m-medial n-quasigroups

Tomáš Kepka

Abstract. For $n \geq 4$, every n-medial n-quasigroup is medial. If $1 \leq m < n$, then there exist m-medial n-quasigroups which are not $(m+1)$-medial.

Keywords: n-quasigroup, medial

Classification: 20N15

Idempotent symmetric 3-medial 2-quasigroups (also known as distributive Steiner quasigroups, idempotent Manin quasigroups, Hall triple systems, affine triple systems, planarily affine Steiner–Kirkman (2, 3)-systems, etc., etc.) possess many interesting algebraical, geometrical and combinatorial properties (see e.g. [1], [2], [5] for some of them). Similarly, idempotent symmetric 3-quasigroups corresponding to Steiner–Kirkman (3, 4)-systems, are 3-medial and, certainly, they are of some combinatorial interest. On the other hand, it is not clear whether the same applies to the general case of m-medial n-quasigroups, $1 \leq m \leq n^2$. In the present note, an investigation is started in this respect. It is shown that every n-medial n-quasigroup is medial for $n \geq 4$ and that for every $1 \leq m < n$ there exist m-medial n-quasigroups which are not $(m+1)$-medial.

1. Introduction.

An n-groupoid, where $n \geq 1$, is a non-empty set together with an n-ary operation (usually denoted multiplicatively). If G is an n-groupoid, $1 \leq i \leq n$ and $a = (a_1, \dots, a_{n-1}) \in G^{n-1}$, then we put $T_{i,a}(x) = a_1 \dots a_{i-1} x a_i \dots a_{n-1}$ for each $x \in G$. This transformation $T_{i,a}$ of G is called the i-th translation of G by a.

An n-groupoid G is said to be

- idempotent, if $x \dots x = x$ for each $x \in G$;
- commutative, if $x_1 \dots x_n = x_{p(1)} \dots x_{p(n)}$ for all $x_1, \dots, x_n \in G$ and any permutation p of $\{1, 2, \dots, n\}$;
- medial, if $(x_{11} \dots x_{1n})(x_{21} \dots x_{2n}) \dots (x_{n1} \dots x_{nn}) = (x_{11} \dots x_{n1})(x_{12} \dots x_{n2}) \dots (x_{1n} \dots x_{nn})$ for all $x_{ij} \in G$, $1 \leq i, j \leq n$;
- m-medial, where $1 \leq m$, if every subgroupoid of G generated by at most m elements is medial;
- symmetric if all the translations of G are involutions;
- an n-quasigroup if all the translations of G are permutations.

The following result is well known (see e.g. [6]):

Proposition 1.1. *Let $n \geq 2$. The following conditions are equivalent for an n-groupoid G:*

(i) *G is a medial n-quasigroup.*
(ii) *There exist an abelian group $G(+)$, pair-wise commuting automorphisms $f_1, \dots, f_n$ of the group and an element $s \in G$ such that $x_1 \dots x_n = f_1(x_1) + \dots + f_n(x_n) + s$ for all $x_1, \dots, x_n \in G$.*

For $n \geq 1$, let R_n designate the polynomial ring $Z[\alpha_1, \dots \alpha_n, \alpha_1^{-1}, \dots \alpha_n^{-1}]$.

Proposition 1.2. *Let $n \geq 2$. The following conditions are equivalent for an n-groupoid G:*
(i) *G is a medial n-quasigroup.*
(ii) *There exist an R_n-module $G(+, \alpha x)$ and an element $s \in G$ such that $x_1 \dots x_n = \alpha_1 x_1 + \dots + \alpha_n x_n + s$ for all $x_1, \dots, x_n \in G$.*

Proof: If the condition (i) is satisfied, one may define a scalar multiplication on $G(+)$ (see 1.1) whose domain of operators is R_n by setting $\alpha_i \cdot x = f_i(x)$. $\square$

Proposition 1.3. *Let $n \geq 2$. The following conditions are equivalent for an n-groupoid G:*
(i) *G is idempotent, symmetric and medial.*
(ii) *There exists an abelian group $G(+)$ such that $(n+1)x = 0$ and $x_1 \dots x_n = -x_1 - \dots - x_n = n(x_1 + \dots + x_n)$ for all $x, x_1, \dots, x_n \in G$.*

Proof: Let (i) be satisfied. First of all, $0 = 0 \dots 0 = s$. Next, $0 = b0 \dots 0(b0 \dots 0)$ $= \alpha_1 b + \alpha_n \alpha_1 b = a + \alpha_n a$, $b = \alpha_1^{-1} a$, $\alpha_n a = -a$ and $\alpha_n = -1$. Similarly, $\alpha_1 = \dots = \alpha_{n-1} = -1$. $\square$

2. Auxiliary results.

In this section, let Q be an n-quasigroup, where $n \geq 2$, and let $a_1, \dots, a_n \in Q$. Put $f = T_{1,u}$, $g = T_{2,v}$, $u = (a_2, a_3, \dots, a_n)$, $v = (a_1, a_3, \dots, a_n)$ and $x \circledast y = f^{-1}(x) g^{-1}(y) a_3 \dots a_n$ for all $x, y \in Q$. It is easy to check that the 2-groupoid $Q(\circledast)$ is a loop and $e = a_1 a_2 \dots a_n$ is its neutral element.

Observation 2.1. Let P be a subquasigroup of the n-quasigroup Q and suppose that $a_1, \dots, a_n \in P$ and P is medial. By 1.2 (ii) there exist an R_n-module $P(+, \alpha x)$ and an element $s \in P$ such that $x_1 \dots x_n = \alpha_1 x_1 + \dots + \alpha_n x_n + s$ for all $x_1, \dots, x_n \in P$. Now, $f^{-1}(x) = \alpha_1^{-1} x - \alpha_1^{-1} \alpha_2 a_2 - \dots - \alpha_1^{-1} \alpha_n a_n - \alpha_1^{-1} s$ and $g^{-1}(y) = \alpha_2^{-1} y - \alpha_2^{-1} \alpha_1 a_1 - \alpha_2^{-1} \alpha_3 a_3 - \dots - \alpha_2^{-1} \alpha_n a_n - \alpha_2^{-1} s$, and hence $x \circledast y = x - \alpha_2 a_2 - \dots - \alpha_n a_n - s + y - \alpha_1 a_1 - \alpha_3 a_3 - \dots - \alpha_n a_n - s + \alpha_3 a_3 + \dots + \alpha_n a_n + s = x + y - \alpha_1 a_1 - \alpha_2 a_2 - \dots - \alpha_n a_n - s = x + y - e$ for all $x, y \in P$. We have shown that

$$x \circledast y = x + y - e \tag{2.1.1}$$

for all $x, y \in P$.

Lemma 2.2. *Let $a, b, c \in Q$ be such that the subquasigroup generated by $a, b, c, a_1, \dots, a_n$ is medial. Then $a \circledast b = b \circledast a$ and $a \circledast (b \circledast c) = (a \circledast b) \circledast c$.*

Proof: This follows easily from (2.1.1). $\square$

Now, put $w = ee \dots e$ and denote by z the unique element of Q such that $w \circledast z = e$. For $1 \le i \le n$ and $x \in Q$, let $g_i(x) = (ee \dots exe \dots e) \circledast z$, where x is on the i-th position. Clearly, these transformations g_i are permutations.

Observation 2.3. Consider the situation from 2.1. Then $e = w \circledast z = w + z - e$, and so $w + z = 2e$. Further, $ee \dots exe \dots e = w - \alpha_i e + \alpha_i x$ and we have $g_i(x) = w - \alpha_i e + \alpha_i x + z - e = \alpha_i x - \alpha_i e + e$. Thus

$$g_i(x) = \alpha_i(x - e) + e \tag{2.1.2}$$

for all $1 \le i \le n$ and $x \in P$.

Lemma 2.4. *Let $a, b \in Q$ be such that the subquasigroup generated by $a, b, a_1, \dots, a_n$ is medial. Then $g_i(a \circledast b) = g_i(a) \circledast g_i(b)$ for every $1 \le i \le n$.*

Proof: This follows easily from (2.1.) and (2.1.2). □

Lemma 2.5. *Let $a \in Q$ be such that the subquasigroup generated by $a, a_1, \dots, a_n$ is medial. Then $g_i g_j(a) = g_j g_i(a)$ for all $1 \le i, j \le n$.*

Proof: This follows easily from (2.1.2). □

Lemma 2.6. *Let P be a medial subquasigroup of Q such that $a_1, \dots, a_n \in P$. Then $P(\circledast)$ is an abelian group and $g_i \mid P$ are pair-wise commuting automorphisms of $P(\circledast)$.*

Proof: Use 2.2, 2.3 and 2.4. □

Lemma 2.7. *Let P be a medial subquasigroup of Q such that $a_1, \dots, a_n \in P$. Then $u_1 \dots u_n = g_1(u_1) \circledast \dots \circledast g_n(u_n) \circledast w$ for all $u_1, \dots, u_n \in P$.*

Proof: By (2.1.1) and (2.1.2), $g_1(u_1 \circledast \dots \circledast g_n(u_n) \circledast w = (\alpha_1(u_1 - e) + e) \circledast \dots \circledast (\alpha_n(u_n - e) + e) \circledast w = \alpha_1 u_1 + \dots + \alpha_n u_n - \alpha_1 e - \dots - \alpha_n e + ne + w - ne = \alpha_1 u_1 + \dots + \alpha_n u_n + s = u_1 \dots u_n$, since $w = \alpha_1 e + \dots + \alpha_n e + s$. □

3. Auxiliary results.

In this section, let Q be a 4-medial n-quasigroup, where $n \ge 2$. For every $a \in Q$, let $u_a = (a, a, \dots, a) \in Q^{(n-1)}$, $f_a = T_{1,u_a}$, $g_a = T_{2,u_a}$, $e_a = aa \dots a \in Q$ and $xo_a y = f_a^{-1}(x) g_a^{-1}(y) a \dots a$ for all $x, y \in Q$. By 2.2, $Q(o_a)$ is an abelian group and e_a is its neutral element.

Further, let $w_a = e_a e_a \dots e_a$, $w_a o_a z_a = e_a$ and let $g_{i,a}(x) = (e_a e_a \dots e_a x e_a \dots e_a)$ $o_a z_a$, $1 \le i \le n$. By 2.4 and 2.5, $g_{i,a}$ are pair-wise commuting automorphisms of $Q(o_a)$, and hence they induce a structure of an R_n-module on $Q(o_a)$. We denote by $(\alpha, x) \longrightarrow q_a x$ the corresponding scalar multiplication, so that $\alpha_i q_a x = g_{i,a}(x)$.

Lemma 3.1. *$xo_b y = xo_a(e_a o_b e_a)$ for all $a, b, x, y \in Q$.*

Proof: Denote by P the subquasigroup generated by x, y, a, b. Then P is medial and let $P(+, \alpha x, s)$ be a corresponding pointed R_n-module (see 1.2). By (2.1.1), $uo_a v = u + v - e_a$ and $uo_b v = u + v - e_b$ for all $u, v \in P$. Hence $xo_a yo_a(e_a o_b e_a) = x + y + 2e_a - 2e_a - e_b = x + y - e_b = xo_b y$. □

Lemma 3.2. *$\alpha_i q_b x = (\alpha_i q_a x) o_a (\alpha_i q_b e_a)$ for all $a, b, x \in Q$ and $1 \le i \le n$.*

PROOF: Let P be the subquasigroup generated by x, a, b and consider a corresponding pointed R_n-module $P(+, \alpha x, s)$. By (2), $\alpha_i q_a u = \alpha_i u - \alpha_i e_a + e_a$ and $\alpha_i q_b u = \alpha_i u - \alpha_i e_b + e_b$ for each $u \in P$. Consequently, $(\alpha_i q_a x) o_a (\alpha_i q_b e_a) = \alpha_i x - \alpha_i e_a + e_a) o_a (\alpha_i e_a - \alpha_i e_b + e_b) = \alpha_i x - \alpha_i e_a + e_a + \alpha_i e_a - \alpha_i e_b + e_b - e_a = \alpha_i x - \alpha_i e_b + e_b = \alpha_i q_b x$. □

In the remaining part of this section, suppose that Q is n-medial. Further, let $a \in Q, e = e_a, w = w_a, \divideontimes = o_a$ and $o = q_a$.

Lemma 3.3. *There is a transformation h of Q such that $x_1 \dots x_n = (\alpha_1 o x_1) \divideontimes \dots \divideontimes (\alpha_n o x_n) \divideontimes h(x_1)$ for all $x_1, \dots, x_n \in Q$.*

PROOF: Put $b = x_1$ and denote by P the subquasigroup generated by $x_1, \dots, x_n$. Then P is medial and we have $x_1 \dots x_n = (\alpha_1 q_b x_1) o_b \dots o_b (\alpha_n q_b x_n) o_b w_b$ by 2.7. However, by 3.1 and 3.2, we can write $x_1 \dots x_n = (\alpha_1 q_b x_1) \divideontimes \dots \divideontimes (\alpha_n q_b x_n) \divideontimes w_b \divideontimes r$, where $r = (e o_b e) \divideontimes \dots \divideontimes (e o_b e)$ (n-times), and $x_1 \dots x_n = (\alpha_1 o x_1) \divideontimes \dots \divideontimes (\alpha_n o x_n) \divideontimes w_b \divideontimes r \divideontimes t$, where $t = (\alpha_1 q_b e) \divideontimes \dots \divideontimes (\alpha_n q_b e)$. Now, it is enough to put $h(x_1) = h(b) = w_b \divideontimes r \divideontimes t$. □

Lemma 3.4. *$x_1 \dots x_n = (\alpha_1 o x_1) \divideontimes \dots \divideontimes (\alpha_n o x_n) \divideontimes w$ for all $x_1, \dots, x_n \in Q$.*

PROOF: With respect to 3.3, we have to show that $h(y) = w$ for every $y \in Q$. Denote by P the subquasigroup generated by y and a and let $P(+, \alpha x, s)$ be a corresponding pointed module. Then $ye \dots e = (\alpha_1 o y) \divideontimes h(y)$ by 3.3. But $ye \dots e = \alpha_1 y + \alpha_2 e + \dots + \alpha_n e + s$ and $(\alpha_1 o y) \divideontimes h(y) = (\alpha_1 o y) + h(y) - e = \alpha_1 y - \alpha_1 e + e + h(y) - e = \alpha_1 y - \alpha_1 e + h(y)$. Thus $h(y) = \alpha_1 e + \dots + \alpha_n e + s = ee \dots e = w$. □

4. Main results.

Construction 4.1. Let $2 \le m \le n$, let p be a prime dividing n and let $Q(+, F)$ be an m-ary ring satisfying the following identities: $px = 0$; $F(x_1, \dots x_m) = 0$ whenever $x_i = x_j$ for some $i < j$; $F(F(x_1, \dots, x_m), y_2, \dots, y_m) = F(y_1, F(x_1, \dots, x_m), y_3, \dots, y_m) = \dots = F(y_1, \dots, y_{m-1}, F(x_1, \dots, x_m)) = 0$. Now define an n-ary operation on Q by $x_1 \dots x_n = x_1 + \dots + x_n + F(x_1, \dots, x_m)$. In this way, we get an n-groupoid Q.

Lemma 4.1.1. *The n-groupoid Q is an $(m-1)$-medial n-quasigroup and $xx \dots x = 0$ for every $x \in Q$.*

PROOF: Let $1 \le i \le n$, $a_1, \dots, a_n \in Q$, $a = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in Q^{(n-1)}$ and $T = T_{i,a}$. Further, let $b = a_1 + \dots + a_{i-1} + a_{i+1} + \dots + a_n$ and $x \in Q$. If $i \le m$, then $T(x) = x + b + F(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_m) = x + b + f(x), T^2(x) = x + 2b + 2f(x) + c$, where $c = F(a_1, \dots, a_{i-1}, a_{m+1} + \dots + a_n, a_{i+1}, \dots, a_m)$, and $T^k(x) = x + kb + kf(x) + (k(k-1)/2)c$ for $k \ge 3$. Consequently, $T^{2p} = id_Q$ ($T^p = id_Q$ provided that p is odd). If $m < i$, then $T(x) = x + b + F(a_1, \dots, a_m)$ and $T^p = id_Q$. We have proved that every translation of Q is a permutation, i.e. Q is an n-quasigroup.

Now, let $a_1, \dots, a_{m-1} \in Q$ and let P be the subgroup generated by these elements in the additive group $Q(+)$ of the m-ary ring. Then $F \mid P^{(m)} = 0$, so that P is a subring as well. However, then P is a subquasigroup which is clearly medial. □

Lemma 4.1.2. *Suppose that $3 \le n$ and $F \ne 0$. Then the n-quasigroup Q is not m-medial.*

PROOF: Let $a_1, \dots, a_m \in Q$ be such that $F(a_1, \dots, a_m) \ne 0$. Denote by P the subquasigroup generated by these elements and suppose that P is medial. Since $a_1 a_1 \dots a_1 = 0$, we have also $0 \in P$. By 1.2, there exists a pointed R_n-module $P(\circledast, \alpha x, s)$ such that $x_1 \dots x_n = \alpha_1 x_1 \circledast \dots \circledast \alpha_n x_n \circledast s$ for all $x_1, \dots, x_n \in P$. Let $e \in P$ be the neutral element of the abelian group $P(\circledast)$. We have $x_1 + \dots + x_n + F(x_1, \dots, x_m) = \alpha_1 x_1 \circledast \dots \circledast \alpha_n x_n \circledast s$ for all $x_1, \dots, x_n \in P$. In particular, $x_1 = \alpha_1 x_1 \circledast \alpha_2 0 \circledast \dots \circledast \alpha_n 0 \circledast s$, $e = e \circledast \alpha_2 0 \circledast \dots \circledast \alpha_n 0 \circledast s$, $e = \alpha_2 0 \circledast \dots \circledast \alpha_n 0 \circledast s$ and $x_1 = \alpha_1 x_1 \circledast e = \alpha_1 x_1$. Similarly, $x_2 = \alpha_2 x_2$, etc., and we have proved that $x_1 + \dots + x_n + F(x_1, \dots, x_m) = x_1 \circledast \dots \circledast x_n \circledast s$. Consequently, $x + y = x \circledast y \circledast 2e$ for all $x, y \in P$, and therefore $x_1 + \dots + x_n + F(x_1, \dots, x_m) = x_1 \circledast \dots \circledast x_n \circledast F(x_1, \dots, x_m) \circledast u$, where $u = 2e \circledast \dots \circledast 2e$ (n-times). Now, we conclude that $x_1 \circledast \dots \circledast x_n \circledast s = x_1 \circledast \dots \circledast x_n \circledast F(x_1, \dots, x_m) \circledast u$, $s = F(x_1, \dots, x_m) \circledast u$ and $F \mid P^{(m)}$ is constant. Since $0 \in P$, $F \mid P^{(m)} = 0$, a contradiction. □

Example 4.2. Let $2 \le m \le n, 3 \le n$, let p be the least prime dividing n and let $q = Z_p^{(m+1)}$. For $x_i = (x_{ij}) \in Q, 1 \le i \le m, 1 \le j \le m+1$, put $F(x_1, \dots, x_m) = (0, \dots, 0\ det\, X) \in Q$, $X = (x_{rs)}, _{1 \le r,s \le m}$. Then $Q(+, F)$ is an m-ary ring satisfying the identities from 4.1 and $F \ne 0$. Now, the corresponding n-quasigroup (see 4.1) is $(m-1)$-medial but not m-medial.

Theorem 4.3. *Let $n \ge 4$.*

(i) *If $m \ge n$, then every m-medial n-quasigroup is medial.*
(ii) *If $1 \le m < n$, then there exists an m-medial n-quasigroup which is not $(m+1)$-medial.*

PROOF: (i) This follows from 3.4 and 1.2.
(ii) See 4.2. □

Example 4.4. Let $n \ge 3$ and $Q = Z_2^{(n+1)}$. Define an n-ary ring $Q(+, F)$ in the same way as in 4.2 and consider the corresponding n-quasigroup Q. Then Q is $(n-1)$-medial. For $n \ge 4$, Q is not n-medial and for $n = 3$, Q is 3-medial and not 4-medial. For n odd, Q is idempotent and symmetric.

Remark 4.5. By 3.4, every m-medial 3-quasigroup is medial for $m \ge 4$. On the other hand, by 4.2 and 4.4, for every $1 \le m \le 3$ there exists an m-medial 3-quasigroup which is not $(m+1)$-medial.

Remark 4.6. Obviously, for $m \ge 4$, every m-medial 2-quasigroup is medial and it is easy to show that, for $m = 1, 2$, there exists an m-medial 2-quasigroup which is not $(m+1)$-medial. As concerns the 3-medial 2-quasigroups, the following example is well known (see [4]): Let $Q = Z_3^{(4)}$ and $x \circledast y = -x - y + (0, 0, 0, x_1 x_3 y_2 - x_2 x_3 y_1 -$

$x_1y_2y_3 + x_2y_1y_3)$ for all $x, y \in 0$. Then $Q(\circledast)$ is an idempotent symmetric 3-medial 2-quasigroup and it is not medial. By [7], every non-medial 3-medial 2-quasigroup contains at least 81 elements and, by [3], there exist up to isomorphism just 35 non-medial 3-medial 2-quasigroups of order 81.

Remark 4.7. Every 1-groupoid, and hence every 1-quasigroup, is medial.

References

[1] Bénéteau L., *Free commutative Moufang loops and anticommutative graded rings*, J. Algebra **67** (1980), 1–35.

[2] Bénéteau L., *Une classe particulière de matroïdes parfaits*, Annals of Discr. Math. **8** (1980), 229–232.

[3] Bénéteau L., Kepka t., Lacaze J., *Small finite trimedial quasigroups*, Commun. Algebra **14** (1986), 1067–1090.

[4] Bol G., *Gewebe und Gruppen*, Math. Ann. **114** (1937), 414–431.

[5] Deza M., Hamada N., *The geometric structure of a matroid design derived from some commutative Moufang loops and a new MDPB association scheme*, Techn. report nr. 18, Statistic Research group, Hiroshima Univ., 1980.

[6] Evans T., *Abstract mean values*, Duke Math. J. **30** (1963), 331–347.

[7] Kepka T., *Structure of triabelian quasigroups*, Comment. Math. Univ. Carolinae **17** (1976), 229–240.

Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 00 Praha 8, Czechoslovakia

(*Received* September 24, 1990)