Booklet of Abstracts

LOOPS'11

Třešť

July 25-27, 2011

Main Lectures

The structure of the finite Bruck loops

Barbara Baumeister (Freie Universitaet Berlin, Germany)

The group theory behind Moufang loops

Stephen Gagola III (Bowling Green State University, USA)

Finite centrally nilpotent loops

Markku Niemenmaa (University of Oulu, Finland)

We concentrate on the relation between the structures of finite centrally nilpotent loops and their multiplication groups and inner mapping groups. We shall introduce some major and minor results from the years 1946–2011.

Quo vadis theory of loops and quasigroups?

Karl Strambach (University of Erlangen, Germany)

Automorphic loops

Petr Vojtěchovský (University of Denver, USA)

A loop is called automorphic if all its inner mappings are automorphisms. Hence every group and every commutative Moufang loop is an automorphic loop, but there are many other examples. Our understanding of the structural theory of automorphic loops has been greatly expanded in the last 4 years, thanks to the work of P. Csörgő, D. deBarros, A. Grishkov, P. Jedlička, K. Johnson, M. Kinyon, G. Nagy, and others.

In this talk I will present a survey of all known results and some of the techniques concerning automorphic loops. For instance, I will show that every automorphic loop of odd order is solvable and every finite simple commutative automorphic loop is a group (using Lie algebras), prove that every commutative automorphic p-loop is centrally nilpotent when p is an odd prime (using associated operations in the spirit of Glauberman), give the classification of commutative automorphic loops of order p^3 (using modules), and construct a family of automorphic loops of order p^3 with trivial nucleus (using anisotropic planes in the vector space of 2×2 matrices). The talk will conclude with open problems.

The number of subsquares of a latin square

Ian Wanless (Monash University, Australia)
Coauthors: Josh Browning, Doug Stones, Petr Vojtěchovský, Michael Kinyon

A subsquare of a latin square is a submatrix that is itself a latin square. I will survey old and new results relating to the question 'How many subsquares of order k can there be

in a latin square of order n?'. I will consider the minimum possible (usually zero, though not always easy to show it is), the maximum possible and talk briefly about the typical number (if a latin square is generated randomly). Unsurprisingly, the squares with the maximum number of subsquares tend to have interesting algebraic structure.

Contributed Talks

Comparison of performances of random codes based on quasigroups, Reed-Muller Codes and Reed-Solomon Codes

Verica Bakeva (Ss Cyril and Methodius University, Skopje, Macedonia)
Coauthors: Aleksandra Popovska-Mitrovikj, Smile Markovski

Random error-correcting codes based on quasigroups transformations are proposed elsewhere. They are similar to convolution codes and the dependence of the properties of the codes from the used quasigroups are investigated in earlier paper of ours. In this paper we compare the Random error correcting codes based on quasigroups with the well know Reed-Muller and Reed-Solomon codes. The obtained experimental results show that in the case when the bit-error probability of binary symmetric channel is $p > 0.05$ ($p > 0.06$) then the random codes based on quasigroups overperform the Reed-Muller and Reed-Solomon codes for the packet-error probability (for the bit-error probability).

Classification of nonassociative Moufang loops of odd order pq^3, $p \neq 3$

Wing Loon Chee (Universiti Sains Malaysia, Penang, Malaysia)
Coauthors: Andrew Rajah

In [2001, J. Algebra 235, 66–93], Rajah showed the existence of a new class of nonassociative Moufang loops: For distinct odd primes p and q, there exists a nonassociative Moufang loop of order pq^3 if and only if q is congruent to 1 modulo p. In this talk, we present the classification of these Moufang loops for the case $p \neq 3$. We also discuss the recent progress when $p = 3$.

A standard form of the MQQ generating function and its applications

Yanling Chen (Norwegian University of Science and Technology, Trondheim, Norway)
Coauthors: Danilo Gligoroski, Svein J. Knapskog

In this paper, we study a special class of recently introduced quasigroups called Multivariate Quadratic Quasigroups (MQQ). Based on a few noteworthy observations, we derive a standard form of the MQQ generating function, which gives us insights into how to construct MQQs of higher orders, yield lower bounds on the number of MQQs, and eventually solve several open research problems about them. Besides, we also introduce a refined notion, "MQQs of strict type", by which, a new classification of the MQQs is defined. This concept has an advantage to be invariant under linear transformations and thus better characterize the complexity of the underneath multivariate quadratic system. Last but not least, we show that the standard generating function can be used to creat (linear) orthogonal Latin squares of certain orders.

On the centrally and nuclearly nilpotence of Moufang loops

Piroska Csörgő (Eotvos University, Budapest, Hungary)

Let Q be a finite Moufang loop with nucleus $N(Q)$ and associator subloop $A(Q)$. We prove that if the factorloop over the nucleus $Q/N(Q)$ has nontrivial center,then the

center of Q is nontrivial too. By using this result we show that the centrally nilpotence of $Q/N(Q)$ implies the centrally nilpotence of $A(Q)$ and we can verify that for the centrally nilpotence of a finite Moufang loop Q is necessary and sufficient the centrally nilpotence of $Q/N(Q)$ and $Q/A(Q)$. Finally as a corollary we give a necessary and sufficient condition for the equivalence of centrally and nuclearly nilpotence of finite Moufang loops, namely the centrally nilpotence of $Q/A(Q)$.

Primary and derivative quasigroups

Ivan Deriyenko (Kremenchuk State Polytechnical University, Ukraine)

The construction of complete quasigroups prolongation offered by R.H.Bruck 'Some results in the theory of quasigroups, TAMS, 1944,55,19-24' is well-known. It will be referred to as the classical one. Quasigroup B of the order $n+1$ will be called a derivative one, if it is a prolongation of some complete quasigroup A of the order n, otherwise quasigroup B will be referred to as a primary quasigroup. I. Deriyenko and W. Dudek in their papers 'On prolongations of quasigroups, QRS vol.16 no.2 (2008), 187-198', supplemented the classical construction of quasigroup prolongation, which makes it possible to prolong not only complete, but also quasicomplete quasigroups. If Brualdi's conjecture proves to be true, it will result in the idea that every quasigroup has a prolongation. In this connection the derivative quasigroup class enlarges and the primary quasigroup class constricts. The author has determined the criterion of a derivative quasigroup. Corollary: every cyclic group is primary.

Classifications of quasigroups of order 4 by parastrophic quasigroup transformation

Vesna Dimitrova (Ss Cyril and Methodius University, Skopje, Macedonia)
Coauthors: Verica Bakeva, Aleksandra Popovska-Mitrovikj, Aleksandar Krapež

In this paper, we propose a new quasigroup string transformation PE based on quasigroup parastrophes. Previously, using E-transformation a classification by image pattern of quasigroups of order 4 as fractal and non-fractal is made. With PE transformation we classify the quasigroups of order 4 in three classes: 1) parastrophic fractal; 2) fractal and parastrophic non-fractal; and 3) non-fractal. Also, we investigate the algebraic properties of the previous classes and present a connection between fractal properties and algebraic properties of quasigroups of order 4. In addition we find a number of different parastrophes of each quasigroup of order 4 and divide the set of all quasigroups of order 4 in 4 classes. These classifications increase the number of quasigroups of order 4 which are suitable for designing of cryptographic primitives.

Golden quasigroups, hexagonal quasigroups, and constructions

Jitka Doležalová (Palacky University of Olomouc, Czechia)
Coauthors: Alena Vanžurová

We consider special subvarieties in the variety of idempotent medial quasigroups, namely, so-called GS-quasigroups and hexagonal quasigroups. We mention the Toyoda Theorem and prove a specialization of the Toyoda-like Theorem for each of the classes. We

show a method of construction of some examples of such quasigroups from finite fields.

A simplified proof of Moufang's theorem

Aleš Drápal (Charles University in Prague, Czechia)

Moufang's theorem states that if three elements x, y, z of a Moufang loop Q associate (i.e. they satisfy $x \cdot (y \cdot z) = (x \cdot y) \cdot z$), then they generate a subgroup of Q. The original proof of Ruth Moufang runs by a very long and complicated induction argument. The later proof of Bruck is shorter, but far from being transparent. The main novel idea of the new proof is to use the fact that a Moufang loop Q generated by a set X is associative if $x_1(x_2(x_3(\dots(x_{k-1}x_k)\ )))\ =\ (\ ((x_1x_2)x_3)\dots x_{k-1})x_k$ holds for all $x_1, \dots, x_k \in X^{\pm 1}$. The talk is based upon a paper that has been accepted for Proceedings of AMS.

D-loops

Wieslaw A. Dudek (University of Wroclaw, Poland)
Coauthors: Ivan Deriyenko

A loop $Q(\cdot)$ is called a D-loop if it satisfies the *dual automorphic inverse property*, i.e., if $(xy)^{-1} = y^{-1}x^{-1}$ holds for all $x, y \in Q$, where x^{-1} denotes the right inverse element. In this loop x^{-1} also is a left inverse element. There are D-loops which are not IP-loops. We present various characterizations of D-loops by permutations φ_a such $x \cdot \varphi_a(x) = a$ for all $x \in Q$. The necessary and sufficient conditions under which a quasigroup isotopic to D-loop is a D-loop will be given. Some methods of constructions of D-loops will be presented.

Extensions of groups by weighted Steiner loops

Ágota Figula (University of Debrecen, Hungary)
Coauthors: Karl Strambach

A loop L is a quasigroup with identity element e. A Steiner triple system σ is an incidence structure consisting of points and blocks such that two distinct points are contained in precisely one block and every block has precisely three points. With a Steiner triple system σ is associated a Steiner loop $(S(\sigma), \circ)$ such that the elements of $S(\sigma) \setminus \{e\}$, where e is the identity of $S(\sigma)$, are the points of the Steiner triple system σ, the product $a \circ b$ is the third point of the block determined by a, b and $a \circ a = e$ for all $a \in S(\sigma)$. A weighted Steiner loop (S, h) is a Steiner loop S with a map $h : S \setminus \{e\} \to A$, where A is a group. Solving functional equations given in [1] for extensions of a group A by a weighted Steiner loop S we obtain concrete description for all loops with interesting weak associativity properties if the Steiner loop S induces only the trivial automorphism on A. The restricted Fischer groups and their geometry play an important role for loop extension with right alternative property. Also the automorphism groups of these extensions as well as the conditions for isomorphisms between two extensions are studied.

[1] Peter T. Nagy and Karl Strambach, *Schreier loops*, Czechoslovak Math. J. 58, 759-786, 2008.

About half-automorphisms of Chein loops

Maria de Lourdes Merlini Giuliani (Santo André, Brazil)
Coauthors: Stephen Gagola III

A half-automorphism (or h-automorphism) is a bijection $f : G \to G$ such that $f(ab) = f(a)f(b)$ or $f(b)f(a)$, for any a, b in G, where G is a multiplicative system. W.R.Scott showed that 'every h-homomorphism of groups is either a homomorphism or an anti-homomorphism'. We call this case a 'trivial h-homomorphism'. For arbitrary Moufang loops this result is not valid since I presented a counter-example in the last Conference in Notre Dame. At that time Kenneth and I conjectured that 'every h-automorphism of a Chein loop is trivial'. This is actually not true. Steve and I have found a counter-example but also showed that this is true under certain conditions.

The public key encryption scheme MQQ-ENC

Danilo Gligoroski (Norwegian University of Science and Technology, Trondheim, Norway)
Coauthors: Simona Samardjiska

The class of Multivariate Quadratic Quasigroups (MQQ) has been used in the design of one multivariate public key encryption algorithm. However, the encryption scheme was successfully cryptanalysed using the Gröbner basis approach and also by the MutantXL algorithm – an improved variant of the XL algorithm (shown to be actually equivalent to the Gröbner basis approach). A classical way to thwart the successful attacks on multivariate public key systems is to use the so called *minus modifier* i.e., to remove some equations from the public key. The removal causes the remaining public key part to lack a crucial information that is necessary for Gröbner basis attacks to easily solve the system. However, this reduces the functionality of such systems only to digital signatures, and concretely for MQQ, recently such a digital signature scheme called MQQ-SIG was designed. In this work we describe our solution of how to keep the encryption/decryption property of MQQ in the presence of the *minus modifier* by adding an additional redundancy and paying an additional work overload in the decryption phase. The scheme is called MQQ-ENC. The decryption in MQQ-ENC is not deterministic, but depending on the size of the introduced redundancy, the probability of incorrect decryption can be exponentially small.

A construction of commutative automorphic loops

Mark Greer (University of Denver, USA)

Baer showed that on a nilpotent group G with unique square roots (*e.g.*, of odd order) and of class at most two, the new operation $x \circ y = xy[y, x]^{1/2}$ defines an abelian group structure on G such that powers in G coincide with powers in $(G, \circ)$. Under the class 2 assumption, the operation $\circ$ coincides with the operation $x \oplus y = (xy^2x)^{1/2}$. As is well-known from work of Bruck, Glauberman and others, $\oplus$ defines a Bruck loop on any group with unique square roots. This talk will focus on $\circ$ itself. For any group G with unique square roots, $(G, \circ)$ turns out to be a commutative loop, and it is quite often, though not always, an automorphic loop. We will discuss the relationships, some proven and some conjectural, between properties of G weaker than nilpotency class 2 and properties of $(G, \circ)$.

DTS-quasigroups

Terry S. Griggs (The Open University, Milton Keynes, UK)
Coauthors: Aleš Drápal, Andrew Kozlik

A Steiner triple system of order v, STS(v), exists if and only if $v \equiv 1$ or 3 (mod 6). It is well known that given an STS(v), an algebraic structure, called a Steiner quasigroup, can be defined by introducing a binary operation with the properties that $x \cdot x = x$ and, if $x \neq y$, $x \cdot y = z$, where z is the third element in the triple containing the pair $\{x, y\}$. If we introduce order, then an ordered triple (x, y, z) can be thought of as covering either the ordered pairs (x, y), (y, z), (z, x) (cyclic ordering) or (x, y), (y, z), (x, z) (transitive ordering). The former are called Mendelsohn triple systems, MTS(v), and the latter directed triple systems, DTS(v). Both exist if and only if $v \equiv 0$ or 1 (mod 3), except that there is no MTS(6). Given a Mendelsohn triple system, again a quasigroup can be defined in the same manner as for a Steiner triple system, respecting the order of the cyclic triples. But this is not so for directed triple systems in general. However some directed triple systems do yield quasigroups and we call these systems Latin directed triple systems and the associated quasigroups, DTS-quasigroups. I will present some of our work in this area. Three features are of note. First, DTS-quasigroups do not form a variety. Secondly, there is a one-one correspondence between both Steiner and Mendelsohn triple systems and their quasigroups. This is not so for directed triple systems. Non-isomorphic DTS(v) can give isomorphic quasigroups. Thirdly both Steiner and Mendelsohn quasigroups satisfy the flexible law $x \cdot (y \cdot x) = (x \cdot y) \cdot x$. DTS-quasigroups need not.

Comparison of two error-detecting codes based on quasigroups of order 4

Natasha Ilievska (Ss. Cyril and Methodius University, Skopje, Macedonia)

In one previous paper, we proposed a new model of error-detecting codes based on quasigroups on the following way. Each input block $a_1a_2 \dots a_n$ is extended to a block $a_1a_2 \dots a_nb_1b_2 \dots b_n$ where $b_i = a_i * a_{r_{i+1}} * a_{r_{i+2}} * a_{r_{i+k-1}}$, $i \in \{1, 2, \dots, n\}$, $*$ is a quasigroup operation and

$$r_j = \begin{cases} j, & j \leq n \\ j \mod n, & j > n \end{cases}$$

We have already derived approximate formula for the probability of undetected errors when quasigroups of order 4 are used for coding and $k = 2$. Now, we derive approximate formula for the probability of undetected errors when also quasigroups of order 4 are used for coding, but $k = 3$. We find the optimal block length such that the probability of undetected errors is smaller than some previously given value ε and give classification of quasigroups of order 4 according to goodness for the code when $k = 3$. At the end, we compare these two considered codes and conclude that the code with $k = 3$ gives much smaller probability of undetected errors.

Commutative centerless loops with metacyclic inner mapping group

Přemysl Jedlička (Czech University of Life Sciences, Prague, Czechia)
Coauthors: Denis Simon

Aleš Drápal described a contruction yielding and commutative loop Q with metacyclic $\mathrm{Inn}(Q)$ and $Z(Q) = 1$. This construction was, however, not very transparent and it was

not clear how to explicitly obtain (all) such loops. We analyzed this construction in some specific cases, obtaining the following results:

Theorem. *Let M be a module over a ring R, which is either a field or the ring $\mathbb{Z}_n$ and which is not of characteristic 2. Suppose that there exists ζ, an element of an odd order k, lying either in R^*, or in a quadratic extension of R and being of norm 1, with respect to R. Then we can define a commutative A-loop Q on the set $M \times \mathbb{Z}_k$ as follows:*

$$(a,i)\cdot(b,j) = \left((a+b)\cdot\frac{(\zeta^i+1)(\zeta^j+1)}{2\cdot(\zeta^{i+j}+1)}, i+j\right).$$

Moreover, $N_\mu(Q) = M$ and $N_\lambda = \{1\}$.

Theorem. *Let q be an odd prime and $k > 1$. The number of centerless loops of order $k \cdot q$ with the middle nucleus equal to $\mathbb{Z}_q$, that arise from the construction, is, up to isomorphism,*

- $q-2$ *if* $k = 2$;
- $(q-k+2)/2$ *if k is an odd divisor of $q+1$;*
- $(q-k+1)/2$ *if k is an even divisor of $q+1$ and $k > 2$;*
- $(q-k)/2$ *if k is an odd divisor of $q-1$;*
- $(q-k-1)/2$ *if k is an even divisor of $q-1$ and $k > 2$;*
- 0 *otherwise.*

Determinants of latin squares and quasigroups

Kenneth W. Johnson (Penn State University, USA)

The determinant of a finite loop or quasigroup (or equivalently a latin square) was introduced the 90's. For a latin square the elements are replaced by variables and the determinant of the resulting matrix is taken. If the latin square is the multiplication table of a group, the factorisation of the determinant led Frobenius to define group characters for arbitrary groups and the many tools of group representation theory developed out of this. A calculation on the latin squares of order 8 showed that 'almost all' have distinct determinants. Recently (after conversations at Denver 2009) Donovan and Wanless have obtained a criterion for when latin squares have the same determinant. I will present a survey of results and some conjectures on latin square determinants, for example for squares arising from Moufang loops and whether there exist analogues of the k-characters which arise from groups.

Quasigroup laws which imply that the quasigroup is a loop or group

Donald Keedwell (University of Surrey, Guildford, UK)

Any quasigroup which satisfies the law $(xx\cdot y)z = zy$ is a commutative loop of exponent two. One which which satisfies $x \cdot yz = y \cdot zx$ is an abelian group. Fiala has proved with computer aid that in fact there are 35 laws of length six which have the property of the title

(discounting renaming, cancelling, mirroring and symmetry). We show that it is possible to give short humanely-comprehensible proofs of Fiala's results and to separate the loops and groups into classes.

Sign matrices for frames of $2n$-ons

Benard Kivunge (Kenyatta University, Kenya)

There has been a great desire to develop doubling formulas that give better algebraic structures as the dimensions of the algebras so formed increase. Whenever these doubling formulas are applied, several interesting loop and algebraic properties are observed on the structures so formed. The Cayley-Dickson formula is given by while the Smith-Conway doubling formula is . A Hadamard matrix of order is a matrix with entries such that where is the identity matrix. It is shown that the sign matrices for the frame multiplication under the Smith-Conway and Cayley-Dickson multiplications are Hadamard matrices. Kronecker products are also introduced, and it is shown that the sign matrices for the quaternion and octonion frames are equivalent to Kronecker products.

Affine–regular octahedron in GS–quasigroups

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

A golden section quasigroup (shortly GS-quasigroup) is defned as an idempotent quasigroup which satisfies the mutually equivalent identities $a(ab \cdot c) \cdot c = b$, $a \cdot (a \cdot bc)c = b$. In a general GS-quasigroup the geometrical concept of an affine–regular octahedron will be introduced. A number of statements about the relationships between an affine–regular octahedron and some other geometric concepts in a general GS-quasigroup will be proved. The geometrical representation of all proved statements will be given in the GS-quasigroup $\mathbb{C}(\frac{1}{2}(1+\sqrt{5}))$.

Parastrophically uncancellable quadratic quasigroup equations

Aleksandar Krapež (Serbian Academy of Sciences and Arts, Beograd, Serbia)

A general solution is given (in closed form) for an arbitrary equation of the type described in the title. A solution depends in an explicit way on the tree of the equation, the order of (object) variables occurring in the equation and the following parameters: one (abelian) group and three families of permutations. The permutations satisfy conditions which again depend on the tree of the equation and the order of variables in it.

SQBC - block cipher defined by small quasigroups

Smile Markovski (Ss Cyril and Methodius University, Skopje, Macedonia)
Coauthors: Vesna Dimitrova, Aleksandra Mileva

A block cipher is a symmetric key algorithm, which encrypts plaintext in fixed-length groups of bits, called blocks, with an unvarying transformation. There are almost no applications of quasigroup transformations for defining a block cipher. Here we propose a

new design of block ciphers SQBC (Small Quasigroup Block Cipher) based entirely on quasigroup transformations. The order n of the used quasigroups can be quite small, for example $n = 4$, $n = 16$ or $n = 256$. The design of SQBC is very flexible and one can choose different level of security and different kind of performances, by choosing the key length, the plaintext length and suitable quasigroups. In such a way, SQBC can be used for defining a lightweight block cipher, by taking the plaintext lengths of 64 bits. Several security aspects of SQBC have been investigated as well.

Obtaining cryptographic S-boxes from quasigroups

Hristina Mihajloska (University Ss. Cyril and Methodius, Skopje, Macedonia)
Coauthors: Danilo Gligoroski

We present a new method for constructing cryptographic 4×4-bit S-boxes from quasigroups of order 4. So far, cryptographers were constructing 4×4-bit S-boxes used in cryptographic primitives suitable for lightweight cryptography, only by exhaustive search of permutations of order 16. Our construction of 4×4-bit Quasigroup-S-boxes (Q-S-boxes) use orthogonal right quasigroups. Two right quasigroups h, g of order 4 are orthogonal if and only if there exist a quasigroup q of the same order such that $h \cdot q = g$. For every quasigroup out of 576 of order 4 we find all pairs of orthogonal right quasigroups that satisfy $h^{-1} \cdot g = q$. From these pairs of right quasigroups we made our Q-S-boxes, and we found 331,776 different 4×4-bit Q-S-boxes for every quasigroup. From cryptographic point of view for any S-box used in cryptographic designs the most important thing is to investigate its linear and differential characteristics. We have tested these characteristics of our Q-S-boxes and in this paper we give a comparison table with S-boxes used in PRESENT and Serpent block ciphers.

On some constructions of shapeless quasigroups

Aleksandra Mileva (University Goce Delcev, Štip, Macedonia)
Coauthors: Smile Markovski

In this paper we examine algebraic properties of quasigroups produced by diagonal method from orthomorphisms and we give a construction of shapeless quasigroups of different orders. We examine different types of Extended Feistel Networks (EFN) and Generalized Feistel-Non Linear Feedback Shift Registers (GF-NLFSR) as orthomorphisms of an abelian group $(G, +)$. It is shown that *type-1* EFN produced by a bijection is an orthomorphism of the abelian group $(G, +)$ and that GF-NLFSR produced by a bijection is an orthomorphism of the group $(\mathbb{Z}_2^m, \oplus)$. Also, we parameterized these orthomorphisms for the need of cryptography, so we can work with different quasigroups in every iterations of the future cryptographic primitives.

Characterization of left or right linear (T-linear) invertible algebras by functional equations

Yuri M. Movsisyan (Yerevan State University, Armenia)

An algebra, (Q, Σ), with quasigroup operations is called an invertible algebra. A binary algebra, $(Q; \Sigma)$, is called left linear (T-linear) if there exists a group (abelian group), $Q(\cdot)$,

such that every operation, $A \in \Sigma$, is determined by the rule:

$$A(x, y) = \varphi x \cdot \sigma y,$$

where $\varphi \in \operatorname{Aut} Q(\cdot)$ and $\sigma \in S_Q$. The concept of a right linear (T-linear) algebra is defined by the equality:

$$A(x, y) = \sigma x \cdot \psi y,$$

where $\psi \in \operatorname{Aut} Q(\cdot)$ and $\sigma \in S_Q$. A binary algebra, (Q, Σ), is called linear (T-linear) if there exists a group (abelian group), $Q(\cdot)$, such that every operation, $A \in \Sigma$, is determined by the rule:

$$A(x, y) = \varphi x \cdot t \cdot \psi y,$$

where $\varphi, \psi \in \operatorname{Aut} Q(\cdot)$ and $t \in Q$.

We give simple characterization of left or right linear (T-linear) invertible algebras by functional equations.

Projective realizations of loops and groups

Gabor Nagy (University of Szeged, Hungary)

Let Q be a loop. A *realization* of Q is a triple (α, β, γ) of maps from Q to the point set of the complex projective plane such that the points $\alpha(x), \beta(y), \gamma(z)$ are collinear if and only if $xy = z$. In fact, this is an embedding of the dual 3-net corresponding to Q.

The study of realizations is motivated by the construction of Sylvester-Gallai configurations. Recently, their investigation was renewed by Yuzvinsky, Dolgachev and their students. The basic construction of the realization of finite abelian groups is based on the abelian group structure on the cubic curve. Surprisingly, some nonabelian groups and even some nonassociative loops of order 5 and 6 can also be realized. (Stipins, Urzua.)

With G. Korchmaros and N. Pace we showed that if a finite group can be realized then it is either abelian, or dihedral, or the quaternion group of order 8. In my talk, I will explain the backgrounds, the main constructions and some tools from the proof of this theorem.

Isotopy-isomorphy properties of (r, s, t)-inverse loops

Yakub 'Tunde Oyebo (Lagos State University, Nigeria)
Coauthors: John O. Adéníran

In this paper, isotopy-isomorphy properties (r, s, t)-inverse loop is considered. We employed the use of derivatives of a function F on Q, to obtained some necessary and sufficient conditions for isotopic invariant of Q. Also, treading the same path with Bryant-Schneider, we obtained some new identities of Q. Some of these results were found to be true for m-inverse loops, whenever $r = t = m$ and $s = m + 1$.

Quasigroup identities on division algebras

José Pérez-Izquierdo (University of La Rioja, Spain)

In this talk we explore the consequences of quasigroup identities on the quasigroup of non-zero elements of a finite-dimensional real division algebra. Many of these identities

usually imply that the algebra is an isotope of a Hurwitz algebra. Our methods rely on the study of the tangent space of certain groups of autotopies.

Bol-Moufang groupoids of 'group-like' type

J.D. Phillips (Northern Michigan University, USA)

In this talk, we investigate conditions under which Bol-Moufang groupoids axiomatized as algebras of type $\langle 2, 1, 0\rangle$ (i.e., with two-sided identity element and inverses, in the manner of groups), are, in fact, loops.

More properties of minimally nonassociative Moufang loops

Andrew Rajah (Universiti Sains Malaysia, Penang, Malaysia)
Coauthors: Wing Loon Chee

The term 'minimally nonassociative Moufang loops' was first introduced by O. Chein and E. G. Goodaire in 2001. However, they defined minimally nonassociative Moufang loops as Moufang loops that are not associative but all proper subloops are associative. In this talk, we impose the additional condition 'all proper quotient loops are associative' to obtain some extra results.

On a class of left MQQs with degree invariant to parastrophy

Simona Samardjiska (Norwegian University of Science and Technology, Trondheim, Norway)
Coauthors: Danilo Gligoroski

A left quasigroup $(Q, *)$ of order 2^n that can be represented as a vector valued Boolean function of degree 2 is called a left multivariate quadratic quasigroup (LMQQ). For a given LMQQ we can define the parastrophe operation $\backslash_*$ by: $x\backslash_* y = z \Leftrightarrow x * z = y$ that also defines a left multivariate quasigroup. However, in general, $(Q, \backslash_*)$ is not quadratic. Even more, representing it in a symbolic form may require exponential time and space. In this work we investigate the problem of finding a subclass of LMQQs whose parastrophes are again quadratic, and in the same time can be easily constructed. Our class of LMQQs is linear in y, and their parastrophes can be easily expressed from the quasigroup operation. We give necessary and sufficient conditions for a LMQQ of this type to have a degree invariant to parastrophy, i.e. to have a parastrophe that is again a LMQQ. Based on this, we distinguish a spe cial class that satisfies our requirements and whose construction is deterministic and straightforward.

A-nuclei of a quasigroup

Victor A. Shcherbacov (Institute of Mathematics and Computer Science, Chisinau, Moldova)

Basic definitions are in [1].

Definition. The set of all autotopisms of the form $(\alpha, \varepsilon, \gamma)$ of a quasigroup $(Q, \circ)$, where ε is the identity mapping, is called the *left autotopy nucleus* (left A-nucleus) of quasigroup

$(Q, \circ)$.

Similarly, the sets of autotopisms of the forms $(\alpha, \beta, \varepsilon)$ and $(\varepsilon, \beta, \gamma)$ form the *middle and right A-nuclei* of $(Q, \circ)$. We shall denote these three sets of mappings by N_l^A, N_m^A and N_r^A respectively.

Definition. A quasigroup $(Q, \cdot)$ with transitive action on the set Q of at least one from its components of A-nuclei will be called *A-nuclear quasigroup.*

Theorem 1. *A quasigroup is A-nuclear if and only if it is group isotope.*

Definition. A quasigroup $(Q, \circ)$ is an $(\alpha; \beta; \gamma)$-inverse quasigroup if there exist permutations α, β, γ of the set Q such that $\alpha(x \circ y) \circ \beta x = \gamma y$ for all $x, y \in Q$ [2].

Theorem 2. *1. If $\alpha = \varepsilon$, then in $(\varepsilon; \beta; \gamma)$-inverse loop $(Q, \circ)$ $N_l = N_r = N_m \trianglelefteq Q$.*

2. If $\gamma = \varepsilon$, then in $(\alpha; \beta; \varepsilon)$-inverse loop $(Q, \circ)$ $N_l = N_r = N_m \trianglelefteq Q$.

3. If $\beta = \alpha^{-1}$, then in $(\alpha; \alpha^{-1}; \gamma)$-inverse loop $(Q, \circ)$ $N_l = N_r = N_m \trianglelefteq Q$.

4. If $\gamma = \beta^{-1}$, then in $(\alpha; \beta; \beta^{-1})$-inverse loop $(Q, \circ)$ $N_l = N_r = N_m \trianglelefteq Q$ [3].

[1] V. D. Belousov, Foundations of the Theory of Quasigroups and Loops, Moscow, Nauka, 1967, (in Russian).

[2] A. D. Keedwell, V. A. Shcherbacov, Quasigroups with an inverse property and generalized parastrophic identities, Quasigroups Relat. Syst., 13, 2005, 109-124.

[3] V. A. Shcherbacov. A-nuclei and A-centers of a quasigroup, http://arxiv.org/1102.3525, 2011.

On equational quasigroup definitions

Victor A. Shcherbacov (Institute of Mathematics and Computer Science, Chisinau, Moldova)
Coauthors: Dmitrii Pushkashu, Alexei Shcherbacov

Basic definitions are in [1, 2].

Garrett Birkhoff in his famous book [3] defined equational quasigroup as an algebra with three binary operations $(Q, \cdot, /, \backslash)$ that fulfils the following six identities

$$x \cdot (x \backslash y) = y \tag{1}$$

$$(y / x) \cdot x = y \tag{2}$$

$$x \backslash (x \cdot y) = y \tag{3}$$

$$(y \cdot x) / x = y \tag{4}$$

$$x / (y \backslash x) = y \tag{5}$$

$$(x / y) \backslash x = y \tag{6}$$

Theorem. [4]

1. An algebra $(Q, \cdot, \backslash, /)$ with identities (2), (3), (5) is a quasigroup.

2. An algebra $(Q, \cdot, \backslash, /)$ with identities (1), (4), (6) is a quasigroup.

3. *An algebra* $(Q, \cdot, \backslash, /)$ *with identities (1), (3), (5), (6) is a quasigroup.*

4. *An algebra* $(Q, \cdot, \backslash, /)$ *with identities (2), (4), (5), (6) is a quasigroup.*

5. *An algebra* $(Q, \cdot, \backslash, /)$ *with any five identities from identities (1)–(6) is a quasigroup.*

[1] V. D. Belousov. *Foundations of the Theory of Quasigroups and Loops*. Nauka, Moscow, 1967. (in Russian).

[2] V. A. Shcherbacov. Elements of quasigroup theory and some its applications in code theory, 2003. www.karlin.mff.cuni.cz/ drapal/speccurs.pdf.

[3] G. Birkhoff. *Lattice Theory*. Nauka, Moscow, 1984. (in Russian).

[4] V. A. Shcherbacov, D. I. Pushkashu, and A. V. Shcherbacov. Equational quasigroup definitions. *http://arxiv.org/*, arXiv:1003.3175:4 pages, 2010.

Invertibility of repetition compositions and its connection with orthogonality

Fedir M. Sokhatsky (Vinnytsia Institute of University 'Ukraina')
Coauthors: Iryna V. Fryz

Repetition-free composition of quasigroups is a quasigroup, but it is not true for repetition composition. Naturally there exists certain interest in finding an invertibility criterion: relationships under which composition of quasigroups is invertible. An invertibility criterion for repetition compositions of the same arity quasigroups follows from the results of V. D. Belousov [1], G. B. Belyavskaya [2], but it is unknown for different arities. Let g and h be quasigroup operations of the arities $n+1$ and $k+1$ respectively and υ be an arbitrary monotonically ascendant mapping from $\overline{0,k} := \{0, \dots, k\}$ to $\overline{0,n}$, where $k \leqslant n$. The terms $g(x_0, \dots, x_n)$ and $h(x_{\upsilon 0}, \dots, x_{\upsilon k})$ when $x_j = a_j$ for all $j \neq \upsilon m, \upsilon p$, where $p \neq m$, define a pair of binary operations, which will be called *υ-respective $\{m; p\}$-retracts*. The operations g and h are called *orthogonal of the type* (m, υ), if for all $p \in \overline{0,k} \backslash \{m\}$ their arbitrary pair of υ-respective $\{m; p\}$-retracts is orthogonal.

Theorem. *Let υ be an arbitrary monotonically ascendant mapping of the set $\overline{0,k}$ into $\overline{0,n}$, where $k \leqslant n$ and g, h be arbitrary $(n+1)$- and $(k+1)$-ary operations be defined on a set Q respectively and f be defined by*

$$f(x_0, \dots, x_n) = g(x_0, \dots, x_{\upsilon m-1}, h(x_{\upsilon 0}, \dots, x_{\upsilon k}), x_{\upsilon m+1}, \dots, x_n).$$

Then f is invertible iff g and $h^{(m)}$ are orthogonal of the type (m, υ).

It is well-known, to every n-ary quasigroup there corresponds an n-dimensional Latin hypercube and to k-tuple orthogonal n-ary quasigroup operations there corresponds a k-tuple orthogonal Latin hypercubes of dimension n. Thus the following question naturally arises: what relationship is there between the hypercubes corresponding to the orthogonal operations of the type (m, υ)? If all coordinates in a hypercube are fixed except m and p, then the obtained square will be called *$\{m, p\}$-slice*. Then two hypercubes H_1 and H_2 of dimensions $n+1$ i $k+1$ respectively, will be called *orthogonal of the type* (m, υ), if every $\{m, p\}$-slice of H_1 and every $\{\upsilon m, \upsilon p\}$-slice of H_2 are orthogonal for all $p \in \overline{0,k} \backslash \{m\}$. The theorem implies analogical statement for Latin hypercubes.

[1] Belousov V. D. Cross isotopy of quasigroup.// Quasigroups and their systems. Chishinau: Stiintsa, 1990. P. 14–20. (in Russian).

[2] Belyavskaya G. Pairwise ortogonality of n-ary operations. Buletinul academiei de stinte a Republicii Moldova. Matematica. No 3 (49), 2005. P. 5–18.

About classification of generalized functional equations on quasigroups

Fedir M. Sokhatsky (Vinnytsia Institute of University 'Ukraina')
Coauthors: Halyna V. Krainichuk

It is well known, that every quasigroup (i.e. invertible) function is a composition of binary invertible functions defined on the same set [1]. The problem is: *describe all such decompositions of the same invertible function*. The problem occurs in various branches of mathematics. For example, if a groupoid satisfies an identity $\omega = \upsilon$, then ω and υ are decompositions of a function. If we consider repetition-free composition only, then the problem has been solved in [2], where he has proved that every two full decompositions of a finite-valued strongly dependent function are almost the same (every invertible function is strongly dependent). There is a number of articles concerning the study of the repetition-free case of the problem, but the author has not come across any article devoted to the repetition case of the problem. We consider two of the possible decompositions of a ternary function: repetition-free de! compositions (for example, $g_1(x, g_2(y, z))$) and decompositions having two appearances of a subject variable (for example, $g_3(g_4(x, y), g_5(x, z))$). Equating these decompositions, we obtain a solution of one of the following type of functional equations (f.equ.): 1) *balanced*, i.e. (2;2;2)-type f.equ. (every subject variable has two appearances); 2) *distributive-like*, i.e. (3;2;2)-type f.equ.; 3) *Bol-Moufang type*, i.e. (4;2;2)-type f.equ.; 4) (3;3;2)-type f.equ.

Theorem 1. *Any generalized distributive-like functional equation without squares is parastrophically equivalent to exactly one of the following five functional equations:*

$$F_1(x; F_2(y; z)) = F_3(F_4(x; y); F_5(x; z));$$
$$F_1(y; F_2(x; z)) = F_3(F_4(y; F_5(x; z)); x);$$
$$F_1(F_2(x; y); y) = F_3(x; F_4(F_5(x; z); z));$$
$$F_1(F_2(x; y); y) = F_3(F_4(x; z); F_5(x; z));$$
$$F_1(y; F_2(x; z)) = F_3(y; F_4(x; F_5(x; z))).$$

The first of the functional equations is called a *functional equation of generalized left distributivity. "To find its all solutions over quasigroup functions of a set"* is a well known open problem. A partial case of this problem has been solved by V.D. Belousov [3]. All other four equations have been solved in [4].

Theorem 2. *Any generalized functional equation Bol-Moufang type without squares pa-*

rastrophically equivalent exactly one of the following eight functional equations:

$$
\begin{aligned}
&F_1(x;F_2(y;F_3(x;z))) = F_4(z;F_5(x;F_6(x;y))),\\
&F_1(F_2(x;y);F_3(x;y)) = F_4(F_5(x;z);F_6(x;z)),\\
&F_1(F_2(F_3(y;x);x);z) = F_4(y;F_5(x;F_6(x;z))),\\
&F_1(F_2(x;y);z) = F_3(x;F_4(x;F_5(x;F_6(y;z)))),\\
&F_1(x;F_2(F_3(x;y);y)) = F_4(x;F_5(F_6(x;z);z)),\\
&F_1(x;F_2(F_3(x;y);y)) = F_4(F_5(x;F_6(x;z));z),\\
&F_1(y;F_2(x;F_3(x;z))) = F_4(y;F_5(x;F_6(x;z))),\\
&F_1(x;F_2(x;F_3(x;y))) = F_4(F_5(F_6(x;z);z);y).
\end{aligned}
$$

The first equation of Theorem 2 is well known Bol equation [5]. Finding of full solutions set of Moufang equation over set of quasigroup operation is also known problem in theory of functional equations and quasigroups theory. All other seven equations have been solved.

[1] Glukhov M.M. About α-closed classes and α-complete systems of functions of k-valued logic. // Discrete mathematics, 1989. **1**, No 1. – P.16–21.

[2] Fedir M. Sokhatsky. The Deepest Repetition-Free Decompositions of Non-Singular Functions of Finite Valued Logics. Proceeding of the 26-th International symposium on Multiple-Valued Logic (May 29-31, 1996, Santiago de Compostela, Spain), 279–282.

[3] Some remarks on the functional equation of generalized distributivity. Aequationes Mathematicae. **1**, fasc.1/2, 1968.- 54–65.

[4] Sokhatsky F. M., Krainichuk H. V. Solving of some functional equations having invertible binary functions: Academician Ya.S. Pidstryhach conference of young scientist 'Modern problems of mathematics and mechanics' Lviv Ivan Franko State University, - Lviv, - 2009. (Ukrainian)

[5] Belousov V. D., Kannappan P. L. Generalized Bol functional equation // Pacific journal of mathematics: **35**, No 2, 1970, 259–265.

Nuclear extension of quasigroups

Izabella Stuhl (University of Debrecen, Hungary)
Coauthors: Péter T. Nagy

We study the right nuclei of quasigroups with right unit element. An extension process is investigated in this category of quasigroups, which is defined by a slight modification of non-associative Schreier-type extensions of groups or loops. We give characterizations of quasigroup extensions satisfying particular nuclear conditions. These results are applied for constructions of right nuclear quasigroup extensions with right inverse property having a prescribed right nucleus.

Quasiidentities of finitely generated nilpotent Moufang loop

Vasilii Ursu (Technical University, Chisinau, Moldova)

The problem about finite basis of quasi-identities for finitely generated nilpotent Moufang loop is solved.

Pentagonal quasigroups

Stipe Vidak (University of Zagreb, Croatia)

A pentagonal quasigroup is an idempotent medial quasigroup which satisfies additional identity $((ab \cdot a) \cdot b) \cdot a = b$. Along with that identity, some other algebraic identities and their mutual relations are studied. The geometrical concepts of parallelogram, midpoint and regular pentagon can be defined in a general pentagonal quasigroup. The geometrical representation of these concepts and relations between them will be given in the quasigroup $C(q)$, where q is a solution of the equation $q^4 - 3q^3 + 4q^2 - 2q + 1 = 0$. The characterization of pentagonal quasigroups using abelian groups with automorphism φ which satisfies $\varphi^4 - 3\varphi^3 + 4\varphi^2 - 2\varphi + 1 = 0$ is given. This characterization gives an algorithm for construction of some finite pentagonal quasigroups.

Towards the classification of left distributive quasigroups

Jan Vlachý (Universiteit Utrecht, Netherlands)

A left distributive quasigroup (LDQ) is a quasigroup satisfying

$$x(yz) = (xy)(xz).$$

In this talk I will mention some (both classical and recent) results related to the classification of finite LDQ. The original motivation for my work on LDQ stemmed from the eighth Belousov's problem. LDQ are moreover interesting as a special case of *quandles*. In contrast to a general quasigroup, there are methods which make LDQ more amenable to investigation: Galkin proved that every finite LDQ can be represented as $(G/T, \circ)$, where G is a finite group, T is the subgroup of fixed points for a suitable automorphism ϕ of G and the binary operation on cosets is given by

$$xT \circ yT = x\phi(x^{-1}y)T.$$

Yet another recent approach to LDQ will be also mentioned. In the end, some recent interesting results obtained using the above methods will be mentioned: classification of simple LDQ and classification of LDQ of order p^2.

Probability distributions convoluted by quasigroups

Alexey Yashunsky (Keldysh Institute of Applied Mathematics, Moscow, Russia)

Let Q be a finite binary quasigroup, with multiplication $\cdot$ and left division $/$. We consider probability distributions over Q. The convolution $u*v$ of two distributions u and v is defined as a distribution whose components are $(u * v)_i = \sum_{j \in Q} u_{i/j} v_j$. Starting from an initial distribution π one may apply multiple convolutions. This procedure can be represented by an oriented binary planar tree with leaves labeled by π and inner nodes labeled by convolutions of inbound distributions. The root distribution is then the result of an iterated convolution. It is shown that if the initial distribution support (the elements $i \in Q$ such that $\pi_i > 0$) contains more than a half of Q's elements, iterated convolutions approach the uniform distribution over Q, exponentially in tree depth. This is not necessarily true for initial distributions with a smaller support, yet the average of iterated convolutions

with a given depth always converges to a uniform distribution over some subquasigroup of Q, exponentially in depth. Similar results hold for averages over convolutions with a given number of inner nodes. These results generalize known properties of random walks on finite groups.