NOTES ON THE NUMBER OF ASSOCIATIVE TRIPLES

J. Ježek and T. Kepka

1. INTRODUCTION

For a quasigroup Q, let

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

$B(Q) = Q^3 - A(Q)$, $\quad b(Q) = \mathrm{card}(B(Q))$.

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

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

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

$\mathrm{assspec}(1) = \{1\}$,
$\mathrm{assspec}(2) = \{8\}$,
$\mathrm{assspec}(3) = \{9, 27\}$,
$\mathrm{assspec}(4) = \{16, 24, 32, 64\}$,
$\mathrm{assspec}(5) = \{15, \dots, 57, 59, 62, 63, 74, 79, 80, 89, 125\}$,
$\mathrm{assspec}(6) = \{16, 19, \dots, 114, 116, 117, 118, 120, 121, 122, 124, \dots, 128, 130, \dots, 137, 141, 142, 144, 148, 152, 160, 162, 168, 172, 184, 189, 216\}$.

Hence

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

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 1128960 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 nonidempotent 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 $a(Q) = 189$:

Typeset by $\mathcal{AMS}$-TEX

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 $n \geq 4$ 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 $\mathrm{b}(a+b) = (a+b)b = 2b$. It is easy to verify that Q is a commutative loop and that $(x, y, z) \in \mathrm{B}(Q)$ 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

$$n^3 - 16n + 64 \in \mathrm{assspec}(n),$$

$$\mathrm{b}_{min}(n) \leq 16n - 64,$$

$$\mathrm{a}_{max}(n) \geq n^3 - 16n + 64$$

for any even number $n \geq 6$.

2.2.EXAMPLE. Let $n \geq 3$ 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 even number, take $Q(+) = C_1(+) \times \cdots \times C_m(+) \times D(+)$ where C_i is the two-element group and D is the cyclic group of order d and put $f(x_1, \dots, x_m, y) = (x_1 + x_2, x_3, \dots, x_m, x_1, 2y)$. 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

$$n^2 \in \mathrm{assspec}(n),$$

$$\mathrm{a}_{min}(n) \leq n^2,$$

$$\mathrm{b}_{max}(n) \geq n^3 - n^2$$

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

2.3.EXAMPLE. Let $G(+)$ be an abelian group of an odd order $m \geq 3$ 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 $\mathrm{A}(Q) = \{((a, 0), (b, y), (c, z)); a, b, c \in Z_2, \quad y, z \in G\}$.

As a consequence we get

$$2n^2 \in \mathrm{assspec}(n),$$

$$\mathrm{a}_{min}(n) \leq 2n^2,$$

$$\mathrm{b}_{max}(n) \geq n^3 - 2n^2$$

for every number $n \geq 6$ 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 $\mathrm{dist}(Q(*), Q(\circ)) = \mathrm{card}(\{(x, y) \in Q^2; x*y \neq x\circ y\})$. 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 $\mathrm{gdist}(Q)$ the minimum of the numbers $\mathrm{dist}(Q, Q(*))$, $Q(*)$ being an arbitrary group with underlying set Q. Clearly, $\mathrm{gdist}(Q) = 0$ iff Q is a group.

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

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

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

A. Drápal has found in [1] some connections between the numbers $\mathrm{b}(Q)$ and $\mathrm{gdist}(Q)$. 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 $g = \mathrm{gdist}(Q)$. Then:*

$4gn - 2g^2 - 24g \leq b \leq 4gn$;
$4gn - 2g^2 - 16g \leq b$, *provided that* $g \geq 24$;
$3gn < b$, *provided that* $1 \leq b < 3n^2/32$.

3.2.PROPOSITION. *Let $n \geq 3$; put $b = \mathrm{b}_{min}(n)$ and $g = \mathrm{gdist}(n)$. Then $4ng - 2g^2 - 24g \leq b \leq 4ng$ 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 $\mathrm{gdist}(Q) = g$.*

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

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

3.4.PROPOSITION. *Let $n \geq 29124$. Then $\mathrm{b}_{min}(n) < 3n^2/32$.*

Proof. If $n \geq 29128$ then $4\sqrt{n} < 3n/128$ and the result follows from 3.3. The number 29127 is divisible by 3, the number 29125 by 5 and the numbers 29126 and 29124 are even.

3.5.PROPOSITION. *Let $n \geq 29124$ be not a prime number and let Q be a quasigroup of order n such that $\mathrm{b}(Q) = \mathrm{b}_{min}(n)$. Then $\mathrm{gdist}(Q) = \mathrm{gdist}(n)$.*

Proof. By 3.4, $\mathrm{b}_{min}(n) < 3n^2/32$. Denote by p the least prime number dividing n. Then $p1 \leq 70$ 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 $n \geq 168$ be even. Then $\mathrm{b}_{min}(n) = 16n - 64$ and $\mathrm{a}_{max}(n) = n^3 - 16n + 64$.*

3.7.PROPOSITION. *Let $n \geq 194$ be even and let Q be a quasigroup of order n such that $\mathrm{b}(Q) \leq 18n$. 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 $\mathrm{b}(Q) \leq 18n < 3n^2/32$ and so $\mathrm{gdist}(Q) < 6$ by 3.1(3). Now, it is easy to show that $\mathrm{gdist}(Q) = 4$ and the result follows from Proposition 10.4 of [1].

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

Proof. The inequality $\mathrm{b}_{min}(n) \leq 16n - 64$ 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), $g = \mathrm{gdist}(Q) < n/32$. Since $g \geq 4$, we have $n \geq 130$. We have $\mathrm{gdist}(n) = 4$ and $g = 4$ by 3.2. By Proposition 10.4 of [1] we get $b \geq 16n - 64$, a contradiction.

3.9.REMARK. By 3.8, $2584 \leq \mathrm{b}_{min}(166) \leq 2592$. Let Q be a quasigroup of order 166 with $\mathrm{b}(Q) = \mathrm{b}_{min}(166)$. Then either $\mathrm{gdist}(Q) = 4$ (and then $\mathrm{b}_{min}(166) = 2592$) or $\mathrm{gdist}(Q) \geq 320$ (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 $8 \leq n \leq 166$ is not clear.

3.11.REMARK. In contrast to the numbers $\mathrm{b}_{min}(n)$ 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

$n \leq \mathrm{a}_{min}(n) \leq n^2$ for $n \geq 3, n \neq 4k+2$,

$n \leq \mathrm{a}_{min}(n) \leq 2n^2$ for every $n \geq 3$.

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

References

[1] A. Drápal: On quasigroups rich in associative triples. Discrete Math. 44(1983), 251-265.

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

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