Report on Doctoral Thesis: '*Designs and Their Algebraic Theory*' by Andrew Kozlík

It is well know that Steiner triple systems (STS) and Mendelsohn triple systems (MTS) can be characterised algebraically as quasigroups. Interestingly this is not necessarily the case for the related designs, Directed triple systems (DTS) and Hybrid triple systems (HTS). Further, even when it is possible to achieve a quasigroup the resulting structures need not exhibit the same global properties. For instance, quasigroups arising from STSs and MTSs satisfy the flexible law and so $x(yx)=(xy)x$, for all x and y, while DTSs and HTSs need not exhibit this property. Historically, considerable effort has be placed on studying algebraic structures which exhibit different properties, properties which manifest as algebraic laws. It is these laws which allow us to reduce computation when applying these structures to solve real world problems.

The diversity of the underlying algebraic structure for DTSs and HTSs provides a unique challenge in terms of characterising subclasses of designs, especially those that replicate as closely as possible the properties of STSs and MTSs, as well as those that are as far from STSs and MTSs as possible.

This thesis makes a substantial contribution to our knowledge of these important structures by settling existence questions for Latin DTSs and Latin HTSs, and in particular those that are flexible, non-flexible and anti-flexible. That is, those that satisfy in all possible cases the flexible law, those that don't satisfy the flexibly law and those that satisfy the flexible law in the least possible number of cases-- this last category makes them as distinct as possible from STSs.

In addition the thesis examines how these properties manifest themselves in systems which are two fold systems, and systematically documents results on cyclic or rotational automorphisms.

The thesis concludes with a discussion of the centre of a Steiner loop (associated quasigroup for a STS) and the connection to the maxi-Pasch problem in STSs.

As is appropriate, the thesis provides a detailed discussion of the history of the problem, including a discussion of the importance of the results to the broader combinatorial theory and their connections with algebra, geometry and topology.

The main body of the thesis begins with a study of Latin DTSs; that is, DTSs which give rise to quasigroups. It provides the first substantial study of these objects, providing comprehensive enumeration results for admissible orders less than or equal to 12. This is a substantial feat as the number of such systems is combinatorially explosive. For orders, between 12 and 20 the thesis documents specific existence or non-existence results, and in many cases establishes the

existence of cyclic designs using theoretical arguments, with structures being classified according to the flexible property. General construction techniques are given for flexible DTSs for all orders congruent to 1 or 3 modulo 6 and non-flexible DTSs for most orders congruent to 0 or 1 modulo 3.

More generally the thesis develops geometric and algebraic techniques to enumerate Latin DTSs and establishes the staggering result that there exists 1206969 non-isomorphism Latin DTSs of order 13. The size of this number necessitated the development of clever theoretical arguments to identify structure invariants and enumerate all possible DTS quasigroups. These arguments exploited the rich connection with geometry and combine this work with combinatorial techniques such as prolongation, demonstrating the breadth of the submitted work.

The thoroughness of this work is clearly demonstrated in the sections on the enumeration of HTSs where the thesis documents substantial results on their spectrum. All orders less than or equal to 10 are studied and classified together with their automorphism groups. Existence results are given for Latin HTSs as well as various subclasses of designs. The connections with well know structures such as STSs are documented, adding to the relevance of the results. Pages 84 and 85 provide an excellent summary of the results obtained in relation to Latin DTSs and Latin HTSs and demonstrate the comprehensive nature of this work and the substantial contribution it makes to the general theory.

In later sections the emphasis shifts to the study of pure flexible and non-flexible Latin DTSs providing detailed existence results for these designs and for completeness a detailed study of anti-flexible Latin DTSs.

In order to achieve the above results the candidate has developed new procedures in the model building tool Mace4 that is part of the package Prover9. Given the extensive nature of the computational results presented in this thesis, it is clear that the author has demonstrated considerable prowess in this and other programming packages.

All of the above work is new and original, and has been accepted for publication in internationally renowned journals.

The thesis concludes with a discussion of the centre for a sloop (a sloop is a particular sort of quasigroup arising from an STS). Substructures defined by central elements are of interest as these entries commute and associate, with other elements of the system. These properties can be used to reduce computation. Thus if, for instance, the sloop is used as part of an encryption procedure it might be possible to exploit this commutativity and associativity to attack the encryption algorithm. The final chapter of this thesis derives necessary and sufficient conditions for the existence of sloops that contain non-trivial central elements. In addition it discusses the connection of this problem to the question of the maximum number of Pasch configurations that can occur in an STS. This is an interesting section which is highly relevant to the application of STSs and associated quasigroups to, for instance, cryptographic systems. I believe that the work presented in this thesis provides an independent proof of the given results, however the author has overlooked early work on this topic and should add references to the papers.

- *The centre of a sloop* by Diane Donovan published in Australasian Journal of Combinatorics, 1, (1990) 83-89.
- *The central spectrum of the order of a Steiner Loop*, by Diane Donovan and Alan Rahilly published in Southeast Asian Bulletin of Mathematics, 15(2), (1991) 115-121.

This thesis constitutes a substantial piece of work with seven paper accepted or appearing in publications and a further paper submitted for publication. These publications attest to the quality of this work and its interest to the general research community.

While this work settles many existence questions, it also raises a number of important open questions suggesting future research directions. For instance, there are a few tantalising open results in Table 1 on page 56.

In conclusion, this is an outstanding thesis that clearly verifies that the candidate has the ability to produce original and creative scientific work. Therefore, I strongly recommend the awarding of this doctorate.

Diane Donovan

Diane Donovan

School of Mathematics and Physics

The University of Queensland

11/8/2015