Report from Dagstuhl Seminar 23161

Pushing the Limits of Computational Combinatorial Constructions

Lucia Moura^{*1}, Anamari Nakic^{*2}, Patric Östergård^{*3}, Alfred Wassermann^{*4}, and Charlene Weiß^{†5}

- 1 University of Ottawa, CA. lmoura@uottawa.ca
- 2 University of Zagreb, HR. anamari.nakic@fer.hr
- 3 Aalto University, FI. patric.ostergard@aalto.fi
- 4 Universität Bayreuth, DE. alfred.wassermann@uni-bayreuth.de
- 5 Universität Paderborn, DE. chweiss@math.uni-paderborn.de

— Abstract -

This report documents the program and the outcomes of Dagstuhl Seminar 23161 "Pushing the Limits of Computational Combinatorial Constructions".

In this Dagstuhl Seminar, we focused on computational methods for challenging problems in combinatorial construction. This includes algorithms for construction of combinatorial objects with prescribed symmetry, for isomorph-free exhaustive generation, and for combinatorial search. Examples of specific algorithmic techniques are tactical decomposition, the Kramer-Mesner method, algebraic methods, graph isomorphism software, isomorph-free generation, clique-finding methods, heuristic search, SAT solvers, and combinatorial optimization. There was an emphasis on problems involving graphs, designs and codes, also including topics in related fields such as finite geometry, graph decomposition, Hadamard matrices, Latin squares, and q-analogs of designs and codes.

Seminar April 16–21, 2023 – https://www.dagstuhl.de/23161

2012 ACM Subject Classification Mathematics of computing \rightarrow Discrete mathematics; Mathematics of computing \rightarrow Mathematical software

Keywords and phrases automorphism groups, combinatorial algorithms, finite geometries, subspace designs

Digital Object Identifier 10.4230/DagRep.13.4.40

1 Executive Summary

Lucia Moura (University of Ottawa, CA) Anamari Nakic (University of Zagreb, HR) Patric Östergård (Aalto University, FI) Alfred Wassermann (Universität Bayreuth, DE)

> License ⊛ Creative Commons BY 4.0 International license © Lucia Moura, Anamari Nakic, Patric Östergård, and Alfred Wassermann

Objectives of the seminar

In this Dagstuhl Seminar, the focus was on computational methods for challenging problems in combinatorial construction. This seminar brought together researchers with different expertise: those with a deep understanding of combinatorial objects and experts in algorithm design and high-performance computing. Participants identified important problems for

Except where otherwise noted, content of this report is licens under a Creative Commons BY 4.0 International license

Pushing the Limits of Computational Combinatorial Constructions, *Dagstuhl Reports*, Vol. 13, Issue 4, pp. 40–57 Editors: Lucia Moura, Anamari Nakic, Patric Östergård, Alfred Wassermann, and Charlene Weiß DAGSTUHL Dagstuhl Reports

^{*} Editor / Organizer

[†] Editorial Assistant / Collector

Except where otherwise noted, content of this report is licensed

REPORTS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

codes, graphs, and designs; and discussed state-of-the-art methods for challenging problems in constructing combinatorial objects. Additionally, the seminar brought together experts on combinatorial algorithms and representatives from different scientific communities developing practical techniques for attacking general hard problems, for example, in the framework of SAT solving, integer linear programming, and optimization.

General overview of the research topic

In discrete mathematics, construction and classification of structures are core problems. Computational methods have been essential in settling important mathematical questions, such as the proof of the four color theorem (Apel and Haken, 1976) and the nonexistence of projective planes of order 10 (Lam et al., 1989). Isomorph-free exhaustive searches are quite challenging with the number of nonequivalent objects often growing exponentially with the input size. For example, the classification of Steiner triple systems of order 19 (Kaski and Östergård, 2004) involved producing a list of more than 11 billion such objects. Vast exhaustive searches are also used to establish negative results, as in the non-existence of 16-clue Sudoku puzzles (McGuire et al., 2012), celebrated by the media due to its connection with the famous puzzle. Many of the central problems, even subproblems, are (NP-)hard, but with improved algorithms and general approaches, it is still possible to handle instances with not too small parameters.

Structure of the seminar

This seminar was conducted in three main forms: plenary sessions, tutorials, and working groups. Each morning started with a plenary session, where we asked four speakers to give 60 minute lectures:

- Curtis Bright (University of Windsor, CA): SAT + Isomorph-free Generation ... and the Quest for the Minimum Kochen-Specker System
- Daniel Heinlein (Aalto University, FI): Enumerating Steiner Triple Systems: Counting STS(21)s
- Vedran Krčadinac (University of Zagreb, HR): On higher-dimensional designs
- Pascal Schweitzer (TU Darmstadt, DE): Automorphisms, Isomorphisms, and Canonization: recent developments

In the first two days of the seminar six leading experts gave 30 minute tutorials and provided input on the current limits of the area:

- Brendan McKay (Australian National University Acton, AU): SURGE : A fact opensource chemical graph generator
- Gordon Royle (The University of Western Australia Crawley, AU): Three stories about computational combinatorics
- Manfred Scheucher (TU Berlin, DE): Using SAT Solvers in Combinatorics and Geometry
- Brett Stevens (Carleton University Ottawa, CA): Thoughts on Computational Design Theory
- Leo Storme (Ghent University, BE): Computational methods in finite geometry
- Ian M. Wanless (Monash University Clayton, AU): Open problems on orthogonal(ish) arrays

In the remaining time participants were partitioned into five working groups, brainstorming and exchanging ideas:

- *Improving reliability and usability of computational projects*
- SAT working group
- Isomorphism Solvers
- Design theory working group
- **—** Tactical decompositions working group

2 Table of Contents

Executive Summary	
Lucia Moura, Anamari Nakic, Patric Östergård, and Alfred Wassermann	40
Overview of Talks	
SAT + Isomorph-free Generationand the Quest for the Minimum Kochen–Specker System Curtis Bright	44
Enumerating Steiner Triple Systems: Counting STS(21)s Daniel Heinlein	45
On higher-dimensional designs Vedran Krčadinac	45
SURGE : A fact open-source chemical graph generator Brendan McKay	46
Three stories about computational combinatorics Gordon Royle	46
Using SAT Solvers in Combinatorics and Geometry <i>Manfred Scheucher</i>	46
Automorphisms, Isomorphisms and Canonization: recent developments Pascal Schweitzer	47
Thoughts on Computational Design Theory Brett Stevens	48
Computational methods in finite geometry Leo Storme	48
Open problems on orthogonal(ish) arrays Ian M. Wanless	49
Working groups	
Improving reliability and usability of computational projects Gordon Royle	49
SAT working group Manfred Scheucher, Curtis Bright, Daniel Heinlein, Petteri Kaski, Leonard H. Soicher, and Alfred Wassermann	50
Isomorphism Solvers Pascal Schweitzer	50
Design theory working group Ian M. Wanless, Ilias S. Kotsireas, Denis Krotov, and Leo Storme	51
Tactical decompositions working group Alfred Wassermann	52
Participants	57

```
3 Overview of Talks
```

3.1 SAT + Isomorph-free Generation ...and the Quest for the Minimum Kochen–Specker System

Curtis Bright (University of Windsor, CA)

License

 © Creative Commons BY 4.0 International license
 © Curtis Bright

 Joint work of Zhengyu Li, Curtis Bright, Vijay Ganesh
 Main reference Zhengyu Li, Curtis Bright, Vijay Ganesh: "An SC-Square Approach to the Minimum Kochen–Specker Problem, SC-Square Workshop, 2022.
 URL https://cs.uwaterloo.ca/ cbright/reports/sc2-ks-preprint.pdf

I will describe a new approach for exhaustively generating combinatorial objects by combining a satisfiability (SAT) solver with an isomorph-free exhaustive generation method such as orderly generation. The SAT solver is able to limit the search to objects that satisfy given criteria, while the isomorph-free generation method ensures that the objects are generated up to isomorphism. The combined search procedure performs orders-of-magnitude faster than a pure SAT or pure computer algebraic approach, as the SAT solver tailors the search to the object in question while the isomorph-free generation avoids duplication of work when the search space is highly symmetrical.

As a motivating example, I will discuss how this approach can be applied to search for Kochen–Specker (KS) systems, an important combinatorial object arising in quantum physics. An exhaustive computer search in 2016 was able to disprove the existence of a KS system of 21 or fewer vectors. Our SAT and orderly generation approach is over 32,000 times faster than the previously used approach and has also ruled out the existence of a KS system with 22 vectors.

- 1 J. Conway, S. Kochen. *The Free Will Theorem*. Foundations of Physics, 2006.
- 2 S. Uijlen, B. Westerbaan. A Kochen-Specker System Has at Least 22 Vectors. New Generation Computing, 2016.
- 3 C. Bright, J. Gerhard, I. Kotsireas, V. Ganesh. Effective Problem Solving Using SAT Solvers. Maple Conference 2019.
- 4 C. Bright, K. Cheung, B. Stevens, D. Roy, I. Kotsireas, V. Ganesh. A nonexistence certificate for projective planes of order ten with weight 15 codewords. Applicable Algebra in Engineering, Communication and Computing, 2020.
- 5 C. Bright, K. Cheung, B. Stevens, I. Kotsireas, V. Ganesh. A SAT-based Resolution of Lam's Problem. AAAI 2021.
- 6 T. Junttila, M. Karppa, P. Kaski, J. Kohonen. An adaptive prefix-assignment technique for symmetry reduction. Journal of Symbolic Computation, 2020.
- 7 J. Savela, E. Oikarinen, M. Järvisalo. Finding periodic apartments via Boolean satisfiability and orderly generation. LPAR 2020.
- 8 M. Kirchweger, M. Scheucher, S Szeider. A SAT Attack on Rota's Basis Conjecture. SAT 2022.
- **9** Z. Li, C. Bright, V. Ganesh. An SC-Square Approach to the Minimum Kochen–Specker Problem, SC-Square Workshop, 2022.
- 10 C. Bright, I. Kotsireas, V. Ganesh. When Satisfiability Checking Meets Symbolic Computation. Communications of the ACM, 2022.

3.2 Enumerating Steiner Triple Systems: Counting STS(21)s

Daniel Heinlein (Aalto University, FI)

License

 © Creative Commons BY 4.0 International license
 © Daniel Heinlein

 Joint work of Östergård, Patric R. J.
 Main reference Daniel Heinlein, Patric R. J. Östergård: "Enumerating Steiner Triple Systems", CoRR, Vol. abs/2303.01207, 2023
 URL https://arxiv.org/abs/2303.01207

Steiner triple systems (STSs) have been classified up to order 19. Earlier estimations of the number of isomorphism classes of STSs of order 21, the smallest open case, are discouraging as for classification, so it is natural to focus on the easier problem of merely counting the isomorphism classes. Computational approaches for counting STSs are here considered and lead to an algorithm that is used to obtain the number of isomorphism classes for order 21: 14,796,207,517,873,771.

3.3 On higher-dimensional designs

Vedran Krčadinac (University of Zagreb, HR)

License

 © Creative Commons BY 4.0 International license
 © Vedran Krčadinac

 Joint work of Vedran Krčadinac, Mario Osvin Pavčević, Kristijan Tabak
 Main reference Vedran Krčadinac, Mario Osvin Pavčević, Kristijan Tabak: "Cubes of symmetric designs", CoRR, Vol. abs/2304.05446, 2023.
 URL https://doi.org/10.48550/arXiv.2304.05446

Higher-dimensional Hadamard matrices were introduced in the 1970s by Paul Shlichta [3, 4]. In 1990, Warwick de Launey [1] developed a general framework for higher-dimensional designs of various types, including symmetric designs, Hadamard matrices, and their generalizations. In this talk I will focus on *n*-dimensional Hadamard matrices and symmetric designs. I will give an overview of the known constructions and present a new construction giving examples that may have inequivalent slices. The new construction was recently discovered in a joint work with Mario Osvin Pavčević and Kristijan Tabak [2]. There are many open questions in this area, including the existence of symmetric designs for some small parameters (v, k, λ) and dimensions $n \geq 3$ when they are known to exist for n = 2. Some of these problems could be good candidates for clever computer constructions.

- W. de Launey, On the construction of n-dimensional designs from 2-dimensional designs, Combinatorial mathematics and combinatorial computing, Vol. 1 (Brisbane, 1989). Australas. J. Combin. 1 (1990), 67–81.
- 2 V. Krčadinac, M. O. Pavčević, K. Tabak, Cubes of symmetric designs, preprint, 2023. http://arxiv.org/abs/2304.05446
- P. J. Shlichta, Three- and four-dimensional Hadamard matrices, Bull. Amer. Phys. Soc. 16 (8) (1971), 825–826.
- 4 P. J. Shlichta, *Higher dimensional Hadamard matrices*, IEEE Trans. Inform. Theory 25 (1979), no. 5, 566–572.

3.4 SURGE : A fact open-source chemical graph generator

Brendan McKay (Australian National University – Acton, AU)

License

 © Creative Commons BY 4.0 International license
 © Brendan McKay

 Joint work of Brendan D. McKay, Christoph Steinbeck, Mehmed Aziz Yirik
 Main reference Brendan D. McKay, Mehmet Aziz Yirik, Christoph Steinbeck: "Surge: a fast open-source chemical graph generator", J. Cheminformatics, Vol. 14(1), p. 24, 2022.
 URL https://doi.org//10.1186/s13321-022-00604-9

Chemical structure generators are used in cheminformatics to produce or enumerate virtual molecules based on a set of boundary conditions. The result can then be tested for properties of interest, such as adherence to measured data or for their suitability as drugs. The starting point can be a potentially fuzzy set of fragments or a molecular formula. In the latter case, the generator produces the set of constitutional isomers of the given input formula. Here we present the novel constitutional isomer generator surge based on the canonical generation path method. Surge uses the nauty package to compute automorphism groups of graphs. We outline the working principles of surge and present benchmarking results which show that surge is currently the fastest structure generator. Surge is available under a liberal open-source license.

3.5 Three stories about computational combinatorics

Gordon Royle (The University of Western Australia - Crawley, AU)

License
 $\textcircled{\mbox{\scriptsize \mbox{\scriptsize \mbox{\mbox{\scriptsize \mbox{\scriptsize \mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\scriptsize \mbox{\mbox}\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox}\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mbox{\mb}\mbox{\mbox{\mb}\mbox{\mbox{\mb}\m$

I discuss three projects in computational combinatorics that highlight issues relating to correctness, reliability and re-usability of the results obtained by such projects.

The three projects discussed are the proof of the four-colour theorem, the proof of the non-existence of a projective plane of order 10 and the construction of the catalogue of 8-element matroids.

3.6 Using SAT Solvers in Combinatorics and Geometry

Manfred Scheucher (TU Berlin, DE)

In this talk, we discuss how modern SAT solvers can be used to tackle mathematical problems. We discuss various problems to give the audience a better understanding, which might be tackled in this fashion, and which might not. Besides the naive SAT formulation further ideas are sometimes required to tackle problems. Additional constraints such as statements which hold "without loss of generality" might need to be added so that solvers terminate in reasonable time.

3.7 Automorphisms, Isomorphisms and Canonization: recent developments

Pascal Schweitzer (TU Darmstadt, DE)

License
Creative Commons BY 4.0 International license
Pascal Schweitzer
Joint work of Markus Anders, Jendrik Brachter, Martin Grohe, Pascal Schweitzer, Julian Stieß, Daniel Wiebking

The Graph Isomorphism Problem, the task of computing automorphisms groups, and Canonization are closely related tasks revolving around symmetries. Indeed, the task of computing symmetries is known to be equivalent to the isomorphism problem, both theoretically and practically. In my talk I will survey two recent advances in the area of algorithmic symmetry detection and exploitation.

I will describe recent improvements in practical graph isomorphism solvers. I will also hint at new insights regarding the structure of automorphism groups of graphs subject to various restrictions. Finally, I will relate canonization algorithms of general combinatorial objects to canonization of graphs and describe new algorithmic ideas for this problem.

The talk reports on various papers including joint work with Markus Anders, Jendrik Brachter, Martin Grohe, Julian Stieß, and Daniel Wiebking.

- Markus Anders, Jendrik Brachter, and Pascal Schweitzer. A characterization of individualization-refinement trees. In Hee-Kap Ahn and Kunihiko Sadakane, editors, 32nd International Symposium on Algorithms and Computation, ISAAC 2021, December 6-8, 2021, Fukuoka, Japan, volume 212 of LIPIcs, pages 24:1–24:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
- 2 Markus Anders and Pascal Schweitzer. Engineering a fast probabilistic isomorphism test. In Martin Farach-Colton and Sabine Storandt, editors, *Proceedings of the Symposium on Algorithm Engineering and Experiments, ALENEX 2021, Virtual Conference, January 10-11, 2021*, pages 73–84. SIAM, 2021.
- 3 Markus Anders and Pascal Schweitzer. Parallel computation of combinatorial symmetries. In Petra Mutzel, Rasmus Pagh, and Grzegorz Herman, editors, 29th Annual European Symposium on Algorithms, ESA 2021, September 6-8, 2021, Lisbon, Portugal (Virtual Conference), volume 204 of LIPIcs, pages 6:1–6:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
- 4 Markus Anders and Pascal Schweitzer. Search problems in trees with symmetries: Near optimal traversal strategies for individualization-refinement algorithms. In Nikhil Bansal, Emanuela Merelli, and James Worrell, editors, 48th International Colloquium on Automata, Languages, and Programming, ICALP 2021, July 12-16, 2021, Glasgow, Scotland (Virtual Conference), volume 198 of LIPIcs, pages 16:1–16:21. Schloss Dagstuhl Leibniz-Zentrum für Informatik, 2021.
- 5 Markus Anders, Pascal Schweitzer, and Julian Stieß. Engineering a preprocessor for symmetry detection. In 21st International Symposium on Experimental Algorithms, SEA 2023, July 24-26, 2023, Barcelona, Spain, 2023. to appear.
- 6 Pascal Schweitzer and Daniel Wiebking. A unifying method for the design of algorithms canonizing combinatorial objects. In Moses Charikar and Edith Cohen, editors, Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019, pages 1247–1258. ACM, 2019.

3.8 Thoughts on Computational Design Theory

Brett Stevens (Carleton University - Ottawa, CA)

License ☺ Creative Commons BY 4.0 International license © Brett Stevens

I will briefly review a history of computational design theory with a bias towards highlighting the breadth of approaches available. I will state three theoretical ideas which seem to be highly relevant to implementing searches: the existence of designs with prescribed automorphism groups, the relationship between designs and codes and the existence of designs derived from other designs. There is a small set of particular algorithms which are heavily used and software systems and implementations which are very useful. I will end with some open problems from large and significant to modest, personal and idiosyncratic.

3.9 Computational methods in finite geometry

Leo Storme (Ghent University, BE)

 $\begin{array}{c} \mbox{License} \ensuremath{\,\textcircled{\textcircled{}}}\xspace{\ensuremath{\bigcirc}}\xspace{\ensuremath{\mathbb{C}}\xspac$

In finite geometries, many different substructures are investigated. Many are investigated for their geometrical interest, but many are also investigated because of their relevance for other domains, such as coding theory.

Many examples of substructures have not yet been found. It is therefore a good idea to search for examples of substructures in finite geometries. It is also good to classify substructures with computational methods. Some computational methods search specifically for substructures in the respective finite geometries. But there are also many graphs associated to finite geometries, so some searches for substructures can be retranslated to clique or coclique problems in the corresponding graphs.

Concrete problems that can be investigated via computational methods:

- searches for large partial spreads in finite projective spaces and in finite classical polar spaces [4],
- searches for even sets in the projective plane PG(2, q), q even,
- 2-colorings in Grassmann graphs [3],
- computational searches for open problems on strongly regular graphs [2],
- Cameron-Liebler sets in finite projective spaces and in finite classical polar spaces, and
- the classification of small affine vector subspace partitions in AG(5,2) [1].

- J. Bamberg, Y. Filmus, F. Ihringer, and S. Kurz, Affine vector space partitions, preprint, 2022. http://arxiv.org/abs/2211.16561.
- 2 A.E. Brouwer and H. Van Maldeghem, *Strongly regular graphs*. Encyclopedia of Mathematics and its Applications, 182. Cambridge University Press, Cambridge, 2022.
- 3 S. De Winter and K. Metsch, Perfect 2-Colorings of the Grassmann Graph of Planes. Electron. J. Combin. 27 (2020), no. 1, Paper No. 1.21, 19 pp.
- 4 S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence, The maximum size of a partial 3-spread in a finite vector space over GF(2). *Des. Codes Cryptogr.* **54** (2010), 101-107.

3.10 Open problems on orthogonal(ish) arrays

Ian M. Wanless (Monash University - Clayton, AU)

License ☺ Creative Commons BY 4.0 International license © Ian M. Wanless Joint work of Ian M. Wanless, Michael Gill, Balázs Pozsgay, Marton Mestyan

A famous combinatorial problem is to find the largest set of MOLS (Mutually orthogonal Latin squares) of order 10. After more than 200 years of research on this question, all that is known is that the answer is in the interval [2,6]. In 2014 Dukes and Howard showed that any set of 4 or more MOLS of order 10 must satisfy two non-trivial relations; that is linear dependencies in their incidence matrix. In recent work with my student Michael Gill we have ruled out any relations on pairs of MOLS of order 10. The logical next step is to attempt a computation of triples of MOLS that satisfy two relations. I discussed the feasibility of such a computation and some of the theory of relations.

Another open problem that I discussed was motivated by recent work on multidirectional unitary operators in quantum information theory. That work has inspired us to define a new combinatorial object called a cyclically orthogonal array (COA). This is a variant of traditional orthogonal arrays where we now only require (combinatorial) orthogonality between sets of columns that are cyclically consecutive. Many open problems were discussed, since this is a brand new field. From the physics point-of-view there is interest in COAs that have symmetries which result in space-reflexive or time-reflexive unitary operators.

References

- M. J. Gill and I. M. Wanless, Pairs of MOLS of order ten satisfying non-trivial relations, Des. Codes Cryptogr. 91 (2023), 1293–1313.
- 2 M. Mestyán, B. Pozsgay and I. M. Wanless, Multi-directional unitarity and maximal entanglement in spatially symmetric quantum states, preprint, 2022. http://arxiv.org/abs/ 2210.13017.

4 Working groups

4.1 Improving reliability and usability of computational projects

Gordon Royle (The University of Western Australia – Crawley, AU)

License ☺ Creative Commons BY 4.0 International license © Gordon Royle Joint work of Working group members

We had a wide-ranging discussion on a variety of issues relating to the practice of combinatorial computing.

This included discussions about a number of aspects:

- Making data sets accessible and persistent, even if its creator retires, dies or loses interest.
- Certificates of non-existence of solutions for SAT and/or ILP and CSP solvers.
- What journals should do with respect to computational papers in terms of how much detail of the computation is needed, and how to permit referees and/or readers to replicate the results.
- Discussion of other attempts to tackle this question, such as funding bodies' requirements for "data management plans" and initiatives like MARDI.

 A variety of other anecdotes, personal viewpoints, pointers to successful and unsuccessful examples of how data can or should be shared, discussion on programs such as GAP, Magma and SageMath.

This was all useful and interesting, but it was more a sharing of opinions and knowledge, and we do not have a specific ongoing "problem" to be solved.

4.2 SAT working group

Manfred Scheucher (TU Berlin, DE), Curtis Bright (University of Windsor, CA), Daniel Heinlein (Aalto University, FI), Petteri Kaski (Aalto University, FI), Leonard H. Soicher (Queen Mary University of London, GB), and Alfred Wassermann (Universität Bayreuth, DE)

License

 Creative Commons BY 4.0 International license
 Manfred Scheucher, Curtis Bright, Daniel Heinlein, Petteri Kaski, Leonard H. Soicher, and Alfred Wassermann

In this working group we have discussed how to model various mathematical problems. Alfred Wassermann and Leonard Soicher both presented interesting instances of the exact cover problem, but for none of the instances we managed to find a solution or disprove existence yet. Apparently, the clique finding tools by Leonard Soicher still outperformed the sat solvers. Together with Curtis Bright we successfully tackle a problem by Ian Wanless on maximally nonassociative quasigroups. More specifically, while the solver managed to show that there exists a unique example on 9 elements in about 10 CPU hours, further engineering (dynamic symmetry breaking) will be required to progress on 10 and 11 elements.

4.3 Isomorphism Solvers

Pascal Schweitzer (TU Darmstadt, DE)

License $\textcircled{\textbf{ co}}$ Creative Commons BY 4.0 International license $\textcircled{ \ \ 0}$ Pascal Schweitzer

Among other things, graph isomorphism solvers and canonization tools find application in the context of isomorphism-free exhaustive generation.

The Working Group on Isomorphism Solvers discussed numerous recent developments regarding theoretical and practical aspects of the development of symmetry detection, isomorphism, and canonization tools. The discussions extended to the limits of current solvers, recent new algorithmic ideas, and low-level implementation details in the core subroutines of existing libraries.

Specifically, the following topics were discussed: current implementations of the software libraries NAUTY/TRACES, BLISS, and DEJAVU, the performance of isomorphism solvers on Latin squares and similar combinatorial objects, and efficient implementations of color refinement. We also discussed design questions regarding the interface that isomorphism solvers do, and should, provide. Finally, the current benchmark library for isomorphism testing was discussed. The authors of the symmetry software libraries present in the Working Group expressed that they welcome the challenging instances that other participants may encounter in their research.

L. Moura, A. Nakic, P. Östergård, A. Wassermann, and C. Weiß

4.4 Design theory working group

Ian M. Wanless (Monash University – Clayton, AU), Ilias S. Kotsireas (Wilfrid Laurier University – Waterloo, CA), Denis Krotov (Sobolev Institute of Mathematics – Novosibirsk, RU), and Leo Storme (Ghent University, BE)

A number of open problems in design theory were discussed, involving areas as diverse as Golay pairs, Hadamard matrices, orthogonal arrays and finite geometry.

4.4.1 Cyclically orthogonal arrays

Motivated by recent work in quantum physics we studied objects called cyclically orthogonal arrays (COAs). These are similar to standard orthogonal arrays except that the orthogonality is only required for sets of columns which are consecutive (in a cyclic order). We found that linear cyclic COAs can be built using cyclotomic polynomials. Also linear space- or time-reflexive examples can be made using generator matrices that satisfy particular symmetries. We also found that non-linear COAs can be built from right-inverse-property quasigroups.

4.4.2 Hadamard matrices

A conjecture of O'Cathain and Wanless [1] states that any trade in a complex Hadamard matrix of order n must contain at least n entries. This conjecture is known to be true for real Hadamard matrices, and for trades that result from multiplying a rectangular subarray by a scalar. A special case of Hadamard matrices with a trade of size n placed in diagonal entries has a skew structure in the real case and skew or mixed-skew structure in the case of complex Hadamard $\{1, -1, i, -i\}$ -matrices. The existence of mixed-skew Hadamard matrices is known only for several small orders. Bicyclic mixed-skew complex Hadamard matrices of order 2n are equivalent to *i*-reversible periodic complex Golay pairs of sequences of length n, whose existence is also unknown for large n.

4.4.3 Golay pairs

Periodic Golay pairs constitute the periodic analog of the well-studied Golay pairs. The computational state-of-the-art in Periodic Golay pairs is contained in the 3 papers [2, 3, 4]. We pose as an open problem the construction of Periodic Golay pairs of order 90. Given that 90 is a highly composite number, the method of compression seems like an appropriate tool.

4.4.4 Finite geometry

See the separate abstract by Leo Storme in Section 3.9.

- P. Ó Catháin and I. M. Wanless, Trades in complex Hadamard matrices, in C. J. Colbourn (ed.), Algebraic Design Theory and Hadamard Matrices, Springer Proceedings in Mathematics and Statistics 133 (2015), 213–221.
- 2 D.Z. Djoković, I.S. Kotsireas, Periodic Golay pairs of length 72. Algebraic design theory and Hadamard matrices, 83–92, Springer Proc. Math. Stat., 133, Springer, Cham, 2015.
- 3 D.Z. Djoković, I.S. Kotsireas, Some new periodic Golay pairs. Numer. Algorithms 69 (2015), no. 3, 523–530.
- 4 D.Z. Djoković, I.S. Kotsireas, D. Recoskie, J. Sawada, Charm bracelets and their application to the construction of periodic Golay pairs. Discrete Appl. Math. 188 (2015), 32–40.

4.5 Tactical decompositions working group

Alfred Wassermann (Universität Bayreuth, DE)

Combinatorial designs. A combinatorial t- (v, k, λ) design (V, \mathcal{D}) is a set V consisting of v points together with a set \mathcal{D} of k-subsets of V called blocks such that each t-subset of V is contained in exactly λ blocks, see e.g. [1, 2] or [7]. The q-analogs of combinatorial designs are called subspace designs, see [5] for an introduction and overview.

It is well known that a t- (v, k, λ) design (V, \mathcal{D}) is also an s- (v, k, λ_s) design for $0 \le s \le t$ where

$$\lambda_s = \lambda \, \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} \, .$$

In particular, λ_0 is the number of blocks of the design and λ_1 is the number of blocks each point is contained in, which is called the *replication number*. It is also well known that for a t- (v, k, λ) design the number of blocks which contain a given *i*-set of points and are disjoint to a given *j*-set of points is equal to

$$\lambda_{i,j} = \lambda \, \frac{\binom{v-i-j}{k-j}}{\binom{v-t}{k-t}} \,,$$

see e.g. [7, II.4.2, p. 80].

Incidence matrices. The $v \times \lambda_0$ point-block incidence matrix N of a t- (v, k, λ) design (V, \mathcal{D}) is defined by

$$N_{P,B} = \begin{cases} 1, & \text{if } P \in B, \\ 0, & \text{otherwise} \end{cases}$$

for $P \in V$ and $B \in \mathcal{D}$. Bose [4] showed for the point-block incidence matrix N of a 2- (v, k, λ) design the equation

$$NN^{\top} = \lambda_1 I + \lambda (J - I), \tag{1}$$

where I is the $v \times v$ identity matrix and J is the $v \times v$ all-ones matrix.

For a general t- (v, k, λ) design with $t \ge 2$, the $\binom{v}{e} \times \lambda_0$ higher incidence matrix $N^{(e)}$ for $e \le k$ is defined by

$$N_{E,B}^{(e)} = \begin{cases} 1, & \text{if } E \subset B, \\ 0, & \text{otherwise} \end{cases}$$

for $E \in \binom{V}{e}$ and $B \in \mathcal{D}$. The $\binom{v}{s} \times \binom{v}{e}$ incidence matrix $W^{(se)}$ between s-subsets and all e-subsets of V is defined by

$$W_{S,E}^{(se)} = \begin{cases} 1, & \text{if } S \subset E, \\ 0, & \text{otherwise} \end{cases}$$

L. Moura, A. Nakic, P. Östergård, A. Wassermann, and C. Weiß

for $S \in \binom{V}{s}$ and $E \in \binom{V}{e}$. Wilson [18] showed for $e + f \leq t$ the equation

$$N^{(e)} (N^{(f)})^{\top} = \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i,i} (W^{(ie)})^{\top} W^{(if)}.$$
⁽²⁾

Note that $N^{(e)}(N^{(f)})^{\top}$ contains in the row labeled by the *e*-subset *E* and in the column labeled by the *f*-subset *F* the number of blocks of the design which contain both *E* and *F*. It is clear that this number is $\lambda_{e+f-\mu}$ with $\mu = \#(E \cap F)$, i.e.

$$\left(N^{(e)} \left(N^{(f)}\right)^{\top}\right)_{E,F} = \lambda_{\#(E\cup F)} \,.$$

Also in [18], Wilson proved among others the equation

$$W^{(ie)} N^{(e)} = \binom{k-i}{e-i} N^{(i)} \quad \text{for } 0 \le i \le e \le k \,.$$

$$\tag{3}$$

For e = 1 and i = 0 equation (3) simply states that each block of the design contains k points.

Tactical decomposition matrices. The use of *tactical decompositions* in design theory has been initiated by Dembowski [9], see also [10] and Beutelspacher [3, pp. 210–220]. Dembowski's main interest was to use tactical decompositions to study properties of symmetric designs. From an algorithmic point of view, tactical decompositions were first used by Janko and Tran Van Trung [11] to construct symmetric (78, 22, 6) designs. Their method was picked up and generalized in numerous papers, see [6, 8, 14] to name just a few. In [17] the use of tactical decompositions has been generalized to subspace designs.

Dembowski [9, 10] studied tactical decompositions of incidence structures from group actions, see also Beutelspacher [3, pp. 210–220].

Let (V, \mathcal{D}) be a 2- (v, k, λ) design invariant under some group G. The action of G partitions V into orbits $\mathcal{P}_1, \ldots, \mathcal{P}_m$ and \mathcal{D} into orbits $\mathcal{B}_1, \ldots, \mathcal{B}_n$. Let N be the point-block incidence matrix of (V, \mathcal{D}) and for $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ let $N_{i,j}$ be the submatrix of N whose rows are assigned to the elements \mathcal{P}_i and whose columns to the elements of \mathcal{B}_j . Then $N_{i,j}$ has a constant number of ones in each row and a constant number of ones in each column. Such a decomposition of N into submatrices $N_{i,j}$ is called *tactical*.

If we replace for all i, j the submatrix $N_{i,j}$ by the number of ones in each row we get an $(m \times n)$ -matrix ρ , and if we replace the submatrix $N_{i,j}$ by the number of ones in each column we get an $(m \times n)$ -matrix κ . The matrices ρ and κ are both called *tactical decomposition matrix*. In [9] the following properties of ρ and κ and the matrices $P = \text{diag}(\#\mathcal{P}_i)$ and $B = \text{diag}(\#\mathcal{B}_i)$ are shown:

$$P \cdot \rho = \kappa \cdot B \tag{4}$$

$$\rho \cdot (1, \dots, 1)^{\top} = (\lambda_1, \dots, \lambda_1)^{\top} \tag{5}$$

$$(1,\ldots,1)\cdot\kappa = (k,\ldots,k) \tag{6}$$

$$\rho \cdot \kappa^{\top} = (\lambda_1 - \lambda) \cdot I + \lambda \cdot P \cdot J \tag{7}$$

The general approach outlined by Janko and Tran Van Trung is to first enumerate all tactical decomposition matrices of designs with prescribed automorphisms up to permutations of rows and columns. For this, Dembowski [9] has given powerful constraints for a matrix to be a tactical decomposition of the point-block incidence matrix of a 2-design. In a second step, all remaining tactical decomposition matrices are expanded – if possible – to point-block incidence matrices of designs.

Compared with the well-known method of Kramer and Mesner [13] which also restricts the search space to designs with prescribed automorphisms, the method of Janko and Tran Van Trung has the advantage that it is not necessary to compute all orbits of k-subsets of V and therefore allows the search for 2- (v, k, λ) designs with larger k and smaller automorphism group. The drawback however is that it does not reduce the search space if the prescribed group of automorphisms is point-transitive, and that it seemed to be restricted to 2-designs for a long time.

In recent years two generalizations to t-designs for $t \ge 2$ have been published.

The first generalization in [14, 15, 16] gives constraints for the tactical decomposition of the point-block incidence matrix of a t-design of general strength $t \ge 2$:

▶ **Theorem 1.** Let $1 \le s \le t$ and m_1, \ldots, M_s be positive integers, such that $m_s + \cdots + m_s \le t$. Let $\mathfrak{P}_{i_1}, \ldots, \mathfrak{P}_{i_s}$ be mutually distinct. Then

$$\sum_{j=1}^{n} \rho_{i_1 j} \kappa_{i_1 j}^{m_1 - 1} \kappa_{i_2 j}^{m_2} \cdots \kappa_{i_s j}^{m_s} = \sum_{\omega \in \Omega} \lambda_{\omega_1 + \dots + \omega_s} \begin{Bmatrix} m_1 \\ \omega_1 \end{Bmatrix} (\# \mathfrak{P}_{i_1} - 1)_{\omega_1 - 1} \prod_{j=2}^{s} \begin{Bmatrix} m_j \\ \omega_j \end{Bmatrix} (\# \mathfrak{P}_{i_j})_{\omega_j} + \sum_{j=1}^{s} \binom{m_j}{\omega_j} \binom{m_j}{\omega_j} (\# \mathfrak{P}_{i_j})_{\omega_j} + \sum_{j=1}^{s} \binom{m_j}{\omega_j} \binom{m_j}{\omega_j}$$

where

 $\Omega = \{(\omega_1, \ldots, \omega_s) \mid 1 \le \omega_j \le m_i\},\$

 $\begin{cases} n \\ k \end{cases} are the Stirling numbers of second kind and <math>(x)_n = \prod_{i=0}^{n-1} (x-i)$ is the falling factorial.

The second generalization in [12] defines higher tactical decomposition matrices and shows the Wilson's equations can be generalized to these higher tactical decomposition matrices.

For $x \in \{0, \ldots, v\}$, let \mathfrak{P}_x be a partition of the set $\binom{V}{x}$. The part of \mathfrak{P}_x containing some $X \in \binom{V}{x}$ will be denoted by [X]. We call $(\mathfrak{P}_0, \ldots, \mathfrak{P}_v)$ a *tactical sequence of partitions* on V if for all $x, y \in \{0, \ldots, v\}$ with $x \leq y$ and for all $[X], \mathcal{X} \in \mathfrak{P}_x$ and $[Y], \mathcal{Y} \in \mathfrak{P}_y$, the numbers

$$R_{[X],\mathcal{Y}}^{(xy)} = \#\{Y \in \mathcal{Y} \mid X \subseteq Y\} \quad \text{and} \quad K_{\mathcal{X},[Y]}^{(xy)} = \#\{X \in \mathcal{X} \mid X \subseteq Y\}$$

are well-defined, i.e. they do not depend on the choice of the representative X of [X] nor of the representative Y of [Y]. In this case, the above defined numbers yield matrices $R^{(xy)}, K^{(xy)} \in \mathbb{Z}^{\mathfrak{P}_x \times \mathfrak{P}_y}$. A common source of tactical sequences of partitions are permutation groups $G \leq S_V$, where for all $x \in \{0, \ldots, v\}$ the partition \mathfrak{P}_x is the set of orbits of the induced action of G on $\binom{V}{x}$.

In the following, a tactical sequence $(\mathfrak{P}_0, \ldots, \mathfrak{P}_v)$ of partitions on V is fixed. The matrices $R^{(xx)}$ and $K^{(xx)}$ are $\#\mathfrak{P}_x \times \#\mathfrak{P}_x$ identity matrices. The matrices $R^{(0x)}$ and $K^{(0x)}$ are of size $1 \times \#\mathfrak{P}_x$, where all entries of $K^{(0x)}$ are 1, and $R^{(0x)}$ contains the part sizes, i. e. $R_{\{\emptyset\},\mathcal{X}}^{(0x)} = \#\mathcal{X}$.

Let (V, \mathcal{D}) be t- (v, k, λ) design with $t \leq k \leq v - t$, such that the block set is the union of parts in \mathfrak{P}_k , i.e. $\mathcal{D} = \bigcup \mathfrak{B}$ with $\mathfrak{B} \subseteq \mathfrak{P}_k$.

For $x \in \{0, \dots, k\}$ we define the tactical decomposition matrices $\rho^{(x)}, \kappa^{(x)} \in \mathbb{Z}^{\mathfrak{P}_x \times \mathfrak{P}}$ via

$$\rho_{[X],\mathcal{B}}^{(x)} = \#\{B \in \mathcal{B} \mid X \subseteq B\} \quad \text{and} \quad \kappa_{\mathcal{X},[B]}^{(x)} = \#\{X \in \mathcal{X} \mid X \subseteq B\}.$$

By the properties of the fixed tactical sequence $(\mathfrak{P}_0, \ldots, \mathfrak{P}_v)$ of partitions on V, this definition does not depend on the choice of the representatives. Note that $\rho^{(x)}$ is the restriction of $R^{(xk)}$ to the columns whose labels are contained in \mathfrak{B} . In particular, $\rho^{(0)}$ and $\kappa^{(0)}$ are of size $1 \times \#\mathfrak{B}$, where all entries of $\kappa^{(0)}$ are 1, and $\rho^{(0)}$ contains the sizes of the block parts.

In [12] the following theorem has been proved for these higher tactical decomposition matrices.

L. Moura, A. Nakic, P. Östergård, A. Wassermann, and C. Weiß

▶ **Theorem 2.** Let V be a finite set of size v and let $(\mathfrak{P}_0, \ldots, \mathfrak{P}_v)$ be a tactical sequence of partitions on V. Let (V, \mathcal{D}) be a non-empty t- (v, k, λ) design with $t \leq k \leq v - t$, such that the block set has the form $\mathcal{D} = \bigcup \mathfrak{B}$ with $\mathfrak{B} \subseteq \mathfrak{P}_k$. Let e, f be non-negative integers with $e + f \leq t$.

Then

$$\rho^{(e)} \left(\kappa^{(f)} \right)^{\top} = \sum_{j=0}^{\min(e,f)} \lambda_{e+f-j,j} \left(K^{(je)} \right)^{\top} R^{(jf)}$$

Moreover, for non-negative integers x, y with $x \leq y \leq k$

$$R^{(xy)} \rho^{(y)} = \binom{k-x}{y-x} \rho^{(x)} \quad and \quad K^{(xy)} \kappa^{(y)} = \binom{k-x}{y-x} \kappa^{(x)}.$$

It should be noted that the above theorem has a q-analog version for subspace designs.

Summary of the work. In the working group an introduction to tactical decomposition matrices has been given. This was followed by a long discussion in which the two generalizations were compared and where it was attempted to derive the first generalization from the second. As a result, the exact relation of the two generalizations could not be determined easily and will be subject of future research work.

Next, algorithmic use of the second generalization was studied. The participants of the working group agreed that the approach by Janko and Tran van Trung might be generalized to higher tactical decompositions, however its applicability will be restricted to a very specific set of parameters of combinatorial designs and choice of prescribed automorphism groups.

As a followup, research groups from Zagreb and Bayreuth are planning to write a proposal for a joint research project to develop a practical algorithm based on higher tactical decomposition matrices.

Another topic of the working group was the indexing step of the Janko-Tran van Trung algorithm and possible generalizations.

Finally, for graphs and hypergraphs the concept of tactical decomposition matrices is known as *equitable partitions*. Main contributions for these have been given by the research group in Novosibirsk. The presentation of results on equitable partitions lead to surprising connections to the so called Hartman's conjecture in design theory. This was explored and further research on this connection seems to be promising.

- T. Beth, D. Jungnickel, and H. Lenz. *Design theory*. 2nd ed. Vol. I. Encyclopedia of Mathematics and its Applications 69. Cambridge: Cambridge University Press, 1999. DOI: 10.1017/CB09780511549533.
- 2 T. Beth, D. Jungnickel, and H. Lenz. *Design theory*. 2nd ed. Vol. II. Encyclopedia of Mathematics and its Applications 78. Cambridge: Cambridge University Press, 1999. DOI: 10.1017/CB09781139507660.
- 3 A. Beutelspacher. *Einführung in die endliche Geometrie*. Vol. I: *Blockpläne*. Mannheim: Bibliographisches Institut, 1982.
- 4 R. C. Bose. "A note on Fisher's inequality for balanced incomplete block designs". In: Ann. Math. Statistics 20.4 (1949), pp. 619–620. DOI: 10.1214/aoms/1177729958.
- 5 M. Braun, M. Kiermaier, and A. Wassermann. "q-analogs of designs: subspace designs". In: Network coding and subspace designs. Ed. by M. Greferath, M. O. Pavčević, N. Silberstein, and M. Á. Vázquez-Castro. Signals Commun. Technol. Cham: Springer, 2018, pp. 171–211. DOI: 10.1007/978-3-319-70293-3_8.

- 6 V. Ćepulić. "On symmetric block designs (40, 13, 4) with automorphisms of order 5". In: Discrete Math. 128.1 (1994), pp. 45–60. DOI: 10.1016/0012-365X(94)90103-1.
- 7 C. J. Colbourn and J. H. Dinitz, eds. Handbook of combinatorial designs. 2nd ed. Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC, 2007. DOI: 10.1201/9781420010541.
- 8 D. Crnković and S. Rukavina. "Construction of block designs admitting an Abelian automorphism group". In: Metrika 62.2–3 (2005), pp. 175–183. DOI: 10.1007/ s00184-005-0407-y.
- P. Dembowski. "Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen". In: Math. Z. 69.1 (1958), pp. 59–89. DOI: 10.1007/BF01187393.
- 10 P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete 44. Berlin and New York: Springer-Verlag, 1968.
- 11 Z. Janko and T. V. Trung. "Construction of a new symmetric block design for (78, 22, 6) with the help of tactical decompositions". In: J. Combin. Theory, Ser. A 40.2 (1985), pp. 451–455. DOI: 10.1016/0097-3165(85)90107-4.
- 12 M. Kiermaier and A. Wassermann. "Higher incidence matrices and tactical decomposition matrices". In: *Glasnik Matematički* to appear (2023).
- 13 E. S. Kramer and D. M. Mesner. "t-designs on hypergraphs". In: Discrete Math. 15.3 (1976), pp. 263–296. DOI: 10.1016/0012-365X(76)90030-3.
- 14 V. Krčadinac, A. Nakić, and M. O. Pavčević. "The Kramer-Mesner method with tactical decompositions: some new unitals on 65 points". In: J. Combin. Des. 19.4 (2011), pp. 290–303. DOI: 10.1002/jcd.20277.
- 15 V. Krčadinac, A. Nakić, and M. O. Pavčević. "Equations for coefficients of tactical decomposition matrices for t-designs". In: Des. Codes Cryptogr. 72.2 (2014), pp. 465–469. DOI: 10.1007/s10623-012-9779-y.
- A. Nakić. "Non-existence of a simple 3-(16,7,5) design with an automorphism of order 3".
 In: *Discrete Math.* 338.4 (2015), pp. 555–565. DOI: 10.1016/j.disc.2014.11.016.
- 17 A. Nakić and M. O. Pavčević. "Tactical decompositions of designs over finite fields". In: Des. Codes Cryptogr. 77.1 (2015), pp. 49–60. DOI: 10.1007/s10623-014-9988-7.
- 18 R. M. Wilson. "Incidence matrices of t-designs". In: Linear Algebra Appl. 46 (1982), pp. 73–82. DOI: 10.1016/0024-3795(82)90027-1.

Participants

Thais Bardini Idalino Federal University of Santa Catarina, BR Curtis Bright University of Windsor, CA Jan De Beule Free University of Brussels, BE Alena Ernst Universität Paderborn, DE Tuvi Etzion Technion – Haifa, IL Marcus Greferath University College Dublin, IE Daniel Heinlein Aalto University, FI Delaram Kahrobaei City University of New York, US Petteri Kaski Aalto University, FI Sandra Kiefer University of Oxford, GB Michael Kiermaier Universität Bayreuth, DE Ilias S. Kotsireas Wilfrid Laurier University – Waterloo, CA Vedran Krcadinac University of Zagreb, HR

Aleksandr Krotov Innopolis University, RU Denis Krotov Sobolev Institute of Mathematics - Novosibirsk, RU Sascha Kurz Universität Bayreuth, DE Pekka Lampio Aalto University, FI Brendan McKay Australian National University -Acton, AU Lucia Moura University of Ottawa, CA Gábor P. Nagy Budapest University of Technology & Economics, HU Anamari Nakic University of Zagreb, HR Eamonn O'Brien -University of Auckland, NZ Patric Östergård -Aalto University, FI Mario Osvin Pavcevic University of Zagreb, HR David Pike Memorial University of Newfoundland – St. John's, CA

Adolfo Piperno Sapienza University of Rome, IT Gordon Royle The University of Western Australia – Crawley, AU Manfred Scheucher TU Berlin, DE Pascal Schweitzer TU Darmstadt, DE Leonard H. Soicher Queen Mary University of London, GB Brett Stevens Carleton University -Ottawa, CA Leo Storme Ghent University, BE Ana Sumberac University of Rijeka, HR Edwin van Dam Tilburg University, NL Ian M. Wanless Monash University -Clayton, AU Alfred Wassermann Universität Bayreuth, DE Charlene Weiß Universität Paderborn, DE

