

MAIN SPEAKERS

Advances in Loop Rings and their Loops

Edgar G. Goodaire (Memorial University, St. John's, Canada)

We describe some of the advances in the theory of loops whose loop rings satisfy “interesting” identities that have taken place in the past ten years. The major emphasis is on Bol loops that have strongly right alternative loop rings and on “Jordan loops,” a hitherto largely ignored class of commutative loops some of whose loops rings satisfy the Jordan identity $(x^2y)x = x^2(yx)$. We raise a number of open questions and include several suggestions for further research.

Central automorphisms of Latin square designs and loops

Jonathan I. Hall (Michigan State University, USA)

We discuss special automorphisms of Latin square designs or equivalently the 3-nets that are dual to them. We focus on the relationships between these automorphisms and the algebraic properties of the associated loops, especially Moufang loops

Structure of some p-local subgroups in the Monster

Alexander A. Ivanov (Imperial College, London, UK)

J.H.Conway made use of the Parker loop to describe the normalizer in the Monster of an elementary abelian subgroup of order 4. T.M.Richardson used similar technique to describe the normalizers of certain subgroups in the Monster of order p^2 . I intend to discuss these result along with some recent development.

Loops related to geometric structures

Helmut Karzel (Technical University of Munich, Germany)

There are many connections between loops and geometries:

- One can derive loops from several geometries and then use these loops for a ”coordinatization” of the geometries,
- one can start from loops with certain properties and associate to them geometric structures or
- one can use geometric structures - for instance ”chain structures” or ”graphs” - in order to represent loops.

Some of these relations I like to discuss here.

F–quasigroups

Tomas Kepka (Charles University, Prague, Czech Republic)

Coauthors: M. Kinyon (University of Denver, USA), J. D. Phillips (Wabash College, USA)

All F–quasigroups are isotopic to Moufang loop. Both these isotopes and those loops are of special type.

The numbers of Latin squares, quasigroups and loops

Brendan McKay (Australian National University, Canberra, Australia)

The problem of counting Latin squares was studied by Euler more than 220 years ago and interest has not declined since then. Since the multiplication tables of quasigroups are Latin squares, the counting of quasigroups and loops is closely related.

Two types of enumeration are involved, which can be called *labelled* and *unlabelled*. In labelled enumeration, each Latin square is regarded as distinct from all others. The most recent result, by the speaker and Ian Wanless, is that the number of Latin squares of order 11 is 776966836171770144107444346734230682311065600000.

In the case of unlabelled enumeration, various definitions of equivalence are defined and one tries to determine the number of equivalence classes. The best known types of equivalence for Latin squares are isotopism and paratopism. If the Latin squares are interpreted as the tables of quasigroups or loops, the obvious equivalence relation is isomorphism. We will explain how counts of all these equivalence classes up to order 10 have been obtained by the speaker with Alison Meynert and Wendy Myrvold. The numbers of isomorphism classes of loops and quasigroups of order 10 are 20890436195945769617 and 2750892211809150446995735533513, respectively.

All of the techniques can be extended to d -ary operations. With Ian Wanless, the author has enumerated d -ary Latin hypercubes, quasigroups and loops for $d \leq 5$ and order $n \leq 5$.

Gyrogroups, the Special Grouplike Loops in the Service of Hyperbolic Geometry and Einstein's Special Theory of Relativity

Abraham A. Ungar (North Dakota State University, Fargo, USA)

In this era of an increased interest in loop theory, the Einstein velocity addition law has fresh resonance. One of the most fascinating aspects of recent work in Einstein's special theory of relativity is the emergence of Special grouplike loops. The special grouplike loops, known as *gyrocommutative gyrogroups*, have thrust the Einstein velocity addition law, which previously has operated mostly in the shadows, into the spotlight. We will find that Einstein (Möbius) addition is a gyrocommutative gyrogrooup operation that forms the setting for the Beltrami-Klein (Poincaré) ball model of hyperbolic geometry just as the common vector addition is a commutative group operation that forms the setting for the standard model of Euclidean geometry. The resulting analogies to which the special grouplike loops give rise lead us to new results in (i) hyperbolic geometry; (ii) relativistic physics; and (iii) quantum information and computation.

SUBMITTED ABSTRACTS

Identities with permutations providing linearity (alinearity) of quasigroups

Galina Belyavskaya (Academy of Sciences, Moldova)

Coauthor: A. Tabarov (Tajik State National University)

Linear quasigroups are a particular case of quasigroups isotopic to groups and arise by investigation of many questions of the quasigroup theory and in applications.

A quasigroup (Q, \cdot) is called linear (alinear) (over a group) if there exist a group $(Q, +)$, its automorphisms (antiautomorphisms) φ, ψ and an element $c \in Q$ such that $xy = \varphi x + c + \psi y$. A quasigroup (Q, \cdot) is linear (alinear) on the left (on the right) if φ (ψ) is an automorphism (an antiautomorphism) and ψ (φ) is a permutation of Q . We call such quasigroups semilinear (semialinear) and use the identities with permutations in (Q, \cdot) of the form: $\alpha_1(\alpha_2(x \otimes_1 y) \otimes_2 z) = \alpha_3 x \otimes_3 \alpha_4(\alpha_5 y \otimes_4 \alpha_6 z)$, where $\alpha_i, i \in \overline{1, 6}$, are permutations of Q and $\otimes_j = (\cdot)$ or $\otimes_j = (*)$, $j \in \overline{1, 4}$ ($x * y = y \cdot x$), for finding the identities providing semilinearity, semialinearity, linearity or alinearity of a quasigroup (Q, \cdot) over a group (an abelian group).

A quasigroup (Q, \cdot) is linear on the left (on the right), if one of the following identities holds: $\alpha_1(xy \cdot z) = \alpha_3 x \cdot \alpha_4(\alpha_5 y \cdot \alpha_6 z)$, $xy \cdot z = \alpha_3 x \cdot \alpha_4(\alpha_5 y * \alpha_6 z)$; $(\alpha_2(xy) \cdot z = \alpha_3 x \cdot (\alpha_5 y \cdot \alpha_6 z)$, $\alpha_2(x * y) \cdot z = \alpha_3 x \cdot (\alpha_5 y \cdot \alpha_6 z)$); (Q, \cdot) is linear if the following identity holds: $\alpha_1(xy \cdot z) = \alpha_3 x \cdot (\alpha_5 y \cdot \alpha_6 z)$ where $\alpha_i, i \in \overline{1, 6}$, are any permutations of Q .

Similar identities are pointed for the rest types of linearity (alinearity). These results allow to describe infinite number of identities (without permutations) in a primitive quasigroup $(Q, \cdot, \setminus, /)$ providing linearity of any given type over a group or over an abelian group of the quasigroup (Q, \cdot) . From these results it also follows that the known identities, involving four variables, in a primitive quasigroup $(Q, \cdot, \setminus, /)$ which characterize linearity on the left (on the right), linearity and alinearity of (Q, \cdot) are sufficient if to fix a value of the one suitable variable.

On power sets and s-systems of n-quasigroups

G. Belyavskaya (Academy of Sciences, Moldova)

In the case of n -ary quasigroups for $n > 2$ it is possible to consider distinct versions of orthogonality. The pairwise orthogonality of n -quasigroups is an algebraic equivalent of the pairwise orthogonality of n -dimensional hypercubes.

Two n -operations A and B defined on a set Q of order m are said to be orthogonal if the pair of equations $\{A(x_1^n) = a, B(x_1^n) = b\}$ has exactly m^{n-2} solutions for any $a, b \in Q$.

We introduce and study the (k) -power sets of n -quasigroups $\Sigma_k = \{A, A^2, \dots, A^s\}$ for $k \in \overline{1, n}$ with respect to the k -multiplication \oplus_k of n -operations ($A \oplus_k B = A(x_1^{k-1}, B(x_1^n), x_{k+1}^n)$).

Any (k) -power set of n -quasigroups is pairwise orthogonal.

The following result gives distinct possibilities for construction of quasigroup (k) -power sets using binary groups.

Let (Q, A) be a finite n -quasigroup of the form $A(x_1^n) = \alpha_1 x_1 \cdot \dots \cdot \alpha_{k-1} x_{k-1} \cdot x_k \cdot \alpha_{k+1} x_{k+1} \cdot \dots \cdot \alpha_n x_n$ for some fixed $k \in \overline{1, n}$, where α_i is a permutation of Q for every $i \in \overline{1, n}$, $i \neq k$, (Q, \cdot) is a binary group. Then Σ_k is a (k) -power set of n -quasigroups if and only if in the group (Q, \cdot) the mapping $x \rightarrow x^l$ is a permutation for each $l \in \overline{2, s}$.

We also generalize the Belousov's one-sided S -systems of binary quasigroups: A system $\Sigma_k = \{E_k, A_1^s\}$, $s \geq 1$, $A_i, i \in \overline{1, s}$, are n -quasigroups, given on a set Q , $E_k(x_1^n) = x_k$, is called a (k) - S -system if Σ_k is a group with respect to the k -th multiplication of n -operations.

It is proved that a (k) - S -system Σ_k , $n \geq 3$, $|Q| = m$, is a pairwise orthogonal set of n -operations, $s \leq m - 1$ and for any $n \geq 3$, any $k \in \overline{1, n}$ there exist (k) - S -systems of n -quasigroups of each prime order $m = p \geq 3$ with $s = m - 1$ of n -quasigroups.

Cyclic entropic quasigroups

G. Binczak (Warsaw University of Technology, Poland)

Coauthor: J. Kaleta (Warsaw Agricultural University, Poland)

Using equivalence between some entropic quasigroups and abelian groups with involution I describe cyclic entropic quasigroups such that $x \cdot 1 = x$ and $1 \cdot (1 \cdot x) = x$.

A connection between a finite faithful A_l -left-envelope $\xi = 3D(G, H, L)$ and the lattice of subgroups of H

Raffaello Caserta (Università degli Studi di Palermo, Italy)

We term the triple $\xi = 3D(G, H, L)$ a faithful left-envelope when G is a (finite) group, H a subgroup of G with

trivial core $C_G H$ and $L \subseteq G$ a set of representatives of left cosets of G with respect to H which contains the identity 1_G and generates G .

Let Ω be the set of all G -conjugated subgroups of H and fix an element $x \in L \setminus \{1_G\}$. Since $C_H(x) = 3DH \cap H^x$, it is worth to consider the action

$$\begin{aligned} G \times \Omega &\rightarrow \Omega \\ (g, H) &\mapsto H^g \end{aligned}$$

In this view, since $h^g \in H$ implies $h \in C_H(x)$ for some $x_1 = nL$, we have

Theorem. The following are equivalent:

- i. L is H -invariant with respect to the action of H on L by conjugation;
- ii. $\delta_{g|C_H(x)} = 3D\delta_{h|C_H(x)}$ for all $g \in G$ and some $h \in H, x \in L$;

δ_g, δ_h being the inner automorphisms of G supplied by $g, h_1 = nG$.

Denote by $L(H)$ the lattice of subgroups of some finite non-abelian group H . We can use the previous

theorem to construct a finite left-loop which satisfies the well-known $A_l =$ condition and admits H/N as group of

left-deviations for a suitable normal subgroup N .

Bol loops with a large left nucleus

Orin Chein (Temple University, Philadelphia, USA)

Coauthor: Edgar G. Goodaire (Memorial University, St. John's, Canada)

Possession of a unique nonidentity commutator/associator is a property which dominates the theory of loops whose loop rings, while not associative, nevertheless satisfy an identity with a repeated variable. Indeed, until now, with the exception of some ad hoc examples, the only known class of Bol loops whose loop rings satisfy the right Bol identity have this property. In this paper, we identify another class of loops whose loop rings are "strongly right alternative" and present various constructions of these loops.

Abelian inner mappings and Buchsteiner loops

Piroska Csorgo (Eotvos University, Budapest, Hungary)

The study of the nilpotency class of a loop Q with abelian $\text{Inn}(Q)$ in case the factor loop Q/N is abelian -where N is the nucleus of Q . The description of the structure of $\text{Mlt}(Q)$, if Q is a Buchsteiner loop of nilpotency class 3 with abelian $\text{Inn}(Q)$. The proof of that the minimal order of a Buchsteiner loop Q with before mentioned properties and with some reasonable conditions is 128. Giving the construction of $\text{Mlt}(Q)$, where Q is a Buchsteiner loop of order 128 and nilpotency class 3 with abelian inner mapping group.

On products of partially ordered quasigroups

Milan Demko (Prešov University, Slovakia)

There are given necessary and sufficient conditions for a direct product and a lexicographic product of a family of partially ordered quasigroups to be a left positive (right positive) quasigroup. Further, conditions for a lexicographic product of partially ordered quasigroups to be a Riesz quasigroup are discussed.

Middle translations in the study of quasigroups

Ivan Ivanovich Deriyenko (Kremenchuk State Polytechnical University, Ukraine)

In the study of quasigroups left and right translations often are used. We propose to use middle translations. A permutation $\varphi_a : Q \rightarrow Q$, $x \cdot \varphi_a x = a$ for all $x \in Q$ is called a *middle translation*. See, V.D. Belousov. On a group associated to a quasigroups. *Matem. Issledovaniya*, 4:3, Shtiinta, Kishinev, (1969), 21-39 (in Russian).

In I.I. Deriyenko, Necessary conditions of the isotopy of finite quasigroups, *Mat Issled.* No. 120, Kishinev, Stiinta, 1991, 51-63, a concept of *quasigroup spin* was introduced. A permutation $\varphi_{ab} = \varphi_a \varphi_b^{-1}$ is called a *spin of the permutations φ_a and φ_b* .

Using spins it is possible to obtain invariants of quasigroups under isotopy. Some results from the book J. Dénes, A. D. Keedwell, *Latin Squares and their Applications*, Budapest, Akadémiai Kiadó, 1974 about quasigroups of order six are improved.

On the basis of spins the concept of a spectrum of a quasigroup is introduced. The order of a spectrum of a quasigroup shows a degree of its associativity. If the order of a group is equal to n , then the order of its spectrum is equal to n . If the order of spectrum of a quasigroup is "small", then degree of associativity of this quasigroup is "big".

Formulas for loop operations

Aleš Drápal (Charles University, Prague)

It has been a habit in loop theory to restrict the description of various loop classes to the question of orders (i.e. for which orders an example exists) and to the enumeration of small order examples. I will argue that there are important loop classes where the total description is possible and that the efforts to find such a description help to bring the loop theory into contact with mainstream mathematics. This thesis will be illustrated by a number of cases. For the first time I will discuss the results pertaining to the description of loops Q with $Z(Q) = 1$ and $|\text{Inn}(Q)| = pq$, where $q < p$ are primes.

Loops on spheres having a compact-free inner mapping group

Agota Figula (University of Debrecen, Hungary)

Coauthor: Karl Strambach (University of Erlangen, Germany)

We prove that any topological loop homeomorphic to a sphere or to a real projective space and having a compact-free Lie group as the inner mapping group is homeomorphic to the circle. Moreover, we classify the differentiable 1-dimensional compact loops explicitly using the theory of Fourier series.

Construction of huge quasigroups of orders 2^{256} , 2^{384} and 2^{512} for construction of fast cryptographic hash functions

Danilo Gligoroski (Norwegian University of Science and Technology, Norway)

On the second NIST Hash Workshop a family of hash functions Edon- \mathcal{R} was proposed. The initial design was by general quasigroups of relatively small order (up to 256), and the approach was without concrete realization of those hash functions. No concrete measurements about the speed of those hash functions were given, although the authors admitted that computational speed of their design is slow.

Recently on IACR eprint archive a fast implementation of Edon- \mathcal{R} was described by constructing quasigroups of huge order (2^{256} , 2^{384} and 2^{512}) only by using bitwise operations on 32 bit values (additions modulo 2^{32} , XORs and left rotations). In my talk I will explain this construction and I will post several design challenges that can lead to even more efficient and secure designs of cryptographic hash functions.

Modelling designs by means of (2,n)-quasigroups

Lidija Goracinova-Ilieva (Pedagogical Faculty, Stip, Macedonia)

Coauthor: Smile Markovski (Ss Cyril and Methodius University, Skopje, Macedonia)

Let k and n be positive integers, $k \leq n$. An algebra \mathbf{A} is a (k, n) -algebra if every subalgebra of \mathbf{A} , which is generated by k distinct elements has exactly n elements. A variety of algebras is a (k, n) -variety if its algebras are (k, n) -algebras. If \mathcal{V} is a (k, n) -variety of groupoids, $k < n$, then $k = 2$ and every \mathcal{V} -groupoid is a quasigroup. The problem of the existence of $(2, n)$ -variety of groupoids is solved for $2 \leq n \leq 9$. The quasigroups of $(2, n)$ -varieties are used for obtaining various combinatorial designs: Mendelsohn designs, Steiner systems, and other 2-designs.

3-homogeneous Latin trades

Terry Griggs (The Open University, UK)

Coauthors: M.J.Grannell (The Open University, UK), A. Drápal (Charles University, Praha)

. Let T be a partial Latin square and L be a Latin square with $T \subseteq L$. Then T is a *Latin trade* if there exists a partial Latin square T' with $T \cap T' = \emptyset$ such that $(L \setminus T) \cup T'$ is also a Latin square. A Latin trade is *minimal* if it contains no smaller Latin trade. It is said to be k -homogeneous if it intersects each row, each column and each entry either 0 or k times. Cavenagh, Donovan and Drápal gave a construction of 3-homogeneous Latin trades from hexagonal packings of the plane with circles and asked whether the construction gave every minimal 3-homogeneous Latin trade. In a further paper, Cavenagh showed that this was indeed the case. In this talk I will present an alternative classification of 3-homogeneous Latin trades, relating it to two further problems: the embedding of 6-regular graphs in the torus or Klein bottle, and the biembedding of pairs of symmetric configurations of triples in a closed surface.

Configurations and Latin Squares

Harald Gropp (Universitaet Heidelberg, Germany)

A configuration is a linear regular uniform hypergraph.

The talk will probably consist of two parts. First, configurations are discussed as structures close to projective planes which are the geometric counterparts of MOLS (mutually orthogonal Latin squares). E.g. there are no 2 OLS of order 6, only some which are nearly orthogonal. In a similar sense there is no configuration 43_7 which would be a plane of order 6 and hence be equivalent to 5 MOLS of order 6. As an approximation in the sense of configurations there is a configuration 45_7 . Secondly, some $(r,1)$ -designs will be discussed which contain Latin squares and/or configurations as substructures in a certain sense.

On operations defined on a finite set

Vladimir I. Izbash (Academy of Sciences, Moldova)

We study the family $\Omega_n(Q)$ of all n -ary operations defined on a finite set Q ($|Q| = m$). We classify and obtain a description of some classes of $\Omega_n(Q)$. The ordered sequence (k_1, k_2, \dots, k_m) of m nonnegative integers such that $k_1 + k_2 + \dots + k_m = m^n$ is named a type. Each operation of $\Omega_n(Q)$ is related to some type in natural way. The set $\Omega_n(Q)$ is divided into classes of same-typed operations. Operations $A, B \in \Omega_n(Q)$ are named same-typed operations if they have the same type. It is proved that $A, B \in \Omega_n(Q)$ are same-typed operations if and only if there is a permutation θ on Q^n such that $B(x_1^n) = A\theta(x_1^n)$ for all $x_1^n \in Q^n$. If $A(x_1^n) = A\theta(x_1^n)$ for all $x_1^n \in Q^n$ then θ is said to be invariant for A . For $A \in \Omega_n(Q)$ of type (k_1, k_2, \dots, k_m) it is proved that the set $[A]$ of all invariant permutations form a group which is isomorphic to the direct product $S(k_1) \times S(k_2) \times \dots \times S(k_m)$, where $S(k_i)$ is the group of all permutations on $\{1, 2, \dots, k_i\}$. Some questions of orthogonality, isomorphism and automorphism of operations are studied.

The Universality of Osborn loops

Temitope Gbolahan Jaiyeola (Obafemi Awolowo University, Ile Ife, Nigeria)

Coauthor: John Olushola Adeniran (University of Abeokuta, Abeokuta, Nigeria)

The 2005 open problem of Michael Kinyon, based on the universality of Osborn loops is solved. Two nice identities that characterize universal Osborn loops are established. Kinyon's conjecture that 'every CC-quasigroup is isotopic to an Osborn loop' is shown to be true for universal Osborn loops if and only if every CC-quasigroup obeys any of the two nice identities. An Osborn loop is proved to be universal if and only if any of its principal isotopes is isomorphic to some principal isotopes of the loop. The existence of some mappings called bi-mappings and tri-mapping in the Bryant-Schneider group of a universal Osborn loop is investigated and it is discovered that there is no non-trivial universal Osborn loops that can form a special class of G-loops under such mappings. A new identity is found for a universal Osborn loop. Particularly, Moufang loops are discovered to obey the new identity $[y(x^{-1}u) \cdot u^{-1}](xu) = [y(xu) \cdot u^{-1}](x^{-1}u)$ surprisingly. Furthermore, the ideas of left and right universality are introduced and studied for Osborn loops.

On loop identities that can be obtained by a nuclear identification

Premysl Jedlicka (Czech University of Agriculture, Prague)

Coauthor: Aleš Drápal (Charles University, Prague)

We describe all the varieties of loops Q that can be defined by autotopisms α_x , $x \in Q$, where α_x is a composition of two triples, each of which becomes an autotopism when the element x

belongs to one of the nuclei. In this way we obtain a unifying approach to Bol, Moufang, extra, Buchsteiner and conjugacy closed loops. We reprove some classical facts in a new way and show how Buchsteiner loops fit into the traditional context.

Loop tables and webs

Kenneth W. Johnson (Penn State University, USA)

I will describe some connections between loop tables written in special forms and the closure of various diagrams in the theory of webs.

The equivalence between some entropic quasigroups and abelian groups with involution.

J. Kaleta (Warsaw Agricultural University, Poland)

Coauthor: G. Binczak (Warsaw University of Technology, Poland)

We show the equivalence between entropic quasigroups such that $x \cdot 1 = x$ and $1 \cdot (1 \cdot x)$ and abelian groups with involution.

How to find elements of the nuclei by hand.

A.D.Keedwell (University of Surrey, UK)

We shall describe a simple (fairly new) method of determining (by hand) from the Cayley table of a loop $(N, *)$ whether a particular element of N does or does not belong to the left, right or middle nucleus of $(N, *)$. This leads to a criterion (different from the quadrangle criterion and the criterion of Suschkewitch) for a latin square to be group-based.

If time permits, we shall also discuss matters arising from the question of when a quasigroup is a loop (essentially solved by K.Kunen).

Buchsteiner loops

Michael Kinyon (University of Denver, USA)

Coauthors: P. Csörgő (Eötvös University), A. Drápal (Charles University)

Buchsteiner loops (after H.-H. Buchsteiner, who wrote the first paper on them back in 1976) are loops which satisfy $xy \cdot z = xu \iff y \cdot zx = ux$, or equivalently, the identity $x \setminus (xy \cdot z) = (y \cdot zx) / x$. Their study is partially motivated by the fact that Buchsteiner loops form one of the varieties of loops arising naturally from nuclear identification. Buchsteiner loops turn out to be highly structured. The main technical lemma, which we obtained with the help of Prover9, is that Buchsteiner loops satisfy the “doubly weak inverse property” $I(y) = I(xy)I^2(x)$ (where $x \cdot I(x) = 1$). From this, we show that every Buchsteiner loop is isomorphic to all of its loop isotopes. Further work with associator calculus shows that the quotient of a Buchsteiner loop by its nucleus is an abelian group of exponent 4. The smallest Buchsteiner loops which are not conjugacy closed have order 32, and can all be described by a general construction. The smallest Buchsteiner loops with nonnuclear squares have order 64. Finally, there exists a Buchsteiner loop of order 128 which is nilpotent of class 3, but has an abelian inner mapping group. So far, this is the only known example of such a loop occurring within a structured variety.

Projective geometry and frame multiplication in 2^n -ons

Benard M. Kivunge (Kenyata University (Kenya))

The multiplication of the basis elements of the octonions can be fit in the Fano plane, the projective space $PG(2,2)$. The basic elements corresponding to each line, together with 1, linearly generate a subalgebra isomorphic to the quaternions. Conway and Derek Smith doubling processes is given by the formula

$$(a, b)(c, d) = \begin{cases} (ac, \bar{a}d) & \text{if } b = 0 \\ (ac - \bar{b}\bar{d}, \bar{b}\bar{c} + \bar{b}\bar{a}\bar{b}^{-1}\bar{d}) & \text{if } b \neq 0. \end{cases} \quad (1)$$

The two have come up with a new and more recent approach based on matrix multiplications. The multiplication is given by

$$(a, b)(c, d) = \begin{cases} (ac, \bar{a}d) & \text{if } b = 0 \\ (ac - \bar{b}\bar{d}, \bar{b}\bar{c} + \bar{b}\bar{a}\bar{b}^{-1}\bar{d}) & \text{if } b \neq 0. \end{cases} \quad (2)$$

We show that the multiplication of the basic elements of the sedenions under these doubling formulas can be fit into the three-dimensional projective space $PG(3,2)$. Each of the 35 lines in the projective space corresponds to a triple of basic elements which, together with 1, linearly generate a subalgebra isomorphic to the quaternions, while each of the 15 Fano planes corresponds to a septuple of basic elements which, together with 1, linearly generates a subalgebra isomorphic to the Cayley numbers. More generally, we show that the multiplication of the basic elements of the 2^n -ons fits in to the $PG(n-1, 2)$ projective geometry. In doing so, it is convenient to consider this projective geometry from several different viewpoints: as a design, in terms of Nim addition, and as the geometry of linear subspaces of a vector space. It is then shown that the number of nontrivial subloops of order 2^k inside the loop formed by the *frame* of the 2^n -ons, the set of basic elements together with their negatives, is given by

$$\begin{bmatrix} n \\ k \end{bmatrix}_2 = \frac{(2^n - 1)(2^{n-1} - 1)(2^{n-2} - 1) \cdots (2^{n-k+1} - 1)}{(2^1 - 1)(2^2 - 1)(2^3 - 1) \cdots (2^k - 1)}.$$

Pseudosquares in quadratical quasigroups

Ružica Kolar-Šuper (University of Osijek, Croatia)

Coauthors: Zdenka Kolar-Begović, (University of Osijek, Croatia), Vladimir Volenec (University of Zagreb, Croatia)

A quadratical quasigroup is defined as a quasigroup which satisfies identity $ab \cdot a = ca \cdot bc$. The geometrical concept of a square and parallelogram can be defined in a general quadratical quasigroup.

The concept of a skewsquare will be introduced in a general quadratical quasigroup. The statements referring to the connection between a skewsquare and geometrical concepts of the midpoint, a parallelogram and a square will be obtained. The mentioned statements will be proved by means of identities and equivalences which hold in a general quadratical quasigroup. The geometrical representation of the obtained concepts and relations between them will be given in the quadratical quasigroup $C(\frac{1+i}{2})$.

Affine regular decagons in GS–quasigroup

Zdenka Kolar–Begović (University of Osijek, Croatia)

Coauthors: Ružica Kolar–Šuper, (University of Osijek, Croatia) Vladimir Volenec (University of Zagreb, Croatia)

A GS–quasigroup is defined as an idempotent quasigroup which satisfies the mutually equivalent identities $a(ab \cdot c) \cdot c = b$, $a \cdot (a \cdot bc)c = b$. Some interesting geometric concepts can be defined in a general GS–quasigroup.

The concept of the affine regular decagon and affine regular star shaped decagon in a general GS–quasigroup will be defined through the concept of GS–deltoid. Introducing a number of new points besides the vertices of affine regular decagon some statements about parallelograms and affine regular pentagons will be proved. Using obtained points it will be shown how to construct the affine regular icosahedron from the affine regular decagon. The geometrical representation of the introduced concepts and relations between them will be given in the GS–quasigroup $C(\frac{1}{2}(1 + \sqrt{5}))$

Quadratic level equations with four variables

A. Krapež (Mathematical Institute, SASA, Serbia)

We consider a class of functional equations with one operational symbol which is assumed to be a quasigroup. Equations are quadratic, level and have four variables each. Therefore, they are of the form $x_1x_2 \cdot x_3x_4 = x_5x_6 \cdot x_7x_8$, $x_i \in \{x, y, u, v\}$ ($1 \leq i \leq 8$) with each of the variables occurring exactly twice in the equation. There are 105 such equations. They separate into 19 equivalence classes of equations defining 19 quasigroup varieties.

The graph of the partially ordered set of these varieties is given.

Transversals in n -ary groups and generalization of Gluskin-Hossu theorem

Kuznetsov E.A. (Academy of Sciences, Moldova)

All necessary definitions (an n -ary group (n -group), a unit of an n -group, an n -ary subgroup (n -subgroup) of an n -group, a left (right) k_i^j -coset of the n -group G to its n -subgroup H), and notations are given in (Rusakov S.A. Algebraic n -ary systems. Sylow theory of n -ary groups - Minsk, 1992).

Definition 1 Let $G = \langle Q, ({}^n) \rangle$ be an n -group, $H = \langle M, ({}^n) \rangle$ be an n -subgroup of the n -group G and $e \in G$ be a unit of the n -group G . A set $T = \{t_x\}_{x \in E} \subset Q$ is called a **left non-reduced transversal** in the n -group G to its n -subgroup H , if there exist an unique element $t_x \in T$ in every left k_i^j -coset ${}_xH = (a_1^{s-1}x a_{s+1}^i \overset{(k)}{H} b_1^j)$ for every $x \in E$ (set E is a set of indexes numbering the distinct left k_i^j -cosets of the n -group G to its n -subgroup H). If we have $t_{u_0} = e$ for some $u_0 \in E$, then such transversal T is called a **left transversal** in the n -group G to its n -subgroup H (usually we will denote $u_0 = 1$). A **right non-reduced transversal** $T = \{t_x\}_{x \in E}$ in the n -group G to its n -subgroup H is defined by the analogical way.

For every left (non-reduced) transversal $T = \{t_x\}_{x \in E}$ in the n -group G to its n -subgroup H it may be defined correctly a following n -ary operation (**transversal operation**) on the set E :

$$\overset{(T)}{(x_1^n)} = \overset{(T)}{(x_1, \dots, x_n)} = y \stackrel{def}{\Leftrightarrow} (t_{x_1}, \dots, t_{x_n}) \in t_y H = (a_1^{s-1} t_y a_{s+1}^i \overset{(k)}{H} b_1^j). \quad (3)$$

A transversal operation for every right (non-reduced) transversal $T = \{t_x\}_{x \in E}$ in the n -group G to its n -subgroup H it may be defined by the analogical way.

Because of n -group $G = \langle Q, (\cdot)^n \rangle$ have a unit e , then according to the Gluskin-Hossu' theorem [1] it can be represented in a following form:

$$(a_1^n) = a_1 \cdot a_2 \cdot \dots \cdot a_n, \quad (4)$$

where $\langle Q, \cdot \rangle$ is some binary group. The n -subgroup $H = \langle Q_1, (\cdot)^n \rangle$ may be represented by the form (4) too, and, moreover, a system $\langle Q_1, \cdot \rangle$ is a subgroup of the group $\langle Q, \cdot \rangle$.

Using the representation (4) we can prove some elementary properties of the left and right transversals and transversal operations in the n -groups.

Theorem 1 *Let an n -group $G = \langle Q, (\cdot)^n \rangle$ have a unit e , and (according to the Gluskin-Hossu' theorem) represented in a following form:*

$$(a_1^n) = a_1 \cdot a_2 \cdot \dots \cdot a_n, \quad (5)$$

where $\langle Q, \cdot \rangle$ is some binary group. Let a set $T = \{t_x\}_{x \in E} \subset Q$ is a left transversal in the n -group G to its n -subgroup $H = \langle Q_1, (\cdot)^n \rangle$, and $(x_1^n) = (x_1, \dots, x_n)$ is a corresponding n -ary transversal operation on the set E . Then the following statements are true:

1. The set $T = \{t_x\}_{x \in E}$ is a transversal in the binary group $\langle Q, \cdot \rangle$ to its subgroup $\langle \pi Q_1 \pi^{-1}, \cdot \rangle$ for some $\pi \in Q$;
2. If the n -ary transversal operation $(x_1^n) = (x_1, \dots, x_n)$ is an n -ary loop, then the set $T = \{t_x\}_{x \in E}$ is a loop transversal in the binary group $\langle Q, \cdot \rangle$ to its subgroup $\langle Q_1, \cdot \rangle$;
3. The n -ary transversal operation $(x_1^n) = (x_1, \dots, x_n)$ may be represented as a derivative operation of some binary operation $\langle Q, \circ \rangle$ (with some placement of brackets), i.e.

$$(x_1, \dots, x_n) = a_1 \circ (a_2 \circ \dots \circ a_n). \quad (6)$$

Corollary 2 *Any n -ary operation $(x_1^n) = (x_1, \dots, x_n)$, which can be represented as a transversal operation in some n -group G to its n -subgroup H may be represented as a derivative operation of some binary operation $\langle Q, \circ \rangle$ (with some placement of brackets).*

Application of quasigroups, represented as vector valued Boolean functions, in cryptography

Smile Markovski (Ss Cyril and Methodius University, Skopje, Macedonia)

Given a quasigroup $(Q, *)$ of order 2^n , we can represent the quasigroup operation $*$ as vector valued Boolean function $f : \{0, 1\}^{2^n} \rightarrow \{0, 1\}^n$ as follows:

$$a * b = c \Leftrightarrow f(a_1^n b_1^n) = c_1^n$$

where x_1^n denotes a binary presentation of an element $x \in Q$ ($x_i \in \{0, 1\}$). The vector valued operation f can be represented by n Boolean functions $f_i : \{0, 1\}^{2^n} \rightarrow \{0, 1\}$, i.e., $f = (f_1, f_2, \dots, f_n)$. The Boolean functions f_i can be represented in many different manners, like Algebraic Normal Forms, or Conjunctive Normal Forms, or Disjunctive Normal Forms, and so on. These representations allows us to infer several properties of the quasigroup, that can be used in definitions of many cryptographic primitives.

Some classes of finite simple Bol loops

Gabor P. Nagy (University of Szeged, Hungary)

The existence of finite simple proper Bol loops was considered as one of the main open problem in the theory of loops and quasigroups. In this talk we present two constructions which yield infinite classes of such loops. The first construction results G-loops which can be of odd order, as well. The second construction gives simple Bol loops of exponent 2.

Loops osculating with a group

Péter T. Nagy (University of Debrecen, Hungary)

Let (L, \cdot) be a monoassociative loop. We say that the loop (L, \cdot) is *osculating with a group* if there exists a group multiplication $(x, y) \mapsto x \circ y : L \times L \rightarrow L$ on L such that any element of L generates the same subgroup of the loop (L, \cdot) and of the group (L, \circ) .

Two classes of loops osculating with groups are investigated. The loops belonging to the first class are strongly left alternative left A -loops, satisfying $x \cdot y = x^\alpha \circ y \circ x^{1-\alpha}$, where $0 < \alpha < 1$ is a rational number. In the case $\alpha = \frac{1}{2}$ the loop is a Bruck loop isotopic to the core of the group (L, \circ) .

The second class consists of algebraic Moufang loops corresponding to the minimal dimensional Malcev algebra.

On finite loops with nilpotent inner mapping groups

Markku Niemenmaa (University of Oulu, Finland)

Coauthor: Miikka Rytty (University of Oulu, Finland)

We consider two special cases where a finite loop has a nilpotent inner mapping group. In both cases it follows that our loop is centrally nilpotent. We also discuss the general case and our conjecture is that the nilpotency of the inner mapping group implies the central nilpotency of the corresponding loop.

Moufang loops and generalized Lie-Cartan theorem

Eugen Paal (Tallinn University of Technology, Estonia)

The generalized Lie-Cartan theorem for linear birepresentations of the analytic Moufang loops is considered. Based on this theorem, the Moufang-Noether current algebras may be constructed. The corresponding charge algebra turns out to be a birepresentation of the tangent Mal'tsev algebra of an analytic Moufang loop.

The restricted Burnside problem for some varieties of loops.

Peter Plaumann (Universität Erlangen-Nürnberg, Germany)

Coauthor: Liudmila Sabinina (UAEM, Cuernavaca, México)

For the class of all groups the restricted Burnside problem is the question whether there exist bounds $f(n, d)$ such that every finite group of exponent n with d generators has cardinality $\leq f(n, d)$. The positive answer to this problem was proved by E. Zelmanov.

We present a reduction principle to treat the restricted Burnside problem for some varieties of loops to result for the class of groups. Our principle covers the following cases:

- (1) CC -loops,
- (2) Moufang A -loops,
- (3) Bruck loops which are obtained by Glauberman's construction $M(1/2)$ from a Moufang A -loop M ,
- (4) Bol A -loops which modulo their left nucleus are as in (3).

Cryptosystems based on semi-distributive algebras

Andrei V. Prasolov (University of Tromsøe, Norway)

We propose a new cryptographic scheme of ElGamal type. The scheme is based on semi-distributive algebras, shortly – semialgebras. A semialgebra over a commutative ring K is a K -module R together with an associative mapping $\mu : R \times R \rightarrow R$ which is K -linear on the first variable. The main examples are semialgebras of polynomial mappings over a finite field K , and their factor-semialgebras. Given such a semialgebra R , one chooses an invertible element $a \in R^*$ of finite order r , and a random integer s . One chooses also a finite dimensional K -submodule V of R . The 4-tuple (R, V, a, b) where $b = a^s$ form the **public key** for the cryptosystem, while r and s form the **secret key**. A plain text can be viewed as a sequence of elements of the field K . That sequence is divided into blocks of length $\dim(V)$ which, in turn, correspond to uniquely determined elements X_i of V . We propose three different methods of encoding/decoding the sequence of X_i .

The complexity of cracking the proposed cryptosystem is based on the Discrete Logarithm Problem (DLP) for polynomial mappings. There exist many efficient methods of cracking the “usual” DLP. However, for this particular DLP, no methods of cracking the problem, except for the “brute force” with $\Omega(r)$ time, are known so far.

Admissible Orders of Jordan Loops

Kyle Pula (University of Denver, USA)

Coauthors: Michael K. Kinyon (University of Denver, USA), Petr Vojtěchovský (University of Denver, USA)

A commutative loop is Jordan if it satisfies the identity $x^2(yx) = (x^2y)x$. Using an amalgam construction and its generalizations, we prove that a nonassociative Jordan loop of order n exists if and only if $n \geq 6$ and $n \neq 9$. We also consider whether powers of elements in Jordan loops are well-defined, and we construct an infinite family of finite simple nonassociative Jordan loops.

Moufang loops of odd order $p_1 p_2 \dots p_k q^3$

Andrew Rajah (Universiti Sains Malaysia, Malaysia)

Coauthor: Kam Yoon Chong (Universiti Sains Malaysia, Malaysia)

A Moufang loop is a loop which satisfies the Moufang identity $(x \cdot y) \cdot (z \cdot x) = (x \cdot (y \cdot z)) \cdot x$. A Moufang loop that is associative becomes a group. We can determine associativity of Moufang

loops by studying their orders.

It is known that there exist nonassociative Moufang loops of order pq^3 , where p and q are distinct odd primes, if and only if $q \equiv 1 \pmod{p}$. It is also known that all Moufang loops of order $p_1p_2 \dots p_kq^3$, where p_1, p_2, \dots, p_k, q are distinct odd primes, are associative if $q \not\equiv 1 \pmod{p_1}$ and for each $i > 1$, $q^2 \not\equiv 1 \pmod{p_i}$.

We shall show that all Moufang loops of order $p_1p_2 \dots p_kq^3$, where p_i and q are primes with $2 < p_1 < p_2 < \dots < p_k < q$, are associative if $q \not\equiv 1 \pmod{p_i}$ and $p_i \not\equiv 1 \pmod{p_j} \forall i, j \in \{1, 2, \dots, k\}$.

PL-loops and -hyperalgebras

Larissa Sbitneva, Morelos State University, Mexico

We consider smooth PL-loops being a generalization of M-loops related to geometry of transsymmetric spaces. The binary operation of PL-loops can be considered as the solution of some differential equation. The examination of the integrability conditions allows us to introduce proper infinitesimal objects. This consideration leads to a Lie algebra g and a subalgebra h with the decomposition $g = h + m$, which is not reductive in this case. Furthermore, we note that general (not almost regular) smooth PL-loops are of special interest, so that this case needs some new approaches different from the generalization of the Bol loop case because here we cannot expect to reduce the case to the investigation of certain Lie algebras. The analog of Lie algebra for a smooth loop is called a ν -hyperalgebra.

On simple groupoids and T-groupoids

Victor Shcherbacov (Academy of Sciences, Moldova)

Coauthor: Abdullo Tabarov (Tajik National State University, Tajikistan)

We study conditions when groupoids of some classes are simple.

We slightly generalize well known, and it is possible to say classical, definition of T-quasigroup which have been given by Tomas Kepka and Petr Němec.

Definition. Let $(Q, +)$ be an abelian group, φ, ψ be some its endomorphisms. A groupoid (Q, \cdot) of the form $x \cdot y = \varphi x + \psi y + a$, where a is a fixed element of the set Q , will be called a *T-groupoid*.

We start the study of this class of groupoids and n -*T*-groupoids in the spirit of Jezek, Kepka and Němec articles.

In particular, congruences of T-groupoids and finite simple T-groupoids are researched.

Systems of axioms for some classes of groupoids and quasigroups

Victor Shcherbacov (Academy of Sciences, Moldova)

Both “existencial” and “equational” definitions of binary quasigroups and groupoids closely connected with quasigroups, including definitions of classes of left quasigroups, division groupoids, cancellation groupoids and some combinations of these classes are given.

Theorem. A groupoid (Q, \cdot) is a quasigroup if and only if all middle translations of (Q, \cdot) are bijective maps of the set Q .

Let h be a homomorphism of a groupoid (Q, \cdot) with a property T , θ be a congruence which corresponds to h . We shall call θ and h T -closed (often, simply, “closed”) if and only if $h(Q, \cdot)$ has the property T .

Theorem. A congruence θ of a left division groupoid (Q, \cdot) is closed if and only if θ is a congruence of corresponding algebra (Q, \cdot, \setminus) with identity $x \cdot (x \setminus y) = y$.

Theorem. An equivalence θ is closed congruence of a left division groupoid (Q, \cdot) if and only if θ admits any element of the semigroup $\Pi_1(Q, \cdot) = \langle L_x, R_x, L_x \setminus, R_x \setminus \mid x \in Q \rangle$, where $L_x L_x \setminus = \varepsilon$ for all $x \in Q$.

Theorem. A groupoid (Q, \cdot) is strongly simple if and only if its multiplicative semigroup $\Pi(Q, \cdot)$ is primitive.

Defining quasigroups

Jonathan Smith (Iowa State University, Ames, USA)

Quasigroups were originally defined combinatorially, as Latin squares. Over 50 years ago, Trevor Evans redefined quasigroups algebraically as sets with three binary operations, and proved a Normal Form Theorem for them. Now, binary, ternary, and more general quasigroups will be given a much shorter definition. The definition includes group actions as unary quasigroups. There is algebraic structure on the underlying set of the quasigroup, and also on the set of operations. The new definition reveals a strong form of triality symmetry for quasigroups, leading to considerable simplification in the proof of Evans’ Theorem, and an extension of its scope to other varieties.

Parastrophic equivalence of functional equations on quasigroup operations

Fedir M. Sokhatsky (Vinnytsia, Ukraine)

Functional equations on quasigroup operations of an arbitrary fixed set are under consideration. A collection of subterms of a functional equation $\omega = v$ is said to be: *self-contained*, if it contains all occurrences in $\omega = v$ of all subject variables having an occurrence in a subterm of the collection; *essentially self-contained*.

Two functional equations are said to be: *parastrophic*, if one can be got from the other by a finite number of parastrophic transformations: replacing a functional variable with one of its parastrophs together with the corresponding permutation of subterms of $\omega = v$. Let $\langle \omega = v \rangle$ denote a set of all pairwise parastrophic functional equations.

A functional equation $\omega = v$ is called: *quadratic*, if every its subject variable has exactly two occurrences; *parastrophically cancelable*, if a functional equation from $\langle \omega = v \rangle$ has a self-contained subterm collection; *reducible*, if a functional equation from $\langle \omega = v \rangle$ is equivalent to a system of functional equations, every of which has less subject variables than $\omega = v$ has.

It is found parastrophic equivalence classes of binary general quadratic parastrophically uncancelable functional equations having small number of subject variables. If a functional equation

has a parastrophically essential subterm collection, then it is reducible. Every binary parastrophically cancelable quadratic functional equation is reducible.

Towards automating classification of quasigroup structures

Volker Sorge (University of Birmingham, UK)

Coauthors: Simon Colton (Imperial College London, UK) Roy McCasland (University of Edinburgh, UK)

In recent years we have developed a procedure to classify simple algebraic structures of a given size into equivalence classes by discriminating them with respect to algebraic properties. The basic idea is to take two non-equivalent structures, find a distinguishing property, and then show if either structure already represents an equivalence class. If not, we generate a new structure, not equivalent to the former and this process iterates until all equivalence classes are found. The result of the procedure is a set of equivalence classes, each given by representant and a property that uniquely describes the class.

The procedure is fully automatic and uses a multitude of Automated Reasoning techniques and, in particular, Machine Learning to construct algebraic properties that uniquely distinguish two non-equivalent algebraic structures. In our experiments, we have mainly concentrated on the domain of quasigroups and loops using isomorphism and isotopism as the equivalence relation. Using this procedure, we have generated classification theorems for structures up to size 8.

In future work, we intend to examine these results in order to recognise common patterns among the occurring properties, to possibly find characterisations of equivalence classes regardless of the size of the structures. We also want to look at how to automate the discovery of results relating to products of algebraic structures, e.g., direct products. We want to present our work to the Loops community both to get feedback on our ideas as well as to consult with experts on possible future directions.

Every quasigroup is a factor of a subdirectly irreducible quasigroup

David Stanovský (Charles University, Prague, Czech Republic)

Coauthor: Ralph McKenzie (Vanderbilt University, USA)

Every quasigroup (loop, Bol loop, group, resp.) is isomorphic to the factor of a subdirectly irreducible quasigroup (loop, Bol loop, group, resp.) over its monolithic congruence. The result is achieved by means of a wreath product of the given quasigroup and a simple non-abelian group.

This is a part of a general project, to investigate factoralgebras of subdirectly irreducible algebras; we will shortly survey the other results, too.

Embedding algebras into entropic polyquasigroups

Michał Stronkowski (Warsaw University of Technology, Poland)

Groupoids that satisfy the identity $(xy)(uv) = (xu)(yv)$ are called entropic. M. Sholander showed that each entropic groupoid G embeds into an entropic quasigroup. Let us denote the smallest such quasigroup by $Q(G)$. J. Ježek and T. Kepka showed that the assignment Q is in fact the left adjoint functor to the inclusion functor. In the talk we will present a generalization of this result. An algebra (A, F) is a polyquasigroup if for each n -ary operation $f \in F$ the reduct (A, f) is an n -quasigroup. Moreover (A, F) is entropic if each n -ary operation $f \in F$ is a homomorphism from (A^n, F) into (A, F) . We will show that there exists a functor Q , from the category of cancellative entropic algebras into the category of entropic polyquasigroups, which is left adjoint to the inclusion functor. Moreover all units of this adjunction $A \rightarrow Q(A)$ are 1-1. We will present properties of Q and show some corollaries.

The K-Loops of hyperbolic spaces

Torben Steckelberg (University of Hamburg, Germany)

First we'll consider hyperbolic spaces of dimension $n \in \mathbb{N}$ with $n > 1$ and postulate necessary axioms.

An ordered field R will be called n -real, if the characteristic polynomial of every positive definite hermitian $n \times n$ -matrix splits into linear factors.

Then we'll construct special Loops $L(p)$ over $(p + 1)$ -real fields R for all $p \in \mathbb{N}$. They are sets of invertible positive definite hermitian $(p + 1) \times (p + 1)$ -matrices with an additional postulate, and with a special binary operation even K-Loops.

These are incidence spaces and for an euclidean $(p + 1)$ -real field R there exists a bijection, so that the incidence spaces are isomorphic to the p -dimensional Klein-type of hyperbolic spaces, which means the unit sphere in R^p with the secants as lines.

We'll define the congruence and arrangement in the K-Loops appropriately, so that they will be isomorphic to the hyperbolic spaces of Klein-type. Therefore every hyperbolic space over an euclidean $(p + 1)$ -real field R of dimension $p \in \mathbb{N}$ is isomorphic to the K-Loop $L(p)$.

Steiner loops and their small extensions

Izabella Stuhl (University of Debrecen, Hungary)

Coauthor: Karl Strambach (University of Erlangen, Germany)

If the order of any product of two left translations of a finite Steiner loop S is not divisible by 4 then the group G generated by the left translations of S is either an alternating or a symmetric group. Investigating extensions L of a group of order 2 by a Steiner loop S we show that the group generated by the translations of L is an extension of an elementary abelian 2-group by G . We study thoroughly the relations between extensions L and oriented Steiner triple systems, in order to obtain more detailed knowledge about these loops L , about the structure of their automorphism groups and the isomorphism classes.

On Π -quasigroups

Parascovia Syrbu (Moldova State University, Moldova)

A binary quasigroup $Q(A)$ which satisfies the identity

$${}^{\alpha}A(x, {}^{\beta}A(x, {}^{\gamma}A(x, y))) = y,$$

where $\alpha, \beta, \gamma \in S_3$, is called a Π -quasigroup of type $[\alpha, \beta, \gamma]$. Π -quasigroups have been defined by V. Belousov in a preprint published in 1983.

Consider the following transformations of types on S_3^3 : $f[\alpha, \beta, \gamma] = [\beta, \gamma, \alpha]$, $h[\alpha, \beta, \gamma] = [r\gamma, r\beta, r\alpha]$, where $r = (23)$, and denote by U the group generated by f and h . Two types T' and T are called orthogonal equivalent (denote $T' \sim T$) if there exists a substitution $\theta \in S_3$ and a transformation $g \in U$ such that $T' = gT\theta$. Then $|S_3^3 / \sim| = 7$ and a system of representatives of the equivalence classes are: $T_1 = [\varepsilon, \varepsilon, \varepsilon]$, $T_2 = [\varepsilon, \varepsilon, l]$, $T_3 = [\varepsilon, \varepsilon, lr]$, $T_4 = [\varepsilon, l, lr]$, $T_5 = [\varepsilon, lr, l]$, $T_6 = [\varepsilon, rl, lr]$, $T_7 = [\varepsilon, lr, rl]$. Denoting $A = " \cdot "$ the following identities are obtained, which correspond to the seven types, respectively: $x(x \cdot xy) = y$, $x(y \cdot yx) = y$, $x \cdot xy = yx$ (Stein's 1st law), $xy \cdot x = y \cdot xy$ (Stein's 2nd law), $xy \cdot yx = y$ (Stein's 3d law), $xy \cdot y = x \cdot xy$ (Schröder's 1st law), $yx \cdot xy = y$ (Schröder's 2nd law) ([1,3]). Remark that these identities give only a part of the existing orthogonal pairs of parastrophes of the quasigroup $Q(\cdot)$.

It was proved by Belousov and Gwaramija that if a quasigroup satisfying the identity $x \cdot yx = yx \cdot y$, respectively $x \cdot xy = yx$, is isotopic to a group then this group is metabelian (i.e. all commutators belong to the center of the group). Also V. Belousov proved that if a group $Q(+)$ is

isotopic to a Π -quasigroup of type T_6 than $Q(+)$ is abelian of exponent two. More, every finite group of exponent two is isotopic to a Π -quasigroup of type T_6 . Π -quasigroups and, in particular, Π -quasigroups isotopic to groups are studied. Characterizations of Π -quasigroups isotopic to abelian groups are found.

Identities in linear and alinear quasigroups

A.H. Tabarov (Tajik State National University, Tajikistan)

Linear quasigroups have arisen in connection with research of balanced identities in quasigroups (V.D. Belousov. Balanced identities in quasigroups. Mat. sb. 1966. v. 70, no. 1, p. 55-97).

Alinear quasigroups were defined by G.B. Belyavskaya and the author in (Belyavskaya G.B., Tabarov A.H. A characteristic of linear and alinear quasigroups. Discrete mathematics, 1992, v.4, no. 2, p. 142-147), where linear (alinear) quasigroups are characterized by one identity.

In other works of G.B. Belyavskaya and the author various primitive linear, semilinear and mixed linear quasigroups in language of identities are described.

A quasigroup (Q, \cdot) is called linear over a group $(Q, +)$, if (Q, \cdot) has the form

$$xy = \varphi x + c + \psi y, \quad (7)$$

where $\varphi, \psi \in \text{Aut}(Q, +), c \in Q$.

Theorem 1. All primitive linear quasigroups are characterized by the following system of identities:

$$[x(u \setminus y)]z = [x(u \setminus u)](u \setminus yz)$$

$$x[(y/u)z] = (xy/u)[(u/u)z]$$

Theorem 2. All primitive quasigroups of the form $xy = \overline{\varphi}x + c + \psi y$, where $\psi \in \text{Aut}(Q, +), c \in Q, \overline{\varphi}$ is an antiautomorphism of the group $(Q, +)$, are characterized by the following system of identities:

$$[x(y/u)z] = (xy/u)[(u/u)z]$$

$$[u \setminus ((x \setminus u)y)]v = y[u \setminus ((u \setminus x)v)].$$

Theorem 3. All primitive quasigroups of the form $xy = \varphi x + c + \overline{\psi}y$, where $\varphi \in \text{Aut}(Q, +), c \in Q, \overline{\psi}$ is an antiautomorphism of the group $(Q, +)$, are characterized by the following system of identities:

$$[x(u \setminus y)]z = [x(u \setminus u)](u \setminus yz)$$

$$[u \setminus ((x/u)y)]v = y[u \setminus ((u/x)v)],$$

where $\varphi \in \text{Aut}(Q, +), c \in Q, \overline{\psi}$ is an antiautomorphism of the group $(Q, +)$.

Classes of T-quasigroups, left (right) T-quasigroups also are described by a system of identities. We remark, that there are also other systems of identities, which define various types of linear quasigroups.

FA-presentable structures

Rick Thomas (University of Leicester, UK)

Abstract: We are interested in the notion of computing in structures (where a structure consists of a set together with a collection of relations). The natural approach would be to take some general model of computation (such as a Turing machine). A structure would then be said to be computable if its domain can be represented by a set which is accepted by a Turing machine and if there are decision-making Turing machines for each of its relations. However, there have been

various ideas put forward to restrict the model of computation used; whilst the range of structures decreases, the computation can become more efficient and certain properties of the structure may become decidable.

One interesting approach was introduced by Khoussainov and Nerode who considered structures whose domain and relations can be checked by finite automata as opposed to Turing machines. Such a structure is said to be "FA-presentable". This was inspired, in part, by the theory of "automatic groups" introduced by Epstein et al; however, the definitions are somewhat different.

We will survey some of what is known about FA-presentable structures, contrasting it with the theory of automatic groups and posing some questions about FA-presentable loops. The talk is intended to be self-contained, in that no prior knowledge of these topics is assumed.

On Bol closure condition

Henrietta Toman, University of Debrecen, Hungary

V. V. Goldberg and S. A. Gerasimenko gave some equivalent conditional Bol identities for $(n + 1)$ -web and the corresponding coordinate n -loop satisfying the Bol closure condition. We discuss further properties of this kind of n -loops. We apply these results in special case when 3-loop is given by iterated loop multiplication.

On inversion matrices of n -IP-loops

Leonid A. Ursu (Technical University of Moldova)

A quasigroup $Q(A)$ of an arity n with the identity

$$A(\{\nu_{ij}x_j\}_{i=1}^{i-1}, A(x_1^n), \{\nu_{ij}x_j\}_{j=i+1}^n) = x_i,$$

$i \in \overline{1, n}, j \in \overline{1, n+1}$ is called an n -IP-quasigroup, where ν_{ij} are inversion permutations, $\nu_{ii} = \nu_{i, n+1} = \varepsilon$, where ε is an identity permutation of the set Q , $[\nu_{ij}]$ is an inversion matrix.

It is known that an n -IP-quasigroup has more than one of inversion matrices.

An n -loop is an n -quasigroup with an identity element. If all inversion permutations are equal, then $Q(A)$ is called n -IP-loop with one parameter of inversion.

An n -quasigroup is called *symmetrical*, if $A(x_{\alpha 1}^{\alpha n}) = A(x_1^n)$ for any $\alpha \in S_n$, where S_n is the symmetrical group of permutations of the set Q of a finite order. Otherwise it is called *unsymmetrical*.

For any n -IP-loop with an identity e there exists the matrix $[I_{ij}]$, where the permutations I_{ij} are defined by the equalities:

$$A(e^{i-1}, x, e^{j-i-1}, I_{ij}x, e^j) = e$$

for any $x \in Q; i, j \in \overline{1, n}$.

V.D. Belousov has raised the following questions: is always the matrix $[I_{ij}]$ one of the inversion matrices of an n -IP-loop?

The positive answer on this question the author has given for n -IP-groups with an identity, for symmetrical n -IP-loops and for n -IP-loops with one parameter of inversion.

Now we prove that the inversion matrix $[I_{ij}]$ is one of inversion matrices of unsymmetrical 3-IP-loops.

For the case arity $n > 3$ this question is open till now.

Medial Quasigroups and Geometry

A. Vanžurová (Palacky Univerzity, Olomouc, Czech Republic)

Coauthor: V.J. Havel

We mention: Medial quasigroups and incidence structures. The approach of Pucharev, parallelism via term functions. Transfer group and parallelogram space of a medial quasigroup. Golden section (GS-) quasigroups, GS-parallelograms and GS-trapezoids. From Toyoda's theorem for idempotent medial quasigroups to Toyoda's theorem for GS-quasigroups. Construction of (finite) GS-quasigroups from fields.

Loops with commuting inner mappings and of nilpotency class three

Petr Vojtěchovský (University of Denver, USA)

Coauthor: Aleš Drápal (Charles University, Czech Republic)

The first (and only) example of a loop with commuting inner mappings and of nilpotency class three has been obtained recently by Piroska Csörgő, using the method of connected transversals. As in our earlier work, we take advantage of group modifications to reconstruct the above loop and to obtain numerous nonisomorphic loops with similar properties. The modifications are ultimately based on symmetric trilinear forms, and, surprisingly, it suffices to start with a group of nilpotency class two.