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


Persistent URL: [http://dml.cz/dmlcz/142611](http://dml.cz/dmlcz/142611)

**Terms of use:**

© Univerzita Karlova v Praze, 1990

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
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.

Diskutuji 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

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

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

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

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

For every $n \geq 1$ denote by $\text{assspec } (n)$ 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 $\{n, n + 1, \ldots, n^3\}$. We have $\text{asspec } (1) = \{1\}$.

*) Department of Mathematics, Charles University, 186 00 Praha 8, Sokolovská 83, Czechoslovakia.
assspec (2) = \{8\},  
assspec (3) = \{9, 27\},  
assspec (4) = \{16, 24, 32, 64\},  
assspec (5) = \{15, ..., 57, 59, 62, 63, 74, 79, 80, 89, 125\},  
assspec (6) = \{16, 19, ..., 114, 116, 117, 118, 120, 121, 122, 124, ..., 128, 130, ..., 137, 141, 142, 144, 148, 152, 160, 162, 168, 172, 184, 189, 216\}. 

Hence

\[
\begin{align*}
\text{a}_{\text{min}}(3) &= \text{a}_{\text{max}}(3) = 9, \\
\text{a}_{\text{min}}(4) &= 16, \quad \text{a}_{\text{max}}(4) = 32, \\
\text{a}_{\text{min}}(5) &= 15, \quad \text{a}_{\text{max}}(5) = 89, \\
\text{a}_{\text{min}}(6) &= 16, \quad \text{a}_{\text{max}}(6) = 189.
\end{align*}
\]

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 \(a(Q) = 189:\)

\[
\begin{array}{cccccc}
H & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
1 & 2 & 1 & 4 & 3 & 5 & 6 \\
2 & 1 & 2 & 5 & 6 & 4 & 3 \\
3 & 6 & 5 & 1 & 2 & 3 & 4 \\
4 & 5 & 6 & 3 & 4 & 1 & 2 \\
5 & 4 & 3 & 2 & 1 & 6 & 5 \\
6 & 3 & 4 & 6 & 5 & 2 & 1
\end{array}
\quad
\begin{array}{cccccc}
Q & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
1 & 2 & 3 & 1 & 5 & 6 & 4 \\
2 & 3 & 1 & 2 & 6 & 4 & 5 \\
3 & 1 & 2 & 3 & 4 & 5 & 6 \\
4 & 6 & 5 & 1 & 3 & 2 & 4 \\
5 & 4 & 6 & 5 & 2 & 1 & 3 \\
6 & 5 & 4 & 6 & 3 & 2 & 1
\end{array}
\]

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 \(b(a + b) = (a + b)b = 2b\). 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 \( z \not\in \{0, a, b, a + b\} \) 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 \( b(Q) = 16n - 64 \).

As a consequence we get

\[
\begin{align*}
n^3 - 16n + 64 & \in \text{assspec}(n), \\
b_{\min}(n) & \leq 16n - 64, \\
a_{\max}(n) & \geq n^3 - 16n + 64
\end{align*}
\]

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 \( f(x) = x \) 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 \( A(Q) = \{(x, y, x); x, y \in Q\} \).

As a consequence we get

\[
\begin{align*}
n^2 & \in \text{assspec}(n), \\
a_{\min}(n) & \leq n^2, \\
b_{\max}(n) & \geq n^3 - n^2
\end{align*}
\]

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 \( A(Q) = \{((a, 0), (b, y), (c, z)); a, b, c \in Z_2, y, z \in G\} \).

As a consequence we get

\[
\begin{align*}
2n^2 & \in \text{assspec}(n), \\
a_{\min}(n) & \leq 2n^2, \\
b_{\max}(n) & \geq n^3 - 2n^2
\end{align*}
\]

for every number \( n \geq 6 \) such that \( n = 4k + 2 \) for some \( k \).

### 3. The group distance and the numbers \( b_{\min}(n) \)

Let \( Q(*) \) and \( Q(\circ) \) be two quasigroups with the same underlying set \( Q \). We put \( \text{dist}(Q(*), Q(\circ)) = \text{card}\{\{(x, y) \in Q^2; x * y \neq x \circ y\}\} \). 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 $\text{gdist} (Q)$ the minimum of the numbers $\text{dist} (Q, Q(\ast))$, $Q(\ast)$ being an arbitrary group with underlying set $Q$. Clearly, $\text{gdist} (Q) = 0$ iff $Q$ is a group.

For $n \geq 3$, let $\text{gdist} (n)$ designate the minimum of the numbers $\text{gdist} (Q)$, where $Q$ is a nonassociative quasigroup of order $n$; further, put $\text{gdist} (2) = 4$. Obviously, if $m \geq 2$ and if $m$ divides $n$ then $\text{gdist} (n) \leq \text{gdist} (m)$. In particular, $\text{gdist} (n) \leq \text{gdist} (p)$, $p$ being the least prime number dividing $n$, and we have $\text{gdist} (n) = 4$ 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 $e \ln p + 3 < \text{gdist} (p)$ and according to a private communication of A. Drápal, $\text{gdist} (p) < 4 \sqrt{p}$ for every prime number $p \geq 3$.

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

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

$$
4gn - 2g^2 - 24g \leq b \leq 4gn;
$$

$$
4gn - 2g^2 - 16g \leq b, \quad \text{provided that} \quad g \geq 24;
$$

$$
3gn < b, \quad \text{provided that} \quad 1 \leq b < 3n^2/32.
$$

3.2. Proposition. Let $n \geq 3$; put $b = b_{\min}(n)$ and $g = \text{gdist} (n)$. 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 $b(Q) = b$ then $\text{gdist} (Q) = g$.

3.3. Proposition. Let $n \geq 3$ be such that $\text{gdist} (n) < 3n/128$. Then $b_{\min}(n) < 3n^2/32$.

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

3.4. Proposition. Let $n \geq 29 124$. Then $b_{\min}(n) < 3n^2/32$.

Proof. If $n \geq 29 128$ 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 $n \geq 29 124$ be not a prime number and let $Q$ be a quasigroup of order $n$ such that $b(Q) = b_{\min}(n)$. Then $\text{gdist} (Q) = \text{gdist} (n)$.

Proof. By 3.4, $b_{\min}(n) < 3n^2/32$. Denote by $p$ the least prime number dividing $n$. Then $p - 1 \leq 70$ 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 $b_{\min}(n) = 16n - 64$ and $a_{\max}(n) = n^3 - 16n + 64$.  

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

Proof. Assume that \( Q \) is not a group. We have \( b(Q) \leq 18n < 3n^2/32 \) and so \( \text{gdist}(Q) < 6 \) by 3.1 (3). Now, it is easy to show that \( \text{gdist}(Q) = 4 \) 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 \( 3n^2/32 \leq b_{\min}(n) \leq 16n - 64 \).

Proof. The inequality \( b_{\min}(n) \leq 16n - 64 \) follows from 2.1. Now, let \( Q \) be a quasigroup of order \( n \) with \( b = b(Q) = b_{\min}(n) \). Suppose that \( b < 3n^2/32 \). By 3.1 (3), \( g = \text{gdist}(Q) < n/32 \). Since \( g \geq 4 \), we have \( n \geq 130 \). We have \( \text{gdist}(n) = 4 \) 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, \( 2584 \leq b_{\min}(166) \leq 2592 \). Let \( Q \) be a quasigroup of order \( 166 \) with \( b(Q) = b_{\min}(166) \). Then either \( \text{gdist}(Q) = 4 \) (and then \( b_{\min}(166) = 2592 \)) or \( \text{gdist}(Q) \geq 320 \) (use 3.1).

3.10. Remark. We have \( b_{\min}(6) = 27 \), 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 \( b_{\min}(n) \) and \( a_{\max}(n) \), almost nothing is known about the numbers \( a_{\min}(n) \). It follows from 2.2 and 2.3 that

\[
\begin{align*}
    n \leq a_{\min}(n) & \leq n^2 \quad \text{for} \quad n \geq 3, \quad n \neq 4k + 2, \\
    n \leq a_{\min}(n) & \leq 2n^2 \quad \text{for every} \quad n \geq 3.
\end{align*}
\]

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

References