RESEARCH PROGRAMME

MICHAEL K. KINYON

Although I started my mathematical career as a differential equations specialist (albeit
with an algebraic bent), since about the turn of the millenium, my research has been in
areas which are either part of algebra or closely related to it. First, I have been working
in loop and quasigroup theory, especially using tools and methods of automated deduction.
Second, I have been working in geometric structures related to (non)associative algebras.
And finally, in just the last year, I have also started working in noncommutative lattice
theory and semigroup theory.

In these notes, I will give a brief description of what prior work I have done in these areas
and then follow with future plans.

1. LOOPS AND QUASIGROUPS

1.1. Introduction. A loop is essentially a “nonassociative group”. There are natural ex-
amples, the best known of which is the set of nonzero octonians; these form a loop under
multiplication. Another example is the space of relativistic velocity vectors with Einsteins
velocity addition law. If nonparallel velocities are considered, this structure is a loop, but
not a group.

In most of my work in loop and quasigroup theory, I have used automated deduction
tools, such as McCune’s Otter and its successor Prover9, to assist in proving theorems.
Group theory is too mature a subject for tools like these to be of much use, but loop and
quasigroup theory is relatively young (about 85 years old), and many unsolved problems
are amenable to computer attacks. Most of my work in this has been in collaboration with
others, such J. D. Phillips (Northern Michigan), Petr Vojtěchovský (Denver), and Ken Kunen
(Wisconsin). Since even the basic terminology of loop and quasigroup theory is unfamiliar
to most mathematicians, it would fill several pages to explain exactly what it is we have
accomplished. I will try to fill in some informal definitions along the way, but in some cases,
I will have to appeal implicitly to the reader’s patience.

Some notions used throughout the following discussion: in a loop or quasigroup, the left
and right translations by an element $a$ are permutations defined by $xL_a = ax$ and $xR_a = xa$,
respectively. The multiplication group of a loop $Q$ is the permutation group $\text{Mlt}(Q)$ generated
by each $L_a$ and each $R_a$ for $a \in Q$. The inner mapping group of $Q$ is the subgroup $\text{Inn}(Q)$ of
$\text{Mlt}(Q)$ which fixes the identity element. The most well-studied class of loops are Moufang
loops, which are defined by the identity $(xy)(zx) = (x(yz))x$. For instance, the loop of
nonzero octonions is a Moufang loop.

1.2. Previous Work. To prevent taxing the reader’s patience, I have limited myself to a
sampling of subareas of quasigroup and loop theory, and within that, a sampling of results.
1.2.1. Automorphic Loops. A loop $Q$ is automorphic (or an $A$-loop, for short) if $\text{Inn}(Q)$ is a group of automorphisms of $Q$. Such loops were introduced in 1956 by Bruck and Paige. A loop is diassociative if any two elements generate a group. Bruck and Paige conjectured that every diassociative, automorphic loop is Moufang. As the statement of the conjecture suggests, many problems in quasigroup and loop theory involve trying to show that a given class of loops is somehow related to Moufang loops.

Kunen, Phillips and I affirmatively solved the Bruck-Paige conjecture. We found a proof using the automated deduction tool OTTER, and then carefully “humanized” the computer-generated proof. Humanization is, in some sense, a dogma among some of us who use automated deduction tools to prove theorems. The philosophy is that the point of mathematics is to improve human understanding, and such understanding comes not just from the statements of theorems, but from knowing their proofs. There are obvious limits to this dogma, such as the law of diminishing returns: some computer-generated proofs are too long to warrant a careful human translation. However, in this case, humanization was relatively straightforward, and we were able to produce an understandable proof of the conjecture.

More recently, Jedlička, Vojtěchovský and I found a detailed structure theory for commutative automorphic loops. The key workhorse result, for which we relied on the automated deduction tool Prover9, was showing that in such loops, the product of squares is a square. With this as our starting point, we were able to derive a decomposition theorem (every finite commutative automorphic loop is the direct product of a loop of odd order and a loop of order a power of 2), Lagrange, Sylow, Hall and Feit-Thompson theorems. In a follow-up paper, we gave various constructions of commutative automorphic loops.

1.2.2. Conjugacy closed loops and Buchsteiner loops. A loop $Q$ is conjugacy closed (CC) if the set $\{L_a | a \in Q\}$ of its left translations is closed under self-conjugation, and likewise for the set $\{R_a | a \in Q\}$ of right translations. CC-loops are highly structured, thanks mostly to Basarab’s theorem: the factor of a CC-loop by its nucleus (the set of all elements that associate with every element) is an abelian group.

In a series of papers, Kunen, Phillips and I explored the structure of various types of conjugacy-closed loops (CC-loops). We showed that every finite, nonassociative Moufang CC-loop (extra loop) has nontrivial center and has order divisible by 16. We also established Sylow and Hall theorems. As a follow-up, Kunen and I studied power-associative CC-loops (PACC). (Power-associative means that any subloop generated by at most one element is a group.) We showed that every such loop modulo its nucleus is an abelian group of exponent 12. We also showed that every finite PACC-loop has order divisible by 16 or by 27, and we have classified all loops of those minimal orders.

Buchsteiner loops are closely related to CC-loops, and are defined by the implication $(xy)z = xu \Rightarrow y(zx) = ux$ (or an equivalent identity). Csörgő, Drápal and I studied these loops in considerable detail. A main result is that the factor of a Buchsteiner loop by its nucleus is an abelian group of exponent 4. We constructed non-CC examples where the exponent 4 is achieved. Buchsteiner loops have a robust associator calculus, where the associator $[x, y, z]$ is defined by the equation $(x(yz))[x, y, z] = (xy)z$, which makes assists both in proofs and in constructions of examples.

1.2.3. F-quasigroups. Kepka, Phillips and I also solved an open problem first posed by Belousov in 1965: every loop isotopic to an F-quasigroup is Moufang. F-quasigroups were
introduced in the mid-1940s, and are defined by certain associative-like identities. The study of quasigroups is often “reduced” to the study of loops via isotopy. If a given class of quasigroups is isotopic to a highly structured class of loops, that usually means that the given class of quasigroups is itself highly structured.

1.2.4. **Bol and Bruck loops.** Phillips and I worked with Aschbacher (Cal Tech) on one form of what used to be the outstanding problem in loop theory: to find a finite, simple Bol loop which is not Moufang, or to show that no such loop exists. Bol loops are defined by the equation \((xy)z = x((yz)y)\). Moufang loops are Bol loops, and Moufang loops are, as indicated, relatively well understood. Another important subvariety of Bol loops are Bruck loops, which satisfy \((xy)^{-1} = x^{-1}y^{-1}\). The space of relativistic velocity vectors mentioned in the introductory remarks forms a Bruck loop. Using the classification of finite, simple groups, and following up on earlier work of Aschbacher, the three of us gave a structure theory of finite Bruck loops, modulo the issue of whether or not a nonassociative simple example exists. (An example was later constructed by G. Nagy, much to the surprise of many who suspected that all finite Bruck loops might be solvable.)

1.3. **Future Work.** Again to keep this part of the programme to a manageable size, I will leave off papers which currently have a semi-complete draft.

1.3.1. **Book Project.** Petr Vojtěchovský, Aleš Drápal and I have decided that loop theory has matured to the point where it is time to write a book—perhaps a monograph, but more likely a textbook—describing the state of the art. The existing books are either considerably outdated or too elementary. At the time of writing (Fall 2009), we are in the planning stages.

1.3.2. **Loops with Abelian Inner Mapping Groups.** For finite loops \(Q\) for which \(\text{Inn}(Q)\) is abelian, it is known that the loop \(Q\) is centrally nilpotent and that the highest nilpotency class yet achieved is 3. I am particularly interested in studying this issue within specific loop varieties. Phillips, Vojtěchovský, Bob Veroff and I now have a complete answer for the variety of Moufang loops (building on earlier work of Nagy and Vojtěchovský), and Vojtěchovský and I also have a complete answer for automorphic loops. We wish to extend these descriptions to other loop varieties.

1.3.3. **Automorphic loops.** The outstanding problem in the theory of automorphic loops is whether or not there exist finite, simple, nonassociative automorphic loops. This is open even in the commutative case. In the latter case, it is known that such a loop must have exponent 2, and a few other additional conditions are known as well, but there is not yet enough information to construct an example or to show that a minimal example leads to a contradiction. I am very interested in cracking this problem, particularly in the commutative case, and have been working on it with P. Vojtěchovský.

1.3.4. **Osborn loops.** Osborn loops are a class simultaneously generalizing Moufang and CC-loops. I have been convinced for some time that they are an important variety. Kunen, Phillips and I have obtained many interesting results about them already. The biggest stumbling block to a complete theory is whether or not they are isotopically invariant, that is, if every isotope of an Osborn loop is also an Osborn loop. Maddeningly, this property is known to hold for nearly every important subvariety of the class of Osborn loops. Veroff and I have started an earnest investigation of the isotopy invariance problem. Perhaps the
biggest result (not published) is that in an Osborn loop satisfying \((xy)^{-1} = x^{-1}y^{-1}\), the mappings \(x \mapsto x(xx)\) and \(x \mapsto (xx)x\) are centralizing endomorphisms. This is a sweeping
generalization of one of the foundational results of the theory of commutative Moufang loops.
It will be interesting to see if this generalization has a combinatorial interpretation, just as
commutative Moufang loops are associated to Hall triple systems.

2. Geometry of (Non)associative Algebra

2.1. Introduction. I have been interested for some time in generalizing or finding analogues
of the natural correspondence between Lie algebras and Lie groups to other types of algebras.
For a while, I worked on this problem for Leibniz algebras and more recently (with W.
Bertram) for associative algebras(!) and associative pairs. We are extending that work to
alternative algebras and alternative pairs.

2.2. Previous Work.

2.2.1. The Coquecigrue Problem for Leibniz algebras. A Leibniz algebra is a non-anticommutative
Lie algebra, that is, it is a nonassociative algebra in which the multiplication satisfies a Ja-
cobi identity, but not necessarily skewsymmetry. Lie’s “Third Theorem” (and Cartan’s global
version) constructs for each Lie algebra a corresponding Lie group. One of the outstanding
problems in the theory of Leibniz algebras is to extend Lie’s third theorem to Leibniz al-
gebras. Loday dubbed the mysterious group-like object corresponding to a Leibniz algebra a
“coquecigrue” (a medieval mythical beast).

A. Weinstein and I made an attempt at constructing coquecigrues: to every Leibniz al-
gebra, we associated a smooth loop satisfying certain properties. However, our loop turned
out not to be the coquecigrue, because in the special case where the Leibniz algebra is a
Lie algebra, the corresponding loop structure is not a Lie group. (Roughly speaking, our
construction “integrates” the adjoint representation of a Lie algebra, not the Lie algebra
itself.) Nevertheless, the loop turned out to be interesting on its own, and it illuminated the
difficulties with the general program.

Later, I gave a partial solution to the coquecigrue problem called a Lie digroup. A digroup
is a set with two semigroup operations satisfying certain compatibility conditions. A digroup
is a group if and only if the two operations coincide. It is easy to show that the tangent
algebra structure for a Lie digroup is a Leibniz algebra. However, not all Leibniz algebras can
be obtained this way, which is why digroups are only a partial solution to the coquecigrue
problem. Roughly speaking, the Leibniz algebras that occur as tangent algebras for Lie
digroups are those which split over their ideals generated by squares. Unfortunately, many
of the Leibniz algebras arising in applied mathematics do not have this property. Whatever
the correct notion of coquecigrue turns out to be, it should reduce to the notion of digroup
in the split case.

Recently, I have been giving the Coquecigrue Problem a break to concentrate on other
projects.

2.3. Current and Future Work. It makes more sense to group my most recent work here
together with the future plans, since a large part of the “previous work” was completed
within just the last couple of weeks of the time of writing (Fall 2009).
2.3.1. **Associative geometries.** Wolfgang Bertram (IECN) and I have recently defined and investigated what we think will turn out to be a very important geometric object, called an *associative geometry*. Any associative algebra (or more generally, any associative pair, which would take up too much space to define here) has an associative geometry corresponding to it. Conversely, to any associative geometry, there is a (functorially constructed) corresponding associative pair. This correspondence is analogous to the correspondence between Lie groups and Lie algebras, or between generalized projective geometries (studied by Bertram) and Jordan pairs.

The model of an associative geometry is, in fact, the Grassmannian \( X := \text{Gr}(W) \) of subspaces of a vector space \( W \) over a field. (This generalizes easily to modules, submodules and rings.) What we discovered is that there is a globally-defined *pentary* map \( \Gamma : X^5 \to X \) with remarkable properties. Fixing subspaces \( a, b \in X \), the ternary map \( \Gamma(\cdot, a, \cdot, b, \cdot) : X^3 \to X \) is a semigroud, which can be thought of as a ternary version of a semigroup. Various restrictions of the pentary map to special values give (affine) group structures, such as the standard affine space structure on the set of all complements to a given subspace, or even general linear groups. In fact, an associative geometry is a canonical semigroup completion of a general linear group and its homotopes, viewed as sitting inside an associative algebra.

Taking involutions of associative algebras and associative geometries into account, we can construct canonical semigroup completions for all classical groups and their homotopes (and, in certain cases, for their analogs in infinite dimension or over general base fields or rings).

There are many directions that this new powerful approach can take us. Firstly, it invites a new look at the geometry underlying Jordan pairs. From Bertram’s earlier work, it is already known that the correct geometric object associated to a Jordan algebra or Jordan pair is a generalized projective geometry. However, part of the broader success of the theory of Jordan pairs is that it allows one to work over base rings of arbitrary characteristic, particularly 2, and Bertram’s earlier theory doesn’t allow this. However, in the same way as associative pairs give rise to Jordan pairs, associative geometries give rise to “Jordan geometries”. New features are introduced from specializing the pentary map. These features can be used to give a new axiomatic foundation of “Jordan geometries”. In this theory, the grouts from the associative theory will be replaced by symmetric spaces.

2.3.2. **Alternative Geometries.** Generalizing associative algebras are *alternative algebras*, which are defined by the identities \( x( (xy)z ) = (x(x)y)z \) and \( (x(y)y)z = x(y(y)z) \). The best known example is the (say, real) octonions. There is a notion of pair in the alternative case just as in the associative case. This brings up the natural question: what is the corresponding notion of *alternative geometry*? Just as an associative geometry is a globally-defined pentary structure that specializes to semigrouds (which are families of semigroups) and grouts (which are families of groups), we expect that an alternative geometry has a globally-defined structure that specializes to to families of Moufang loops and their “semiloop” generalizations. We have already had some success in this direction: we know now what the correct ternary notion of Moufang loop is, and it corresponds to the axiomatics of alternative pairs in the same way that the ternary notion of group, namely grout, corresponds to the axiomatics of associative pairs.
3. Noncommutative Lattices and Semigroup Theory

This is a relatively new direction for me. I do not have previous work to refer to, but will instead describe current and future projects.

3.1. Noncommutative Lattices. A noncommutative lattice \((S, \lor, \land)\) is a set \(S\) with two idempotent semigroup operations on it which satisfy some absorption laws. The best known type are skew lattices, which satisfy \(x \land (x \lor y) = x = x \lor (x \land y)\) and \((x \lor y) \land y = y = (x \land y) \lor y\). Most other types of noncommutative lattices either generalize or specialize skew lattices in some way. There are natural examples of skew lattices arising in ring theory and logic. Noncommutative lattice theory seeks to understand these structures, drawing upon traditional (commutative) lattice theory, semigroup theory and (quasi-)order theory.

3.1.1. Cancellative skew lattices. A skew lattice is said to be cancellative if it satisfies the implication: \(x \land y = x \land z, x \lor y = x \lor z \Rightarrow y = z\) and also its mirror image. There are various generalizations and specializations of this notion, all of which coincide in the commutative case. In commutative lattices, cancellativity is equivalent to distributivity. This is not true in the noncommutative setting; neither notion contains the other as a special case.

An open problem was whether or not cancellative skew lattices (and their various generalizations) actually form an equationally defined variety as opposed to just a quasi-variety. I first became aware of this problem from some unpublished notes of M. Spinks. I began to work on it using PROVER9 and began corresponding with J. Leech (who in some sense is the founder of the contemporary theory of skew lattices), M. Spinks and K. Cvetko-Vah. The four of us together not only solved the problem as posed affirmatively, but also came up with a “forbidden subalgebra” characterization of cancellative skew lattices, analogous to the characterization of distributive commutative lattices in terms of which sublattices they do or do not contain.

3.1.2. Distributive skew lattices. Buoyed by our success, Leech and I decided to see if we could find a similar “forbidden fruit” characterization of distributive skew lattices, which are defined by the identity \(x \land (y \lor z) \land x = (x \land y \land x) \lor (x \land z \land x)\) and its dual obtained from switching \(\land\) and \(\lor\). We are still working on this, because it has turned out to be rather involved. Unlike the cancellative case, where there is a finite list of forbidden subalgebras, in the distributive case there are infinite families of forbidden subalgebras. Further, we still don’t have a complete characterization, even for the case of linear distributivity. (A skew lattice is linearly distributive if every skew subchain is distributive.) Leech and I hope to settle this completely within the next few months.

3.1.3. Modular skew lattices. Another open problem in the theory of skew lattices is: what is the correct notion of modularity for skew lattices? The difficulty here is in the lack of natural models. A natural model for a modular, nondistributive commutative lattice is the lattice of subspaces of a vector space. There is no known analog in the noncommutative setting; “natural” skew lattices are often distributive.

Nevertheless, there does seem to be some hope that the correct notion is within reach. It seems quite likely that linear modularity, the modular analog of linear distributivity, coincides with a notion called categoricity defined earlier by Leech. In addition, some formal guesswork as to what modular identities should look like have led to some results that seem
to be the correct generalizations of the distributive case. Leech and Cvetko-Vah and I hope to look at this in more detail as soon as Leech and I finish the distributivity project.

3.2. Semigroup Theory. In the summer of 2009, I was invited to spend some time at the Center of Algebra at the University of Lisbon as the guest of João Araújo, ostensibly to give a lecture series on the use of automated deduction in algebra. I indeed gave such a series, but at the same time, Araújo introduced me to various problems in semigroup theory which lend themselves well to automated deduction methods. The following subsections essentially describe several papers we are working on.

3.2.1. Tamura bigroupoids. We began with a problem which is essentially a follow-up to earlier work by Araújo and McCune. If, in an inverse semigroup \((S, \cdot, -1)\), we define term operations by \(x \star y = x^{-1}y\) and \(x \circ y = xy^{-1}\), then it turns out that the inverse semigroup itself can be completely axiomatized in terms of \(\star\) and \(\circ\). This was a result of Tamura, and so the resulting structure \((S, \star, \circ)\) is called a Tamura bigroupoid. Araújo and McCune showed that there is a 3-base for the variety of Tamura bigroupoids, but left unanswered whether or not the proof of this fact could be humanized. Araújo and I found a human proof, as well as a solution to another problem posed by Tamura.

3.2.2. Characterizing inverse semigroups. Araújo and McCune also showed that there is a 3-base for the variety of inverse semigroups, but again left unresolved the humanization of a proof. Araújo and I found a human proof, and have expanded the project even further. The conjecture is that there is, in fact, no 2-base for the variety of inverse semigroups, and we think we are quite close to a proof of this fact. We have, however, found a 2-base for commutative inverse semigroups. Also open is whether or not there exists a weak 2-base for inverse semigroups; in a weak 2-base, \(-1\) is not necessarily the natural inverse operation, but may still be an inverse in the broader sense that the term is used in the theory of regular semigroups.

3.2.3. A problem of Schein. In 1978, B. Schein gave a characterization of a certain type of semisimple idempotent semigroups. His characterization involved an infinite sequence of conditions which can be interpreted as referring to minimal possible lengths of certain types of paths in the commutativity graph of the semigroup. The commutativity graph has vertices the elements of the semigroup and two elements are connected by an edge if they commute. Schein conjectured that each of his infinite sequence of conditions is independent of the others. Araújo and I showed that Schein is essentially correct; while there is a dependency relation between two of the conditions of small order, the others are indeed independent. We constructed the necessary examples in small cases using the finite model builder MACE4 and then “reverse engineered” the examples to get general constructions.

3.2.4. Conjugation in semigroups. There are many ways of generalizing the group theoretic notion of conjugacy to semigroups. Together with J. Konieczny, Araújo and I are working on describing some of these, including characterizing when they coincide with the identity relation or the trivial relation, as well as describing conjugate pairs of elements in transformation monoids.
3.2.5. $\ast$-E-inversive semigroups. This is perhaps the most exciting of the various semigroup projects I am now involved in. In Araújo’s opinion, this particular project has the potential to open up a whole new area of semigroup theory.

A semigroup $S$ is said to be regular if for every $x \in S$, there exists $y \in S$ such that $xyx = x$. Of course in general there is more than one such $y$. Nordhal and Scheiblich had the idea of considering regular semigroups to be unary semigroups $(S, \cdot, ')$ satisfying the associativity law and the extra identity $xx'x = x$. However, while we now we have a variety, for a given regular $(S, \cdot)$ there might be a two different unary operations defined in $S$ such that both satisfy $xx'x = x$. To distinguish the two types, the unary semigroups $(S, \cdot, ')$ are sometimes called $\ast$-regular or other names. In any case, in our view, the problem of having the same underlying semigroup for different $\ast$-regular semigroups is small compared with the gains that can be achieved by considering regular semigroups as unary semigroups.

Araújo and I have begun to apply the same idea to E-inversive semigroups thus introducing the class of $\ast$-E-inversive semigroups. A semigroup $S$ is said to be E-inversive if for every $x \in S$ exists $y \in S$ such that $y = yxy$. We define a unary semigroup $(S, \cdot, ')$ is said to be $\ast$-E-inversive if it satisfies $x'xx' = x'$ and the implication $xyx = x \Rightarrow xx'x = x$. Roughly speaking, the implication means that if $x$ is a regular element, then its acts as expected.

We have been able to say quite a bit about the structure of various subclasses of the class of $\ast$-E-inversive semigroups. For instance, we have been able to show that the set of regular elements is a subsemigroup iff the set of idempotents generates a regular subsemigroup iff the product of any two idempotents is regular iff the product of any idempotent and any regular element is regular. We also think we have defined the correct generalizations of inverse semigroups and of completely regular semigroups in the $\ast$-E-inversive setting.