Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica

Alena Vanžurová

Medial quasigroups of type (n, k)

Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica, Vol. 49 (2010), No. 2, 107--122

Persistent URL: `http://dml.cz/dmlcz/141421`

Acta Univ. Palacki. Olomuc., Fac. rer. nat.,
Mathematica **49**, 2 (2010) 107–122

Medial Quasigroups of Type (n, k)*

Alena VANŽUROVÁ

Department of Algebra and Geometry, Faculty of Science, Palacký University
17. listopadu 12, 771 46 Olomouc, Czech Republic
e-mail: alena.vanzurova@upol.cz
and
Brno University of Technology Faculty of Civil Engineering, Dept. of Math.,
Veveri 331/95, 602 00 Brno, Czech Republic
e-mail: vanzurova.a@fce.vutbr.cz

(Received December 8, 2009)

Abstract

Our aim is to demonstrate how the apparatus of groupoid terms (on two variables) might be employed for studying properties of parallelism in the so called (n, k)-quasigroups. We show that an incidence structure associated with a medial quasigroup of type (n, k), $n > k \geq 3$, is either an affine space of dimension at least three, or a desarguesian plane. Conversely, if we start either with an affine space of order $k > 2$ and dimension m, or with a desarguesian affine plane of order $k > 2$ then there is a medial quasigroup of type (k^m, k), $m > 2$ such that the incidence structure naturally associated to a quasigroup is isomorphic with the starting one (the simplest case $k = 2$ can be examined separately but is of little interest). The proofs are mostly based on properties of groupoid term functions, applied to idempotent medial quasigroups (idempotency means that $x \cdot x = x$ holds, and mediality means that the identity $(xy)(uv) = (xu)(yv)$ is satisfied).

Key words: Quasigroup, idempotent groupoid term, mediality, incidence structure, parallelism, affine space, desarguesian affine plane.

2000 Mathematics Subject Classification: 20N05, 05B25

1 Introduction

We consider here a particular type of block designs, or incidence structures, admitting a high degree of "regularity". Recall that the so-called Steiner system $S(\ell, m, n)$ is an n-element set S together with a set of m-element subsets,

*This continued research is supported by the Ministry of Education, Youth and Sports of Czech Republic, grant No. MSM-6198959214 and by the project of specific university research of the Brno University of Technology, No. FAST-S-10-17.

called *blocks* or *lines*, with the property that each ℓ-element subset is contained in exactly one block. Steiner systems were in fact introduced already by Kirkman (1847), and triple systems $S(2,3,n)$ were studied independently by Steiner (1853) which brought the name. As well known, Steiner systems can be interpreted also as algebraic structures. Each Steiner triple system determines either an idempotent commutative quasigroup on S with juxtaposition as a binary operation defined by $aa = a$ for all $a \in S$, and $ab = c$ whenever $\{a, b, c\}$ is a triple, or an sloop on $S \cup \{e\}$, $e \notin S$, see e.g. [8] (where a lot of colloquial results can be found) and the references therein. On the othe hand, there are algebraic structures which yield a Steiner system. We pay attention to such Steiner systems of type $S(2,k,n)$ arising from idempotent medial quasigroups of particular kind. We prove that each of them corresponds either to an (at least three-dimensional, hence desarguesian) affine space ($n > k^2$, $k > 2$, in this case necessarily $n = k^m$) or to a desarguesian affine plane ($n = k^2$, $k > 3$).

2 Preliminaries

Recall some terminology and notation. If $(Q, \cdot)$ is a groupoid we say that an element $q \in Q$ is *idempotent* if $q \cdot q = q$. The groupoid is *idempotent* if all its elements are idempotent, i.e. the identity $x \cdot x = x$ holds, and is said to be *medial*, or *entropic* [12], [20], [21], if the following identity holds:

$$(x \cdot y) \cdot (u \cdot v) = (x \cdot u) \cdot (y \cdot v), \tag{1}$$

or $xy \cdot uv = xu \cdot yv$ (if juxtaposition is preferred to composition with the product written explicitely).

2.1 Quasigroups of type (n,k) and incidence structures

Definition 2.1 *Under a* quasigroup of type (n,k), $n \geq k \geq 2$ *we understand an idempotent quasigroup $\mathcal{Q} = (Q, \cdot)$ of order n in which any two distinct elements a, b of Q generate a subquasigroup $\langle a, b\rangle$ of order k.*

In short, we speak about (n,k)-quasigroups (in [16], [17] they are called A_n^k-algebras).

Recall that a quasigroup is *idempotent* if it satisfies the identity $x \cdot x = x$, and *medial* (sometimes also *entropic* or *abelian*, [9], if it satisfies the identity $(xy)(uv) = (xu)(yv)$.

In [22], (n,k)-quasigroups were introduced for $k = 3, 4$. This concept was generalized for arbitrary k in [16], where the relationship to finite regular planes and construction of algebras from commutative groups for particular k was discussed. In [25], a class of quasigroups (idempotent, generated by two elements and doubly homogeneous) is constructed from finite nearfields; the elements of the class are in fact (n,k)-quasigroups in our terminology. In [17], a class of (n,k)-quasigroups is constructed from a special kind of an algebra with two binary operations, generalizing the right Veblen-Wedderburn systems. In [18],

the theory of medial (n, k)-quasigroups was developed, parallel subquasigroups were studied, and some geometric interpretation was announced, particularly the relationship to (desarguesian) affine spaces was suggested, more or less without proves. We give here a revision of the theory of medial (n, k)-quasigroups in a unified manner, using up-to-date terminology of incidence structures and employing idempotent groupoid term functions, and give full proves of all statements.

Under an *incidence structure* we understand here an ordered pair $(\mathcal{P}, \mathcal{L})$ where $\mathcal{P}$ is a set of elements called *points* and $\mathcal{L}$ is a non-empty set of non-empty subsets of $\mathcal{P}$ called *lines*.

Given a quasigroup $\mathcal{Q}$ of type (n, k) let $\mathcal{L}_\mathcal{Q}$ denote the set of all subquasigroups of order k. Let us call elements from $\mathcal{L}_\mathcal{Q}$ *lines*. In a natural way, an incidence structure

$$\mathcal{I}_\mathcal{Q} = (Q, \mathcal{L}_\mathcal{Q}) \tag{2}$$

is associated to $\mathcal{Q}$. It can be checked that each line of $\mathcal{I}_\mathcal{Q}$ contains just k points, there are just $\frac{n-1}{k-1}$ lines passing through any point, and there is just one line through any pair of distinct points (e.g. [16]). If $n = k^2$ we get an affine plane of order k. Briefly, points of $\mathcal{Q}$ contained in the same line will be called *collinear*.

2.2 Idempotent groupoid terms

Let $\mathcal{F}(x, y) = (W(\{x, y\}), (\cdot))$ denote the absolutely free algebra of type (2) with a single operation symbol "$\cdot$" (called also the term algebra, or the word algebra) over the two-element set $\{x, y\}$ (cf. [10, p. 84], [4, p. 80]). Consider the variety $\mathcal{V}$ of idempotent groupoids and denote by $Id\,\mathcal{V}$ the set of all identities on the alphabet $\{x, y\}$ satisfied in $\mathcal{V}$. Since $Id\,\mathcal{V}$ is a congruence relation on $\mathcal{F}(x, y)$ we can form the quotient algebra $T = \mathcal{F}(x, y)/Id\,\mathcal{V}$ which is called *the relatively free algebra with respect to* $\mathcal{V}$ (cf. [10, p. 92], [4, p. 98]), or simply the *free idempotent groupoid*. Note that the carrier set of T consists of equivalence classes, each of which can be represented by such a term in variables x, y in which subsequent variables are not equal. For simplicity, such representants of elements of the carrier set of T will be called *idempotent groupoid terms* here.

So from now on, let T denote a free idempotent groupoid (of idempotent groupoid terms) on two free generators x, y.

Given an idempotent quasigroup $\mathcal{Q} = (Q, \cdot)$ and a term $t(x, y)$ from T let $t^\mathcal{Q}$ denote the term function corresponding to t in $\mathcal{Q}$ defined as a mapping

$$t^\mathcal{Q} \colon Q \times Q \to Q, \quad (a, b) \mapsto t(x := a,\, y := b).$$

Due to idempotency of $\mathcal{Q}$, $t^\mathcal{Q}(a, a) = a$ for every term function $t^\mathcal{Q}$, $t \in T$ and every $a \in Q$.

Lemma 2.2 *Let $\mathcal{Q} = (Q, \cdot)$ be a medial quasigroup of type (n, k), $n \geq k \geq 2$, and t, t' terms from T. Then for all $a, b, c, d \in Q$ the equalities*

$$t^\mathcal{Q}(a, b) \cdot t^\mathcal{Q}(c, d) = t^\mathcal{Q}(ac, bd), \tag{3}$$

$$a \cdot t^{\mathcal{Q}}(c,d) = t^{\mathcal{Q}}(ac,ad), \tag{4}$$

$$t^{\mathcal{Q}}(a,b) \cdot c = t^{\mathcal{Q}}(ac,bc), \tag{5}$$

$$t^{\mathcal{Q}}(a\cdot t'^{\mathcal{Q}}(c,d), b\cdot t'^{\mathcal{Q}}(c,d)) = t^{\mathcal{Q}}(a,b)\cdot t'^{\mathcal{Q}}(c,d) = t'^{\mathcal{Q}}(t^{\mathcal{Q}}(a,b)\cdot c, t^{\mathcal{Q}}(a,b)\cdot d), \tag{6}$$

$$t'^{\mathcal{Q}}(t^{\mathcal{Q}}(a,b), t^{\mathcal{Q}}(c,d)) = t^{\mathcal{Q}}(t'^{\mathcal{Q}}(a,c), t'^{\mathcal{Q}}(b,d)) \tag{7}$$

are valid.

Proof We proceed by induction on the complexity of terms. If t is a variable term (x or y) then (3) is trivially true. Let t_1, t_2 satisfy (3). Then the compound term $t = t_1 \cdot t_2$ has the same property, since by mediality and the induction assumption,

$$\begin{aligned} t^{\mathcal{Q}}(a,b) \cdot t^{\mathcal{Q}}(c,d) &= (t_1^{\mathcal{Q}}(a,b) \cdot t_2^{\mathcal{Q}}(c,d))(t_1^{\mathcal{Q}}(a,b) \cdot t_2^{\mathcal{Q}}(c,d)) \\ &= (t_1^{\mathcal{Q}}(a,b) \cdot t_1^{\mathcal{Q}}(c,d))(t_2^{\mathcal{Q}}(a,b) \cdot t_2^{\mathcal{Q}}(c,d)) \\ &= t_1^{\mathcal{Q}}(ac,bd) \cdot t_2^{\mathcal{Q}}(ac,bd) = t^{\mathcal{Q}}(ac,bd). \end{aligned}$$

If $a = b$ the equality (3) takes the form (4) (we used $t^{\mathcal{Q}}(a,a) = a$). If $c = d$ we get (5). Similarly for (6). The equality (7) can be proved by induction on complexity of the term t again, with t' being a fixed term. If t is a variable the equality is trivial. So let t_1, t_2 be terms satisfying (7), and let us consider the composed term $t = t_1 t_2$. According to induction assumption and (3),

$$\begin{aligned} t^{\mathcal{Q}}(t'^{\mathcal{Q}}(a,c), t'^{\mathcal{Q}}(b,d)) &= t_1^{\mathcal{Q}}(t'^{\mathcal{Q}}(a,c), t'^{\mathcal{Q}}(b,d)) \cdot t_2^{\mathcal{Q}}(t'^{\mathcal{Q}}(a,c), t'^{\mathcal{Q}}(b,d)) \\ &= t'^{\mathcal{Q}}(t_1^{\mathcal{Q}}(a,b), t_1^{\mathcal{Q}}(c,d)) \cdot t'^{\mathcal{Q}}(t_2^{\mathcal{Q}}(a,b), t_2^{\mathcal{Q}}(c,d)) \\ &= t'^{\mathcal{Q}}(t_1^{\mathcal{Q}}(a,b), t_2^{\mathcal{Q}}(a,b)) \cdot t'^{\mathcal{Q}}(t_1^{\mathcal{Q}}(c,d), t_2^{\mathcal{Q}}(c,d)) = t'^{\mathcal{Q}}(t^{\mathcal{Q}}(a,b), t^{\mathcal{Q}}(c,d)). \end{aligned}$$

□

3 Medial quasigroups of type (n,k) via term functions

3.1 Representation of lines

Note that in a medial quasigroup $\mathcal{Q}$ of type (n,k) (which is idempotent by definition), a line L determined by a pair of distinct points $a \neq b$ from Q consists exactly of points of the form $t^{\mathcal{Q}}(a,b)$, $t \in T$,

$$L = \{t^{\mathcal{Q}}(a,b) \,|\, t \in T\}. \tag{8}$$

In general, we can introduce a *groupoid of type* (n,k) as a groupoid of order n in which subgroupoids generated by two elements are of order k. Such two-generated subgroupoids in a groupoid $\mathcal{D}$ can be called lines again, and a line given by a pair a, b of distinct points consists just of the points of the form $s^{\mathcal{D}}(a,b)$ where s runs through groupoid terms on two variables.

If $\mathcal{Q} = (Q,\cdot)$ is a quasigroup with a selected element e we say that $(\mathcal{Q},e)$ is a *pointed quasigroup*, and e will be called here a *starting element* of $\mathcal{Q}$.

Let $\mathcal{Q} = (Q,\cdot)$ be a pointed medial quasigroup of type (n,k), $n \geq k \geq 2$, and e a starting element.

Definition 3.1 *We say that two lines* L, L' *of the incidence structure* $\mathcal{I}_Q$ *are* parallel *(which we denote by* $L \parallel L'$*), if and only if under any choice of points* a, b, a', b' *with* $a \neq b$, $a' \neq b'$, $a \in L$, $b \in L$, $a' \in L'$, $b' \in L'$, *the points*

$$e, \quad (e/a)b, \quad (e/a')b' \tag{9}$$

are collinear. The binary relation $\parallel$ *is called* parallelism.

We must verify that our definition of parallelism depends neither on a choice of the points $a, b \in L$ and $a', b' \in L'$ nor on the starting element. For this purpose, the equalities from Lemma 2.2 appear to be useful.

3.2 Parallelism in medial (n,k)-quasigroups

Lemma 3.2 *Parallelism of lines in pointed medial* (n,k)*-quasigroups is correctly defined.*

Proof Suppose that $\langle a,b\rangle \parallel \langle c,d\rangle$ for $a \neq b$, $c \neq d$ which means $(e/a)b \in \langle e,(e/c)d\rangle$. Let a', b' be distinct points on $\langle a,b\rangle$ and c', d' distinct points on $\langle c,d\rangle$. Thus there are terms $\alpha, \beta, \gamma, \delta \in T$ such that $a' = \alpha^{\mathcal{Q}}(a,b)$, $b' = \beta^{\mathcal{Q}}(a,b)$, $c' = \gamma^{\mathcal{Q}}(c,d)$, $d' = \gamma^{\mathcal{Q}}(c,d)$. Since $(e/a)b \in \langle e,(e/c)d\rangle$ we have $\langle e,(e/a)b\rangle = \langle e,(e/c)d\rangle$. Therefore $\langle a',b'\rangle = \langle \alpha^{\mathcal{Q}}(a,b), \beta^{\mathcal{Q}}(a,b)\rangle$, $\langle c',d'\rangle = \langle \gamma^{\mathcal{Q}}(c,d), \delta^{\mathcal{Q}}(c,d)\rangle$, and according to Lemma 2.2,

$$\begin{aligned}(e/a')b' &= (e/\alpha^{\mathcal{Q}}(a,b))\beta^{\mathcal{Q}}(a,b) = \alpha^{\mathcal{Q}}(e/a, e/b)\cdot\beta^{\mathcal{Q}}(a,b)\\ &= \alpha^{\mathcal{Q}}((e/a)\cdot\beta^{\mathcal{Q}}(a,b), (e/b)\cdot\beta^{\mathcal{Q}}(a,b))\\ &= \alpha^{\mathcal{Q}}(\beta^{\mathcal{Q}}((e/a)a, (e/a)b), \beta^{\mathcal{Q}}((e/b)a, (e/b)b))\\ &= \alpha^{\mathcal{Q}}(\beta^{\mathcal{Q}}(e, (e/a)b), \beta^{\mathcal{Q}}((e/b)a, e)).\end{aligned}$$

By mediality and idempotency,

$$((e/a)(e/b))\cdot(ab) = ((e/a)a)((e/b)b) = e\cdot e = e$$

while by right and left distributivity,

$$((e/a)(e/b))\cdot(ab) = [((e/a)a)((e/a)b)]\cdot[((e/b)a)((e/b)b)] = [e((e/a)b)]\cdot[((e/b)a)e].$$

Therefore

$$(e((e/a)b))\cdot(((e/b)a)e) = e.$$

From $e((e/a)b) \in \langle e,(e/a)b\rangle$ we get $((e/b)a)e \in \langle e,(e/a)b\rangle$, and finally $(e/b)a \in \langle e,(e/a)b\rangle$. Consequently,
$(e/a')b' = (e/\alpha^{\mathcal{Q}}(a,b))\cdot\beta^{\mathcal{Q}}(a,b) = \alpha^{\mathcal{Q}}(\beta^{\mathcal{Q}}(e,(e/a)b), \beta^{\mathcal{Q}}((e/b)a,e))) \in \langle e,(e/a)b\rangle$.

Analogously we get
$(e/c')d' = (e/\gamma^{\mathcal{Q}}(c,d))\cdot\delta^{\mathcal{Q}}(c,d) = \gamma^{\mathcal{Q}}(\delta^{\mathcal{Q}}(e,(e/c)d), \delta^{\mathcal{Q}}((e/d)c,e)) \in \langle e,(e/c)d\rangle$

so that $\langle e,(e/c')d'\rangle = \langle e,(e/c)d\rangle = \langle e,(e/a)b\rangle = \langle e,(e/a')b'\rangle$, and $(e/a')b' \in \langle e,(e/c')d'\rangle$ which means $\langle a',b'\rangle \parallel \langle c',d'\rangle$. That is, parallelism of lines does

not depend on a particular choice of point pairs determining the lines under consideration. □

Two lines contained in the same subquasigroup of type (k^2, k) may be called *complanar*.

Lemma 3.3 *Let $\mathcal{Q} = (Q, \cdot)$ be a pointed medial (n, k)-quasigroup, $n \geq k \geq 2$. Let $t \in T$ and $a, b \in Q$. Then*

$$e/t^{\mathcal{Q}}(a, b) = t^{\mathcal{Q}}(e/a, e/b). \tag{10}$$

Proof Obviously $(e/t^{\mathcal{Q}}(a, b)) \cdot t^{\mathcal{Q}}(a, b) = e$. According to Lemma 2.2,

$$t^{\mathcal{Q}}(e/a, e/b) \cdot t^{\mathcal{Q}}(a, b) = t^{\mathcal{Q}}((e/a)a, (e/b)b) = t^{\mathcal{Q}}(e, e) = e.$$

We obtain the equality

$$(e/t^{\mathcal{Q}}(a, b)) \cdot t^{\mathcal{Q}}(a, b) = t^{\mathcal{Q}}(e/a, e/b) \cdot t^{\mathcal{Q}}(a, b).$$

By right cancellation, $e/t^{\mathcal{Q}}(a, b) = t^{\mathcal{Q}}(e/a, e/b)$. □

As expected, parallelism is an equivalence relation.

Proposition 3.4 *Let $\mathcal{Q} = (Q, \cdot)$ be a medial (n, k)-quasigroup, $n \geq k \geq 2$. Then the relation of parallelism on the set $\mathcal{L}_{\mathcal{Q}}$ of lines is an equivalence relation.*

Proof Parallelism is reflexive. Given $a, b \in Q$ the points e, $(e/a) \cdot b$, $(e/a) \cdot b$ are collinear, hence $\langle a, b\rangle \parallel \langle a, b\rangle$ is valid. Further, if $a, b, c, d \in Q$ are points such that $a \neq b$, $c \neq d$ then the collinearity of e, $(e/a) \cdot b$, $(e/c) \cdot d$ is equivalent to $\langle a, b\rangle \parallel \langle c, d\rangle$ as well as to $\langle c, d\rangle \parallel \langle a, b\rangle$ which proves symmetry. To prove transitivity let $a_1, b_1, a_2, b_2, a_3, b_3 \in Q$ be points such that $a_1 \neq b_1$, $a_2 \neq b_2$, $a_3 \neq b_3$, and $\langle a_1, b_1\rangle \parallel \langle a_2, b_2\rangle \parallel \langle a_3, b_3\rangle$. So we have collinear triples e, $(e/a_1) \cdot b_1$, $(e/a_2) \cdot b_2$ and e, $(e/a_2) \cdot b_2$, $(e/a_3) \cdot b_3$. Consequently e, $(e/a_1) \cdot b_1$, $(e/a_3) \cdot b_3$ is a collinear triple, and $\langle a_1, b_1\rangle \parallel \langle a_3, b_3\rangle$. □

An element of the factor-set $\mathcal{L}_{\mathcal{Q}}/\parallel$ will be is called a *parallelism class*. Each parallelism class determines a decomposition of the carrier set Q:

Proposition 3.5 *Any element of the factor-set $\mathcal{L}_{\mathcal{Q}}/\parallel$ determines a decomposition of Q into pairwise disjoint pairwise parallel lines such that for any point $a \in Q$ there is just one line of the class passing through a.*

Proof First show that there exists at most one line through the point c parallel to $\langle a, b\rangle$. Indeed, assume parallel lines $\langle a, b\rangle$, $\langle a, c\rangle$ where $a \neq b$, $a \neq c$, $c \notin \langle a, b\rangle$. Then $b \neq c$, $(e/a)b \neq (e/a)c$, and e, $(e/a)b$, $(e/a)c$ are collinear points. This means that there exists a term $t \in T$ such that $e = t^{\mathcal{Q}}((e/a)b, (e/a)c)$. By the Lemma 2.2, $t^{\mathcal{Q}}((e/a)b, (e/a)c) = (e/a) \cdot t^{\mathcal{Q}}(b, c)$ so that $e = (e/a)t^{\mathcal{Q}}(b, c)$, and consequently $t^{\mathcal{Q}}(b, c) = a$ which expresses collinearity of the points a, b, c, a contradiction.

Now let $a,b,c \in Q$, $a \neq b$. Let us verify existence of a line through the point c parallel to the line $\langle a,b\rangle$. In fact, denote $d := (e/c)\backslash((e/a)\cdot b)$; so $(e/c)d = (e/a)b$. It can be checked that $e \neq (e/a)b$ (the equality $e = (e/a)b$ would imply $e/a = e/b$, and hence $a = b$). Trivially, the triple e, $(e/a)b$, $(e/c)d$ is collinear. It implies $\langle a,b\rangle \parallel \langle c,d\rangle$. □

If $t \in T$ we use the notation $t^{\mathcal{Q}}(c,\langle a,b\rangle) := \{t^{\mathcal{Q}}(c,p) \mid p \in \langle a,b\rangle)\}$; more generally, $t^{\mathcal{Q}}(c,Q') := \{t^{\mathcal{Q}}(c,p) \mid p \in Q'\}$ for any nonempty subset $Q' \subseteq Q$.

Lemma 3.6 *Let $\mathcal{Q} = (Q,\cdot)$ be a pointed medial (n,k)-quasigroup, $n > k \geq 2$, and $a,b,c \in Q$ such that $a \neq b$ and $c \notin \langle a,b\rangle$. Let $t \in T$ be such a term that $\langle a,b\rangle \to Q$, $p \mapsto t^{\mathcal{Q}}(c,p)$ is not a constant mapping. Then $t^{\mathcal{Q}}(c,\langle a,b\rangle) \in \mathcal{L}_{\mathcal{Q}}$, and $t^{\mathcal{Q}}(c,\langle a,b\rangle) \parallel \langle a,b\rangle$ holds.*

Proof Since $t^{\mathcal{Q}}(c,p)\cdot t^{\mathcal{Q}}(c,q) = t^{\mathcal{Q}}(c,pq)$ by Lemma 2.2, the set $t^{\mathcal{Q}}(c,\langle a,b\rangle)$ is a subquasigroup of order l, $1 \leq l \leq k$, and consequently of order k. So $t^{\mathcal{Q}}(c,\langle a,b\rangle) \in \mathcal{L}_{\mathcal{Q}}$. Take elements $t^{\mathcal{Q}}(c,a)$, $t^{\mathcal{Q}}(c,b)$ as generators, and investigate the point triple e, $(e/a)\cdot b$, $(e/t^{\mathcal{Q}}(c,a))\cdot t^{\mathcal{Q}}(c,b)$. By Lemma 3.3, $e/t^{\mathcal{Q}}(c,a) = t^{\mathcal{Q}}(e/c,e/a)$, and by Lemma 2.2, $t^{\mathcal{Q}}(e/c,e/a)\cdot t^{\mathcal{Q}}(c,a) = t^{\mathcal{Q}}((e/c)c,(e/a)a) = t^{\mathcal{Q}}(e,e) = e$. Also, $(e/a)\cdot b \neq e$ (if $(e/a)\cdot b = e$ then $e/a = e/b$ and $a = b$, a contradiction). Thus the point triple under consideration consists of e, $(e/a)b$, a, and the points are collinear. Therefore $\langle a,b\rangle$ and $t^{\mathcal{Q}}(c,\langle a,b\rangle)$ are parallel lines. □

3.3 How term functions characterize parallelism

Parallelism of lines in (n,k)-quasigroups is characterized in the language of term functions as follows.

Proposition 3.7 *Let $\mathcal{Q} = (Q,\cdot)$ be a pointed medial (n,k)-quasigroup with $n > k \geq 2$, L and L' distinct parallel lines in $\mathcal{I}_{\mathcal{Q}}$, and a,b,c collinear pairwise distinct points such that $a \in L$, $b \in L'$. Then there is a term $t \in T$ such that $t^{\mathcal{Q}}(c,L) = L'$.*

Proof Under our assumptions there exists a term $t \in T$ such that $b = t^{\mathcal{Q}}(c,a)$. The mapping $L \to Q$, $p \mapsto t^{\mathcal{Q}}(c,p)$ cannot be constant. Indeed, if in the contrary, $t^{\mathcal{Q}}(a,d) = b$ would hold for a point $d \in L\backslash\{a\}$ then the points a, d would lie on the same line $\langle b,c\rangle$, fig. 1, which contradicts the obvious fact that $\langle a,d\rangle = L \neq \langle b,c\rangle$. □

Proposition 3.8 *Let $\mathcal{Q} = (Q,\cdot)$ be a medial (n,k)-quasigroup with $n > k \geq 2$. The lines $L,L' \in \mathcal{L}_{\mathcal{Q}}$ are parallel if and only if there exists a point $c \in Q$ and a term $t \in T$ such that $t^{\mathcal{Q}}(c,L) = L'$.*

Proof If $L \parallel L'$ with $a \in L$, $a' \in L'$ it is sufficient to choose $c = a'/a$ and $t = x\cdot y$. To check it we verify that the mapping $L \to Q$, $p \mapsto (a'/a)p$ is injective, and then apply Lemma 3.6.

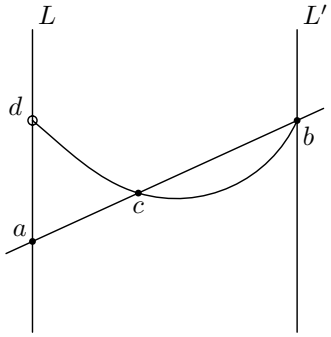

Fig. 1

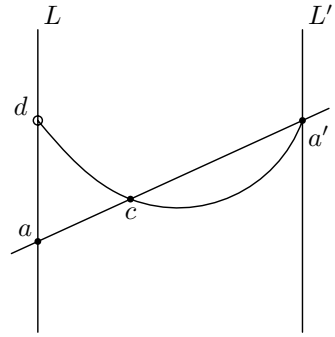

Fig. 2

Note that our mapping is a reduction (to L) of the left translation $L_{a'/a}$ by a'/a, and hence is injective. If $L = L'$ we are done. Assume $L \neq L'$, and choose a point $c \in \langle a, a'\rangle \backslash \{a, a'\}$. Then also $a' \in \langle c, a\rangle$, and there is a term $t \in T$ such that $t(c, a) = a'$. Now the mapping $L \to Q$, $p \mapsto t(c, p)$ cannot be constant since in the opposite case, for any point $d \neq a$ on L, both points a, d would lie simultaneously on L as well as on $\langle a, a'\rangle \neq L$ (fig. 2); a contradiction. Since according to Lemma 3.6, $t^{\mathcal{Q}}(c, L)$ is a (unique) line through a' parallel to L it must coincide with L'.

Vice versa, let $L, L' \in \mathcal{L}_{\mathcal{Q}}$, and let there exist $c \in Q$, $t \in T$ such that $t^{\mathcal{Q}}(c, L) = L'$. Denote $a' := t^{\mathcal{Q}}(c, a)$, $b' := t^{\mathcal{Q}}(c, b)$ for distinct a, $b \in L$. The mapping $L \to L'$, $p \mapsto t^{\mathcal{Q}}(c, p)$ must be bijective, so that $a' \neq b'$. Now the points e, $(e/a)b$, $(e/a')b'$ are collinear since according to Lemmas 3.3, 2.2, $(e/a')b' = (e/t^{\mathcal{Q}}(c, a))\cdot t^{\mathcal{Q}}(c, b) = t^{\mathcal{Q}}(e/c, e/a)\cdot t^{\mathcal{Q}}(c, b) = t^{\mathcal{Q}}((e/c)c, (e/a)b) = t^{\mathcal{Q}}(e, (e/a)b)$. Hence the lines L and L' are parallel. □

4 Characterization of incidence structures associated to medial (n, k)-quasigroups

Proposition 4.1 *Let $\mathcal{Q} = (Q, \cdot)$ be a medial (n, k)-quasigroup, $n > k \geq 3$, possessing generators $a, b, c \in Q$ such that $a \neq b$, $c \notin \langle a, b\rangle$. Then the cardinality of Q is $n = k^2$.*

Proof Denote $L = \langle a, b\rangle$, $L' = \langle a, c\rangle$ (fig. 3). If $x \in L$, then xL' is a line parallel to L' (which follows by left distributivity of the quasigroup multiplication, or also directly by Lemma 3.6). Note that $L' \cap xL' \neq \emptyset$ for all $x \in L\backslash\{a\}$ (suppose y_0 is a common point of L' and xL, then $y_0 = xy_1$ for some $y_1 \in L'$; hence $x \in L'$ since L' is a subquasigroup; a contradiction). Furthermore, the assumption $x_1L' \cap x_2L' \neq \emptyset$ for x_1, $x_2 \in L\backslash\{a\}$, $x_1 \neq x_2$ is equivalent with $x_1L' = x_2L'$; particularly, the common point of L and $x_1L' = x_2L'$ must be of the form $x_1a = x_2a$, a contradiction with $x_1 \neq x_2$. So we obtain just k lines of the form xL', including L' (since $aL' = L'$). Denote by S the set of all points that lie on these lines; obviously, $\operatorname{card} S = k \cdot k = k^2$. Now let us check that

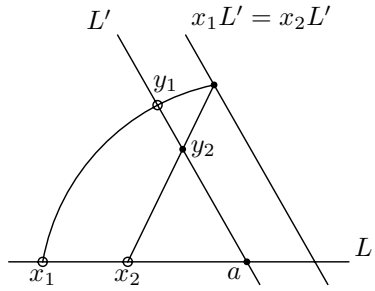

Fig. 3

the set S is closed under the quasigroup multiplication. If two points of S lie on the same line xL' then also their product lies on this line since xL' is a subquasigroup of $\mathcal{Q}$. Investigate points $x_1y_1 \in x_1L'$, $x_2y_2 \in x_2L'$. By mediality, $(x_1y_1) \cdot (x_2y_2) = (x_1x_2) \cdot (y_1y_2) \in x_1x_2L'$. Hence S is a carrier set of a subquasigroup of $\mathcal{Q}$ which involves generators a, b, c of $\mathcal{Q}$. S must coincide with the carrier set Q. □

Theorem 4.2 *The incidence structure $\mathcal{I}_\mathcal{Q}$ associated to the quasigroup $\mathcal{Q}$ from Theorem 4.1 is an affine plane of order k.*

For the definition of an affine plane of order q, e.g. [13, p. 32].

Proof The type of $\mathcal{Q}$ is (k^2, k), $k \geq 2$, so that there are just k^2 points, every line contains exactly k points, and there are just $\frac{k^2-1}{k-1} = k + 1$ lines passing through any point. Let p be a point and L a line not containing p. Then there are just k lines $\langle p, x\rangle$ for $x \in L$, and consequently it remains a single line disjoint to L through p. Since for any two distinct points p, q there is just one line $\langle p, q\rangle$ containing them, and there exist three noncollinear points a, b, c, the incidence structure $\mathcal{I}_\mathcal{Q}$ must be an affine plane. □

Lemma 4.3 (Trapezoid property) *Let $\mathcal{Q} = (Q, \cdot)$ be a medial (n, k)-quasigroup with $n > k \geq 3$. If a, b, c are collinear pairwise distinct points in $\mathcal{I}_\mathcal{Q}$, and A, B parallel lines such that $a \in A$, $b \in B$, $c \notin A$, then $\langle c, p\rangle \cap B \neq \emptyset$ for all $p \in A$.*

Proof By Lemma 3.8, there exists $t \in T$ such that $B = t^\mathcal{Q}(c, A)$. But this means that $t^\mathcal{Q}(c, p) \in B$ for all $p \in A$. □

4.1 Affine space

Recall how affine spaces distinct from affine planes can be introduced. We adopt here a view-point of H. Lenz, [14], with axioms a bit reformulated.

An *affine space* (distinct from affine planes) is introduced as an incidence structure $(\mathcal{P}, \mathcal{L})$ together with an equivalence relation of *parallelism* defined on

$\mathcal{L}$ (which decomposes L into classes of *parallel lines*) such that the following conditions hold:

(i) Any two distinct points a, b are simultaneously contained in just one line (denoted by ab).

(ii) To every point p and every line L there exists just one line through p parallel to L.

(iii) (*Trapezoid property*) If a, b, c are pairwise distinct collinear (=contained in the same line) points and A, B parallel lines such that $a \in A$, $b \in B$, $c \notin A$, then for any $p \in A$ the line pc intersects B.

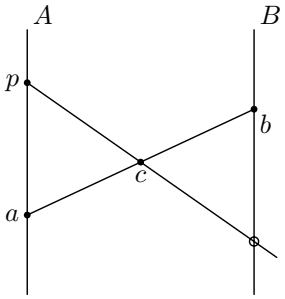

Fig. 4

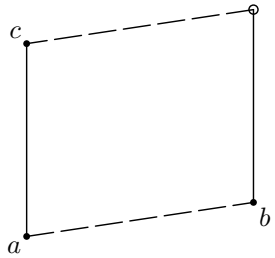

Fig. 5

(iv) (*Parallelogram property*) If every line consists of just two points and a, b, c are non-collinear points then the line through c parallel to ab intersects the line through b parallel to ac.

(v) Every line contains at least two points, and there exist two distinct lines which are not parallel.

Theorem 4.4 *For every medial quasigroup $\mathcal{Q} = (Q, \cdot)$ of type (n, k), $n > k^2$, $k \geq 3$, the associated incidence structure $\mathcal{I}_\mathcal{Q}$ is an affine space $\mathbb{A}$ of finite dimension ≥ 3.*

Proof Let us start with the incidence structure $\mathcal{I}_\mathcal{Q}$ and take the parallelism relation introduced for the affine space parallelism (sec. 2.1). The condition (i) from the previous definition of affine space is satisfied, since lines are subquasigroups generated by point pairs, and (ii) follows by Prop. 3.5. The trapezoid axiom is valid by Lemma 4.3. The parallelogram axiom is here redundant because of the assumption $k > 2$, that also guarantees the validity of the first part of the axiom (v). The second part of the axiom (v) follows from the assumption $n > k^2$ as follows. Take arbitrary points $a \neq b$. Since $\operatorname{card} Q = n > k^2$ there must exist further points c, d such that the points a, b, c, d do not generate a subquasigroup of order k^2, so that $\langle a, b\rangle, \langle c, d\rangle$ must be disjoint, and cannot be parallel. □

Corollary 4.5 *For the medial quasigroup $\mathcal{Q} = (Q, \cdot)$ from Theorem 4.4 there exists $m \geq 3$ such that $n = k^m$ holds, m is the dimension of the affine space $\mathbb{A}$ and equals to the minimal number of generators of $\mathcal{Q}$.*

4.2 Isomorphism of incidence structures

Two incidence structures $(\mathcal{P}, \mathcal{L})$ and $(\mathcal{P}', \mathcal{L}')$ are said to be *isomorphic* if there exists a bijection φ, called *isomorphism* of $(\mathcal{P}, \mathcal{L})$ onto $(\mathcal{P}', \mathcal{L}'))$ such that $L \in \mathcal{L} \Rightarrow \{\varphi(x) \mid x \in L\} \in \mathcal{L}'$, and $L' \in \mathcal{L}' \Rightarrow \{\varphi^{-1}(x) \mid x \in L'\} \in \mathcal{L}$.

Particularly, if both structures are affine spaces then the last condition $L' \in \mathcal{L}' \Rightarrow \{\varphi^{-1}(x) \mid x \in L'\} \in \mathcal{L}$ can be omitted if we add the condition that parallel lines are mapped onto parallel lines. An affine space which has only finite number of points is called *finite*.

The *order* of a finite affine space is the number of points on a line, which is independent of the choice of a particular line. It is well known that two finite affine spaces, with dimension at least three, of the same order and the same dimension are isomorphic.

Lemma 4.6 *(i) Any two subquasigroups of order k in a medial quasigroup $\mathcal{Q} = (Q, \cdot)$ of type (k^2, k), $k > 1$, are isomorphic.*

(ii) Any two medial quasigroups of type (k, k), $k > 1$, are isomorphic.

Proof Part (i): Let $\mathcal{Q} = (Q, \cdot)$ be a medial quasigroup of type (k^2, k), $k > 1$. If A, B are parallel lines in $\mathcal{I}_\mathcal{Q}$ then by Lemma 3.8, $B = cA$ for some $c \in Q$. However, the mapping $A \to B$, $a \mapsto ca$ is a bijection satisfying (by mediality) the equality $c \cdot aa' = (cc)(aa') = (ca)(ca')$ for a, $a' \in A$. Hence this mapping is an isomorphism.

If t is a term from T such that the mappings $A \to Q$, $p \mapsto t(c, p)$ are not constant (we can choose e.g. $t \equiv xy$), A a line, $a_1 \in A$, and if c runs over a line $C_1 \neq A$ going through a_1 then $t^\mathcal{Q}(c, A)$ runs over all lines parallel to A, fig. 6. If c' is another point on C_1 then $t^\mathcal{Q}(c, a_1) = b_1$, $t^\mathcal{Q}(c', a_1) = b_1'$ are points also belonging to C_1. Similarly, if a_2 is another point on A then $t^\mathcal{Q}(c, a_2) = b_2$, $t^\mathcal{Q}(c', a_2) = b_2'$ are points on the same line, let us say C_2. Changing points in other admissible positions allows to reach all other positions of a line C non-parallel to C_1. The points b_1, b_2 are on the same line parallel to A, and b_1', b_2' are on the same line parallel to A as well, fig. 7. Now by Lemma 3.3 $b_1 b_1' = t^\mathcal{Q}(c, a_1) t^\mathcal{Q}(c', a_1) = t^\mathcal{Q}(cc', a_1)$, $b_2 b_2' = t^\mathcal{Q}(c, a_2) t^\mathcal{Q}(c', a_2) = t^\mathcal{Q}(cc', a_2)$, so that also $b_1 b_1'$, $b_2 b_2'$ lie on the same line parallel to A. We conclude that the "parallel projection" from C_1 onto C_2 induced by lines parallel to A is a quasigroup isomorphism.

Part (ii): Every medial quasigroup $\mathcal{Q} = (Q, \cdot)$ of type (k, k) can be deduced from a field $(Q, +, \circ)$ of order k in such a way that $a \cdot b = a + \nu \circ (b - a)$ for all a, $b \in Q$ where ν is a generating element of the multiplicative group of the field (briefly, a *primitive element*, cf. [19], Theorem 7, pp. 82–83).

Let us assume two medial quasigroups $\mathcal{Q} = (Q, \cdot)$, $\mathcal{Q}' = (Q', \cdot')$ of type (k, k). Let us assume fields $(Q, +, \circ)$, $(Q', +', \circ')$ of order k, and in each of them a primitive element, ν or ν', respectively, so that $a \cdot b = a + \nu \circ (b - a)$ for all $a, b \in Q$ and $a' \cdot' b' = a' +' \nu' \circ' (b' - a')$ for all $a', b' \in Q'$. We know that the fields are isomorphic. In particular, we can choose an isomorphism φ so that $\varphi(\nu) = \nu'$ (then φ is unique up to isomorphism of the quasigroups, cf. [25], Theorem 2.8 on p. 1097). Hence we can express the operation of $\mathcal{Q}'$ in the

form $\varphi(a) \cdot' \varphi(b) = \varphi(a) +' \varphi(\nu) \circ' (\varphi(b) - \varphi(a)) = \varphi(a + \nu \circ (b - a))$ which yields $\varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$ for all $a, b \in Q$. The quasigroups $\mathcal{Q}, \mathcal{Q}'$ under consideration are therefore isomorphic. □

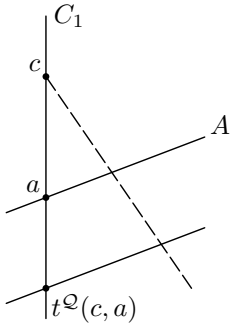

Fig. 6

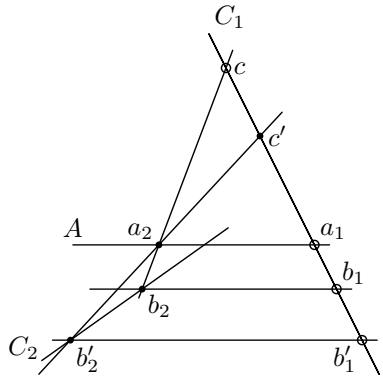

Fig. 7

4.3 Parallelism is independent of the choice of a starting element

Now let us go back to explanation why the choice of a fixed element e for the definition of the parallelism introduced after Lemma 2.2 plays no role whatever as far as the result of the construction is concerned.

One explanation of this fact uses isomorphism between both copies of affine spaces. If e is chosen in another position then $\mathcal{I}_{\mathcal{Q}}$ is also a copy of an affine space of the same dimension, with the same point set and the same line set, and the relation of parallelism between lines must be the same as well.

An alternative explanation of this fact can be based on the characteristic property of parallel lines, namely that two distinct lines are parallel if and only if they are disjoint and "complanar". Let $\mathcal{Q} = (Q, \cdot)$ be a medial quasigroup of type (k^m, k). In subquasigroups of type (k^2, k), parallelism of two lines, defined after Lemma 3.3, coincides with the relation "to be disjoint or to be equal". Since the last relation is independent of a choice of the starting point, parallelism of lines must be independent of the starting point also in the whole quasigroup $\mathcal{Q}$.

In Theorems 4.4 and 4.7, we will prove that for a medial quasigroup $\mathcal{Q} = (Q, \cdot)$ of type (n, k), $n > k^2$, $k \geq 3 > 2$, the incidence structure $\mathcal{I}_{\mathcal{Q}}$ is an affine space distinct from an affine plane, and that for every medial quasigroup of type (k^2, k), $k > 2$, the incidence structure $\mathcal{I}_{\mathcal{Q}}$ is a desarguesian affine plane. Note that another proof of Theorem 4.7 can be deduced from Theorem 4.4 via embedding.

Let us present now an alternative proof of Lemma 4.6 (i) according to considerations of [7, p. 103].

Let $\mathcal{Q} = (Q, \cdot)$ be a medial quasigroup of type (k^2, k), $k > 1$. That is, $\mathcal{I}_\mathcal{Q}$ is an affine plane. Define $A \cdot B := \{a \cdot b \,|\, a \in A, b \in B\}$ for any nonempty subsets $A, B \subseteq Q$.

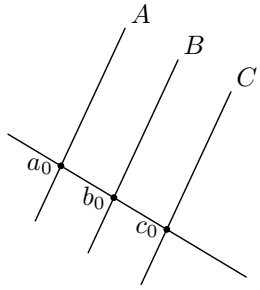

Fig. 8

Let A, B, C be pairwise distinct parallel lines, and let $a_0 \in A$, $b_0 \in B$, $c_0 \in C$ be points satisfying $a_0 \cdot b_0 = c_0$, fig. 8. We assert that $A \cdot B = C$. First we have $C = a_0 B$. In fact, C is the unique line parallel to A going through c_0, but the line $a_0 B$ going through $c_0 = a_0 b_0$ has the same property (A, $a_0 B$ are disjoint and hence parallel since if $a_0 b' \in A$ would be satisfied for $b' \in B$ it would follow $b' \in A$, a contradiction to parallelism of A, B). Hence $C \subseteq A \cdot B$. Since a_0 was an arbitrary point on the line A we have $aB = C$ for all $a \in A$, so that $A \cdot B \subseteq C$.

Let L, L' be distinct lines, and L'' a line non-parallel to any of L, L'. Define a mapping $\varphi\colon L \to L'$, $p \mapsto p'$ such that either $p = p'$, or $p \neq p'$ and $\langle p, p' \rangle \parallel L''$. By the previous assertion, the mapping φ is a quasigroup isomorphism between L and L', and can be called *parallel perspectivity*. It follows that any two subquasigroups of order k in $\mathcal{Q}$ are necessarily isomorphic. □

Theorem 4.7 *Let $\mathcal{Q} = (Q, \cdot)$ be a medial quasigroup of type (k^2, k), $k > 3$. Then $\mathcal{I}_\mathcal{Q}$ is a desarguesian plane.*

Proof (After [7]) Let e, a, c' be non-collinear points, and let $b = t(e, a)$, $c = t'(e, b)$ for suitable terms t, $t' \in T$; whence $c = t'(e, t(e, a))$. Let a', b' lie on $\langle e, c' \rangle$ in such a position that $\langle b, c' \rangle \parallel \langle b', c \rangle$, $\langle a, b' \rangle \parallel \langle b, a' \rangle$. Since parallel perspectivity is a quasigroup isomorphism it follows that $b' = t'(e, c')$, $a' = t(e, b')$, fig. 9. Therefore $a' = t(e, t'(e, c'))$ and by Lemma 2.2, $a' = t'(e, t(e, c'))$. Since $c = t'(e, t(e, a))$ we conclude $\langle a', c \rangle \parallel \langle a, c' \rangle$. □

Theorem 4.8 *Let n, m be integers with $n > 2$, $m \geq 2$. Let $\mathbb{A}$ be the "arithmetical exemplar" of an m-dimensional affine space over a field $(F, +, \cdot)$ of order n. That is, $\mathbf{x} = (x_1, \ldots, x_m) \in F^m$ are points of $\mathbb{A}$, $\{\mathbf{a} + t \cdot \mathbf{v} \,|\, t \in F\}$, $\mathbf{a} \in F^m$ arbitrary, $\mathbf{v} \in F^m \backslash \{\underbrace{(0, \ldots, 0)}_{m}\}$ are lines of $\mathbb{A}$, and the parallelism relation for lines is given by*

$$\{\mathbf{a}_1 + t\mathbf{v}_1 \,|\, t \in F\} \parallel \{\mathbf{a}_2 + t\mathbf{v}_2 \,|\, t \in F\}$$

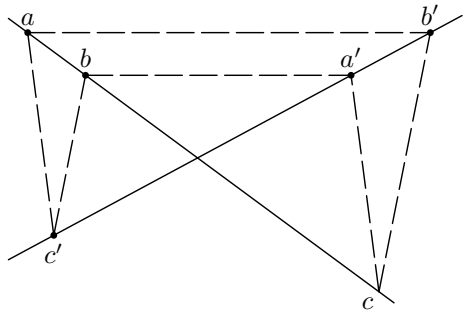

Fig. 9

if and only if $\mathbf{v}_1, \mathbf{v}_2 \in F^m$ *are proportional* m*-tuples (i.e. each of them is a non-zero multiple of the other by an element from* $F\backslash\{0\}$[*]*). Then the binary operation* $\circ$ *on* F^m *introduced by*

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \nu(\mathbf{y} - \mathbf{x}), \quad \mathbf{x}, \mathbf{y} \in F^m$$

where ν *is a primitive element of the field, establishes on* F^m *a structure of a medial quasigroup of type* (n^m, n)*. Moreover,* $\mathcal{I}_{(F^m,\circ)}$ *is isomorphic to* $\mathbb{A}$*.*

Proof $(F^m, \circ)$ is a quasigroup since for given m-tuples $\mathbf{a}, \mathbf{b}, \mathbf{c} \in F^m$, both equations $\mathbf{x} \circ \mathbf{b} = \mathbf{c}$, $\mathbf{a} \circ \mathbf{y} = \mathbf{c}$ are uniquely solvable in F^m. Indeed, $\mathbf{x} + \nu(\mathbf{b} - \mathbf{x}) = \mathbf{c} \Leftrightarrow (1-\nu)\mathbf{x} = \mathbf{c} - \nu\mathbf{b} \Leftrightarrow \mathbf{x} = \frac{1}{1-\nu}(\mathbf{c} - \nu\mathbf{b})$, and $\mathbf{a} + \nu(\mathbf{y} - \mathbf{a}) = \mathbf{c} \Leftrightarrow \nu\mathbf{y} = \mathbf{c} - (1-\nu)\mathbf{a} \Leftrightarrow \mathbf{y} = \frac{1}{\nu}(\mathbf{c} - (1-\nu)\mathbf{a})$. Mediality of $\circ$ can be verified as follows: $(\mathbf{a} \circ \mathbf{b}) \circ (\mathbf{c} \circ \mathbf{d}) = (\mathbf{a} + \nu(\mathbf{b} - \mathbf{a}) \circ (\mathbf{c} + \nu(\mathbf{d} - \mathbf{c})) = \mathbf{a} + \nu(\mathbf{c} + \nu(\mathbf{d} - \mathbf{c}) - \mathbf{a} - \nu(\mathbf{b} - \mathbf{a})) = \mathbf{a} - \nu\mathbf{a} - \nu\mathbf{a} + \nu^2\mathbf{a} + \nu\mathbf{b} - \nu^2\mathbf{b} + \nu\mathbf{c} - \nu^2\mathbf{c} + \nu^2\mathbf{d}$, similarly $(\mathbf{a} \circ \mathbf{c}) \circ (\mathbf{b} \circ \mathbf{d}) = (\mathbf{a} + \nu(\mathbf{c} - \mathbf{a}) \circ (\mathbf{b} + \nu(\mathbf{d} - \mathbf{b})) = \mathbf{a} + \nu(\mathbf{c}\nu(\mathbf{a}) + \nu(\mathbf{b} + \nu(\mathbf{b} + \nu(\mathbf{d} - \mathbf{b}) - \mathbf{a} - \nu(\mathbf{c} - \mathbf{a})) = \mathbf{a} - \nu\mathbf{a} - \nu\mathbf{a} + \nu^2\mathbf{a} + \nu\mathbf{b} - \nu^2\mathbf{b} + \nu\mathbf{c} - \nu^2\mathbf{c} + \nu^2\mathbf{d}$, the same formula as before. Every line of $\mathbb{A}$ contains just n points, and is generated in $(F^m, \circ)$ by any pair of its distinct points. If $\mathbf{a}$, $\mathbf{b}$ are distinct points then

$$\mathbf{a}, \mathbf{a} \circ \mathbf{b}, \mathbf{a} \circ (\mathbf{a} \circ \mathbf{b}), \ldots, \underbrace{\mathbf{a} \circ (\mathbf{a} \circ \ldots (\mathbf{a} \circ \mathbf{b}) \ldots)}_{n}$$

exhaust just all n points of the line $L = \{\mathbf{a} + t(\mathbf{b} - \mathbf{a})\}$. Indeed, if we rewrite these expressions by means of the operations $+, \cdot$ of the field $(F, +, \cdot)$ it turns out that these elements are pairwise distinct, and therefore must exhaust the whole set L. Moreover, it can be verified that L is closed under $\circ$. The fact that $\{\nu, \nu^2, \ldots, \nu^{n-1}\} = F\backslash\{0\}$ is crucial. Hence $(F^m, \circ)$ is a medial quasigroup of type (n^m, n). Of course, the associated incidence structure $\mathcal{I}_{(F^m,\circ)}$ is, by Theorem 4.4, an m-dimensional affine space. □

[*]We use operations of the arithmetical m-dimensional vector space over F.

4.4 Embedding of medial quasigroups

Briefly, let us mention embeddings.

Every medial quasigroup $\mathcal{Q} = (Q, \cdot)$ *of type* (k^2, k), $k \geq 2$ *can be embedded into a medial quasigroup of type* (k^3, k).

For this purpose, let us use the direct product of $(Q, \cdot)$ with the medial quasigroup $(A, \cdot)$ where A is an arbitrary line in the incidence structure $\mathcal{I}_{\mathcal{Q}}$. By [16], p. 894, Theorem 2, the direct product of $(Q, \cdot)$ and $(A, \cdot)$ is a medial idempotent quasigroup of type $(k^2 \cdot k, k)$. In fact, both assumptions of [16], Theorem 2 are satisfied. The fact that every subquasigroup of order k in $\mathcal{Q}$ is doubly homogeneous, [19], p. 82, Theorem 6, plays an important role.

References

[1] Belousov, V. D.: *Transitive distributive quasigroups*. Ukr. Mat. Zhur **10**, 1 (1958), 13–22.

[2] Belousov, V. D.: Foundations of the theory of quasigroups and loops. *Nauka*, Moscow, 1967, (in Russian).

[3] Bruck, R. H.: A Survey of Binary Systems. *Springer*, Berlin, 1958.

[4] Denecke., K., Wismath, Sh. L.: Universal Algebra and Applications in Theoretical Computer Science. *Chapman and Hall/CRC*, 2002.

[5] Duplák, J.: *On some permutations of a medial quasigroup*. Mat. Čas. **24** (1974), 315–324, (in Russian).

[6] Duplák, J.: *On some properties of transitive quasigroups*. Zborník Ped. fak. Univ. Šafárika **1** (1976), 29–35, (in Slovak).

[7] Duplák, J.: *Quasigroups and translation planes*. J. Geom. **43** (1992), 95–107.

[8] Ganter, B., Werner, H.: *Co-ordinatizing Steiner systems*. Ann. Disc. Math. **7** (1980), 3–24.

[9] Havel, V. J., Vanžurová, A.: Medial Quasigroups and Geometry. *Palacky University Press*, Olomouc, 2006.

[10] Ihringer, Th.: Allgemeine Algebra. *Teubner*, Stuttgart, 1988.

[11] Lindner, C. C., Rodger, C. A.: Design Theory. *CRC Press*, London, New York, Washington, 1997.

[12] Ježek, J., Kepka, T.: Medial Groupoids. *Academia*, Praha, 1983.

[13] Kárteszi, F.: Introduction to Finite Geometries. Budapest, 1976.

[14] Lenz, H.: *Über die Einführung einer absoluten Polarität in die projektive und affine Geometrie des Raumes*. Math. Ann. **128** (1954), 363–373.

[15] Pflugfelder, H. O.: Quasigroups and Loops, Introduction. *Heldermann Verlag*, Berlin, 1990.

[16] Pukharev, N. K.: *On* A_n^k*-algebras and finite regular planes*. Sib. Mat. Zhur. **6**, 4 (1965), 892–899, (in Russian).

[17] Pukharev, N. K.: *On construction of* A_n^k*-algebras*. Sib. Mat. Zhur. **7**, 3 (1966), 724–727, (in Russian).

[18] Pukharev, N. K.: *Geometric questions of some medial quasigroups*. Sib. Mat. Zhur. **9**, 4 (1968), 891–897, (in Russian).

[19] Pukharev, N. K.: *Some properties of groupoids and quasigroups connected with balanced incomplete block schemes*. Quasigroups and Latine squares, Mat. Issl., Kishinev **71** (1983), 77–85, (in Russian).

[20] Romanowska, A., Smith, J. D. H.: Modal Theory, An Algebraic Approach to Order, Geometry, and Convexity. *Heldermann Verlag*, Berlin, 1985.

[21] Romanowska, A., Smith, J. D. H.: Modes. *World Scientific*, New Jersey, London, Singapore, Hong Kong, 2002.

[22] Szamkolowicz, L.: *On the problem of existence of finite regular planes*. Colloq. Math. **9** (1962), 245–250.

[23] Szamkolowicz, L.: *Remarks on finite regular planes*. Colloq. Math. **10** (1963), 31–37.

[24] Šiftar, J.: *On affine planes over A_n^k-quasigroups*. J. Geom. **20** (1983), 1–7.

[25] Stein, S. K.: *Homogeneous quasigroups*. Pacif. J. Math. **14** (1964), 1091–1102.

[26] Szmielew, W.: From Affine to Euclidean Geometry. *Polish Scientific Publishers & D. Reidel Publishing Company*, Warszawa & Dordrecht–Boston–London, 1983.