October 24, 2022

Final report

on the **OTKA K 134851** Research Project, October 1, 2021 – September 20, 2022

1. Three quotations from the original project proposal of February 4, 2020

(a) From the ``*Summary and aims of the research for the public*'' part: ``*If interested students come in the future, the results of the project can be exploited in PhD training*.''

(b) From the ``*Workplan*'' part: ``*The results of the project will be disseminated in at least three mathematical research papers. (But, hopefully, in more than three papers.) These papers will be submitted to international mathematical journals during the project. At least one of these papers will be submitted in the first year of the project*.''

(c) The ``*What is the major research question*'' part of the project proposal was the following: ``*The research focuses on semimodular lattices, their congruence lattices, planar lattices, convex geometry, lattices generated by few elements, rotational lattices, principal congruences of lattices, lattices of compatible quasiorders and other relations of algebras, and also on any related problem and topic that might naturally arise but not listed here*. ''

2. Results obtained

The results are in the 16 research papers listed below. They belong exclusively to this OTKA K 134851. Papers [1]–[11] have appeared in journals (at least online), and [12]–[16] are under review at journals.

Technical remark: DOI's and links in upright normal font are permanent ones. Links in *italic* are either easier to use, or point at more recent versions, or allow downloading author-made pdf files. The earlier (arXiv) versions slightly differ from the journal versions and some of them are extended on purpose or with different titles. {Links in this font are (mainly) for subscribers} The site http://www.math.u-szeged.hu/~czedli/ contains all these links, too, and it contains some computer programs related to some of these papers.

[1] Gábor Czédli and Lillian Oluoch: Four-element generating sets of partition lattices and their direct products. *Acta Sci. Math. (Szeged)* 86 (2020) 405-448. https://doi.org/10.14232/actasm-020-126-7, (arXiv).

Let n > 3 be a natural number. By a 1975 result of H. Strietz, the lattice Part(n) of all partitions of an n-element set has a four-element generating set. We give a lower bound on the number ν(n) of four-element generating sets of Part(n), and present a computer-assisted statistical approach to ν(n) for small values of n. Solving L. Zádori's problem from 1983, we prove that Part(n) has a four element generating set that is not an antichain for n = 6 but not for n = 5. By our main theorem, the direct product of some powers of partition lattices is four-generated. In particular, Part(n) × Part(m) is four-generated for any integers 4<n<m and, say, so is the 10127-th direct power of Part(1011) × Part(1012) × · · · × Part(2020).

[2] Ahmed Delbrin and Gábor Czédli: (1+1+2)-generated lattices of quasiorders. *Acta Sci. Math. (Szeged)*, 87 (2021), 415-427. https://doi.org/10.14232/actasm-021-303-1, (arXiv) .

A lattice is (1+1+2)-generated if it has a four-element generating set such that exactly two of the four generators are comparable. We prove that the lattice Quo(n) of all quasiorders (also known as preorders) of an n-element set is (1 + 1 + 2)-generated for n = 3 (trivially), n = 6 (when Quo(6) consists of 209 527 elements), n = 11, and for every natural number n > 12. In 2017, the second author and J. Kulin proved that Quo(n) is (1 + 1 + 2)-generated if either n is odd and at least 13 or n is even and at least 56. Compared to the 2017 result, this paper presents twenty-four new numbers n such that Quo(n) is (1 + 1 + 2)-generated.

[3] Gábor Czédli: Four-generated direct powers of partition lattices and authentication, *Publicationes Math. (Debrecen)* 99 (2021), 447-472. *https://tinyurl.com/czedli-161*, (arXiv),

{https://doi.org/10.5486/PMD.2021.9024}.

For motivations and notations, see [1] above. The paper proves that, in addition to Part(n), even the k-th direct power $\mathrm{Part}(n)^k$ of Part(n) is four-generated for many but only finitely many exponents k. For much larger k's as in [1], as the "Chronology" part of [3] explains. E.g., $\mathrm{Part}(100)^k$ is four-generated for every k not greater than 3×10^{89} (three times ten to the eighty-nine). Also, $\mathrm{Part}(100)^k$ is (1 + 1 + 2)-generated for every k at most 1.4×10^{34}. In connection with these results, we outline a protocol how to use these lattices in authentication and secret key cryptography.

[4] Gábor Czédli: Lamps in slim rectangular planar semimodular lattices, Acta Sci. Math. (Szeged), 87 (2021), 381-413. https://doi.org/10.14232/actasm-021-865-y (arXiv).

This paper deals with the congruence lattices of *slim planar semimodular* lattices, *SPS lattices* for short. A planar (upper) semimodular lattice L is *slim* if the five-element nondistributive modular lattice M_3 does not occur among its sublattices. (Planar lattices are finite by definition.) These lattices have some connection with finite model theory (see [6] below) and they have already led to new results both in combinatorial geometry and in group theory. In particular, G. Czédli and E. T. Schmidt, 2011, used these lattices to add a uniqueness part to the classical Jordan–Hölder theorem for finite groups. Since a 2007 paper of G. Grätzer and E. Knapp, where these lattices were introduced, SPS lattices have constituted the most intensively studied part of lattice theory. As the appendix of http://arxiv.org/abs/2107.10202 or the updated https://tinyurl.com/czedli-publ-psml lists, more than four dozen papers have been published on or in connection with these lattices since 2007. Note that planar semimodular lattices are easily described by their slimmings, which are SPS lattices. To understand the congruence lattices of SPS lattices, it suffices to deal with *slim rectangular* lattices; they are SPS lattices with a complemented pair of doubly irreducible elements; they were defined by G. Grätzer and E. Knapp in 2009. SPS lattices are best drawn by C_1-*diagrams*, defined by the author in 2017. Based on C_1-diagrams and to provide an effective tool for studying the congruence lattices of SPS lattices, we introduce the concept of *lamps of slim rectangular lattices* and prove several properties of lamps. Lamps and the toolkit based on them allow us to prove in a new and easy way that the congruence lattices of SPS lattices satisfy both previously known properties. Furthermore, lamps allow us to find and prove four new properties; here we only mention the Bipartite Maximal Elements Property, *BMEP* for short.

[5] Gábor Czédli and George Grätzer: A new property of congruence lattices of slim, planar, semimodular lattices. Categories and General Algebraic Structures with Applications, 16 (2022) 1-28. https://cgasa.sbu.ac.ir/article_101508.html, *https://tinyurl.com/czedli-166*, (arXiv).

In this joint paper, using the tools (lamps) developed in [4], we prove yet another property of the congruence lattices of SPS lattices, the Three-pendant Three-crown Property.

[6] Gábor Czédli: Cyclic congruences of slim semimodular lattices and non-finite axiomatizability of some finite structures, Archivum Mathematicum (Brno), 58 (2022) 15-33. http://dml.cz/dmlcz/149444, (arXiv).

This paper gives a new proof of the fact that *finite* bipartite graphs cannot be axiomatized by finitely many first-order sentences among *finite* graphs. (This fact is a consequence of a general theorem proved by L. Ham and M. Jackson, and the counterpart of this fact for *all* bipartite graphs in the class of *all* graphs is a well-known consequence of the compactness theorem.) Also, to exemplify that our method is applicable in various fields of mathematics, we prove that neither finite simple groups, nor the ordered sets J(Con(L)) of join-irreducible congruences of SPS lattices L (see [4]) can be described by finitely many axioms in the class of finite structures. Furthermore, we present a new property, called Decomposable Cyclic Elements Property (DCEP), of the congruence lattices Con(L) of SPS lattices L. The results of the paper lead to the following. (a) The lattice Con(L) satisfies DCEP if and only if the poset J(Con(L)) satisfies BMEP, see [4]. (b) Con(L) and J(Con(L)) mutually determine each other (up to isomorphism), as it has been known for long. (c) DCEP and all propertied proved or mentioned in [4] and [5] are finitely axiomatized in the class of finite *lattices*. However, (d) BMEP cannot be finitely axiomatized in the class of finite *posets*.

[7] Gábor Czédli and Ali Molkhasi: Is there an absolute retract for the class of slim semimodular lattices? Order, 22 pages, SharedIt (read-only) https://rdcu.be/cLHkn, {https://doi.org/10.1007/s11083-021-09592-1}, (arXiv).

Let K be a concrete category of algebras. For A and B in K, we say that B is a *K-extension* of A if A is a subalgebra of B and the ``natural'' x→x embedding is an A→B morphism in K. An algebra A in K is said to be an *absolute retract* for K if for any K-extension B of A there is a retraction f: B→A (that is, a homomorphism satisfying f(x)=x for all x in A) such that f is a morphism in K. Let n denote a positive integer. We describe the absolute retracts for the following five categories of finite lattices: (1) SPS lattices, see [4], (2) finite distributive lattices, (3) at most n-dimensional finite distributive lattices, (4) at most n-dimensional finite distributive lattices with cover-preserving {0,1}-homomorphisms, and (5) finite distributive lattices with cover-preserving {0,1}-homomorphisms. Although the singleton lattice is the only absolute retract for the first category, this result has paved the way to some other categories. For the second category, we prove that the absolute retracts are exactly the finite boolean lattices; this generalizes a 1979 result of Jürg Schmid. For the third and fourth categories, the absolute retracts are the finite boolean lattices of dimension at most n and the direct products of n nontrivial finite chains. For the fifth category, the absolute retracts are the same as those for the second.

[8] Gábor Czédli: *A property of lattices of sublattices closed under taking relative complements and its connection to* 2*-distributivity*. Mathematica Pannonica 28 (2022) 109-117. https://doi.org/10.1556/314.2022.00014, (arXiv).

For a modular lattice L of finite length, we prove that the distributivity of L is a sufficient condition while its 2-distributivity is a necessary condition that those sublattices of L that are closed under taking relative complements form a ranked lattice of finite length.

[9] Gábor Czédli: *Atoms and coatoms in three-generated lattices*. Novi Sad Journal of Mathematics, 26 pages, published online, https://doi.org/10.30755/NSJOM.12402 , (arXiv).

In addition to the unique cover M^+ of the variety of modular lattices, this paper deals with those twenty-three known covers of M^+ that can be extracted from the literature. For M^+ and for each of these twenty-three known varieties covering it, we determine what the pair formed by the number of atoms and that of coatoms of a three-generated lattice belonging to the variety in question can be. Furthermore, for each variety W of lattices that is obtained by forming the join of some of the twenty-three varieties mentioned above, that is, for 2^{23} = 8 388 608 possible choices of W, we determine how many atoms a three-generated lattice belonging to W can have. The greatest number of atoms occurring in this way is only six. In order to point out that this need not be so for larger varieties, we construct a 47092-element three-generated lattice that has exactly eighteen atoms. In addition to purely lattice theoretical proofs, which constitute the majority of the paper, some computer-assisted arguments are also presented.

[10] Gábor Czédli: *Lattices of retracts of direct products of two finite chains and notes on retracts of lattices*. Algebra Universalis (2022) 83:34 (19 pages). SharedIt (read-only): https://rdcu.be/cSVBh, author's pdf *https://tinyurl.com/czedli-172*, (arXiv), {https://doi.org/10.1007/s00012-022-00788-z}.

Ordered by set inclusion, the retracts of a lattice L together with the empty set form a bounded poset Ret(L). By a grid we mean the direct product of two non-singleton finite chains. We prove that if G is a grid, then Ret(G) is a lattice. We determine the number of elements of Ret(G). Some easy properties of retracts, retractions, and their kernels called retraction congruences of (mainly distributive) lattices are found. Also, we present several examples, including a 12-element modular lattice M such that Ret(M) is not a lattice.

[11] Gábor Czédli: *A property of meets in slim semimodular lattices and its application to retracts*. Acta Sci. Math. (Szeged), 16 pages, published online, SharedIt (read-only): https://rdcu.be/cX3mh, author's pdf *https://tinyurl.com/czedli-170*, (arXiv), {https://doi.org/10.1007/s44146-022-00040-z}.

We prove that if x and y are incomparable elements in an SPS lattice L, see [4], then the interval C = [x ∧ y, x] is a chain, C is of a normal slope in every C_1-diagram of L, see [4], and every u in C-{x} is meet-reducible. In the direct square K_1 of the three-element chain, let X_1 and A_1 be the set of atoms and the sublattice generated by 0 and the coatoms, respectively. Denote by K_2 the unique eight-element

lattice embeddable in K_1. Let A_2 be the sublattice of K_2 consisting of 0, 1, the meet-reducible atom, and the join-reducible coatom. Let X_2 stand for the singleton consisting of the doubly reducible element of K_2. For $i = 1, 2$, we apply the above-mentioned property of meets to prove that whenever K_i is a sublattice and S_i is a retract of an SPS lattice L, then $A_i \subseteq S_i$ implies that $X_i \subseteq S_i$.

[12] Gábor Czédli: Slim patch lattices as absolute retracts and maximal lattices. **Submitted** to Algebra Universalis, *https://tinyurl.com/czedli-patchretract*, (arXiv).

A slim patch lattice is an SPS lattice, see [4], with two doubly irreducible coatoms the meet of which is 0. They were introduced by G. Czédli and E. T. Schmidt in 2013 as the building stones for SPS lattices with respect to gluing. Let K be the category of at least 3-element SPS lattices with length-preserving lattice embeddings forming the class Mor(K) of morphisms. We prove that the slim patch lattices are exactly (a) the absolute retracts for K, see [7], and (b) the maximal objects of K. If we change Mor(K) to the class of {0, 1}-preserving lattice homomorphisms, then the absolute retracts are the at most 4-element boolean lattices.

[13] Gábor Czédli: *Revisiting Faigle geometries from a perspective of semimodular lattices*. **Submitted** to Discussiones Mathematicae –General Algebra and Application. *https://tinyurl.com/czedli-rev-faigle*, (extended arXiv version).

In 1980, U. Faigle introduced a sort of finite geometries on posets that are in a canonical bijective correspondence with finite semimodular lattices. His result has almost been forgotten in lattice theory. Here we simplify the axiomatization of these geometries, which we call Faigle geometries. To exemplify their usefulness, we give a short proof of a theorem of Grätzer and E. Knapp (2009) asserting that each slim semimodular lattice L has a congruence-preserving extension to a slim rectangular lattice of the same length as L. As another application of Faigle geometries, we give a short proof of G. Grätzer and E. W. Kiss' result from 1986 (also proved by M. Wild in 1993 and the present author and E. T. Schmidt in 2010) that each finite semimodular lattice L has a length-preserving extension to a geometric lattice.

[14] Gábor Czédli: *Length-preserving extensions of a semimodular lattice by lowering a join-irreducible element*. **Submitted** to Order; *https://tinyurl.com/czedli-ext-low-j*, (extended arXiv version).

By passing from "finite semimodular" to "finite length semimodular", we extend the canonical bijective correspondence mentioned in [13] to more general geometries. Using this correspondence, we prove that if e is a join-irreducible element of a semimodular lattice L of finite length and h<e in L such that e does not cover h, then e can be "lowered" to a covering of h by taking a length-preserving semimodular extension K of L but not changing the rest of join-irreducible elements. With the help of our "lowering construction", we prove a general theorem on length-preserving semimodular extensions of semimodular lattices of finite lengths. The results of Grätzer and Kiss, Wild, and the author and Schmidt mentioned in [13] are corollaries. Our method offers shorter proofs than those in 1986, 1993, and 2010.

[15] Gábor Czédli: *Infinitely many new properties of the congruence lattices of slim semimodular lattices*. **Submitted** to Acta Sci. Math. (Szeged); *https://tinyurl.com/czedli-cde-con-sps*, (different earlier arXiv version).

In addition to the eight previously known properties of the congruence lattices of SPS lattices, see [4,5,6], we prove infinitely many more. The approach is based on lamps introduced in [4].

[16] Gábor Czédli: *Quotient diagrams of slim rectangular semimodular lattices and some related questions.* To be **submitted** to Acta Sci. Math. (Szeged), *https://tinyurl.com/czedli-qdiagr-sr* , (arXiv).

For a (Hasse) diagram F of a finite lattice L and a congruence α of L, we define the "quotient diagram" F/α by taking the maximal elements of the α-blocks and preserving the geometric positions of these elements. While F/α is not even a Hasse diagram in general, we prove that whenever L is an slim rectangular lattice, see [4], and F is a C_1-diagram of L, mentioned in [4], then F/α is a C_1-diagram of the slim rectangular lattice L/α. The class of lattices isomorphic to the congruence lattices of SPS lattices is closed under taking filters. We prove that this class is closed under two more constructions, which are inverses of taking filters in some sense; one of the two respective proofs relies on an inverse of the quotient diagram construction.

3. Compliance with the original research plan and possible exploitation

Here we repeat Part (c) of Section 1 in italic so that after each topic in it, we insert the labels of the relevant publications, if any, in parentheses.

The research focuses on semimodular lattices (see [4], [5], [6], [7], [11], [12], [13], [14], [15], [16]), *their congruence lattices* (see [4], [5], [6], [15], [16]), *planar lattices* (see [4], [5], [6], [7], [11], [12], [15], [16]; indeed, slim lattices are planar), *convex geometry* ([13] and [14] are somewhat related if we disregard convexity), *lattices generated by few elements* (see [1], [2], [3], [9]), *rotational lattices, principal congruences of lattices, lattices of compatible quasiorders and other relations of algebras* (see [1], [2], [3]; indeed, sets are trivial algebras where every relation is compatible and partitions are canonically the same as equivalence relations), *and also on any related problem and topic that might naturally arise but not listed here* (see [8], [10]).

In connection with Part (a) of Section 1, note that some of the 16 papers contain results, methods and (usually implicitly) problems that could be used PhD training in the future. This exploitation of the project has partly been realized since [1] and [2] are joint work with Tempus-supported former PhD students in Szeged; both of them put parts of the joint work into their theses.

In the future, the authentication protocol outlined in [3] could be inspected from cryptanalysts' point of view and implemented.