Self-distributive quasigroups and quandles

David Stanovský

Charles University, Prague, Czech Republic

Kazakh-British Technical University, Almaty, Kazakhstan

stanovsk@karlin.mff.cuni.cz

June 2015

Outline

1. Motivation: Where self-distributivity comes from
2. Medial, trimedial and distributive quasigroups
   - 2a. affine representation in general
   - 2b. representation of distributive and trimedial quasigroups over commutative Moufang loops
   - 2c. the structure of distributive quasigroups
3. Left distributive quasigroups (and quandles)
   - 3a. (almost) linear representation
   - 3b. homogeneous representation
4. Applications in knot theory

1a. Historical motivation

Self-distributivity

Let $(A, *)$ be a *binary algebraic structure*.

Left translations are mappings $L_a : A \to A$, $x \mapsto a * x$.

$(A, *)$ is *left self-distributive* if all L_a's are endomorphisms.

$$a * (x * y) = (a * x) * (a * y)$$

"I think that there is a philosophical difference between an associative world and a distributive world. The associative world is a geometric world; a world in which space and time are important and fundamental concepts. The distributive world seems different to me. I think that it is a quantum world without space and time, in which only information exists."

Dan Moskovich

Self-distributivity

Let $(A,*)$ be a *binary algebraic structure*.

Left translations are mappings $L_a : A \to A$, $x \mapsto a * x$.

$(A,*)$ is *left self-distributive* if all L_a's are endomorphisms.

$$a * (x * y) = (a * x) * (a * y)$$

Self-distributivity appears naturally in

- low dimensional topology (knot and braid invariants)
- set theory (Laver's groupoids of elementary embeddings)
- Loos's symmetric spaces
- etc.

Self-distributive quasigroups

$(Q, *)$ is a *quasigroup* if $a * x = b$, $y * a = b$ have unique solutions $\forall a, b$
I.e., all left and right translations are permutations

In combinatorics: latin squares = (finite) quasigroups

Early studies on self-distributive quasigroups:

- Burstin, Mayer: *Distributive Gruppen von endlicher Ordnung* (1929)
- Anton Sushkevich: Lagrange's theorem under weaker assumptions
- Toyoda, Murdoch, Bruck: medial quasigroups are affine (1940s)
- Orin Frink: abstract definition of mean value (1950s)
- Sherman Stein (1950s)
- Soviet school: V. D. Belousov, V. M. Galkin, V. I. Onoi (1960-70s)

Spaces with reflection

In a space X (euclidean or wherever it makes sense), let

$$a * b = \text{the reflection of } b \text{ over } a.$$

Then $(X, *)$ is

- left distributive
- idempotent
- $a * x = b$ always has a unique solution, $x = a * b$
- (usually not a quasigroup, e.g. on a sphere)

Nowadays we say $(X, *)$ is an *involutory quandle*.

- observed by Takasaki (1942)
- elaborated by Loos (1960s): *symmetric spaces*

Conjugation in groups

In a group G, let $a * b = aba^{-1}$.

Then $(G, *)$ is

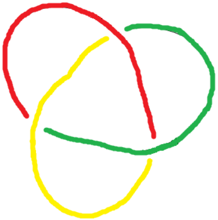
- left distributive
- idempotent
- $a * x = b$ always has a unique solution, $x = a^{-1}ba$

Nowadays we say $(G, *)$ is a *quandle*.

Observation: Left distributive quasigroups are quandles.

- Stein (1959): left distributive quasigroups embed into conjugation quandles (quandles do not, in general)
- Conway and Wraithe (1960s): *wrack of a group*
- Joyce and Matveev (1982): quandles as knot invariants

Knot coloring: 3-coloring

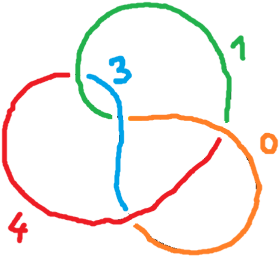


To every arc, assign one of three colors in a way that

every crossing has one or three colors.

Invariant: count non-trivial (non-monochromatic) colorings.

Knot coloring: Fox n-coloring

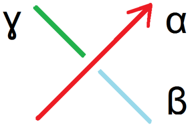


To every arc, assign one of n colors, $0, ..., n-1$, in a way that

at every crossing, $2\cdot$ bridge $=$ left $+$ right, modulo n

Invariant: count non-trivial colorings.

Quandle coloring



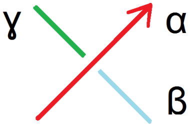
Fix a set C of colors, and a ternary relation T on C.

To every arc, assign one of the colors in a way that

$$(c(\alpha), c(\beta), c(\gamma)) \in T$$

Invariant: count non-trivial colorings. Really?

Quandle coloring



Fix a set C of colors, and a ternary relation T on C.

To every arc, assign one of the colors in a way that

$$(c(\alpha), c(\beta), c(\gamma)) \in T$$

Invariant: count non-trivial colorings. Really?

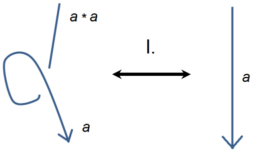
Fact (implicitly Joyce, Matveev (1982))

Coloring by (C, T) is an invariant if and only if T is a graph of a quandle.

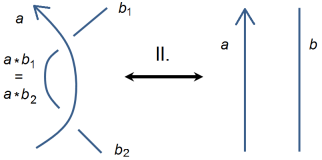
Quandle coloring

Fact (implicitly Joyce, Matveev (1982))

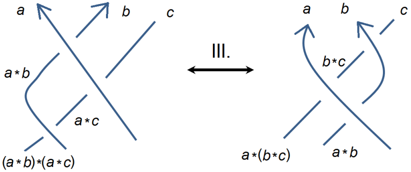
Coloring by (C, T) is an invariant if and only if T is a graph of a quandle.



$a * a = a$



unique left division



$a * (b * c) = (a * b) * (a * c)$

2a. Linear and affine representation of quasigroups

Quasigroups and loops

If I say "quasigroup $(Q,*)$", I often implicitly mean $(Q,*,\backslash,/)$.

If I say "loop $(Q,\cdot)$", I often implicitly mean $(Q,\cdot,\backslash,/,1)$.

(For universal algebraic considerations, you need $\backslash, /$ as basic operations.)

Term / polynomial equivalence

term operation = any composition of basic operations

polynomial operation = term op. with some var's substituted by constants

two algebras are *term equivalent* if they have the same term operations

two algebras are *poly. equivalent* if they have the same poly. operations

... "the two algebras are essentially the same algebraic object"

Examples:

- term equivalent: group $(G, \cdot, ^{-1}, 1)$ and the corresponding associative loop $(G, \cdot, /, \backslash, 1)$
- term equivalent: Boolean algebra and the corresponding Boolean ring
- polynomially equivalent: the quasigroup ($\mathbb{Q}$, arithmetic mean) and the module $\mathbb{Z}[1/2]$-module $\mathbb{Q}$.

Observation:

- term equivalent algebras have identical subalgebras
- polynomially equivalent algebras have identical congruences

Loop isotopes

isotope = shuffle rows and columns, rename elements in the table

Fact

Given a quasigroup $(Q, *)$, the only loop isotopes (up to isomorphism) are $(Q, \cdot)$ with $a \cdot b = (a/e_1) * (e_2 \backslash b)$, with $e_1, e_2 \in Q$ arbitrary.

Note: The loop operation $\cdot$ is polynomial over $(Q, *)$.

We can recover the quasigroup operation as $a * b = R_{e_1}(a) \cdot L_{e_2}(b)$.

- this is rarely a polynomial operation over $(Q, \cdot)$
- the best case: $*$ is a linear / affine form over $(Q, \cdot)$
  i.e. R_{e_1}, L_{e_2} are linear / affine mappings over $(Q, \cdot)$

Linear / affine quasigroups

A permutation φ of Q is *affine* over $(Q,\cdot)$ if

$$\varphi(x)=\tilde\varphi(x)\cdot u \quad \text{or} \quad \varphi(x)=u\cdot\tilde\varphi(x)$$

where $\tilde\varphi$ is an automorphism of $(Q,\cdot)$ and $u\in Q$.

Affine quasigroup over a loop $(Q,\cdot)$ is $(Q,*)$ with

$$a*b=\varphi(a)\cdot\psi(b)$$

for some affine mappings φ,ψ over $(Q,\cdot)$ such that $\tilde\varphi\tilde\psi=\tilde\psi\tilde\varphi$.

Linear / affine quasigroups

A permutation φ of Q is *affine* over $(Q,\cdot)$ if

$$\varphi(x)=\tilde\varphi(x)\cdot u \quad \text{or} \quad \varphi(x)=u\cdot\tilde\varphi(x)$$

where $\tilde\varphi$ is an automorphism of $(Q,\cdot)$ and $u\in Q$.

Affine quasigroup over a loop $(Q,\cdot)$ is $(Q,*)$ with

$$a*b=\varphi(a)\cdot\psi(b)$$

for some affine mappings φ,ψ over $(Q,\cdot)$ such that $\tilde\varphi\tilde\psi=\tilde\psi\tilde\varphi$.

Linear quasigroups over a loop $(Q,\cdot)$: φ,ψ are automorphisms, i.e. $u=v=1$.

Example:

- the quasigroup ($\mathbb{Q}$, arithmetic mean) is linear over the group $(\mathbb{Q},+)$
- the quasigroup $(\mathbb{O},*)$ with $x*y=ix\cdot jy$ is affine over the octonion loop $(\mathbb{O},\cdot)$
- quasigroups affine over abelian groups are medial (see blackboard)

Module-theoretical point of view

How to turn an affine representation into a polynomial equivalence?

(remember: the loop isotope is always polynomial over the quasigroup)

Consider wlog $\varphi(x) = u \cdot \tilde{\varphi}(x)$, $\psi(x) = v \cdot \tilde{\psi}(x)$.

Then $x * y = \varphi(x) \cdot \psi(y) = (u \cdot \tilde{\varphi}(x)) \cdot (v \cdot \tilde{\psi}(y))$ is a polynomial operation over the algebra $(Q, \cdot, \tilde{\varphi}, \tilde{\psi})$.

Conversely, $\cdot, \tilde{\varphi}, \tilde{\psi}$ are polynomial operations over $(Q, *)$,

$$\text{e.g. } \tilde{\varphi}(x) = (x * e_1)/^{\cdot}(1 * e_1)$$

Hence, $(Q, *)$ and $(Q, \cdot, \tilde{\varphi}, \tilde{\psi})$ are polynomially equivalent.

Module-theoretical point of view

$(Q,*)$ and $(Q,\cdot,\tilde\varphi,\tilde\psi)$ are polynomially equivalent.

What is $(Q,\cdot,\tilde\varphi,\tilde\psi)$, a loop expanded by commuting automorphisms?

The classical case: the loop is an abelian group, $(Q,+)$.

Then $(Q,+,\tilde\varphi,\tilde\psi)$ is term equivalent to a module over Laurent polynomials $\mathbb{Z}[s,s^{-1},t,t^{-1}]$:

- the additive structure is $(Q,+)$
- the action of s,t is that of $\tilde\varphi,\tilde\psi$, respectively

The corresponding quasigroup operation can be written as an affine form:

$$x*y = sx + ty + c.$$

Module-theoretical point of view

$(Q, *)$ and $(Q, \cdot, \tilde{\varphi}, \tilde{\psi})$ are polynomially equivalent.

What is $(Q, \cdot, \tilde{\varphi}, \tilde{\psi})$, a loop expanded by commuting automorphisms?

The classical case: the loop is an abelian group, $(Q, +)$.

Then $(Q, +, \tilde{\varphi}, \tilde{\psi})$ is term equivalent to a module over Laurent polynomials $\mathbb{Z}[s, s^{-1}, t, t^{-1}]$:

- the additive structure is $(Q, +)$
- the action of s, t is that of $\tilde{\varphi}, \tilde{\psi}$, respectively

The corresponding quasigroup operation can be written as an affine form:

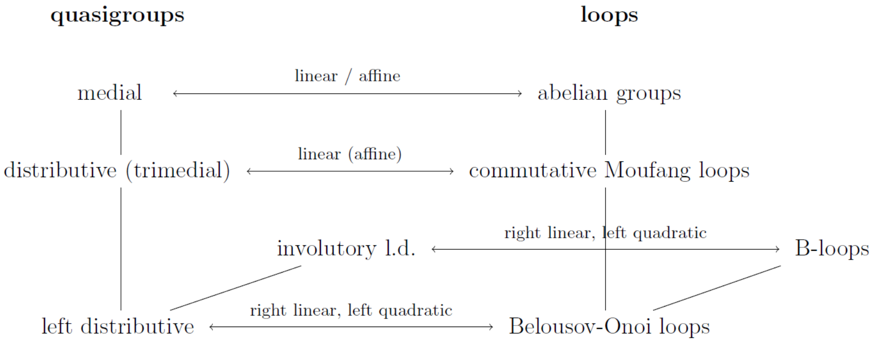
$$x * y = sx + ty + c.$$

General case: The same idea works, forget associativity of $(Q, +)$.

Loops expanded by automorphisms = "non-associative modules"

(things work particularly nicely e.g. for diassociative loops)

An outline of the representation theorems



2b. Medial, trimedial and distributive quasigroups

(Belousov, Soublin, Kepka, 1960s-70s)

Medial quasigroups are affine over abelian groups

mediality = the identity $(x * y) * (u * v) = (x * u) * (y * v)$

Note: medial idempotent quasigroups are left and right distributive

Theorem (Toyoda-Murdoch-Bruck, 1940's)

The following are equivalent for a quasigroup $(Q, *)$:

1. *it is medial,*
2. *it is affine over an abelian group.*

Moreover, for an idempotent quasigroup, TFAE:

1. it is *medial idempotent*,
2. it is *linear* over an abelian group and $\varphi = 1 - \psi$, i.e.

$$x * y = (1 - \psi)(x) + \psi(y) = x - \psi(x) + \psi(y).$$

Medial quasigroups are affine over abelian groups

Theorem (Toyoda-Murdoch-Bruck, 1940's)

The following are equivalent for a quasigroup $(Q,*)$:

1. *it is medial;*
2. *it is affine over an abelian group.*

$(2) \Rightarrow (1)$ is straightforward.

$(1) \Rightarrow (2)$: Pick arbitrary $e_1, e_2 \in Q$, define $a \cdot b = (a/e_1) * (e_2 \backslash b)$. Prove that

- $(Q,\cdot)$ is a medial loop, hence an abelian group
- the mappings $\varphi(x) = x/e_1$ and $\psi(x) = e_2\backslash x$ are affine over $(Q,\cdot)$.
- the mappings $\tilde{\varphi}, \tilde{\psi}$ commute

Medial quasigroups are affine over abelian groups

Let $(Q,*)$ be a medial quasigroup.
We prove that $(Q,\cdot)$ with $a\cdot b=(a/e_1)*(e_2\backslash b)$ is a medial loop.

First, prove that $(Q,\circ)$ with $a\circ b=(a/e_1)*b$ is medial.

$$\begin{aligned}(a\circ b)\circ(c\circ d)&=(((a/e_1)*b)/e_1)*((c/e_1)*d)\\&=(((a/e_1)*b)/((e_1/e_1)*e_1))*((c/e_1)*d)\\&=(((a/e_1)/(e_1/e_1))*(b/e_1))*((c/e_1)*d)\end{aligned}$$

Now, interchange b/e_1 and c/e_1 and get equality to $(a\circ c)\circ(b\circ d)$.

Proving that $(Q,\cdot)$ is medial is a dual argument over $(Q,\circ)$.

Trimedial quasigroups are affine over c. Moufang loops

trimediality = every 3-generated subquasigroup is medial
= mediality holds upon any substitution in 3 variables

Theorem (Kepka, 1976)

The following are equivalent for a quasigroup $(Q, *)$:

1. *it is trimedial;*
2. *whenever $(a * b) * (c * d) = (a * c) * (b * d)$, the subquasigroup $\langle a, b, c, d \rangle$ is medial,*
3. *it satisfies, for every $a, b, c \in Q$, the identities*

$$(c * b) * (a * a) = (c * a) * (b * a),$$
$$(a * (a * a)) * (b * c) = (a * b) * ((a * a) * c),$$

4. *it is 1-nuclear affine over a commutative Moufang loop.*

1-nuclear = $x\varphi(x) \in N$, $x\psi(x) \in N$ for every $x \in Q$

Distributive quasigroups are linear over c. Moufang loops

distributive = both left and right distributive

Corollary (Belousov-Soublin, around 1970)

The following are equivalent for an idempotent quasigroup $(Q, *)$:

1. *it is trimedial,*
2. *whenever $(a * b) * (c * d) = (a * c) * (b * d)$, the subquasigroup $\langle a, b, c, d \rangle$ is medial,*
3. *it is distributive,*
4. *it is 1-nuclear linear over a commutative Moufang loop.*

1-nuclear = $x\varphi(x) \in N$, $x\psi(x) \in N$ for every $x \in Q$

Distributive quasigroups are linear over c. Moufang loops

Commutative Moufang loops of order 81 (Kepka-Němec 1981):

- consider the groups $G_1 = (\mathbb{Z}_3)^4$ and $G_2 = (\mathbb{Z}_3)^2 \times \mathbb{Z}_9$
- let $e_1, e_2, e_3(, e_4)$ be the canonical generators
- let t_1 be the triaditive mapping over G_1 satisfying

$$t_1(e_2, e_3, e_4) = e_1, \ t_1(e_3, e_2, e_4) = -e_1, \ t_1(e_i, e_j, e_k) = 0 \text{ otherwise.}$$

- let t_2 be the triaditive mapping over G_2 satisfying

$$t_2(e_1, e_2, e_3) = 3e_3, \ t_2(e_2, e_1, e_3) = -3e_3, \ t_2(e_i, e_j, e_k) = 0 \text{ otherwise.}$$

- consider the loops $Q_i = (G_i, \cdot)$ with

$$x \cdot y = x + y + t_i(x, y, x - y)$$

Sample 1-nuclear automorphisms: $x \mapsto x^{-1}$, $x \mapsto x^2$

Distributive quasigroups are linear over c. Moufang loops

Distributive quasigroups of order 81 (Kepka-Němec 1981):

1. $(G_1,*)$ with $x*y=x^{-1}\cdot y^{-1}$
2. $(G_1,*)$ with $x*y=\varphi(x)\cdot\psi(y)$ where
   $\varphi(x)=(x_2-x_1)e_1-x_2e_2-x_3e_3-x_4e_4$ and $\psi=1-\varphi$
3. $(G_2,*)$ with $x*y=\sqrt{x}\cdot\sqrt{y}$
4. $(G_2,*)$ with $x*y=x^{-1}\cdot y^2$
5. $(G_2,*)$ with $x*y=x^2\cdot y^{-1}$
6. $(G_2,*)$ with $x*y=\varphi(x)\cdot\psi(y)$ where
   $\varphi(x)=-x_1e_1-x_2e_2-(3x_1+x_3)e_3$ and $\psi=1-\varphi$

Recall:

- $G_1=(\mathbb{Z}_3)^4$ and $G_2=(\mathbb{Z}_3)^2\times\mathbb{Z}_9$
- $Q_i=(G_i,\cdot)$ with $x\cdot y=x+y+t_i(x,y,x-y)$

Theorem (Kepka, 1976)

The following are equivalent for a quasigroup $(Q, *)$:

1. *it is trimedial,*
2. *whenever $(a * b) * (c * d) = (a * c) * (b * d)$, the subquasigroup $\langle a, b, c, d\rangle$ is medial,*
3. *it satisfies the identities .....,*
4. *it is 1-nuclear affine over a commutative Moufang loop.*

(2) $\Rightarrow$ (1): $(b * a) * (a * c) = (b * a) * (a * c)$, hence $\langle a, b, c\rangle$ medial.

(1) $\Rightarrow$ (3) is obvious.

(3) $\Rightarrow$ (4). Pick an arbitrary square $e \in Q$ and define the loop operation on Q by $a \cdot b = (a/e) * (e\backslash b)$. Use a neat theorem of Pflugfelder to prove that this a commutative Moufang loop (plus the other facts).

(4) $\Rightarrow$ (2). Find a subloop Q' of $(Q, \cdot)$ that contains all four elements a, b, c, d and is generated by three elements u, v, w that associate. Then, by Moufang's theorem, Q' is an abelian group, hence $\langle a, b, c, d\rangle$ medial.

Pflugfelder's characterization of c. Moufang loops

Theorem (Bruck 1⇔2⇔3, Pflugfelder ⇔4)

The following are equivalent for a commutative loop $(Q,\cdot)$:

1. *it is diassociative and automorphic,*
2. *it is Moufang,*
3. *the identity $xx\cdot yz = xy\cdot xz$ holds,*
4. *the identity $f(x)x\cdot yz = f(x)y\cdot xz$ holds for some $f: Q\to Q$.*

Moreover, if $(Q,\cdot)$ is a commutative Moufang loop, than the identity $f(x)x\cdot yz = f(x)y\cdot xz$ holds if and only if f is a (-1)-nuclear mapping.

(-1)-*nuclear* $= x^{-1}\varphi(x)\in N,\ x^{-1}\psi(x)\in N$ for every $x\in Q$

2c. The structure of distributive quasigroups

Recap

Distributive quasigroups are essentially the same objects as

- commutative Moufang loops with a 1-nuclear automorphism
- "1-nuclear commutative Moufang modules" over the ring of Laurent polynomials $\mathbb{Z}[t, t^{-1}]$

Idea: use known properties of commutative Moufang loops to reason about distributive quasigroups

Decomposition theorem

Theorem (Fischer-Smith)

Let Q be a finite distributive quasigroup of order $p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$. Then

$$Q \simeq Q_1 \times \ldots \times Q_k$$

where $|Q_i| = p_i^{k_i}$. Moreover, if Q_i is not medial, then $p_i = 3$ and $k_i \geq 4$.

... an analogy holds for commutative Moufang loops

Enumeration

$MI(n)$ = the number of medial idempotent quasigroups of order n up to isomorphism

$D(n)$ = the number of distributive quasigroups of order n up to isomorphism

Fisher-Smith says: with $p_i \neq 3$ pairwise different,

$$D(3^k \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}) = D(3^k) \cdot MI(p_1^{k_1}) \cdot \ldots \cdot MI(p_n^{k_n})$$

Moreover, $D(3^k) = MI(3^k)$ for $k < 4$.

Enumeration

Let $\mathcal{Q}(Q,\psi)$ denote the quasigroup $(Q,*)$ with $x*y=(1-\psi)(x)+\psi(y)$.

Observe:

- $\mathcal{Q}(Q,\psi)$ is medial iff $(Q,\cdot)$ is an abelian group
- $\mathcal{Q}(Q,\psi)$ is distributive iff $(Q,\cdot)$ is a commutative Moufang loop and ψ is 1-nuclear

Lemma (Kepka-Němec)

Let $(Q_1,\cdot)$, $(Q_2,\cdot)$ be commutative Moufang loops, ψ_1,ψ_2 their 1-nuclear automorphisms. TFAE:

- $\mathcal{Q}(Q_1,\psi_1)\simeq\mathcal{Q}(Q_2,\psi_2)$
- *there is a loop isomorphism $\rho: Q_1\simeq Q_2$ such that $\psi_2=\rho\psi_1\rho^{-1}$*

Enumeration

Theorem (Hou 2012)

- $MI(p) = p - 2$
- $MI(p^2) = 2p^2 - 3p - 1$
- $MI(p^3) = 3p^3 - 6p^2 + p$
- $MI(p^4) = 5p^4 - 9p^3 + p^2 - 2p + 1$

n	3	3^2	3^3	3^4	3^5	3^6
$CML^*(n)$	0	0	0	2	6	≥ 8
$3M^*(n)$	0	0	0	35		
$D^*(n)$	0	0	0	6		
$DS^*(n)$	0	0	0	1	1	3
$MI(n)$	1	8	30	166		

Here $X^*(n) = X(n) - MI(n)$.