LOOPS 2019 Conference

July 7, 2019 – July 13, 2019

Budapest University of Technology and Economics, Hungary

This is a conference about loops, quasigroups and the related geometric, algebraic and combinatorial structures:

- nonassociative algebras and semifields
- loops in group theory
- loops in universal algebra
- loops in combinatorics
- quandles

Invited speakers

- Nicholas Cavenagh (New Zealand)
  Trades and defining sets in Latin squares and related combinatorial arrays
- Jose Maria Pérez-Izquierdo (Spain)
  Applications of nonassociative Hopf algebras to loop theory
- Simona Samardjiska (The Netherlands)
  Quasigroups for cryptography
- Jonathan D. H. Smith (USA)
  Augmented quasigroups: From group duals to Heyting algebras
- David Stanovský (Czech Republic)
  Quasigroups and the Yang-Baxter equation
- Petr Vojtěchovský (USA)
  Enumeration of racks, quandles and Bruck loops
- Yue Zhou (China)
  Semifields, planar functions and MRD codes

Scientific Board

- Piroska Csörgő (Eger, Hungary), Ágota Figula (Debrecen, Hungary), Alexander Grishkov (São Paulo, Brazil), Michael Kinyon (Denver, USA), Alexander Pott (Magdeburg, Germany), Victor Shcherbacov (Chişinău, Republic of Moldova), Jonathan D. H. Smith (Ames, USA), David Stanovský (Prague, Czech Republic), Petr Vojtěchovský (Denver, USA), Ian Wanless (Melbourne, Australia)

Local organiser

- Gábor P. Nagy, Algebra Department of the Budapest University of Technology
- Conference web page: https://algebra.math.bme.hu/LOOPS19/
- Conference email address: loops19@math.bme.hu

Programme

Monday, July 8, 2019

08:00 – 09:15	*Registration*
09:15 – 09:30	*Opening*
09:30 – 10:30	**Petr Vojtechovsky** (University of Denver, USA) *Enumeration of racks, quandles and Bruck loops*
10:30 – 11:00	**Coffee break**
11:00 – 11:30	**Piroska Csörgő** (Eszterhazy Karoly University, Hungary) *Every Moufang loop of odd order has nontrivial nucleus*
11:30 – 11:55	**Lee Raney** (University of North Alabama, USA) *Commutative automorphic loops arising from groups*
11:55 – 12:20	**Mariah Barnes** (University of Denver, USA) *Quasigroups Isotopic to Commutative Moufang Loops*
12:20 – 14:30	**Lunch break**
14:30 – 14:55	**Seonmi Choi** (Kyungpook National University, South Korea) *On marked Conway algebras and their invariants*
14:55 – 15:20	**Byeorhi Kim** (Kyungpook National University, South Korea) *On relationship between a 2nd group cohomology group and a 2nd quandle cohomology group*
15:20 – 15:50	**Coffee break**
15:50 – 16:15	**Alexey Yashunsky** (Keldysh Institute of Applied Mathematics, Moscow, Russia) *Can quasigroup transformations of random variables be spoofed?*
16:15 – 16:40	**Janusz Grabowski** (Polish Academy of Sciences, Poland) *Tangent and cotangent loopoids*
16:40 – 17:05	**Parascovia Syrbu** (Moldova State University, Moldova) *On total multiplication groups of loops*
17:05 – 17:30	**Izabella Stuhl** (Penn State, USA) *On some progress in Steiner loops*

Tuesday, July 9, 2019

09:00 – 10:00	**Nicholas Cavenagh** (University of Waikato, New Zealand) *Trades and defining sets in Latin squares and related combinatorial arrays*
10:00 – 10:25	**Stefanie Wang** (Smith College, USA) *Counting Quasigroup Words*
10:25 – 10:55	**Coffee break**
10:55 – 11:25	**Ivan Deriyenko** (Ukraine) *Rectangular Transformations in Latin Squares*
11:25 – 11:50	**Mark Greer** (University of North Alabama, USA) *Complete graph decompositions and P-groupoids*
11:50 – 12:15	**Ian Wanless** (Monash University, Australia) *Generalised transversals of Latin squares*

12:15 – 14:30	**Lunch break**
14:30 – 15:30	**Yue Zhou** (National University of Defense Technology, China) *Semifields, planar functions and MRD codes*
15:30 – 15:55	**Agota Figula** (University of Debrecen, Hungary) *Affine Steiner loops*
15:55 – 16:25	**Coffee break**
16:25 – 16:50	**Eugene Kuznetsov** (Institute of Mathematics and Computer Science, Moldova) *Algebraic structures related with finite projective planes*
16:50 – 17:15	**Alex Nowak** (Iowa State University, USA) *On the classification of distributive Mendelsohn triple systems*
17:15 – 17:40	**Žaneta Semanišinová** (Charles University, Prague, Czech Republic) *Paramedial quasigroups of prime and prime square order*
17:40 – 18:05	**Alexander Pott** (Otto von Guericke University, Germany) *Partial almost perfect nonlinear permutations*

Wednesday, July 10, 2019

09:00 – 10:00	**David Stanovský** (Charles University, Prague, Czech Republic) *Quasigroups and the Yang-Baxter equation*
10:00 – 10:25	**Přemysl Jedlička** (Czech University of Life Sciences, Prague, Czech Republic) *Yang-Baxter equation and a congruence of biracks*
10:25 – 10:55	**Coffee break**
10:55 – 11:20	**Agata Pilitowska** (Warsaw University of Technology, Poland) *2-permutational left-quasigroups*
11:20 – 11:45	**Anna Zamojska-Dzienio** (Warsaw University of Technology, Poland) *Distributive biracks*
11:45 – 12:10	**Jieon Kim** (Pusan National University, South Korea) *Biquandle cocycle invariants of surface-links*
12:10 – 12:35	**Pavol Zlatoš** (Comenius University, Slovakia) *The Finite Embedding Property for IP Loops and Local Embeddability of Groups into Finite IP Loops*
12:35 – 15:00	**Lunch break**
15:00 – 19:00	*Cultural programme*

Thursday, July 11, 2019

09:00 – 10:00	**Jose Maria Pérez-Izquierdo** (Universidad de La Rioja, Spain) *Applications of nonassociative Hopf algebras to loop theory*
10:00 – 10:25	**Dylene Agda Souza de Barros** (Universidade Federal de Uberlândia, Brazil) *The free commutative automorphic 2-generated loop of nilpotency class 3*
10:25 – 10:55	**Coffee break**
10:55 – 11:20	**Kenneth Johnson** (Penn State Abington, USA) *Projective representations for loops*
11:20 – 11:45	**Anna Romanowska** (Warsaw University of Technology, Poland) *Beyond barycentric algebras and convex sets*

11:45 – 12:10	**Branimir Seselja** (University of Novi Sad, Serbia) *Ω-groupoids and Ω-quasigroups*
12:10 – 14:10	**Lunch break**
14:10 – 14:30	**Petr Vojtechovsky** (University of Denver, USA) *Highlights from the research of Jonathan D.H. Smith*
14:30 – 15:30	**Jonathan D. H. Smith** (Iowa State University, USA) *Augmented quasigroups: From group duals to Heyting algebras*
15:30 – 16:00	**Coffee break**
16:00 – 16:25	**Aleksandar Krapez** (Mathematical Institute SASA, Serbia) *Functional Equations and their Graphs*
16:25 – 16:50	**Fedir Sokhatsky** (Vasyl Stus Donetsk National University, Ukraine) *TBA*
16:50 – 17:15	**Victor Shcherbacov** (Institute of Mathematics and Computer Science, Moldova) *Units in quasigroups with Bol-Moufang type identities*
17:15 – 17:40	**J.D. Phillips** (Northern Michigan University, USA) *Generalized Bol-Moufang loop varieties – not just for breakfast!*
19:30 – 22:00	*Conference dinner*

Friday, July 12, 2019

09:00 – 10:00	**Simona Samardjiska** (Radboud University, The Netherlands) *Quasigroups for cryptography*
10:00 – 10:25	**Nadezhda Malyutina** (State University Dimitrie Cantemir, Moldova) *Cryptanalysis of some stream ciphers*
10:25 – 10:55	**Coffee break**
10:55 – 11:20	**Tomas Nagy** (Charles University, Prague, Czech Republic) *Left distributive quasigroups of order 2^k*
11:20 – 11:45	**Rosemary Miguel Pires** (Fluminense Federal University, Brazil) *Representations of code loops by binary codes*
11:45 – 12:10	**Vasile Ursu** ("Simion Stoilow" Institute of Mathematics of the Romanian Academy Technical University of Moldova, Moldova) *Archimedes automorphic loops*
12:10 – 14:20	**Lunch break**
14:20 – 14:45	**Ales Drapal** (Charles University, Prague, Czech Republic) *Quasigroups with very few associative triples*
14:45 – 15:10	**Heghine Ghumashyan** (Vanadzor State University, Armenia) *Essentially equivalence of hyperidentities in semigroups*
15:10 – 15:40	**Coffee break**
15:40 – 16:30	*Panel discussion on the future of LOOPS*
16:30 – 16:45	*Closing*

List of participants

№	Name	Affiliation
1.	Mariah Barnes	University of Denver (USA) mariah.barnes@du.edu
2.	Nicholas Cavenagh	University of Waikato (New Zealand) nicholas.cavenagh@waikato.ac.nz
3.	Seonmi Choi	Kyungpook National University (South Korea) csm123c@gmail.com
4.	Piroska Csörgő	Eszterhazy Karoly University (Hungary) piroska.csorgo@gmail.com
5.	Ivan Deriyenko	Ukraine ivan.deriyenko@gmail.com
6.	Ales Drapal	Charles University, Prague (Czech Republic) drapal@karlin.mff.cuni.cz
7.	Clifton Edgar Ealy Jr.	Western Michigan University (USA) clifton.e.ealy@wmich.edu
8.	Agota Figula	University of Debrecen (Hungary) figula@science.unideb.hu
9.	Marcell Gaál	Rényi Institute (Hungary) marcell.gaal.91@gmail.com
10.	Heghine Ghumashyan	Vanadzor State University (Armenia) hgumashyan@mail.ru
11.	Janusz Grabowski	Polish Academy of Sciences (Poland) jagrab@impan.pl
12.	Mark Greer	University of North Alabama (USA) mgreer@una.edu
13.	Alexander Grishkov	University of Sao Paulo (Brazil) shuragri@gmail.com
14.	Přemysl Jedlička	Czech University of Life Sciences, Prague (Czech Republic) jedlickap@tf.czu.cz
15.	Suhyeon Jeong	Pusan National University (South Korea) j00399501303@gmail.com
16.	Kenneth Johnson	Penn State Abington (USA) kwj1@hotmail.com
17.	Jelena Jovanović	Union University Belgrade (Serbia) jelena.jovanovic55@gmail.com

№	Name	Affiliation
18.	Byeorhi Kim	Kyungpook National University (South Korea) kbrdooly@naver.com
19.	Jieon Kim	Pusan National University (South Korea) jieonkim7@gmail.com
20.	Michael Kinyon	University of Denver (USA) mkkinyon@gmail.com
21.	Aleksandar Krapez	Mathematical Institute SASA (Serbia) sasa@mi.sanu.ac.rs
22.	Eugene Kuznetsov	Institute of Mathematics and Computer Science (Moldova) kuznet1964@mail.ru
23.	Nadezhda Malyutina	State University Dimitrie Cantemir (Moldova) 231003.bab.nadezhda@mail.ru
24.	Rosemary Miguel Pires	Fluminense Federal University (Brazil) rosemarypires@id.uff.br
25.	Gábor P. Nagy	Budapest University of Technology and University of Szeged (Hungary) nagyg@math.bme.hu
26.	Péter T. Nagy	Óbuda University (Hungary) nagy.peter@nik.uni-obuda.hu
27.	Tomas Nagy	Charles University, Prague (Czech Republic) tomas.nagy@email.com
28.	Alex Nowak	Iowa State University (USA) anowak@iastate.edu
29.	Yakub Oyebo	Lagos State University (Nigeria) yakub.oyebo@lasu.edu.ng
30.	Oyeyemi Oyebola	Federal University of Agriculture Abeokuta (Nigeria) oooyeyemi@gmail.com
31.	Jose Maria Pérez-Izquierdo	Universidad de La Rioja (Spain) jm.perez@unirioja.es
32.	J.D. Phillips	Northern Michigan University (USA) jophilli@nmu.edu
33.	Agata Pilitowska	Warsaw University of Technology (Poland) apili@mini.pw.edu.pl
34.	Alexander Pott	Otto von Guericke University (Germany) alexander.pott@ovgu.de

№	Name	Affiliation
35.	Lee Raney	University of North Alabama (USA) lraney@una.edu
36.	Marina Rasskazova	Omsk State Technic University (Russia) marinarasskazova@yandex.ru
37.	Anna Romanowska	Warsaw University of Technology (Poland) A.Romanowska@mini.pw.edu.pl
38.	Simona Samardjiska	Radboud University (The Netherlands) simonas@cs.ru.nl
39.	Žaneta Semanišinová	Charles University, Prague (Czech Republic) zaneta.semanisinova@gmail.com
40.	Branimir Seselja	University of Novi Sad (Serbia) seselja@dmi.uns.ac.rs
41.	Victor Shcherbacov	Institute of Mathematics and Computer Science (Moldova) victor.scerbacov@math.md
42.	Jonathan Smith	Iowa State University (USA) jdhsmith@iastate.edu
43.	Fedir Sokhatsky	Vasyl Stus Donetsk National University (Ukraine) fmsokha@ukr.net
44.	Dylene Agda Souza de Barros	Universidade Federal de Uberlândia (Brazil) dyagda@gmail.com
45.	David Stanovsky	Charles University, Prague (Czech Republic) david.stanovsky@gmail.com
46.	Izabella Stuhl	Penn State (USA) stuhlizabella@gmail.com
47.	Parascovia Syrbu	Moldova State University (Moldova) syrbuviv@yahoo.com
48.	Abdullo Tabarov	Academy of Science of Tajikistan (Tajikistan) tabarov2010@gmail.com
49.	Vasile Ursu	"Simion Stoilow" Institute of Mathematics; Technical University of Moldova Vasile.Ursu@imar.ro
50.	Petr Vojtechovsky	University of Denver (USA) petr@math.du.edu
51.	Stefanie Wang	Smith College (USA) sgwang.math@gmail.com

№	Name	Affiliation
52.	Ian Wanless	Monash University (Australia) ian.wanless@monash.edu
53.	Alexey Yashunsky	Keldysh Institute of Applied Mathematics, Moscow (Russia) yashunsky@keldysh.ru
54.	Li Yubo	National University of Defense Technology (China) leeub_0425@hotmail.com
55.	Anna Zamojska-Dzienio	Warsaw University of Technology (Poland) A.Zamojska-Dzienio@mini.pw.edu.pl
56.	Yue Zhou	National University of Defense Technology (China) yue.zhou.ovgu@gmail.com
57.	Pavol Zlatoš	Comenius University (Slovakia) zlatos@fmph.uniba.sk

Abstracts of main talks

Trades and defining sets in Latin squares and related combinatorial arrays

Nicholas Cavenagh

University of Waikato (New Zealand)

Latin squares are an example of an array where for each row, column (and sometimes cell), the frequency of each element is prescribed. Other examples include 0-1 matrices, frequency squares and the many generalizations of Latin squares such as Latin cubes and multi-Latin squares. For each of these combinatorial structures, we may ask: What is the minimum amount of information needed to define the structure uniquely? What is the minimum amount of information possible to change one structure to another of the same order? When can a partial structure be completed?

These interrelated questions all relate to the idea of a combinatorial trade – this is a substructure which may be replaced with a disjoint "trade mate" to obtain another array satisfying the same parameters. We first take a global look at arrays with prescribed row and column frequencies to see what properties all (or many) of these arrays have in common. One such property is that the smallest possible trade is always an intercalate, equivalently a Latin subsquare of order 2. Any trade in the arrays of interest can be thought of in some sense as a "sum" of intercalates. We will also look more specifically on the above questions, where techniques and proofs may be specific to certain types of arrays. Here we will focus mostly on Latin squares. The aim will be to give a survey which will highlight both the variety of proof techniques and connections with other branches of mathematics.

Applications of nonassociative Hopf algebras to loop theory

José M. Pérez-Izquierdo

Universidad de La Rioja (Spain)

Nonassociative Hopf algebras allow an algebraic approach to the infinitesimal theory of analytic loops from a formal point of view.

In this talk, after reviewing the foundations of nonassociative Hopf algebras, I will present some recent applications of them to the theory of loops. For instance, I will discuss a general nonassociative Baker-Campbell-Hausdorff formula developed under this perspective, the embedding of free loops as loops of formal power series on nonassociative and noncommutative variables, and several results on the integration of tangent algebras to formal loops.

Quasigroups for Cryptography

Simona Samardjiska

Digital Security Group, Radboud University (The Netherlands)

Quasigroups have been used in more than a dozen cryptographic designs over the past two decades. Admittedly, the success of these designs has been varying. Although many of them caught the attention of the cryptographic community, they were either broken, or it proved difficult to gain the necessary confidence in their security. The main reason is the lack of systematic analysis of the desired properties established as crucial for cryptographic use. Indeed, very few papers deal with this issue and usually provide criteria that are incompatible with the cryptographic practice.

With this talk I hope to spark your interest in this matter and introduce you to some of the most important and well established criteria for functions for cryptographic use. I will focus on several criteria important both for symmetric and assymetric cryptography. Among others, I will talk about linear and differential properties of vectorial functions and how they relate to the state of the art attacks. I will further discuss in this context some of the good and bad choices made in previous cryptographic designs using quasigroups. The lessons learned will hopefully be insightful enough to lead to new ideas in constructing quasigroups that have strong cryptographic properties. I will further, yet again, raise the question whether hard problems on quasigroups can be successfully used in public key cryptography.

Augmented quasigroups: From group duals to Heyting algebras

Jonathan D. H. Smith

Iowa State University (USA)

Compact closed categories are categories that abstract the basic features of the duality between finite-dimensional vector spaces and the spaces of linear functionals on them. Examples beyond the motivating categories of vector spaces include the category of relations on sets, the category of finite-dimensional Hilbert spaces, categories of finitely-generated free semimodules over commutative semirings, and Joyal's category of Conway games.

Augmented magmas and augmented quasigroups are structures defined in compact closed categories. Together with a comultiplication and an augmentation, augmented magmas include a multiplication structure where the products take values in the dual space. An augmented magma is an augmented quasigroup if its multiplication structure twists to right and left division structures which also form augmented magmas.

The characters of a finite group form an augmented quasigroup in the compact closed category of finitely-generated free commutative monoids. The augmented quasigroup is a quotient of a quasigroup by an equivalence relation that is not necessarily a congruence relation. The quasigroup has the same order as the group, and is a natural candidate for being a dual of the original finite group.

Quasigroups, and quasigroup-like relational structures with set-valued products, form augmented quasigroups in the category of relations on sets. In particular, certain such augmented quasigroups are defined by Heyting algebras (e.g., lattices of open sets on a topological space, or sets of truth values for intuitionistic logic). Hitherto, the only known tight connection between Heyting algebras and quasigroups was that both form Mal'cev varieties.

Quasigroups and the Yang-Baxter equation

David Stanovský

Charles University, Prague (Czech Republic)

I will discuss two classes of quasigroups that can be interpreted as set-theoretic solutions to the quantum Yang-Baxter equation, their similarities and fundamental differences. One of them is the well known class of (left) self-distributive quasigroups (or latin quandles, in an alternative terminology). I will briefly review some older and newer results on the representation, structure and enumeration, including the recent project with Marco Bonatto on the commutator theory for quandles. The other one is the class of quasigroups satisfying the identity $(xy)(xz) = (yx)(yz)$. I will report on our initial results with Bonatto, Kinyon and Vojtechovsky, leading to interesting open problems.

Enumeration of racks, quandles and Bruck loops

Petr Vojtěchovský

University of Denver (USA)

We present recent enumeration results for racks, quandles and Bruck loops. The enumeration of racks and quandles is based on the Joyce-Blackburn representation in transitive permutation groups, while the enumeration of Bruck loops is mostly based on central extensions. We will also mention connections with commutative automorphic loops and Γ-loops.

(Involutory) racks and quandles are algebraic structures designed to capture Reidemeister moves on (un)oriented knots—they are left quasigroups satisfying the left distributive law $x(yz) = (xy)(xz)$. We enumerate racks and quandles up to order $n \leqslant 13$, improving upon previously known results for $n \leqslant 8$ and $n \leqslant 9$, respectively. We rely in part on the enumeration of 2-reductive racks by Jedlička, Pilitowska, Stanovský and Zamojska-Dzienio.

Bruck loops are Bol loops satisfying the automorphic inverse property $(xy)^{-1} = x^{-1}y^{-1}$. By a result of Kikkawa and Robinson, uniquely 2-divisible Bruck loops are in one-to-one correspondence with involutory latin quandles. Glauberman proved that Bruck loops of odd order are solvable and Bruck loops of odd prime power order are centrally nilpotent. We enumerate Bruck loops of odd order p^k for small values of p and k.

Greer established a one-to-one correspondence between Bruck loops of odd order and Γ-loops of odd order, the latter class properly containing commutative automorphic loops of odd order. For which order $n = p^k$ are all Γ-loops commutative automorphic loops? The answer is positive for odd p^3: there are 7 commutative automorphic loops of order p^3 by a result of de Barros, Grishkov and the author, and there are 7 involutory latin quandles of order p^3 by a recent result of Bianco and Bonatto. The answer is negative for $n = 3^5$, while the case $n = p^4$ remains open.

This is joint work with Izabella Stuhl and Seung Yeop Yang.

References

[1] Giuliano Bianco and Marco Bonatto, *On connected quandles of prime power order*, preprint, arXiv:1904.12801.

[2] Simon R. Blackburn, *Enumerating finite racks, quandles and kei*, Electron. J. Combin. **20** (2013), no. **3**, Paper 43, 9 pp.

[3] Dylene Agda De Barros, Alexander Grishkov and Petr Vojtěchovský, *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), no. **5**, 1250100, 15 pp.

[4] George Glauberman, *On loops of odd order*, J. Algebra **1** (1964), 374–396.

[5] George Glauberman, *On loops of odd order II*, J. Algebra **8** (1968), 393–414.

[6] Mark Greer, *A class of loops categorically isomorphic to Bruck loops of odd order*, Comm. Algebra **42** (2014), no. **8**, 3682–3697.

[7] Přemysl Jedlička, Agata Pilitowska, David Stanovský and Anna Zamojska-Dzienio, *The structure of medial quandles*, J. Algebra **443** (2015), 300–334.

[8] David Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), no. **1**, 37–65.

[9] Michihiko Kikkawa, *On some quasigroups of algebraic models of symmetric spaces*, Mem. Fac. Lit. Sci. Shimane Univ. Natur. Sci. No. **6** (1973), 9–13.

[10] Michael K. Kinyon, Gábor P. Nagy and Petr Vojtěchovský, *Bol loops and Bruck loops of order pq*, J. Algebra **473** (2017), 481–512.

[11] D.A. Robinson, *A loop-theoretic study of right-sided quasigroups*, Ann. Soc. Sci. Bruxelles Sr. I **93** (1979), no. 1, 7–16.

[12] Izabella Stuhl and Petr Vojtěchovský, *Enumeration of involutory Latin quandles, Bruck loops and commutative automorphic loops of odd prime power order*, Nonassociative mathematics and its applications 261-276, Contemp. Math., **721**, Amer. Math. Soc., Providence, RI, 2019.

[13] Petr Vojtěchovský and Seung Yeop Yang, *Enumeration of racks and quandles up to isomorphism*, Math. Comp. **88** (2019), no. **319**, 2523–2540.

Abstracts of contributed talks

Quasigroups Isotopic to Commutative Moufang Loops

Mariah Barnes

University of Denver (United States)

(Joint work with M.K. Kinyon)

One of the important ways in which quasigroups are studied is through their loop isotopes. For some interesting varieties of quasigroups, it turns out that these loop isotopes live in some highly structured class of loops in such a way that the quasigroups can be represented in terms of those loops. This has been accomplished largely through the work of Bruck, Murdoch, Toyoda, Kepka, and Němac for quasigroups isotopic to abelian groups, and our goal in this talk will be to explore the natural generalization to quasigroups isotopic to commutative Moufang loops.

In particular, for a quasigroup $(Q, \cdot)$, it can be shown that all principal loop isotopes $(Q, +_e)$ of the form $x +_e y = (x/e)(e\backslash y)$ are commutative Moufang loops if and only if $(Q, \cdot)$ satisfies the identity (Q1): $x(y\backslash(zz)) = z(y\backslash(xz))$.

Furthermore, the following holds:

Theorem 1. *For a quasigroup $(Q, \cdot)$, TFAE:*

1. *For each $e \in Q$, $(Q, \cdot)$ is affine over a commutative Moufang loop $(Q, +_e)$;*
2. *Q satisfies (Q1) and the following identities:*

$$(xx \cdot yz)/(xz) = (xx \cdot yu)/(xu), \tag{1}$$

$$(zx)\backslash(zy \cdot xx) = (ux)\backslash(uy \cdot xx); \tag{2}$$

3. *Q satisfies (Q1) and the following identities:*

$$(xx \cdot yz)/(yx) = (xx \cdot uz)/(ux), \tag{3}$$

$$(xy)\backslash(zy \cdot xx) = (xu)\backslash(zu \cdot xx). \tag{4}$$

Lastly, we will apply this theorem to specific classes of quasigroups to obtain a full characterization of these quasigroups in terms of their commutative Moufang loop isotopes.

On marked Conway algebras and their invariants

Seonmi Choi

Kyungpook National University (South Korea)

(This is a joint work with Y. Bae and S. Kim.)

In 1987, the HOMFLY-PT polynomial is a 2-variable polynomial invariant discovered by Hoste, Ocneanu, Millett, Freyd, Lickorish, Yetter, Przytycki and Traczyk. Przytycki and Traczyk introduced a new algebraic structure, called *the Conway algebra*, and constructed invariants of oriented links valued in Conway algebras. The HOMFLY polynomial can be obtained from the invariant. In 2018, Kim constructed a generalized Conway algebra, which is an algebraic structure with two skein relations related to a self crossing and a mixed crossing. A generalized Conway algebra can be used to construct polynomial invariants. In this talk, we deal with surface-links in a 4-dimensional space represented by marked graph diagrams. In 2017, Joung, Kamada, Kawauchi and Lee constructed a polynomial invariant of oriented surface-links by using marked graph diagrams. We will define a generalization of a Conway algebra, which is called *a marked Conway algebra*, and construct invariants for oriented surface-links valued in marked Conway algebras. The polynomial invariant constructed by Joung, Kamada, Kawauchi and Lee is obtained from the invariant valued in the marked Conway algebra satisfying additional conditions. In the end of this talk, we will also introduce a generalized marked Conway algebra and construct invariants.

Every Moufang loop of odd order has nontrivial nucleus

Piroska Csörgő

Eszterházy Károly University, Eger (Hungary)

Glauberman and Doro studied the structure of Moufang loops of odd order. Glauberman proved that Feit–Thompson's Theorem can be extended to Moufang loops, namely every Moufang loop of odd order is solvable. It turned out that the multiplication group G of a Moufang loop of odd order with trivial nucleus is a group with triality, i.e. $S_3 \leqslant \operatorname{Aut} G$ with special identities.

One of the main problems in Moufang loops: Does there exist a Moufang loop of odd order with trivial nucleus? We give a negative answer by proving that every Moufang loop of odd order has nontrivial nucleus.

Key words: Moufang loop, nucleus, center, commutant, multiplication group, inner mapping group, central nilpotence.

2000 Mathematics Subject Classification: 20N05, 08A05.

Rectangular Transformations in Latin Squares

Ivan Deriyenko

Ukraine

The *distance* between two latin squares $||a_{ij}||$ and $||b_{ij}||$ of the same size $n > 2$ is equal to the number of cells in which the corresponding elements a_{ij} and b_{ij} are not equal. The minimal distance between two latin squares is equal 4 [1].

We say that elements $x, y, z, u \in Q$, $x \neq z$, $y \neq u$, determine a *rectangle* in a quasigroup Q if $xy = zu = a$ and $xu = zy = b$ for some $a, b \in Q$. Vertices of such rectangle have the form xy, xu, zx and zu. Such determined rectangle will be denoted by $\langle x, y, z, u\rangle$ or by $\langle x, u, z, y\rangle$.

Theorem 1. *Isotopic* (*antiisotopic*) *quasigroups have the same number of rectangles.*

An interesting question is how to find rectangles in a given quasigroup. Direct calculation of $\langle x, y, z, u\rangle$ is rather trouble. We present simplest method based on left translations.

Two rectangles $\langle x, y, z, u\rangle$ and $\langle x', y', z', u'\rangle$ of a quasigroup $(Q, \cdot)$ are *equivalent* if there exists an autotopism (α, β, γ) of $(Q, \cdot)$ such that $\alpha(x) = x'$, $\beta(y) = y'$, $\alpha(z) = z'$ and $\beta(u) = u'$.

Theorem 2. *A rectangle transformation by equivalent rectangles gives isotopic quasigroups.*

References

[1] A. Drápal, Hamming distances of groups and quasigroups, Discrete Math. 235 (2001), 189-197

Quasigroups with very few associative triples

Aleš Drápal

Charles University (Prague, Czech Rep.)

(Joint work with Petr Lisoněk, Simon Fraser, Canada)

An associative triple of a quasigroup Q is a triple (x, y, z) such that $x \cdot yz = xy \cdot z$. Associative triples always exist. If $x, y \in Q$ and $x/x = (xy)/(xy)$, then $(x/x, x, y)$ is an associative triple. Such triples are called *left elementary*. Right elementary associative triples are defined in a mirror way. Thus $(x/x, x, x\backslash x)$ is both left and right elementary, for each $x \in Q$. If $y = x\backslash x = z/z$, then (x, y, z) is a *middle elementary* associative triple. By [1] the number of elementary triples is at least $2ni(Q) + \delta(Q)$, where $n = |Q|$, $i(Q)$ is the number of idempotents, $\delta(Q) = \delta_L + \delta_R$ and δ_L is the number of fixed point free left translations.

Denote by $a(Q)$ the number of associative triples of Q. The least n for which there exists Q with $a(Q) = 2n - i(Q)$ is 8. In such a case $i(Q) = 0$. The least n for which $a(Q) = n$ is 9 [2]. Note that $a(Q) \geq n$ in all cases and that if $a(Q) = n$, then Q is idempotent.

22

Call Q *maximally nonassociative* if $a(Q) = n$. Computer experiments show that from each proper (left) nearfield it is possible to derive a maximally nonassociative quasigroup by a construction of Sherman Stein [4]. The construction uses multiplication and addition of the nearfield, and a parameter c, and defines the quasigroup operation by $x + (y - x)c$. Not every c yields a maximally nonassociative quasigroup, but the fraction of such c exceeds one quarter in all nearfields that were tested. What we can prove is more modest [3]:

Theorem 1. *In each quadratic proper nearfield there exists at least one c such that the operation $x + (y - x)c$ yields a maximally nonassociative quasigroup.*

References

[1] A. Drápal, V. Valent: *High nonassociativity in order 8 and an associative index estimate,* J Combin Des. **27** (2019) 205–228

[2] A. Drápal, V. Valent: *Extreme nonassociativity in order 9 and beyond,* J Combin Des. (accepted)

[3] A. Drápal, P. Lisoněk: *Maximal nonassociativity via nearfields* (submitted)

[4] S. Stein: *Homogeneous quasigroups,* Pacif. J. Math. **14** (1964), 1091–1102

Affine Steiner loops

Giovanni Falcone, Ágota Figula, Carolin Hannusch

University of Debrecen (Hungary)

A Steiner triple system STS is an incidence structure consisting of points and blocks such that every two distinct points are contained in precisely one block and any block has precisely three points (cf. [3]). A loop $(L, \cdot)$ is a quasigroup which has identity element e. To any STS one can associate two different commutative loops ([2], Chapter II), that we call projective and affine Steiner loop associated to STS. Affine Steiner loops behave to elementary abelian 3-groups as Steiner triple systems behave to affine geometries over $GF(3)$. We investigate the interplay between algebraic and geometrical properties of affine Steiner loops in connections for Pash- and mitre configurations ([1]), Veblen points, Hall triple systems. We study the structure of these loops in particular affine Steiner loops which are extensions of normal subloops by (factor) loops as well as simple affine Steiner loops. We prove that the multiplication group of every affine Steiner loop with n elements is contained in the alternating group A_n. We give conditions for the loop such that the multiplication group is A_n.

References

[1] A. Caggegi, G. Falcone, M. Pavone, *On the additivity of block designs* J. Algebr. Comb. 45 (1), 271-294, DOI 10.1007/s10801-016-0707-5 (2017)

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

[3] Ch. J. Colbourn, A. Rosa, *Triple Systems*, Oxford mathematical monographs, Clarendon Press, 1999

[4] G. Falcone, Á. Figula, C. Hannusch, *Affine Steiner loops*, submitted for publication (2019)

[5] K. Strambach, I. Stuhl, *Translation groups of Steiner loops.* Discrete Mathematics, 309(13), 4225-4227. DOI 10.1016/j.disc.2008.12.019 (2009)

Essentially equivalence of hyperidentities in semigroups

Heghine Ghumashyan

Vanadzor State University (Armenia)

(Joint work with Yu. Movsisyan, Yerevan State University)

The present talk is devoted to the necessary and sufficient conditions of semigroups, which essentially satisfy one of the following hyperidentities:

$$X(X(x,y),z) = X(x,Y(y,z)) \quad (1)$$
$$X(X(x,y),z) = Y(x,X(y,z)) \quad (2)$$
$$X(X(x,y),z) = Y(x,Y(y,z)) \quad (3)$$
$$X(Y(x,y),z) = X(x,Y(y,z)) \quad (4)$$
$$X(Y(x,y),z) = Y(x,X(y,z)) \quad (5)$$

References

[1] H. O. Pflugfelder, Quasigroups and Loops: Introduction, Helderman Verlag Berlin, 1990.

[2] Yu. M. Movsisyan, Introduction to the theory of algebras with hyperidentities, Yerevan State University Press, Yerevan, 1986. (Russian)

[3] Yu. M. Movsisyan, Hyperidentities and hypervarieties in algebras, Yerevan State University Press, Yerevan, 1990. (Russian)

[4] Yu. M. Movsisyan, *Hyperidentities and hypervarieties*, Scientiae Mathematicae Japonicae, 54(3), (2001), 595-640.

[5] J.D.H. Smith, *On groups of hypersubstitutions*, Algebra Universalis, 64, (2010), 39-48.

[6] K. Denecke, S. L. Wismath, Hyperidentities and Clones. Gordon and Breach Science Publishers, 2000.

Tangent and cotangent loopoids

Janusz Grabowski

Polish Academy of Sciences

In this project, we would like to propose a concepts of a *loopoid*, defined as a nonassociative generalization of a groupoid. Note that here by *groupoid* we understand a *Brandt groupoid*, i.e. a small category in which every morphism is an isomorphism, and not an object called in algebra also a *magma*. These are loops which can be considered as nonassociative generalizations of groups. In the case of genuine groupoids, however, the situation is more complicated, because the multiplication is only partially defined, so the axioms of a loop must be reformulated.

The projected concept of a differential loopoid should be of course the subject of canonical constructions in differential geometry. In particular, the tangent and the cotangent bundles of a differential loopoid should be canonically differential loopoids.

It is well known that TG of a Lie group is a Lie group itself. The appearance of Lie groupoids in differential geometry is comes necessary, as the cotangent bundle of a Lie group G is canonically not a group but a Lie groupoid over the dual $\mathfrak{g}^*$ of the Lie algebra of G. The situation with the tangent loopoid is rather obvious. The structure of T^*G is much more complicated and it is not clear yet under what conditions about the inverse it carries a structure of a differentiable groupoid (and which one). The main result is the following:

Theorem 1. *There is a canonical differential loopoid structures on the tangent TG and cotangent bundle T^*G of a differential loopoid G.*

Contrary to the case of differentiable loops, the literature in this subject oriented on 'nonassociative Lie groupoids' is not very extensive. Besides some aspects contained in the Sabinin's monograph [3], we can indicate our short introductory note [1]. However, the term *loopoid* has appeared already in a paper by Kinyon [2] in a slightly similar context. The motivating example, however, built as an object 'integrating' the Courant bracket on $TM \oplus_M T^*M$, uses the group of diffeomorphisms of the manifold M as integrating the Lie algebra of vector fields on M, not the pair groupoid $M \times M$ as 'integrating' the Lie algebroid TM.

References

[1] J. Grabowski, *An introduction to loopoids*, Comment. Math. Univ. Carolin. **57** (2016), 515-526.

[2] M. Kinyon, *The coquecigrue of a Leibniz algebra*, preprint, 2003.

[3] L. V. Sabinin, *Smooth Quasigroups and Loops*, Kluwer Academic Press, 1999.

Complete graph decompositions and P-groupoids

Mark Greer

University of North Alabama (USA)

(Joint work with J. Carr)

P-groupoids arise from decompositions of complete graphs into disjoint cycles. We show that left distributive P-groupoids are distributive quasigroups. The rest of the talk will focus on characterizing P-groupoids when the corresponding decomposition is a Hamiltonian decomposition. We focus on a specific example of a P-quasigroups constructed from cyclic groups of odd order as motivation.

Yang-Baxter equation and a congruence of biracks

Přemysl Jedlička

Czech University of Life Sciences Prague (Czechia)

(Joint work with Agata Pilitiowska, Anna Zamojska-Dzienio)

Set-theoretic solutions of Yang-Baxter equation are simplifications of a topic studied in particle physics. Their universal algebraic counterparts are called biracks; an algebra $(X, \circ, \bullet, \backslash, /)$ is called a birack if $(X, \circ, \backslash)$ is a left quasigroup, $(X, \bullet, /)$ is a right quasig-roup and the operations satisfy the following identities:

$$\begin{aligned} x \circ (y \circ z) &= (x \circ y) \circ ((x \bullet y) \circ z), \\ (x \circ y) \bullet ((x \bullet y) \circ z) &= (x \bullet (y \circ z)) \circ (y \bullet z), \\ (x \bullet y) \bullet z &= (x \bullet (y \circ z)) \bullet (y \bullet z). \end{aligned}$$

A birack is said to be involutive if it satisfies one of the two equivalent identities

$$(x \circ y) \circ (x \bullet y) = x \qquad \Leftrightarrow \qquad (x \circ y) \bullet (x \bullet y) = y.$$

The following congruence

$$x \sim y \equiv x \circ z = y \circ z, \quad \text{forall } z \in X$$

of an involutive birack is often studied in the literature. We present a generalization of the congruence for non-involutive biracks.

Projective representations for loops

Kenneth W. Johnson

Penn State Abington (USA)

Projective representations for groups were introduced by Schur in the early 20th century. Such a representation for a group G can be thought of a map $\kappa : G \to M_{n\times n}(\mathbb{C})$ together with a factor set $\alpha : G \times G$ such that

$$\kappa(g)\kappa(h) = \alpha(g,h)\kappa(gh)$$

for all g, h in G. To each group G there is a covering group $D(G)$ and a surjection $f : D(G) \to G$ such that the kernel of f is an abelian group $M(G) \subseteq G' \cap Z(G)$ called the Schur multiplier of G.

The question which I will address is the extent to which there is a theory of projective representations of loops for particular classes: Chein loops, Moufang loops, automorphic loops... . The particular question of whether a covering loop always exists for a Moufang loop appears to be interesting. Another interesting question is whether there is a combinatorial definition of projective characters of a loop or quasigroup.

On relationship between a 2nd group cohomology group and a 2nd quandle cohomology group

Byeohi Kim

Kyungpook National University (Rep. of Korea)

In [1], Carter, Jelsovsky, Kamada, Langford and Saito developed the quandle homology theory by modifying the group homology theory. In [2], Carter, Kamada and Saito showed that there exists a one-to-one correspondence between quandle second cohomology group $H^2_q(Q;A)$ and the set of abelian extensions of Q by A up to equivalence.

In [3], Joyce proposed that every quandle can be represented by using its automorphism group, so we can study a quandle extension by using this group representations of quandles.

In this talk, we begin studying the mod-2 quandle extension of the 4-elements tetrahedral quandle that is defined by a quandle cocycle in terms of the inner automorphism groups of each. We also observe the relationship between 2nd quandle cohomology group and 2nd group cohomology group in the example. This is a joint work with Y. Bae and J. S. Carter.

References

[1] J. S. Carter, D. Jelsovsky, S. Kamada, L. Langford and M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces,* Trans. Amer. Math. Soc., **355** (2003) 3947-3989.

[2] J. S. Carter, S. Kamada and M. Saito *Diagrammatic computations for quandles and cocycle knot invariants,* https://arxiv.org/pdf/math/0102092.pdf

[3] D. Joyce, *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Alg., **23** (1983) 37-65.

Biquandle cocycle invariants of surface-links

Seiichi Kamada, Akio Kawauchi, Jieon Kim* and Sang Youl Lee

Pusan National University (Korea)

A quandle is a set equipped with a binary operation satisfying certain axioms derived from the Reidemeister moves in knot theory. On the other hand, a generalization of quandles (called biquandles) is introduced in [3]. In [2], J.S. Carter, M. Elhamdadi and M. Saito defined a (co)homology theory and cocycle invariants for biquandles. J.S. Carter, S. Kamada and M. Saito defined shadow quandle colored diagrams and shadow quandle cocycle invariants of oriented links and surface-links [1]. Surface-links are represented by broken surface diagrams and marked graph diagrams. In this talk, wed like to introduce shadow biquandle colorings of oriented broken surface diagrams and those of oriented marked graph diagrams, and describe shadow biquandle cocycle invariants of oriented surface-links via broken surface diagrams and marked graph diagrams. This is a joint work with S. Kamada, A. Kawauchi, and S.Y. Lee.

References

[1] J. S. Carter, S. Kamada, M. Saito, Geometric interpretations of quandle homology, *J. Knot Theory Ramifications* **10** (2001) 345386.

[2] J. S. Carter, M. Elhamdadi and M. Saito, Homology Theory for the Set-Theoretic Yang-Baxter Equation and Knot Invariants from Generalizations of Quandles, *Fund. Math.* **184** (2004) 3154.

[3] L. H. Kauffman and D. E. Radford, Bi-oriented quantum algebras, and generalized Alexander polynomial for virtual links, *Contemp. Math.*, **318** (2003) 113140.

Functional Equations and their Graphs

Aleksandar Krapež

Mathematical Institute of the SASA, Belgrade (Serbia)

(Joint work with S. K. Simić and D. Živković)

In his PhD thesis [3], S. Krstić did establish the correspondence between quadratic quasigroup equations and connected cubic graphs. It turns out that this correspondence connects important properties of equations to familiar notions of the graph theory. For example, 3–connectivity of vertices in a graph is relevant to isostrophy of operations in all solutions of an equation. Furthermore, the properties of solutions depend on size and planarity of 3–connected subgraphs etc.

In [2], A. Krapež, D. Živković made this correspondence more precise by proving that the parastrophic equivalence of functional equations is replaced by the isomorphism of corresponding graphs (see also A. Krapež and M. A. Taylor [1]). Here, we refine the notion of graphs to *Eq–graphs* which are bidirected connected cubic coloured (multi)graphs with a designated edge. It is proved that isomorphic *Eq*–graphs correspond to unique (up to notation) generalized quadratic functional equation and are an appropriate tool for investigating equations.

References

[1] A. Krapež, M. A. Taylor: *Gemini functional equations on quasigroups*, Publ. Math. Debrecen **47/3–4**, (1995), Zbl 0859.39014.

[2] A. Krapež, D. Živković: Parastrophically equivalent quasigroup equations, Publications de l'Institut Mathematique 87 (101) (2009), 39-58. DOI: 10.2298/PIM1001039K.

[3] S. Krstić: *Quadratic quasigroup identities* (Serbian), PhD thesis, University of Belgrade, (1985).

Algebraic structures related with finite projective planes

Kuznetsov Eugene

Institute of Mathematics and Computer Science (Republic of Moldova)

This is a brief survey of the authors works about of algebraic coordinatization of the finite projective planes and the studying of the internal structure of the corresponding algebraic objects.

Such objects are: a finite DC-ternar [1], a strictly 2-transitive set of permutations in symmetric permutation group S_n [1, 2], a loop transversal L in S_n to the stabilizer of 2 elements [1, 2]. The internal structure of the above mentioned loop transversal L and the corresponding loop transversal operation $(L, \cdot)$ were investigated. As a result it was shown that in the loop $(L, \cdot)$ there exists an unique loop transversal T to its subloop R of all substitutions fixed one symbol [3]. This transversal consists of all fixed-point-free permutations and the identity permutation. It was also shown that it is possible to investigate the properties of the above mentioned transversal T in the loop $(L, \cdot)$ by examining their multiplicative groups the group S_n and its subgroups (stabilizers of 1 and 2 elements) [4, 5].

A study is being carried out on the possibility of constructing the different loop transversals in a loop $(L, \cdot)$ by its subloop R, using the transversal T. This makes it possible to further advance in the proof of the prime power conjecture for finite projective planes.

References

[1] Kuznetsov E. About some algebraic systems related with projective planes. Quasigroups and related systems, 2(1995), 1, p. 6-33.

[2] Kuznetsov E. Kuznetsov E. Loop transversals in S_n to $St_{a,b}(S_n)$ and coordinatizations of projective planes. Bulletin of the Acad. of Sci. of Moldova, Mathematics, No. 2 (36), 2001, p. 125-135.

[3] Kuznetsov E. A loop transversal in a sharply 2-transitive permutation loop. Bulletin of the Acad. of Sci. of Moldova, Mathematics, No. 3 (49), 2005, p. 101-114.

[4] Kuznetsov E.A. Transversals in loops. 1. Elementary properties. Quasigroups and related systems, 2010, No. 1 (18), p. 43-58.

[5] Kuznetsov E.A. Transversals in loops. 2. Structural theorems. Quasigroups and related systems, 2011, No. 2 (19), p. 279-286.

Cryptanalysis of some stream ciphers

Nadezhda Nikolayevna Malyutina

State University Dimitrie Cantemir (Moldova)

In this paper, a generalized Markovski algorithm for i-invertible n-groupoids is presented. A cryptanalysis is done on cipher and there are analyzed crypto attacks, built by M. Vojvoda for quasigroups, chosen ciphertext and plaintext.

Today, various cryptosystems based on quasigroups have appeared, which show that the use of quasigroups opens new ways in construction of stream and block ciphers [1, 2]. We continue researches of applications of n-ary groupoids that are invertible on i-th place in cryptology [5, 6].

Definition 1. *n-Ary groupoid (Q, f) is called invertible on the i-th place, $i \in \overline{1,n}$, if the equation $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n) = a_{n+1}$ has a unique solution for any elements $a_1, \ldots, a_{i-1}$, $a_{i+1}, \ldots, a_n, a_{n+1} \in Q$.*

In this case operation ${}^{(i,n+1)}f(a_1, \ldots, a_{i-1}, a_{n+1}, a_{i+1}, \ldots, a_n) = x_i$ is defined in the unique way.

Algorithm 1. *Let Q be a non-empty finite alphabet and k be a natural number, $u_i, v_i \in Q$, $i \in \{1, ..., k\}$. Define an n-ary groupoid (Q, f) which is invertible on the n-th place. It is clear that groupoid $(Q, {}^{(n,n+1)}f)$ is defined in a unique way.*

Take the fixed elements $l_1^{(n-1)(n-1)}$ ($l_i \in Q$), which are called leaders.

Let $u_1u_2...u_k$ be a k-tuple of letters from Q.

The following ciphering (encryption) procedure is proposed:

$$\begin{aligned}
v_1 &= f(l_1^{n-1}, u_1),\\
v_2 &= f(l_n^{2n-2}, u_2),\\
&\ldots,\\
v_{n-1} &= f(l_{n^2-3n+3}^{(n-1)(n-1)}, u_{n-1}),\\
v_n &= f(v_1^{n-1}, u_n),\\
v_{n+1} &= f(v_2^{n}, u_{n+1}),\\
v_{n+2} &= f(v_3^{n+1}, u_{n+2}),\\
&\ldots
\end{aligned} \tag{1}$$

Therefore we obtain the following ciphertext: $v_1v_2 \ldots, v_{n-1}, v_n, v_{n+1}, \ldots$.

The deciphering algorithm is constructed similarly with the binary case:

$$\begin{aligned}
u_1 &= {}^{(n,n+1)}f(l_1^{n-1}, v_1),\\
u_2 &= {}^{(n,n+1)}f(l_n^{2n-2}, v_2),\\
&\dots,\\
u_{n-1} &= {}^{(n,n+1)}f(l_{n^2-3n+3}^{(n-1)(n-1)}, v_{n-1})\\
u_n &= {}^{(n,n+1)}f(v_1^{n-1}, v_n),\\
u_{n+1} &= {}^{(n,n+1)}f(v_2^{n}, v_{n+1}),\\
u_{n+2} &= {}^{(n,n+1)}f(v_3^{n+1}, v_{n+2}),\\
&\dots
\end{aligned} \tag{2}$$

M.Vojvoda has given the cryptoanalysis of the file encoding system based on quasigroups [3, 4] and showed how to break this cipher. The binary analogue of this attack is described for quasigroups by M. Vojvoda [4].

Consider an attack with text constructed using an n-ary groupoid, which is invertible in the last place obtained using the generalized Markovski algorithm.

Assume the cryptanalyst has access to the decryption device loaded with the key. He can then construct the following ciphertext:

$q_1q_1\dots q_1q_1q_1q_1\dots q_1q_2q_1q_1\dots q_1q_m$
$q_1q_1\dots q_2q_1q_1q_1\dots q_2q_2q_1q_1\dots q_2q_m$
$q_1q_1\dots q_3q_1q_1q_1\dots q_3q_2q_1q_1\dots q_3q_m$
$\dots$
$q_1q_1\dots q_mq_1q_1q_1\dots q_mq_2q_1q_1\dots q_mq_m\dots$
and enter it into the decryption device.

For a complete reconstruction of the table of values of the operation ${}^{(i,n+1)}f$, and hence the table of values of the operation f, it is sufficient to submit at the input: $(n\cdot m^{n-1}+1)(m-1)$ characters to get all the values or $n\cdot m^{n-1}(m-1)+(m-2)$ characters, when the last value is found by the exception method.

Example 1. *Let (R^3, f) be a ternary groupoid,which is defined over the ring $(R^3, +, \cdot)$ of residues modulo 3 and which is invertible on the third place. We define ternary operation f on the set R^3 in the following way: $f(x_1, x_2, x_3) = \alpha x_1 + \beta x_2 + x_3 = x_4$, where $\alpha 0 = 2, \alpha 1 = 2, \alpha 2 = 0, \beta 0 = 1, \beta 1 = 1, \beta 2 = 1$.*

Inverse operation for f is ${}^{(3,4)}f(x_1, x_2, x_4) = x_3 = 2\cdot\alpha x_1 + 2\cdot\beta x_2 + x_4$. We propose the following elements: $l_1 = 1, l_2 = 2, l_3 = 0, l_4 = 1$ as leader elements.

Enter the following text into the decryption device:

$q_1q_1q_1q_1q_1q_2q_1q_1q_3q_1q_2q_1q_1q_2q_2q_1q_2q_3q_1q_3q_1q_1q_3q_2q_1q_3q_3$
$q_2q_1q_1q_2q_1q_2q_2q_1q_3q_2q_2q_1q_2q_2q_2q_2q_2q_3q_2q_3q_1q_2q_3q_2q_2q_3q_3$
q_3q_1

or
000001002010011012020021022
100101102110111112120121122
20
At the output we get:
0000010020000110120100212220201011021001111121100210221 2

Thus, for a complete reconstruction of the table of values of the operation ${}^{(3,4)}f$, and hence the table of values of the operation f, it is enough to supply 55 characters (without the last one) for the ternary groupoid at the input, or 56 characters to restore all values.

To understand the situation with burglary of the decrypted text and the leaders, consider the plaintext of the form: 201121. Using the table of values of function f, we get 4 different versions of the decrypted text, i.e., it is not particularly difficult to determine the true value in this case. As for the values of the leaders, for our example of their various sets will be 81 characters. However, in essence, we do not need to determine the exact values of the leaders. At the moment, we are trying to reduce the number of symbols used in attacks and generalize this result.

The process of carrying out attacks continues, various examples are built, generalizations of the results are made.

References

[1] S. Markovski and D. Gligoroski and S. Andova. *Using quasigroups for one-one secure encoding.* Proc. VIII Conf. Logic and Computer Science "LIRA'97", Novi Sad, 1997, 157-167.

[2] E. Ochodkov and V. Snashel. *Using Quasigroups for Secure Encoding of File System.* Proceedings of the International Scientific NATO PfP/PWP Conference "Security and Information Protection 2001", May 9-11, 2001, Brno, Czech Republic, pp.175-181.

[3] M. Vojvoda. Cryptanalysis of a file encoding system based on quasigroup. presented at the ISCAM 2003, April 11-12, 2003, submitted to the Journal of Electrical Engineering.

[4] Milan Vojvoda. Attacks on a file encryption system based on quasigroup. Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Bratislava, Slovak Republic, 2004.

[5] V. A. Shcherbacov and N. N. Malyutina. Role of quasigroups in cryptosystems. Generalization of Markovski algorithm. International Conference on Mathematics, Informatics and Information Technologies dedicated to the Illustrious Scientist Valentin Belousov, Balti, Communications, 2018, p. 88-89

[6] V. A. Shcherbacov and N. N. Malyutina. Role of quasigroups in cryptosystems. Generalization of Markovski algorithm. *Bulletin of the Transnistrian University*, 60(3):53–57,2018. (Russian).

Representations of code loops by binary codes

Rosemary Miguel Pires

Fluminense Federal University (Brazil)

In this presentation, first we recall how to construct a code loop from a doubly even code V and the classification of non-associative code loops of rank 3 and 4. Then for a given code loop L (rank 3 or 4) we show how to determine a doubly even code V such that $L \simeq L(V)$, where $L(V)$ is the code loop constructed from V. For definition, a representation of a code loop L is a doubly even code $V \subseteq \mathbf{F}_2^m$ such that $L \simeq L(V)$. The degree of such a representation is the number m. We notice that there are many different representations for a same code loop, but we present that there are representations of non-associative code loops of rank 3 and 4 such that the degree of each representation is the smallest possible. This is joint work with Prof. Alexandre Grishkov (University of Sao Paulo).

References

[1] R. L. Griess Jr., *Code loops*, J.Algebra 100 (1986), 224-234.

[2] A. Grishkov and R. Miguel Pires, *Variety of loops generated by code loops*, International Journal of Algebra and Computation, Volume 28, No. 1 (2018), 163-177.

[3] R. Miguel Pires, *Loops de código: automorfismos e representações*. Tese de Doutorado, Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo (2011).

Left distributive quasigroups of order 2^k

Tomas Nagy

Charles University (Czech Republic)

We will show that a non-affine left distributive quasigroup of order 2^k exists if and only if $k = 6$ or $k \geqslant 8$.

The first example of a left distributive quasigroup not isotopic to a Bol loop was found by Onoi in 1970 [2]; its order is 2^{16}. Subsequently, Galkin developed a representation theory for left distributive quasigroups over transitive groups, which allowed to settle many problems. For example, he proved that the smallest left distributive quasigroup not isotopic to a Bol loop has order 15, and that every smaller left distributive quasigroup is affine over an abelian group.

A computer search over the library of transitive groups, based on Galkin's ideas, quickly reveals that there are no non-affine left distributive quasigroups of order 2^k for $k \leqslant 5$. Elaborating Onoi's ideas in the setting of central extensions, we will present how to construct non-affine left distributive quasigroups of order 2^{2k} for every $k \geqslant 3$. We will also outline how to set a computer search that proves that there are none of order 2^7.

References

[1] M. Bonatto, D. Stanovsky, Commutator theory for racks and quandles, arXiv:1902.08980.

[2] V. I. Onoi, Left distributive quasigroups that are left homogeneous over a quasigroup (Russian), Bul. Akad. Stiince RSS Moldoven, 1970 no. 2 (24-31).

On the classification of distributive Mendelsohn triple systems

Alex W. Nowak

Iowa State University (USA)

A distributive Mendelsohn (semisymmetric and idempotent) quasigroup is necessarily affine over a commutative Moufang loop [1]. Building on the work of [1], we prove that Mendelsohn quasigroups affine over abelian groups decompose into a direct product of subquasigroups that are defined on sets of the form $(\mathbb{Z}/_{p^n})^i$, for p prime and $i \in \{1, 2\}$. This classification then permits a complete description and enumeration of isomorphism classes for distributive Mendelsohn quasigroups of order not divisible by 3. We present the complications related to the order 3 case. We conclude with a discussion of the prospects for a process of "reverse linearization" of quasigroup identities and a type of Morita equivalence such a process would establish between varieties of quasigroups.

References

[1] D. M. Donovan, T. S. Griggs, T. A. McCourt, J. Opršal, and D. Stanovský, *Distributive and anti-distributive Mendelsohn triple systems*, Canadian Math. Bull., **59** (2016), 36-49.

Generalized Bol-Moufang loop varieties—not just for breakfast!

J.D. Phillips

Northern Michigan University (U.S.A.)

In this talk, we give an overview of the generalized Bol-Moufang loop varieties, and we give detailed structural descriptions of the two most interesting varieties of this type: the FRUTE loops (mmmmm!), and another, as yet unnamed, variety.

2-PERMUTATIONAL LEFT-QUASIGROUPS

Agata Pilitowska

Warsaw University of Technology, (Poland)

(Joint work with Přemysl Jedlička and Anna Zamojska-Dzienio)

There is a one-to-one correspondence between non-degenerate involutive solutions of the Yang-Baxter equation of multipermutation level 2 and non-degenerate right cyclic 2-permutational left quasigroups.

A left quasigroup $(X, \circ, \backslash)$ is *non-degenerate right cyclic* 2*-permutational*, if for every $x, y, z, t \in X$:

$$(x\backslash y)\backslash(x\backslash z) = (y\backslash x)\backslash(y\backslash z),$$
$$(z \circ x) \circ y = (t \circ x) \circ y,$$

and the mapping $x \mapsto x\backslash x$ is a bijection.

We characterize all non-degenerate right cyclic 2-permutational left quasigroups. We show that such left quasigroups fall into two classes – distributive ones and non-distributive ones. We present algorithms how effectively construct them. We also enumerate all distributive right cyclic left quasigroups up to size 14.

References

[1] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups*, Adv. Math. **338** (2018), 649–701.

[2] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *The construction of multipermutation solutions of the Yang-Baxter equation of level 2*, submitted, available at `http://arxiv.org/abs/1901.01471`

[3] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), 153-170.

Partial almost perfect nonlinear permutations

Alexander Pott

Otto von Guericke University Magdeburg (Germany)

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if $f(x) + f(y) + f(z) + f(x + y + z) \neq 0$ for all x, y, z such that $|\{x, y, z, x + y + z\}| = 4$. The motivation to study these functions comes from cryptography, since the defining property is somehow oposite to linearity. The big open problem on APN functions is the question whether there are APN permutations if n is even. There is only one example known if $n = 6$ [1].

Recently, a relaxation of APN functions has been introduced [2]: A function is called partially APN if $f(y) + f(z) + f(y + z) \neq 0$ for all $y, z \neq 0$, $y \neq z$. That means that the APN property is satisfied for $x = 0$ only.

The main result is the following:

Theorem 1. *Partially APN permutations exist for all n.*

The proof is non-constructive and uses an interesting connection (rather an observation than a theorem) to Steiner triple systems as well as [3].

References

[1] K.A. Browning, J.F. Dillon, M.T. McQuistan and A.J. Wolfe, *An APN Permutation in Dimension Six*. In: Finite Fields: Theory and Application, Contemporary Mathematics **518** (2010), pp 33–42.

[2] Lilya Budaghyan, Nikolay S. Kaleyski, Nikolay S, Soonhak Kwon, Constanza Riera and Pantelimon Stanica, *Partially APN Boolean functions and classes of functions that are not APN infinitely often*. To appear in Cryptograpy and Communications (2019). arXiv:1905.13025 (24 pages).

[3] Luc Teirlinck, *On Making Two Steiner Systems Disjoint*, Journal of Combinatorial Theory A **23**, 349–350 (1977).

Commutative automorphic loops arising from groups

Lee Raney

University of North Alabama (USA)

(Joint work with Mark Greer)

Γ-loops are commutative loops which (in the odd order case) arise from groups via a construction of Baer. Utilizing a known correspondence between Γ-loops and Bruck loops, we provide results on the classification of commutative automorphic loops of certain orders. Finally, we suggest an alternative approach to the aforementioned classification via the correspondence between between Bruck loops and involutory latin quandles.

Beyond barycentric algebras and convex sets

Anna B. Romanowska

Warsaw University of Technology, Warsaw, Poland

Affine spaces over a subfield F of the field of reals are viewed as abstract algebras, sets equipped with binary affine combinations, one for each element r of the field F. Under a unique operation determined by r, not equal to 0 or 1, such an affine space is a quasigroup. Under the set of operations determined by the open unit interval of F, a subalgebra of such an affine space is a convex set. Convex sets generate the variety of barycentric algebras. Barycentric algebras are fundamental for modeling convex sets, semilattices, affine spaces and related structures.

Algebraic extensions of the concept of a convex set are obtained by considering various (symmetrical) intervals J of F containing 1/2. In threshold affine spaces, the basic set of binary operations is replaced by a set determined by an interval J, declaring the remaining operations to be trivial left or right projections. A similar approach to convex sets provides threshold barycentric algebras. If the closed unit interval I of F is a proper subset of J, then the operations from J generate all the affine space operations. As a consequence, it transpires that threshold affine spaces over F are equivalent to one of three types of algebras: affine spaces, barycentric algebras, or commutative binary modes (idempotent commutative entropic magmas). An analysis of the identities holding in threshold affine spaces reveals dependencies between the axioms of affine spaces, and between the axioms of affine spaces and barycentric algebras.

References

[1] A. Komorowski, A. Romanowska, J.D.H. Smith, Keimel's problem on the algebraic axiomatization of convexity, Algebra Universalis 79 (2018), Art. 22.

[2] A. Komorowski, A. Romanowska, J.D.H. Smith, Barycetric algebras and beyond, Algebra Universalis, to appear.

[3] A. Romanowska, Convex sets and barycntric algebras, Contemporary Mathematics 721 (2019), 243-259.

Paramedial quasigroups of prime and prime square order

Žaneta Semanišinová

Charles University, Prague (Czech Republic)

A quasigroup $(Q, \cdot)$ is called paramedial, if it satisfies the identity

$$(xy) \cdot (uv) = (vy) \cdot (ux),$$

for all $x, y, u, v \in Q$. We will show that, for every odd prime number p, there are $2p - 1$ paramedial quasigroups of order p and $\frac{11}{2}p^2 + \frac{3}{2}p - 4$ paramedial quasigroups of order p^2, up to isomorphism. The proof is based on the fact that all paramedial quasigroups are affine over an abelian group (Němec and Kepka, 1971) and thus their enumeration reduces to an analysis of square roots and conjugacy classes in (certain subgroups of) automorphism groups of finite abelian groups (in our case, cyclic and elementary abelian of rank 2).

References

[1] P. Němec and T. Kepka, T-quasigroups. I, II, Acta Univ. Carolinae – Math. et Phys., 1971.

Ω-GROUPOIDS AND Ω-QUASIGROUPS

Branimir Šešelja

University of Novi Sad (Serbia)

(Joint work with **Aleksandar Krapež** (MI SANU Beograd) and **Andreja Tepavčević** (Univ. of Novi Sad and MI SANU Beograd))

Starting with Ω-sets, we deal with generalizations of groupoids, quasigroups and related structures. Ω is a complete lattice, and an Ω-*set* (A, E) is a nonempty set equipped with a symmetric and transitive map $E : A^2 \to \Omega$ (as introduced by Fourman and Scott in late seventies for modeling the intuitionistic logic). E is an Ω-*valued equality* on A and it is a generalization of the classical equality. In our framework, the set A is equipped with operations, which makes it a classical, *basic structure* $\mathcal{A}$. In this case Ω-valued equality E is supposed to be accordingly compatible with these operations. For the present research a basic structure is a groupoid $\mathcal{A} = (A, \cdot)$, or an algebra with several at most binary operations. Hence, we investigate Ω-groupoids and similar Ω-structures (Ω-algebras) denoted generally by $(\mathcal{A}, E)$. In this context, identities and polynomial formulas with equality are formulated as particular lattice-theoretic formulas in which the equality sign is replaced by E. Then an identity (formula) holds in $(\mathcal{A}, E)$ if the corresponding lattice formula is satisfied in Ω.

In particular, an Ω-groupoid is an Ω-*quasigroup* if the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions with respect to E, as it is defined in our research.

A connection to classical quasigroups is that *an* Ω-*groupoid* $(\mathcal{A}, E)$ *is an* Ω-*quasigroup if and only if the quotient subgroupoids over the congruences obtained by a special decomposition of the* Ω-*valued equality* E*, are classical quasigroups.*

We also prove the equivalence of Ω-quasigroups with Ω-*equasigroups*. The basic structure in the latter is an algebra with three binary operations and the classical equasigroup identities are supposed to hold, which, as mentioned, means that particular lattice-theoretic formulas are satisfied.

Further we investigate Ω-groupoids with a unit (neutral element). We prove that *such an element is unique, provided that the language contains a nullary operation.* Otherwise, *an* Ω-*groupoid might contain several units, which are equal up to the* Ω-*valued equality* E*.*

As a consequence, we show that Ω-groups can be naturally defined as Ω-groupoids, but also as Ω-algebras in the language with a nullary, a unary and a binary operation. In both cases the mentioned quotient substructures are classical groups, but the obtained versions of Ω-groups are not equivalent. Still, using the Axiom of Choice, we were able to prove that an Ω-*loop having a nullary operation in the language and fulfilling associativity with respect to* E *is an* Ω-*group.*

Finally, we deal with (unique) solutions of equations $a \cdot x = b$ and $y \cdot a = b$ in the framework of Ω-quasigroups and Ω-groups. For an Ω-quasigroup (Ω-group) $(\mathcal{A}, E)$ we obtain solutions with respect (up to) the Ω-equality E. Considering the basic structure $\mathcal{A}$ (which is not generally a group nor a quasigroup) we get approximate solutions which could be explained by the nature or origin of the generalized equality.

References

[1] O.S. Almabruk Bleblou, B. Šešelja, A. Tepavčević, Normal Omega-Subgroups, *Filomat* 32(19) (2018) 6699–6711.

[2] E. Eghosa Edeghagba, B. Šešelja, A. Tepavčević, Congruences and homomorphisms on Ω-algebras, *Kybernetika* (2017) 53(5) 892–910.

[3] M.P. Fourman, D.S. Scott, Sheaves and logic, in: M.P. Fourman, C.J. Mulvey D.S. Scott (Eds.), Applications of Sheaves, *Lecture Notes in Mathematics* 753 Springer 1979 302–401.

[4] A. Krapež, B. Šešelja, A. Tepavčević, Solving linear equations by fuzzy quasigroups techniques, *Information sciences* 491 (2019) 179–189.

[5] B. Šešelja, V. Stepanović, A. Tepavčević, A note on representation of lattices by weak congruences, *Algebra Univers.* 68 (2012) 287–291.

[6] B. Šešelja, A. Tepavčević, Ω-algebras, *Proceedings of ALHawai'i 2018, A conference in honor of Ralph Freese, William Lampe, and J.B. Nation*, 96–106.

[7] B. Šešelja, A. Tepavčević, Ω-groups in the language of Ω-groupoids (submitted).

Units in quasigroups with Bol-Moufang type identities

Victor Alekseevich Shcherbacov

Institute of Mathematics and Computer Science, Chişinău (Moldova)

(Joint work with Natalia Nikolaevna Didurik, State University Dimitrie Cantemir, Chişinău, Moldova)

Groupoid $(Q, *)$ is called a quasigroup, if the following conditions are true [1]: $(\forall u, v \in Q)(\exists! \, x, y \in Q)(u * x = v \,\&\, y * u = v)$.

An identity based on a single binary operation is of Bol-Moufang type if "both sides consist of the same three different letters taken in the same order but one of them occurs twice on each side"[2].

We detail Kunen's results about quasigroups with Bol-Moufang identities [4]. We have used Prover 9 [6] and Mace 4 [5]. Numeration of identities is taken from [2, 3].

Theorem 1. *Quasigroup $(Q, \cdot)$ with any from the following identities F_7, F_{16}, F_{26}, F_{40}, F_{36}, F_{42}, F_{43}, F_{44}, F_{45}, F_{49} is a left loop.*

Quasigroup $(Q, \cdot)$ with any from the following identities F_9, F_{19}, F_{29}, F_{35}, F_{39}, F_{54}, F_{51}, F_{52}, F_{60}, F_{59} is a right loop.

References

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

[2] F. Fenyves. Extra loops. II. On loops with identities of Bol-Moufang type. *Publ. Math. Debrecen*, 16:187–192, 1969.

[3] T.G. Jayeola, E. Ilojide, M. O. Olatinwo, and F. Smarandache. On the Classification of Bol-Moufang Type of Some Varieties of Quasi Neutrosophic Triplet Loop (Fenyves BCI-Algebras). *Symmetry*, 10:1–16, 2018. doi:10.3390/sym10100427.

[4] K. Kunen. Quasigroups, loops and associative laws. *J. Algebra*, 185(1):194–204, 1996.

[5] W. McCune. *Mace 4*. University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

[6] W. McCune. *Prover 9*. University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

The free commutative automorphic 2-generated loop of nilpotency class 3

Dylene Agda Souza de Barros

Universidade Federal de Uberlândia (Brazil)

A loop is automorphic if all its inner mappings are automorphisms. Groups are automorphic loops, commutative Moufang loops are automorphic and diassociative automorphic loops are Moufang.

Automorphic loops were first studied by Bruck and Paige [2] and, among other results, they proved that automorphic loops form a variety and are *power-associative*, which means, every element generates a group. For introduction to structural theory of automorphic loops and commutative automorphic loops, see [3], [4] and [5].

For a loop Q, define $Z_0(Q) = 1$, $Z_1(Q) = Z(Q)$ (the center of Q) and for $i \geqslant 1$ let $Z_{i+1}(Q) = 1$ be the preimage of $Z(Q/Z_i(Q))$ under the canonical projection $Q \to Q/Z_i(Q)$. Then, a loop Q is *nilpotent of class* n if $Z_{n-1}(Q) \neq Z_n(Q) = Q$.

50

It was shown independently in [6] and [7] that for an odd prime p every commutative automorphic loop of order p^k is nilpotent. Commutative automorphic loops of order p^2 are abelian groups and there exist nonassociative commutative automorphic loops of order p^3.

For $n \geqslant 2$, let $F_n(x, y)$ be the free commutative automorphic loop of nilpotency class n and free generators x, y. In this work, we construct $F_3(x, y)$ and prove that it has dimension 8 over $\mathbb{Z}$.

(Joint work with Alexander Grishkov and Petr Vojtěchovský)

References

[1] Bruck R. H., *A Survey of Binary Systems*, Springer, 1971.

[2] Bruck R. H., Paige L. J., *Loops whose inner mappings are automorphisms,* Ann. of Math (2) **63** (1956), 308 - 323.

[3] Jedliča P., Kinyon M., Vojtěchovský P., *The structure of commutative automorphic loops,* Trans. Amer. Math. Soc. **363** (2011), no. 1, 365 - 384.

[4] Jedliča P., Kinyon M., Vojtěchovský P., *Constructions of commutative automorphic loops,* Comm. Algebra **38** (2010), no. 9, 3243 - 3267.

[5] Kinyon M., Kunen K., Phillips J.D., Vojtěchovský P. *The structure of automorphic loops*,Trans. Amer. Math. Soc. **368** (2016), no. 12, 8901 - 8927.

[6] Csorgo P., *The multiplication group of a finite commutative automorphic loop of ordem power of an odd prime p is a p-group,* J. Algebra **350** (2012), no. 1, 77 - 83.

[7] Jedliča P., Kinyon M., Vojtěchovský P., *Nilpotency in automorphic loops of prime power order,* J. Algebra **350** (2012), no. 1, 64 - 76.

[8] Barros, D. A. S., Grishikov A. N., Vojtěchovský P., *Commutative automorphic loops of order* p^3, J. Algebra Appl. **11** (2012), 15 pages.

[9] Johnson K. W., Kinyon M., Nagy G. P., Vojtěchovský P., *Searching for small simple automorphic loops,* LMS J. Comput. Math. **14** (2011), 200 - 2013.

[10] Grishkov A. N., Shestakov I. P., *Commutative Moufang loops and alternative algebras,* J. Algebra **333** (2011), 1 - 13.

On some progress in Steiner loops

Izabella Stuhl

Penn State

(Joint work with A. Grishkov, D. and M. Rasskazova.)

Steiner loops are non-associative algebraic objects originated from Steiner triple systems. In this talk, I will describe the structure of the n-generated free Steiner loop of nilpotency class 2 and - as an application - present the classification of finite 3-generated 2-step nilpotent Steiner loops. Furthermore, the universal central extension of Steiner loops will be discussed.

On total multiplication groups of loops

Parascovia Syrbu

Moldova State University (Republic of Moldova)

(Joint work with Aleš Drápal, Charles University, Prague)

Let $Q(\cdot)$ be a quasigroup, $a \in Q$ and $L_a : x \mapsto ax$, $R_a : x \mapsto xa$, $D_a : x \mapsto a/x$. Permutation groups $\mathrm{Mlt(Q)} = \langle L_a, R_a; a \in Q\rangle$ and $\mathrm{TMlt(Q)} = \langle L_a, R_a, D_a; a \in Q\rangle$ are called the multiplication group and the total multiplication group of $Q(\cdot)$, respectively. If $Q(\cdot)$ is a loop with the unit 1, then $\mathrm{Inn(Q)} = (\mathrm{Mlt(Q)})_1$ (the stabilizer of 1) is called the inner mapping group of Q. Also, will denote $(\mathrm{TInn(Q)})_1$ by $\mathrm{TInn(Q)}$.

Multiplication groups of loops are a standard tool of algebraic loop theory. The structure of TMlt(Q) may be of importance when mappings D_a cannot be avoided. Connections to paratopic (i.e., isostrophic) loops are another reason why to study the total multiplication group, in particular in cases when the paratopic loops belong to well known varieties — like left, right and middle Bol loops. And, of course, questions about behavior of TMlt(Q) may point to properties of loops that have not been discussed yet.

Note that if Q is an IP-loop, then Mlt(Q) is of index two in TMlt(Q), while in the general case Mlt(Q) need not be be a normal subgroup. As will be shown, isosotrophic loops possess isomorphic total multiplication groups, generators of TInn(Q) and the center of TMlt(Q) can be characterized in a straightforward way, and from that it may be deduced when TMlt(Q) is nilpotent.

Archimedes automorphic loops

Vasile Ion Ursu

"Simion Stoilov" Indtitute of Mathematics of the Romanian Academy,
Technical University of Moldova

Loops whose inner mappings are automorphisms are called automorphic loops [1].

Right-ordered automorphic loop L is called Archimedean, if in L the following Archimedean axiom is true: for strictly positive elements $x, y \in L$ there exists a natural number n such that $x^n > y$.

In [2] P. E. Conrad using result of O. Hölder [3] proved that every right-ordered Archimedean group is orderly isomorphic to a subgroup of additive group of real numbers with natural order.

We prove that right-ordered Archimedean automorphic loop is commutative and associative, and, therefore, is orderly isomorphic to a subgroup of additive group of real numbers with natural order.

References

[1] R. H. Bruck, L. J. Paige, Loops whose inner mappings are automorphisms. *Ann. of Math.* v. (2) 63 (1956), 308-323.

[2] P. Conrad, Right-ordered groups. *Michigan Math. J.,* v. 6 (1959), 267-275.

[3] O. Hölder, The axioms of quantity and the theory of measurement. Translated from the 1901 German original and with notes by Joel Michell and Catherine Ernst. With an introduction by Michell. *J. Math. Psych.* 41 (1997), no. 4, 345-356.

Counting Quasigroup Words

Stefanie G. Wang

Smith College of Northampton, MA (USA)

This talk will discuss the method used to count the number of reduced words in free quasigroups on s generators of a given length n, the so-called *peri-Catalan numbers*. I will present a closed formula for the peri-Catalan numbers, based on the Euclidean Algorithm, and discuss conjectures about the asymptotic behavior of the peri-Catalan numbers.

Generalised transversals of Latin squares

Ian M. Wanless

Monash University (Australia)

A k-plex in a Latin square is a selection of entries which has exactly k representatives from each row, column and symbol. The 1-plexes are *transversals* and have been studied since Euler. In [2], I conjectured that for all even orders $n > 4$ there is a Latin square that has 3-plexes but no transversal. Here is an example of order 6, with a 3-plex highlighted:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 5 & 1 & 6 & 2 & 4 \\ 4 & 6 & 2 & 5 & 3 & 1 \\ 5 & 4 & 6 & 2 & 1 & 3 \\ 6 & 3 & 5 & 1 & 4 & 2 \end{bmatrix}$$

Much more recently, in joint work with Nick Cavenagh [1], we proved the aforementioned conjecture. We also showed that there are super-exponentially many Latin squares without transversals. I will discuss these two papers and briefly review the intervening history.

References

[1] N. J. Cavenagh and I. M. Wanless, Latin squares with no transversals, *Electron. J. Combin.* **24(2)** (2017), #P2.45.

[2] I. M. Wanless, A generalisation of transversals for Latin squares, *Electron. J. Combin.*, **9(1)** (2002), #R12.

Can quasigroup transformations of random variables be spoofed?

Alexey D. Yashunsky

Keldysh Institute of Applied Mathematics, Moscow (Russia)

A random variable with values in $E_k = \{0, 1, \ldots, k-1\}$ is defined by its distribution, a vector $\mathbf{p} \in \mathbf{S}^{(k)} = \{(p_0, \ldots, p_{k-1}) \mid \sum p_i = 1, p_i \geqslant 0, i = 0, \ldots, k-1\}$. If the arguments of a function $f(x_1, \ldots, x_n)$: $E_k^n \to E_k$ are mutually independent random variables with distributions $\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)}$ respectfully, its value is a new random variable whose distribution is a function $\widehat{f}(\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)})$ of the distributions $\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)}$, $\widehat{f}$: $\left(\mathbf{S}^{(k)}\right)^n \to \mathbf{S}^{(k)}$.

Studying the expressive power of probability distribution transformations eventually leads to the concept of a *probability distribution algebra*, a set of distributions closed under operations from $\widehat{B} = \{\widehat{f} \mid f \in B\}$. Let $V_B(\mathbf{G})$ denote the closure of $\mathbf{G}$ under $\widehat{B}$. If B is made up of quasigroup operations, the set $V_B(\mathbf{G})$ often exhibits a special property: its only limit point is the uniform distribution, which is of particular interest for stream filters in cryptography [1]. This behavior is formalized by the following statement initially proved for binary quasigroup operations in [2]. Let $\lambda(\mathbf{H})$ be the set of limit points of the set $\mathbf{H}$ and $\mu(\mathbf{p}) = \{i \in E_k \mid p_i > 0\}$.

Theorem 1. *Let $\mathbf{G} \subset \mathbf{S}^{(k)}$ be a finite set, $|\mu(\mathbf{g})| > k/2$ for every $\mathbf{g} \in \mathbf{G}$, and B be a finite set of quasigroup operations on E_k of arity greater than* 1. *Then $\lambda(V_B(\mathbf{G})) = \left\{\left(\frac{1}{k}, \ldots, \frac{1}{k}\right)\right\}$.*

Theorem 1 can be in a certain sense partly inverted. A set $\mathbf{H}$ is said to be *essentially flat* if for some finite set $\mathbf{H}'$ the affine hull of $\mathbf{H} \backslash \mathbf{H}'$ does not contain $\mathbf{S}^{(k)}$. A set $\mathbf{H}$ is said to be an *X-set* if $\mathbf{H} \subseteq \mathbf{H}_1 \cup \mathbf{H}_2$ and the affine hull of neither $\mathbf{H}_1$ nor $\mathbf{H}_2$ contains $\mathbf{S}^{(k)}$.

Theorem 2. *Let $\langle \mathbf{H}, \widehat{B} \rangle$ be a probability distribution algebra on E_k, $\lambda(\mathbf{H}) = \{\mathbf{q}\}$, $|\mu(\mathbf{q})| = k$, $\mathbf{H}$ be neither essentially flat nor an X-set, and B contain at least one operation of arity greater than* 1. *Then $\mathbf{q} = \left(\frac{1}{k}, \ldots, \frac{1}{k}\right)$ and every $f \in B$ is a quasigroup operation on E_k.*

Conditions of Theorem 2 cannot be relaxed as there exist non-quasigroup operations producing single limit point algebras that are either X-sets or essentially flat.

References

[1] S. Markovski, D. Gligoroski, V. Bakeva, Quasigroup string processing: Part 1, Contrib., Sec. Math. Tech. Sci., MANU, **XX** 1-2 (1999) 13–28.

[2] A. D. Yashunskii, On transformations of probability distributions by read-once quasigroup formulae, Discr. Math. Appl. **23**, (2013) 211–223.

Distributive biracks

Anna Zamojska-Dzienio

Warsaw University of Technology (Poland)

(Joint work with Přemysl Jedlička and Agata Pilitowska)

Biracks are algebras studied in low-dimensional topology which provide solutions to the Yang-Baxter equation [1]. A structure $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ with four binary operations is called a *birack*, if the following holds for any $x, y, z \in X$:

$$x \circ (x\backslash_\circ y) = y = x\backslash_\circ (x \circ y), \tag{1}$$

$$(y/_\bullet x) \bullet x = y = (y \bullet x)/_\bullet x, \tag{2}$$

$$x \circ (y \circ z) = (x \circ y) \circ ((x \bullet y) \circ z), \tag{3}$$

$$(x \circ y) \bullet ((x \bullet y) \circ z) = (x \bullet (y \circ z)) \circ (y \bullet z), \tag{4}$$

$$(x \bullet y) \bullet z = (x \bullet (y \circ z)) \bullet (y \bullet z). \tag{5}$$

58 Condition (1) means that $(X, \circ, \backslash_\circ)$ is a left quasigroup and, similarly by (2), $(X, \bullet, /_\bullet)$ is a right quasigroup. Identities (3)-(5) come from *braid relation*. We are interested in *distributive* biracks in which $(X, \circ, \backslash_\circ)$ and $(X, \bullet, /_\bullet)$ are *racks*, i.e. are *self-distributive* [3]. They give an interesting class of non-involutive solutions which behave differently of those decribed thoroughly in literature, e.g. [2] and the references there.

References

[1] R. Fenn, M. Jordan-Santana, L. Kauffman, *Biquandles and virtual links*, Topology and its Appl. **145** (2004), 157–175.

[2] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups*, Adv. Math. **338** (2018), 649–701.

[3] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *Multipermutation distributive solutions of Yang-Baxter equation have nilpotent permutation groups*, submitted, available at `http://arxiv.org/abs/1906.03960`

The Finite Embedding Property for IP Loops and Local Embeddability of Groups into Finite IP Loops

Pavol Zlatoš

Faculty of Mathematics, Physics and Informatics, Comenius University (Slovakia)

(Joint work with Martin Vodička, Max-Planck-Institut für Mathematik in den Naturwissenschaften, Germany)

A class $\mathbf{K}$ of groupoids has the *Finite Embedding Property* (FEP) if for every $(G,\cdot)\in\mathbf{K}$ and each finite nonempty subset $X\subseteq G$ there is a *finite* $(H,*)\in\mathbf{K}$ extending $(X,\cdot)$, i.e., $X\subseteq H$ and $x\cdot y=x*y$ for all $x,y\in X$, such that $x\cdot y\in X$.

It is known that the class of all abelian groups has the FEP while the class of all groups has not.

More generally, a groupoid $(G,\cdot)$ is *locally embeddable into a class of groupoids* $\mathbf{M}$ if for every finite set $X\subseteq G$ there is a grupoid $(H,*)\in\mathbf{M}$ such that $X\subseteq H$ and $x\cdot y=x*y$ for all $x,y\in X$ satisfying $x\cdot y\in X$. Informally this means that every finite cut-out from the multiplication table of $(G,\cdot)$ can be embedded into a groupoid from $\mathbf{M}$. A standard model-theoretic argument shows that this condition is equivalent to the embeddability of $(G,\cdot)$ into an *ultraproduct* of groupoids from $\mathbf{M}$.

We prove that the class of all loops with the *inverse property* (IP loops) has the FEP. As a consequence, every group is locally embeddable into the class of all finite IP loops. The proof uses mainly some graph theoretical constructions based on the Dirac's criterion for the existence of hamiltonian cycles and Steiner triple systems.

We will close with formulating some open problems and conjectures dealing with the existence of minimal axiomatic classes $\mathbf{K}$ of IP loops such that every group were locally embeddable into the class $\mathbf{K}_{\text{fin}}$ of all finite members of $\mathbf{K}$, and with the possible role of the class of all Moufang loops within this connection, as well as in the characterization of the so called *sofic groups* in terms of local embeddability.

Notes

Local wifi access:	SSID:	BME-A
	User name:	loops
	Password:	ui7ka7ooxu9v