q, Q(*))$, $Q(*)$ being an arbitrary group with underlying set Q. Clearly, gdist $(Q) = 0$ iff Q is a group.

For $n \geqq 3$, let gdist (n) designate the minimum of the numbers gdist (Q), where Q is a nonassociative quasigroup of order n; further, put gdist $(2) = 4$. Obviously, if $m \geqq 2$ and if m divides n then gdist $(n) \leqq$ gdist (m). In particular, gdist $(n) \leqq$ $\leqq$ gdist (p), p being the least prime number dividing n, and we have gdist $(n) = 4$ for every even number n. Using mechanical means (or making a tedious handwork), one can establish

$$\text{gdist}(3) = 6\,, \quad \text{gdist}(5) = 8\,, \quad \text{gdist}(7) = 9\,, \quad \text{gdist}(11) = 11\,.$$

By [2], we have $e \ln p + 3 <$ gdist (p) and according to a private communication of A. Drápal, gdist $(p) < 4\sqrt{p}$ for every prime number $p \geqq 3$.

A. Drápal has found in [1] some connections between the numbers $\mathrm{b}(Q)$ and gdist (Q). Namely, he proved the following two propositions.

3.1. Proposition. Let Q be a finite quasigroup of order n; put $b = \mathrm{b}(Q)$ and $g =$ $=$ gdist (Q). Then:

$$\begin{aligned} &4gn - 2g^2 - 24g \leqq b \leqq 4gn\,; \\ &4gn - 2g^2 - 16g \leqq b\,, \quad \text{provided that} \quad g \geqq 24\,; \\ &3gn < b\,, \quad \text{provided that} \quad 1 \leqq b < 3n^2/32\,. \end{aligned}$$

3.2. Proposition. Let $n \geqq 3$; put $b = \mathrm{b}_{\min}(n)$ and $g =$ gdist (n). Then $4ng - 2g^2 -$ $- 24g \leqq b \leqq 4ng$ and $3ng < b$. If $b < 3n^2/32$, $g^2 + 14g + 13 < 2n$ and if Q is a quasigroup of order n such that $\mathrm{b}(Q) = b$ then gdist $(Q) = g$.

3.3. Proposition. Let $n \geqq 3$ be such that gdist $(n) < 3n/128$. Then $\mathrm{b}_{\min}(n) < 3n^2/32$.

Proof. Put $g =$ gdist (n). Let Q be a quasigroup of order n such that gdist $(Q) = g$. By 3.1 (1), $\mathrm{b}_{\min}(n) \leqq \mathrm{b}(Q) \leqq 4gn$. Since $g < 3n/128$, we have $4gn < 3n^2/32$.

3.4. Proposition. Let $n \geqq 29\,124$. Then $\mathrm{b}_{\min}(n) < 3n^2/32$.

Proof. If $n \geqq 29\,128$ then $4\sqrt{n} < 3n/128$ and the result follows from 3.3. The number 29 127 is divisible by 3, the number 29 125 by 5 and the numbers 29 126 and 29 124 are even.

3.5. Proposition. Let $n \geqq 29\,124$ be not a prime number and let Q be a quasigroup of order n such that $\mathrm{b}(Q) = \mathrm{b}_{\min}(n)$. Then gdist $(Q) =$ gdist (n).

Proof. By 3.4, $\mathrm{b}_{\min}(n) < 3n^2/32$. Denote by p the least prime number dividing n. Then $p - 1 \leqq 70$ and $16p + 56\sqrt{p} + 13 < 2n$. The result follows from 3.2.

If n is even then a considerably more complete result is known (see [1]):

3.6. Proposition. Let $n \geqq 168$ be even. Then $\mathrm{b}_{\min}(n) = 16n - 64$ and $\mathrm{a}_{\max}(n) =$ $= n^3 - 16n + 64$.

3.7. Proposition. Let $n \geqq 194$ be even and let Q be a quasigroup of order n such that $\mathrm{b}(Q) \leqq 18n$. Then $\mathrm{b}(Q) \in \{0, 16n - 64, 16n - 56, 16n - 48, 16n - 36, 16n - - 32\}$.

Proof. Assume that Q is not a group. We have $\mathrm{b}(Q) \leqq 18n < 3n^2/32$ and so gdist $(Q) < 6$ by 3.1 (3). Now, it is easy to show that gdist $(Q) = 4$ and the result follows from Proposition 10.4 of [1].

3.8. Proposition. Let n be an even number, $6 \leqq n \leqq 166$. Then $3n^2/32 \leqq \mathrm{b}_{\min}(n) \leqq \leqq 16n - 64$.

Proof. The inequality $\mathrm{b}_{\min}(n) \leqq 16n - 64$ follows from 2.1. Now, let Q be a quasigroup of order n with $b = \mathrm{b}(Q) = \mathrm{b}_{\min}(n)$. Suppose that $b < 3n^2/32$. By 3.1 (3), $g = \text{gdist}\,(Q) < n/32$. Since $g \geqq 4$, we have $n \geqq 130$. We have gdist $(n) = 4$ and $g = 4$ by 3.2. By Proposition 10.4 of [1] we get $b \geqq 16n - 64$, a contradiction.

3.9. Remark. By 3.8, $2584 \leqq \mathrm{b}_{\min}(166) \leqq 2592$. Let Q be a quasigroup of order 166 with $\mathrm{b}(Q) = \mathrm{b}_{\min}(166)$. Then either gdist $(Q) = 4$ (and then $\mathrm{b}_{\min}(166) = 2592$) or gdist $(Q) \geqq 320$ (use 3.1).

3.10. Remark. We have $\mathrm{b}_{\min}(6) = 27$, so that 3.6 is not true for $n = 6$. The situation for $8 \leqq n \leqq 166$ is not clear.

3.11. Remark. In contrast to the numbers $b_{\min}(n)$ and $\mathrm{a}_{\max}(n)$, almost nothing is known about the numbers $\mathrm{a}_{\min}(n)$. It follows from 2.2 and 2.3 that

$$n \leqq \mathrm{a}_{\min}(n) \leqq n^2 \quad \text{for} \quad n \geqq 3\,, \quad n \neq 4k + 2\,,$$
$$n \leqq \mathrm{a}_{\min}(n) \leqq 2n^2 \quad \text{for every} \quad n \geqq 3\,.$$

It is not clear whether $n < \mathrm{a}_{\min}(n)$ for every $n \geqq 3$. By [3], if Q is a quasigroup of order $n \geqq 3$ such that $\mathrm{a}(Q) = n$, then Q is idempotent and not isotopic to a group.

References

[1] DRÁPAL A.: On quasigroups rich in associative triples. Discrete Math. 44 (1983), 251—365.

[2] DRÁPAL A., KEPKA T.: On a distance of quasigroups and groups. (To appear).

[3] KEPKA T.: A note on the associative triples of elements in cancellation groupoids. Comment. Math. Univ. Carolinae 21 (1980), 479—487.