Discrete Mathematics **203** (1999) 169–194

Matroid Representations by Partitions*

František Matúš†

Statistik und Informatik, Universität Bielefeld, Postfach 100131,

33501 Bielefeld, Germany

matus@utia.cas.cz

Abstract. A matroid on the ground set N with the rank function r is said to be partition representable of degree $d \geqslant 2$ if partitions ξ_i, $i \in N$, of a finite set Ω of the cardinality $d^{r(N)}$, exist such that the meet-partition $\xi_I = \wedge_{i \in I} \xi_i$ has $d^{r(I)}$ blocks of the same cardinality for every $I \subseteq N$. Partition representable matroids are called also secret-sharing or almost affinely representable and partition representations correspond to ideal secret-sharing schemes or to almost affine codes. These notions are shown to be closely related to generalized quasigroup equations read out of the matroid structure. A special morphism of partition representations, called partition isotopy, is introduced. For a few matroids, the partition isotopy classes of partition representations are completely classified. An infinite set of excluded minors for the partition representability is constructed.

1. Introduction and basic definitions. Matroid representations have received considerable attention from the very beginnings of the matroid theory. The subject of linear representations, see the corresponding chapters in [42], [4], [10], [25], [44] and [38], remains the most attractive but also algebraic representations, see [42], [27], [28], [38], and other embeddings into geometric lattices of various structures (uniform geometries of [9], simplicial geometries in [44] Chapter 6, partition matroids determined by finite groups [42] p. 189, modules over syzygy rings [43], etc.) have been investigated in detail.

A central notion of the present study has emerged to us, maybe quite unexpectedly in context of the matroid representation theories, from an investigation of conditional independence structures among random variables, see [33]. After recognition of the role of entropy functions, cf. [17], some conditional independence structures were related to matroids and some of their probabilistic representations appeared to have a highly symmetric combinatorial form. The resulting notion is that of partition representable matroid as presented in Definition 1.1. below. Only much later we realized that the same notion

*This work was done while the author was Research Fellow of Alexander von Humboldt Foundation.

†*Permanent postal address:* Academy of Sciences of the Czech Republic, Institute of Information Theory and Automation, Pod vodárenskou věží 4, 182 08 Prague, Czech Republic.

E-mail address: matus@utia.ca.cz

1991 Mathematics Subject Classification. Primary 05B35, 51E14; Secondary 05A18, 05B15, 20N05, 20N15, 39B52, 51A20, 94A17.

Keywords: matroid representations, partitions, excluded minors, quasigroup equations, associative law, medial law, latin squares and hypercubes, orthogonal arrays, quadrangle criterion, entropy fuctions, probabilistic representability, almost affine codes, secret-sharing schemes.

was introduced independently in cryptology under the label 'secret-sharing matroid' [39] and in coding theory as 'almost affinely representable matroid' [40]. There, a starting point was the result of [8] relating ideal secret-sharing schemes to matroids. Since then a considerable work has been done on these secret-sharing schemes, for references see [5], [7], [22], [29], viewing them also as codes or incidence geometries [40].

The aim of this work is to examine partition (p-) representations of matroids along the traditional lines of linear and algebraic representation theories. In the next section we observe that the p-representations of a matroid are closely related to the solutions of a system of generalized quasigroup equations associated to the matroid. In Section 3 we are able to classify completely the p-representations of a few small matroids and relate them to some classical generalized quasigroup equations. Based on these results, new examples of non-p-representable matroids are found and an infinite set of excluded minors for the class of p-representable matroids is constructed in Section 4. Finally, we discuss related material and open problems in Section 5.

Definition 1.1. *Let (N, r) be a matroid with the finite ground set N and the rank function r, and let $d \geqslant 2$ be an integer number. The matroid is* p-representable of degree d *if there exist a finite set Ω of cardinality $d^{r(N)}$ and partitions ξ_i of Ω, $i \in N$, such that for every $I \subseteq N$ the meet-partition $\xi_I = \wedge_{i\in I}\xi_i$ has $d^{r(I)}$ blocks all of the same cardinality.*

The above system of partitions $\xi = (\xi_i)_{i\in N}$ will be called p-representation of the matroid of degree d (the letter 'p' abbreviates the word 'partition'). A matroid is *p-representable* if it is p-representable of degree d for some $d \geqslant 2$. A partition with all blocks having the same number of elements will be termed *uniform*. All meet-partitions of a p-representation ξ are uniform: all blocks of ξ_I have the cardinality $d^{r(N)-r(I)}$; especially, $\xi_\emptyset$ has only one block being the whole set Ω and ξ_N has $d^{r(N)}$ blocks being the singletons of Ω.

Before presenting two easy examples we need to fix notation about the Cartesian products and quasigroups. Where $Q \neq \emptyset$ and I are two sets, elements of Q^I will be denoted by $x_I = (x_i)_{i\in I}$ and the coordinate projection of $x_I \in Q^I$ on Q^J, $J \subseteq I$, by $\pi_J(x_I) = (x_i)_{i\in J}$; $Q^\emptyset$ is a fixed one-element set. Subsets S of Q^I will be projected similarly $\pi_J(S) = \{\pi_J(x_I) \in Q^J;\ x_I \in S\}$. If C is a nonempty set then a *C-quasigroup* on $Q \neq \emptyset$ will be for us a special subset $\mathfrak{q}_C$ of Q^C defined as follows. For every $i \in C$, to every $x_{C-i} \in Q^{C-i}$ there exists a unique $y_i \in Q$ such that the C-tuple z_C composed from $\pi_{C-i}(z_C) = x_{C-i}$ and $\pi_i(z_C) = y_i$ belongs to $\mathfrak{q}_C$. The corresponding mappings $\mathfrak{q}_C^i\colon Q^{C-i} \to Q$ are parastrophic quasigroups on Q (of arity $|C|-1$) in the usual sense; for background on the quasigroup theory see [14] and [15]. Note that for all $i \in C$

$$\mathfrak{q}_C = \{x_C \in Q^C;\ \mathfrak{q}_C^i(\pi_{C-i}(x_C)) = \pi_i(x_C)\}\ .$$

Example 1.2. Let (N, r) be the free matroid on N ($r(I) = |I|$, $I \subseteq N$) and Q a finite set of cardinality $d \geqslant 2$. We set $\Omega = Q^N$ and ξ_i, $i \in N$, to be the partition of Ω with the blocks $\{x_N \in \Omega;\ \pi_i(x_N) = a\}$, $a \in Q$. Verbally expressed, the blocks are i-th parallel coordinate layers of Q^N. It is obvious that $\xi = (\xi_i)_{i\in N}$ is a p-representation of the free matroid of degree d. If a partition of an arbitrary subset Ω of Q^N is specified by the coordinate projection as above (its blocks are intersections of the coordinate layers with Ω) we speak about a *coordinate partition* of Ω. The system of all coordinate partitions of any N-quasigroup $\Omega = \mathfrak{q}_N \subseteq Q^N$ on Q can be easily identified as a p-representation of the uniform matroid $U_{n-1,n}$ of degree d. This matroid has a ground set N of the cardinality $n \geqslant 1$ and the rank function $r(I) = \min\{|I|, n-1\}$, $I \subseteq N$; the only circuit of the matroid is $C = N$. $\square$

An intuition, to be formalized below, is that all p-representations of the two examined matroids are 'essentially covered' by the constructed examples.

Definition 1.3. *Two p-representations $\xi = (\xi_i)_{i\in N}$ and $\eta = (\eta_i)_{i\in N}$ of a matroid (N, r), living on two sets Ω_ξ and Ω_η, respectively, are* p-isotopic *if there exists a bijection f of Ω_ξ onto Ω_η such that $f\xi_i = \eta_i$ for all $i \in N$.*

P-isotopic p-representations of a matroid must be of the same degree; η is said to be a *p-isotope* of ξ. Blocks of ξ_I are mapped by f onto blocks of η_I for all $I \subseteq N$.

Let ξ be a p-representation of a matroid of degree d living on Ω_ξ. If Q is a set of the cardinality d and $f_i\colon \Omega_\xi \to Q$ is a function distinguishing and constant on the blocks of ξ_i, $i \in N$, then the composed function f_N defined by $f_N(\omega) = (f_i(\omega))_{i\in N}$, $\omega \in \Omega_\xi$, maps Ω_ξ injectively into Q^N. Let $\Omega_\eta = f_N(\Omega_\xi)$ be the image of Ω_ξ and $\eta_i = f_N\xi_i$ be the partitions of Ω_η. Obviously, $\eta = (\eta_i)_{i\in N}$ is a p-isotope of ξ. It is also straightforward that all partitions within η are the coordinate partitions of Ω_η.

We have just seen that every p-representation ξ of a matroid is p-isotopic to the p-representation η which lives on a subset of a Cartesian product and consists of all coordinate partitions of the subset. It is not difficult to see that $\pi_I(\Omega_\eta) = Q^I$ for any base I of the matroid (and consequently for every independent set of the matroid) and that $\pi_C(\Omega_\eta)$ is a C-quasigroup for every circuit C of the matroid. The following lemma asserts that these two properties characterize those subsets of Cartesian products that support p-representations consisting of coordinate partitions.

Lemma 1.4. *Let N be a finite nonempty set and $\mathcal{I}$ a nonempty hereditary family of subsets of N ($I \in \mathcal{I}$ and $J \subseteq I$ implies $J \in \mathcal{I}$). We denote by $\mathcal{C}$ the family of all inclusion-minimal subsets of N out of $\mathcal{I}$. If Ω is a subset of a Cartesian product Q^N, $|Q| \geqslant 2$ finite, such that $\pi_I(\Omega) = Q^I$ for $I \in \mathcal{I}$ and $\pi_C(\Omega)$ is a C-quasigroup on Q for $C \in \mathcal{C}$ then $\mathcal{I}$ is the family of independent sets of a matroid on N. The coordinate partitions of the set Ω form a p-representation of the matroid of the degree $|Q|$.*

Proof. If the matroid axiom for independent sets were not valid in $\mathcal{I}$ then there exist $I, J \in \mathcal{I}$, $|J| < |I|$ such that $J \cup i \notin \mathcal{I}$ for all $i \in I - J$. Let us chose these I, J to have in addition the cardinality of $J - I$ minimal. This implies $j \cup I \notin \mathcal{I}$ for all $j \in J - I$. Once $j \in J - I$ (and this set must be nonempty) is fixed there exists $C \in \mathcal{C}$ such that $C \subseteq j \cup I$, $j \in C$ and $C - J \neq \emptyset$. For every $i \in C - J$ we can get $\pi_{(I-i)\cup j}(\Omega) = Q^{(I-i)\cup j}$ using that $\pi_I(\Omega) = Q^I$ and $\pi_C(\Omega)$ is a C-quasigroup. Then both sets $(I - i) \cup j$ and J belong to $\mathcal{I}$ and $|J - ((I - i) \cup j)| < |J - I|$. They contradict the choice of I, J.

At the moment we know that the sets from $\mathcal{I}$ are exactly the independent sets of a matroid. Let us recall that to every base I of a matroid and $i \in N - I$ there exists a unique circuit $\gamma(i, I)$ of the matroid contained in $i \cup I$, namely the *fundamental circuit of i in the base I*. Let I be a base of the matroid. Since $\pi_I(\Omega) = Q^I$ the cardinality of Ω is at least $|Q|^{|I|}$. But, if $x_N \in \Omega$ then for every $i \in N - I$ the single coordinate $\pi_i(x_N)$ can be uniquely computed as $\mathfrak{q}^i_{\gamma(i,I)}(\pi_{\gamma(i,I)-i}(x_N))$ where $\mathfrak{q}_{\gamma(i,I)} = \pi_{\gamma(i,I)}(\Omega)$ is a $\gamma(i, I)$-quasigroup on Q. Every $x_N \in \Omega$ is therefore uniquely determined by its projection $\pi_I(x_N)$ and thus $|\Omega| = |Q|^{r(N)}$. If J is a subset of N of rank $r(J)$ we can find a base I of the matroid such that $r(I \cap J) = |I \cap J| = r(J)$. Similarly as above we can recognize that the $(J - I)$-coordinates of any $x_N \in \Omega$ are determined by its $I \cap J$ coordinates. Denoting by ξ_i, $i \in N$, the coordinate partitions of Ω this leads to $\xi_J = \xi_{I\cap J}$. Since $\xi_{I\cap J}$ is a uniform partition of Ω with $|Q|^{|I\cap J|}$ blocks the partition ξ_J is uniform with $|Q|^{r(J)}$ blocks. ∎

In [40], a subset Ω of Q^N, $|Q| \geqslant 2$ finite, is called *almost affine code* if the cardinality of every projection $\pi_I(\Omega)$, $I \subseteq N$, is a power of $|Q|$. The family $\mathcal{I} = \{I \subseteq N;\ \pi_I(\Omega) = Q^I\}$ is nonempty, hereditary and obviously for the minimal C out of $\mathcal{I}$ the projection $\pi_C(\Omega)$ is a C-quasigroup. The above lemma implies that $|\pi_I(\Omega)| = |Q|^{r(I)}$, $I \subseteq N$, for a unique matroid (N, r). The matroids arising in this way, for us the p-representable matroids, are called in [40] almost affinely representable.

Let us remark that in the first half of the previous proof we did not employ the finiteness of Q. Hence, p-representations of degrees which are arbitrary infinite cardinals can be defined as subsets of Cartesian products Q^N satisfying the assumptions of Lemma 1.4. Some results of this paper admit a generalization in this direction but we do not follow this idea here. From now on, all our quasigroups will be on finite sets.

At this moment we can turn back to Example 1.2. and make comments on the p-isotopy classes of p-representations. It is trivial that for the free matroid any two of its p-representations of the same degree are p-isotopic. Let us suppose now that ξ and η are two p-representations of $U_{n-1,n}$, $n \geqslant 1$, living on $\Omega_\xi \subseteq Q^N$ and $\Omega_\eta \subseteq R^N$ and consisting of the coordinate projections, correspondingly. Necessarily, Ω_ξ is an N-quasigroup on Q and Ω_η is an N-quasigroup on R. If the two N-quasigroups are *isotopic*, i.e. there exist bijections $g_i \colon Q \to R$, $i \in N$, such that the composed mapping g_N is a bijection between Ω_ξ and Ω_η, then ξ and η are obviously p-isotopic. But it is not difficult to reverse the assertion, namely, if ξ and η are p-isotopic then every their p-isotopy must have the composed form g_N for some bijections g_i, $i \in N$. Hence, the p-isotopy classes of the p-representations of $U_{n-1,n}$ are in a one-to-one correspondence with the isotopy classes of the usual $(n-1)$-ary nontrivial finite quasigroups. ('Nontrivial quasigroup' means that its supporting set has cardinality at least 2.) This very point made us to decide for the term of p-isotopy.

Example 1.5. Let (N, r) be the uniform matroid $U_{t,n}$ where $0 < t < n = |N|$ and $r(I) = \min\{|I|, t\}$, $I \subseteq N$. A p-representation of $U_{t,n}$ is nothing else but a set $\Omega \subseteq Q^N$ such that the projections $\pi_C(\Omega)$ are C-quasigroups for all C of the cardinality $t+1$; the condition on bases from Lemma 1.4. follows and is thus redundant. These sets Ω correspond, by a fixed base I, $|I| = t$, to the families of $n-t$ orthogonal t-ary quasigroups $\mathfrak{q}^i_{I\cup i}$, $i \in N - I$, where $\mathfrak{q}_{I\cup i} = \pi_{I\cup i}(\Omega)$. (The orthogonality can be defined by demanding injectiveness of the mapping $x_I \mapsto (\pi_{I\cap J}(x_I), (\mathfrak{q}^j_{I\cup j}(x_I))_{j\in J-I})$ for every $J \subseteq N$, $|J| = t$.) In a combinatorial language, the p-representations of uniform matroids of rank at least two are the orthogonal latin hypercubes, see [14]. In coding theory one uses, equivalently, the term 'orthogonal arrays of size $|Q|^t$, n constraints, $|Q|$ levels, strength t, and index 1', cf. [31]; see also [15], Chapter 9. □

To describe efficiently a p-representation of a matroid of small rank we prefer to have the following terminology.

Definition 1.6. *Let (N, r) be a matroid and ξ its p-representation of degree $d \geqslant 2$ on Ω_ξ. A p-isotope η of ξ living on Ω_η is called* coordinatization of ξ w.r.t. a base I *of the matroid if $\Omega_\eta = Q^I$ for some finite set Q of cardinality d and η_i, $i \in I$, are the coordinate partitions of Q^I. When $\eta = \xi$ here we say that ξ is in the* coordinate form w.r.t. I.

It is easy to see that every p-representation ξ can be brought into the coordinate form w.r.t. any basis I of the underlying matroid; it suffices to transform it by a composed function f_I. A partition of Q^I is called a *latin partition* if its blocks can be given as $\{x_I \in Q^I;\ \mathfrak{q}^i_{C-i}(\pi_{C-i}(x_I)) = a\}$, $a \in Q$, where $\mathfrak{q}_C$ is a C-quasigroup on Q, $i \notin I$, and

$i \in C \subseteq i \cup I$. We will use equivalently also the term *level partition of a quasigroup.* Latin partitions are obviously uniform. All 'nonbasical' partitions of a p-representation in the coordinate form w.r.t. a base I are latin, they are constructed from $\gamma(i, I)$-quasigroups, $i \in N - I$. To recognize which $\gamma(i, I)$-quasigroups, $i \in N - I$, can be used to specify a p-representation we will use later this lemma.

Lemma 1.7. *Let I be a base of a matroid (N, r), $\mathfrak{q}_{\gamma(i,I)}$, $i \in N - I$, be a $\gamma(i, I)$-quasigroup on Q, $|Q| \geqslant 2$, and*

$$\Omega = \left\{x_N \in Q^N;\ \pi_i(x_N) = \mathfrak{q}^i_{\gamma(i,I)}(\pi_{\gamma(i,I)-i}(x_N)),\ i \in N - I\right\}.$$

If $\pi_C(\Omega)$ is a C-quasigroup on Q for every circuit C, $|C - I| \geqslant 2$, then the coordinate partitions of Ω (of Q^I together with the level partitions of $\mathfrak{q}_{\gamma(i,I)}$, $i \in N - I$) provide a p-representation of (N, r) (in the coordinate form w.r.t. I).

Proof. By Lemma 1.4. it suffices to prove that $\pi_J(\Omega) = Q^J$ for every base J of the matroid. We proceed by finite induction on $|J - I| = 0, \dots, r(N)$. For $J = I$ it is obvious. If $i \in I - J$ then there exists $j \in \gamma(i, J) - I$ and then $K = (J - j) \cup i$ is a base satisfying $\pi_K(\Omega) = Q^K$ by induction. Since $\pi_{\gamma(i,J)}(\Omega)$ is a $\gamma(i, J)$-quasigroup we can deduce $\pi_J(\Omega) = Q^J$. ∎

A variation on this lemma, to be stated in a moment, will be used repeatedly later. Let $\mathcal{D}$ be a subfamily of the family $\mathcal{C}$ of all circuits of a matroid. Two bases I and J of the matroid are $\mathcal{D}$-*linked* if there exists a sequence of bases $I = I_0, I_1, \dots, I_t = J$, $t \geqslant 0$, such that $|I_s - I_{s+1}| = 1$ and the unique circuit contained in the union of I_s and I_{s+1} belongs to $\mathcal{D}$, $0 \leqslant s < t$. To be linked is a relation of equivalence.

Lemma 1.8. *Let (N, r) be a paving matroid, $r(N) \geqslant 2$, I be its base and the family $\mathcal{D}$ contain its circuits C, $|C| = r(N)$, $|C - I| \geqslant 2$. Let $\mathcal{D}' = \mathcal{D} \cup \{\gamma(i, I);\ i \in N - I\}$ and $\mathcal{B}'$ be an arbitrary family of its bases such that every base not $\mathcal{D}'$-linked to I is $\mathcal{D}'$-linked to some base from $\mathcal{B}'$. Let a set Ω be constructed from $\gamma(i, I)$-quasigroups on Q as in Lemma 1.7. If the projections $\pi_C(\Omega)$ are C-quasigroups for $C \in \mathcal{D}$ and $\pi_J(\Omega) = Q^J$ for $J \in \mathcal{B}'$ then the coordinate partitions of Ω p-represent the matroid (N, r).*

Proof. First, let us observe that $\pi_C(\Omega)$ is a C-quasigroups for $C \in \mathcal{D}'$. If $\pi_J(\Omega) = Q^J$ for some base J then the same is valid for any base $\mathcal{D}'$-linked to J. Consequently, we have it for all bases of the matroid. By Lemma 1.4. it remains to show that $\pi_C(\Omega)$ is a C-quasigroup for every circuit C, $|C - I| \geqslant 2$, of the cardinality $r(N) + 1$. This is obvious because the set Ω has $|Q|^{r(N)}$ elements and $\pi_{C-i}(\Omega) = Q^{C-i}$ for any i in such a set C. ∎

2. Matroid quasigroup equations.

In the next definition we are going to associate a new system of equations to every matroid. They belong to the class of generalized quasigroup equations, for definitions see [6] and for a recent progress on the topic [24]. Some authors prefer to speak alternatively about general quasigroup identities or about functional equations for functions with more general domains. The unknowns in these equations are quasigroups (functions) which after substitutions of their arguments satisfy ordinary quasigroup equations.

Definition 2.1. *Let (N, r) be a matroid and Q a nonempty set. A family of C-quasigroups $\mathfrak{q}_C$ on Q for C running through all circuits of the matroid solves the* matroid quasigroup equations *if the following is satisfied. For every base I, for every $i \in N - I$,* *for every circuit C containing i and for every $x_I \in Q^I$*

$$\mathfrak{q}^i_{\gamma(i,I)}(\pi_{\gamma(i,I)-i}(x_I)) = \mathfrak{q}^i_C(y_{C-i})$$

where $y_{C-i} = (y_j)_{j\in C-i}$ has the coordinates $y_j = \mathfrak{q}^j_{\gamma(j,I)}(\pi_{\gamma(j,I)-j}(x_I))$ for $j \in C-(i\cup I)$ and $y_j = x_j$ for $j \in C\cap I$. In a single instance of I, i and C we speak about a matroid quasigroup equation *of (N,r).*

For a free matroid the system of its matroid quasigroup equations is empty and it is solved by the void family of quasigroups. If (N,r) is the uniform matroid $U_{n-1,n}$, having the single circuit $C = N$, every N-quasigroup solves its matroid quasigroup equations. Indeed, the displayed equations are always trivially satisfied if $C = \gamma(i,I)$; from now on we consider only C distinct from $\gamma(i,I)$. If the cardinality of Q in Definition 2.1. is one the matroid quasigroup equations have a unique solution to be called trivial.

Example 2.2. Let $N = \{1,2,3,4\}$ and $U_{2,4} = (N,r)$ be the uniform matroid of rank two on N. There are 24 matroid quasigroup equations of $U_{2,4}$. The unknowns are four C-quasigroups $\mathfrak{q}_{123}$, $\mathfrak{q}_{124}$, $\mathfrak{q}_{134}$ and $\mathfrak{q}_{234}$ on a set Q (we should write correctly $\mathfrak{q}_{\{1,2,3\}}$, etc.). Two of the equations have the form

$$\begin{aligned} \mathfrak{q}^4_{134}(x_1,x_3) &= \mathfrak{q}^4_{124}(x_1,\mathfrak{q}^2_{123}(x_1,x_3)), \qquad && x_1,x_3 \in Q,\\ \mathfrak{q}^4_{234}(x_2,x_3) &= \mathfrak{q}^4_{124}(\mathfrak{q}^1_{123}(x_2,x_3),x_2), \qquad && x_2,x_3 \in Q, \end{aligned}$$

being indexed by $i = 4 \in C = \{1,2,4\}$, $I = \{1,3\}$ and $I = \{2,3\}$, respectively. Note that $I\cap C$ is always a singleton. Schematically we will write e.g. $4(1,3) = 4(1,2(1,3))$ as an abbreviation for the first equation.

For given $j \in N$ let us consider the group of six equations indexed by I, i and C satisfying $I \cap C = j$. The equation $4(1,3) = 4(1,2(1,3))$ belonging to the first group can be rewritten equivalently as $4(1,2) = 4(1,3(1,2))$ or $2(1,3) = 2(1,4(1,3))$ and further as $2(1,4) = 2(1,3(1,4))$ or $3(1,2) = 3(1,4(1,2))$ or $3(1,4) = 3(1,2(1,4))$. Hence, by symmetry, the six matroid equations within each of the four groups are mutually equivalent. The displayed two equations belong to the first and second group, respectively. If rewritten as $4(1,2) = 4(1,3(1,2))$ and $4(1,2) = 4(2,3(1,2))$, they can be compared to derive an equation $4(1,3) = 4(2(1,3),3)$ of the third group. One can recast them also into $3(1,2) = 3(1,4(1,2))$ and $3(1,2) = 3(2,4(1,2))$ leading to an equation of the fourth group $3(1,4) = 3(2(1,4),4)$. We conclude that the starting two equations are equivalent to the whole system of 24 equations.

Recasting the two above equations into

$$\begin{aligned} \mathfrak{q}^4_{124}(x_1,x_2) &= \mathfrak{q}^4_{134}(x_1,\mathfrak{q}^3_{123}(x_1,x_2)), \qquad && x_1,x_2 \in Q,\\ \mathfrak{q}^4_{124}(x_1,x_2) &= \mathfrak{q}^4_{234}(x_2,\mathfrak{q}^3_{123}(x_1,x_2)), \qquad && x_2,x_2 \in Q, \end{aligned}$$

wee see that the mapping $(x_1,x_2) \mapsto (\mathfrak{q}^3_{123}(x_1,x_2)),\mathfrak{q}^4_{124}(x_1,x_2))$ must be bijective. In the language of quasigroup theory, $\mathfrak{q}^3_{123}$ and $\mathfrak{q}^4_{124}$ are orthogonal. In the oposite direction, if $\mathfrak{r}^3_{123}$ and $\mathfrak{r}^4_{124}$ are two orthogonal binary quasigroups on Q then the mappings $(x_1,x_3) \mapsto \mathfrak{r}^4_{124}(x_1,\mathfrak{r}^2_{123}(x_1,x_3))$ and $(x_2,x_3) \mapsto \mathfrak{r}^4_{124}(\mathfrak{r}^1_{123}(x_2,x_3),x_2)$ define two quasigroups on Q to be denoted by $\mathfrak{r}^4_{134}$ and $\mathfrak{r}^4_{234}$, respectively. The quadruple of C-quasigroups $(\mathfrak{r}_{123},\mathfrak{r}_{124},\mathfrak{r}_{134},\mathfrak{r}_{234})$ solves the matroid quasigroup equations of $U_{2,4}$, cf. Example 1.5. □

Definition 2.3. *Let (N,r) be a matroid with the collection of circuits $\mathcal{C}$. A family $(\mathfrak{q}_C)_{C\in\mathcal{C}}$ of C-quasigroups on a set Q is said to be* simultaneously isotopic *with a family*

$(\mathfrak{r}_C)_{C\in\mathcal{C}}$ *of* C*-quasigroups on a set* R *if there exist bijections* $g_i\colon Q\to R$, $i\in N$, *such that* $(x_i)_{i\in C}\in\mathfrak{q}_C$ *if and only if* $(g_i x_i)_{i\in C}\in\mathfrak{r}_C$ *for all* $C\in\mathcal{C}$.

It is a matter of easy technicalities to see that if a family $(\mathfrak{q}_C)_{C\in\mathcal{C}}$ solves the matroid quasigroup equations then every its simultaneous isotope solves the same set of equations as well. The simultaneous isotopy is a natural equivalence on the class of all solutions of the matroid quasigroup equations. The main result of this section establishes a connection between p-representations and matroid quasigroup equations.

Proposition 2.4. *For any matroid* (N,r) *there is a one-to-one correspondence between the p-isotopy classes of the p-representations of* (N,r) *and the simultaneous isotopy classes of the nontrivial solutions of the matroid quasigroup equations associated to* (N,r).

Proof. If a family $(\mathfrak{q}_C)_{C\in\mathcal{C}}$ of C-quasigroups on Q, $|Q|\geqslant 2$, solves the matroid quasigroup equations of (N,r) we set

$$\Omega=\left\{x_N\in Q^N;\ \pi_C(x_N)\in\mathfrak{q}_C \text{ once } C\in\mathcal{C}\right\}.$$

Let I be any base and $\Omega_{[I]}$ be defined as in Lemma 1.7.; obviously $\Omega\subseteq\Omega_{[I]}$. If $x_N\in\Omega_{[I]}$ then, for every circuit C, the matroid quasigroup equations (indexed by the base I) imply $x_i=\mathfrak{q}^i_C(\pi_{C-i}(x_N))$, $i\in C-I$, i.e. $\pi_C(x_N)\in\mathfrak{q}_C$. Thus, $\Omega=\Omega_{[I]}$ what entails $\pi_J(\Omega)=Q^J$ for every independent set J. For circuits, the inclusion $\pi_C(\Omega)\subseteq\mathfrak{q}_C$ is trivial but it cannot be strict due to $\pi_{C-i}(\Omega)=Q^{C-i}$, $i\in C$. Using Lemma 1.4. we see that we ascribed to every nontrivial solution $(\mathfrak{q}_C)_{C\in\mathcal{C}}$ a p-representation living on Ω. To a simultaneously isotopic solution a p-isotopic p-representation is ascribed in this way.

In the opposite direction, let ξ be a p-representation of (N,r). One can suppose ξ to live on $\Omega\subseteq Q^N$ (and to consist of the coordinate partitions of Ω, as usually in these cases). We are going to show that the family of C-quasigroups $\mathfrak{q}_C=\pi_C(\Omega)$, $C\in\mathcal{C}$, constructed from Ω solves the matroid quasigroup equations of (N,r). Now, let I, i, C, x_I and y_{C-i} be as in Definition 2.1. We saw in the proof of Lemma 1.4. that to every $x_I\in Q^I$ there is a unique $x_N\in\Omega$ such that $\pi_I(x_N)=x_I$. The 'additional' coordinates of x_N are $\mathfrak{q}^j_{\gamma(j,I)}(\pi_{\gamma(j,I)-j}(x_I))$, $j\in N-I$. Hence, $\pi_{C-i}(x_N)=y_{C-i}$. The i-th coordinate of x_N must be therefore equal to $\mathfrak{q}^i_C(y_{C-i})$ owing to $\pi_C(x_N)\in\mathfrak{q}_C$ and, at the same time, to $\mathfrak{q}^i_{\gamma(i,I)}(\pi_{\gamma(i,I)-i}(x_I))$ owing to $\pi_{\gamma(i,I)}(x_N)\in\mathfrak{q}_{\gamma(i,I)}$. Therefore, every p-representation of the matroid gives rise to a nontrivial solution of the matroid quasigroup equations. It is also easy to show that p-isotopes of the p-representation give rise to simultaneous isotopes of the solution. ∎

Now, it becomes evident that the p-representations can be systematically studied in the disguise of quasigroup equations: according to Proposition 2.4. a matroid is p-representable if and only if the system of its matroid quasigroup equations has a nontrivial solution. A look into the first part of the previous proof reveals that the equality $\Omega=\Omega_{[I]}$ for a base I is equivalent to the assertion '$(\mathfrak{q}_C)_{C\in\mathcal{C}}$ solves the subsystem of those matroid quasigroup equations which are indexed by the very base I, any $i\in N-I$ and any circuit C containing i'. If the equality takes place for one base then it is valid for all bases because the sets $\Omega_{[I]}$ contain Ω and have the same cardinality. Therefore, while solving the matroid quasigroup equations for a matroid one can fix an appropriate base I of the matroid freely, cf. Example 2.2.

3. P-representations of some small matroids. Given a matroid and an integer $d\geqslant 2$ the problem is to recognize whether the matroid is p-representable of degree d

and, if it is for some d, then to classify its p-isotopy classes. We have seen that this is a difficult task even for such 'easy' matroids as the uniform matroids. In this section we confine ourselves to three relatively small p-representable matroids, namely $\mathsf{M}(K_4)$, $\mathsf{M}^*(K_{3,3})$ and P_7 in the notation of [38], and describe the structure of their p-isotopy classes. Their matroid quasigroup equations will be related to some classical generalized quasigroup equations that are here, in fact, resolved in a new geometric way.

First, let us consider the graphic matroid $\mathsf{M}(K_4)$, i.e. the cycle matroid of the clique on four vertices. This matroid has rank three, the ground set $N = \{1, 2, 3, 4, 5, 6\}$, and seven circuits $\{1, 2, 4\}$, $\{1, 3, 6\}$, $\{2, 3, 5\}$, $\{4, 5, 6\}$, $\{1, 2, 5, 6\}$, $\{1, 3, 4, 5\}$, $\{2, 3, 4, 6\}$, as drawn on Fig. 1 left.

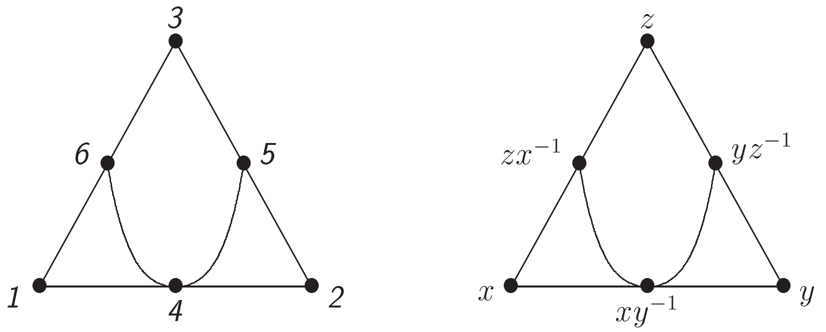


Figure 1. P-representations of $\mathsf{M}(K_4)$ via groups.

Let $(G, \cdot)$ be a finite multiplicative group of order $d \geqslant 2$ and let the labels in Fig. 1 right define six partitions of G^3 as follows. For the points 1, 2 and 3 the partitions $\xi_1^{(G,\cdot)}$, $\xi_2^{(G,\cdot)}$ and $\xi_3^{(G,\cdot)}$ consist of the x-, y- and z-coordinate layers of G^3, respectively, and further

$$\xi_4^{(G,\cdot)} = \big\{\{(x, y, z) \in G^3;\ xy^{-1} = a\};\ a \in G\big\}$$
$$\xi_5^{(G,\cdot)} = \big\{\{(x, y, z) \in G^3;\ yz^{-1} = a\};\ a \in G\big\}$$
$$\xi_6^{(G,\cdot)} = \big\{\{(x, y, z) \in G^3;\ zx^{-1} = a\};\ a \in G\big\}$$

are level partitions of three binary quasigroups. Equivalently, one can imagine the six coordinate partitions of

$$\Omega^{(G,\cdot)} = \big\{(x, y, z, xy^{-1}, yz^{-1}, zx^{-1}) \in G^6;\ x, y, z \in G\big\}\ .$$

Using symmetries, it is not difficult to see directly from Definition 1.1. that the system of partitions $\xi^{(G,\cdot)} = (\xi_i^{(G,\cdot)})_{i\in N}$ is a p-representation of $\mathsf{M}(K_4)$ of degree d in the coordinate form w.r.t. the base $|I| = \{1, 2, 3\}$. (Since the matroid is paving one can apply also Lemma 1.8. where $\mathcal{D}$ contains $\{4, 5, 6\}$ and all 16 bases are $\mathcal{D}'$-linked; then only $\pi_{\{4,5,6\}}(\Omega^{(G,\cdot)})$ is to be examined.) Note e.g. that $\xi_{\{4,5\}}^{(G,\cdot)} = \xi_{\{4,6\}}^{(G,\cdot)} = \xi_{\{5,6\}}^{(G,\cdot)} = \xi_{\{4,5,6\}}^{(G,\cdot)}$ has d^2 blocks of size d. No other p-representations of $\mathsf{M}(K_4)$ are, in fact, possible as expressed by the following assertion.

Proposition 3.1. *Every p-representation of $\mathsf{M}(K_4)$ is p-isotopic to the system of partitions $\xi^{(G,\cdot)}$ constructed from a finite group $(G, \cdot)$. Two p-representations $\xi^{(G,\cdot)}$ and $\xi^{(H,\circ)}$ are p-isotopic if and only if the groups $(G, \cdot)$ and $(H, \circ)$ are isomorphic.*

Proof. Let η be a p-representation of $\mathsf{M}(K_4)$ in the coordinate form w.r.t. the base $I = \{1, 2, 3\}$ and let η live on G^3. Blocks of η_4 have the form $A \times G$ where A ranges over blocks of a latin partition $\sim$ of G^2 and, cyclically, blocks of η_5 and η_6 originate from latin partitions $\approx$ and $\approxeq$, respectively. Permuting y- and z-layers of G^3 we can suppose that the diagonal of G^2, $\mathrm{diag}(G^2) = \{(x, x) \in G^2;\ x \in G\}$, is a block in $\sim$ and also in $\approx$; this corresponds to taking an appropriate p-isotope of η at the beginning. The implication (we employ $\sim$, $\approx$ and $\approxeq$ also as equivalences on G^2)

$$\big[(a_1,b_1)\sim(a_2,b_2) \text{ and } (b_1,c_1)\approx(b_2,c_2)\big] \Rightarrow (c_1,a_1)\approxeq(c_2,a_2)$$

follows from the fact that if (a_1,b_1,c_1) and (a_2,b_2,c_2) are in the same block of $\eta_{\{4,5\}}$ then they are in the same block of η_6. Taking $a_1=b_1$ and $a_2=b_2$ we conclude $\approx^{\mathsf{tr}}=\approxeq$ and $b_1=c_1$ and $b_2=c_2$ entails $\sim^{\mathsf{tr}}=\approxeq$. Here, blocks of the transposed partition $\sim^{\mathsf{tr}}$ are $\{(x,y)\in G^2;\ (y,x)\in A\}$, $A\in\sim$. Note that $\operatorname{diag}(G^2)$ is now a block of $\approxeq$. Due to the cyclical symmetry all three partitions coincide and are selftransposed.

Double use of the above implication yields

$$\big[(a_1,c_1)\sim(a_2,c_2) \text{ and } (a_1,d_1)\sim(a_2,d_2) \text{ and } (b_1,c_1)\sim(b_2,c_2)\big] \Rightarrow (b_1,d_1)\sim(b_2,d_2)$$

i.e. the *quadrangle criterion* for $\sim$, see [14], p. 18. Namely, $(d_1,a_1)\sim(d_2,a_2)$ combined with $(a_1,c_1)\sim(a_2,c_2)$ imply $(d_1,c_1)\sim(d_2,c_2)$, which together with $(b_1,c_1)\sim(b_2,c_2)$ lead to the claim. Standard considerations around the Cayley tables of groups, quasigroups and latin squares entail existence of a group $(G,\cdot)$ such that blocks of the partition $\sim$ are $\{(x,y)\in G^2;\ xy^{-1}=a\}$, $a\in G$.

If $\xi^{(G,\cdot)}$ and $\xi^{(H,\circ)}$ are p-isoptopic p-representations of $M(K_4)$ then the p-isotopy between them must have the form $(x,y,z)\mapsto(\alpha(x),\beta(y),\gamma(z))$ where α, β and γ are three bijections of G onto H. Since blocks of $\xi_4^{(G,\cdot)}$ are moved onto blocks of $\xi_4^{(H,\circ)}$ we deduce that $\alpha(x)\circ\beta(y)^{-1^\circ}=\rho(xy^{-1})$, $x,y\in G$, for a bijection ρ; on the left the inversion in $(H,\circ)$ is to be performed. But then $(G,\cdot)$ and $(H,\circ)$ are isotopic and thus isomorphic. The opposite implication of the second assertion is trivial. ∎

As a consequence, the p-isotopy classes of $M(K_4)$ correspond exactly to the isomorphism classes of finite groups with the trivial exception of the class of one-element groups.

Let $\xi^{(G,\cdot)}$ be the p-representation of $M(K_4)$ from Fig. 1. Its p-isotope $f\xi^{(G,\cdot)}$ obtained by use of the permutation $f(x,y,z)=(x,y^{-1},yz^{-1})$ of G^3 is depicted in the middle of Fig. 2. The associative law is included there not accidentally. The following classical result on generalized associativity of quasigroups, see [3], [6], [1], [14], can be now easily reproved.

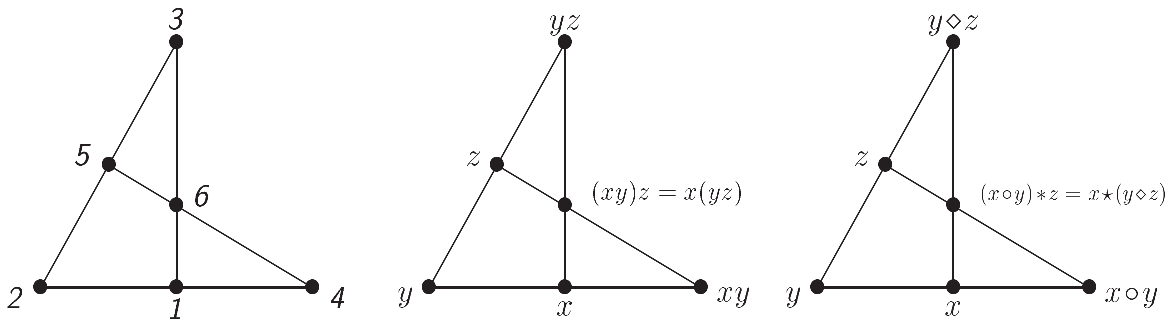


Figure 2. General associative law.

Consequence 3.2. *If four binary quasigroup operations on a finite set Q satisfy the equation $(x\circ y)*z=x\star(y\diamond z)$ for all $x,y,z\in Q$ then there exist a group $(Q,\cdot)$, unique up to isomorphisms, and five permutations α, β, γ, δ, ϵ of Q such that*

$$x\circ y=\delta^{-1}(\alpha(x)\cdot\beta(y)) \qquad x*z=\delta(x)\cdot\gamma(z)$$
$$y\diamond z=\epsilon^{-1}(\beta(y)\cdot\gamma(z)) \qquad x\star z=\alpha(x)\cdot\epsilon(z)$$

is valid for all $x,y,z\in Q$.

Proof. Owing to Lemma 1.8. we see ($I = \{1, 2, 5\}$, all bases are $\mathcal{D}'$-linked) that Fig. 2 right defines a p-representation $\eta^{\circ\ast\star\diamond}$ of $M(K_4)$ living on Q^3, provided Q has at least two elements. By Proposition 3.1. this $\eta^{\circ\ast\star\diamond}$ must be a p-isotope of the p-representation $\xi^{(G,\cdot)}$ defined by Fig. 2 middle with an appropriate underlying group $(G, \cdot)$, $G = Q$. The p-isotopy has necessarily the following form $(x, y, z) \mapsto (\alpha^{-1}(x), \beta^{-1}(y), \gamma^{-1}(z))$ where α, β and γ are permutations of Q. Since the level partitions of the quasigroups $(x, y) \mapsto \alpha(x) \cdot \beta(y)$ and $(x, y) \mapsto x \circ y$ are identical we have $x \circ y$ in the announced form and similarly with $y \diamond z$. The same argumentation applies to the level partitions (of the set G^3) of the ternary quasigroups $(x, y, z) \mapsto \alpha(x) \cdot \beta(y) \cdot \gamma(z)$ and $(x, y, z) \mapsto (x \circ y) \ast z$ yielding $(x \circ y) \ast z = \phi(\alpha(x) \cdot \beta(y) \cdot \gamma(z)) = x \star (y \diamond z)$. By choice of an isomorph of the group $(G, \cdot)$ the permutation ϕ can be set equal to the identity. For the uniqueness of the five permutations see [3]. ∎

Since the matroid $M(K_4)$ has seven circuits its matroid quasigroups equations involve seven C-quasigroups, e.g. ($I = \{1, 2, 3\}$, $i = 4$ and $C = \{4, 5, 6\}$)

$$\mathfrak{q}^{4}_{124}(x_1, x_2) = \mathfrak{q}^{4}_{456}\big(\mathfrak{q}^{5}_{235}(x_2, x_3), \mathfrak{q}^{6}_{136}(x_1, x_3)\big), \qquad x_1, x_3 \in Q,$$

which is the general transitive equation for quasigroups, cf. [6] p. 97 and [14] p. 76. By the substitution $x_6 = \mathfrak{q}^{6}_{136}(x_1, x_3)$ the (equivalent) general associative law is obtained. The latter is not a matroid quasigroup equation. To solve the matroid quasigroup equations of $M(K_4)$ one can restrict to the single general associative (or transitive) law and the three equations (for schematic forms see Example 2.2.) $4(1, 2) = 4(1, 3, 5(2, 3))$, $5(2, 3) = 5(1, 2, 6(1, 3))$, and $6(1, 3) = 6(2, 3, 4(1, 2))$. Indeed, four quasigroups $\mathfrak{q}^{4}_{124}$, $\mathfrak{q}^{5}_{235}$, $\mathfrak{q}^{6}_{136}$ and $\mathfrak{q}^{4}_{456}$ solving the above displayed equation can be used to construct three nonbasic partitions of a p-representation of $M(K_4)$ similarly as in the previous proof. For them and for the C-quasigroups $\mathfrak{q}_{1256}$, $\mathfrak{q}_{1345}$, $\mathfrak{q}_{2346}$ constructed from the three equations the remainig matroid quasigroup equations must be valid; an argumentation is as in the second part of the proof of Proposition 2.4.

Let $M^{*}(K_{3,3})$ be the cocycle (bond) matroid of the complete bipartite graph $K_{3,3}$, see [38] p. 89 and p. 514. It has nine points, $N = \{1, 2, \ldots, 9\}$, and rank four. Fig. 3 left exhibits its affine representation.

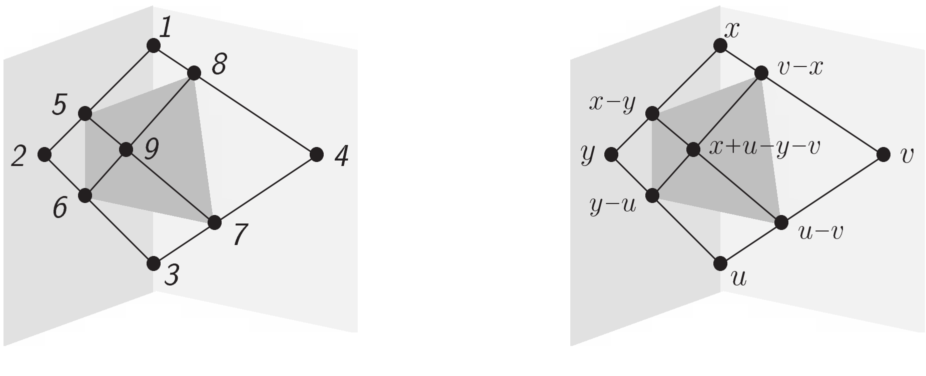


Figure 3. P-representations of $M^{*}(K_{3,3})$ via Abelian groups.

Let $(G, +)$ be a finite Abelian group of order $d \geqslant 2$ and $\xi^{(G,+)}$ be defined by Fig. 3 right similarly as in the case of $M(K_4)$, for example

$$\xi^{(G,+)}_{9} = \big\{\{(x, y, u, v) \in G^4;\ x + u - y - v = a\};\ a \in G\big\}\ .$$

It is easy but a bit laborious to verify that this system of partitions of G^4 is a p-representation of $M^*(K_{3,3})$ in the coordinate form w.r.t. $I = \{1, 2, 3, 4\}$ (we listed the 24 minimal edge-cutsets of $K_{3,3}$ corresponding to the circuits of $M^*(K_{3,3})$, and for each circuit we checked visually in Fig. 3 right that the assumptions of Lemma 1.7. are satisfied).

Proposition 3.3. *Every p-representation of $M^*(K_{3,3})$ is p-isotopic to $\xi^{(G,+)}$ for a finite Abelian group $(G, +)$. Two p-representations $\xi^{(G,+)}$ and $\xi^{(H,\oplus)}$ are p-isotopic if and only if the underlying Abelian groups are isomorphic.*

Proof. Let η be a p-representation of $M^*(K_{3,3})$ in the coordinate form w.r.t. the base $I = \{1, 2, 3, 4\}$ and let η live on G^4. Blocks of η_5 are $A \times G^2$ for A from a latin partition $\sim$ of G^2 and cyclically for η_6, η_7 and η_8 with $\approx$, $\approxeq$ and $\approxeq$, respectively. By permuting y-, u- and v-layers of G^4 we can have $\mathrm{diag}(G^2) \in \sim \cap \approx \cap \approxeq$. Two quadruples (a_1, b_1, c_1, d_1) and (a_2, b_2, c_2, d_2) in the same block of $\eta_{\{5,6,7\}}$ must be in the same block of η_8 because 5,6,7 and 8 are coplanar. Thus,

$$\big[(a_1, b_1) \sim (a_2, b_2) \text{ and } (b_1, c_1) \approx (b_2, c_2) \text{ and } (c_1, d_1) \approxeq (c_2, d_2)\big] \Rightarrow (d_1, a_1) \approxeq (d_2, a_2)\ .$$

If $c_1 = d_1$ and $c_2 = d_2$ then we have exactly the first implication of the proof of Proposition 3.1., which yields $\sim^{\mathsf{tr}} = \approx^{\mathsf{tr}} = \approxeq$ and $\mathrm{diag}(G^2) \in \approxeq$. By symmetry, all four partitions coincide and the blocks of $\sim = \sim^{\mathsf{tr}}$ can be described by a group $(G, \cdot)$. Let $1 \in G$ be the identity element of $(G, \cdot)$ and $\equiv$ be the equivalence on G^4 corresponding to η_9. Then $(1, 1, 1, 1) \equiv (1, 1, b, b)$ as $\eta_{\{5,7\}} = \eta_{\{5,7,9\}}$ and $(1, 1, b, b) \equiv (1, a, ba, b)$ as $\eta_{\{6,8\}} = \eta_{\{6,8,9\}}$. Similarly, $(1, 1, 1, 1) \equiv (1, a, a, 1) \equiv (1, a, ab, b)$ and the latinness of $\equiv$ implies that the group is commutative, $\cdot = +$ and $1 = 0$. The blocks of η_9 are then recognizable from

$$(a, 0, 0, 0) \equiv (x, x - a, 0, 0) \equiv (x, y, y - x + a, 0) \equiv (x, y, u, u - y + x - a)\ .$$

The remaining assertion can be proved by analogous arguments as in the proof of Proposition 3.1. ■

Let us transform a p-representation $\xi^{(G,+)}$ of $M^*(K_{3,3})$ by the function f specified as $f(x, y, u, v) = (x, -y, u, -v)$. One obtains the p-isotope $f\xi^{(G,+)}$ exhibited in Fig. 4 left. The label of the central point is nothing else as the medial law, see [3] and [6] p. 96.

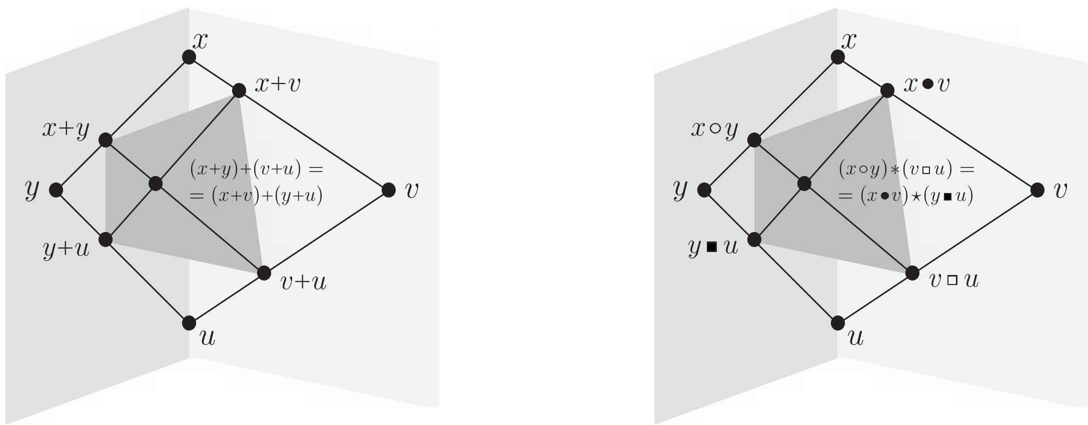


Figure 4. General medial law.

Consequence 3.4. *If six binary quasigroup operations on a finite set Q satisfy the equation $(x \circ y) * (v \,\square\, u) = (x \bullet v) \star (y \blacksquare u)$ for all $x, y, u, v \in Q$ then there exist an Abelian* *group $(G,+)$, unique up to isomorphisms, and eight permutations α, β, γ, δ, $\hat\alpha$, $\hat\beta$, $\hat\gamma$ and $\hat\delta$ of Q such that*

$$x \circ y = \hat\alpha^{-1}(\alpha(x) + \beta(y)) \qquad x \bullet v = \hat\delta^{-1}(\alpha(x) + \delta(v)) \qquad x * y = \hat\alpha(x) + \hat\gamma(y)$$
$$v \,\square\, u = \hat\gamma^{-1}(\delta(v) + \gamma(u)) \qquad y \blacksquare u = \hat\beta^{-1}(\beta(y) + \gamma(u)) \qquad x \star y = \hat\delta(x) + \hat\beta(y) \ .$$

Proof. Fig. 4 right defines a p-representation $\eta^{\circ*\square\bullet\star\blacksquare}$ of $M^*(K_{3,3})$ on Q^4, $|Q| \geqslant 2$. This $\eta^{\circ*\square\bullet\star\blacksquare}$ is p-isotopic to the p-representation $\xi^{(G,+)}$ defined by Fig. 4 left based on an Abelian group $(G,+)$, $G = Q$. Every p-isotopy between them must have the following form $(x,y,u,v) \mapsto (\alpha^{-1}(x), \beta^{-1}(y), \gamma^{-1}(u), \delta^{-1}(v))$. Then the operations $\circ$, $\square$, $\bullet$ and $\blacksquare$ can be obviously expressed as announced; the argumentation is exactly the same as in the proof of Consequence 3.2. Further,

$$(x\circ y)*(v\square u) = \phi(\alpha(x) + \beta(y) + \gamma(u) + \delta(v)) = (x\bullet v)\star(y\blacksquare u)$$

for a permutation ϕ of Q whence

$$(x\circ y)*(v\square u) = \phi(\hat\alpha(x\circ y) + \hat\gamma(v\square u)) = \phi(\hat\delta(x\bullet v) + \hat\beta(y\square u)) = (x\bullet v)\star(y\blacksquare u) \ .$$

By choice of an isomorph of $(G,+)$ one can drop out ϕ. ∎

The general distributive law $x\star(y\circ z) = (x\square y)*(x\diamond z)$, $x,y,z \in Q$, has not been solved completely for arbitrary quasigroups, cf. [1], [2] and [24]. It is not a balanced equation, see [41]. Obviously, when five quasigroup operations $\star$, $\circ$, $\square$, $*$ and $\diamond$ solve the equation then also the following five quasigroup operations

$$x \circledast y = \phi(\alpha(x) \star \hat\alpha(y)) \qquad y \circledcirc z = \hat\alpha^{-1}(\beta(y) \circ \gamma(z))$$
$$x \circledast y = \phi(\hat\beta(x) * \hat\gamma(y)) \qquad x \boxed{\circ}\, y = \hat\beta^{-1}(\alpha(x) \square \beta(y))$$
$$x \circledcirc z = \hat\gamma^{-1}(\alpha(x) \diamond \gamma(z))$$

constructed by use of arbitrary seven permutations α, β, γ, $\hat\alpha$, $\hat\beta$, $\hat\gamma$ and ϕ solve the equation, as well. The two quintuples of operations will be termed *equivalent.*

Proposition 3.5. *Let Q be a finite set of cardinality $d \geqslant 2$. There is a bijective correspondence between the equivalence classes of the solutions $(\star,\circ,\square,*,\diamond)$ of the general distributive law, consisting of quintuples of quasigroups on Q, and the p-isotopy classes of degree d of the matroid P_7 from Fig. 5 left.*

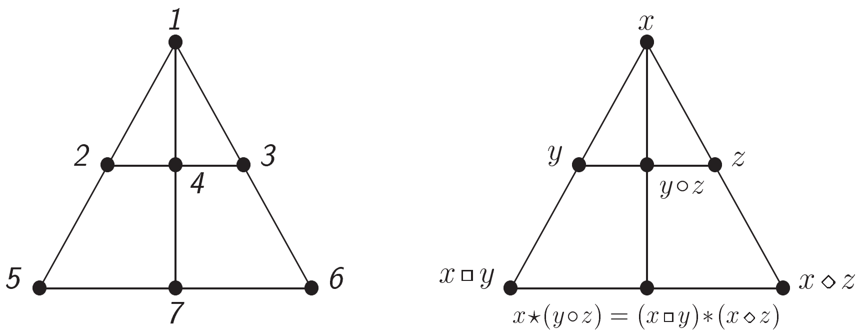


Figure 5. General distributive law and p-representations of P_7.

Proof. If a quintuple $(\star,\circ,\square,*,\diamond)$ solves the identity then Fig. 5 right defines a p-representation $\eta^{\star\circ\square*\diamond}$ of P_7 in the usual way (use Lemma 1.8. where $I = \{1,2,3\}$ and

$\mathcal{D}$ contains $\{\mathit{1}, \mathit{4}, \mathit{7}\}$ and $\{\mathit{5}, \mathit{6}, \mathit{7}\}$; all bases are $\mathcal{D}'$-linked). If another quintuple of circled operations is equivalent to the starting one then $\eta^{\circledstar\circledcirc\boxdot\circledast\circleddiamond}$ is p-isotopic to $\eta^{\star\circ\square*\diamond}$ by a mapping $(x, y, z) \mapsto (\alpha^{-1}(x), \beta^{-1}(x), \gamma^{-1}(x))$ constructed from three permutations. For example, the block $\{(x, y, z);\ y \circ z = a,\ x, y, z \in Q\}$, $a \in Q$, of $\eta_{\mathit{4}}^{\star\circ\square*\diamond}$ is mapped onto

$$\big\{\big(x, \beta^{-1}(y), \gamma^{-1}(y \mathbin{\backslash\!\!\!\circ} a)\big);\ x, y \in Q\big\} = \big\{(x, y, z);\ \hat{\alpha}^{-1}(\beta(y) \circ \gamma(z)) = \hat{\alpha}^{-1}(a),\ x, y, z \in Q\big\} =$$
$$= \big\{(x, y, z);\ y \circledcirc z = \hat{\alpha}^{-1}(a),\ x, y, z \in Q\big\}$$

where $y \circ z = a$ is equivalent to $y \mathbin{\backslash\!\!\!\circ} a = z$. We have been employing the standart notation for parastrophs, see [15], p. 206, in this proof. Thus an equivalence class of quintuples is transformed into a p-isotopy class via Fig. 5 right.

If ξ is a p-representation of P_7 on Q^3 in the coordinate form w.r.t. $I = \{\mathit{1}, \mathit{2}, \mathit{3}\}$ then ξ_{4}, ξ_{5} and ξ_{6} can be specified by binary quasigroup operations $\circ$, $\square$ and $\diamond$ on Q, respectively. Having a look at the p-isotope $f\xi$ of ξ where $f(x, y, z) = (x, y \circ z, z)$ we see that $f\xi_{\mathit{7}}$ has the blocks $\{(x, y, z);\ x \star y = a,\ x, y, z \in Q\}$, $a \in Q$, for a quasigroup operation $\star$. Hence, the blocks of ξ_{7} are

$$f^{-1}\{(x, x \mathbin{\backslash\!\!\!\star} a, z);\ x, z \in Q\} = \{(x, (x \mathbin{\backslash\!\!\!\star} a) \mathbin{/\!\!\!\circ} z, z);\ x, z \in Q\} =$$
$$= \{(x, y, z);\ x * (y \circ z) = a,\ x, y, z \in Q\}$$

where $f^{-1}(x, y, z) = (x, y \mathbin{/\!\!\!\circ} z, z)$. A closer examination of the second p-isotope $g\xi$ where $g(x, y, z) = (x, x \square y, x \diamond z)$ reveals analogously that the blocks of ξ_{7} are

$$\{(x, y, z);\ (x \square y) \circledast (x \diamond z) = a,\ x, y, z \in Q\}, \qquad a \in Q,$$

for an operation $\circledast$. Finally, we arrive at the generalized distributive law where $*$ is a principal isotope of $\circledast$. P-isotopes of ξ lead to equivalent quintuples. ∎

Note that the generalized distributive law is not a matroid quasigroup equation of P_7 but it follows from the two matroid quasigroup equations $\mathit{7}(\mathit{1}, \mathit{2}, \mathit{3}) = \mathit{7}(\mathit{1}, \mathit{4}(\mathit{2}, \mathit{3}))$ and $\mathit{7}(\mathit{1}, \mathit{2}, \mathit{3}) = \mathit{7}(\mathit{5}(\mathit{1}, \mathit{2}), \mathit{6}(\mathit{1}, \mathit{3}))$.

Example 3.6. P-representations of P_7 (solutions of the distributive law) can be constructed from diagonal Moufang loops $(Q, \cdot)$, cf. [6], pp. 99–102; for background on these loops see [11], [12], [14] and [16]. Let us recall that Moufang loops are defined by the identity $(xy)(zx) = [x(yz)]x$ and that the diagonalness means the mapping $x \mapsto x^2$ is a permutation of Q; these loops are diassociative and $(x, y) \mapsto xyx$ is a quasigroup operation. If we set $x \star y = xyx$, $x \diamond z = zx$, and $\circ = \square = * = \cdot$ the quintuple $(\star, \circ, \square, *, \diamond)$ solves the generalized distributive identity and, at the same time, gives rise to a p-representation of P_7 depicted in Fig. 6 left.

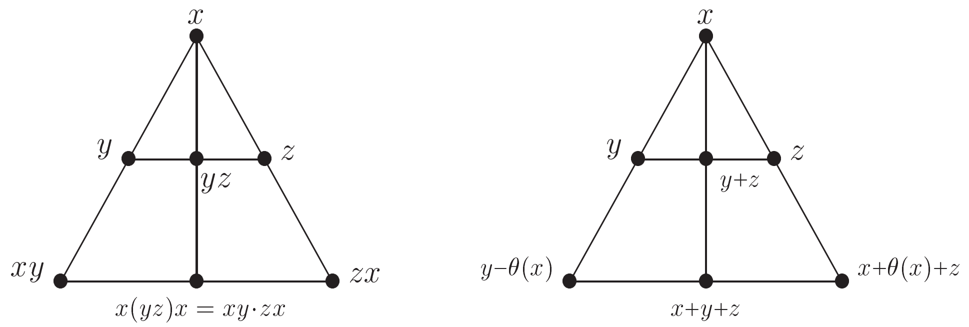


Figure 6. Examples of p-representations of P_7.

Another kind of p-representations of P_7 is related to finite Abelian groups $(G,+)$ admitting a complete mapping, i.e. a permutation θ of G such that the mapping $x \mapsto x+\theta(x)$ is a permutation, too. (A necessary and sufficient condition for an Abelian group to have a complete mapping is that the number of its elements of order two is not equal to one, see [14], p. 34.) These p-representations are outlined in Fig. 6 right; the corresponding quintuple is given by $\star = \circ = * = +$, $x \,\square\, y = y - \theta(x)$ and $x \diamond z = x + \theta(x) + z$. $\square$

4. Non-p-representable matroids. Understanding the structure of p-representations of the matroid $M(K_4)$, we can say something more about matroids containing this graphical matroid as subconfigurations. Some classical nonlinear matroids will be shown here not to be p-representable as well.

Proposition 4.1. *The two matroids of rank three from Fig. 7 are not p-representable.*

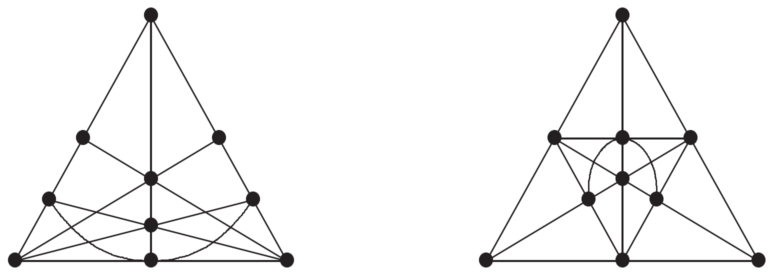


Figure 7. Two examples of non-p-representable matroids.

Proof. Both matroids of Fig. 7 contain as restrictions (submatroids) the Fano and non-Fano matroids. We shall classify the p-isotopy classes of the latter matroids here. All p-representations of the Fano matroid will be found to have their degrees equal to powers of two and all p-representations of the non-Fano matroid to have only odd degrees. The matroids of Fig. 7 must be then non-p-representable.

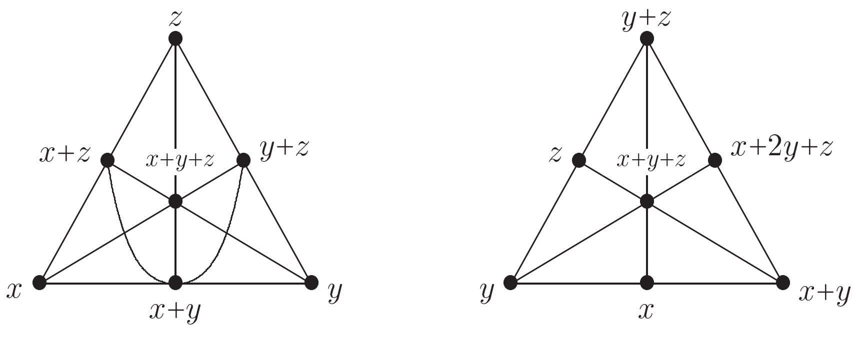


Figure 8. P-representations of Fano and non-Fano matroids.

Points of the Fano and non-Fano matroids will be labeled as in Fig. 1 left and the center point gets the label 7. Let ξ be a p-representation of the Fano matroid in the coordinate form w.r.t $\{1,2,3\}$ and let $(G,\cdot)$ be a finite group defining the six partitions of ξ according to Fig. 1 right. The seventh partition of ξ will be treated by an equivalence $\equiv$ on G^3. Where 1 is the unit element of $(G,\cdot)$, $(1,1,1) \equiv (a,a,1)$ because the blocks of ξ_7 are unions of blocks of $\xi_{\{3,4\}}$ and analogously $(a,a,1) \equiv (a,ab,b) \equiv (ac,ab,bc)$ thinking about $\xi_{\{1,5\}}$ and $\xi_{\{2,6\}}$. Hence $\{(c,b,bc);\ b,c \in G\} = \{(ac,a,c);\ a,c \in G\}$ is a block of ξ_7 and we read out the idempotence $a^2 = 1$, $a \in G$, of the group operation. Then the group must be a power of the cyclic group $\mathbb{Z}_2$ of order two and ξ_7 is the level partition of ternary quasigroup $(x, y, z) \mapsto x+y+z$. Any system of seven partitions defined by Fig. 8 left with the addition in $\mathbb{Z}_2^m$, $m \geqslant 1$, is obviously a p-representation of the Fano matroid.

Let ξ be a p-representation of the non-Fano matroid and six of its partitions be defined as in the middle of Fig. 2 via a group $(G, \cdot)$. The argumentation is similar to the Fano case;

$$(1,1,1) \equiv (a^{-1}b^{-1}, 1, ba) \equiv (a^{-1}b^{-2}, b, a) \;\text{ and }\; (1,1,1) \equiv (b^{-1}, b, b^{-1}) \equiv (b^{-1}a^{-1}b^{-1}, b, a)$$

where $\equiv$ is the partition corresponding to ξ_5. Hence, the group must be Abelian. If it had even order d then the set $\{(-a-2b, b, a);\ a, b \in G\}$ would have cardinality smaller than d^2 and could not be a block of the latin partition ξ_5. With an odd order d, Fig. 8 right works. ∎

The matroids which are not linearly representable have been frequently obtained by relaxing a circuit-hyperplane of a configuration in projective geometry, see for example [30], [25], [10], [38].

Proposition 4.2. *The two non-Desargues matroids (on ten element sets) of the ranks three and four are both non-p-representable.*

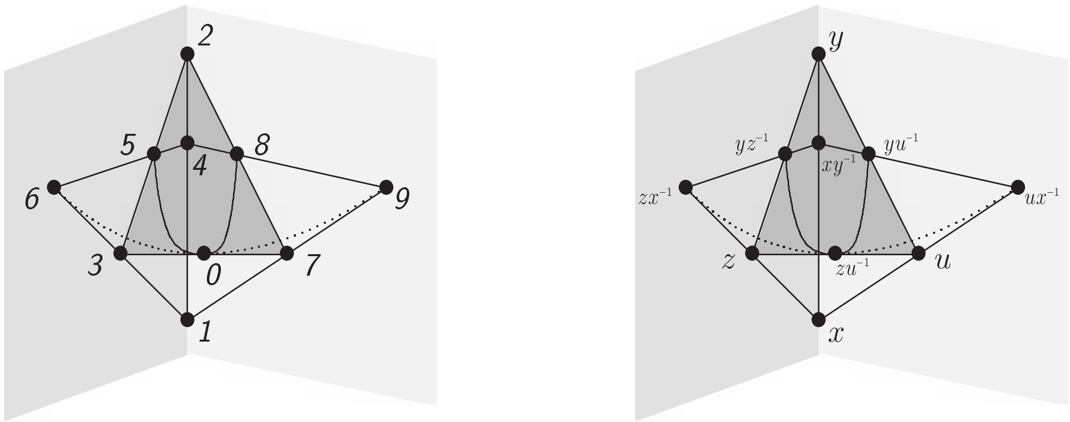


Figure 9. Non-Desargues matroids are non-p-representable.

Proof. Let ξ be a p-representation of the non-Desargues matroid of rank four, see Fig. 9 left. It is supposed to be in the coordinate form w.r.t. the base $I = \{1, 2, 3, 7\}$. Permuting y- and z-layers, the left-sheet-partitions $\xi_1, \ldots, \xi_6$ can be brought to the form of Fig. 9 right, cf. Fig. 1 right and Proposition 3.1. Here, any finite group $(G, \cdot)$, $|G| \geqslant 2$, is in the background. Permuting u-layers one can obtain similarly ξ_8 and ξ_9 as in Fig. 9 right. Finally, ξ_0 is specified by the expression zu^{-1} being present in the subconfiguration on $\{2, 3, 7, 5, 0, 8\}$. But then $\xi_{\{0,6,9\}}$ has only d^2 blocks, a contradiction.

In the case of the non-Desargues matroid of rank three, the partitions $\xi_1, \ldots, \xi_6$ will be fixed as above. The partition ξ_7 is assumed to be given by a quasigroup $\pi_7 \colon G^3 \to G$. Then the p-isotope $f\xi$ is considered where $f(x, y, z) = (x, y, \pi_7(x, y, z))$. By choice of the (principal isotope of the) quasigoup, ξ_8 and ξ_9 can be specified as $\pi_7(x, y, z)y^{-1}$ and $\pi_7(x, y, z)x^{-1}$, respectively. Then, by use of Proposition 3.1., ξ_0 is found from the p-isotope $g\xi$ where $g(x, y, z) = (\pi_7(x, y, z), y, z)$. The contradiction is now again that $\xi_{\{0,6,9\}}$ behaves as if $\{0, 6, 9\}$ were collinear. ∎

Further we examine a sequence of matroids L_n, $n \geqslant 2$, that have rank three and the ground set of cardinality $2n+3$. These matroids, see Fig. 10 left, were examined in [10] p. 108, [26], [18]. Note that L_2 is the Fano matroid and L_3 is the Reid geometry, see [38], p. 516.

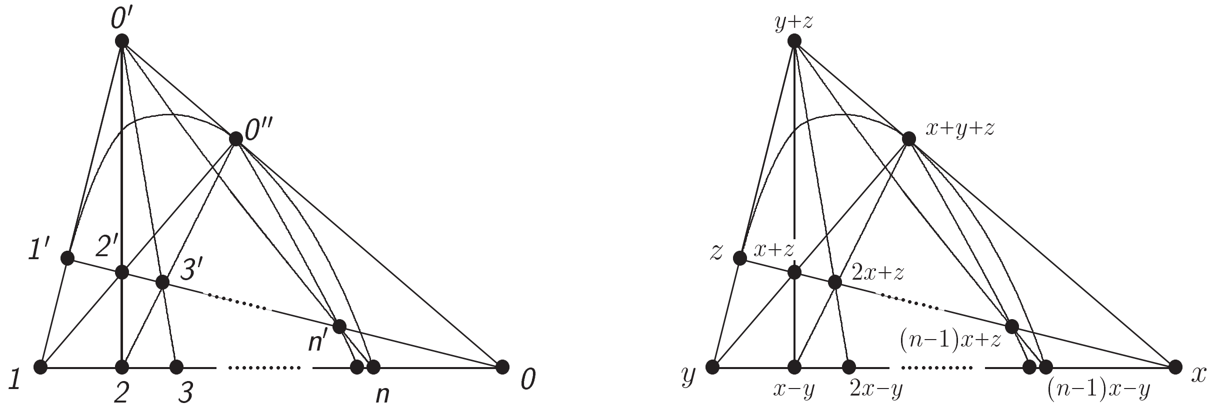


Figure 10. P-representations of L_n, n prime.

Proposition 4.3. *The matroid L_n is p-representable if and only if n is prime. In this case every p-representation of L_n is p-isotopic to the one given in Fig. 10 right where the addition is in the group $\mathbb{Z}_n^m$, $m \geqslant 1$.*

Proof. For $n = 2$ the assertion was settled in the previous proof. Let $n \geqslant 3$ and ξ be a p-representation of L_n. Then the submatroid on $\{0, 1, 2, 0', 1', 2', 0''\}$ is the non-Fano matroid and the corresponding partitions of ξ can be taken as in the p-isotope of Fig. 8 right given by $f(x, y, z) = (x + y, y, z)$; formally, it is a substitution $x \to x - y$. They live in the cube of an Abelian group $(G, +)$ of odd order. Then $\xi_{3'}$ is given by $2x + z$ using a similar equivalence method as in the foregoing proof (blocks of $\xi_{3'}$ are composed of blocks of $\xi_{\{0,1'\}}$ and of blocks of $\xi_{\{0'',2\}}$). The same argumentation specifies ξ_3 as $2x - y$. By induction, the label of i' is $(i - 1)x + z$ and the label of i is $(i - 1)x - y$, $1 \leqslant i \leqslant n$. But the points $1'$, $0''$ and n are colinear due to the twisted line. That entails $nx = 0$ for all $x \in G$. Since the labels of $\{2, 3, \dots, n\}$ must define orthogonal binary quasigroups on G, the numbers $2, 3, \dots, n-1$ cannot divide the order of G. Hence, n is a prime number and the group must be $\mathbb{Z}_n^m$, for some $m \geqslant 1$. On the other hand it is not difficult to verify that labels in Fig. 10 right, with the addition in $\mathbb{Z}_n^m$, $m \geqslant 1$, do define a p-representation of L_n for prime n and that every p-representation of L_n is a p-isotope of some p-representation of this kind. ∎

5. Discussion. We now overview some topics related to the presented results. First, entropy functions and probabilistic representations of matroids and semimatroids are mentioned to outline notions paving our way to the partition representability. Then, ideal secret-sharing schemes are related to the p-representations. Matroid duality is considered and comparisions with the linear, multilinear and algebraic representations are made. Finally, forbidden minors for p-representability, p-characteristic sets of matroids and a related notion of irreducibility seem to be worth mentioning.

5.1. Entropy functions. Let us suppose that $\xi = (\xi_i)_{i \in N}$ is a system of partitions of a finite set Ω and p is a nonnegative function on Ω summing to one. Equivalently, we will say that ξ is a system of random variables. Then ξ_I, $I \subseteq N$, can be considered for a set algebra of of the probability space (Ω, p) and it has the Shannon entropy

$h_\xi(I) = -\sum_{A\in\xi_I} p(A)\ln p(A)$ where $p(A) = \sum_{\omega\in A} p(\omega)$ is the probability of the block A from ξ_I. The set function h_ξ defined in this way is called the *entropy function* of ξ and the couple (N, h_ξ) is known to be a polymatroid, cf. [17], [42], [37] and [35]; for recent progress on the very difficult problem which polymatroid can be obtained in this way see [45], [46] and [47].

If ξ is a partition representation of a matroid (N, r) living on Ω and $p(\omega) = |\Omega|^{-1}$, $\omega \in \Omega$, then clearly $h_\xi = r \cdot \ln d$ where d is the degree of ξ. In [32], [33] we defined a matroid (N, r) to be *strongly probabilistically representable* if for a system ξ of random variables on (Ω, p) the entropy function of ξ is proportional to the rank function r, in symbols if $h_\xi = c \cdot r$ for a positive number c. Every strong probabilistic representation ξ (over some (Ω, p)) of a connected matroid with rank at least two was proved, [33], to have associated a unique integer number $d \geqslant 2$ such that $p(A) = d^{-r(I)}$, $A \in \xi_I$, $I \subseteq N$. This means in fact that a matroid is partition representable if and only if it is strongly probabilistically representable and that there are only trivial differences between partition representations and probabilistic representations.

5.2. Semimatroids and their representations. Let (N, g) be a polymatroid and $[\![g]\!]$ be the family of those triples $(i, j|K)$, $K \subseteq N$, $i, j \in N - K$, which satisfy

$$g(i \cup K) + g(j \cup K) = g(K) + g(i \cup j \cup K)\,.$$

We coin, starting from [33], the name *semimatroid* for such a family $[\![g]\!]$. A semimatroid is *probabilistically representable* if for a system of random variables ξ on (Ω, p) a triple $(i, j|K)$ belongs to it if and only if ξ_i is stochastically conditionally independent of ξ_j given ξ_K. A necessary and sufficient condition for this is the equality $h_\xi(i \cup K) + h_\xi(j \cup K) = h_\xi(K) + h_\xi(i \cup j \cup K)$; note that if $i = j$ this means a functional dependence. Thus, a semimatroid $[\![g]\!]$ is probabilistically representable if and only if $[\![g]\!] = [\![h_\xi]\!]$ for some ξ. Semimatroids provide a natural environment for studying conditional independences among partitions (set algebras, random variables) simultaneously. In [37], [34] and [36] all probabilistically representable semimatroids on a four-element set N were found and in [35] various classes of semimatroids and their minors were examined.

A matroid (N, r) is *weakly probabilistically representable* if the semimatroid $[\![r]\!]$ is probabilistically representable, i.e. if for a system of random variables on some (Ω, p) the equality $h_\xi(i\cup K)+h_\xi(j\cup K) = h_\xi(K)+h_\xi(i\cup j\cup K)$ is equivalent to $r(i\cup K)+r(j\cup K) = r(K)+r(i\cup j\cup K)$ whatever $K \subseteq N$ and $i, j \in N - K$. Note that by a theorem of Nguyen (see his chapter in [43]) weak probabilistic representability is equivalent to the strong one on connected matroids. However, *the direct sum of the Fano and non-Fano matroids is weakly and not strongly probabilistically representable*; this is the first example of this kind we know. In fact, let ξ be a partition representation of the Fano matroid on $N = \{\mathit{1}, \ldots, \mathit{7}\}$ and let η be a partition representation of the non-Fano matroid on $N' = \{\mathit{1}', \ldots, \mathit{7}'\}$; let ξ live on $\mathbb{Z}_2^3$ and η on $\mathbb{Z}_3^3$. Then the partitions $\{A \times \mathbb{Z}_3^3;\ A \in \xi_i\}$, $i \in N$, and $\{\mathbb{Z}_2^3 \times B;\ B \in \eta_j\}$, $j \in N'$, of $\Omega = \mathbb{Z}_2^3 \times \mathbb{Z}_2^3$ with $p(\omega) = 2^{-3}3^{-3}$, $\omega \in \Omega$, provide a weak probabilistic representation of the direct sum. At the same time, the direct sum is not partition representable, see the proof of Propositon 4.1., and thus not strongly probabilistically representable.

5.3. Ideal secret-sharing schemes. Let N be a finite set (of participants), $\mathit{0} \in N$ be a distinguished element of N (dealer), and $\mathcal{A}$ a nonempty family (access structure) of subsets of $N - \mathit{0}$ no two of them being in a set inclusion. Let us suppose that every $i \in N - \mathit{0}$ is contained in some $J \in \mathcal{A}$ (no bystanders). A system of random variables $\xi = (\xi_i)_{i\in N}$ is called (probabilistic) *secret-sharing scheme* for $\mathcal{A}$ if $h_\xi(0 \cup I) = h_\xi(I)$ for every $I \subseteq N - 0$ containing some $J \in \mathcal{A}$. A secret-sharing scheme is *perfect* if $h_\xi(0 \cup I) = h_\xi(0) + h_\xi(I)$ for every $I \subseteq N - 0$ containing no $J \in \mathcal{A}$; in such a scheme if $i \in N - 0$ then $i \in J$ for some $J \in \mathcal{A}$ and

$$h_\xi(i) \geqslant h_\xi(J) - h_\xi(J - i) = h_\xi(0 \cup J) - h_\xi(J - i) \geqslant h_\xi((0 \cup J) - i) - h_\xi(J - i) = h_\xi(0)\,.$$

A perfect secret-sharing scheme is *ideal* if $h_\xi(i) = h_\xi(0) > 0$ for all $i \in N - 0$. For interpretations and further references see [8], [21] and [13].

If ξ is an ideal secret-sharing scheme for some $\mathcal{A}$ then there exists a unique connected matroid (N, r) such that

$$\mathcal{A} = \{J \subseteq N - 0;\ 0 \cup J \text{ is a circuit of } (N, r)\}$$

and $h_\xi = c \cdot r$ for a positive number c, see [8], [7] and [22] for an overview of related results. Thus an ideal secret-sharing scheme is one of the strong probabilistic representations of a connected matroid and, omitting trivial situations, it is a partition representation of a connected matroid. In the reverse direction, all strong probabilistic representations give rise in a straightforward manner to ideal secret-sharing schemes.

5.4. Duality. It is a natural question how partition (p-) representations of matroids behave when going to the matroid duals. Especially intriguing seems to be the problem, formulated in [32], whether the dual of a p-representable matroid is p-representable. We have two remarks to the point. First, there is a natural extension of the matroid duality to the class of semimatroids containing only the triples $(i, j|K)$ with $i \neq j$, see [33]. In [34] an example of a probabilistically representable semimatroid having the probabilistically nonrepresentable dual was found. Second, the p-representations of a matroid can have different structure than the p-representations of its dual and this will be in a moment visible on the graphical matroid $M(K_{3,3})$. To this end p-representations of the matroid $M(K_n)$, $n \geqslant 2$, will be constructed starting from an arbitrary finite group $(G, \cdot)$ of order $d \geqslant 2$ as follows. If K_n has vertices $\{1, 2, \dots, n\}$ and edges $i = uv$, $1 \leqslant u < v \leqslant n$, then we let $\xi^{(G,\cdot)}$ live on G^{n-1} and consist of the partitions $\xi_i^{(G,\cdot)}$ having the blocks

$$\{(x_1, \dots, x_{n-1}) \in G^{n-1};\ x_u \cdot \ldots \cdot x_{v-1} = a\}, \quad a \in G\,.$$

For $n = 4$ see again Fig. 2 middle. It is obvious that $\xi^{(G,\cdot)}$ is indeed a p-representation of $M(K_n)$. But, $M(K_{3,3})$ is a restriction of $M(K_6)$ and when we take the p-representation $\xi^{(G,\cdot)}$ of the latter and omit the partitions corresponding to the nonedges of $K_{3,3}$ we obtain a p-representation of $M(K_{3,3})$. It is not difficult to recognize that two such p-representations of $M(K_{3,3})$ are p-isotopic if and only if the underlying groups are isomorphic. A conclusion can be drawn that some p-isotopy classes of p-representations of $M(K_{3,3})$ match with the isomorphism classes of finite groups whereas the p-representations of the dual $M^*(K_{3,3})$ are governed 'only' by finite Abelian groups owing to Proposition 3.3.

For duality in perfect secret-sharing schemes see [21] and for duality in almost affine codes [40].

5.5. Comparing matroid representations. Linearly (l-) representable matroids are p-representable, see e.g. [32]. The reasoning is quite short. If a matroid (N, r) is l-representable over a field then it is l-representable also over a finite field of sufficiently high cardinality d, cf. [38], p. 225. That means there are linear functionals x_i, $i \in N$, on a linear space E of the dimension $r(N)$ over the finite field such that $r(I)$ is the rank of the hull of $(x_i)_{i\in I}$, $I \subseteq N$. Blocks of a partition ξ_i of $\Omega = E$ are then taken as the shifts of the null-space of the functional x_i, $i \in N$, and it is almost straightforward that the system of partitions $\xi = (\xi_i)_{i\in N}$ is a p-representation of the matroid (N, r) of degree d. The idea is close to the notion of arrangement from [48], p. 526, and from this point of view the p-representations are generalizations of the arrangements beyond the linear structure.

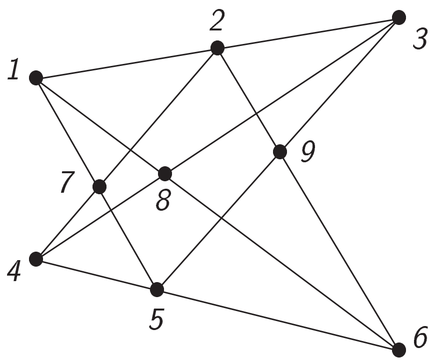
The non-Pappus matroid, see Fig. 11 left or [38] p. 43, which is known not to be l-representable over a field, was found in [40] to be p-representable of degree 9; a verification was done by two independent computer programs. We prove in a moment that Fig. 11 right defines its p-representation ξ in the coordinate form w.r.t. the basis $I = \{1, 3, 5\}$. It lives on Q^I where $Q = \mathbb{Z}_3^n \times \mathbb{Z}_3^n$, $n \geqslant 1$ (the case $n = 1$ comes from [40]), and, for example, the label at the point 4 specifies the ternary quasigroup

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} w \\ z \end{bmatrix}, \begin{bmatrix} u \\ v \end{bmatrix}\right) \mapsto \begin{bmatrix} x+u+2z \\ y+2v+w+z \end{bmatrix}.$$

Equivalently, one can think about the coordinate partitions of this set $\Omega \subseteq Q^N$

$$\left\{ \left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} x+w \\ y+z \end{bmatrix}, \begin{bmatrix} w \\ z \end{bmatrix}, \begin{bmatrix} x+u+2z \\ y+2v+w+z \end{bmatrix}, \begin{bmatrix} u \\ v \end{bmatrix}, \begin{bmatrix} x+2u+2v+2z \\ y+u+w+z \end{bmatrix}, \begin{bmatrix} x+v \\ y+u+2v \end{bmatrix}, \begin{bmatrix} x+u+w+z \\ y+2v+w \end{bmatrix}, \begin{bmatrix} u+w \\ v+z \end{bmatrix}\right);\ \begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} w \\ z \end{bmatrix}, \begin{bmatrix} u \\ v \end{bmatrix} \in Q \right\}.$$

To see that ξ is a p-representation Lemma 1.8. is evoked. The non-Pappus matroid is paving and its eight circuits of the cardinality 3 (the lines in the figure) are packed into a family $\mathcal{C}'$. For $I = \{1, 3, 5\}$ the family $\mathcal{D}$ contains five circuits and $\mathcal{D}'$ contains $\mathcal{C}'$ and $\{\{1, 3, 4, 5\}, \{1, 3, 5, 6\}, \{1, 3, 5, 8\}\}$. We claim that every base of the matroid is $\mathcal{D}'$-linked to I or to some base of $\mathcal{B}' = \{\{1, 4, 9\}, \{2, 5, 8\}, \{3, 6, 7\}, \{7, 8, 9\}\}$. In fact, if J is a base, $|J \cap \{7, 8, 9\}| = 2$, then it is easy to see by symmetry that J is $\mathcal{C}'$-linked to a base K, $K \cap \{7, 8, 9\} = \emptyset$, and K is $\mathcal{C}'$-linked to I or $\{2, 4, 6\}$. But these two bases are $\mathcal{D}'$-linked (consider the sequence *135*, *358*, *345*, *135*, *459*, *469*, *246*). If J is a base, $|J \cap \{7, 8, 9\}| = 1$, and $J \notin \mathcal{B}'$ then it is $\mathcal{C}'$-linked to a base K, $K \cap \{7, 8, 9\} = \emptyset$, and thus $\mathcal{D}'$-linked to I. Further, one has to verify that for $i \in N - I$ the labels of Fig. 11 right do define $\gamma(i, I)$-quasigroups which is trivial if $i \in \{2, 7, 9\}$ and needs a few visual checkings for $i \in \{4, 6, 8\}$. This goes through even for Abelian groups of odd order on the place of $\mathbb{Z}_3^n$. It remains to prove, cf. Lemma 1.8., that $\pi_C(\Omega)$ is a C-quasigroup for $C \in \mathcal{D}$ and $\pi_J(\Omega) = Q^J$ for $J \in \mathcal{B}'$. The second task can be done visually but the first one needs a sheet of paper and easy computations (the structure of $\mathbb{Z}_3^n$ has to be used e.g. for $C = \{2, 4, 7\}$).



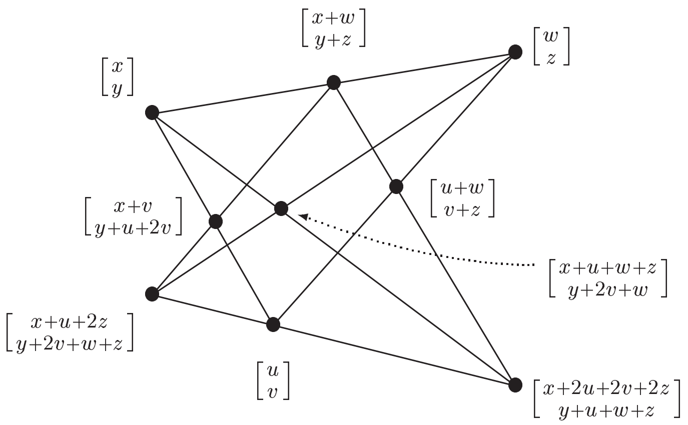


Figure 11. P-representations of the non-Pappus matroid.

A matroid (N, r) is *multilinearly (ml-) representable* if at least one of the polymatroids (N, nr), $n \geqslant 1$, has an l-representable expansion; equivalently, if for some $n \geqslant 1$ there exist subspaces D_i, $i \in N$, of a linear space E over a field such that the rank of the hull of D_i, $i \in I$, is $nr(I)$, for every $I \subseteq N$. If the subspaces have ranks at most 1 we have an l-representation. Obviously, ml-representable matroids are p-representable. Since the non-Pappus matroid is ml-representable, as shown above, the problem whether there exists a p-representable non-ml-representable matroid, formulated in [40], remains open. To solve it it would suffice to find a p-representable matroid such that its rank function does not satisfy the Ingleton inequality, see [19], [38] p. 177. This inequality is a necessary condition for a matroid to be ml-representable but entropy functions do exist violating it, see the examples in [34], [36], [13] and [47].

For representations of matroids in free modules over commutative rings and their relation to ideal homomorphic secret-sharing schemes (what are, in fact, special p-representations) see [29]. A trial to relate matroid representations in (right near-) vector spaces over (right) nearfields and ideal secret-sharing schemes presented in [8] was found to be erroneous in [40].

An algebraically (a-) representable matroid need not be p-representable. As an example one can take the matroid of Example 15 from [20] (see also [38], Fig. 6.29 on p. 220); this matroid on a set of eleven elements is a-representable but not p-representable because of the presence of the Fano and non-Fano subconfigurations, cf. the proof of Proposition 4.1. A natural question is whether a p-representable and non-a-representable matroid exists.

5.6. Remarks. Any minor of a matroid having a p-representation of some degree d is p-representable of the same degree d, [33] and [40]. It is then not difficult to establish that a matroid is p-representable of degree two and three if and only if it is binary and ternary, respectively, see [33] and [5]. Even more, all its p-representations are p-isotopic to l-representations, [40]. Since the matroids L_n, $n \geqslant 2$ nonprime, from Fig. 10 are non-p-representable and all their proper minors are l-representable, see [26], [10], they are forbidden minors for the p-representability. Hence, *the class of p-representable matroids has an infinite number of forbidden minors.*

In [39] the Vamos cube, a matroid of rank four on an eight-element set, was found not to be secret-sharing (i.e. non-p-representable) by ingenious graph-theoretical methods. A short proof of the probabilistic non-representability of the Vamos cube was done in [33]. Also all properties of probabilistically representable semimatroids over a four-element set presented in [34] and [36] imply the fact. Yet another short proof of a projective geometry flavour of the almost affine non-representability of the Vamos cube is in [40], p. 195.

The *p-characteristic set* of a matroid is the set of all integers $d \geqslant 2$ such that the matroid has a p-representation of degree d, cf. [20], [23], [18], [38]. A natural question is which subsets of $\{2, 3, 4, \dots\}$ are the p-characteristic sets of matroids. We want to remark that the p-characteristic sets are multiplication closed. In fact, if ξ and η are two p-representations of a matroid (N, r) having the degrees d_ξ and d_η and living on Ω_ξ and Ω_η, respectively, then their *product* $\xi \otimes \eta = (\zeta_i)_{i \in N}$ will consist of the partitions ζ_i of $\Omega_\xi \times \Omega_\eta$ having the blocks $A \times B$ for $A \in \xi_i$ and $B \in \eta_i$. The product $\xi \otimes \eta$ is obviously a p-representation of the matroid of degree $d_\xi \cdot d_\eta$.

Classifying the p-representations of a matroid, the most interesting are irreducible p-representations, i.e. those that are not p-isotopic to the product of two p-representations of the matroid. For example, the Fano matroid (and similarly any matroid L_n, $n \geqslant 2$

prime) has, up to p-isotopy of course, only one irreducible p-representation ξ. Namely, the one of Fig. 8 left over the group $\mathbb{Z}_2$. All the remaining p-representations are simply $\xi \otimes \xi$, $\xi \otimes \xi \otimes \xi, \ldots$. Another example of an irreducible p-representation of $U_{2,4}$ can be obtained from two orthogonal quasigroups of order ten as in Example 2.2. It is a natural question which p-representable matroids have only one irreducible p-representation.

References

[1] J. Aczél (1966) *Lectures on Functional Equations and their Applications.* Academic Press, New York, London.

[2] J. Aczél (1984) *Functional Equations: History, Applications and Theory.* D. Reidel Publ. Company, Dordrecht, Boston, Lancaster.

[3] J. Aczél, V.D. Belousov and M. Hosszú (1960) Generalized associativity and bisymmetry on quasigroups. *Acta Mathematica, Academiae Scientiarum Hungaricae* **11** 127–136.

[4] M. Aigner (1979) *Combinatorial Theory.* Springer-Verlag, Berlin, Heidelberg, New York.

[5] A. Beimel and B. Chor (1994) Universally ideal secret-sharing schemes. *IEEE Trans. Information Theory* **40** 786–794.

[6] V.D. Belousov (1965) Systems of quasigroups with generalized identities. *Russian Math. Surveys* **20** 73–143.

[7] G.R. Blakley and G.A. Kabatianski (1997) Generalized ideal secret-sharing schemes and matroids. *Problems of Information Transmission* **33** 277–284.

[8] E.F. Brickell and D.M. Davenport (1991) On the classification of ideal secret-sharing schemes. *J. Cryptology* **4** 123–134.

[9] T. Brylawski (1979) Intersection theory for embeddings of matroids into uniform geometries. *Studies in Applied Math.* **61** 211–244.

[10] T. Brylawski and D. Kelly (1980) *Matroids and Combinatorial Geometries.* Carolina Lecture Series, Department of Mathematics, Univ. of North Carolina at Chapel Hill.

[11] R.H. Bruck (1966) *A Survey of Binary Systems.* Springer-Verlag, Berlin, Heidelberg, New York.

[12] O. Chein (1978) Moufang loops of small order. *Memoirs Amer. Math. Soc.* **13**(1) No. 197.

[13] L. Csirmaz (1996) The dealer's random bits in perfect secret-sharing schemes. *Studia Scient. Math. Hungarica* **32** 429–437.

[14] J. Dénes and A.D. Keedwell (1974) *Latin Squares and their Applications.* Akadémiai Kiadó, Budapest; Academic Press, New York; English Universities Press, London.

[15] J. Dénes and A.D. Keedwell (1991) *Latin Squares: New Developments in the Theory and Applications.* North Holland, Amsterdam, New York, Oxford, Tokyo.

[16] L. Fook and T.P. Eng (1994) Moufang loops of even order. *J. of Algebra* **164** 409–414.

[17] S. Fujishige (1978) Polymatroidal dependence structure of a set of random variables. *Information and Control* **39** 55–72.

[18] G. Gordon (1988) Algebraic characteristic sets of matroids. *J. Comb. Theory B* **44** 64–74.

[19] A.W. Ingleton (1971) Conditions for representability and transversality of matroids. *Proc. Fr. Br. Conf.* (1970), Springer Lecture Notes **211** 62–67.

[20] A.W. Ingleton (1971) Representation of matroids. In: *Combinatorial Mathematics and its Applications* (ed. D.J.A. Welsh) Academic Press, London, New York, 149–169.

[21] W.-A. Jackson and K.M. Martin (1994) Geometric secret-sharing schemes and their duals. *Designs, Codes and Cryptography* **4** 83–95.

[22] W.-A. Jackson and K.M. Martin (1998) Combinatorial models for perfect secret-sharing schemes. *J. Comb. Math. Comb. Comput.* **28** 249–265.

[23] J. Kahn (1982) Characteristic sets of matroids. *J. London Math. Soc.* (2) **26** 207–217.

[24] A. Krapež and M.A. Taylor (1993) Irreducible Belousov equations on quasigroups. *Czechoslovak Math. J.* **43(118)** 157–175.

[25] J.P.S. Kung (1986) *A Source Book in Matroid Theory.* Birkhäuser, Boston, Basel, Stuttgart.

[26] B. Lindström (1987) A class of non-algebraic matroids of rank three. *Geometriae Dedicata* **32** 255–258.

[27] B. Lindström (1988) Matroids, algebraic and non-algebraic. In: *Algebraic, Extremal and Metric Combinatorics.* (eds. M-M. Deza, P. Frankl and I.G. Rosenberg) Cambridge University Press, Cambridge, New York.

[28] B. Lindström (1993) On algebraic matroids. *Discrete Math.* **111** 357–359.

[29] M. Liu and Z. Zhou (1998) Ideal homomorphic secret-sharing schemes over cyclic groups. *Science in China, Ser. E* (Science in China Press) **41** 650–660.

[30] S. MacLane (1936) Some interpretations of abstract linear dependence in term of projective geometry. *Amer. J. of Math.* **58** 236–240.

[31] F.J. MacWilliams and N.J.A. Sloane (1983) *The Theory of Error-Correcting Codes.* North Holland, Amsterdam, London, New York, Tokyo.

[32] F. Matúš (1992) Ascending and descending conditional independence relations. *Transactions of the 11-th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes*, Vol. B, 189–200, Academia, Prague (also Kluwer, Dordrecht).

[33] F. Matúš (1994) Probabilistic conditional independence structures and matroid theory: background. *Int. J. of General Systems* **22** 185–196.

[34] F. Matúš (1995) Conditional independences among four random variables II. *Comb., Probab. and Comput.* **4** 407–417.

[35] F. Matúš (1997) Conditional independence structures examined via minors. *The Annals of Math. and AI* **21** 99–128.

[36] F. Matúš (1999) Conditional independences among four random variables III. *Comb., Probab. and Comput.* **8** (to appear in No. 3)

[37] F. Matúš and M. Studený (1995) Conditional independences among four random variables I. *Comb., Probab. and Comput.* **4** 269–278.

[38] J.G. Oxley (1992) *Matroid Theory.* Oxford University Press, Oxford, New York, Tokyo.

[39] P.D. Seymour (1992) On secret-sharing matroids. *J. Comb. Theory B* **56** 69–73.

[40] J. Simonis and A. Ashikhmin (1998) Almost affine codes. *Designs, Codes and Cryptography* **14** 179–197.

[41] M.A. Taylor (1978) A generalization of a theorem of Belousov. *Bull. London Math. Soc.* **10** 285–286.

[42] D.J.A. Welsh (1976) *Matroid Theory.* Academic Press, London.

[43] N. White (1986), ed. *Theory of Matroids.* Cambridge University Press, Cambridge.

[44] N. White (1987), ed. *Combinatorial Geometries.* Cambridge University Press, Cambridge.

[45] R.W. Yeung (1996) A framework for information-theoretic inequalities. *IEEE Trans. Information Theory* **43** 1924–1934.

[46] Z. Zhang and R.W. Yeung (1997) A non-Shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory* **43** 1982–1986.

[47] Z. Zhang and R.W. Yeung (1998) On characterization of entropy function via information inequalities. *IEEE Trans. Information Theory* **44** 1440–1452.

[48] G.M. Ziegler (1990) Matroid representations and free arrangements. *Trans. Amer. Math. Soc.* **320** 325–341.