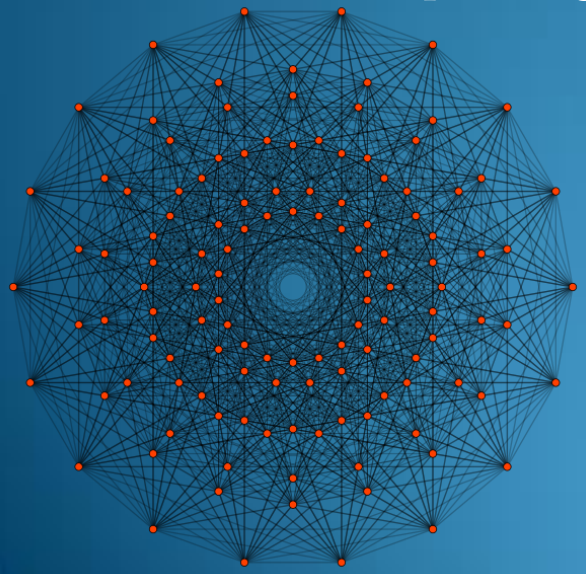
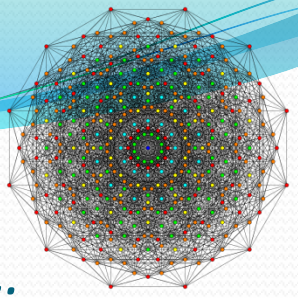
Partition representable matroids - Analysis of paper: Matroid representations by Partitions by Frantisek Matus

Presented by: Alexander Erick Trofimoff
PhD Student, Graduate Research Assistant
Adaptive Signal Processing and Information Theory Research Group
Drexel University
Summer 2013
Philadelphia, Pennsylvania





Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

General Objective of the Paper:

The aim of this work is to examine partition (p-) representations of matroids along the traditional lines of linear and algebraic representation theories.

Principal Results:

p-representations of a matroid are closely related to the solutions of a system of generalized quasigroup equations associated to the matroid.

Classify completely the p-representations of a few small matroids and relate them to some classical generalized quasigroup equations.

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.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Representable Matroids:

Let $\mathbb{K}$ be a field. A matroid $\mathcal{M}=(\mathcal{Q},\mathcal{I})$ is $\mathbb{K}$-representable (or representable for short) if there exists a matrix M over $\mathbb{K}$ whose columns are indexed by the elements of $\mathcal{Q}$ such that a subset $I=\{i_1,\ldots,i_k\}\subseteq\mathcal{Q}$ is independent if and only if the matrix corresponding columns of M are independent. In this situation, we say that the M is a $\mathbb{K}$-representation of the matroid $\mathcal{M}$

Linear Matroid:

if $(E,\mathcal{I})$ is any matroid, then a representation of $(E,\mathcal{I})$ may be defined as a function f that maps E to a vector space V, with the property that a subset A of E is independent if and only if $f(A)$ is linearly independent.

if V is a vector space over field *F* then the matroid is called an *F*-linear matroid.

Thus, the linear matroids are exactly the matroids that are isomorphic to the matroids defined from sets or multisets of vectors.

If a matroid is linear, it may be representable over some but not all fields.

Regular Matroids: The unimodular or regular matroids are the matroids that can be represented over all fields;

If a matroid is regular, so is its dual matroid, and so is every one of its minors.· · Every direct sum of regular matroids remains regular.

Every graphic matroid (and every co-graphic matroid) is regular. Conversely, every regular matroid may be constructed by combining graphic matroids, co-graphic matroids, and a certain ten-element matroid that is neither graphic nor co-graphic, using an operation for combining matroids that generalizes the clique-sum operation on graphs.

Uniform Matroids: A uniform matroid U_n^r has n elements, and its independent sets consist of all subsets of up to r of the elements.

Uniform matroids may be represented by sets of vectors in general position in an r-dimensional vector space. The field of representation must be large enough for there to exist n vectors in general position in this vector space, so uniform matroids are *F*-linear for all but finitely many fields *F*.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Partition Matroids:

Let B_i be a collection of disjoint sets, and let d_i be integers with $0 \leq d_i \leq |B_i|$. Define a set I to be "independent" when, for every index i, $|I \cap B_i| \leq d_i$. Then the sets that are independent sets in this way form the independent sets of a matroid, called a partition matroid. The sets B_i are called the blocks of the partition matroid. A basis of the matroid is a set whose intersection with every block B_i has size exactly d_i, and a circuit of the matroid is a subset of a single block B_i with size exactly $d_i + 1$. The rank of the matroid is $\sum d_i$.

Every uniform matroid U_n^r is a partition matroid, with a single block B_1 of n elements and with $d_1 = r$. Every partition matroid is the direct sum of a collection of uniform matroids, one for each of its blocks.

Transversal Matroids:

In some publications, the notion of a partition matroid is defined more restrictively, with every $d_i = 1$. The partitions that obey this more restrictive definition are the transversal matroids of the family of disjoint sets given by their blocks.

Graphic Matroids:

A graphic matroid is the matroid defined from the edges of an undirected graph by defining a set of edges to be independent if and only if it does not contain a cycle. Every graphic matroid is regular, and thus is *F*-linear for every field *F*.

Gammoids:

Like uniform matroids and partition matroids, the gammoids, matroids representing reachability in directed graphs, are linear over every sufficiently large field. More specifically, a gammoid with n elements may be represented over every field that has at least 2^n elements.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Algebraic Matroids:

The algebraic matroids are matroids defined from sets of elements of a field extension using the notion of algebraic independence. Every linear matroid is algebraic, and for fields of characteristic zero (such as the real numbers) linear and algebraic matroids coincide, but for other fields there may exist algebraic matroids that are not linear.

Let *L* be a field. A **subfield** of *L* is a subset *K* of *L* which is closed under the field operations of *L* and under taking inverses in *L*. In other words, *K* is a field with respect to the field operations inherited from *L*. The larger field *L* is then said to be an **extension field** of *K*.

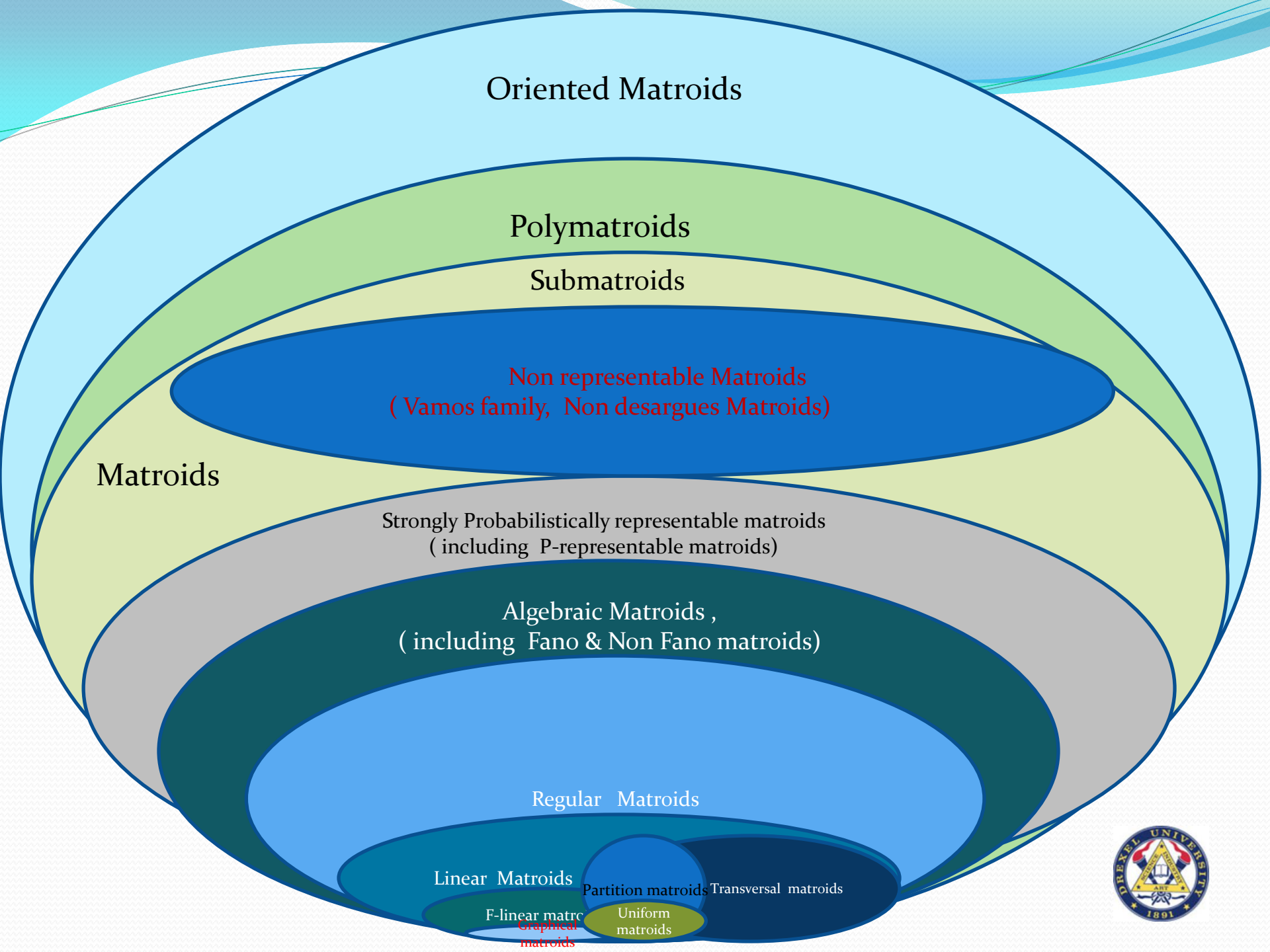
In abstract algebra, a subset *S* of a field *L* is **algebraically independent** over a subfield *K* if the elements of *S* do not satisfy any non-trivial polynomial equation with coefficients in *K*.

Matroids of Entropic Regions:

The **Shannon entropies** of all subvectors of a random vector are considered for the **coordinates of an entropic point** in a Euclidean space. The entropic points in a space define an **entropic region**. The problem to describe the region will be reviewed and connections to the matroid theory discussed.

Two classes of matroids are closely related:

Partition representable and asymptotically entropic. A matroid is **Partition Representable** if its rank function is a multiple of an entropic point. A matroid is **Asymptotically Entropic** if its rank function is in the closure of the entropic region.


Oriented Matroids
Polymatroids
Submatroids
Non representable Matroids
(Vamos family, Non desargues Matroids)
Matroids
Strongly Probabilistically representable matroids
(including P-representable matroids)
Algebraic Matroids ,
(including Fano & Non Fano matroids)
Regular Matroids
Linear Matroids
Partition matroids
Transversal matroids
F-linear matrc
Graphical matroids
Uniform matroids

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Non Representable Matroids:

The first matroid that was known to be not representable was the Vamos Matroid, this structure define an entire family of Non representable matroids. In 2009 the research team of Information Security Lab, College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, China, leaded by Chingfang Hsu and Qi Cheng have shown, based on discretization of the Vamos matroids family, that there is a way to generalize a sufficient condition for not representability of matroids.

Definition The Vamos matroid is defined on $\mathcal{Q}=\{1,2,3,4,5,6,7,8\}$ with bases all 4-sets except the five 4-sets which are: $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,2,7,8\}$, $\{3,4,5,6\}$, $\{3,4,7,8\}$.

Vamos Family

For the Vamos matroid $\mathcal{M}=(\mathcal{Q},\mathcal{I})$, there exists a partition $\Pi_0=\{P_1,P_2,P_3,P_4\}$ ($P_1=\{1,2\}, P_2=\{3,4\}, P_3=\{5,6,\}, P_4=\{7,8\}$) of the ground set $\mathcal{Q}$, and the partition Π_0 defines a mapping $\Pi_0:\mathcal{P}(\mathcal{Q})\rightarrow\mathbb{Z}_+^4$ and, hence, we obtain a discrete polymatroid $D_V=\Pi_0(\mathcal{I})$ corresponding to the Vamos matroid.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Proposition For a discrete polymatroid D with ground set J_m, if there exists $X \subseteq J_m$, where $|X| = 4$, such that $D(X) = D_V$, then D must be a non-representable discrete polymatroid, and hence, the multipartite matroid corresponding to D must be non-representable. All of these discrete polymatroids construct a family of non-representable matroids, that is, $F_{D_V} = \left\{ D \subset \mathbb{Z}_+^m : D(X) = D_V, X \subset J_m \text{且} |X| = 4 \right\}$, which we call Vamos Family.

A Sufficient Condition for a Discrete Polymatroid to Be Non-representable

Theorem Let $D \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m, if there exists $X \subseteq J_m$ such that $D(X) = \{u(X) : u \in D\} \subset \mathbb{Z}_+^{|X|}$ is a non-representable discrete polymatroid, then D must be a non-representable discrete polymatroid and, hence, the multipartite matroid corresponding to D must be non-representable.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Extension of this method to determine Representability using Secret Sharing schemes in general :

Definition of an Ideal Secrete Scheme from a representable matroid, general procedure:

Let $\mathbb{K}$ be a finite field and let $\mathcal{M}=(\mathcal{Q},\mathcal{I})$ be a $\mathbb{K}$-representable matroid. Let $p_0 \in \mathcal{Q}$ be special participant called dealer.and $\mathcal{Q}=P\cup\{p_0\}$. For every $k\times(n+1)$ matrix M representing $\mathcal{M}$ over $\mathbb{K}$, let E be a vector space of finite dimention $\dim E=k$ over $\mathbb{K}$. For every $i\in\mathcal{Q}$, we define a surjective linear mapping: $\pi_i : E\to\mathbb{K}$, and the i-th column of M corresponds to the linear form π_i. In that situation, for every random choice of an element $x\in E$, we can obtain $s_i=\pi_i(x)\in\mathbb{K}$ is the share of the participant $i\in P$ and $s=\pi_{p_0}(x)\in\mathbb{K}$ is the shared secret value. Hence, by the columns of M, we define an ideal secret sharing scheme with access structure $\Gamma_{p_0}(\mathcal{M})$, where $\min\Gamma_{p_0}(\mathcal{M})=\{A\subseteq P : A\cup\{p_0\} \text{is a circuit of } \mathcal{M}\}$. Therefore, the access structures induced by representable matroids are ideal.

Discretization of the Ideal Sharing scheme via Partition of disjoint subsets:

We write $\mathcal{P}(P)$ for the power set of the set P. An m-partition $\Pi=\{P_1,\ldots,P_m\}$ of a set P is a disjoint family of m nonempty subsets of P with $P=P_1\cup\ldots\cup P_m$. Let $\Lambda\subseteq\mathcal{P}(P)$ be a family of subsets of P. For a permutation σ on P, we define $\sigma(\Lambda)=\{\sigma(A) : A\in\Lambda\}\subseteq\mathcal{P}(P)$. A family of subsets $\Lambda\subseteq\mathcal{P}(P)$ is said to be Π-partite if $\sigma(\Lambda)=\Lambda$ for every permutation σ such that $\sigma(P_i)=P_i$ for every $P_i\in\Pi$. We say that Λ is m-partite if it is Π-partite for some m-partition Π. These concepts can be applied to access structures and matroids.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Construction of a discrete Polymatroid from the Partitioned scheme , in the most general case.

For every integer $m \geq 1$, we consider the set $J_m = \{1,...,m\}$. Let $\mathbb{Z}_+^m$ denote the set of vectors $u = (u_1,...,u_m) \in \mathbb{Z}^m$ with $u_i \geq 0$ for every $i \in J_m$. For a partition $\Pi = \{P_1,...,P_m\}$ of a set P and for every $A \subseteq P$ and $i \in J_m$, we define $\Pi_i(A) = |A \cap P_i|$. Then the partition Π defines a mapping $\Pi : \mathcal{P}(P) \to \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A),...,\Pi_m(A))$. If $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda)$. That is, Λ is completely determined by the partition Π and the set of vectors $\Pi(\Lambda) \subset \mathbb{Z}_+^m$.

Definition of needed operators on the vector spaces :

If $u, v \in \mathbb{Z}_+^m$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J_m$, and we write $u < v$ if $u \leq v$ and $u \neq v$. The vector $w = u \vee v$ is defined by $w_i = \max(u_i, v_i)$. The modulus of a vector $u \in \mathbb{Z}_+^m$ is $|u| = u_1 + \cdots + u_m$. For every subset $X \subseteq J_m$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^{|X|}$ and $|u(X)| = \sum_{i \in X} u_i$

Conceptualization of the Discrete Polymatroid:

A discrete polymatroid on the ground set J_m is a nonempty finite set of vectors $D \subset \mathbb{Z}_+^m$ satisfying:

1. if $u \in D$ and $v \in \mathbb{Z}_+^m$ is such that $v \leq u$, then $v \in D$, and
2. for every pair of vectors $u, v \in D$ with $|u| < |v|$, there exists $w \in D$ with $u < w \leq u \vee v$.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

A **relation between multipartite matroids and discrete polymatroids** emerge directly from the axioms of independent sets and can be expressed by the following proposition:

Proposition 2.1. Let Π be a partition of a set $\mathcal{Q}$ and let $\mathcal{I} \subseteq \mathcal{P}(\mathcal{Q})$ be a Π-partite family of subsets. Then $\mathcal{I}$ is the family of the independent sets of a Π-partite matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ if and only if $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is a discrete polymatroid.

The bases of the Polymatroid are defined as:

Proposition 2.2. A nonempty subset $\mathcal{B} \subset \mathbb{Z}_+^m$ is the family of bases of a discrete polymatroid if and only if it satisfies:

1. all elements in $\mathcal{B}$ have the same modulus, and
2. for every $u \in \mathcal{B}$ and $v \in \mathcal{B}$ with $u_i > v_i$, there exists $j \in J_m$ such that $u_j < v_j$ and $u - e_i + e_j \in \mathcal{B}$, where e_i denotes the i-th vector of the canonical basis of $\mathbb{Z}^m$.

While its rank function is given by:

The rank function of a discrete polymatroid D with ground set J_m is the function $h : \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \max\{|u(X)| : u \in D\}$. The next proposition is a consequence of

Properties of its rank function are:

Proposition 2.3. A function $h : \mathcal{P}(J_m) \to \mathbb{Z}$ is the rank function of a discrete polymatroid with ground set J_m if and only if it satisfies

1. $h(\phi) = 0$, and
2. h is monotone increasing: if $X \subseteq Y \subseteq J_m$, then $h(X) \le h(Y)$, and
3. h is submodular: if $X, Y \subseteq J_m$, then $h(X \cup Y) + h(X \cap Y) \le h(X) + h(Y)$.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Characterization of the Polymatroid using its rank function:

$$D = \left\{ u \in \mathbb{Z}_+^m : \ |u(X)| \leq h(X) \text{ for all } X \subseteq J_m \right\}$$

Definition of representability of Matroid based on its rank function:

Let $\mathbb{K}$ be a field, E a $\mathbb{K}$-vector space, and $V_1, \ldots, V_m$ subspaces of E. It is not difficult to check that the mapping $h : \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of a discrete polymatroid $D \subset \mathbb{Z}_+^m$. In this situation, we say that D is $\mathbb{K}$-representable and the subspaces $V_1, \ldots, V_m$ are a $\mathbb{K}$-representation of D.

Criteria of Representability of the Secret Shared scheme Matroid based in the associated discrete polymatroid built through partitions:

Proposition 2.4. Let $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ be a Π-partite matroid and let $D = \Pi(\mathcal{I})$ be its associated discrete polymatroid. If $\mathcal{M}$ is $\mathbb{K}$-representable, then so is D. In addition, if D is $\mathbb{K}$-representable, then $\mathcal{M}$ is representable over some finite extension of $\mathbb{K}$.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Generalizacions of Matroids (Supermatroids and Convex Geometries)

Dunstan, Ingleton, and Welsh introduced the concept of a *supermatroid* in 1972 as a generalization of the concept of an ordinary matroid and integral polymatroid.

Distributive supermatroids or poset matroids are supermatroids defined on distributive lattices or sets of order ideals of partially ordered sets (posets).

Cg Matroids have been defined and worked by a research team of the Kyoto University – Research Institute of Mathematical Sciences and the Central Institute of Economics and Mathematics of the Russian Academy of sciences since 2006.

The concept of a distributive supermatroid (or a poset matroid) can be generalized by considering a convex geometry, instead of a poset, as the underlying combinatorial structure on which we define a matroidal structure, which we call a *cg-matroid*.

Characterizations of cg-matroids is done by means of the exchange property for bases and the augmentation property for independent sets.

Strict cg-matroids will turn out to be exactly cg-matroids that are also supermatroids. In other words, strict cg-matroids are exactly supermatroids defined on the lattices of closed sets of convex geometries.

Closure Space: Let E be a nonempty finite set and $\mathcal{F}$ be a family of subsets of E. The pair $(E, \mathcal{F})$ is called a *closure space* on E if it satisfies the following two conditions:

(F0) $\emptyset,\ E \in \mathcal{F}$.

(F1) $X, Y \in \mathcal{F} \Longrightarrow X \cap Y \in \mathcal{F}$.

Posets: A (non-strict) **partial order** is a binary relation "≤" over a set *P* which is antysymmetric, transitive, and reflexive, i.e., for all *a*, *b*, and *c* in *P*, we have that: $a \le a$ (reflexivity) for all *a* in P; if $a \le b$ and $b \le a$ then $a = b$ (antisymmetry); if $a \le b$ and $b \le c$ then $a \le c$ (transitivity).
In other words, a partial order is an antisymmetric preorder.
A set with a partial order is called a **partially ordered set** (also called a **poset**

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

SuperMatroids:

Let us now deal with supermatroids. A pair $(\mathscr{S}, \mathscr{F})$ is a *supermatroid on* $\mathscr{S}$ if $\mathscr{S} = (\mathscr{S}, \leqslant)$ is a poset with 0 and height function $|\ |$, and $\mathscr{F} \subseteq \mathscr{S}$ is a subset such that:

$(I1)^{SM}$ For all $I \in \mathscr{F}$, if $K \in \mathscr{S}$ and $K \leqslant I$, then $K \in \mathscr{F}$;

$(I2)^{SM}$ $|I| = |K|$ for all maximal $I, K \in [0, A] \cap \mathscr{F}$ and all $A \in \mathscr{S}$.

Convex Geometry:

The set E is called the *ground set* of the closure space $(E, \mathcal{F})$, and each member of $\mathcal{F}$ is called a *closed set*. Moreover, we call the closure space $(E, \mathcal{F})$ a *convex geometry* if it satisfies the following condition:

(F2) $\forall X \in \mathcal{F} \setminus \{E\},\ \exists e \in E \setminus X:\ X \cup \{e\} \in \mathcal{F}.$

Condition (F2) is equivalent to the following chain condition:

(F2)′ Every maximal chain $\emptyset = X_0 \subset X_1 \subset \cdots \subset X_n = E$ in $\mathcal{F}$ has length $n = |E|$.

Closure Operator:

Next we define an operator $\tau : 2^E \longrightarrow 2^E$ associated with the closure space $(E, \mathcal{F})$. For any $X \in 2^E$ define

$$\tau(X) = \bigcap \{Y \in \mathcal{F} \mid X \subseteq Y\}.$$

That is, $\tau(X)$ is the unique minimal closed set containing X. The operator τ satisfies the following properties (cl0)∼(cl3):

(cl0) $\tau(\emptyset) = \emptyset$.

(cl1) $X \subseteq \tau(X)$ for $X \in 2^E$ (Extensionality).

(cl2) $X \subseteq Y \Longrightarrow \tau(X) \subseteq \tau(Y)$ for any $X, Y \in 2^E$ (Monotonicity).

(cl3) $\tau(\tau(X)) = \tau(X)$ for any $X \in 2^E$ (Idempotence).

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

In general, any operator $\tau : 2^E \to 2^E$ satisfying the four conditions given above is called a *closure operator*. Conversely, given a closure operator τ, define $\mathcal{F} = \{X \in 2^E \mid \tau(X) = X\}$. Then $\mathcal{F}$ forms a closure space on E. Hence, for a finite set E and a closure operator τ on E we also call the pair (E, τ) a *closure space*.

In terms of closure operator, a closure space (E, τ) is a convex geometry if and only if it satisfies the following property, called the *anti-exchange property*:

(AE) $X \subseteq E,\ p \in E \setminus \tau(X),\ q \in \tau(X \cup \{p\}) \setminus \{p\} \implies p \notin \tau(X \cup \{q\}).$

Graded lattices Operations:

Every convex geometry forms a graded lattice with respect to set-inclusion, where the lattice operations *join* $\vee$ and *meet* $\wedge$ are given by

$$X \vee Y = \tau(X \cup Y), \qquad X \wedge Y = X \cap Y$$

for any $X, Y \in \mathcal{F}$.

Convex Geometry Matroids:

For a convex geometry $(E, \mathcal{F})$ and a family $\mathcal{B} \subseteq \mathcal{F}$, suppose that $\mathcal{B}$ satisfies the following three conditions:

(B0) $\mathcal{B} \neq \emptyset$.

(B1) $B_1, B_2 \in \mathcal{B},\ B_1 \subseteq B_2 \implies B_1 = B_2$.

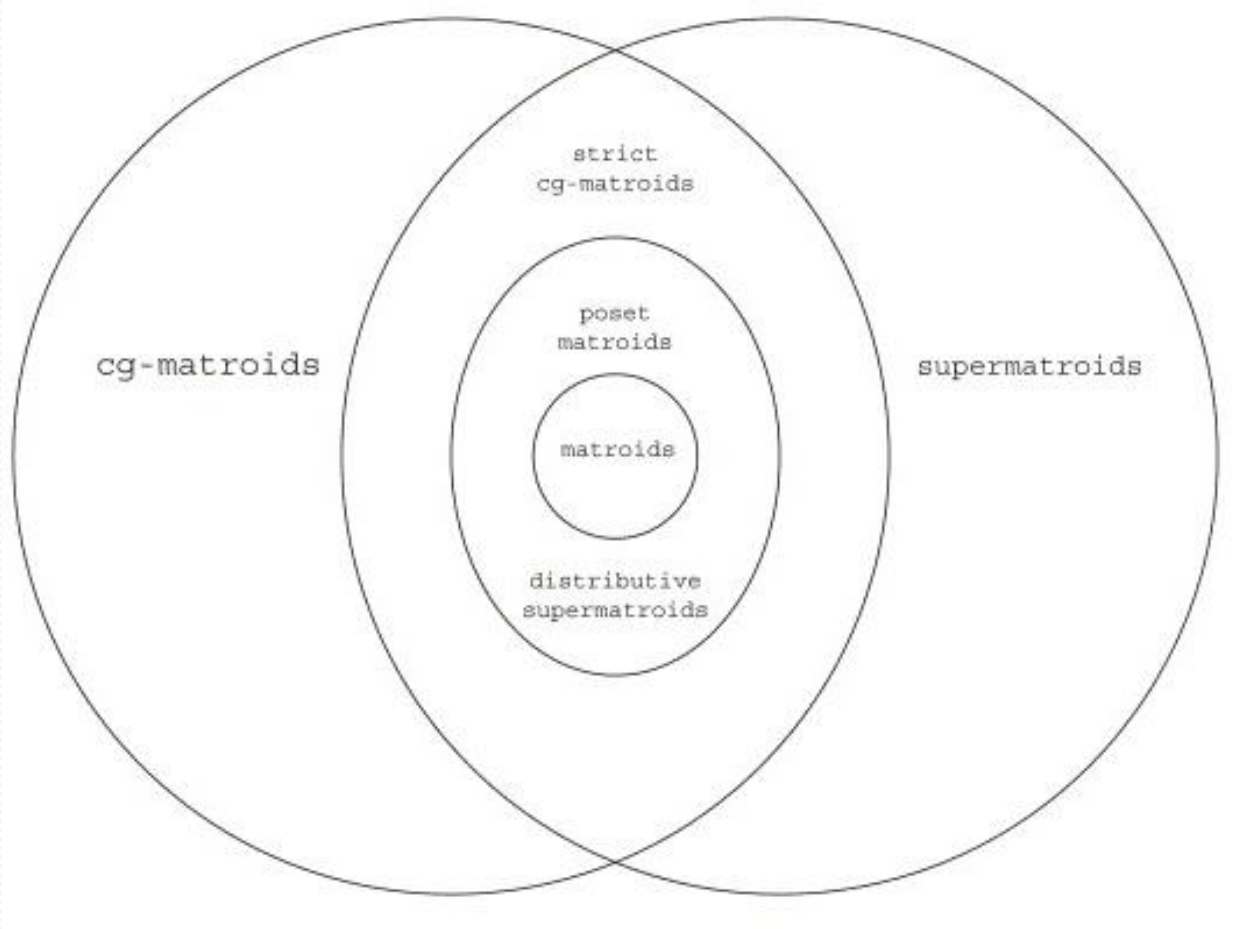
(BM) (Middle Base Property)
For any $B_1, B_2 \in \mathcal{B}$ and $X, Y \in \mathcal{F}$ with $X \subseteq B_1,\ B_2 \subseteq Y$, and $X \subseteq Y$, there exists $B \in \mathcal{B}$ such that $X \subseteq B \subseteq Y$.

Then we call $(E, \mathcal{F}; \mathcal{B})$ a *matroid on the convex geometry* $(E, \mathcal{F})$ (or a *cg-matroid* for short). Each $B \in \mathcal{B}$ is called a *base*, and $\mathcal{B}$ the *family of bases* of cg-matroid $(E, \mathcal{F}; \mathcal{B})$. □

Note that a cg-matroid $(E, \mathcal{F}; \mathcal{B})$ is an ordinary matroid when $\mathcal{F} = 2^E$ and that $(E, \mathcal{F}; \mathcal{B})$ is a poset matroid (or a distributive supermatroid) when $\mathcal{F}$ is the set of order ideals of a poset on E.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Formal definition: Partition Representable Matroid

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 $\xi_I = \bigwedge_{i \in I} \xi_i$ has $d^{r(I)}$ blocks of the same cardinality for every $I \subset N$.

Alternative Names: Secret Sharing Schemes and Almost Affine Codes

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.

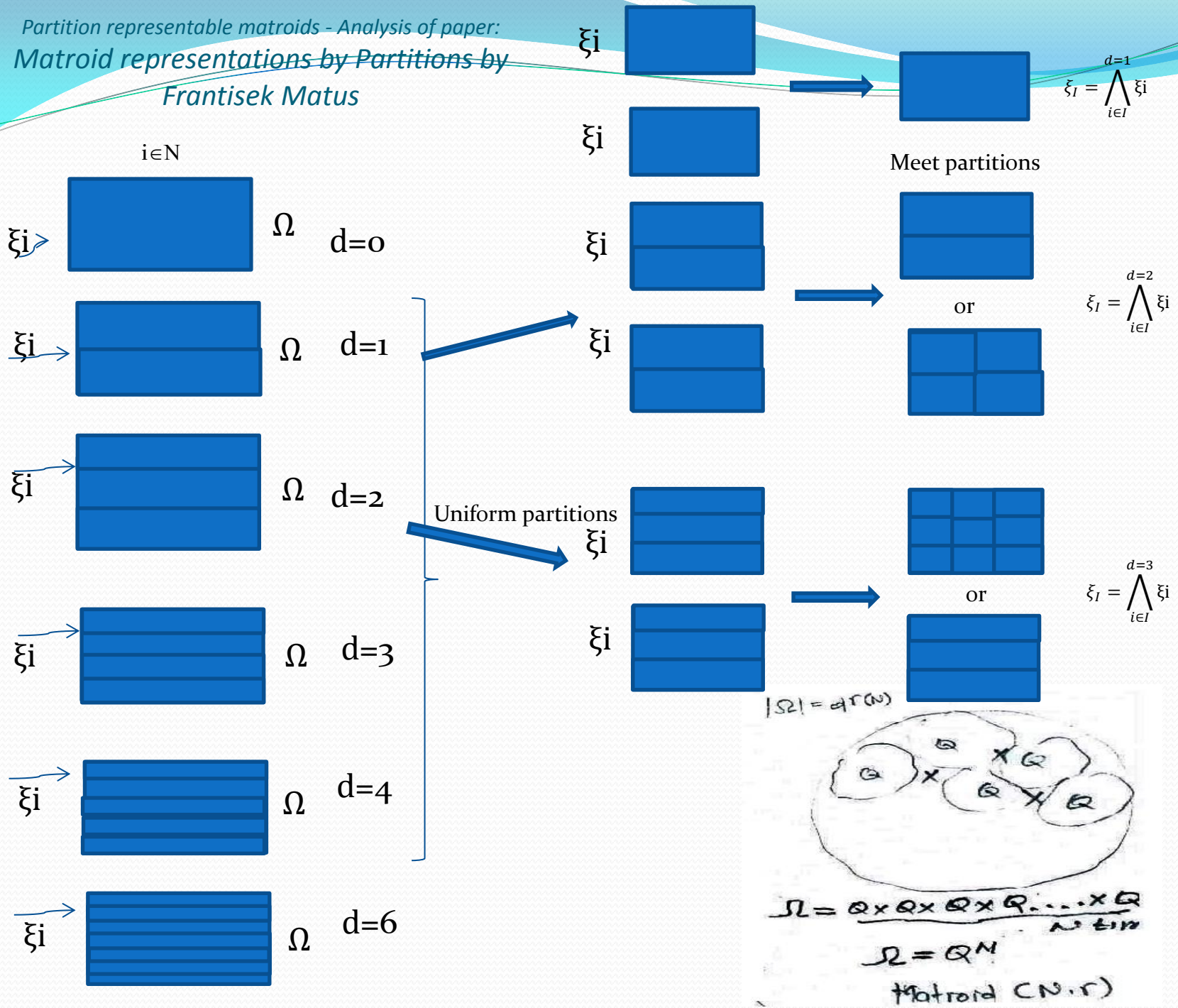
Meet Partitions of P-representation are Uniform:

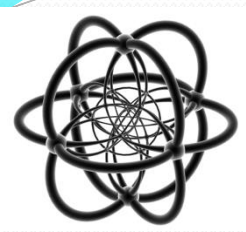
A partition with all blocks having the same number of elements will be termed uniform. All meet-partitions of a p-representation are uniform:

All blocks of ξ_I have the cardinality $d^{r(N)-r(I)}$; especially, ; ξ_ϕ has only one block being the whole set and ξ_N N has $d^{r(N)}$ blocks being the singletons of Ω.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus





Partition representable matroids - Analysis of paper:

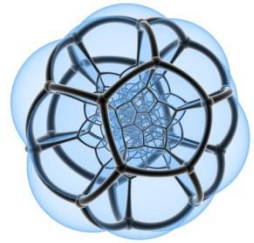
Matroid representations by Partitions by Frantisek Matus

Motivation of the concept in Matroid Theory:

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

Other Research fields that have found the same concept:

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.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Formal definitions: **Partitions are Random Variables**

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.

$\xi_I,\ I \subset N,$ can be considered as a **Set Algebra** with **Probability space** (Ω, p)

Where the **Shannon entropy is defined as:** $h_\xi(I) = -\sum_{A \in \xi_I} p(A) \ln p(A)$

And the Probability of the block A from ξ_I is given by : $p(A) = \sum_{\omega \in A} p(\omega)$

h_ξ is the **entropy function** of ξ.

(N, h_ξ) is known to be a **Polymatroid**.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

What is the meaning that the $\xi_I, I \subset N,$ must be a set algebra? That they must obey the following properties:

The fundamental laws of set algebra

The binary operations of set union and intersection satisfy many identities.

PROPOSITION 1: For any sets *A*, *B*, and *C*, the following identities hold:

commutative laws:

- $A \cup B = B \cup A$
- $A \cap B = B \cap A$

associative laws:

- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \cap B) \cap C = A \cap (B \cap C)$

distributive laws:

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

PROPOSITION 2: For any subset *A* of universal set **U**, where Ø is the empty set, the following identities hold:

identity laws:

- $A \cup \varnothing = A$
- $A \cap U = A$

complement laws:

- $A \cup A^C = U$
- $A \cap A^C = \varnothing$

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Probability space of the Partitions:

At the same time the ξ_I, $I \subset N$, constitute a Probability space:

A probability space is a mathematical triplet $(\Omega, \mathcal{F}, P)$ that presents a model for a particular class of real-world situations.

A probability space consists of three parts:

1. A sample space, Ω, which is the set of all possible outcomes.
2. A set of events $\mathcal{F}$, where each event is a set containing zero or more outcomes.
3. The assignment of probabilities to the events; that is, a function P from events to probabilities.

The prominent Soviet mathematician Andrey Kolmogorov introduced the notion of probability space, together with other axioms of probability, in the 1930s.

An outcome is the result of a single execution of the model. Since individual outcomes might be of little practical use, more complex *events* are used to characterize groups of outcomes. The collection of all such events is a *σ-algebra* $\mathcal{F}$.

Finally, there is a need to specify each event's likelihood of happening. This is done using the *probability measure* function, P.

In short, a probability space is a measure space such that the measure of the whole space is equal to one.

The expanded definition is following: a probability space is a triple $(\Omega, \mathcal{F}, P)$ consisting of:

- the sample space Ω — an arbitrary non-empty set,
- the σ-algebra $\mathcal{F} \subseteq 2^{\Omega}$ (also called σ-field) — a set of subsets of Ω, called events, such that:
  - $\mathcal{F}$ contains the empty set: $\emptyset \in \mathcal{F}$,
  - $\mathcal{F}$ is closed under complements: if $A \in \mathcal{F}$, then also $(\Omega \setminus A) \in \mathcal{F}$,
  - $\mathcal{F}$ is closed under countable unions: if $A_i \in \mathcal{F}$ for $i=1,2,\ldots$, then also $(\cup_i A_i) \in \mathcal{F}$
    - The corollary from the previous two properties and De Morgan's law is that $\mathcal{F}$ is also closed under countable intersections: if $A_i \in \mathcal{F}$ for $i=1,2,\ldots$, then also $(\cap_i A_i) \in \mathcal{F}$
- the probability measure P: $\mathcal{F} \to [0,1]$ — a function on $\mathcal{F}$ such that:
  - P is countably additive: if $\{A_i\} \subseteq \mathcal{F}$ is a countable collection of pairwise disjoint sets, then $P(\sqcup A_i) = \sum P(A_i)$, where "$\sqcup$" denotes the disjoint union,
  - the measure of entire sample space is equal to one: $P(\Omega) = 1$.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Strongly probabilistically representable Matroids

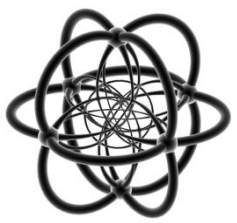
Given this partition, if $p(\omega) = |\Omega|^{-1}$ for $\omega \in \Omega$ then $h_\xi = r \cdot \ln d$ where d is the degree of ξ

We say (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

$$h_\xi = c \cdot r$$

Every strong probabilistic representation ξ (over some (Ω, p)) of a connected matroid with rank at least two has associated a unique integer number $d \geq 2$ such that $p(A) = d^{-r(I)}$, $A \in \xi_I$ $I \subset N$

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.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Semimatroids (Formal definition)

Let (N, g) be a polymatroid and $|[g]|$ be the family of those triples $(i, j|K)$, $K \subset N$, $i, j \in N - K$, which satisfy

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

The family $|[g]|$ defined in this way is called Semimatroid.

Probabilistically representable Semimatroids:

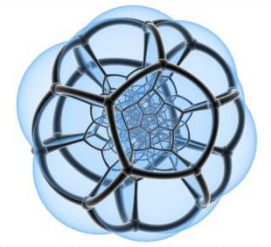
if for a system of random variables ξ on (Ω, p) a triple $(i, j|K)$ belongs to it if and only if ξ_i is stochastically conditionally independent of ξ_j given ξ_K

A necessary and sufficient condition for this is $h_\xi(i \cup K) + h_\xi(j \cup K) = h_\xi(K) + h_\xi(i \cup j \cup K)$
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

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus



Weakly probabilistically representable Matroids:

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 $K \subset N$ and $i, j \in N - K$.

Secret-sharing schemes

Let N be a finite set (of participants), $0 \in N$ be a distinguished element of N (dealer), and $\mathcal{A}$ a nonempty family (access structure) of subsets of $N - 0$ no two of them being in a set inclusion. Let us suppose that every $i \in N - 0$ is contained in some $J \in \mathcal{A}$

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 $I \subset N - 0$ containing some $J \in \mathcal{A}$.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Perfect secret-sharing scheme

A secret-sharing scheme is *perfect* if $h_\xi(0 \cup I)=h_\xi(0)+h_\xi(I)$ for every $I \subset N-0$ containing no $J \in \mathscr{A}$; in such a scheme if $i \in N-0$ then $i \in J$ for some $J \in \mathscr{A}$ and

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

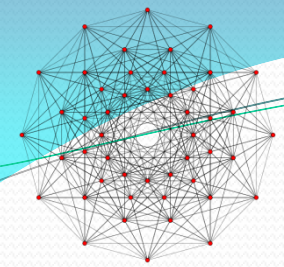
Ideal secret-sharing scheme

if $h_\xi(i) = h_\xi(0) > 0$ for all $i \in N-0$.

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

$$\mathscr{A} = \{J \subset N-0;\ 0 \cup J \text{ is a circuit of } (N,r)\} \quad h_\xi = c \cdot r \text{ for a positive number } c$$

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.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

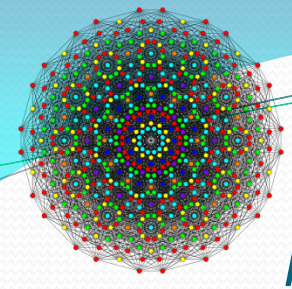
Duality

It is interesting to ask whether the dual of a p-representable matroid is p-representable?

There is a natural extension of the matroid duality to the class of semimatroids containing only the triples (i; j|K) with i /= 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.

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



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Comparing matroid representations

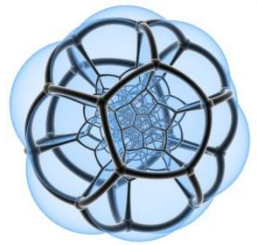
Linearly representable Matroids:

Linearly (l-) representable matroids are p-representable. 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, that is, there are linear functionals x_i , i ∈ 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 ∈ I , I ⊂ 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.

Multilinearly representable 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 $I \subset N$. If the subspaces have ranks at most 1 we have an l-representation. Obviously, ml-representable matroids are p-representable.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Obviously, ml-representable matroids are p-representable. The problem whether there exists a p-representable non-ml-representable matroid, remains open.

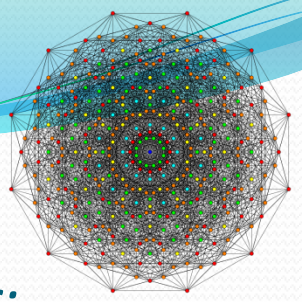
To solve, it would suffice to find a p-representable matroid such that its rank function does not satisfy the Ingleton inequality. This inequality is a necessary condition for a matroid to be ml-representable but entropy functions do exist violating it

An algebraically (a-) representable matroid need not be p-representable. A natural question is whether a p-representable and non-a-representable matroid exists.

Any minor of a matroid having a p-representation of some degree d is p-representable of the same degree d, [33,40].

A matroid is p-representable of degree two and three if and only if it is binary and ternary, respectively, see [33,5]. Even more, all its p-representations are p-isotopic to l-representations, [40].

Since the matroids $L_n,\ n \geqslant 2$ nonprime 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.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

The p-characteristic set of a matroid

It is the set of all integers $d \geqslant 2$ch 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;:: :} 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. All the remaining p-representations are simply $\xi \otimes \xi$, $\xi \otimes \xi \otimes \xi$, ...

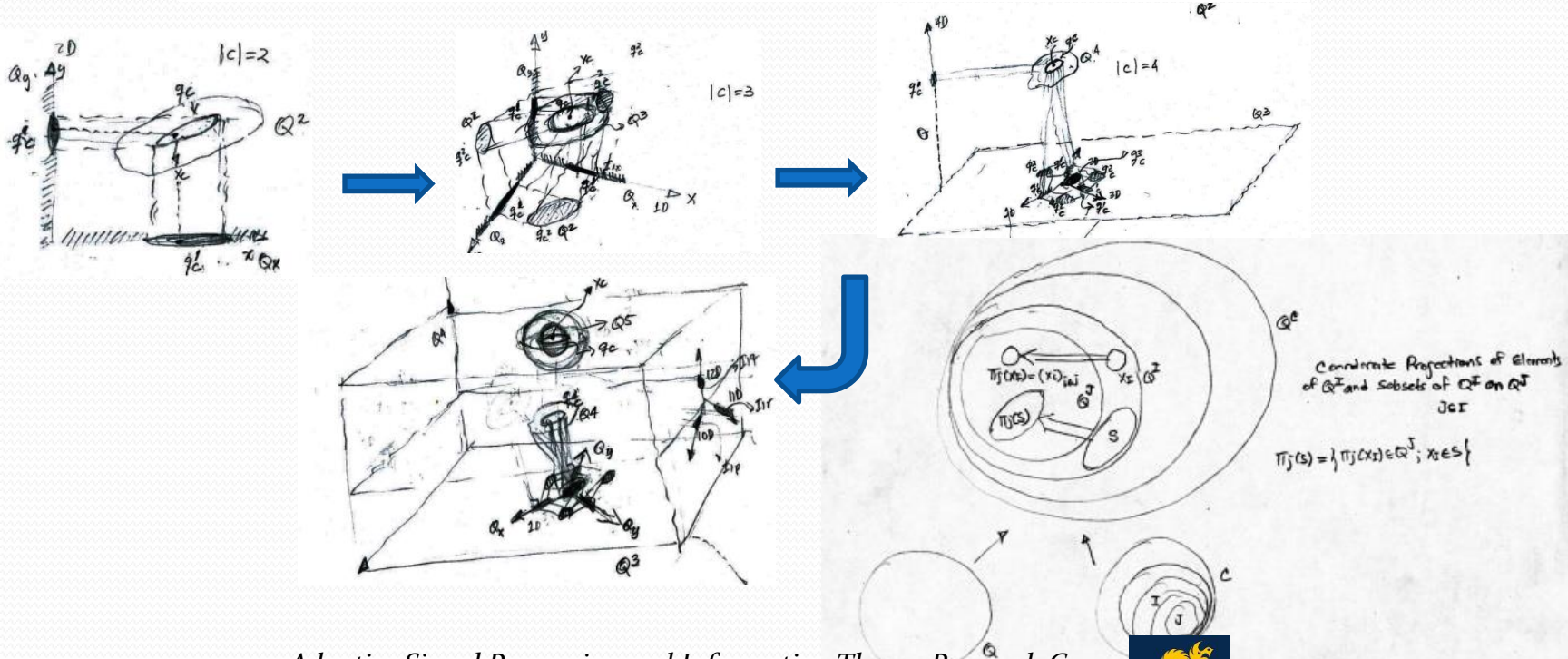
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representaiton of Matroids

Coordinate Projection:

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, $J \subset I$, 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 $\pi_J(S) = \{\pi_J(x_I) \in Q^J;\ x_I \in S\}$.



Partition representable matroids - Analysis of paper:

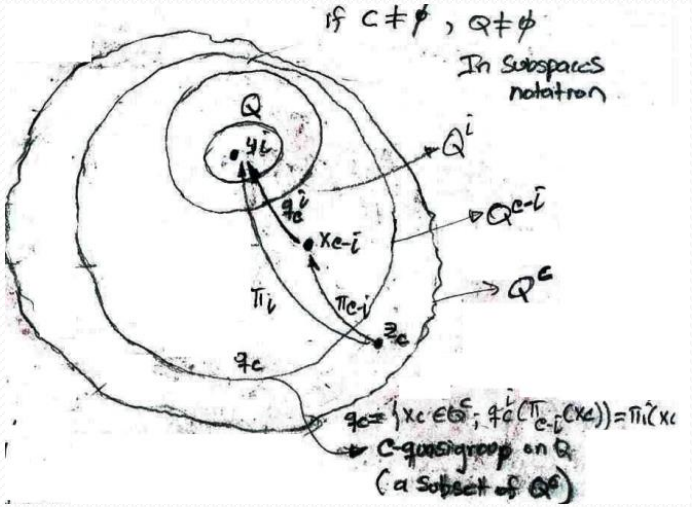
Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representaiton of Matroids

Parastrophic quasigroups mappings:

$q_C^i : Q^{C-i} \to Q$ are parastrophic quasigroups on Q (of arity $|C| - 1$) in the usual sense; for background on the quasigroup theory see [14,15]. Note that for all $i \in C$

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



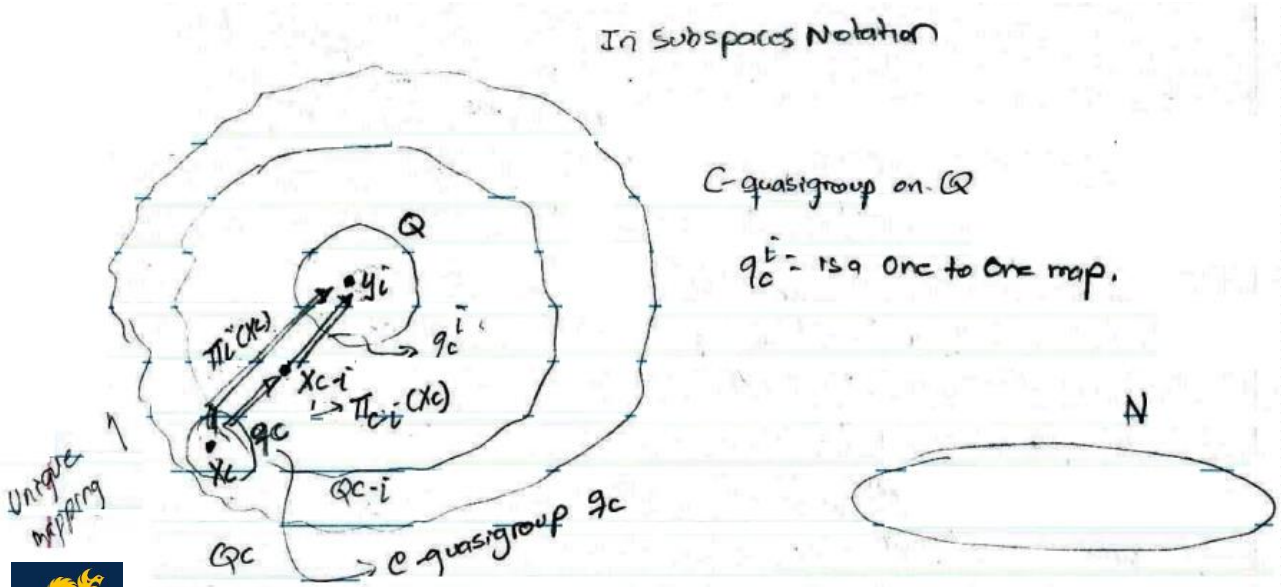
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

C-Quasigroup:

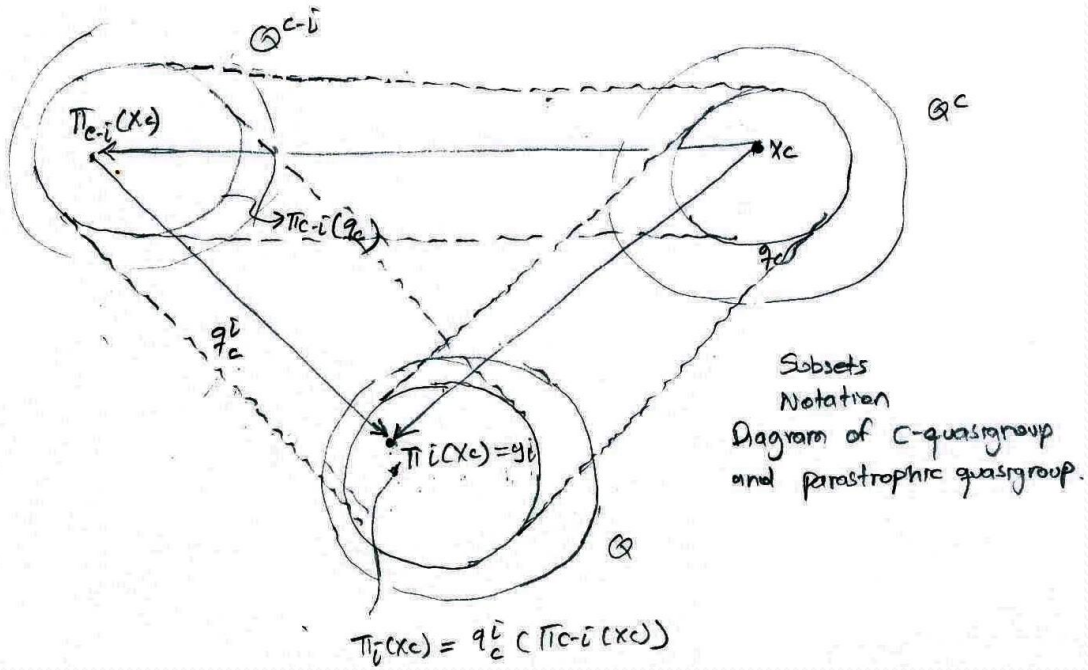
If C is a nonempty set then a *C-quasigroup* on $Q \neq \emptyset$ will be for us a special subset q_C of Q^C defined as follows. For every $i \in C$, to every $x_{C-i} \in Q^{C-i}$ there exists a unique $y_i \in Q$ such that the C-tuple z_C composed from $\pi_{C-i}(z_C) = x_{C-i}$ and $\pi_i(z_C) = y_i$ belongs to q_C.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

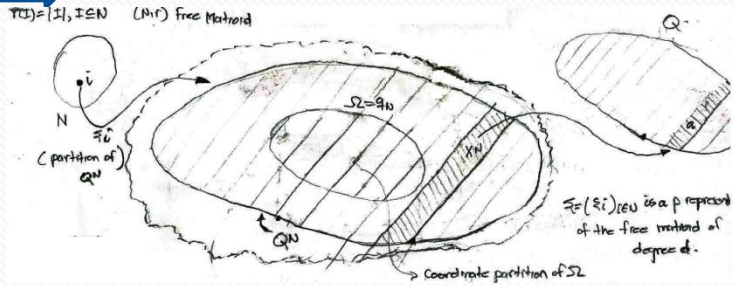
Review Chart: Parastrophic Quasigroups, C-Quasigroups, Coordinate Projections

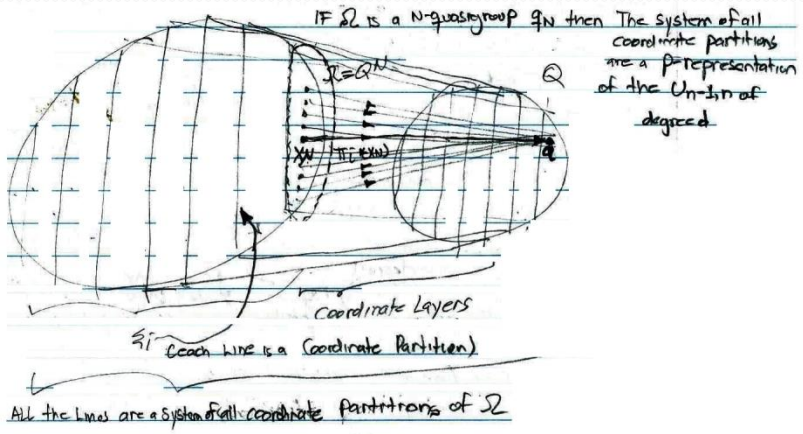


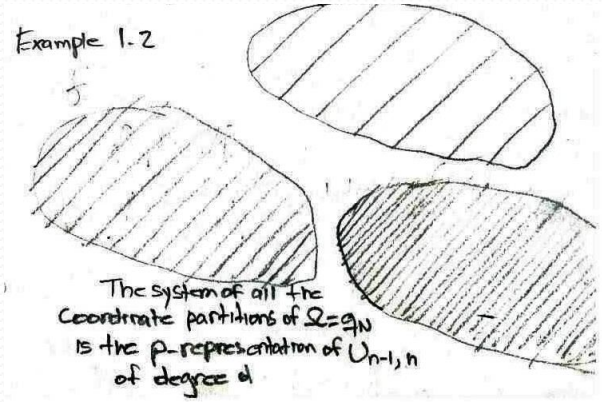
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Example 1.2. Let (N,r) be the free matroid on N $(r(I)=|I|,\ I\subset N)$ 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 ith 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 $\Omega=q_N\subset Q^N$ 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 $r(I)=\min\{|I|,n-1\}$, $I\subset N$; the only circuit of the matroid is $C=N$.







Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

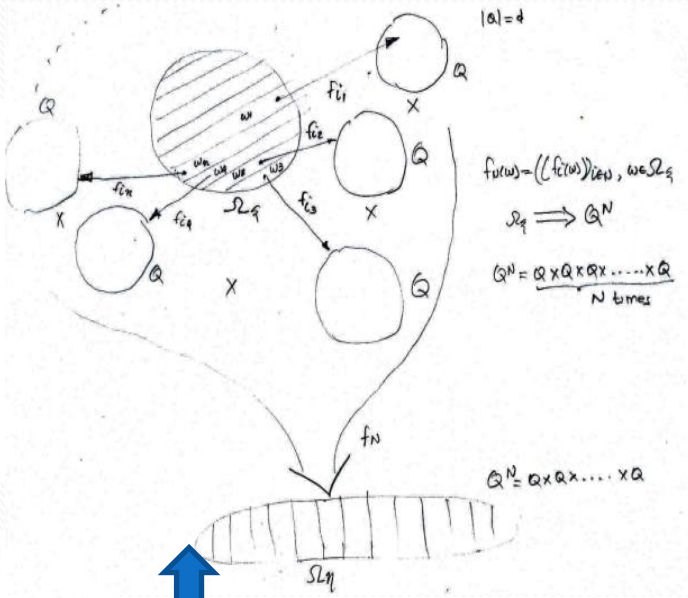
Essential concepts involved in the Partition Representation of Matroids

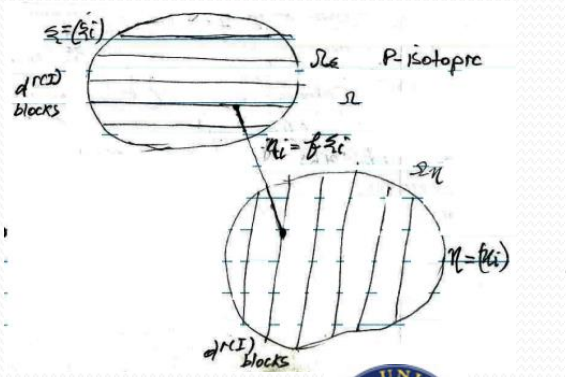
P-isotopic representations:

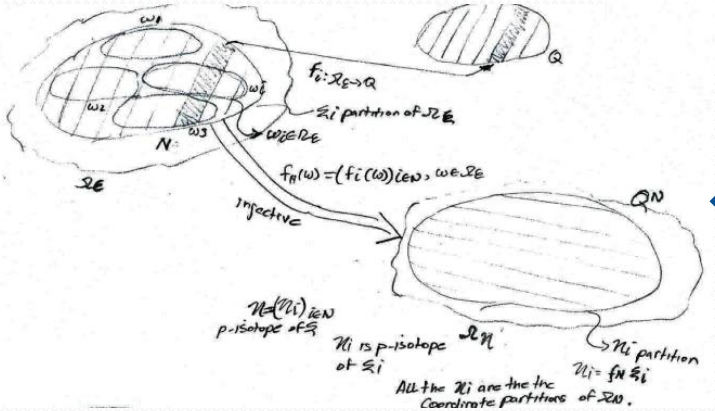
Definition Two p-representations $\xi=(\xi_i)_{i\in N}$ and $\eta=(\eta_i)_{i\in N}$ of a matroid (N,r), living on two sets Ω_ξ and Ω_η, respectively, are *p-isotopic* if there exists a bijection f of Ω_ξ onto Ω_η such that $f\xi_i=\eta_i$ for all $i\in N$.

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 $I\subset N$.

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 $f_i:\Omega_\xi\to Q$ 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 obvious that all partitions within η are the coordinate partitions of Ω_η.







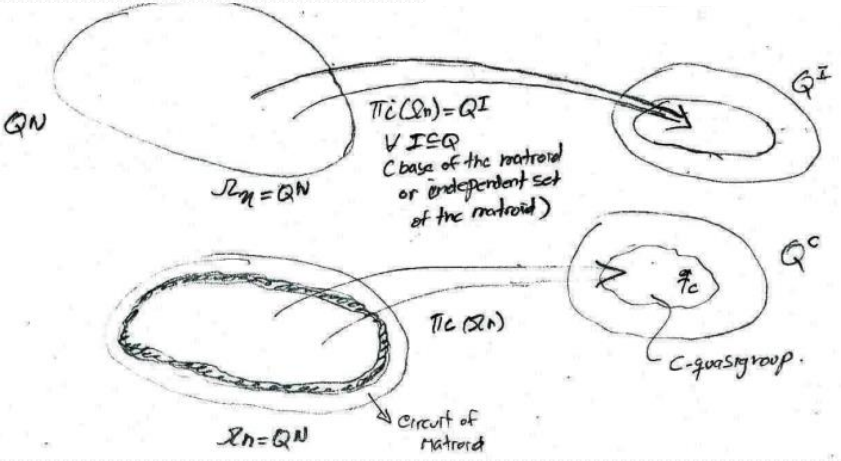
Adaptive Signal Processing and Information Theory Research Group
Drexel University , Philadelphia , Pennsylvania, summer 2013

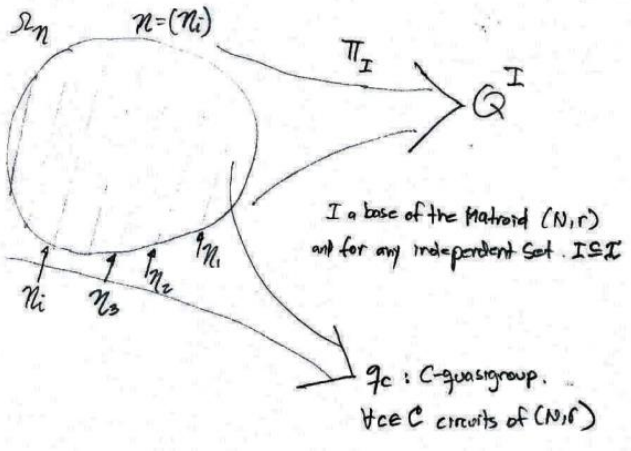
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

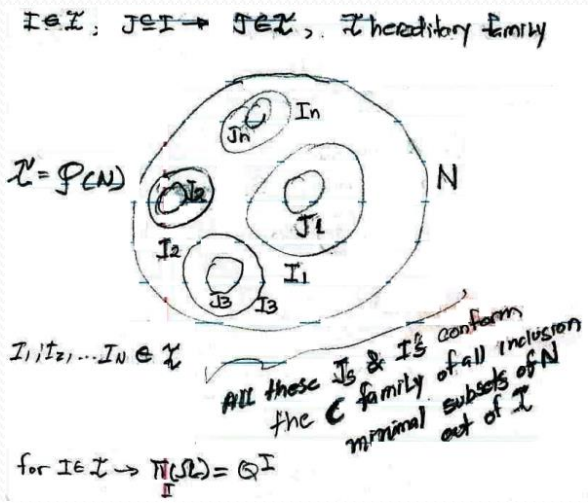
We have just seen that every p-representation ξ of a matroid is p-isotopic to the p-representation η which lives on a subset of a Cartesian product and consists of all coordinate partitions of the subset. It is not difficult to see that $\pi_I(\Omega_\eta) = Q^I$ for any base I of the matroid (and consequently 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.



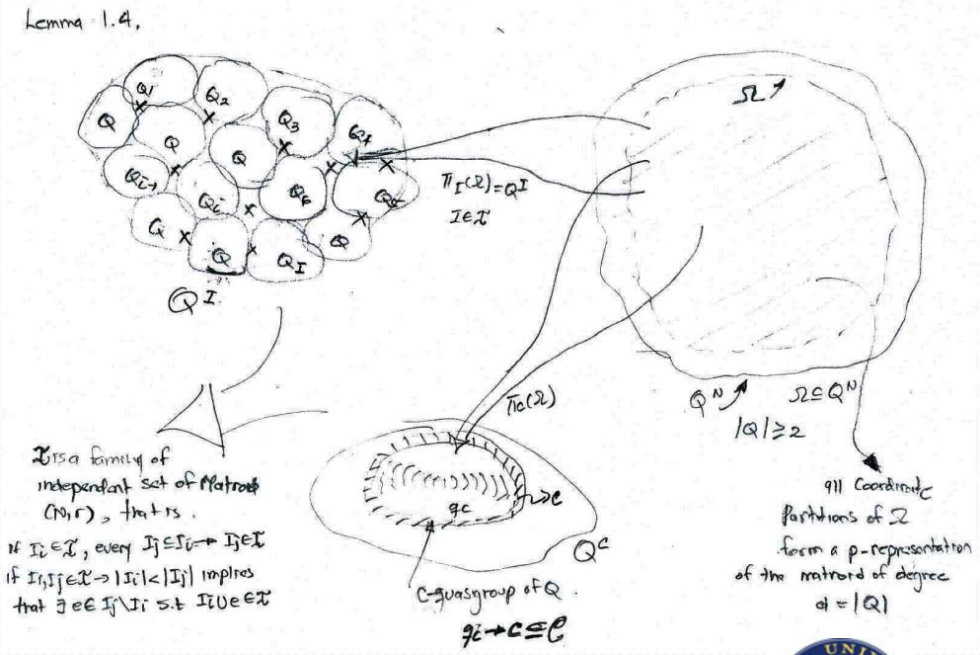


Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus



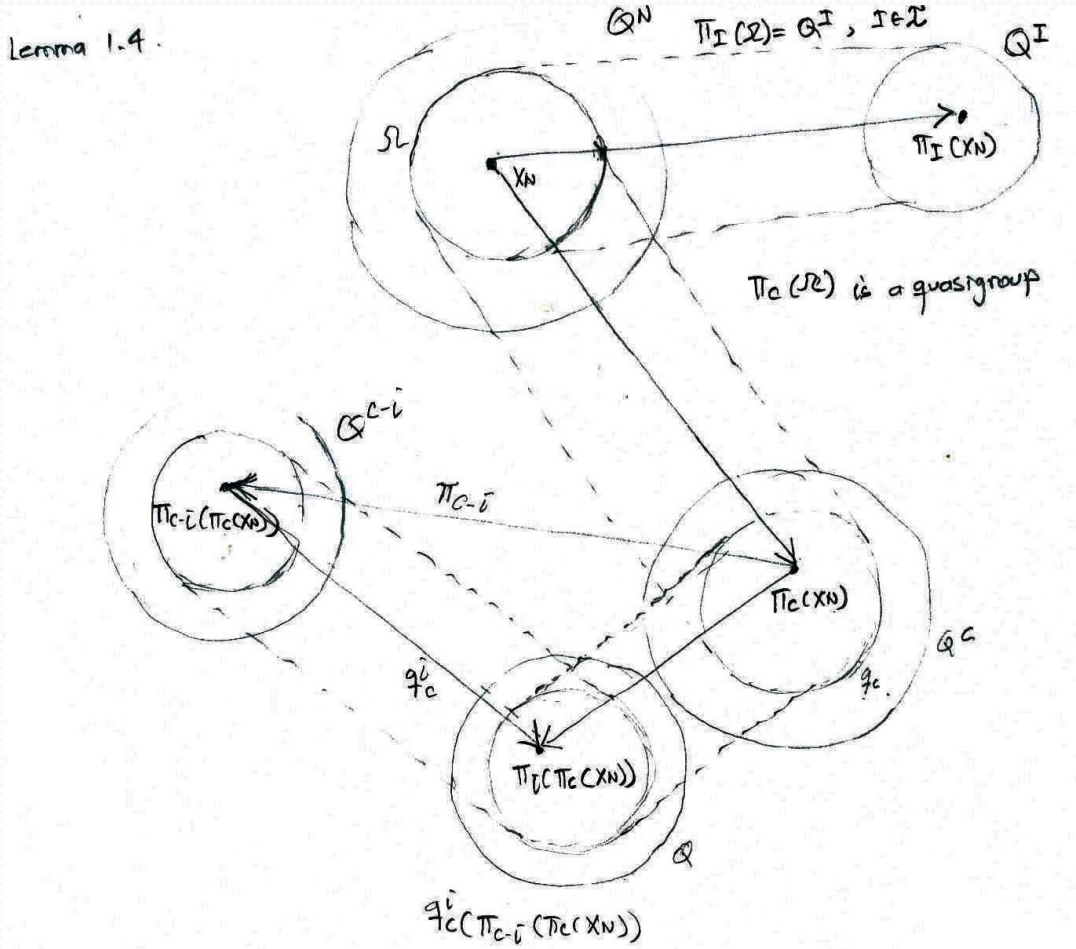
Lemma 1.4. *Let N be a finite nonempty set and $\mathcal{I}$ a nonempty hereditary family of subsets of N ($I \in \mathcal{I}$ and $J \subset I$ implies $J \in \mathcal{I}$). We denote by $\mathscr{C}$ the family of all inclusion-minimal subsets of N out of $\mathcal{I}$. If Ω is a subset of a Cartesian product Q^N, $|Q| \geq 2$ finite, such that $\pi_I(\Omega) = Q^I$ for $I \in \mathcal{I}$* and *$\pi_C(\Omega)$ is a C-quasigroup on Q for $C \in \mathscr{C}$ 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 $|Q|$.*



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Review Chart: Concepts already defined and involved in lemma 1.4



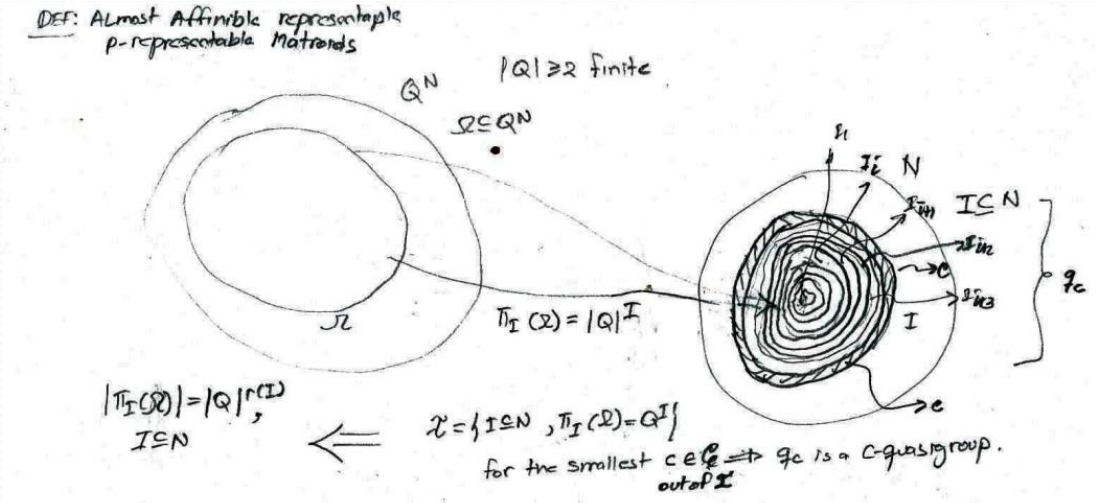
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

Almost Affine codes & Almost affinely representable matroids.

In [40], a subset Ω of Q^N, $|Q| \geqslant 2$ finite, is called *almost affine code* if the cardinality of every projection $\pi_I(\Omega)$, $I \subset N$, is a power of $|Q|$. The family $\mathcal{I} = \{I \subset N; \pi_I(\Omega) = Q^I\}$ 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 $|\pi_I(\Omega)| = |Q|^{r(I)}$, $I \subset N$, 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.

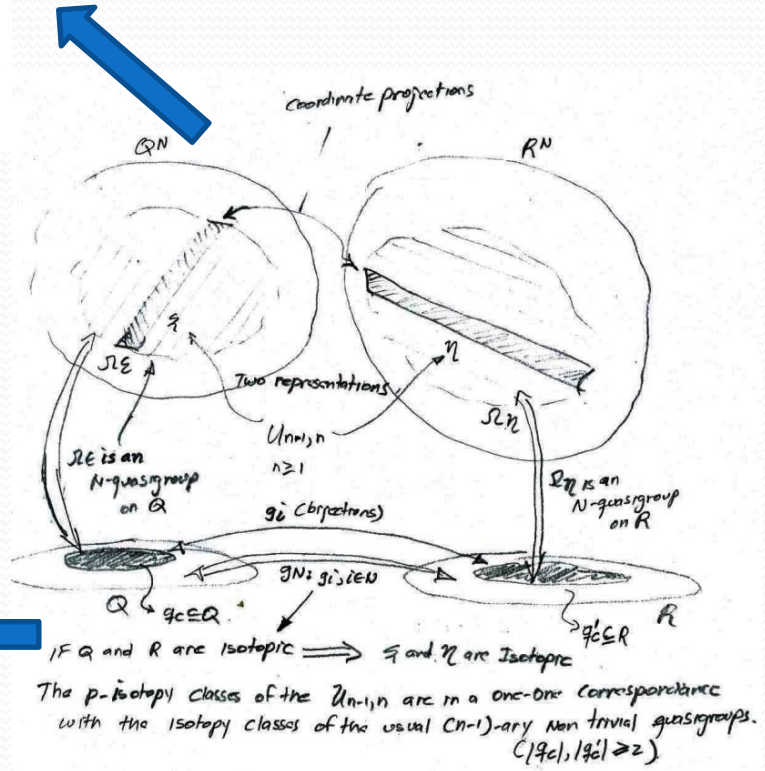


Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Expansion of the the example 1.2

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 $\Omega_\xi \subset Q^N$ and $\Omega_\eta \subset R^N$ 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 $g_i : Q \to R$, $i \in N$, such that the composed mapping

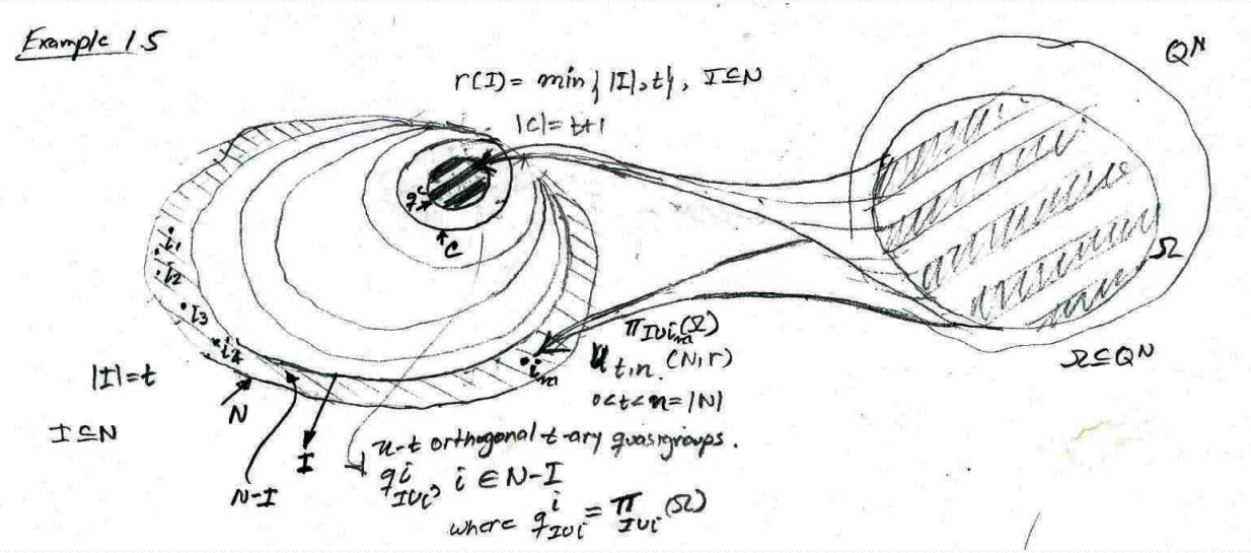


g_N is a bijection between Ω_ξ and Ω_η, then ξ and η are obviously p-isotopic. But it is not difficult to reverse the assertion, namely, if ξ and η are p-isotopic then every p-isotopy must have the composed form g_N for some bijections g_i, $i \in N$. Hence, the p-isotopy classes of the p-representations 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.

Partition representable matroids - Analysis of paper:

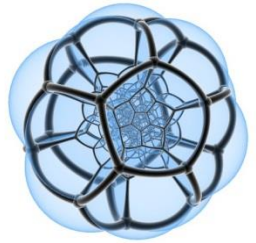
Matroid representations by Partitions by Frantisek Matus

Example 1.5. Let (N,r) be the uniform matroid $U_{t,n}$ where $0<t<n=|N|$ and $r(I)=\min\{|I|,t\}$, $I\subset N$. A p-representation of $U_{t,n}$ is nothing else but a set $\Omega\subset Q^N$ 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 $q^i_{I\cup i}$, $i\in N-I$, where $q_{I\cup i}=\pi_{I\cup i}(\Omega)$. (The orthogonality can be defined by demanding injectiveness of the mapping $x_I\mapsto(\pi_{I\cap J}(x_I),(q^j_{I\cup j}(x_I))_{j\in J-I})$ for every $J\subset N$, $|J|=t$.) 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',



Partition representable matroids - Analysis of paper:

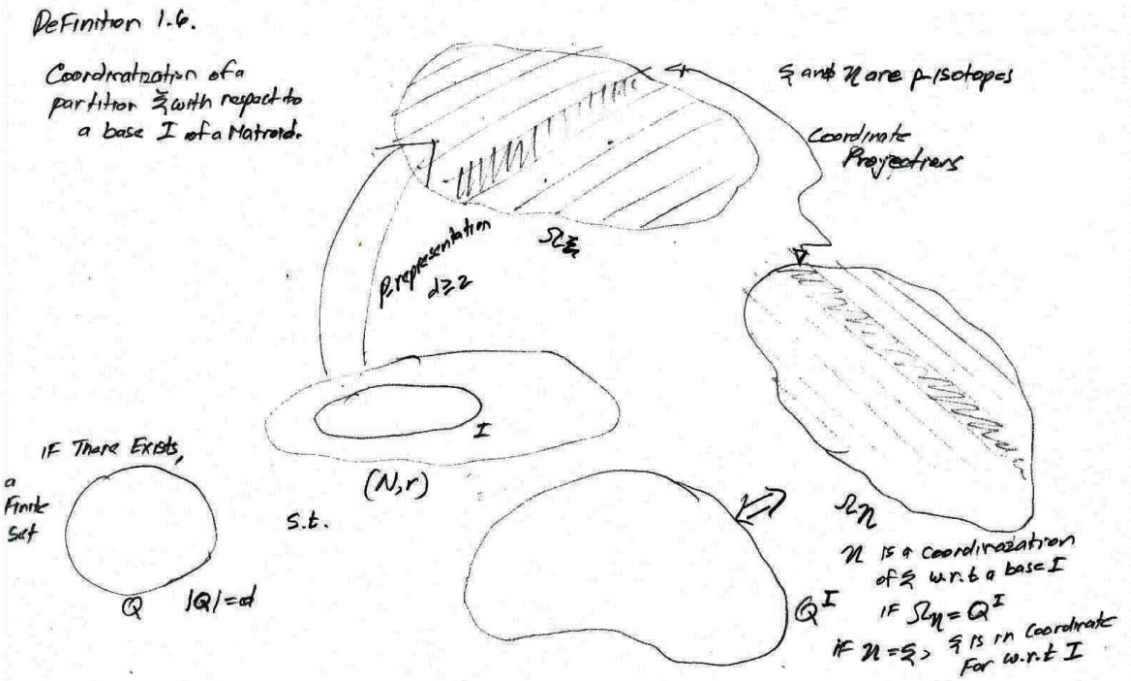
Matroid representations by Partitions by Frantisek Matus



Essential concepts involved in the Partition Representation of Matroids

P-isotope Coordinatization

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*.



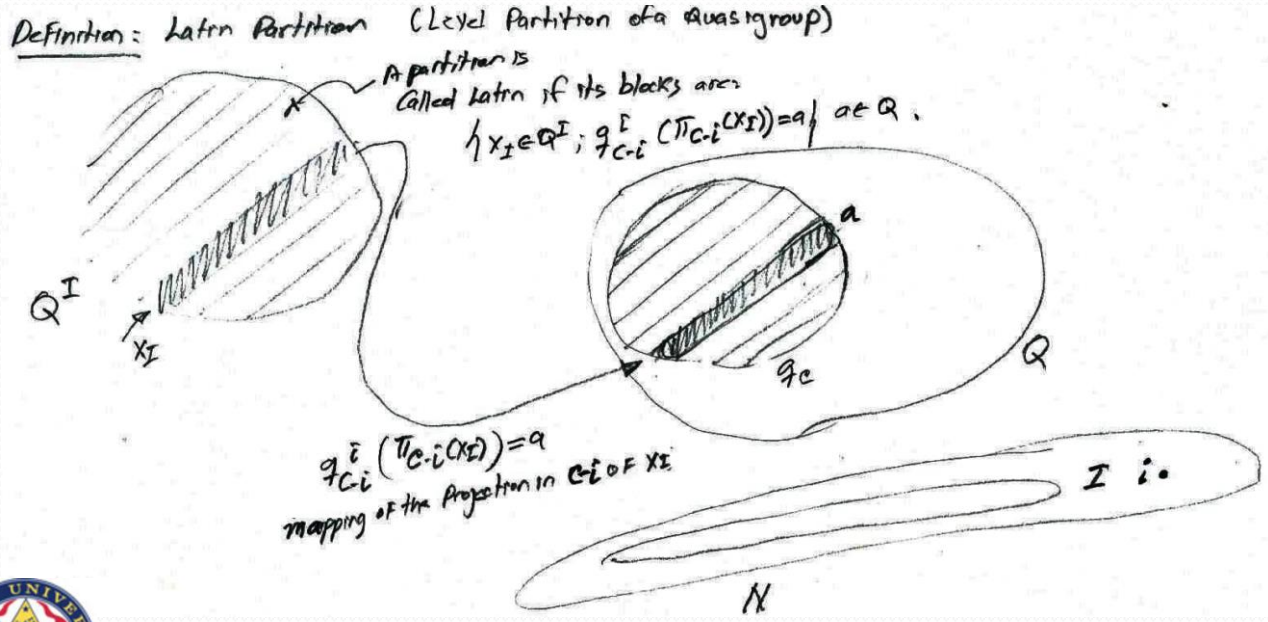
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

Latin Partitions (Level partitions of Quasigroups)

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 $\{x_I \in Q^I; \mathrm{q}^i_{C-i}(\pi_{C-i}(x_I)) = a\}$, $a \in Q$, where q_C is a C-quasigroup on Q, $i \notin I$, and $i \in C \subset i \cup I$. We will use equivalently also the term *level partition of a quasigroup*. Latin partitions are obviously uniform.



Partition representable matroids - Analysis of paper:

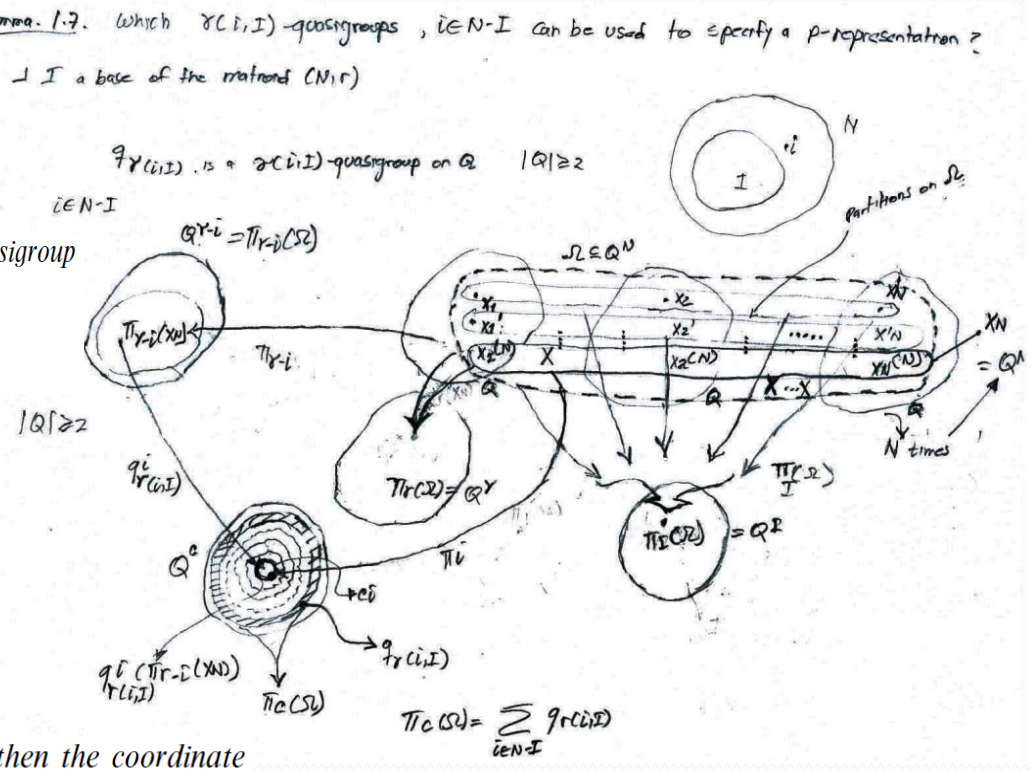
Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

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, $|Q| \geq 2$, and*

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



If $\pi_C(\Omega)$ is a C-quasigroup on Q for every circuit C, $|C - I| \geq 2$, 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).

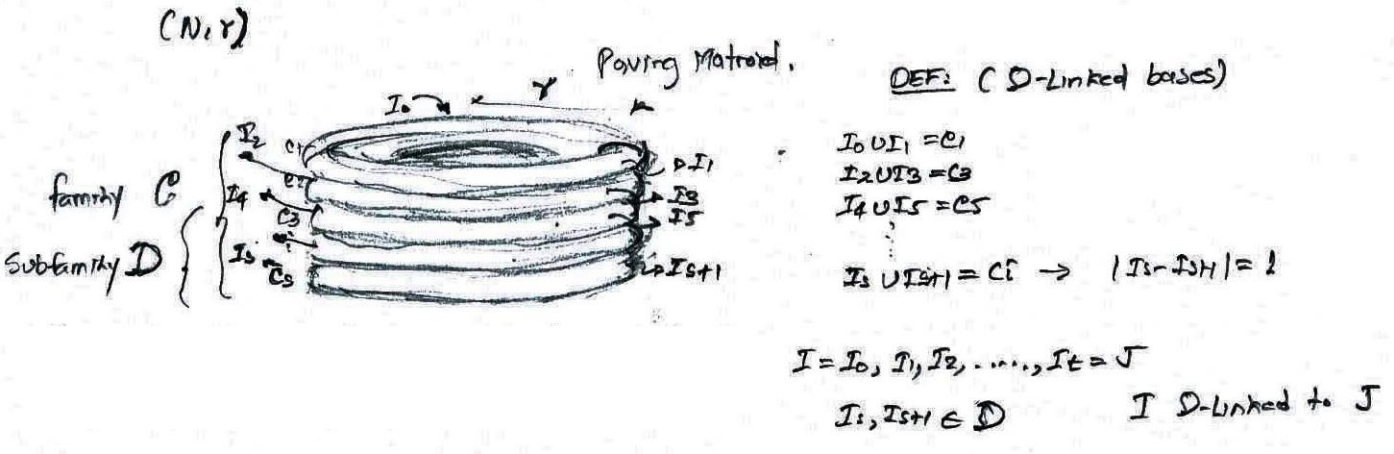
Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

D-Linked bases of a Matroid

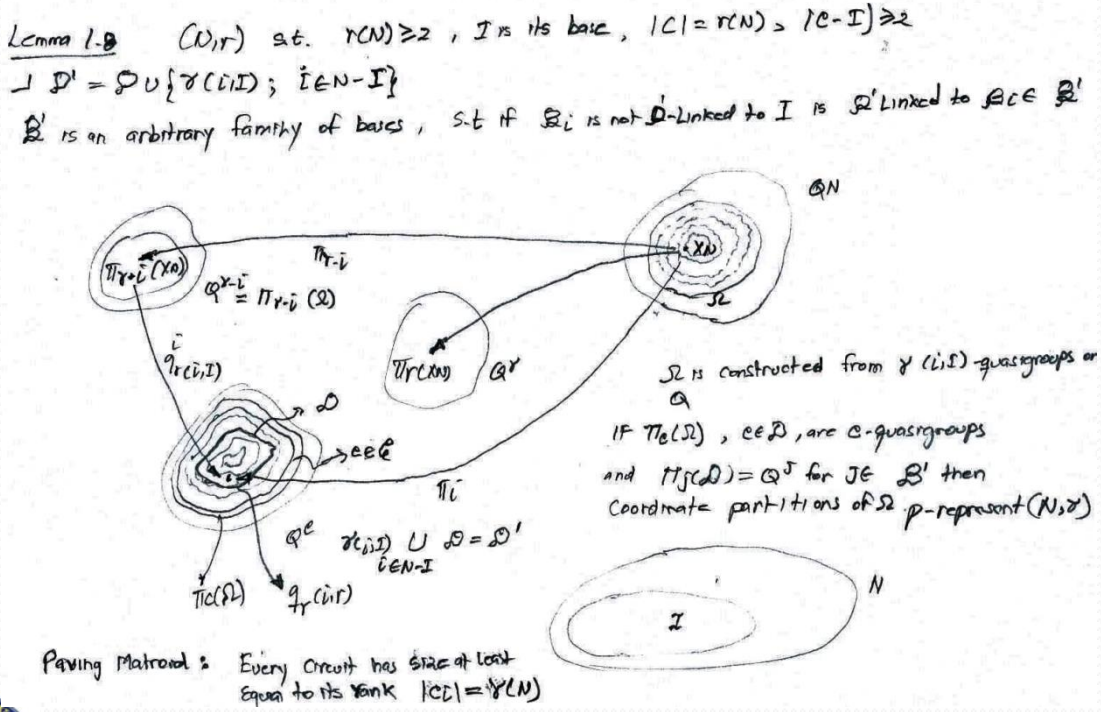
Let $\mathscr{D}$ be a subfamily of the family $\mathscr{C}$ of all circuits of a matroid. Two bases I and J of the matroid are $\mathscr{D}$-*linked* if there exists a sequence of bases $I=I_0, I_1, \ldots, I_t=J$, $t \geqslant 0$, such that $|I_s - I_{s+1}| = 1$ and the unique circuit contained in the union of I_s and I_{s+1} belongs to $\mathscr{D}$, $0 \leqslant s < t$. To be linked is a relation of equivalence.



Partition representable matroids - Analysis of paper:

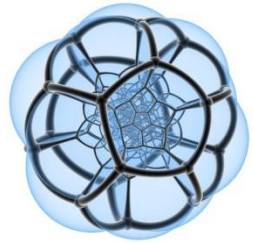
Matroid representations by Partitions by Frantisek Matus

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



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus



Essential concepts involved in the Partition Representation of Matroids

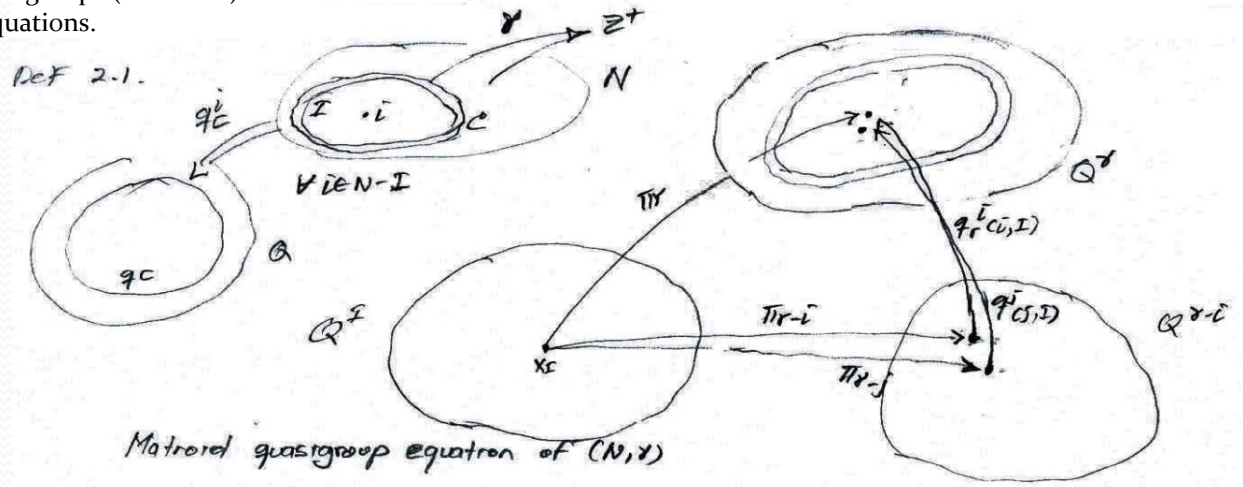
Matroid Quasigroup Equations

Definition 2.1. Let (N,r) be a matroid and Q a nonempty set. A family of C-quasigroups 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 $x_I \in Q^I$

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

where $y_{C-i} = (y_j)_{j \in C-i}$ has the coordinates $y_j = q^j_{\gamma(j,I)}(\pi_{\gamma(j,I)-j}(x_I))$ 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).

The unknowns in these equations are quasigroups (functions) which after substitutions of their arguments satisfy ordinary quasigroup equations.



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

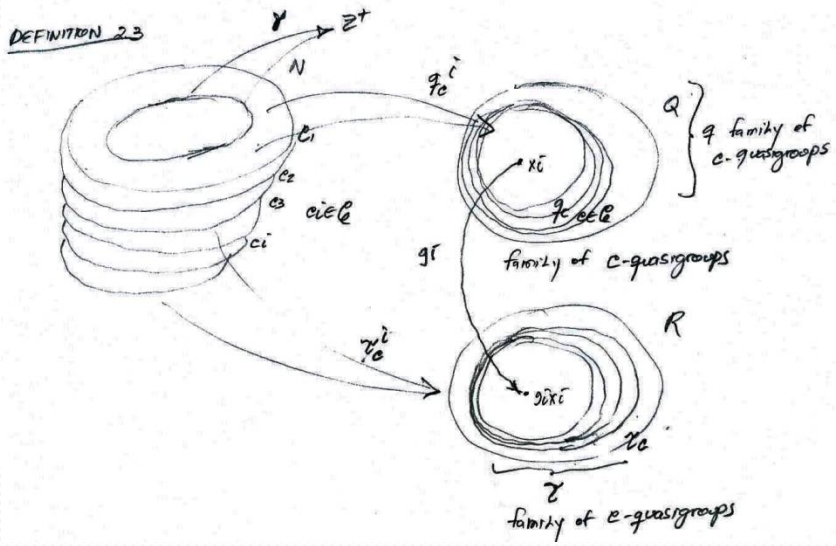
Essential concepts involved in the Partition Representation of Matroids

Simulateneously Isotopic family of C-quasigroups of a Matroid:

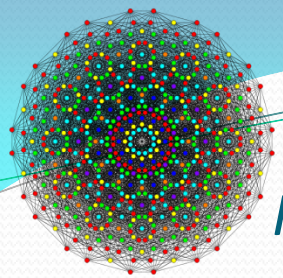
Definition 2.3. Let (N, r) be a matroid with the collection of circuits $\mathscr{C}$. A family $(\mathfrak{q}_C)_{C \in \mathscr{C}}$ of C-quasigroups on a set Q is said to be *simultaneously isotopic* with a family $(\mathfrak{r}_C)_{C \in \mathscr{C}}$ of C-quasigroups on a set R if there exist bijections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

It is a matter of easy technicalities to see that if a family $(\mathfrak{q}_C)_{C \in \mathscr{C}}$ solves the matroid quasigroup equations then its every 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).*



Adaptive Signal Processing and Information Theory Research Group
Drexel University , Philadelphia , Pennsylvania, summer 2013



Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

Necessary and sufficient condition for a Matroid to be P-representable

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 '$(q_C)_{C \in \mathscr{C}}$ 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,

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

Generalized Associativity of Quasigroups

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 $\alpha, \beta, \gamma, \delta, \varepsilon$ of Q such that

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

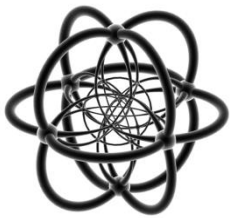
is valid for all $x, y, z \in Q$.

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, unique up to isomorphisms, and eight permutations $\alpha, \beta, \gamma, \delta, \hat{\alpha}, \hat{\beta}, \hat{\gamma}$ and $\hat{\delta}$ of Q such that

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

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus



Essential concepts involved in the Partition Representation of Matroids

General Distributivity of Quasigroups

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. [1,2,24]. 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:

$$y \circledcirc z = \hat{\alpha}^{-1}(\beta(y) \circ \gamma(z)),$$

$$x \circledast y = \phi(\alpha(x) \bigstar \hat{\alpha}(y)), \qquad x \circledcirc y = \hat{\beta}^{-1}(\alpha(x) \square \beta(y)),$$

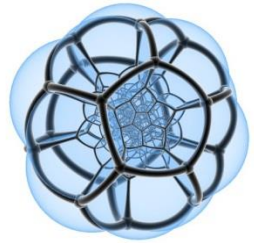
$$x \circledast y = \phi(\hat{\beta}(x) * \hat{\gamma}(y)), \qquad x \circledcirc z = \hat{\gamma}^{-1}(\alpha(x) \diamond \gamma(z)),$$

constructed by use of arbitrary seven permutations $\alpha, \beta, \gamma, \hat{\alpha}, \hat{\beta}, \hat{\gamma}$ 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.*

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus



Essential concepts involved in the Partition Representation of Matroids
Non-p-representable matroids

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

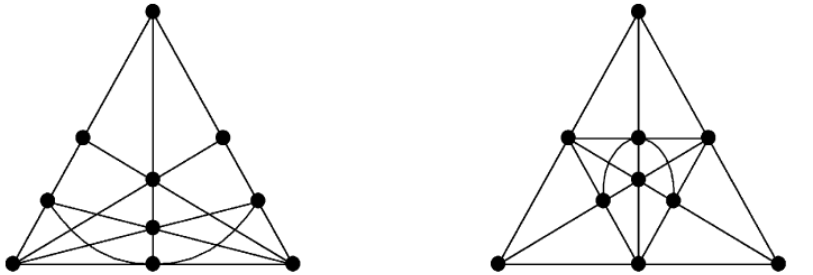


Fig. 7. Two examples of non-p-representable matroids.

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

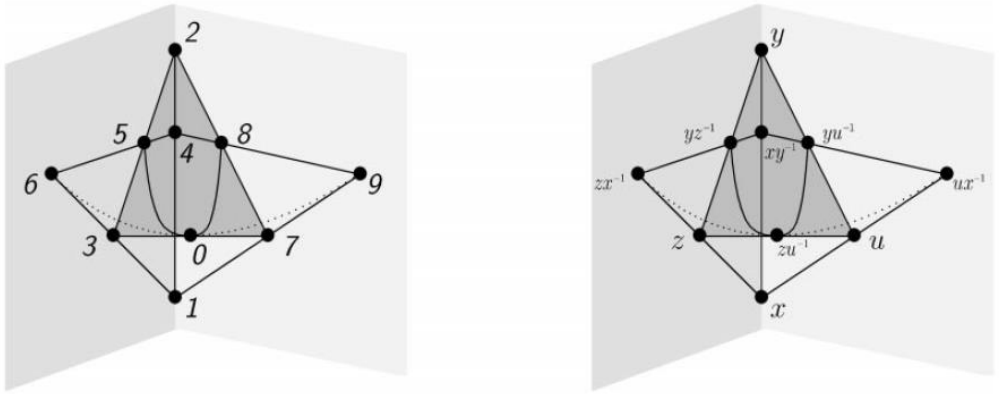


Fig. 9. NonDesargues matroids are non-p-representable.

Partition representable matroids - Analysis of paper:

Matroid representations by Partitions by Frantisek Matus

Essential concepts involved in the Partition Representation of Matroids

Non-p-representable matroids

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* $\mathbb{Z}_n^m, m \geqslant 1$.

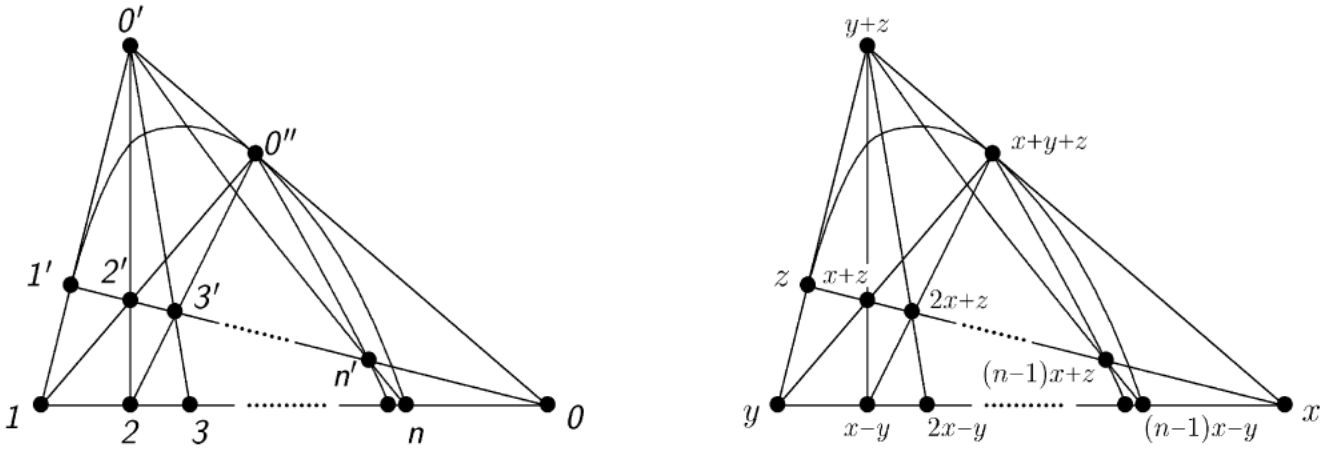


Fig. 10. P-representation of L_n, n prime.

References:

[1] J. Aczél, Lectures on Functional Equations and their Applications, Academic Press, New York, 1966.
[2] J. Aczél, Functional Equations: History, Applications and Theory, D. Reidel Publ. Company, Dordrecht, Boston, Lancaster, 1984.
[3] J. Aczél, V.D. Belousov, M. Hosszú, Generalized associativity and bisymmetry on quasigroups, Acta Math. Acad. Sci. Hungaricae 11 (1960) 127–136.
[4] M. Aigner, Combinatorial Theory, Springer, Berlin, 1979.
[5] A. Beimel, B. Chor, Universally ideal secret-sharing schemes, IEEE Trans. Inform. Theory 40 (1994) 786–794.
[6] V.D. Belousov, Systems of quasigroups with generalized identities, Russian Math. Surveys 20 (1965) 73–143.
[7] G.R. Blakley, G.A. Kabatianski, Generalized ideal secret-sharing schemes and matroids, Problems Inform. Transmission 33 (1997) 277–284.
[8] E.F. Brickell, D.M. Davenport, On the classification of ideal secret-sharing schemes, J. Cryptol. 4 (1991) 123–134.
[9] T. Brylawski, Intersection theory for embeddings of matroids into uniform geometries, Stud. Appl. Math. 61 (1979) 211–244.
[10] T. Brylawski, D. Kelly, Matroids and Combinatorial Geometries, Carolina Lecture Series, Department of Mathematics, Univ. of North Carolina at Chapel Hill, 1980.
[11] R.H. Bruck, A Survey of Binary Systems, Springer, Berlin, 1966.
[12] O. Chein, Moufang loops of small order, Mem. Amer. Math. Soc. 13 (1) (1978) 197.
[13] L. Csirmaz, The dealer's random bits in perfect secret-sharing schemes, Studia Scient. Math. Hungarica 32 (1996) 429–437.

References:

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

[15] J. Dénes, A.D. Keedwell, Latin Squares: New Developments in the Theory and Applications, North-Holland, Amsterdam, 1991.

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

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

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

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

[20] A.W. Ingleton, Representation of matroids, in: D.J.A. Welsh (Eds.), Combinatorial Mathematics and its Applications. Academic Press, London, 1971, pp. 149–169.

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

[22] W.-A. Jackson, K.M. Martin, Combinatorial models for perfect secret sharing schemes, J. Combin. Math. Combin. Comput. (1998), in press.

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

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

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

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

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

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

References:

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

[30] M. Liu, Z. Zhan, Ideal homomorphic secret sharing schemes over cyclic groups, Science in China, Ser. E, Vol. 41, No. 6; Beijing: Science in China Press, pp. 650–660, December 1998.

[31] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.

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

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

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

[35] F. Matúš, Conditional independence structures examined via minors, The Ann. Math. AI 21 (1997) 99–128.

[36] F. Matúš, Conditional independences among four random variables III, Combin. Probab. Comput. 8 (1999) 1–8.

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

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

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

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

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

References:

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

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

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

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

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

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

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