

Algebraic Matroids containing Fano and Non Fano minors as restrictions which are not partition representable



By Alexander Erick Trofimoff
Graduate Research Assistant
PhD program Drexel U.
ECE dept Summer 2016

Matroid Representation Theory: Partition representable Matroid



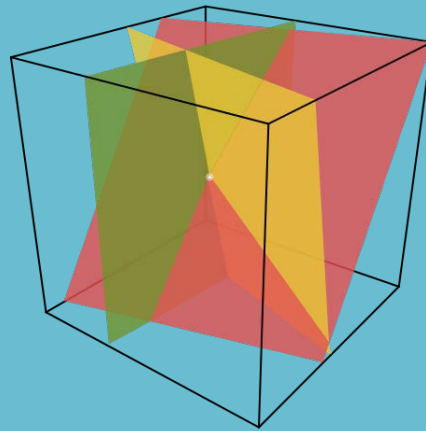
Cryptology: Secret-sharing matroid



Coding Theory: Almost affinely representable matroid

Cryptology: Secret-sharing matroid

Let $A = (a_{ie}: i \in Z, e \in E)$ be a matrix with entries from some finite set S , and let M be a matroid with element set E . Then A is a secret-sharing matrix for M iff $\forall X \subseteq E$, the submatrix $(a_{ie}: i \in Z, e \in X)$ has precisely $|S|^{r_k(X)}$ distinct rows, where $r_k(X)$ denotes the rank of X in M .



Ex: *Blakley's scheme in 3 dimensions:*
each share is a plane, and the secret is the point at which three shares intersect. Two shares are insufficient to determine the secret, although they do provide enough information to narrow it down to the line where both planes intersect.

Coding Theory: Almost affinely representable matroid

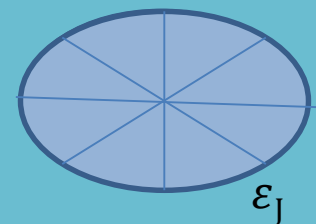
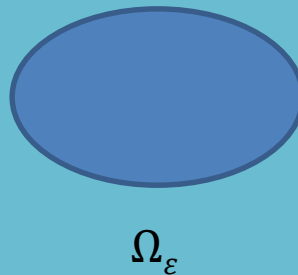
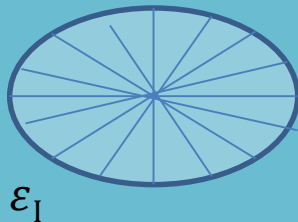
Let F be an m -dimensional vector space over a finite field F_q and let C be a linear subspace of the nm -dimensional vector space F^n . Then C is an almost affine code of length n over the alphabet F iff for all subsets $X \subseteq \{1;2; : : : ;n\}$ the dimension of the vector space C_X is divisible by m .

Ex: $F := (F_3)^2$, then the row space of the matrix is an almost affine code of length 9 over F .

$4 \div 2$				$8 \div 2$				$18 \div 2$			
10	10	00	10	00	10	10	10	00			
01	01	00	01	00	01	01	01	00			
00	00	00	10	10	21	01	10	10			
00	00	00	02	01	20	12	02	01			
00	10	10	01	00	01	00	11	10			
00	01	01	21	00	21	00	10	01			

Partition representable Matroid

Let $(N; r)$ be a matroid, ground set N , rank function r , it is Partition p -representable of degree $d \geq 2$ if \exists partitions $\varepsilon_i; i \in N$, of a finite set Ω , $|\Omega| = d^{r(N)}$, s.t.
 the meet-partition $\varepsilon_I = \bigwedge_{i \in I} \varepsilon_i$
 has $d^{r(I)}$ blocks of cardinality $d^{r(N) - r(I)}$;
 $\forall I \subset N$.

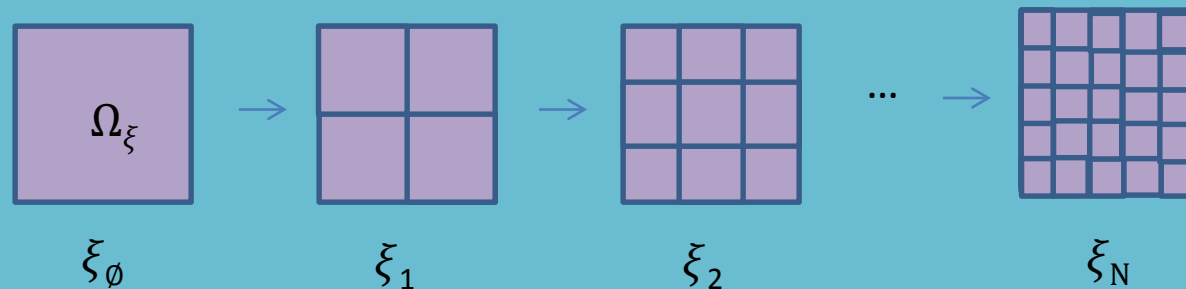


Meet partitions of a Matroid

A partition with all blocks having the same number of elements will be termed uniform.

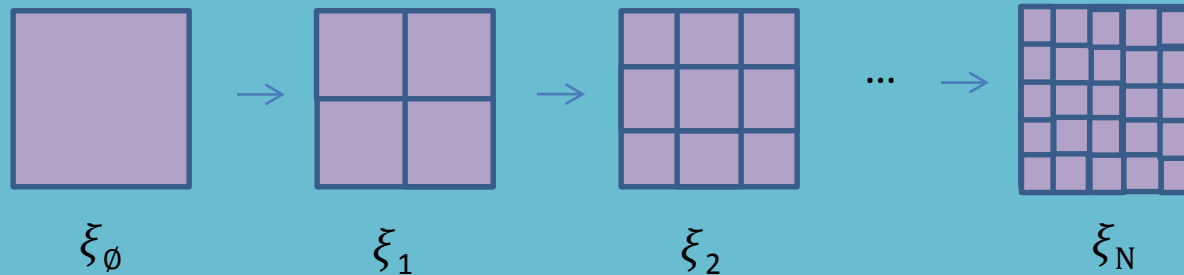
All meet-partitions of a p -representation ξ are uniform:

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

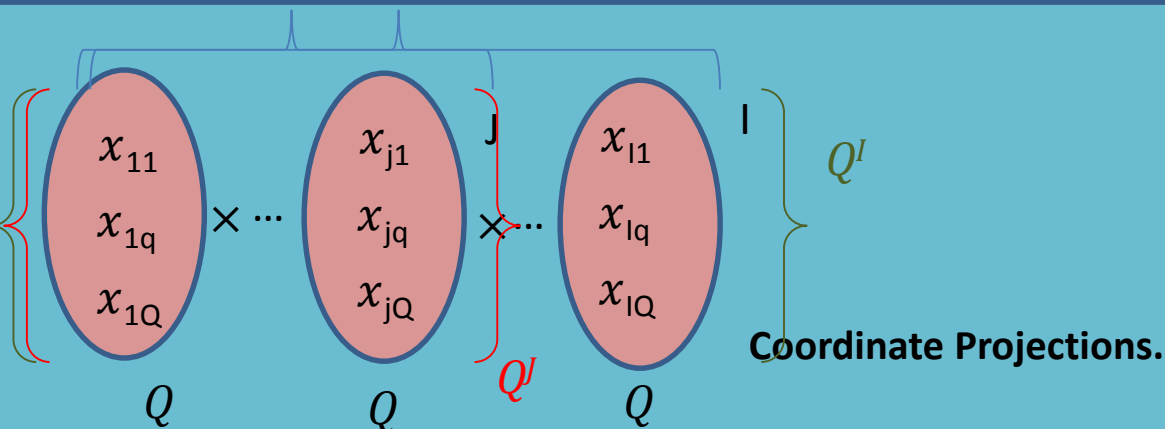


P- representations of a matroid

$\xi_I = (\xi_i) = (\xi_1, \xi_2, \dots, \xi_i)$, $i \in N$ will be called p -representation of the matroid of degree d .



A.W. Ingleton Algebraic Non linear 11 elements Matroid



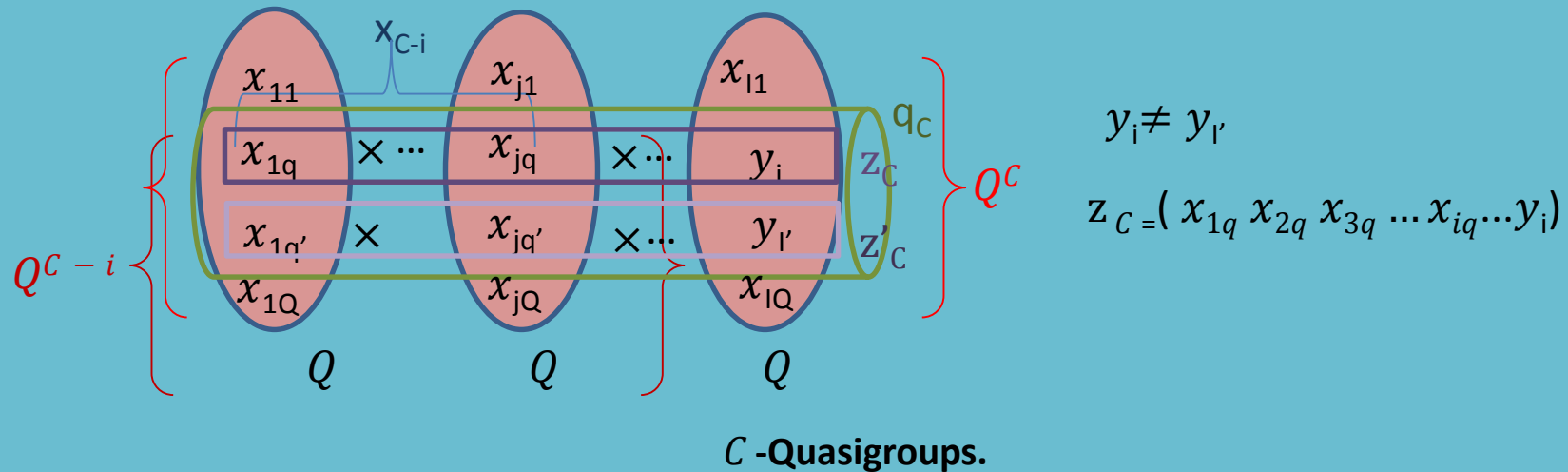
$Q \neq \emptyset$; and I are two sets, elements of Q^I will be denoted by $x_I = (x_i)_{i \in I}$ and the coordinate projection of $x_I \in Q^I$ on Q^J ; $J \subset I$, by $\pi_J(x_I) = (x_i)_{i \in J}$; Q^\emptyset ; is a fixed one-element set.
Subsets S of Q^I will be projected similarly $\pi_J(S) = \{\pi_J(x^I) \in Q^J ; x^I \in S\}$.

Ex:

$$\pi_J(x_I) = \pi_J((x_{1k} x_{2k} x_{3k} \dots x_{gk} \dots x_{jk} \dots x_{lk})) = (x_{1k} x_{2k} x_{3k} \dots x_{jk})$$

$$\pi_g(x_I) = \pi_g((x_{1k} x_{2k} x_{3k} \dots x_{gk} \dots x_{jk} \dots x_{lk})) = (x_{1k} x_{2k} x_{3k} \dots x_{gk})$$

A.W. Ingleton Algebraic Non linear 11 elements Matroid



Let the set $C \neq \emptyset$ then a C -quasigroup on $Q \neq \emptyset$ will be a special subset q_C of Q^C defined as:

$$\forall i \in C,$$

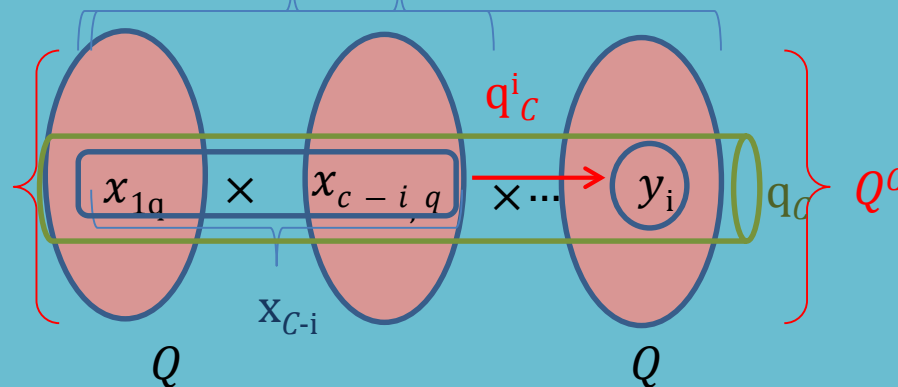
$\forall x_{C-i} \in Q^{C-i} \exists$ a unique $y_i \in Q$ s.t. the C -tuple z_C composed from $\pi_{C-i}(z_C) = x_{C-i}$ and $\pi_i(z_C) = y_i$ belongs to q_C .

$$z_C = ((x_{C-i})(y_i)) \in q_C \subset Q^C = \{(x_{1k} x_{2k} x_{3k} \dots x_{ck}) : x_{lk} \in Q\}$$

Parastrophic quasigroups

$$\begin{aligned} q_C^i &: Q^{C-i} \rightarrow Q \\ (x_{C-i}) &\mapsto (y_i) \\ \pi_{C-i}(x_C) &\mapsto \pi_i(x_C): \end{aligned}$$

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



$q_C^i: Q^{C-i} \rightarrow Q$ are **parastrophic quasigroups** on Q (of arity $|C| - 1$)

Coordinate Partitions of Ω .

Ex.

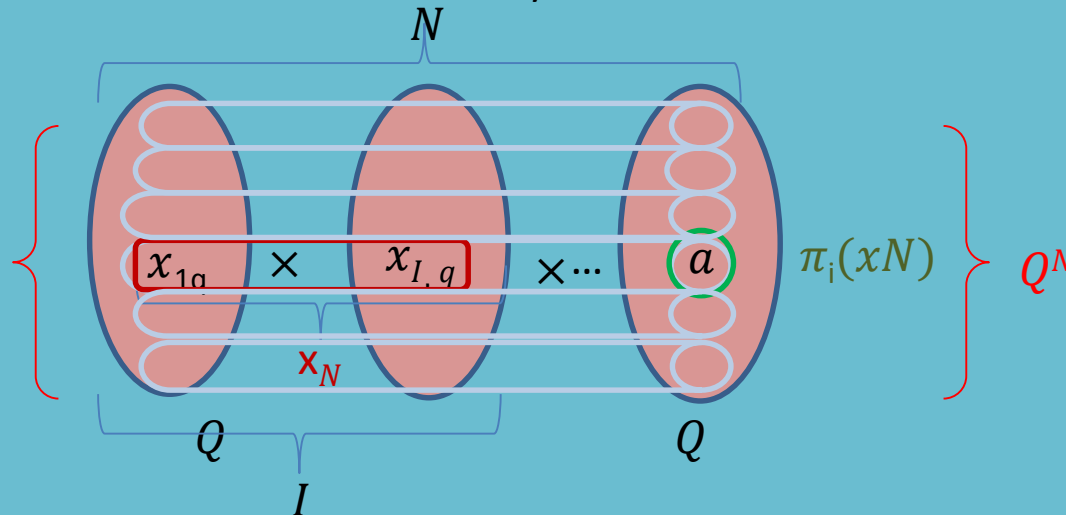
Let $(N; r)$ be the free matroid on N ($r(I) = |I|$; $I \subset N$) and Q a finite set, $|Q| = d \geq 2$.

We set $\Omega = Q^N$ and ξ_i ; $i \in N$, be partition of Ω with the blocks $\{x_N \in \Omega; \pi_i(x_N) = a\}$; $a \in Q$.

The blocks are i^{th} parallel coordinate layers of Q^N .

Hence $\xi = (\xi_i)_{i \in N}$ is a p -representation of the free matroid of degree d .

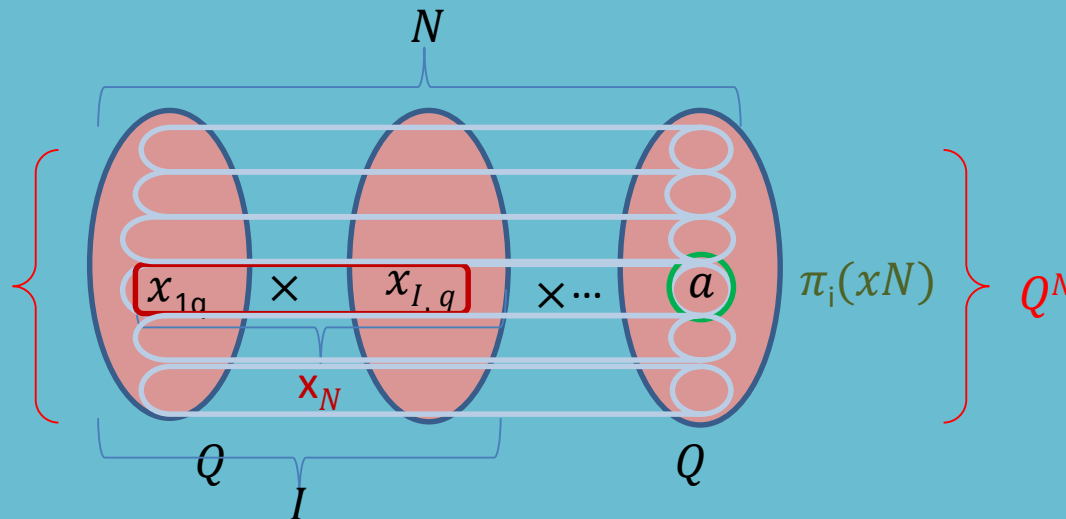
blocks of ξ are intersections of the coordinate layers with Ω , this is a **coordinate partition of Ω**



Coordinate Partitions of Ω .

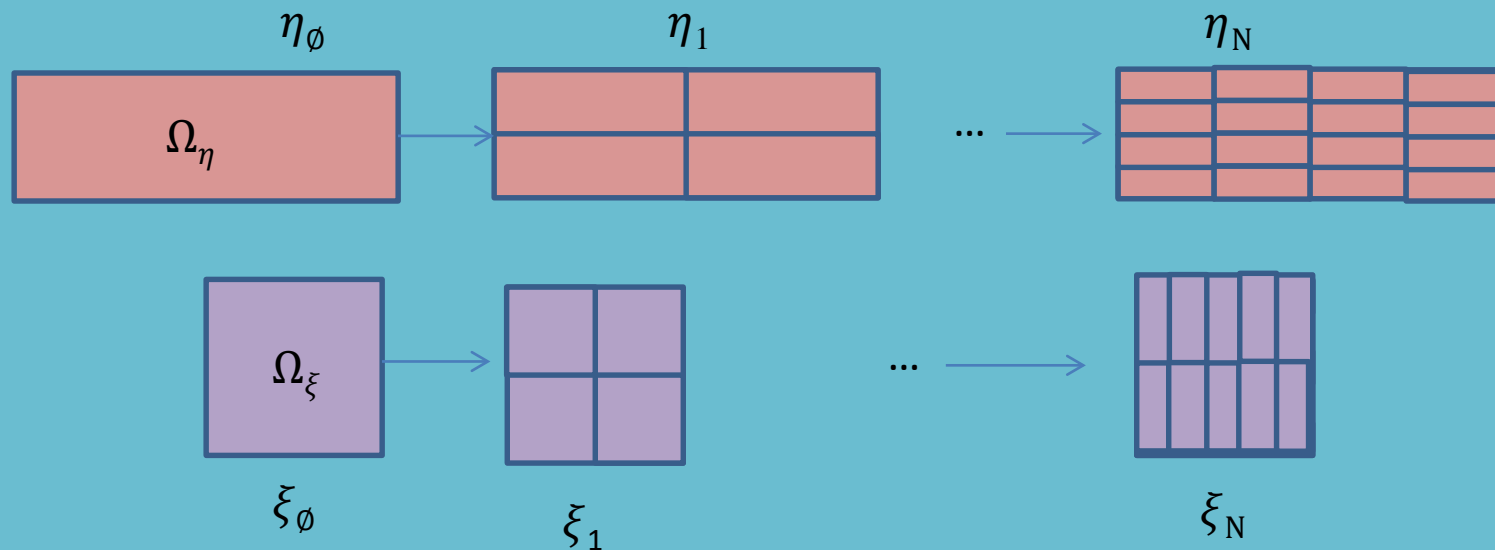
The system of all coordinate partitions
of any N –quasigroup $= q_N \subset Q^N$ on Q is
 p -representation matroid $U_{n-1, n}$
of degree d .

The ground set is N with $|N|=n \geq 1$ and rank function $r(I) = \min\{|I|; n - 1\}$;
 $I \subset N$; the only circuit of the matroid is $C = N$.



P- isotopic representations

Two p -representations $= (\xi_i), i \in N$ and $(\eta_i), i \in N$ 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 $f\xi_i = \eta_i \forall i \in N$

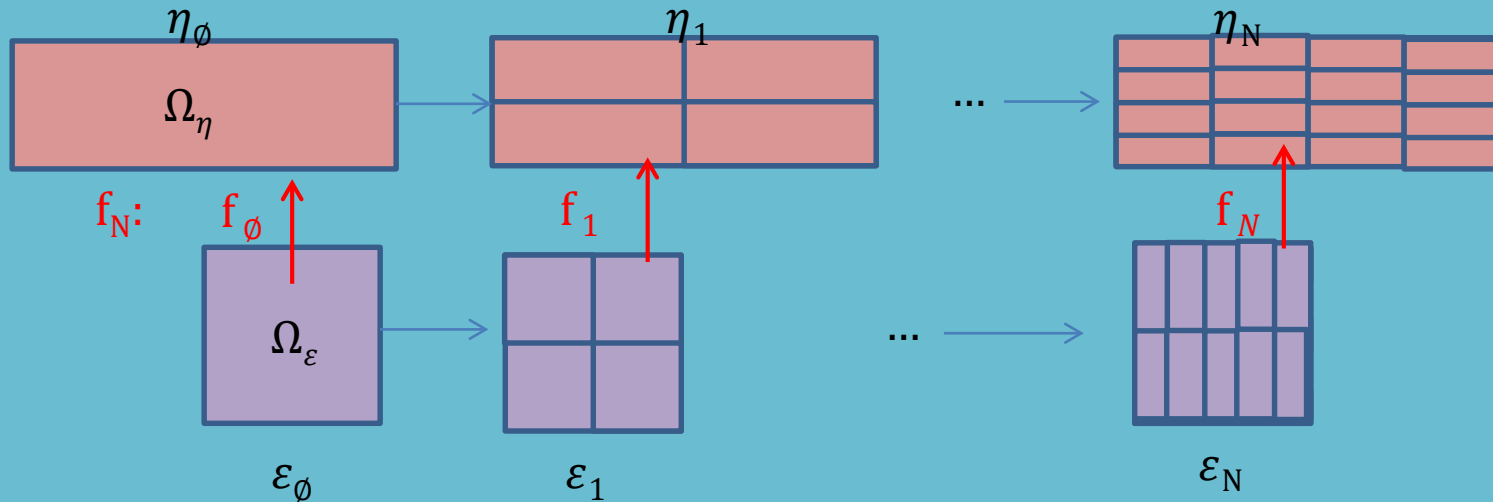


Coordinate Partitions of Ω_η .

If Q is a set of cardinality d and
 $f_i : \Omega_\varepsilon \rightarrow Q$ is a function distinguishing and constant on the blocks of ε_i ; $i \in N$,
 then the composed function f_N defined by $f_N(\omega) = (f_i(\omega))_{i \in N}$; $\omega \in \Omega_\varepsilon$,
 maps injectively into Q^N .

Let $\Omega_\eta = f_N(\Omega_\varepsilon)$ be the image of Ω_ε
 and $f_N \varepsilon_i = \eta_i$ be the partitions of Ω_η .
 Obviously, $\eta = (\eta_i)_{i \in N}$ is a p -isotope of ε .

Hence, $\pi_i(\Omega_\eta) = Q^i$, $\forall i \in N$, π_i is a coordinate partition.



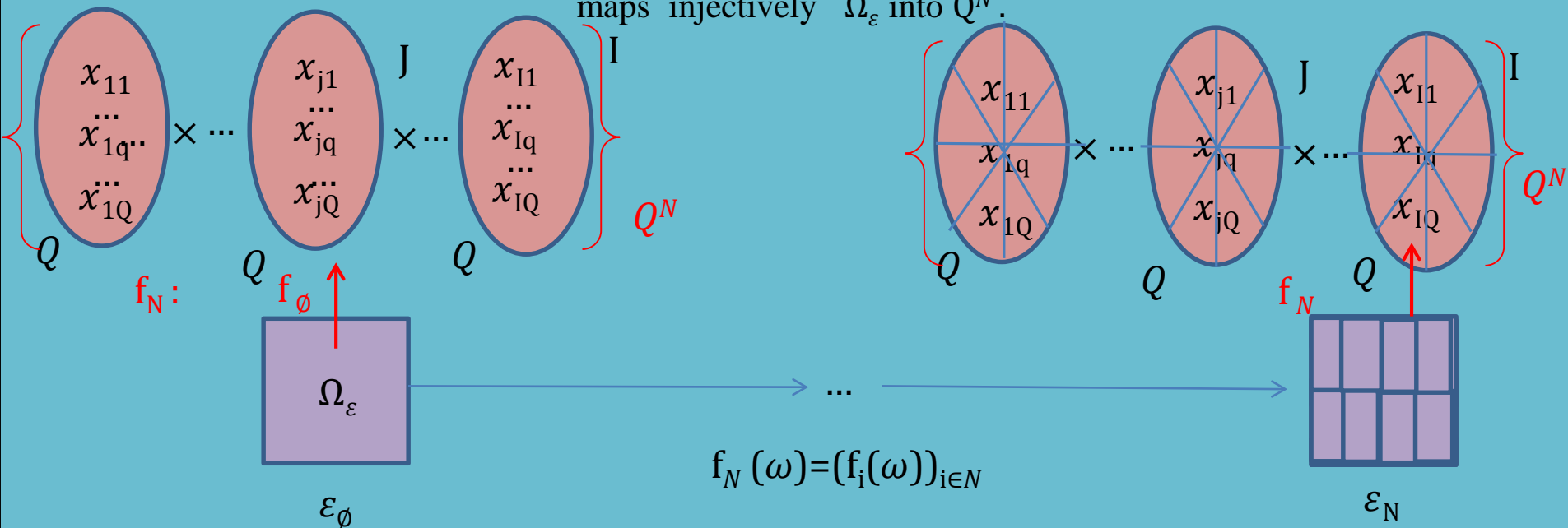
A.W. Ingleton Algebraic Non linear 11 elements Matroid

A p -representation of a matroid is p -isotopic to the p -representation which lives on a subset of a Cartesian product

Let ε be a p -representation of a matroid of degree d living on Ω_ε .

If Q is a set of the cardinality d and $f_i : \Omega_\varepsilon \rightarrow Q$ is a function distinguishing and constant on the blocks of ε_i ; $i \in N$, then the composed function f_N defined by

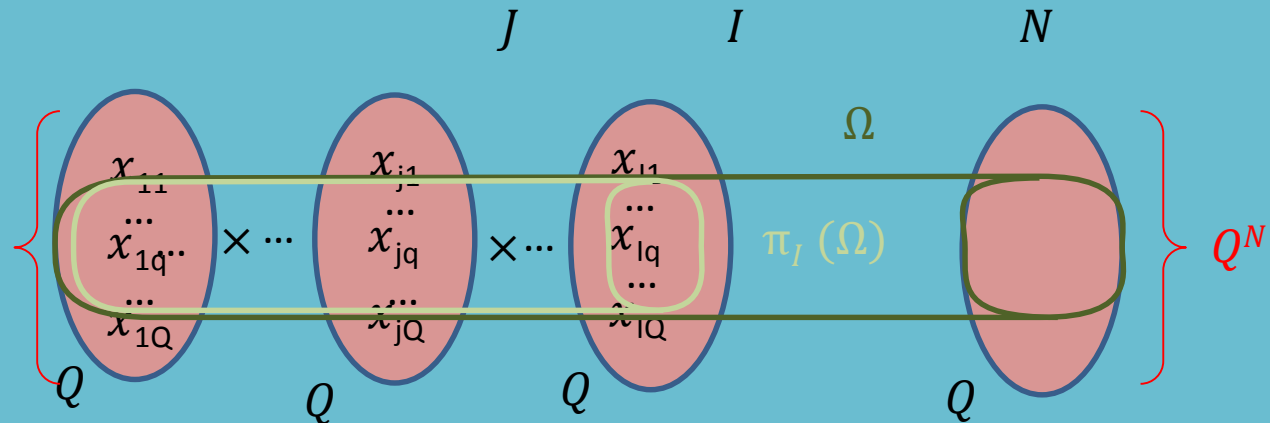
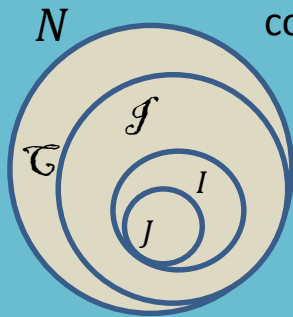
$f_N(\omega) = (f_i(\omega))_{i \in N}$; $\omega \in \Omega_\varepsilon$,
maps injectively Ω_ε into Q^N .



Lemma 1.4 of F . Matus

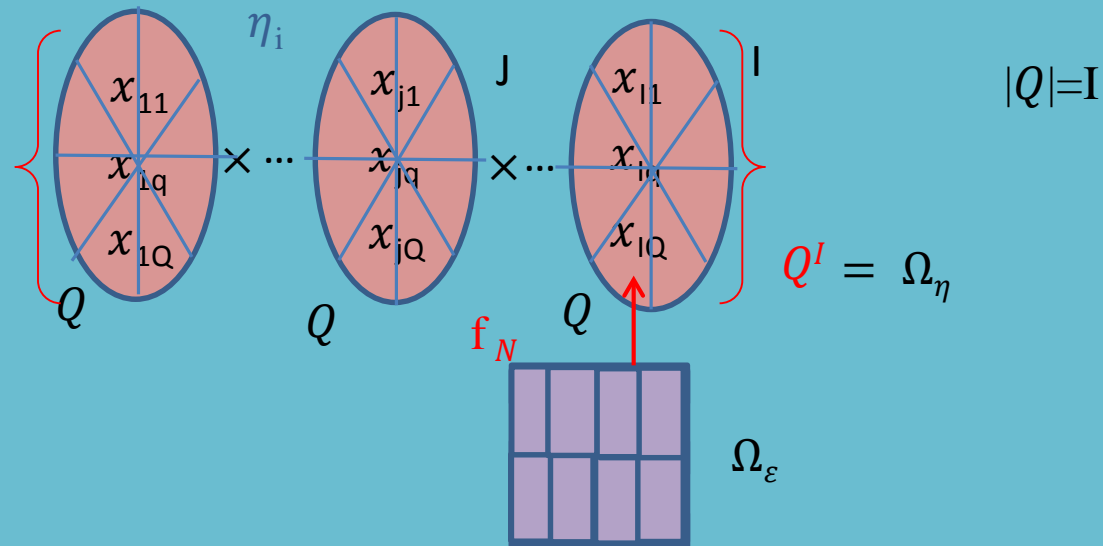
Let N be a finite nonempty set and \mathcal{I} a nonempty hereditary family of subsets of N ($I \in \mathcal{I}$ and $J \subset I$ implies $J \in \mathcal{I}$). Let \mathcal{T} be the family of all inclusion-minimal subsets of N out of \mathcal{I} .

If $\Omega \subset Q^N$; $|Q| \geq 2$ finite; s.t. $\pi_I(\Omega) = QI$ for $I \in \mathcal{I}$ and $\pi_C(\Omega)$ is a C -quasigroup on Q for $C \in \mathcal{T}$ then \mathcal{I} is the family of independent sets of a matroid on N . The coordinate partitions of Ω form a p -representation of the matroid of the degree $|Q|$.



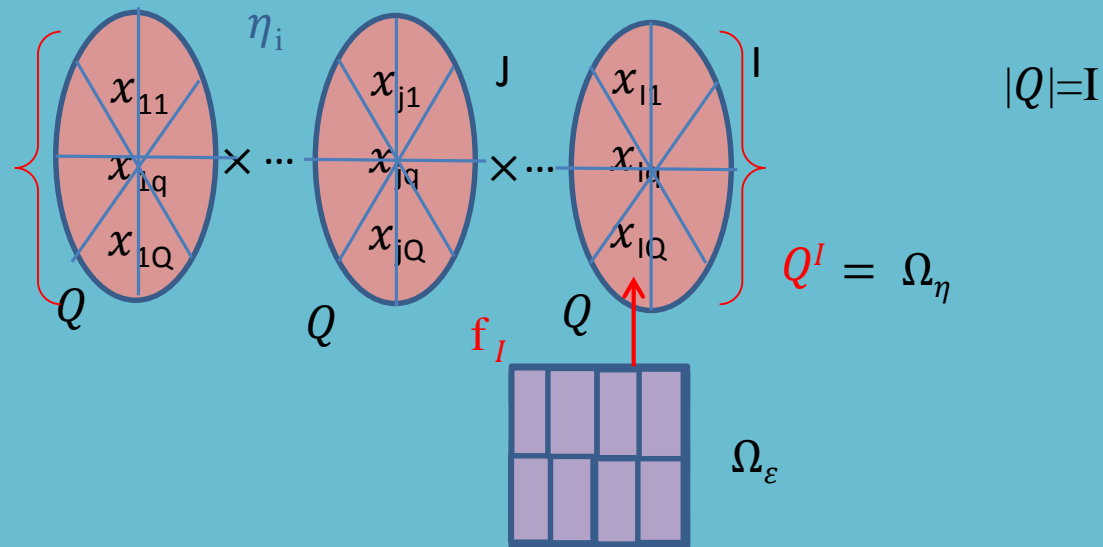
Coordinatizations of p-representations

Let $(N; r)$ be a matroid and ε its p-representation of degree $d \geq 2$ on Ω_ε .
 A p-isotope η of ε living on Ω_η is called coordinatization of ε 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 $\eta = \varepsilon$ here we say that ε is in **the coordinate form**
 w.r.t. I .



Coordinatizations of p -representations

every p -representation 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 $f_I(\omega) = (f_i(\omega))_{i \in I}$; $\omega \in \Omega_\varepsilon$,



A.W. Ingleton Algebraic Non linear 11 elements Matroid

Abstract Algebra Characterization of Quasigroup $(S, *)$

Cayley Table

	a	b	x	s_N
a	s_{11}	s_{21}	b	s_{NN}
b	s_{21}			
y	b			
s_N	s_{N1}			s_{NN}

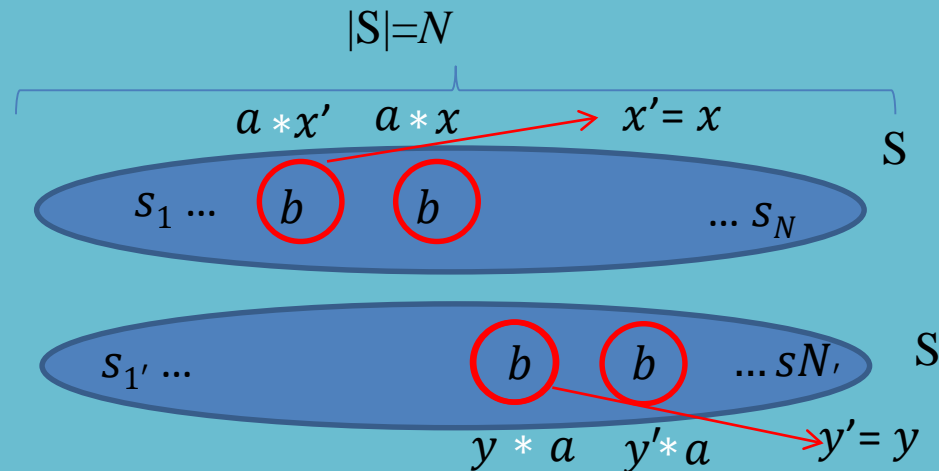
A set S of N **distinct** elements (symbols) is a quasigroup of order N if there is a binary operation $*$ defined on the set s. t. $\forall a, b \in S$ the equation $a * x = b$ and $y * a = b$ each have exactly one solution.

$$s_{ij} = s_i * s_j, s_{ij} \in S$$

$$\forall s_{ij} \exists s_{i'j'} \text{ s.t. } s_{i'j'} = s_{ij}$$

$$s_{ij} = a * x, s_{i'j'} = y * a$$

$$i, j, i', j', ij, i'j' \in \{1, \dots, N\}$$



Latin Squares

A Latin square of order n , $L(n)$, is an arrangement of n symbols (usually the first n positive integers) in an $n \times n$ array where every integer appears exactly once in every row and exactly once in every column.

A **Latin subsquare** of $L(n)$, say $K(m)$ (with $1 \leq m \leq n$), is a subarray which is itself a Latin square.

If m is different from 1 or n , K is called **proper Latin subsquare of L** .

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Latin Square Transversal

Ex. Latin square shown in Fig. has a subsquare of order 2 (an intercalate) at the intersection of rows 2, 3 and columns 1, 4 based on symbols 2 and 3

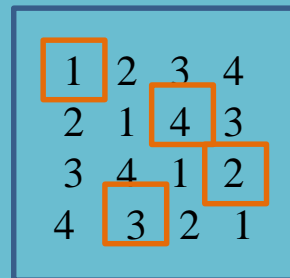
1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Fig. Latin square of order 4 with a transversal and 2×2 subsquare

Latin Square Transversal

A Transversal of a Latin square,
which is a set of n different entries
no pair of which belong to the same row,
column or symbol.

Ex: The set $T=\{(1,1),(2,3),(3,4),(4,2)\}$
is a transversal for the
Latin square given under Fig.



A 4x4 Latin square is shown, enclosed in a blue border. The entries are as follows:

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

The transversal set $T = \{(1,1), (2,3), (3,4), (4,2)\}$ is highlighted with orange boxes around the entries 1, 4, 2, and 3.

A.W. Ingleton Algebraic Non linear 11 elements Matroid

Theorem: The **multiplication table** (unbordered) of a quasigroup is a **Latin square**

Proof.

Let a_1, a_2, \dots, a_N be elements of the quasigroup. Let the Cayley table be (a_{xy}) where entry a_{rc} (r^{th} row and c^{th} column)

is product $a_r a_c$

Since equations $a_r x = b$ and $y a_c = c$

each have exactly one solution,

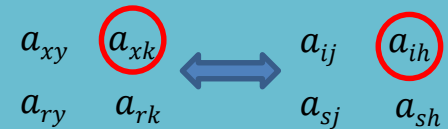
we have each element of the multiplication table occurs exactly once in each row and column.

Thus the Cayley table without the borders represents a Latin square.

	a_1	a_2	a_N
a_1	a_{11}	a_{12}	a_{1N}
a_2	a_{21}	a_{22}	a_{2N}
a_N	a_{N1}	a_{N2}	a_{NN}

Moreover, if the quasigroup is associative, its Cayley table is a Latin square that satisfies a special criterion, quadrangle criterion.

$\forall a_{ij}$ in the set, $a_{xk} = a_{ih}$ whenever $a_{xy} = a_{ij}$, $a_{ry} = a_{sj}$, and $a_{rk} = a_{sh}$.



Universal Algebra Characterization of Quasigroup $(S, *, /, \backslash)$

A **quasigroup** $(S, *, \backslash, /)$ is a type algebra (i.e., a Set S equipped with 3 binary operations) satisfying the identities:

$$y = x * (x \backslash y) ;$$

$$y = x \backslash (x * y) ;$$

$$y = (y / x) * x ;$$

$$y = (y * x) / x .$$

This is a algebraic variety since it is an equationally defined *collection of elements from a single algebra*.

Here left and right division are taken as primitives, (they don't have net effect together with $*$)

.

Universal Algebra Characterization of Loop $(S, *, /, \backslash)$

A **loop** is a quasigroup with an identity element e , s.t.:

$$x * e = x \text{ and } e * x = x \quad \forall x \in Q.$$

It follows that the identity element, e , is unique,
and that every element of Q has a unique left inverse (${}^{-1}x$ or x^{ρ})
and right inverse (x^{-1} or x^{λ})

Since the presence of an identity element is essential,
a loop cannot be empty.

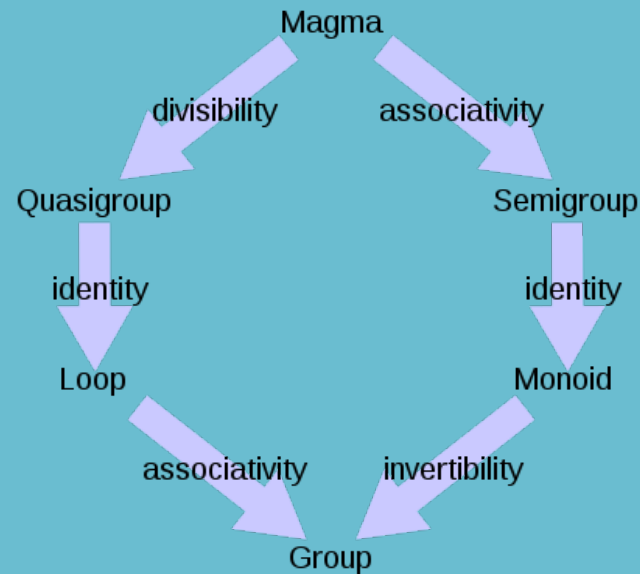
$$\begin{aligned} e &= (x^{-1}) * x = / x * x = * x / x = x * (x^{-1}) \\ x \backslash (x *) &= ({}^{-1}x) * x = x * ({}^{-1}x) = x * (x \backslash) = e. \end{aligned}$$

$$\begin{aligned} e/x &= x^{\lambda} \\ x \backslash e &= x^{\rho} \end{aligned}$$

Algebraic structures between magmas and groups.

Magma (Groupoid) :

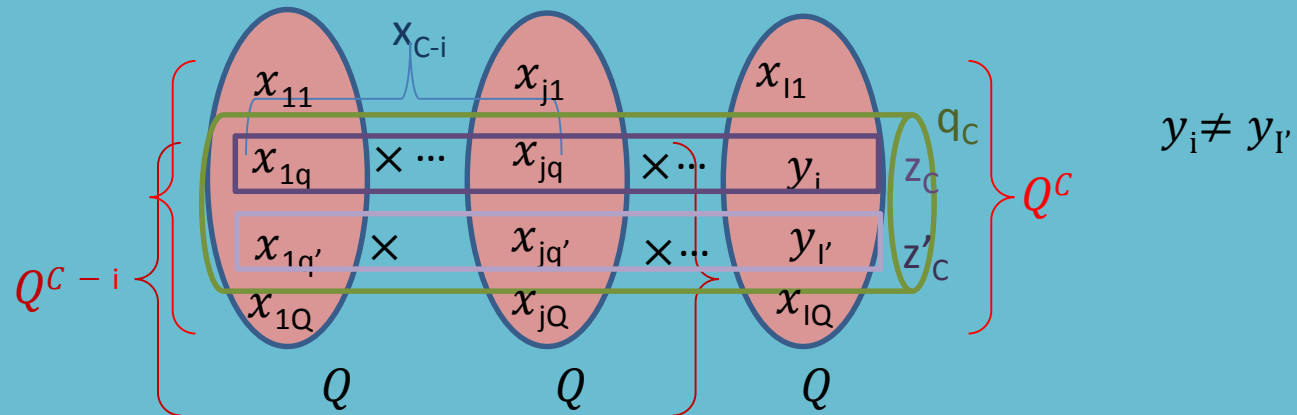
consists of a set, M , equipped with a single binary operation, $M \times M \rightarrow M$.
The binary operation must be closed by definition but no other properties are imposed.



Group: is a set, G , together with an operation \bullet that combines $a, b \in G$ to form $a \bullet b \in G$.
the set and operation, (G, \bullet) , must be closed, associative, has inverse and identity.

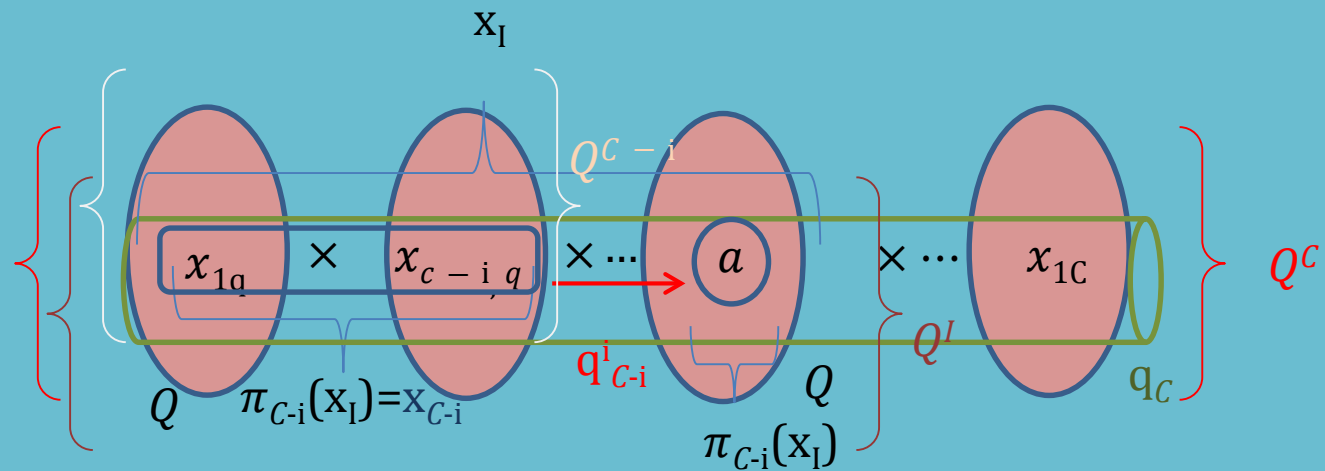
\mathcal{C} -quasigroups

If $\mathcal{C} \neq \emptyset$ then a \mathcal{C} -quasigroup on $Q \neq \emptyset$; will be for us a $q_{\mathcal{C}} \subset Q^{\mathcal{C}}$ s.t.
 $\forall i \in \mathcal{C}$, to $\forall x_{\mathcal{C}-i} \in Q^{\mathcal{C}-i} \exists$ a unique $y_i \in Q$ s.t. the \mathcal{C} -tuple $z_{\mathcal{C}}$ composed from $\pi_{\mathcal{C}-i}(z_{\mathcal{C}}) = x_{\mathcal{C}-i}$ and $\pi_i(z_{\mathcal{C}}) = y_i, z_{\mathcal{C}} \in q_{\mathcal{C}}$.



Latin partition (level partition of a quasigroup)

A partition of Q^I is called a **latin partition** if its blocks can be given as $\{x_I \in Q^I; q_{C-i}^i(\pi_{C-i}(x_I)) = a\}; a \in Q$, where q_C is a C -quasigroup on Q ; $i \notin I$, and $i \in C \subset i \cup I$. Latin partitions are uniform.



Systems of quasigroups with generalized identities.

Let Q be a finite set, Let Λ_o be a the system of all quasigroup operations defined on Q , satisfying **generalized associative law**:

$$A [B (x, y), z] = C [x, D (y, z)] \quad (x, y, z \in Q),$$

A, B may take any value in Λ_o , and C, D may take restricted values in Λ_o , depending on A and B .

Such systems **exist only**
when **$|Q| < 4$** .

Fixing Notation .

Let 's denote Q a **set of elements** .

elements of Q are denoted by lower-case latin letters

$a, b, c, \dots x, y, z, \dots; p, q, r, \dots$.

Binary operations on Q are denoted by capital latin letters $A, B, C, \dots X, Y, Z, \dots; P, \dots$.

Formulas $A(a, b) = c$ means: result of operation

A to a, b in Q , in the given order, is the element c in Q .

Binary operations are also denoted by symbols $\cdot, \circ, \oplus, \dots$

Sets of operations are denoted by capital greek letters: $\Sigma, \Omega, \Phi \dots$

A.W. Ingleton Algebraic Non linear 11 elements Matroid

Essential Universal Algebra Concepts

(free elements, Ω -words and Ω -subwords)

Let M be a non-empty set of elements x, y, z, \dots
the *free elements*, and let Ω be a *set of operations*.

- All free elements are Ω -words,
- If w_1, w_2 are words and $A \in \Omega$, then $w = A(w_1, w_2)$ is a word.
The words w_1 and w_2 are *subwords* of w .

$w = \Phi(W)$, where Φ is the collection of *operations in Ω*
and W for the collection of *free elements*
in M that *actually appear in w* .

Ex: $W = A\{x, B[C(y, z), x]\}$,

then Φ consists of A, B, C and W of x, y, z .

The order of operations acting in Φ acting on the free elements in W ,
Determines uniqueness.

Length(w): number of free elements in w
(including repetitions)

of operations in Φ (including repetitions) = Length(w)-1

Algebra of words and Identity

Let $Q(\Sigma)$ be an algebra, that is, a set Q with some set Σ of operations.

Let $w_1 = \Phi_1(W_1), w_2 = \Phi_2(W_2)$ be two words w.r.t. Ω , that is, w_1 and w_2 lie in the algebra of words $\Sigma(Q, M)$.

DEFINITION. We say that the *identity (or identical relation)*

$$w_1 = w_2 \text{ or } \Phi_1(W_1) = \Phi_2(W_2) \quad (1.1)$$

is *satisfied in $Q(\Sigma)$* if (1.1) holds in $Q(\Sigma)$ whenever the free elements in $W = W_1 \cup W_2$ are replaced by *arbitrary* elements in Q and the operations in $\Phi = \Phi_1 \cup \Phi_2$ by *fixed operations* in Σ .

Balanced Identities.

An identity is called **balanced** if free elements appear on both sides of the identity just once.

The **associative law** ($xy \cdot z = x \cdot yz$),
the **medial law** ($xy \cdot uv = xu \cdot yv$)
and others are balanced.

If an identity is not balanced,
the solution of the corresponding functional equation presents **considerable difficulties**.

Grupoids and Quasigroups.

A set Q with one binary operation A is a **groupoid** and is denoted by $Q(A)$ (or by $Q(\cdot)$)

$Q(A)$ is called a **quasigroup** if A is invertible, that is, if the equations $A(a, x) = b, A(y, a) = b$ are uniquely soluble $\forall a, b \in Q$.

The operation A itself is called a quasigroup if $Q(A)$ is a quasigroup;

Groupoid

a set G with a **unary operation** $^{-1}$ and a **partial function** $*$.

$^{-1}$ is not a binary operation , is an operation with only one operand, i.e. a single input.

$*$ is not forced to map every element of X to an element of Y (only some subset X' of X).

$*$ and $^{-1}$ have the following axiomatic properties.

Let $a, b, c \in G$. Then:

1. *Associativity*: If $a * b$ and $b * c$ are defined, then $(a * b) * c$ and $a * (b * c)$ are defined and equal. Conversely, if either of these last two expressions is defined, then so is the other (and again they are equal).

2. *Inverse*: $a^{-1} * a$ and $a * a^{-1}$ are always defined.

3. *Identity*: If $a * b$ is defined, then $a * b * b^{-1} = a$, and $a^{-1} * a * b = b$.

From these axioms, it follows that :

- $(a^{-1})^{-1} = a$;
- If $a * b$ is defined, then $(a * b)^{-1} = b^{-1} * a^{-1}$.

Loops and Permutations.

If quasigroup $Q(\cdot)$ has an identity, if $\exists e \in Q$ s.t. $ex = xe = x \forall x \in Q$, then $Q(\cdot)$ is called a *loop*.

Mappings from Q to Q will be denoted by lower-case greek letters:

$\alpha, \beta, \gamma, \dots, \rho, \sigma, \dots$, and written on the left.

If α is a one-to-one mapping of Q onto itself, it is a *permutation of Q* even if Q is infinite.

Let $Q(A)$ be a groupoid; then the mappings $L_A(a)x = A(a, x)$ and $R_A(a)x = A(x, a)$ are called *left and right translations of A* , respectively.

Right and left invertible operations.

A is *right invertible operation*, if

$A(a, x) = b$ has a unique solution for any a, b ; we denote it by

$x = A^{-1}(a, b)$. From this we define the *right inverse* A^{-1} of A .

The *left inverse* ${}^{-1}A$ is defined from the solution of $A(y, a) = b$ when A is *left invertible*, and we write $y = {}^{-1}A(b, a)$.

Further one can form the inverse

Operations ${}^{-1}(A^{-1}) = ({}^{-1}A)^{-1} = [{}^{-1}(A^{-1})]^{-1} = {}^{-1}[({}^{-1}A)^{-1}] = A^*$, which is defined by

$A^*(x, y) = A(y, x)$. These are all quasigroups.

No other inverses of A exist.

Isotopism of operations.

Two **operations** B and A defined on the same set Q are called

isotopic (B is an *isotope* of A) if \exists a triplet $T = (\alpha, \beta, \gamma)$ of permutations of Q s.t. $B(x, y) = \gamma^{-1} A(\alpha x, \beta y)$

$\forall x, y \in Q$. In this case $B = A^T$ or $B = A^{(\alpha, \beta, \gamma)}$.

if the groupoid $Q(\circ)$ is isotopic with the groupoid $Q(\cdot)$, then $(\circ) = (\cdot)^T$.

We call the triplet $T = (\alpha, \beta, \gamma)$ an **isotopism**.

If $\alpha = \beta = \gamma$, then $(\alpha, \alpha, \alpha) = \alpha$ and the formula

$B = A^\alpha$ means that B is **isomorphic** to A .

Isotopism is an equivalence relation on the set Λ of all operations

If $A^T = A$, then $T = (\alpha, \beta, \gamma)$ is called an **autotopism** of A . If

$A = A^\alpha$, where $\alpha = (\alpha, \alpha, \alpha)$, then α is an **automorphism** of A .

Principal Isotopism of operations.

A quasigroup (L, \cdot) is isotopic to a quasigroup (M, \circ)
provided there are three one-to-one mappings

α, β, γ of L onto M s.t.

$x, y \in L$ implies $x\alpha \circ y\beta = (x \cdot y)\gamma$;

If γ is the identity mapping, then we say (L, \cdot) is **principally isotopic** to (M, \circ)

Both isotopy and principal isotopy are equivalence relations.

If a quasigroup (L, \cdot) is isotopic to a quasigroup (M, \circ) then
there is a quasigroup $(L, \#)$ such that (L, \cdot) is principally
isotopic to $(L, \#)$ and $(L, \#)$ is isomorphic To (M, \circ)

Loops and Quasigroups.

*we are primarily interested in those
principal isotopes that are loops.
The mappings α, β s.t. the quasigroup
 (L, \cdot) is principally isotopic to a loop
 (L, \circ) under α and β are the mappings
determined by $x\alpha = x.b$ and $y\beta = a.y$,
Where $a, b \in L$*

Loops and Quasigroups.

*Every quasigroup is isotopic, and even **principally isotopic**, to a loop;*

indeed, if Λ is a quasigroup, then A^T , where $T = (R^{-1}_A(a), L^{-1}_A(b), 1)$, is a loop.

THEOREM (Albert). *If a loop $Q(\circ)$ is isotopic to a group $Q(\cdot)$ then it is a group isomorphic to $Q(\cdot)$.*

Some types of Quasigroups & Loops .

A quasigroup $Q(\cdot)$ is called:

- a) *distributive* if $x \cdot yz = xy \cdot xz, yz \cdot x = yx \cdot xz$;
 - b) *medial* if $xy \cdot uv = xu \cdot yv$;
 - c) a *Stein quasigroup* if $x \cdot xy = yx$;
 - d) *linear* if $Q(\cdot)$ is isotopic with a group $Q(\circ)$ and the isotopism has the form $xy = \varphi x \circ t \circ \psi y$, where φ, ψ are automorphisms of $Q(\circ)$ and t is a fixed element;
 - e) a loop $Q(\cdot)$ is called a *Moufang loop* if $x(yz \cdot x) = xy \cdot zx$.
- All equations are valid for all x, y, z, u, v in Q .

Algebra of words and Identity

Ex1.

let Q be the set of integers,
 $\Sigma = \{ -, \cdot \}$, where $(-)$ is subtraction and (\cdot)
multiplication; then the identity
$$A[x, B(y, z)] = B[A(x, y), A(x, z)],$$

is valid in $Q(\Sigma)$, where $A = (\cdot)$ and $B = (-)$, that is, $x \cdot (y - z) = x \cdot y - x \cdot z$.
For instance, the operations A and B cannot be replaced by $(-)$ and (\cdot)
respectively.

Hyperidentity

DEFINITION We say that the *hyperidentity* (1.1) is satisfied in $Q(\Sigma)$ if (1.1) is valid whenever free elements in W are replaced by *arbitrary* elements in Q and operations in $\Phi = \Phi_1 \cup \Phi_2$ by *arbitrary* elements of Σ .

Algebra of words and Identity

Ex2.

We consider a field $Q = Q(+, \cdot)$, and let $\Sigma = \{ A_a \}$ where $A_a(x, y) = (1 - a)x + ya$, 1 being the identity element and a an arbitrary element of Q . Then the following hyperidentity holds in $Q(\Sigma)$:

$$X[x, Y(y, z)] = Y[X(x, y), X(x, z)].$$

This holds when x, y, z are replaced by arbitrary elements of Q and X, Y by arbitrary operations of the form A_a (i.e., a may be any element of Q).

Algebra of words and Identity

Ex3.

Let Q be the set of natural numbers, Σ the set $\{A, B, C, D\}$, where A is addition, B is multiplication, C is greatest common divisor and D is least common multiple of x and y . Then the hyperidentity

$$X[X(x, y), z] = X[x, X(y, z)]$$

holds in $Q(\Sigma)$

Algebra of words and Identity

Ex4.

Suppose that Σ consists of a single operations A and that the identity $\Phi_1(W_1) = \Phi_2(W_2)$ holds in $Q(\Sigma)$ - clearly Φ_1 and Φ_2 consist of A alone. Then in $Q(\Sigma')$, where Σ' consists of all operations isomorphic with A , the hyperidentity $\Phi_1'(W_1) = \Phi_2'(W_2)$ holds, where Φ_1' and Φ_2' both consist of a single operation X , which may take any value in Σ'

Generalized Identity

Finally we say that the *generalized identity*

(1.1) holds in $Q(\Sigma)$ if:

- 1) the equality (1.1) holds whenever free elements of W are replaced by *arbitrary* elements in Q ,
- 2) operations in a subset

Φ' of $\Phi = \Phi_1 \cup \Phi_2$ can be replaced by arbitrary operations in Σ , and those lying in the remainder $\Phi'' = \Phi \setminus \Phi'$ by certain operations in Σ depending on the operations in Φ' .

Generalized Identity

Ex5.

Let $Q = Q(+, \cdot)$ be a field, and let Σ be the set of all operations of the form $A_i(x, y) = I_i x + m_i y + n_i$, where I_i, m_i, n_i run over the whole of Q . Then the generalized identity

$$X[Y(z, y), z] = X'[x, Y'(y, z)] \quad (1.2)$$

holds in $Q(\Sigma)$. Here X, Y may be replaced by any operations in Σ ; for instance $X = A_i, Y = A_j$; consequently $\Phi' = [X, Y]$, and then there are operations X', Y' in Σ such that (1.2) is satisfied.

For instance $X'(x, y) = k l_{ij} x + y$,

$$Y''(x, y) = l_i m_j x + m_i y + l_i n_j + n_i$$

Here $\Phi'' = \{X', Y'\}$

Basic Identities

(rank 1: only one operation, which we denote by ordinary multiplication, is involved)

1. $xy \cdot z = x \cdot yz$ - associativity.
2. $xy \cdot uv = xu \cdot yv$ - mediality (entropy, bisymmetry, quasi-abelianness).
3. $yx \cdot zx = yz$ - transitivity.
4. $x \cdot yz = xy \cdot xz$ - left distributivity. Right distributivity is defined in an analogous way.
5. $x \cdot xy = xx \cdot y$ - left alternativity.
6. $xy \cdot x = x \cdot yx$ - elasticity.
7. $(x \cdot yz)x = xy \cdot zx$ - Moifang identity.
8. $xx = x$ - idempotence.
9. $x \cdot xy = yx$ - Stein identity.
10. $x \cdot xy = y$ - Sade's left "keys" law.

General Identities and Rank of identity

More generally, by the rank of an identity

$\Phi_1(W_1) = \Phi_2(W_2)$ we understand the number of different operations in $\Phi = \Phi_1 \cup \Phi_2$

The rank of $w_1 = w_2$ or $\Phi_1(W_1) = \Phi_2(W_2)$ cannot exceed the number $I = l_1 + l_2 - 2$, where l_1 and l_2 are the lengths of w_1 and w_2 , respectively. We call an identity of highest possible rank a *general identity*

General identities

Exs:

1. $A[B(x, y), z] = C[x, D(y, z)]$ - general associative law (or general associativity).
2. $A[B(x, y), C(u, v)] = A_1[B_1(x, u), C(y, v)]$ - general mediality.
3. $A[B(y, x), C(z, x)] = D(y, z)$ - general transitivity.
4. $A[x, B(y, z)] = H[K(x, y), P(x, z)]$ - general distributivity.
5. $A[x, B(X, y)] = y$ - general (left) keys law.
6. $A(x, y) = B(y, x)$ - general commutativity, and so on.

General Associative Law A-Systems

(Systems of quasigroups with generalized associative law).

A system $Q(\Sigma)$ of quasigroups is called *left generalized associative* (a *left A-system*) if the generalized associative law

$$A[B\{x, y\}, z] = C[x, D(y, z)] \quad (2.7)$$

with the implication $(A, B) \rightarrow (C, D)$ holds in

A *right generalized associative system* is defined similarly using (2.7), but with the implication $(C, D) \rightarrow (A, B)$. If a system is simultaneously a left A-system and a right A-system, it is called an *A-system*.

Ex: Let $Q(+, \cdot)$ be a field, $P(x, y) = kx + ly + r$;
 $k, l, r \in Q, k \neq 0, l \neq 0$.

Then $Q(S)$ is an A-system of Σ consists of all possible operations P .

General Media Law

consider the identity

$$A[B(x, y), C(u, v)] = G[H(x, u), K(y, v)]. \quad (2.10)$$

a) The identity (2.10) occurs under various names: bisymmetry (Theory of functional equations), **Entropy of multigroupoides and quasigroups**, quasi-abelianness, etc.

THEOREM . *If six quasigroups A_j ($j = 1, \dots, 6$) are connected by the general medial law*

$$A_1[A_2(x, y), A_3(u, v)] = A_4[A_5(x, u), A_6(y, v)],$$

then they are all isotopic to one and the same abelian group $Q(+)$

$$\begin{aligned} A_1(x, y) &= \alpha x + \beta y & A_4(x, y) &= \chi x + \varphi y \\ A_2(x, y) &= \alpha^{-1}(\gamma x + \delta y), & A_5(x, y) &= \chi(\gamma x + \theta y), \\ A_3(x, y) &= \beta^{-1}(\theta x + \psi y), & A_6(x, y) &= \varphi^{-1}(\delta x + \psi y) \end{aligned} \quad (2.11)$$

The abelian group $Q(+)$ is determined to within isomorphism, and all the 8 permutations $\alpha, \beta, \gamma, \delta, \theta, \varphi, \psi, \chi$ of Q in (2.11) are determined to within equivalence.

Systems of quasigroups with generalized media law.

A system $Q(\Sigma)$ of quasigroups is called
a generalized medial system (M-system)
if the generalized medial law

$$A [B (x, y), C (u, v)] = A' [B' (x, u), C' (y, v)]$$

with the implication $(A, B, C) \rightarrow (A', B', C')$ holds in $Q(\Sigma)$.

Here it does not make sense to discuss left and right generalized identities
For M-systems, since the implication $(A', B', C') \rightarrow (A, B, C)$ coincides with
the previous one. This is one
of the reasons why the medial is called the bisymmetric law.

Exs.

Let $Q(+)$ be an abelian group, $A_t(x, y) = t - x - y$.

Then $\Sigma = |A_t|$, with t running over the whole of Q , is an M-system.

Let $Q(+)$ be an abelian group and $\Sigma^{(+)}$ the set of all
linear quasigroups over $Q(+)$. Then $Q(\Sigma^{(+)})$ is an M-system.

Matroid quasigroup equations

We are going to associate a new system of equations to every matroid.

These equations belong to the class of
generalized quasigroup equations.

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

Matroid quasigroup equations

Let $(N; r)$ be a matroid and Q a nonempty set.

A family of C -quasi-groups 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 , $\forall i \in N - I$,

for every circuit C containing i and $\forall x_I \in Q^I$

$$q_{\gamma(i,I)}^i (\pi_{\gamma(i,I) - i} (x_I)) = q_{iC}(y_{C - i});$$

where $y_{C - i} = (y_j)_{j \in C - i}$ has the coordinates

$$y_j = q_{\gamma(i,I)}^i (\pi_{\gamma(i,I) - i} (x_I)) \text{ for } j \in C - (i \cup I) \\ \text{and } y_j = x_j \text{ for } j \in C \cap I$$

In a single instance of I, i and C we speak about a matroid quasigroup equation of $(N; r)$.

Matroid quasigroup equations

Exs.

For a free matroid the system of its matroid quasigroup equations
is empty and it
is solved by the void family of quasigroups.

If $|Q| = 1$, the matroid quasigroup equations have a unique solution to be
called trivial.

Matroid quasigroup equations

Exs.

Let $N = \{1; 2; 3; 4\}$ and $U_{2,4} = (N; r)$ uniform matroid rank 2 on N .

There are 24 matroid quasigroup equations of $U_{2,4}$.

The unknowns are four C-quasigroups

$q_{123}; q_{124}; q_{134}$ and q_{234} on a set Q

(Here q_{123} stand for $q_{\{1;2;3\}}$, etc.).

Two of the equations have the form

$$q_{134}^4(x_1; x_3) = q_{124}^4(x_1; q_{123}^2(x_1; x_3)); x_1; x_3 \in Q;$$

$$q_{234}^4(x_2; x_3) = q_{124}^4(q_{123}^1(x_2; x_3); x_2); x_2; x_3 \in Q;$$

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 this is written:

$$4(1; 3) = 4(1; 2(1; 3)) \text{ as}$$

Stands for

$$q_{134}^4(x_1; x_3) = q_{124}^4(x_1; q_{123}^2(x_1; x_3)); x_1; x_3 \in Q;$$

Matroid quasigroup equations

Exs.

For given $j \in N$ consider the group of 6 equations indexed by I ; i and C satisfying $I \cap C = j$.

1st group Eq. $4(1; 3) = 4(1; 2(1; 3))$ is equivalent as

$$4(1; 2) = 4(1; 3(1; 2))$$

$$\text{or } 2(1; 3) = 2(1; 4(1; 3))$$

$$\text{or } 2(1; 4) = 2(1; 3(1; 4))$$

$$\text{or } 3(1; 2) = 3(1; 4(1; 2))$$

$$\text{or } 3(1; 4) = 3(1; 2(1; 4)).$$

Hence, by symmetry,

the 6 matroid equations within each of the 4 groups are mutually equivalent. These 2 equations belong to the 1st and 2nd group.

If rewritten as $4(1; 2) = 4(1; 3(1; 2))$ and $4(1; 2) = 4(2; 3(1; 2))$, and compared we derive $4(1; 3) = 4(2(1; 3); 3)$ of the 3rd group.

$$\text{or } 3(1; 2) = 3(1; 4(1; 2)) \text{ and } 3(1; 2) = 3(2; 4(1; 2))$$

leading to an equation of the 4th group $3(1; 4) = 3(2(1; 4); 4)$.

Matroid quasigroup equations

Exs.

the starting 2 equations are equivalent to
the whole system of 24 equations.

Recasting the 2 above equations into

$$q^4_{124}(x_1; x_2) = q^4_{134}(x_1; q^3_{123}(x_1; x_2)); x_1; x_2 \in Q;$$

$$q^4_{124}(x_1; x_2) = q^4_{234}(x_2; q^3_{123}(x_1; x_2)); x_1; x_2 \in Q;$$

Observe that

the mapping $(x_1; x_2) \mapsto (q^3_{123}(x_1; x_2)); q^4_{124}(x_1; x_2))$
must be bijective.

Hence, quasigroups q^3_{123} and q^4_{124} are orthogonal.

Opposite direction:

if r^3_{123} and r^4_{124} are 2 orthogonal binary quasigroups on Q

then the mappings

$$(x_1; x_3) \mapsto r^4_{124}(x_1; r^2_{123}(x_1; x_3)) \text{ and}$$

$$(x_2; x_3) \mapsto r^4_{124}(r^1_{123}(x_2; x_3); x_2) \text{ define}$$

2 quasigroups on Q denoted by r^4_{134} and r^4_{234} .

C-quasigroups $(r_{123}; r_{124}; r_{134}; r_{234})$ solves the matroid quasigroup equations of $U_{2;4}$

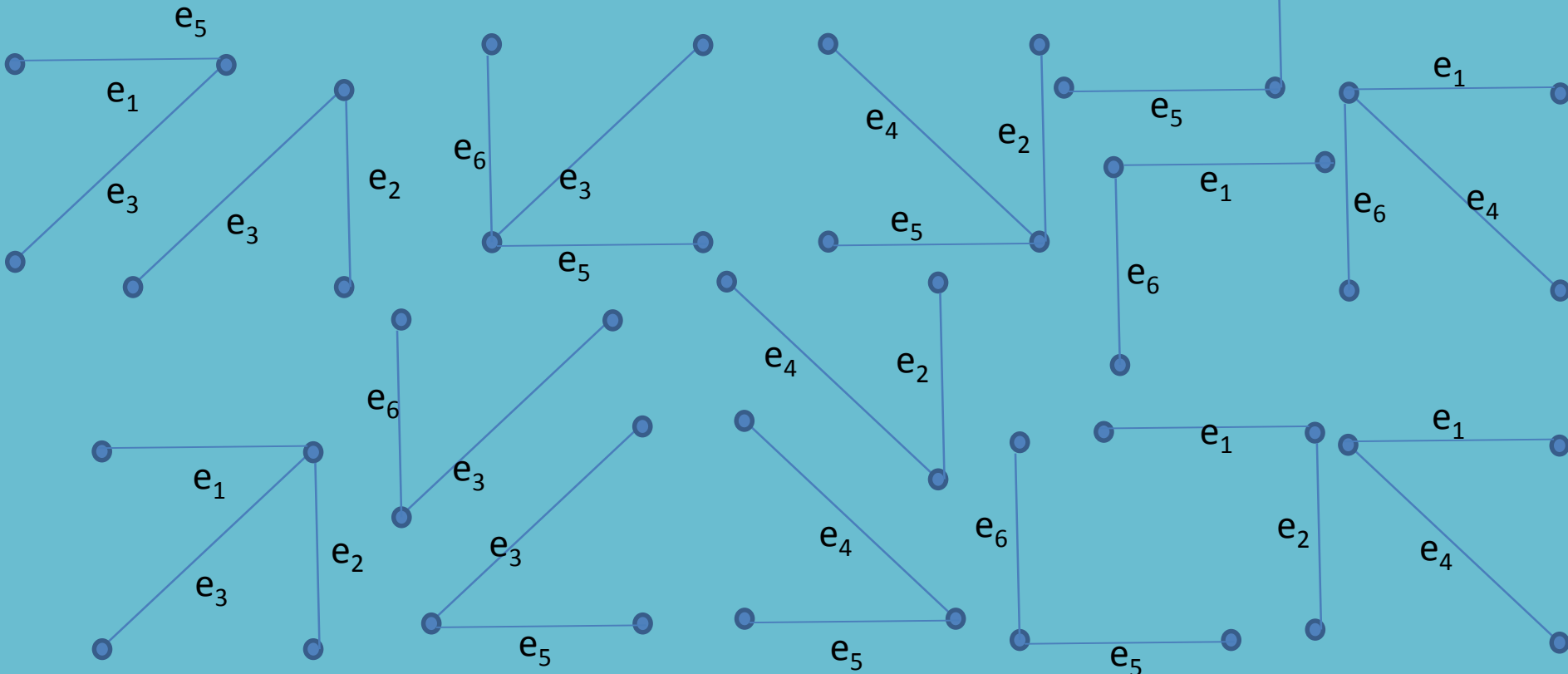
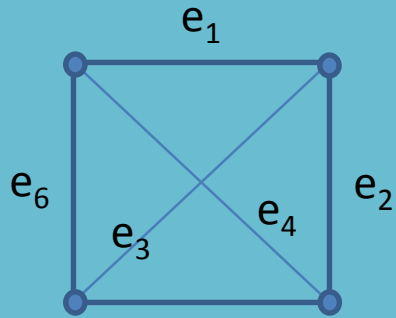
A.W. Ingleton Algebraic Non linear 11 elements Matroid

Graphic Matroid of the Clique on 4 vertices

$M(K_4)$,

$E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$

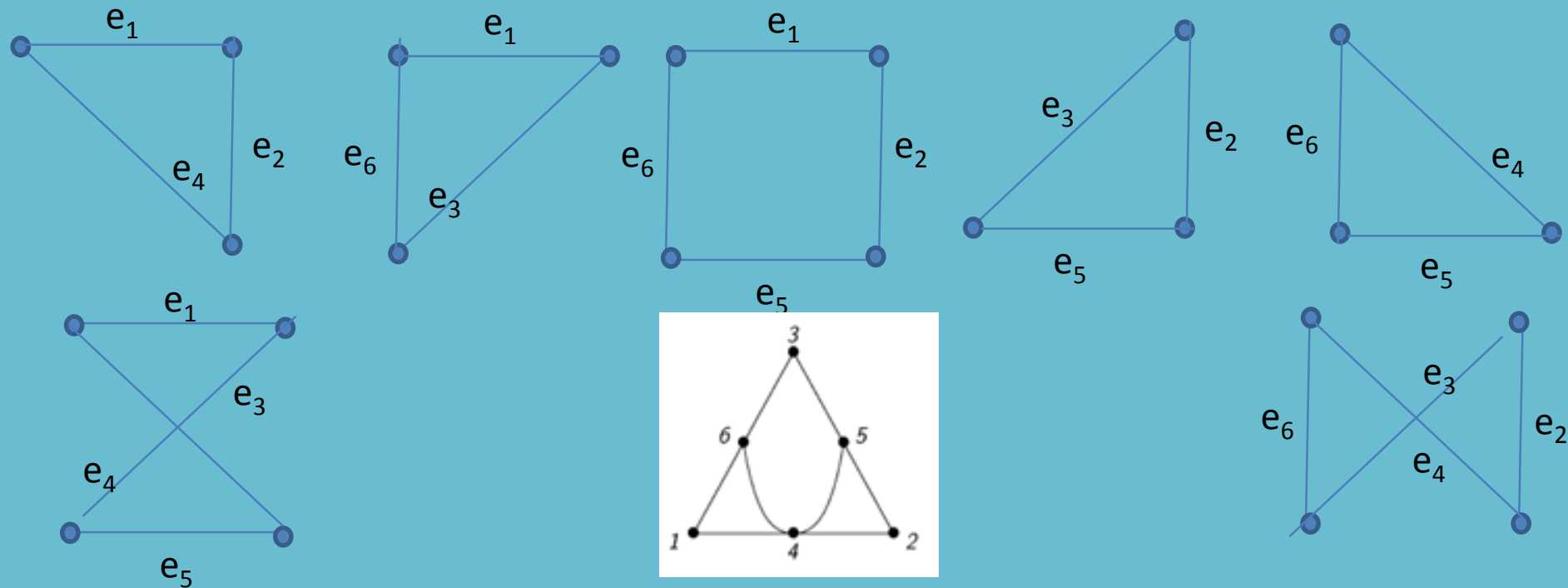
I: independent sets are the following forests



The graphic matroid $M(K_4)$,

The cycle matroid of the clique on 4 vertices.

This matroid has rank 3, the ground set $N = \{1; 2; 3; 4; 5; 6\}$, and seven circuits $\{1; 2; 4\}; \{1; 3; 6\}; \{2; 3; 5\}; \{4; 5; 6\}; \{1; 2; 5; 6\}; \{1; 3; 4; 5\}; \{2; 3; 4; 6\}$,



P-representation of $M(K_4)$,

The graphic matroid $M(K_4)$,

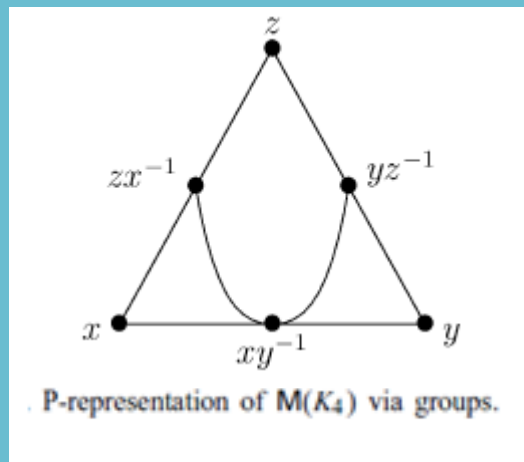
Let $(G;*)$ be a finite multiplicative group of order $d \geq 2$ and let the labels in Fig. define six partitions of G^3 : For points 1; 2 and 3 the partitions $\xi^{(G;.)}_1, \xi^{(G;.)}_2$ and $\xi^{(G;.)}_3$ consist of the x-, y- and z-coordinate layers of G^3 , respectively, and further

$$\xi^{(G;.)}_4 = \{(x; y; z) \in G^3; xy^{-1} = a; a \in G\};$$

$$\xi^{(G;.)}_5 = \{(x; y; z) \in G^3; yz^{-1} = a; a \in G\};$$

$$\xi^{(G;.)}_6 = \{(x; y; z) \in G^3; zx^{-1} = a; a \in G\};$$

are level partitions of 3 binary quasigroups.



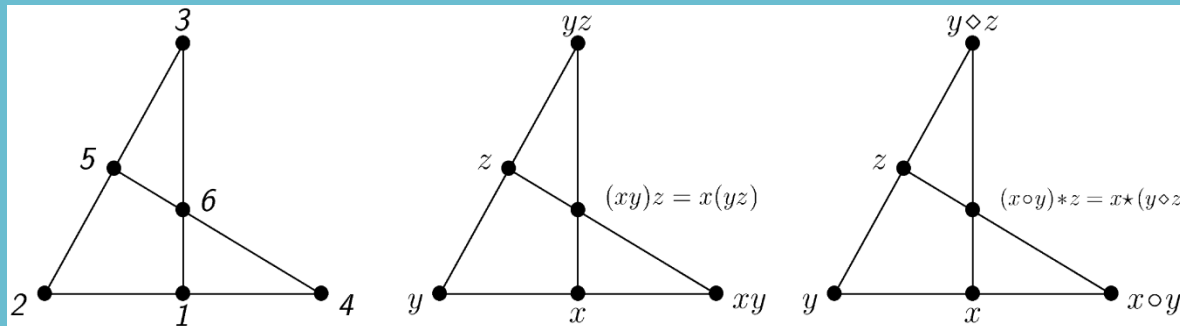
Proposition.

Every p-representation of $M(K_4)$ 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.

Consequence 1.

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 $(G; \cdot)$ 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



From The General associative law.

Consequence 2.

If 4 binary quasigroup operations on a finite set Q satisfy
the equation $(x \circ y) * z = x \star (y \diamond z) \forall x; y; z \in Q$
then \exists a group $(Q; \cdot)$,

unique up to isomorphisms, and 5 permutations $\alpha; \beta; \gamma; \delta; \epsilon$ of Q s.t.

$$x \circ y = \delta^{-1}(\alpha(x), \beta(y)); \quad x * z = \delta(x) \cdot \gamma(z);$$

$$y \diamond z = \epsilon^{-1}(\beta(y), \gamma(z)); \quad x \star z = \alpha(x) \cdot \epsilon(z)$$

is valid $\forall x; y; z \in Q$.

Since the matroid $M(K_4)$ has 7 circuits its matroid quasigroups equations involve
7 C -quasigroups, e.g. $(I = \{1; 2; 3\}, i = 4 \text{ and } C = \{4; 5; 6\})$

$$q_{124}^4(x_1; x_2) =$$

$$q_{456}^4(q_{235}^5(x_2; x_3);$$

$$q_{136}^6(x_1; x_3)); x_1; x_3 \in Q;$$

which is the general transitive equation for quasigroups

Algebraic Matroid is Linearly representable

Fano matroid

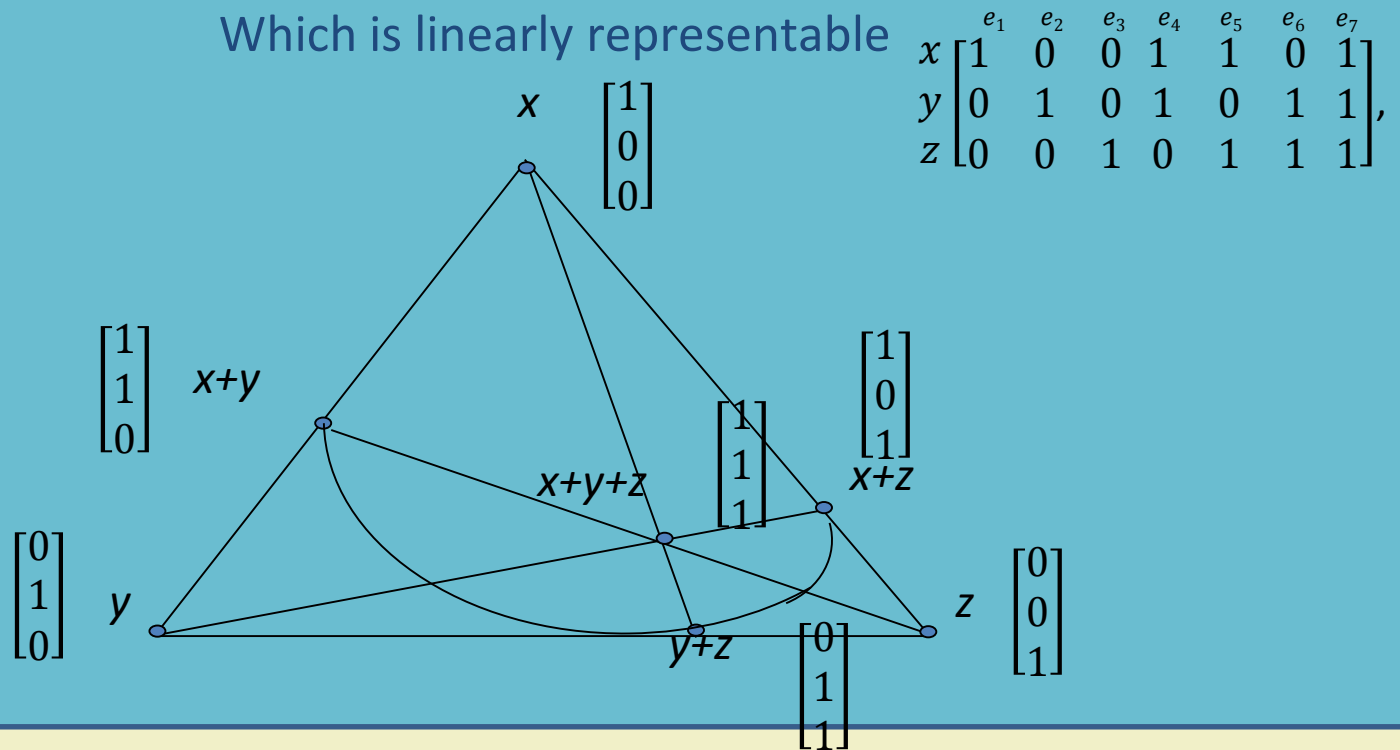
Let $K=GF(2)$, $F=K(x,y,z)$

Where x,y,z are independent transcendentals

The set $S_2=\{x,y,z,x+y,y+z,x+z,x+y+z\}$

Gives a matroid F_7

Which is linearly representable



Fano Matroid F_7

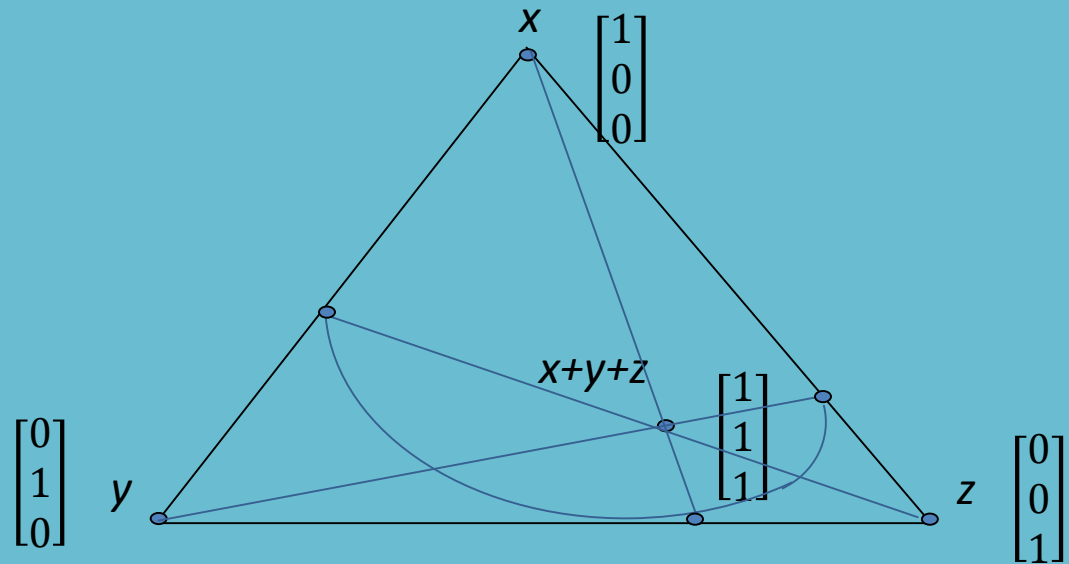
F_7 is linearly representable

$\{e_4, e_5, e_6\} \in \mathcal{C}$, is minimal dependent set (circuit)

(all its subsets are independent.)

1. Given $e_i, e_j, i \neq j$, \exists a unique k s.t. $\{e_i, e_j, e_k\} \in \mathcal{C}$.
(any $e_i, e_j, i \neq j$, determine a e_k -circuit.)
2. Any two 3-element circuits will intersect in a single element.
3. $\{e_1, e_2, e_3, e_7\}$ is a set of 4 elements no 3 of which form a circuit.
4. Any $\{e_i, e_j, e_k\} \in \mathcal{C}$ are on a line (straight or curved)

$$\begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\ x & \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \\ y & & & & & & & \\ z & & & & & & & \end{matrix},$$



Non Fano Matroid

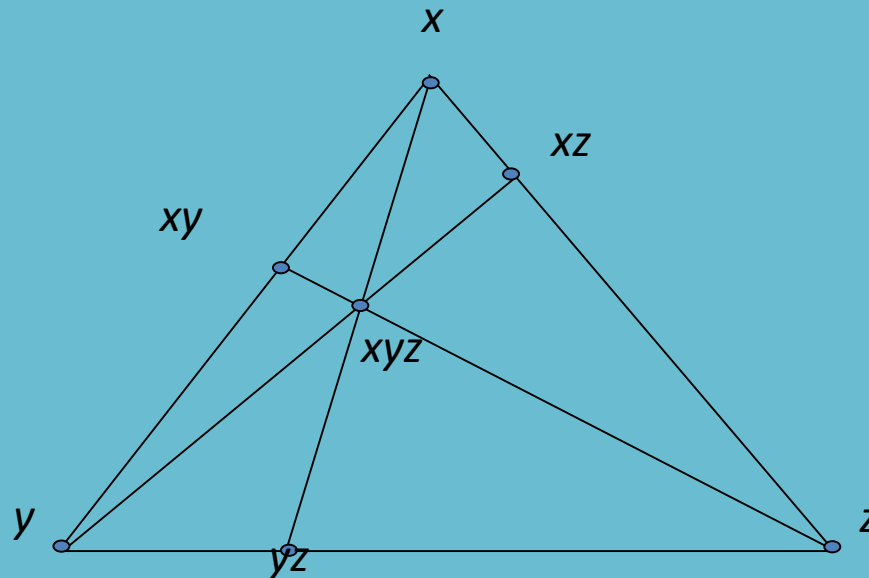
An Algebraically representable Matroid that is not F-representable

Let $K = GF(2)$, $F = K(x, y, z)$

Where x, y, z are independent transcendentals

The set $S_1 = \{x, y, z, xy, yz, xz, xyz\}$

Gives a non Fano matroid
that is not linearly representable



Non Fano Matroid

$$K=GF(2), F=K(x,y,z)$$

x,y,z independent transcendentals

$$S_1=\{x,y,z,xy,yz,xz,xyz\}$$

Non Fano matroid

F_7^- , is a 7-element matroid of rank=3.

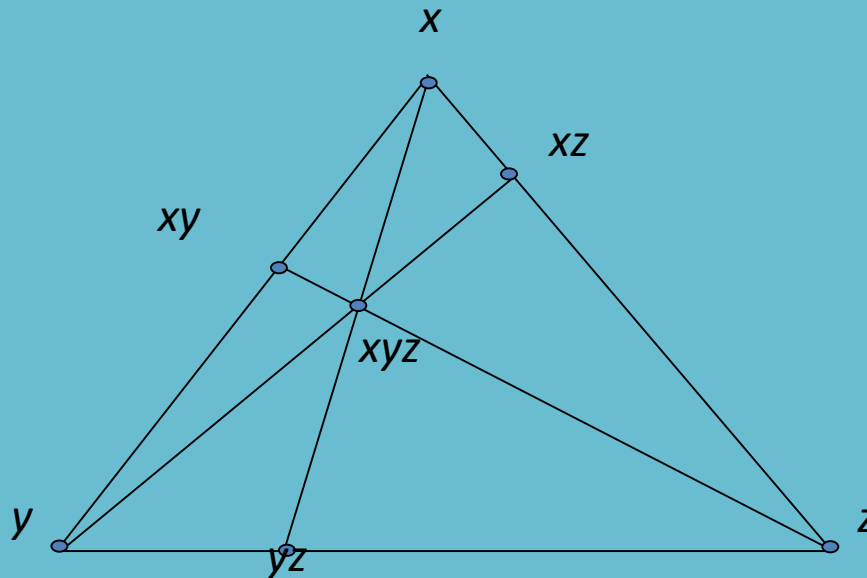
It is representable over a field iff it has characteristic other than two.

$$r(x,y)=r(x,xy)=r(xy,x)=2;$$

$$r(x,xy,x)=r(x,xyz,y)=2;$$

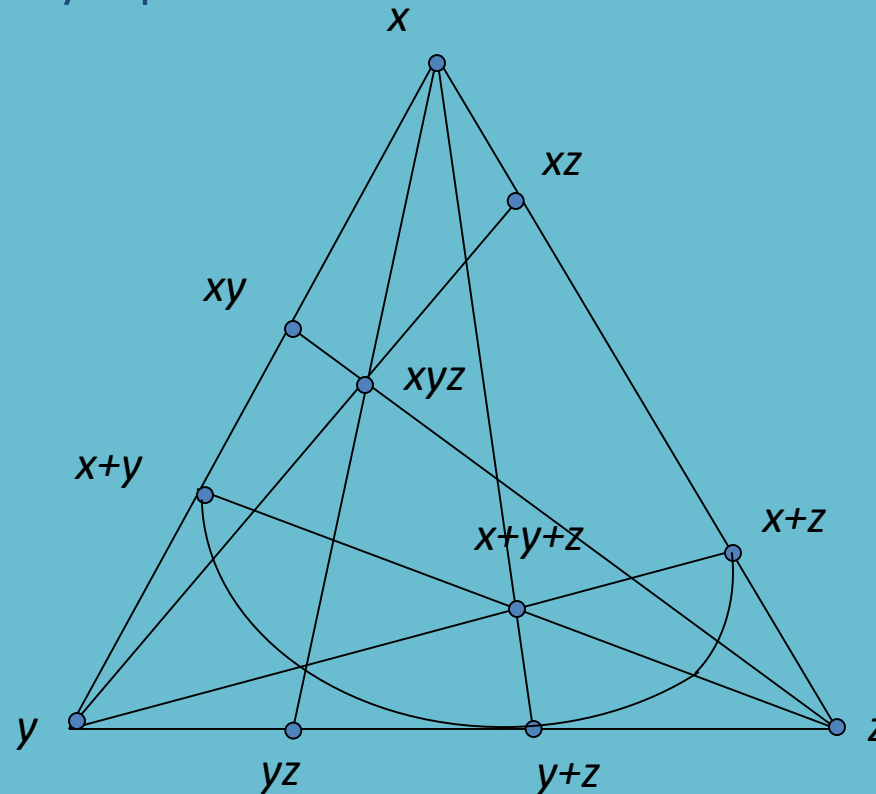
$$r(x,y,z,xy,yz,xz)=3$$

$$r(x,y,z,xy,yz,xz,xyz)=3$$



A.W. Ingleton Algebraic Non linear 11 elements Matroid

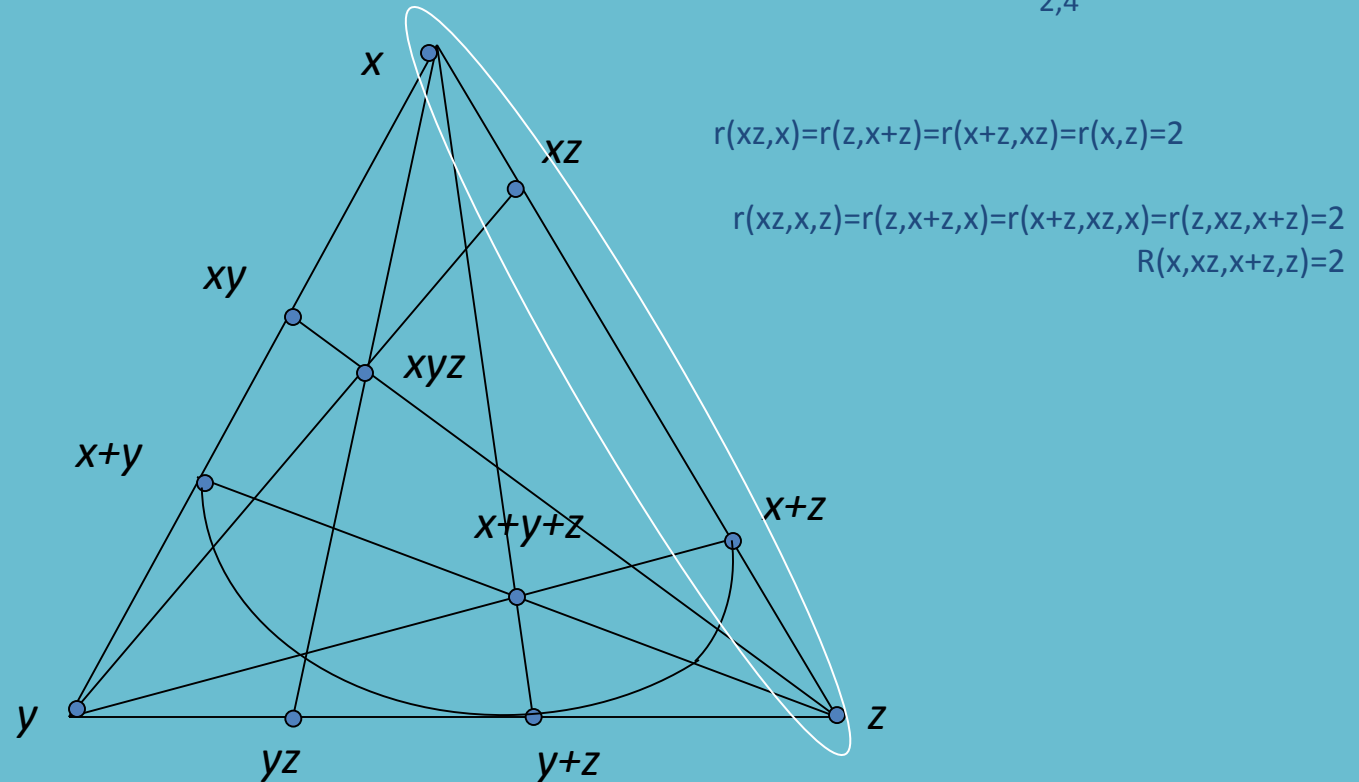
An Algebraically representable Matroid that is not F-representable



An Algebraic Matroid that is not linearly representable
Proposed by A.W. Ingleton

A.W. Ingleton Algebraic Non linear 11 elements Matroid

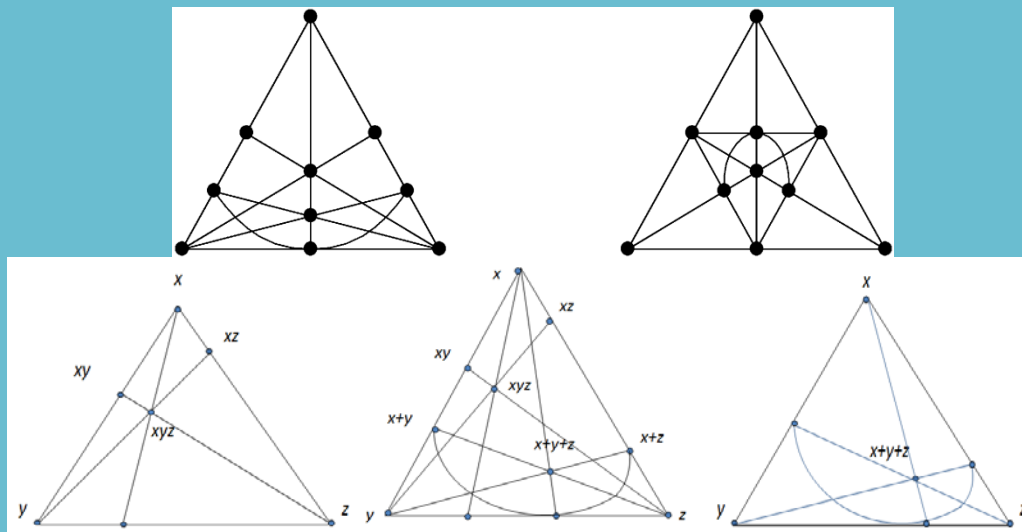
I_{11} is not Binary linearly representable since
It contains in each of its sides the forbidden minor $U_{2,4}$



An Algebraic Matroid that is not linearly representable
Proposed by A.W. Ingleton

Proposition.

Matroids of rank 3 containing the graphical matroid $M(K_4)$ as subcongruation, like some classical nonlinear matroids will be shown here not to be p -representable as well.



Proposition.

Matroids of rank 3 containing the graphical matroid $M(K_4)$ as subcongruation, like some classical nonlinear matroids will be shown here not to be p -representable as well.

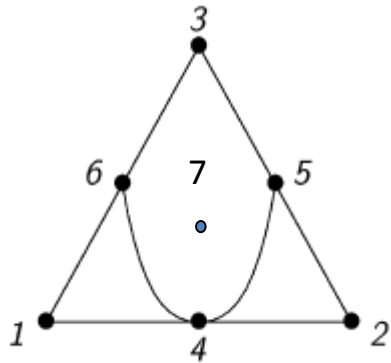
Proof.

All matroids of Fig. previous slide contain as restrictions (submatroids) the Fano and nonFano 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 nonFano matroid to have only odd degrees.

The matroids of Fig. in previous slide must be then non- p -representable.

A.W. Ingleton Algebraic Non linear 11 elements Matroid



Proposition.
All P representations of Fano matroid
will be
found to have their
degrees equal to powers of two.

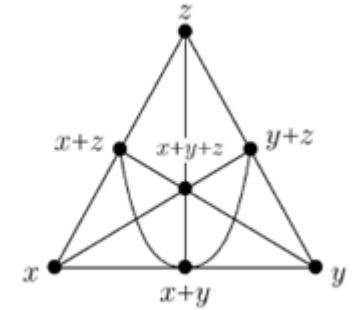


Fig. 8. P-representations of Fano matroid

Proof:

Points of the Fano matroid are labeled as in the $M(k_4)$ Fig. left ,center point gets the label 7.

Let ε be a p-representation of the Fano matroid in the coordinate form w.r.t. $\{1; 2; 3\}$

and let $(G; *)$ be a finite group defining the 6 partitions of ε according to Fig. right.

The 7th partition is treated by an equivalence on G^3 . Where 1 is the unit element of $(G; *)$,

$(1; 1; 1) \equiv (a; a; 1)$ since the blocks of ε_7 are unions of blocks of $\{3; 4\}$

Analogously $(a; a; 1) \equiv (a; ab; b) \equiv (ac; ab; bc)$ thinking about $\{1; 5\}$ and $\{2; 6\}$.

Hence $\{(c; b; bc); b; c \in G\} = \{(ac; a; c); a; c \in G\}$ is a block of ε_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 Z_2 of

order two and ε_7 is the level partition of ternary quasigroup $(x; y; z) \mapsto x + y + z$. Any

system of seven partitions defined by Fig. right with the addition in Z_2^m , $m \geq 1$, is

obviously a p-representation of the Fano matroid.

A.W. Ingleton Algebraic Non linear 11 elements Matroid

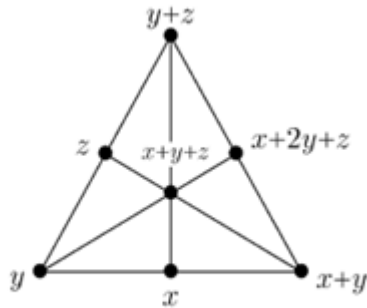
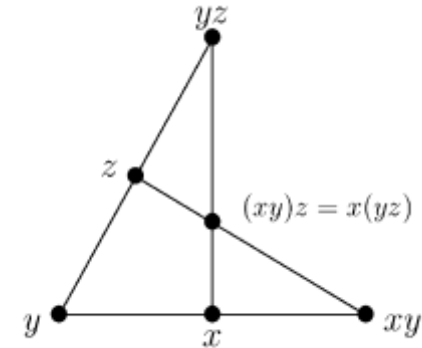


Fig. 8. P-representations nonFano matroid

Proposition.

all p-representations of the nonFano matroid to have only odd degrees.



Proof:

Let be a p-representation of the nonFano matroid and six of its partitions be defined as in the Fig. right via a group $(G; \cdot)$. The argument is similar to the Fano case;

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

where \equiv is the partition corresponding to ε_5 . Hence, the group must be Abelian. If it had even order d then the set $\{(-a^{-2}b; b; a); a; b \in G\}$ would have cardinality smaller than d^2 and could not be a block of the latin partition ε_5 . With an odd order d , Fig. 8 works.

Semi Matroids.

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

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

This family of $|[g]|$ is called a semimatroid

Probabilistically representable Semimatroids

A semimatroid

is probabilistically representable if for a system of random variables on $(\Omega; p)$ a triple $(i; j|K)$ belongs to it if and only if i is stochastically conditionally independent of j given K .

A necessary and sufficient condition for this is the equality

$$h(i \cup K) + h(j \cup K) = h(K) + h(i \cup j \cup K);$$

Conditional Independence among Partitions and Semimatroids

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.

Weakly Probabilitically representable Matroids

A Matroid $(N; r)$
is weakly probabilistically representable if the semimatroid $|[r]|$ is Probabilitically representable
, that is, if for a system of random variables on
 $(\Omega; p)$ 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
$$r(i \cup K) + r(j \cup K) = r(K) + r(i \cup j \cup K)$$

What ever
 $K \subset N;$
 $i, j \in N - K,$

Algebraic Matroid is Linearly representable

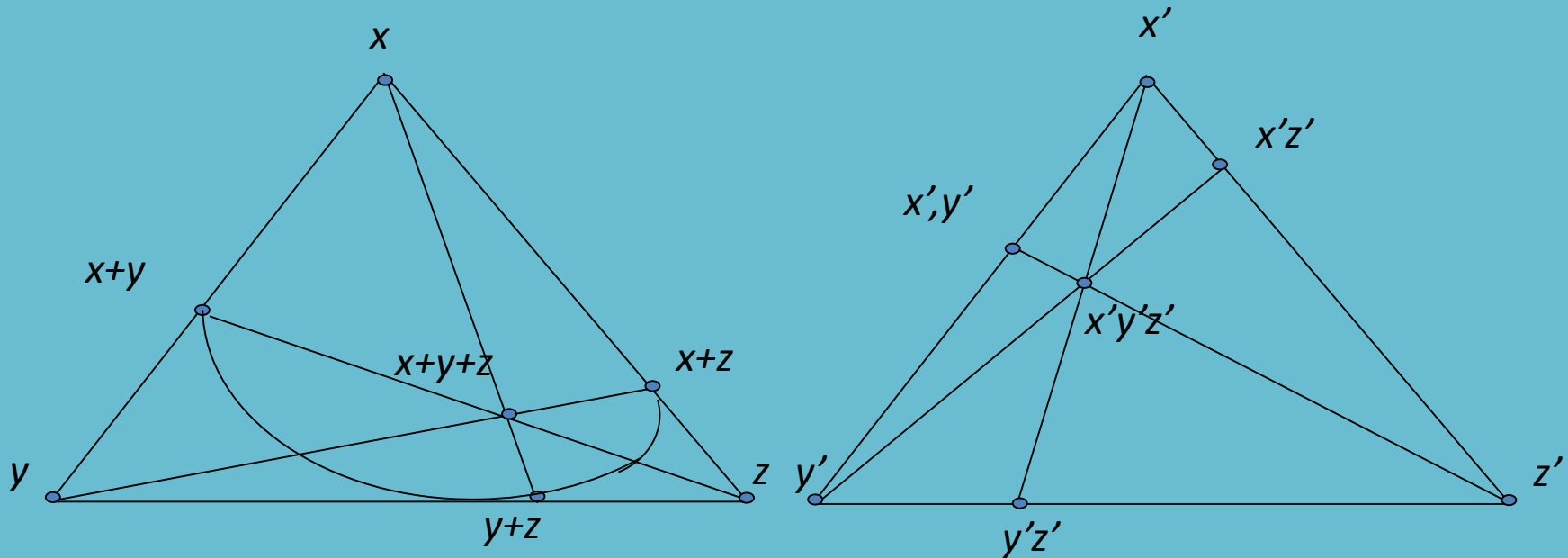
Direct sum of Fano matroid And Non Fano Matroid

Let $K = GF(2)$, $F = K(x, y, z, x', y', z')$

Where x, y, z, x', y', z' are independent transcendentals

The set $S' = S_1 \cup S_2 = \{x, y, z, x+y, y+z, x+z, x+y+z\} \cup \{x', y', z', x'y', y'z', x'z', x'y'z'\}$
 $= \{x, y, z, x', y', z', x+y, y+z, x+z, x+y+z, x'y', y'z', x'z', x'y'z'\}$

Gives a matroid $F_7 \oplus F_7^-$



Algebraic Matroid is Linearly representable

$F_7 \oplus F_7^-$ is weakly and not strongly probabilistically representable;
(1st Known example)

Let ξ be a partition representation of the Fano matroid on $N=\{1; \dots; 7\}$ and
let η be a partition representation of the nonFano matroid on $N'=\{1'; \dots; 7'\}$;

Let ξ live on Z_2^3 and η on Z_3^3

. Then partitions $\{A \times Z_3^3; A \in \xi_i\}$, $i \in N$, and $\{Z_2^3 \times B; B \in \eta_j\}$, $j \in N'$, of $\Omega = Z_2^3 \times Z_3^3$
with $p(\omega) = 2^{-3} 3^{-3}$; $\omega \in \Omega$, provide

a weak probabilistic representation of $F_7 \oplus F_7^-$.

Also $F_7 \oplus F_7^-$ is not partition representable,
and thus not strongly probabilistically representable.

