A Brief Overview of Non-associative Algebra

A Very Personal View

David Stanovský
Charles University, Prague, Czech Republic

Non-associative algebraic structures arise in many situations. Cayley's octonions are a notorious example, but there are far more: for example, non-associative loops arise in coordinatization of projective planes [Pickert 1955], and the Einstein velocity addition in relativity theory also forms a non-associative loop [Ungar 2001]. Selfdistributive algebras appear naturally in the study of braids [Dehornoy 2000], and notably in knot theory, where so called quandles are used as homotopy invariants of knots [Joyce 1982]. And there is so much more. We wish to present a brief overview of the origins of non-associative algebra, and a selection of current research topics and prospects.

Given the width of the subject, we shall focus our attention on three particular classes that currently seem to attract most attention and have been traditionally covered by the algebraic group in Prague:

1. quasigroups and loops,
2. selfdistributive algebras,
3. mediality and modes.

Particularly, we omit all aspects related to geometry, both classical and differential. We also exclude the theory of non-associative algebras in the sense of ring theory, a subject with identical origins, but different evolution.

For us, *an algebra* means just a universal algebra (or general algebra), i.e., a set equipped with (finitary) operations. Algebras with a single binary operation are often called *groupoids*, or *binary systems*, and play a central role in non-associative algebra.

Objects.

1. Quasigroups and loops.

Quasigroups are algebras with a binary operation $*$ such that the equations

$$a * x = b \qquad \text{and} \qquad y * a = b$$

have a unique solution for every a, b. *Loops* are quasigroups with a unit element, or "non-associative groups". While quasigroups are often studied from a combinatorial point of view (note that finite quasigroups are essentially the same objects as latin squares), the loop theory is, to some extent, built as a generalization of group theory, and a great deal of attention is focused on various weak forms of the associative law. The deepest results often exploit advanced group theoretical methods.

This is the oldest and most developed discipline of non-associative algebra, originated in 1930's in works of Sushkevich, Moufang, Bol, Murdoch and others, see [Pflugfelder 2000] for comprehensive historical notes. The topic is covered by several books [Bruck 1958] [Belousov 1967] [Pflugfelder 1990] [Chein et al. 1990] [Nagy and Strambach 2002] [Smith 2007] that study various aspects of the theory, and reflect different eras of non-associative mathematics and different standpoints of the geographically distant schools.

To get a taste of an important recent result, consider the Lagrange property, the one from elementary group theory, stating that the order of a finite group is divisible by the order of every subgroup. It is very easy to prove the property for groups, however it fails for a majority of general loops. The property was recently proven for all (finite) Moufang loops, independently by [Grishkov and Zavarnitsine 2005] and [Gagola and Hall 2005]; the Moufang property is a weaker form of associativity, satisfied e.g. by octonions. Both proofs are based on Doro's classification of finite simple Moufang loops and Kleidman's determination of the maximal subgroups of the orthogonal groups $P\Omega_8(q)$.

2. Selfdistributive algebras.

The notion of *selfdistributivity* refers to the fact that left or right (or both) translations are endomorphisms. A groupoid is called *left distributive*, if

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

for every a, b, c, i.e., if the left translation, $L_a : x \mapsto a * x$, is an endomorphism of the algebra, for every a. A typical example is conjugation in groups: for a group G, consider a new operation, $a * b = aba^{-1}$; the algebra $(G, *)$ is left distributive.

The first explicit allusion to selfdistributivity seems to appear in the 1880 paper *On the algebra of logic* by Benjamin Peirce, and only a little bit later in works of German logicians. The first article fully devoted to selfdistributive structures was published in 1929 by Burstin and Mayer, and addressed finite distributive quasigroups. Later, the theory was developed by various mathematicians, on both sides of the Atlantic, with various motivations in mind. Here are some highlights.

Ottmar Loos, in his book [Loos 1969], used continuous left distributive structures to capture the algebraic properties of symmetric spaces. J. Ježek, T. Kepka and P. Němec studied selfdistributive groupoids extensively in 1970's and 1980's, culminating in their treatise [Ježek et al. 1981], collecting many structural results on (both left and right) distributive groupoids, both in the non-idempotent and idempotent cases, including their symmetric-by-medial decomposition. David Joyce [Joyce 1982] and S. V. Matveev [Matveev 1984] independently discovered the knot quandle, a classifying knot invariant. Richard Laver, a famous set theorist, studied in 1990's left distributive groupoids of elementary embeddings, see e.g. [Laver 1992]. The monograph *Braids and selfdistributivity*, published in 2000 by Patrick Dehornoy, contains deep results on free left distributive groupoids, applications in the theory of braids, and an extension of Laver's investigations.

The subject remains lively until today: during the last decade, over 100 papers have appeared on *quandles* (or idempotent left distributive left quasigroups in our terminology), mostly with respect to their applications in knot theory. See [Carter] for a survey and prospects.

3. Mediality and modes.

Modes are idempotent algebras, with possibly many operations of arbitrary arity, such that all of them are homomorphisms from the respective power of the algebra into itself. In other words, the operations commute one another. Modes have been extensively

studied by Anna Romanowska, J. D. H. Smith, and their collaborators since 1980's, with various goals and motivations, see [Romanowska and Smith 2002], or [Romanowska 2005]. However, algebras with pairwise commuting operations appeared in works of many other mathematicians in various contexts.

Most notably, in algebras with a binary operation, the property that $*$ commutes with itself is described by the identity

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

called *mediality* by most. The medial law was noticed by Sushkevich and Murdoch in their pioneering works of 1930's, in the context of quasigroups. More mathematicians discovered the topic in 1950's, often in connection to abstract properties of arithmetic mean. Many results on medial groupoids were obtained by the Prague algebraic group, culminating in the treatise [Ježek and Kepka 1983], containing important results on linear representations, structural results for various subclasses (commutative, cancellative, divisible) and a classification of simple medial groupoids. Many results obtained in 1980's and 1990's in Warsaw were collected in the book [Romanowska and Smith 2002], including the theory of affine and quasi-affine representations. Keith Kearnes studied modes by methods of universal algebra in 1990's, see e.g. [Kearnes 1999]. Most results however hide in scattered papers under various nick names, and new papers keep appearing in a somewhat weaker current than in the case of selfdistributivity.

1. $\cap$ (2. $\cup$ 3).

The intersection refers to medial and/or selfdistributive quasigroups. Both were one of the first classes of non-associative algebras to be ever considered, see above. The first important result was the Toyoda-Murdoch-Bruck theorem, found independently by the three men in 1940's, stating that medial quasigroups can be derived from abelian groups taking the operation

$$a * b = f(a) + g(b) + c,$$

where f, g are two commuting automorphisms and c a constant. The theorem was generalized in many ways, including a representation of both left and right distributive quasigroups by commutative Moufang loops [Belousov 1967]. A different kind of powerful representation was discovered for left distributive quasigroups by V. M. Galkin [Galkin 1979], on cosets of groups. It is often the case that quasigroups from a certain class are modeled using groups or a sort of weakly associative loops, and the representation theorem is used to prove properties of the class.

Methods.

Most researchers in non-associative algebra use the efficient language of *universal algebra*, including the notions of homomorphism and congruences, structural concepts such as direct and subdirect decompositions, the construction of free algebras using terms and identities, etc., although the advanced methods of modern universal algebra (tame congruence theory, commutator theory, etc.) have found little use so far.

We decided to comment on two powerful methods used in non-associative algebra. *Structure theory* describes objects of an abstract class, often by representing (some of) them using objects of a different, better known, class. Through representations, problems are often translated to a different area of algebra, such as group theory, and solved there.

The second technique we wish to point out is *formal equational reasoning*, including the use of automated theorem provers.

Structure theory and representations.

There is no formal definition of what structure theory means, and we do not intend to give one. For an abstract class of algebras, the general aim is to understand how its objects look like, by means of *decomposition* (congruences and factoralgebras, various forms of products, combinatorial constructions, etc.), *representation* of indecomposable objects, and so on. It is often useful to describe structural elements, such as simple and subdirectly irreducible algebras. The outcome of a structural result may for instance be counting objects up to isomorphism, determination of abstract properties, etc.

There are many ways the term "representation" is used in literature. The general aim is to describe members of one class using a construction over members of another class, usually far better known. Typical constructions involve reducts, embeddings, factors, sums, etc. Typical target classes are modules, groups and other mainstream structures.

To show some examples, note that the classical *Toyoda-Murdoch-Bruck theorem*, mentioned earlier, says that every medial quasigroup is isomorphic to an algebra $(M, *)$, where $*$ is a binary affine function over a module on the set M (over the endomorphism ring of an abelian group). Many properties, such as counting (small) finite medial quasigroups, can be derived easily.

A more complicated result of this sort is the *Galkin's theorem*, stating that every left distributive quasigroup $\mathbf{Q}$ is isomorphic to an algebra $(G/N, \circ)$, where G is the left multiplication group of $\mathbf{Q}$, N is the stabilizer of a fixed element e and

$$aN \circ bN = aea^{-1}bN.$$

The representation was recently used by J. Vlachý to explain why the smallest non-medial left distributive quasigroup has 15 elements. A similar representation can be derived for connected quandles (i.e., those where the left multiplication group acts transitively) too, and L. Vendramin used it recently to compute the number of connected quandles up to order 35, using the computer system GAP and the (built-in) classification of transitive groups of degree ≤ 35.

A different example of a structural result is *the symmetry-by-mediality theorem* for distributive groupoids [Ježek and Kepka 1984]. Every idempotent distributive groupoid G has a congruence α such that G/α is medial and all blocks of α are Steiner quasigroups. One of the consequences is, for instance, that free idempotent distributive groupoids are cancellative and thus embed, in a way, into commutative Moufang loops.

Representation problems.

A complementary question can be asked: given a representation method, which algebras can be represented? Some of the general results have important consequences in non-associative algebra.

For example: which algebras admit a representation by affine functions over a module? An algebra $\mathbf{A}$ is called *quasi-affine*, if there is a module $\mathbf{M}$ over a ring $\mathbf{R}$ such that $A \subseteq M$ and all operations of $\mathbf{A}$ can be represented by affine functions, i.e., by functions

$$f(x_1, \ldots, x_n) = c + r_1x_1 + \cdots + r_nx_n,$$

for some scalars $r_1, \ldots, r_n \in R$ and a constant $c \in M$. An algebra is called *affine*, if moreover $A = M$ and the two algebras are polynomially equivalent, i.e., they have the

same set of derived (polynomial) operations. (Indeed not all algebras are quasi-affine: for instance, a group is quasi-affine iff it is abelian, and if so, it is actually affine.)

Affine representations have a long history. The Toyoda-Murdoch-Bruck theorem actually says that medial quasigroups are affine (over a commutative ring). Kepka and Němec studied affine quasigroups over general rings already in 1970's, and in this context J. D. H. Smith (and in another context H. P. Gumm soon after) realized the connection between affine representability and the abstract condition that is now called abelianess. While it is easy to see that quasi-affine algebras are abelian, the converse in not true, although the two notions are known to be equivalent under many additional assumptions, e.g., for algebras that have a weak near unanimity term [Stronkowski and Stanovský 2010], or that are simple idempotent [Kearnes 1996]. The problem is often refered to as "abelian iff quasi-affine" [Szendrei 1998], and the general aim is, to determine conditions, when the equivalence holds, or provide counterexamples, when it does not.

A more general (and less powerful) type of representation is using semimodules over semirings, instead of modules. It was proved in [Ježek 1979] that all algebras are representable this way. How about restricting to commutative semirings? What we obtain is a proper class of modes, characterized independently in [Stanovský 2009] [Stronkowski 2009]. Characterizing algebras representable by modules over commutative rings remains an open problem; this is in fact equivalent to determine whether "abelian iff quasi-affine" holds for modes.

Equational reasoning.

Many important classes of non-associative algebras can be axiomatized using a finite set of equations. For example, quasigroups can be axiomatized using auxilliary operations $/, \backslash$ for solutions of the equations $a * x = b$ and $y * a = b$, with axioms

$$x\backslash(x * y) = y,\ x * (x\backslash y) = y,\ (y * x)/x = y,\ (y/x) * x = y.$$

Selfdistributivity is an equation, and so is mediality, or more generally, the fact that two operations commute. More importantly, surprisingly many properties can be formalized in first order logic within the theory we study, often using only equations. For example, a group is nilpotent of class 2 iff it satisfies the equation $xyx^{-1}y^{-1}z = zxyx^{-1}y^{-1}$, and analogously one can axiomatize nilpotent groups of an arbitrary (fixed) class.

While the problem whether a given equation follows from a given set of equational axioms is undecidable, there are fairly efficient software systems that perform the job, and, occasionally, succeed in finding highly non-trivial proofs. Automated theorem provers (both equational, such as Waldmeister, and for general first order logic, e.g. Prover9, E, Vampire) found their way into mathematical research, supporting proofs of several important theorems, mostly in loop theory. A thorough survey of methods and results can be found in [Phillips and Stanovský 2010]. Here we mention one of the most important theorems proved with assistance of automated reasoning.

It was a major open problem for several decades, whether diassociative automorphic loops satisfy the Moufang laws. [Kinyon et al. 2002] gave affirmative answer, by first showing that diassociative automorphic loops have so called inverse property, which can be stated using only finitely many equations (unlike diassociativity), and then used a theorem prover, Otter, to assist reasoning in this class. It is worth noticing that unlike Otter a decade ago, the current version of the Waldmeister system can prove the theorem straight from its axioms within minutes, showing the advance in both software development and computer power.

Concluding remarks.

I tried to present the field of non-associative algebra as a lively subject, with many different motivations and goals, using a variety of techniques. I would like to point out, once again, the many connections it has to other fields. Most of all, it is group theory, providing both tools and motivation, particularly in the theory of loops. No less motivation provides geometry: low dimensional topology (braids, knots and selfdistributivity), differential geometry (smooth binary systems, omitted in my text), projective geometry. And I also find interesting the many ways the selfdistributive law has appeared in various subjects of mathematics (such as Laver's groupoids of elementary embeddings). I believe the interactions provide an endless source of inspiration for future research in non-associative algebra.

This text is based on the introduction of my habilitation thesis (Charles University in Prague, 2011).

Bibliography.

V. D. Belousov, *Osnovy teorii kvazigrupp i lup*, Nauka Moskva, 1967 (Russian).

R. H. Bruck, *A survey of binary systems*, Springer Berlin, 1958.

J. S. Carter, *A survey of quandle ideas*, to appear.

O. Chein, H. O. Pflugfelder, J.D.H. Smith (eds.), *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, 1990.

P. Dehornoy, *Braids and Self-Distributivity*, Progr. Math. 192, Birkhauser Basel, 2000.

S. Gagola, J. Hall, *Lagrange's theorem for Moufang loops*, Acta Sci. Math. (Szeged) 71/1-2 (2005), 45-64.

V. M. Galkin, *Levodistributivnye kvazigruppy konechnogo poryadka*, Matematicheskie Zametki, 51 (1979), 43–54.

A. Grishkov, A. Zavarnitsine, *Lagrange's theorem for Moufang loops*, Math. Proc. Cambridge Philos. Soc. 139/1 (2005), 41-57.

J. Ježek, *Terms and semiterms*, Comment. Math. Univ. Carolin. 20/3 (1979), 447-460.

J. Ježek, T. Kepka, P. Němec, *Distributive groupoids*, Rozpravy ČSAV, 91/3 (1981).

J. Ježek, T. Kepka, *Medial groupoids*, Rozpravy ČSAV, 93/2 (1983).

J. Ježek, T. Kepka, *Distributive groupoids and symmetry-by-mediality,* Algebra Universalis 19/2 (1984), 208-216.

D. Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Alg. 23 (1982), 37–66.

K. Kearnes, *Semilattice modes. I. The associated semiring.* Algebra Universalis 34/2 (1995), 220–272.

K. Kearnes, *Idempotent simple algebras*, Lecture Notes in Pure and Appl. Math. 180, Dekker New York, 1996, 529-572.

K. Kearnes, *Subdirectly irreducible modes.* Discuss. Math. Algebra Stochastic Methods 19/1 (1999), 129-145.

M. Kinyon, K. Kunen, J. D. Phillips, *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. 130 (2002), 619-624.

R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Adv. Math. 91/2 (1992), 209–231.

O. Loos, *Symmetric spaces*, J. Benjamin New York, 1969.

S. V. Matveev, *Distributive groupoids in knot theory*, Math. USSR – Sbornik, 47/1 (1984), 73–83.

P. Nagy, K. Strambach, *Loops in group theory and Lie theory*, de Gruyter Berlin, 2002.

H. O. Pflugfelder, *Quasigroups and loops: introduction*, Heldermann Verlag, 1990.
H. O. Pflugfelder, *Historical notes on loop theory,* Comment. Math. Univ. Carolinae 41/2 (2000), 359-370.
J. D. Phillips, D. Stanovský, *Automated theorem proving in quasigroup and loop theory*, Artificial Intelligence Communications 23/2-3 (2010), 267–283.
J. D. Phillips, D. Stanovský, *Bruck loops with abelian inner mapping groups*, to appear in Commun. Algebra.
G. Pickert, *Projective Ebenen*, Springer Berlin, 1955.
A. Romanowska, J.D.H. Smith, *Modes.* World Scientific Publishing, 2002.
A. Romanowska, *Semi-affine modes and modals.* Sci. Math. Jpn. 61/1 (2005), 159–194.
D. Stanovský, *Idempotent subreducts of semimodules over commutative semirings*, Rend. Semin. Mat. Univ. Padova 121 (2009), 33–43.
M. Stronkowski, *Embedding entropic algebras into semimodules and modules*, Internat. J. Algebra Comput. 19/8 (2009), 1025–1047.
M. Stronkowski, D. Stanovský, *Embedding general algebras into modules*, Proc. Amer. Math. Soc. 138/8 (2010), 2687–2699.
Á. Szendrei, *Modules in general algebra*, Contributions to general algebra 10 (1998). 41-53.
J. D. H. Smith, *An Introduction to Quasigroups and their Representations*, Chapman&Hall/CRC Press, 2007.
A. A. Ungar, *Beyond the Einstein Addition Law and Its Gyroscopic Thomas Precession*, Kluwer, 2001.

A note on information sources. It is not always easy to find out what is going on in a field outside one's expertise. Non-associative mathematics is rather fragmented, with no universal forum. The only subject with a developed infrastructure seems to be the theory of quasigroups and loops. To see what are current problems, I recommend visiting websites of the two major conferences in the field: the Loops conference held in Czech Republic, and the Mile High Conference on Non-associative Mathematics, held in Denver, both once in four years.