TRYING TO FIND THE GOLDEN THREAD IN MY RESEARCH FROM 1987 TO 2011

Marcel Wild
10 October

Trying to find the golden thread in my research from 1987 to 2011

Inaugural lecture delivered on 10 October 2011

Prof M Wild
Department of Mathematical Sciences
Faculty of Science

Editor: SU Language Centre
Printing: rsamprinters@gmail.com

ISBN: 978-0-7972-1344-9

ABOUT THE AUTHOR

Marcel Maria Wolfgang Wild was born on 17 July 1958 in Bern (Switzerland). After matriculating from the Gymnasium Rämibühl in Zürich in 1977 he studied Mathematics, Computer Science and (to a lesser degree) Philosophy at the University of Zürich. In 1982 he completed (with highest grade) his Master's thesis "Algorithmische Aspekte bei quadratischen Formen über $\mathbb{Q}$" under the direction of Volker Strassen (The same Strassen who made his name by multiplying matrices faster than Gauss). From 1983 to 1987 he was employed as "Assistent" at the University of Zürich and completed his PhD thesis during this period. This thesis, directed by Herbert Gross, received the Distinction of the University of Zürich. The next ten years saw various grants and teaching appointments, twice in Darmstadt, twice at MIT (as guest of the late Gian-Carlo Rota) and once in Zürich. In 1997 Marcel was appointed as Senior Lecturer at Stellenbosch University, and promoted to Associate Professor in 2001. He received the Rector's Award for Excellent Research in 2000, is listed in the Marquis Who's Who in the World, and obtained the South African Mathematical Society Award for Research Distinction 2010. Marcel is married to Marieke since 1998 and they have two sons, Wolfgang and Andreas.

Trying to find the golden thread in my research from 1987 to 2011

Marcel Wild

1 Introduction

This booklet will highlight some[1] of the mathematics I did after (and during) my PhD that was awarded in 1987. The chosen topics nevertheless constitute a sizeable "transversal" (to use mathematical parlance) of the five fields I worked in:

- Quadratic spaces of uncountable dimension
- Lattices (e.g. modularity, embeddability issues, universal algebra)
- Combinatorial geometries (e.g. binary codes) and convex geometries
- Nonlinear Signal Processing (idempotency and other properties of nonlinear filters)
- MATHEMATICA algorithms (concerning Boolean logic, nonlinear filters, lattices)

This ordering is the temporal one; while it reflects the *first* research contacts with the respective fields, I keep on jumping from one field to another, except for quadratic forms which I have quit. For reasons of coherence it is better, however, not to cut the cake historically. Rather we give center stage to lattices since they, to various extent, show up in all fields (if ever so feebly as in Section 3 and 4.3):

2 Lattices in general: Some specific prerequisites
3 Discrete closure operators
4 Distributivity
5 Modularity
6 The asymptotic number of non-equivalent binary codes

This essay tries to achieve several partly conflicting goals. Firstly, it addresses *mathematicians* rather then the "educated laymen". (The accompanying Inaugural Address is more laid back, however).

Secondly, for mathematicians *not* familiar with lattices, *some* parts (usually at the beginning of sections) hopefully provide a kind of tutorial to lattice theory. In fact, I frequently add snippets like "why?", "how?", "verify", most of which are easily handled. Additionally three known theorems are given with detailed proofs. The proofs are brief and pleasant, and the last one is novel as well.

Thirdly, for readers[2] more knowledgeable in a particular field (as said, some are scarcely related to lattices) I added a record 45 footnotes. In this way I tried to deliver both a readable and a fairly comprehensive account of my research in the past $24+4$ years (including my PhD studies 1983-1987 dealt with in 5.8). Not all footnotes are dry mathematics. A few (notably numbers 3, 14, 15, 17, 42, 43, 44) incorporate personal little experiences or opinions.

[1] For my complete publication list please visit my home page http://math.sun.ac.za/∼mwild/

[2] That includes the author who took this manuscript as an opportunity for taking stock of fading memories.

These days most mathematicians focus on a narrow field and collaborate with many co-authors. Not implying any value judgement, I don't fit that pattern. Thus I enjoy learning about new fields and mainly write single-authored articles, some of which settled problems that eluded the "experts" in the respective fields ([W10], [AW], [W8]). As I see it, exactly *because*[3] tools from seemingly unrelated areas were brought to bear.

2 Lattices in general: Some specific prerequisites

Recall that a *lattice* $L = (L, \leq)$ is a partially ordered set (poset) in which any two elements a and b possess a smallest common upper bound (called the *join* $a \vee b$), and dually a largest common lower bound (called the *meet* $a \wedge b$).

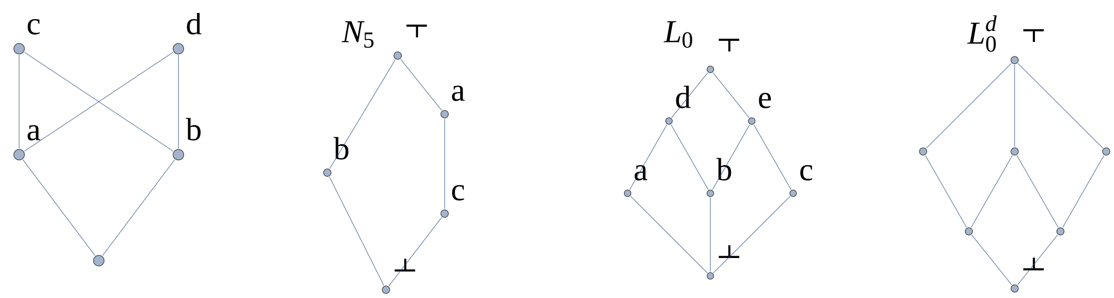

Fig. 1

For instance the first poset in Figure 1 is no lattice because the elements c, d have no common upper bound. Just as bad, a and b have *no smallest* common upper bound (c and d are both minimal common upper bounds but none is smaller than the other). However, the other three posets in Figure 1 are lattices. The lattice N_5 will show up again and again. Ditto the powerset $\mathcal{P}(S)$ of any set S, which is a lattice (why?) with operations $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. It makes an amusing exercise to show that $(a_1 \vee a_2) \vee a_3 = a_1 \vee (a_2 \vee a_3)$ in every lattice. As a consequence multi-joins $a_1 \vee a_2 \vee \cdots \vee a_n$ are independent of the bracketing defined, and so are meets. For any integer $n \geq 1$ we put $[n] := \{1, 2, \cdots, n\}$, and "iff" means "if and only if".

2.1 Join irreducibles and meet irreducibles

The author is particularly interested in *finite* lattices L and often this restriction will be made, even if things could be adapted to the infinite case. Finite lattices possess a smallest element

[3]The South African National Research Foundation (NRF) sees things differently and once commended that I focus on a single field and attend more conferences. Suggestions of how to improve the NRF-rating system can be found on my home page.

$\bot$ and a largest element $\top$. Also the following concepts can be more smoothly defined. Two elements $x, y \in L$ form a *covering* pair, written $x \prec y$, if $x < y$ and there is no z with $x < z < y$. An element $p \in L \setminus \{0\}$ is *join irreducible* if it is not the join of strictly smaller elements. An element a is an *atom* or *co-atom* if $\bot \prec a$ respectively $a \prec \top$. Obviously all atoms are join irreducible and all co-atoms meet irreducible. Each $a \in L$ is a join of join-irreducible elements $p_i \leq a$:

Either $a = p$ is join-irreducible itself or $a = b \vee c$ with $b, c < a$. By induction (why?) say $b = p_1 \vee p_2$ and $c = p_3 \vee p_4 \vee p_5$. This yields $a = p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5$.

Dually an element distinct from $\top$ is called *meet irreducible* if it is not the meet of strictly larger elements. We denote by $J(L)$ and $M(L)$ the sets of join respectively meet irreducibles and

$$j(L) := |J(L)| \quad \text{and} \quad m(L) := |M(L)|.$$

For instance $J(L_0) = \{a, b, c\}$ and $M(L_0) = \{a, c, d, e\}$. A *join representation* $x = p_1 \vee p_2 \vee \cdots \vee p_n$ (all $p_i \in J(L)$) is *irredundant* if $x \neq p_1 \vee \cdots \vee p_{i-1} \vee p_{i+1} \vee \cdots \vee p_n$ for all $i \in [n]$. Mutatis mutandis for meet irreducibles. For instance, $a \wedge c \wedge d = \bot$ is a redundant meet representation of $\bot \in L_0$ since also $a \wedge c = \bot$. Irredundant meet (or join) representations need not be unique: $a \wedge e = \bot$ and $d \wedge c = \bot$. Note that all *join* representations of all elements in L_0 are unique (see also 4.5.1).

Finally, a few loose ends. A subset L' of a lattice L is a *sublattice* if $a \vee b$ and $a \wedge b$ belong to L' for all $a, b \in L'$. In this case L' is a lattice in its own right (why?). For $a, b \in L$ with $a \leq b$ the *interval* $[a, b]$ is defined as $\{x \in L : a \leq x \leq b\}$. It is a sublattice of L. The *direct product* $L_1 \times L_2$ of lattices becomes a lattice under component-wise operations. A brief word on duality is in order. The following sloppy definition will do: The *dual* lattice L^d of a lattice L is obtained by turning the diagram of L on its head, see L_0 and L_0^d in Figure 1. Thus $\wedge$ and $\vee$ switch which entails $J(L^d) = M(L)$ and $M(L^d) = J(L)$. As we shall see, some properties of L are inherited by L^d, others not.

2.2 Finite length lattices and Jordan-Dedekind lattices

A subset X of mutually comparable elements is called a *chain*. A lattice L has *finite length* ($f\ell$) if

$$d(L) \quad := \quad \sup\{|X| : X \subseteq L \text{ is chain}\} \quad < \quad \infty$$

Note that $d(N_5) = 3$ even though N_5 possesses maximal $\bot, \top$-chains of different lengths: $\bot \prec b \prec \top$ and $\bot \prec c \prec a \prec \top$. If say $L =$ Sub$(\mathbb{R}^{41})$ is the lattice of all subspaces of the vector space $\mathbb{R}^{41}$ then $d(L) = 41$ albeit $j(L) = m(L) = \infty$.

Theorem 1: In every $f\ell$-lattice L one has $d(L) \leq j(L)$ and $d(L) \leq m(L)$.

Proof. We only show $d(L) \leq j(L)$, the other claim is proven similarly. Putting $n = d(L)$ let $\bot = a_0 \prec a_1 \prec a_2 \prec \cdots \prec a_n = \top$ be any longest covering $\bot, \top$-chain. Let S_i be the set of all $p \in J(L)$ with $p \leq a_i$ but $p \not\leq a_{i-1}$ $(1 \leq i \leq n)$. It is clear that $d(L) \leq j(L)$ ensues if we can show the following:

(1) Each set S_i is non-empty

(2) $J(L)$ is the disjoint union of $S_1, \ldots, S_n$

As to (1), if each join irreducible $p \leq a_i$ was in fact $\leq a_{i-1}$, then a_i could not be a join of join-irreducibles, contrary to the remark above. Hence $S_i \neq \emptyset$. As to (2), why is $S_i \cap S_j = \emptyset$ for $i \neq j$? Without loss of generality $i < j$, and so $a_i \leq a_{j-1} < a_j$. Now $p \in S_j \Rightarrow p \not\leq a_{j-1} \Rightarrow p \not\leq a_i \Rightarrow p \notin S_i$. To see that $J(L)$ is the union of the sets S_i, fix any $p \in J(L)$. Since $p \leq a_n$ but $p \not\leq a_0$, there must be an index i with $p \leq a_i$ but $p \not\leq a_{i-1}$, and so $p \in S_i$. $\square$

Remark: For later use we record that (1) and (2) remain true when n is the length of *any* covering $\bot, \top$-chain (for instance, both $n = 2$ and $n = 3$ are possible for N_5).

It is convenient to put

$$j(a) := |J(a)| \quad \text{and} \quad m(a) := |M(a)|.$$

Any $f\ell$-lattice L in which all covering $\bot, \top$-chains have the *same* length (necessarily $d(L)$) is said to be a *Jordan-Dedekind* (J.D.) lattice. It then follows (why?) that for each $a \in L$ all covering $\bot, a$-chains also have the same length (denoted by $d(a)$), and that all covering $a, \top$-chains have length $d(L) - d(a)$. What's more, as in the proof of Theorem 1, one argues that

(3) L is J.D. $\Rightarrow$ $d(a) \leq j(a)$ and[4] dually $d(L) - d(a) \leq m(a)$ for all $a \in L$.

2.3 A zoo of functions

Let L and L' be any lattices. A map $f : L \to L'$ is a *homomorphism* if $f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$ for all $a, b \in L$. A bijective homomorphism is an *isomorphism*. We say L is *isomorphic* to L' and write $L \simeq L'$ if there is an isomorphism between them. Unfortunately (or interestingly) a zoo of similar maps accumulates. For starters, $f : L \to L'$ is *monotone* if $a \leq b \Rightarrow f(a) \leq f(b)$ for all $a, b \in L$. In this case one has (why?) that

$$f(a \wedge b) \leq f(a) \wedge f(b) \quad \text{and} \quad f(a) \vee f(b) \leq f(a \vee b)$$

An *order embedding* is a function $f : L \to L'$ such that $a \leq b \Leftrightarrow f(a) \leq f(b)$ for all $a, b \in L$. Each order embedding is necessarily injective (why?). We mention that any *bijective* order embedding $f : L \to L'$ must be an isomorphism. An order embedding $f : L \to L'$ is a *meet-embedding* if $f(a \wedge b) = f(a) \wedge f(b)$ for all $a, b \in L$. Dually *join-embeddings* are defined. An *embedding* is one which is simultaneously a meet and join-embedding. Thus embedding means the same as injective homomorphism.

The following shows that *each* finite lattice L admits a meet-embedding (alternatively join-embedding) into a powerset lattice $\mathcal{P}(S)$. For all $a \in L$ put

$$\begin{aligned} J(a) &:= \{p \in J(L) : \ p \leq a\} \\ M(a) &:= \{q \in M(L) : \ q \geq a\} \end{aligned}$$

[4] Even in a lattice L which is *not* Jordan-Dedekind one can define $d(a)$ as the length of a *longest* covering $\bot, a$-chain. Clearly $d(a) \leq j(a)$ persists. However, $d(L) - d(a) \leq m(a)$ may *fail*; say $d(N_5) - d(b) = 3 - 1 \not\leq 1 = m(b)$. How could that happen?

Since $a \le b \Leftrightarrow J(a) \subseteq J(b)$ (why?), we see that $a \mapsto J(a)$ yields an order embedding $L \to \mathcal{P}(S)$ where $S := J(L)$. It is even a meet-embedding since $J(b \wedge c) = J(b) \cap J(c)$ for all $b, c \in L$ (why?). In general this is no join-embedding since merely $J(b \vee c) \supseteq J(b) \cup J(c)$; see e.g. N_5 in Figure 1. Similarly, putting $S := M(L)$ the rule $a \mapsto S \setminus M(a)$ yields a join-embedding $L \to \mathcal{P}(S)$ (why?) but no meet-embedding.

Various kinds of (order) embeddings will be studied in 4.1, 4.5, 5.4 and 5.5.

2.3.1 From maps $L \to L'$ let's turn to maps $L \to \mathbb{N}$. Namely, a monotone map $r: L \to \mathbb{N}$ is *submodular* if

$$(4) \qquad r(a \vee b) + r(a \wedge b) \quad \le \quad r(a) + r(b)$$

for all $a, b \in L$. Switching $\le$ to $\ge$ or $=$ defines *supermodular* respectively *modular* functions. For later use we record that for any finite lattice L the function $j(a)$ is supermodular:

$$(5) \qquad \begin{aligned} j(a) + j(b) - j(a \wedge b) \quad &= \quad |J(a)| + |J(b)| - |J(a) \cap J(b)| \\ &= \quad |J(a) \cup J(b)| \quad \le \quad |J(a \vee b)| \quad = \quad j(a \vee b) \end{aligned}$$

Similarly $m(a)$ is supermodular:

$$(5') \qquad \begin{aligned} m(a) + m(b) - m(a \vee b) \quad &= \quad |M(a)| + |M(b)| - |M(a) \cap M(b)| \\ &= \quad |M(a) \cup M(b)| \quad \le \quad |M(a \wedge b)| \quad = \quad m(a \wedge b) \end{aligned}$$

If we rewrite submodularity as $r(a) - r(a \wedge b) \ge r(a \vee b) - r(b)$ it becomes evident that it entails $r(a) = r(a \wedge b) \Rightarrow r(a \vee b) = r(b)$. The latter is called *weak submodularity* in [W14], and in turn entails the (long known) concept of *local submodularity*:

$$(a \wedge b \prec a \quad \text{and} \quad a \wedge b \prec b \quad \text{and} \quad r(a \wedge b) = r(a) = r(b)) \quad \Rightarrow \quad r(a \wedge b) = r(a \vee b)$$

3 Discrete closure operators

What is coming up could be adapted in obvious ways to arbitrary lattices L but we stick to the most important case $L = \mathcal{P}(E)$. Thus a map $cl : \mathcal{P}(E) \to \mathcal{P}(E)$, or briefly (E, cl), is a *closure operator* if for all $X, Y \in \mathcal{P}(E)$ the following holds:

$(C01)$ $X \subseteq cl(X)$ (extensivity)

$(C02)$ $X \subseteq Y \Rightarrow cl(X) \subseteq cl(Y)$ (monotonicity)

$(C03)$ $cl(cl(X)) = cl(X)$ (idempotence)

One calls $cl(X)$ the *closure* of X. Closure operators are prominent all over mathematics. In particular, they are connected to lattices as follows. Let

$$\mathcal{L}(E, cl) \quad := \quad \{X \in \mathcal{P}(E) : cl(X) = X\}$$

be the set of all subsets $X \subseteq E$ that happen to be *closed* in the sense that they coincide with their closure $cl(X)$. Trivially the set system $\mathcal{L}(E, cl)$ is a poset with respect to the inclusion relation $\subseteq$ of sets. Less trivial:

Theorem 2: The poset $\mathcal{L}(E, cl)$ is a lattice.

Proof. We claim that $X \vee Y = cl(X \cup Y)$ and $X \wedge Y = X \cap Y$ for all $X, Y \in \mathcal{L}(E, cl)$. As to the former, by (C03) the set $cl(X \cup Y)$ is indeed a member of $\mathcal{L}(E, cl)$. By (C01) we have $X, Y \subseteq X \cup Y \subseteq cl(X \cup Y)$, and so $cl(X \cup Y)$ is a common upper bound of X and Y. To see that it is the *smallest* common upper bound, we show that $cl(X \cup Y) \subseteq Z$ for every other common upper bound $Z \in \mathcal{L}(E, cl)$ of X and Y. Indeed, from $X, Y \subseteq Z$ follows $X \cup Y \subseteq Z$, which by (C02) yields $cl(X \cup Y) \subseteq cl(Z)$. But $cl(Z) = Z$ since $Z \in \mathcal{L}(E, cl)$, and so $cl(X \cup Y) \subseteq Z$ as desired.

As to showing $X \wedge Y = X \cap Y$, any common lower bound $Z \in \mathcal{L}(E, cl)$ of X and Y satisfies $Z \subseteq X \cap Y$ (why?). If we can show that $X \cap Y \in \mathcal{L}(E, cl)$, then $X \cap Y$ is a legal common lower bound itself, and so $X \wedge Y = X \cap Y$. Indeed, $cl(X \cap Y) \subseteq cl(X) = X$ by $(C02)$ and $(C03)$. Similarly $cl(X \cap Y) \subseteq Y$, and so $cl(X \cap Y) \subseteq X \cap Y$. On the other hand $X \cap Y \subseteq cl(X \cap Y)$ by $(C01)$. $\square$

Notwithstanding Theorem 2 one often studies closure operators cl with little reference to the associated lattice $\mathcal{L}(E, cl)$; that's also the case in much of the remainder of section 3.

Closure operators originated in topology, where the underlying topological space E is usually infinite. Topological closure operators are characterized by the additional axiom $(C04)$ below; an example is σ_1 in 5.8. The last fifty years saw *discrete* closure operators, i.e. on finite sets E, spread throughout mathematics; be it (3.1) with an extra *exchange axiom* $(C05)$, be it (3.2) with an *anti-exchange axiom* $(C06)$, or be it without additional axiom (3.3).

$(C04)$ $\quad cl\left(\bigcup_{i \in I} X_i\right) = \bigcup_{i \in I} cl(X_i)$

$(C05)$ $\quad$ From $a \in cl(X \cup \{b\})$ and $a \notin cl(X)$ follows $b \in cl(X \cup \{a\})$

$(C06)$ $\quad$ From $a \in cl(X \cup \{b\})$ and $a \notin cl(X)$ follows $b \notin cl(X \cup \{a\})$

For any closure operator (E, cl) one verifies that $\mathcal{C} = \mathcal{L}(E, cl)$ not just satisfies[5] $X \wedge Y = X \cap Y \in \mathcal{C}$ but even

$$\bigcap_{i \in I} X_i \in \mathcal{C} \quad \text{for all (potentially infinite) families} \quad \{X_i : i \in I\} \subseteq \mathcal{C}$$

Conversely any such *closure system* $\mathcal{C} \subseteq \mathcal{P}(E)$ (i.e. satisfying the above) is coupled to the closure operator (E, cl) that assigns to X the superset

$$cl(X) \quad := \quad \bigcap\{Y \in \mathcal{C} : \; Y \supseteq X\}.$$

[5]Showing, in effect, that $\mathcal{L}(E, cl) \to \mathcal{P}(E) : X \mapsto X$ is a meet embedding.

These correspondencies between closure operators and closure systems are mutually inverse in the obvious sense.

For two closure operators (E_1, cl_1) and (E_2, cl_2) it is natural to consider maps $f : E_1 \to E_2$ such that for all $X \subseteq E_1$ one has

$$(6) \qquad f(cl_1(X)) \quad = \quad cl_2(f(X)).$$

Assuming (6), are there properties of $\mathcal{L}(E_1, cl_1)$ that carry over to $\mathcal{L}(E_2, cl_2)$? Yes, if additionally f is onto (no surprise), and some other more technical condition holds (see footnote 28). Maps f with (6) improve upon *continuous* maps which are defined by switching $=$ to $\subseteq$ in (6).

Observe that *every* lattice L is isomorphic to one of type $\mathcal{L}(E, cl)$ but neither E nor cl is uniquely determined. Let us illustrate one particular instance. If L has finite length and $E = J(L)$ then $cl_J(X) := J(\bigvee X)$ yields a closure operator. The associated closure system is $\mathcal{C} = \{J(a)|\ a \in L\}$; indeed in view of 2.3 one has $J(a) \cap J(b) \in \mathcal{C}$ (why?). Observe that $cl_J(\{p\}) = \{p\}$ for all $p \in E$ iff L is *atomistic* in the sense that $J(L) = \{p \in L : \bot \prec p\}$. Singletons being closed is a natural postulate for any closure operator that aspires to be "geometric" in the widest sense. It is satisfied[6] for the closure operators in 3.1 and 3.2.

3.1 Combinatorial geometries

A finite closure space (E, cl) that satisfies $(CO5)$ is called a *combinatorial geometry* (or *matroid*). These structures arise frequently in combinatorics. For instance, the edge set of a graph or the transversals of a set system lead to matroids in natural ways. Also each vector space V over any field F spawns matroids: Take any $E \subseteq V$, which needs not be a linear subspace, and define for any $X \subseteq E$ its closure by

$$cl(X) := \{y \in E : y \text{ is linearly dependent on } X\}.$$

This closure operator satisfies $(CO5)$, which in this linear algebra context (and in German) is called *Austauschsatz von Steinitz.* The closed sets $X \in \mathcal{L}(E, cl)$ are referred to as *flats*. A fascinating question is which kind of "abstract" matroids are in fact isomorphic to such F-*representable* matroids. In particular, when $F = GF(2) = \{0, 1\}$ is the two element field one speaks of *binary matroids.*

For any closure operator cl one calls a set Y *independent* if $y \notin cl(Y \setminus \{y\})$ for all $y \in Y$. One of the salient features of a matroid (E, cl) is that all maximal independent sets (called *bases*) have the same cardinality, which is called the *rank*[7] of (E, cl). Besides the many applications of matroids and the accompanying algorithms, there is a large body of theory [Ox], a lot of which

[6] Being pedantic we note that in 3.1 points need not be closed with respect to cl, but they are closed with respect to the "trimmed" closure operator cl_J (where $L := \mathcal{L}(E, cl)$).

[7] What's more, all maximal independent sets contained in a fixed subset $X \subseteq E$ also have the same cardinality $r(X)$. This function $r : \mathcal{P}(E) \to \mathcal{P}(E)$ is submodular and it is well known how r and cl determine each other in the case of matroids. A similar link for *arbitrary* closure operators $cl : L \to L$, based on the concept of weakly submodular functions (2.3), is established in [W14]. Other matroid related concepts I grappled with are base exchange properties, Rota's basis conjecture, supermatroids, greedoids, a new axiomatization of binary matroids, and the asymptotic number of binary matroids (the latter are cryptomorphic to binary codes and dealt with in section 6).

dedicated to *regular* matroids, which by definition are F-representable for *each* field F. Harald Fripertinger and I enumerate all regular matroids of cardinality at most 15 in [FW].

3.2 Convex geometries

Convex geometries (briefly c-geometries) are defined as closure operators (E, cl) that satisfy $(CO6)$. Observe that $(C06)$ parallels $(C05)$ except for "$b \notin$" instead of "$b \in$" at the end. There is a natural kind of *Euclidean* c-geometry that originates from points in the Euclidean plane $\mathbb{R}^2$. Namely, having fixed any finite set $E \subseteq \mathbb{R}^2$, define the closure of $X \subseteq E$ as

$$cl(X) := \{y \in E : y \text{ is in the convex hull of } X\}.$$

For instance, let $E = \{x_1, x_2, x_3, x_4, x_5, x_6, a, b\}$:

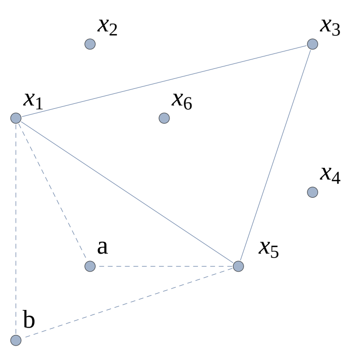

Fig. 2

Take e.g. $X = \{x_1, x_3, x_5\}$. The convex hull of X is the (infinite) triangle $D \subseteq \mathbb{R}^2$ spanned by the points x_1, x_3, x_5. However, we are only interested in the finitely many points of E that happen to be captured by D. Thus $cl(X) = \{x_1, x_3, x_5, x_6\}$. Similarly $cl(X \cup \{b\} = \{x_1, x_3, x_5, x_6, a, b\}$ and $cl(X \cup \{a\}) = \{x_1, x_3, x_5, x_6, a\}$. Notice that in accordance with $(C06)$ we have $b \notin cl(X \cup \{a\})$, and it is obvious that $(C06)$ holds for all Euclidean c-geometries.

As opposed to the F-representability problem for matroids, the representability problem for c-geometries (raised by Edelman-Jamison [EJ]) is about characterizing those c-geometries which are isomorphic to Euclidean c-geometries. Let us expand a bit more. A subset Z of any closure space (E, cl) is *minimal generating* if $cl(Z) = E$ but $cl(Z') \neq E$ for all $Z' \subsetneqq Z$. Most closure spaces (including matroids) possess many minimal generating sets, but c-geometries (E, cl) have only one, namely the set $Z = ex(E)$ of *extreme points.* For Euclidean c-geometries "extreme" means "outermost", for instance $ex(E) = \{x_1, x_2, x_3, x_4, x_5, b\}$ in our example. Returning to the representation problem, each c-geometry (E, cl) with $E = ex(E)$ is trivial in the sense that $cl(X) = X$ for all $X \subseteq E$. Here, any injective function $f : E \to \mathbb{R}^2$ for which $f(E)$ is the vertex set of a convex polygon, yields an Euclidean representation of (E, cl). The second easiest case $E = ex(E) \cup \{p\}$, thus with just *one* non-extreme point p, is already far more complicated. An inherent characterization of the Euclidean ones within this class of c-geometries was achieved by Edelman and Larman in 1990. In [AW] it is shown that the problem is NP-hard[8] in general. The matter is related to what is called *oriented* matroids.

3.3 Implicational bases

Here comes a playful way to construct closure operators. Consider a collection Σ of *implications*, i.e. expressions $A_i \to B_i$ whose *premise* A_i and *conclusion* B_i are just subsets of a fixed set E. For instance, let $E = [8]$ and let Σ consist of these four implications:

(a) $\{3, 5\} \to \{1\}$

(b) $\{1, 3, 7\} \to \{2\}$

(c) $\{2, 5\} \to \{3, 7\}$

(d) $\{4, 5, 6, 7\} \to \{1, 3, 8\}$

From Σ we get a closure operator $cl : X \mapsto X^\Sigma$ as follows. Consider say $X = \{2, 4, 5\}$. Because the premise $\{2, 5\}$ of the implication $\{2, 5\} \to \{3, 7\}$ from (c) happens to be contained in X we may add its conclusion $\{3, 7\}$ and arrive at $X' = \{2, 4, 5, 3, 7\}$. Now (a) applies and we get $X'' = \{2, 4, 5, 3, 7, 1\}$. No further inflating is possible: While the premise of (b) is contained in X'', this has no effect since its conclusion is in X'' already. As to (d), it does not apply since $\{4, 5, 6, 7\}$ is not fully contained in X''. Thus $cl(X) = X''$. Denote by $\mathcal{C}(\Sigma)$ the closure system coupled to cl.

Conversely, for each closure system $\mathcal{C} \subseteq \mathcal{P}(E)$ (coupled to the closure operator cl) there are many choices of Σ such that $\mathcal{C} = \mathcal{C}(\Sigma)$. In this case Σ is called an *(implicational) base* of $\mathcal{C}$. Obviously $\Sigma := \{A \to cl(A) : A \subseteq E\}$ does the job, but for $|E| < \infty$ one often strives for a base $\Sigma_{\min}$ of minimum cardinality (i.e. containing the least possible number of implications), or even for an *optimum* base Σ_{opt}, i.e. one of minimum size[9] $s(\Sigma_{\text{opt}})$. Given any base Σ one can calculate[10] a base $\Sigma_{\min}$ in time $O(|\Sigma|^2)$, but calculating Σ_{opt} is NP-hard. Nevertheless, for binary matroids (3.1), or closure operators (E, cl) with a modular lattice $\mathcal{L}(E, cl)$ (section 5) an optimum implicational base can be found in polynomial time; see [W5] and [W7].

I am currently researching related issues, some of which arising in 3.4 and 4.3, and one of which is this. Each closure system $\mathcal{C} \subseteq \mathcal{P}(E)$ is determined by the family $M(\mathcal{C}) \subseteq \mathcal{C}$ of its meet irreducibles X, i.e. satisfying $X \neq \cap\{Y \in \mathcal{C} : Y \supsetneqq X\}$. Given Σ, how to get $M(\mathcal{C}(\Sigma))$ directly (i.e. avoiding $\mathcal{C}(\Sigma)$)? Conversely, given $M(\mathcal{C})$ (not $\mathcal{C}$), how to get Σ with $\mathcal{C} = \mathcal{C}(\Sigma)$?

[8] More precisely, the following slight variant of the representaton problem is NP-hard: Given any c-geometry (E, cl) and any circular ordering of $ex(E)$, decide whether there is an Euclidean representation $f : E \to \mathbb{R}^2$ that preserves the circular ordering of $ex(E)$.

[9] The size of any family of implications $\Sigma = \{A_1 \to B_1, \cdots, A_n \to B_n\}$ is defined as $s(\Sigma) = \sum_{i=1}^{n}(|A_i| + |B_i|)$. It turns out (not obvious) that every optimum implicational base must be minimum.

[10] There is in fact a canonical "Duquenne-Guiges" implicational base Σ_{DG} which is minimum itself and such that every other $\Sigma_{\min}$ is closely connected to it. Part of [W5], consists in merging the Duquenne-Guiges approach with the relational database approach [M] which struggles to handle implications (called *functional dependencies* there) without any reference to the coupled closure systems.

3.4 Relational Databases and Frequent Set Mining

Relational databases constituted my first encounter with "applied" mathematics way back in 1988. Citing an example of Mannila and Räihä, suppose a book store has a database (= collection) of digital records with attributes AUTHOR, ADDRESS, BOOK and PUBLISHER. Suppose further that the functional dependencies $\{\text{AUTHOR}\} \to \{\text{ADDRESS}\}$ and $\{\text{AUTHOR}, \text{BOOK}\} \to \{\text{PUBLISHER}\}$ hold.[11] In this database the author's address is repeated for each book he/she has published. This is a waste of space since the functional dependency $\{\text{AUTHOR}\} \to \{\text{ADDRESS}\}$ tells that the address does not depend on the book. A better idea, which saves up to 25% space, is to use *two* smaller databases: One according to the scheme $\{\text{AUTHOR}, \text{ADDRESS}\}$, the other according to $\{\text{AUTHOR}, \text{BOOK}, \text{PUBLISHER}\}$. Handling this way databases with hundreds of attributes the space saving can be dramatic.

As to Frequent Set Mining, I only recently stumbled on it as a target for POE (4.3), but it arose already in 1993 from an analysis of customer behaviour in a supermarket. The aim was to investigate how often items were *purchased together*, and it led to the following abstract framework. Let W be a finite set of elements called "items" and let $T_i \subseteq W (i \in I)$ be a collection of subsets called "transactions". Fix an integer threshold $t \geq 1$ and call any subset $X \subseteq W$ *frequent* if it is a subset of at least t transactions. Formally, if

$$\text{supp}(X) := \{i \in I : \; X \subseteq T_i\}$$

then "frequent" means that $|\text{supp}(X)| \geq t$. Obviously the family SC of all frequent sets is a simplicial complex, i.e. from $X \in SC$ and $Y \subseteq X$ follows $Y \in SC$. Generating SC one by one cardinality-wise (starting with ϕ) is not feasible for SC large. Thus efforts eventually shifted towards generating only the maximal members (= facets) of SC or, more generally, its "closed" members $Y \in SC$ in the sense that

$$Y \subsetneqq Y' \;\Rightarrow\; \text{supp}(Y') \subsetneqq \text{supp}(Y).$$

These closed members do indeed form a closure system.

4 Distributivity

A lattice D is called *distributive* if the identity

(7) $\qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

holds for all elements $a, b, c \in D$. Note that any identity holding for all elements of a lattice, also holds in every sublattice (why?). Straightforward but important, any chain is a distributive lattice; the join $a \vee b$ is just $\max\{a, b\}$ and the meet $a \wedge b$ is $\min\{a, b\}$. The two element chain $D_2 = \{\bot, \top\}$ will be of interest in 4.2 and 5.2, and the infinite chain $\mathbb{R} = (\mathbb{R}, \leq)$ in 4.6. It is not hard to show that (7) is equivalent to the dual identity

(7′) $\qquad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

[11] By definition the second (say) dependency holds if any two records that feature the same AUTHOR and the same BOOK, do feature the same PUBLISHER. Thus AUTHOR and BOOK jointly *determine* the PUBLISHER. It could well be that $\{\text{AUTHOR}\} \to \{\text{BOOK}\}$ does *not* hold, namely if some author has written two books.

for all $a, b, c \in D$. In other words, with D also D^d is distributive. Note that if (7) only holds for "cherry-picked" elements a, b, c of a lattice, then (7′) need not hold for these. A case in point are $a, b, c \in L_0$ in Figure 1.

4.1 Combinatorial characterization of finite distributive lattices

Let D be of finite length and distributive. Recall from the proof of Theorem 1 that $J(D)$ is the disjoint union of $S_1, \cdots, S_n$ where $n := d(D)$. We aim to show that $j(D) = n$. This will follow from $j(D) \geq n$ (Theorem 1) if the presence of *distinct* elements p, q in S_i leads to a contradiction. We can assume that $q \not\leq p$ (since $q \leq p$ *and* $p \leq q$ implies $p = q$ which is false). Now $a_{i-1} \vee p = a_i$ (why?), which yields $q \wedge (a_{i-1} \vee p) = q$. By distributivity this can be rewritten as $(q \wedge a_{i-1}) \vee (q \wedge p) = q$. However, this is impossible since $q \wedge a_{i-1} < q$ (because of $q \not\leq a_{i-1}$) and $q \wedge p < q$ (because of $q \not\leq p$) and the join-irreducible q cannot be the join of two strictly smaller elements. We have thus shown that distributivity is *sufficient* for $d(D) = j(D)$. In particular D must be finite. What's more, in view of the **Remark** in 2.2, it follows that *all* covering $\perp, \top$-chains have length $n = j(D)$, and so D is Jordan-Dedekind.

Theorem 3: For each finite length lattice L the following are equivalent:

(a) L is distributive

(b) L is a Jordan-Dedekind lattice with $d(L) = j(L) = m(L)$

Proof.[12] We have just seen that (a) implies J.D. and $d(L) = j(L)$. By duality (see (7′)) also $d(L) = m(L)$. To show that conversely (b) implies (a), observe that $d(L) = j(L) = m(L)$ together with $j(a) \geq d(a)$ and $m(a) \geq d(L) - d(a)$ (see (3)) implies $j(a) = d(a)$ and $m(a) = d(L) - d(a)$ for all $a \in L$. By (5) and (5′) both $j(a)$ and $m(a)$ are supermodular functions in any finite lattice. For the latter that yields

$$d(L) - j(a \vee b) \quad + \quad d(L) - j(a \wedge b) \quad \geq \quad d(L) - j(a) \quad + \quad d(L) - j(b),$$

and so $j(a \vee b) + j(a \wedge b) \leq j(a) + j(b)$. But $\geq$ and $\leq$ is $=$, which forces $j : L \to \mathbb{N}$ to be modular. From (5) hence follows that $J(a) \vee J(b) = J(a \vee b)$ for all $a, b \in L$. This means that $a \mapsto J(a)$ in 2.3 is not just a meet-embedding but an embedding. With $\mathcal{P}(S)$ also the sublattice $f(L) \simeq L$ must be distributive. $\square$

The nondistributive lattice N_5 shows that J.D. cannot be dropped in (b). As seen, each finite distributive lattice embeds into a powerset lattice. It will follow from footnote 31 that *every* distributive lattice has this property. In 5.4 we shall up the game by embedding *modular* lattices: not into $\mathcal{P}(S)$ but $\mathrm{Sub}(V)$. Modular lattices can be defined as J.D. lattices L for which $d : L \to \mathbb{N}$ is a modular function.

[12] Theorem 3 is from [A] which features many other characterizations of distributivity and related properties. The given proof, however, seems to be new and was inspired by conversations with Ulrich Faigle. It circumvents the usual approach where distributive lattices are viewed as the lattices of all order ideals of posets $(P, \leq)$. By the way, encouraged by Rota and previous work of Faigle I embarked on "poset matroids" (= distributive supermatroids) $(P, \leq, cl)$ in [W14]. Their flat lattices are certain upper semimodular lattices which comprise as extreme cases all distributive lattices and all lattices CG in 5.1.

4.2 Boolean lattices and Boolean logic

For a lattice L with $\perp$ and $\top$ a *complement* of $a \in L$ is an element $\overline{a} \in L$ such that $a \vee \overline{a} = \top$ and $a \wedge \overline{a} = \perp$. For instance, the element $b \in N_5$ has the complements a and c. This cannot happen in a distributive lattice D since each $a \in D$ can have *at most one* complement. In order to prove it suppose both $\overline{a}$ and a' are complements of a. Then

$$a' \;=\; a' \wedge \top \;=\; a' \wedge (a \vee \overline{a}) \;=\; (a' \wedge a) \vee (a' \wedge \overline{a}) \;=\; \perp \vee (a' \wedge \overline{a}) \;=\; a' \wedge \overline{a}.$$

This shows that $a' \leq \overline{a}$. Similarly one sees that $\overline{a} \leq a'$, and so $a' = \overline{a}$.

A distributive lattice B in which each element b has a complement is called *Boolean*. In this case the complement is unique (as seen) and is denoted by $\overline{b}$. We leave it to the reader to show[13] the *laws of de Morgan* which state that $\overline{a \vee b} = \overline{a} \wedge \overline{b}$ and $\overline{a \wedge b} = \overline{a} \vee \overline{b}$ for all $a, b \in B$.

The prototypical example of a Boolean lattice is the powerset lattice $\mathcal{P}(W)$ of any set W. For each $A \in \mathcal{P}(W)$ its complement $\overline{A}$ is the usual set-theoretic complement $W \setminus A$. In fact, each *finite length* Boolean lattice is of this type, as we shall argue in 5.1. However, the origin of Boolean lattices is Boolean (or propositional) logic. In brief, let a, b, c be "propositions", i.e. statements which are either true ($\top$) of false ($\perp$) at any given moment. For instance,

a: It rains today
b: I own a Porsche
c: There are extra-terrestrials.

The statement (say) $a \vee b$ is defined to mean "It rains today *or* I own a Porsche". Similarly $a \wedge b$ is obtained by replacing "or" by "and". Finally $\overline{a}$ is the negation "It doesn't rain today". Using Boolean calculus one obtains that

$$a \vee (\overline{b \vee c}) = a \vee (\overline{b} \wedge \overline{c}) = (a \vee \overline{b}) \wedge (a \vee \overline{c}).$$

Spoken out in words the statement $a \vee (\overline{b \vee c})$ of course differs from $(a \vee \overline{b}) \wedge (a \vee \overline{c})$. The point is that they are either both true or both false, *independent* of what the truth values of a, b, c are and whether one knows them. For instance, if $f(\perp, \perp, \top)$ denotes the common truth value when $a = \perp, b = \perp, c = \top$, then $f(\perp, \perp, \top) = \perp$ (why?). This yields a function $f : \{\perp, \top\}^3 \to \{\perp, \top\}$ or equivalently $f : \mathcal{P}(\{a, b, c\}) \to \{\perp, \top\}$.

Conversely, for any finite set W a function of type $g : \mathcal{P}(W) \to \{\perp, \top\}$ is called a *Boolean function*. The *models* of g are the sets $Y \subseteq W$ with $g(Y) = \top$. Counting or generating models (all or specific ones) is useful way beyond propositional logic, and that leads us to 4.3.

4.3 The principle of exclusion

Although an estimated 60% of my research in the last six years has been devoted to the algorithmic side of Boolean logic, the account given here will be brief since things are too much in motion for a more concise assessment.

[13] To prove e.g. the second law, show that both $\overline{a \wedge b}$ and $\overline{a} \vee \overline{b}$ are complements of $a \wedge b$, and then invoke the uniqueness of complements.

Not only in data mining applications (3.4) is it useful to calculate $\mathcal{C}(\Sigma)$ from Σ fast and in a compact way. For instance, from the Cayley tables of any universal algebra A (5.2.3) one immediately gets an implicational base Σ of $\mathrm{Sub}(A)$ (how?), and thus $\mathrm{Sub}(A)$ could be calculated fast as $\mathcal{C}(\Sigma)$. Such a method has been presented in [W16]. Due to space limitations we do not say *how* it works, but rather *what* it delivers. If say Σ consists of the four implications at the beginning of 3.3, then $\mathcal{C}(\Sigma)$ can be compactly represented as a disjoint union $\mathcal{C}(\Sigma) = r_1 \cup r_2 \cup \cdots \cup r_7$ of these seven *multivalued rows*:

r_1	n	2	n	2	0	2	n	2
r_2	1	1	1	2	0	2	1	2
r_3	2	0	0	2	1	2	0	2
r_4	1	0	1	2	1	2	0	2
r_5	2	0	0	n	1	n	1	2
r_6	1	1	1	n	1	n	1	2
r_7	1	1	1	1	1	1	1	1

Table 1

Each r_i contains a bunch of $0,1$-vectors corresponding to subsets of $W = [8]$ in the usual way. The "don't care" symbol 2 indicates that a component is free to be 0 or 1. Slightly more subtle, the wildcard (no pun intended) $nn \cdots n$ means that *at least one* 0 must occur there, i.e. the only forbidden pattern is $11 \cdots 1$. Thus r_1 comprises $2^4 \cdot (2^3 - 1) = 102$ subsets of W, all of them Σ-closed. Due to the disjointness of rows one deduces

$$|\mathcal{C}(\Sigma)| \quad = \quad 102 + 8 + 16 + 8 + 12 + 6 + 1 \quad = \quad 153.$$

We can think of $\mathcal{C}(\Sigma)$ as the set of models of a certain Boolean function (a pure Horn function). Using other types of wildcards the model set $\mathrm{Mod}(f) := \{X \in \mathcal{P}(W) : f(X) = \top\}$ of other Boolean functions $f : \mathcal{P}(W) \to \{\bot, \top\}$ can be compactly represented.

I call this method the *principle of exclusion* (POE) because one starts with $\mathcal{P}(W)$ and iteratively *excludes* non-models until $\mathcal{P}(W)$ has shrunk to $\mathrm{Mod}(f)$. Apart from implications the POE has been applied to Hamiltonian cycles [W13], and several other projects: Anticliques[14] in graphs, generalizing the classic Coupons Collector Problem, counting k-element transversals, determining selection probabilites (4.6), and more are work in progress. As detailed in [W17] the POE competes with binary decision diagrams[15] (BDD). The final verdict of each method's pros and cons is not out yet, but it e.g. seems that the POE can handle better the enumeration of models of fixed cardinality k. For instance, it follows at once (why?) from Table 1 that

$$|\{X \in \mathcal{C}(\Sigma) : |X| = 4\}| \quad = \quad 28 + 1 + 4 + 3 + 5 + 0 + 0 \quad = \quad 41.$$

[14] As testified by colleagues, my "high level" Mathematica program based on POE beat the "hardwired" Mathematcia command `MaximumIndependentSet` by factors up to 100 000. My article was rejected by a junior editor at some "reputed" journal where "fancy but useless" counts more than "simple but efficient". It didn't help my mood that he's one of surprisingly many editors these days with few (if any!) single-authored articles early in their career, who indulge in swarm intelligence (google), and whose horizon is inversely proportional to the number of co-authors they cling on to. Das musste mal gesagt werden. See also footnote 17.

[15] Donald Knuth currently writes the first simultaneously comprehensive and readable account on BDD's as part of his forth-coming fourth volume of "The art of computer programming".

4.4 The Dedekind Problem

Let W be any set and let $A_1, \cdots, A_n \subseteq W$ be any subsets. Consider these three problems:

$\cap$-Problem: What is the number N_1 of distinct sets that arise by taking intersections of sets from $\{A_1, \cdots, A_n\}$ in all possible ways?

$(\cap, \cup)$-Problem: What is the corresponding number N_2 when intersections and unions are allowed?

$(\cap, \cup, -)$-Problem: What is the corresponding number N_3 when intersections, unions and complements are allowed?

As to the $\cap$-Problem, there actually are two variants that need to be distinguished. The first asks for the *maximum* achievable $N_1^{\max}$ and is easily answered: $N_1^{\max} = 2^n - 1$ (why?). The second is harder and asks for a good algorithm to calculate $N_1(A_1, \cdots, A_n) := |\mathcal{C}| - 1$, where $\mathcal{C} \subseteq \mathcal{P}(W)$ is the closure system generated by $\{A_1, \cdots, A_n\} \subseteq \mathcal{P}(W)$. That issue e.g. arises in data management (3.4).

Both variants of the $(\cap, \cup, -)$-Problem are easy. Suffice it to say that $N_3^{\max}(n) = 2^{(2^n)}$ and that $N_3(A_1, \ldots, A_n) = 2^m$ where the number m of atoms of the Boolean lattice generated by $A_1, \cdots, A_n \subseteq W$ is readily determined.

The $(\cap, \cup)$-problem (both variants) is by far the hardest of the three. We only discuss the $N_2^{\max}$-variant. Albeit $|W| = \infty$ is allowed, all $N_2^{\max}(n)$ are known to be finite but only these values[16] are known:

n	$N_2^{\max}(n)$
1	1
2	4
3	18
4	166
5	7579
6	7828352
7	2414682040996
8	56130437228687557907786

I have come to terms with my inability to ever solve a first-rate open problem such[17] as "$P = NP$?", but have managed a few second-rate problems and am cautiously optimistic about the *Dededind Problem* which asks for a sensible formula (explicite or recursive) for $N_2^{\max}(n)$, or at least the next value $N_2^{\max}(9)$. These hopes are based on some highly symmetric decomposition [WW] of $J(FD(n))$ (as to $FD(n)$, see 4.4.1) which in conjunction with POE and BDDs may do the trick.

[16] $N_2^{\max}(n)$ also equals the number of Boolean *monotone* functions $f : P([n]) \to \{\bot, \top\}$ in the sense that from $X \subseteq Y$ and $f(X) = \top$ follows $f(Y) = \top$. The asymptotic value of $N_2^{\max}(n)$ as $n \to \infty$ is known.

[17] Since everyone believes that $P \neq NP$, it seems more sensible to find good algorithms for the NP-hard problems (say provably $O(1.1^n)$ instead $O(2^n)$, or overwhelming experimental performance) rather than incrementally improving problems in P (say from $O(n^3)$ to $O(n^{2.5})$). I have experienced that this view is not dominant yet. See also footnote 14.

4.4.1 The n-generated free algebra $\mathcal{FV}(n)$ within a "variety" $\mathcal{V}$ of algebras will be defined (to sufficient extent) in 5.2.3. It turns out that $N_i^{\max}(n)$ $(i = 1, 2, 3)$ equals $|\mathcal{FV}(n)|$ where $\mathcal{V}$ is the variety of all semilattices, distributive lattices, and Boolean lattices respectively. As to the most intricate second case, the free n-generated distributive lattices is often denoted by $FD(n)$. Albeit its poset $J(FD(n))$ of join irreducibles is isomorphic to the seemingly harmless capped powerset $\mathcal{P}([n]) \setminus \{\phi, [n]\}$, the fine structure of $FD(n)$ remains elusive. Instead of n mutually incomparable free generators (an "antichain") one may generalize to a poset P of free generators and investigate the corresponding lattice $FD(P)$. Still $|FD(P)| < \infty$ if $|P| < \infty$. Yves Semegni devoted his PhD thesis to these matters, e.g. using POE and also calculating the cardinality of certain finite *modular* lattices $FM(P)$. See 5.2.3.

4.5 Cover preserving order embedding into Boolean lattices

An order embedding (2.3) $f : L \to L'$ is *cover preserving* (cp) if $x \prec y$ implies $f(x) \prec f(y)$ for all $x, y \in L$. For instance Figure 3 defines a cp order embedding $f : L_2 \to \mathcal{P}([5])$ where for the elements $a, b \in L_2$ with $f(a) = \{1, 4\}$ and $f(b) = \{2, 3, 4\}$ one has

$$f(a \wedge b) \subsetneqq f(a) \cap f(b), \quad f(a) \cup f(b) \subsetneqq f(a \vee b).$$

Thus f is neither a meet nor a join-embedding. Let **CPOE** be the class of lattices L that admit a cp order embedding $L \to \mathcal{P}(S)$ (S finite). By the proof of Theorem 3 all distributive lattices belong to **CPOE** but some non-distributive lattices like L_2 participate as well. Obviously each $L \in$ **CPOE** is J.D., yet this does not suffice as testified by M_3 (why?). In order to get a necessary and sufficient condition let $PQ(L)$ be the set of all *prime quotients* $a \prec b$ of L, formally

$$PQ(L) := \{(a, b) \in L \times L : a \prec b\},$$

and focus on a certain equivalence relation on $PQ(L)$ which we call *strong projectivity*[18] and denote by $\approx$. For instance the J.D. lattice L_1 in Figure 3 features five strong projectivity classes $\alpha, \beta, \gamma, \delta, \varepsilon$. Call $(a, b), (c, d) \in PQ(L)$ *comparable* if $b \leq c$ or $d \leq a$. It is not hard to see that $L \in$ **CPOE** forces distinct strongly projective prime quotient to be incomparable. Thus $L_1 \notin$ **CPOE** because of α.

Pushing things further define a graph $G(L)$ whose vertices are the strong projectivity classes and where vertices α, β are adjacent if and only if there are comparable $(a, b) \in \alpha$ and $(c, d) \in \beta$. Obviously mentioned incomparability condition amounts to $G(L)$ being loopless. In this case the chromatic number $ch(G(L))$ is well defined and one has $d(L) \leq ch(G(L))$. The following[19] is shown in [W3]:

(8) $\qquad L \in$ **CPOE** $\quad \Leftrightarrow \quad L$ is J.D. and $G(L)$ is loopless with $ch(G(L)) = d(L)$.

For instance, L_2 in Figure 3 is J.D. and $G(L_2)$ has vertices $\alpha, \beta, \gamma, \delta, \varepsilon, \pi, \sigma, \tau$ (ignore the labels 1,2,3,4,5) with say β, τ adjacent but π, τ non-adjacent. One checks (try) that $G(L_2)$ is loopless and has $ch(G(L_2)) = 5 = d(L_2)$. One possible proper colouring $c : G(L_2) \to [5]$ is indicated in Figure 3, e.g. $c(\beta) = 2$. One cp order embedding $f : L_2 \to \mathcal{P}([5])$ is obtained by letting $f(x)$

[18] For $(a, b), (c, d)$ in $PQ(L)$ say that (c, d) is an *upper transpose* of (a, b) if $a \leq c, b \leq d, b \not\leq c$. Dually (c, d) is a *lower transpose* of (a, b) if $c \leq a, d \leq b, d \not\leq a$. Writing $(a, b) \sim (c, d)$ if (c, d) is either a lower or upper transpose of (a, b), one defines $\approx$ as the transitive closure of the symmetric, reflexive relation $\sim$.

[19] In fact all of this holds when L is merely a *poset* which has a smallest ($\perp$) and a largest ($\top$) element.

be the set of colours occuring on prime quotients (a, b) with $b \leq x$; see Figure 3 where e.g. 234 means $\{2, 3, 4\}$.

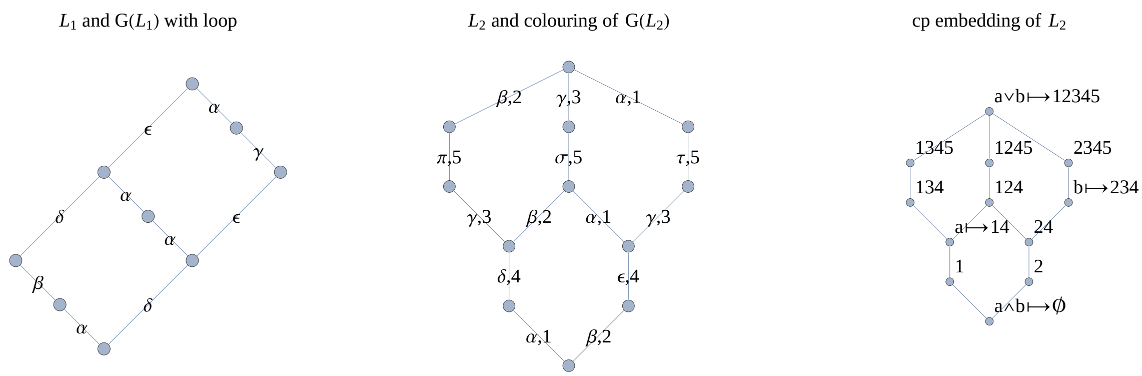

Fig. 3

Additionally certain *isometric* order embeddings $L \to \mathcal{P}(S)$ are considered in [W3] and a problem of Ivan Rival [W3, Thm.12] is settled. In 5.5 the key issue is also “cover preserving”, but in a tougher context that probably precludes a neat characterization like (8).

4.5.1 Four useful parameters

We keep L finite here. Apart from $j(L), m(L), d(L)$ let us add

$$g(L) := \text{ number of vertices of } G(L)$$

as a useful new parameter. Leaving $ch(G(L))$ aside, these four parameters are fit to characterize various types of lattices. We start with distributive lattices by noting that Theorem 3 can be extended as follows:

(9) $\quad L$ distributive $\Leftrightarrow$ L is J.D. and $g(L) = j(L) = m(L) = d(L)$

Suppose L is any lattice that admits a cp order embedding $L \to \mathcal{P}(S)$ that is also *meet preserving*. Then it follows at once (verify) that L has this property:

(10) $\quad$ For each $x \in L$ and any choice of lower covers $x_1, \ldots, x_n$ the interval $[x_1 \wedge \cdots \wedge x_n, x]$ is Boolean of length n.

For instance L_0 in Figure 1 satisfies (10) (with $n = 2$ throughout), and ditto all lattices $L = \mathcal{L}(E, cl)$ where (E, cl) is a convex geometry. For *Euclidean* c-geometries this is clear by looking at the extreme points in Figure 2! The lattices with (10) are called *locally lower distributive* and can be characterized in many equivalent ways. Let us state three more. First, they coincide with those J.D. lattices that have unique irredundant join representations (see 2.1). Second, one has:

(11) $\quad L$ is locally lower distributive $\quad \Leftrightarrow$ L is J.D. and $g(L) = j(L) = d(L)$

Third, recall from 2.3 that $a \mapsto J(a)$ always yields a meet embedding $f : L \to \mathcal{P}(J(L))$. If L is J.D. and $j(L) = d(L)$ as above then f is clearly cover preserving. In view of (10) $\Leftrightarrow$ (11) we deduce that the existence of a cp meet embedding is yet another characterization of locally lower distributivity. From (9) and (11) it is clear that locally lower distributive and its dual *locally upper distributive* are jointly equivalent to distributive.

A lattice L is *join semidistributive* ($SD_\vee$) if $a \vee b = a \vee c$ implies $a \vee b = a \vee (b \wedge c)$. One can show that

(12) $\quad L$ is join semidistributive $\quad \Leftrightarrow \quad g(L) = j(L)$.

Dually everything works for *meet semidistributive* lattice ($SD_\wedge$). For instance L_2 is meet but not join semidistributive. A lattice is *semidistributive* (SD) if it is both $SD_\wedge$ and $SD_\vee$. In view of Theorem 1 it is natural to define:

(13) $\quad L$ is join extremal $\quad :\Leftrightarrow \quad d(L) = j(L)$.

Meet extremal and extremal lattices are defined in the obvious way. Neither (SD) nor extremal implies J.D.. The smallest counter example is $g(N_5) = j(N_5) = m(N_5) = d(N_5)$.

4.6 Application to nonlinear signal processing

Linear filtering theory is a well established subject (see Wikipedia). However, it copes badly with signals infected with *impulsive*[20] noise. The median filter *Med* is a popular remedy. Given a discrete time series x (for convenience taken to be bi-infinite, i.e. $x \in \mathbb{R}^{\mathbb{Z}}$), the i-th component $(Medx)_i$ of the new (cleaned) series $Medx$ is determined as follows. For fixed $n \in \mathbb{N}$ the $2n+1$ components of the *window*

(14) $\quad W(x_i) \quad = \quad \{x_{i-n}, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{i+n}\}$

centered at x_i are ordered and the middle one is picked. Formally, if

$$x_{j_1} \leq x_{j_2} \leq \cdots \leq x_{j_{n+1}} \leq \cdots \leq x_{j_{2n}} \leq x_{j_{2n+1}}$$

and $\{x_{j_1}, \ldots, x_{j_{2n+1}}\} = W(x_i)$, then $(Medx)_i := x_{j_{n+1}}$. Just as for linear filters it is desirable that a nonlinear filter be idempotent. Unfortunately the median filter is not, i.e. $Med \circ Med \neq Med$, as can be seen from this example ($n = 3$):

$$\begin{aligned} x &= (\cdots, \quad 0,0,1,\mathbf{0},1,0,0, \quad \cdots) \\ Medx &= (\cdots, \quad 0,0,0,\mathbf{1},0,0,0, \quad \cdots) \\ Med(Medx) &= (\cdots, \quad 0,0,0,\mathbf{0},0,0,0, \quad \cdots) \end{aligned}$$

[20] To take an example of Carl Rohwer, who got me interested in NSP in 1998, consider the speed recording of a motor boat. Whenever, due to waves, the propeller is forced out of water at time i, the corresponding recording x_i will be an outlier that needs to be deleted.

Most nonlinear filters (including *Med*) are *stack filters* S, i.e. ultimately defined by some monotone (footnote 16) Boolean function. While sufficient conditions for S to be idempotent were known (phrased within the framework of Mathematical Morphology), a characterization of idempotency was lacking. As it turns out [W8], applying distributivity is the key. Namely, $(\mathbb{R}, \leq)$ is a chain and whence a distributive lattice with joins and meets given by $a \vee b = max\{a, b\}$ and $a \wedge b = \min\{a, b\}$. Let us sketch the basic idea on the stack filter $L : \mathbb{R}^{\mathbb{Z}} \to \mathbb{R}^{\mathbb{Z}}$ defined by

$$(15) \qquad (Lx)_i \quad = \quad (x_{i-1} \wedge x_i) \vee (x_i \wedge x_{i+1}) \quad (i \in \mathbb{Z})$$

Thus here the n in (14) is $n = 1$. Our L is idempotent because for all $x \in \mathbb{R}^{\mathbb{Z}}$ and $i \in \mathbb{Z}$ one has

$$\begin{aligned}
[(L \circ L)x]_i &= [L(Lx)]_i \\
&= ((Lx)_{i-1} \wedge (Lx)_i) \quad \vee \quad ((Lx)_i \wedge (Lx)_{i+1}) \\
&= (Lx)_i \ \wedge \ ((Lx)_{i-1} \vee (Lx)_{i+1}) \quad \text{(distributivity)} \\
&= (Lx)_i \ \wedge \ (((x_{i-2} \wedge x_{i-1}) \vee (x_{i-1} \wedge x_i)) \ \vee \ ((x_i \wedge x_{i+1}) \vee (x_{i+1} \wedge x_{i+2}))) \\
&= (Lx)_i \ \wedge \ ((Lx)_i \ \vee \ (x_{i-2} \wedge x_{i-1}) \ \vee \ (x_{i+1} \wedge x_{i+2})) \\
&= (Lx)_i
\end{aligned}$$

Suppose the compenents x_i $(i \in \mathbb{Z})$ are randomly distributed (independently and identically with respect to any kind of distribution). By (15) the ith component $(Lx)_i$ is a member of $W(x_i) = \{x_{i-1}, x_i, x_{i+1}\}$. Distinguishing $3! = 6$ cases one readily finds (try) that $(Lx)_i$ is the smallest, the middle, or the largest of $W(x_i)$ with probability $\frac{1}{3}, \frac{2}{3}, 0$ respectively. For stack filters S with larger windows that approach to find these telling *selection probabilities* is infeasible but some algorithm based on POE (4.3) works well [W18].

As a youngster, being fascinated by the idea to *multiply* two large numbers a and b by simply *adding* their logarithms,[21] I asked my teacher whether there is a similar way to replace addition by some easier operation. He outright denied, but some 30 years later I felt partly vindicated. Not that addition can be replaced, but in the same way that multiplication *distributes* over addition, addition distributes over the max-operation $\vee$. For instance

$$\begin{array}{lcccc}
10 + (12 \vee 15) & = & 10 + 15 & = & 25 \\
(10 + 12) \vee (10 + 15) & = & 22 \vee 25 & = & 25
\end{array}$$

This is not just being playful but serves to decide which stack filters S are *co*-idempotent in the sense that $(I - S) \circ (I - S) = (I - S)$. The proof in [W8] is improved upon in [RW, Thm.32].

The first part of [RW], written by Rohwer, focuses also on practical aspects of $LULU$-operators (= Carl's favorite stack filters) and amply motivates the desirability of idempotency and co-idempotency. The second part, written by me, surveys my (purely theoretical) efforts in nonlinear signal processing from 1998-2006; similar to how the present manuscript covers the whole of my research from 1987-2011. Here *a few* further bits from [RW]. Each stack filter $S : \mathbb{R}^{\mathbb{Z}} \to \mathbb{R}^{\mathbb{Z}}$

[21] Never minding the methods by which the logarithm table was calculated.

is monotone in the usual (2.3) sense that $x \leq y \Rightarrow Sx \leq Sy$. This is not to be confused with *neighbourly trend preservation* which postulates that $x_i \leq x_{i+1} \Rightarrow (Sx)_i \leq (Sx)_{i+1}$ and $x_i \geq x_{i+1} \Rightarrow (Sx)_i \geq (Sx)_{i+1}$. This property can be tested in polynomial time. Furthermore stack filters are pleasant from a semigroup point of view. For instance, our $L = L_1$ naturally generalizes to L_n and these in turn dualize to U_n. The semigroup $S(m,n)$ generated by $L_1, \ldots, L_m, U_1, \ldots, U_n$ has cardinality $\binom{m+n+2}{n+1} - 2$. It turns out that *all* members of $S(m,n)$ are idempotent. My inclination to semigroups was triggered by the co-author of [GW].

5 Modularity

Up and including 5.1 all lattices L are of finite length. Such L is *upper semimodular* if it satisfies the following condition for any two upper covers y, z of an element x:

$$(x \prec y \text{ and } x \prec z) \;\Rightarrow\; (y \prec y \vee z \text{ and } z \prec y \vee z).$$

One can show that

(16) $\quad L$ is upper semimodular $\Leftrightarrow$ L is J.D. and $d : L \to \mathbb{N}$ is submodular.

Dually L is *lower semimodular* if

$$(y \prec x \text{ and } z \prec x) \;\Rightarrow\; (y \wedge z \prec y \text{ and } y \wedge z \prec z).$$

For instance N_5 is neither upper nor lower semimodular. From (10) it's clear that (say) locally lower distributive implies lower semimodular. One calls L *modular* if it is both lower and upper semimodular. As a consequence, each distributive lattice is modular. Combining (16) and its dual yields:

(17) $\quad L$ is modular $\quad\Leftrightarrow\quad$ L is J.D. and $d : L \to \mathbb{N}$ is modular.

Since the lattice $\mathrm{Sub}(F^n)$ of all subspaces X of a vector space F^n is modular,[22] the right hand side of (17) generalizes the well known dimension formula from linear algebra : $\dim(X+Y) + \dim(X \cap Y) = \dim(X) + \dim(Y)$.

Let M_n be the unique length two lattice with $n \geq 3$ atoms. One checks that M_n is modular but not distributive. These lattices will come up[23] frequently.

Subsection 5.1 readies material about complemented modular lattices, 5.2 connects modularity to universal algebra, 5.3 is a variation of 4.1 in the modular case, 5.4 embeds modular lattices in $\mathrm{Sub}(F^n)$, 5.5 embeds them in $\mathrm{Part}(S)$. Subsections 5.6 to 5.8 being about cyclic modules, incidence algebras, and quadratic spaces respectively, are only loosely tied to modularity. Although

[22] That is most easily seen by using the following definition of modularity (which is equivalent to ours for $f\ell$-lattices): $a \leq c \;\Rightarrow\; (a \vee b) \wedge c = a \vee (b \wedge c)$. The same proof shows that $\mathrm{Sub}(H)$ is modular for every R-module H.

[23] Roughly speaking the M_n's are for modular lattices what D_2 is for distributive lattices. One can prove that L is modular iff it doesn't have N_5 as sublattice. In turn a modular lattice is distributive iff it doesn't have M_3 as sublattice. We shall also pay particular attention to M_4 and M_5.

some lattices in 5.7 and 5.8 are actually distributive, I put them in Section 5 instead of Section 4 because another overarching aspect of Section 5 is "subspace lattices" (with respect to vector spaces, modules, universal algebras).

5.1 Three nested classes of complemented lattices

We look at these growing classes of finite length complemented lattices, with emphasis on the middle class:

(a) complemented distributive lattices B
(b) complemented modular lattices PG
(c) complemented upper semimodular lattices CG

As to (a), let us apply induction on $n = d(B)$ to see that the type (a) lattices are exactly the Boolean lattices $(D_2)^n \simeq \mathcal{P}([n])$ from 4.2. The case $n = 1$ being trivial, fix any $a \in B \setminus \{\bot, \top\}$ and check that $x \mapsto (a \wedge x, \overline{a} \wedge x)$ yields an isomorphism $B \to [\bot, a] \times [\bot, \overline{a}]$. Since $[\bot, a]$ and $[\bot, \overline{a}]$ are both distributive and complemented (why?), induction yields $B \simeq (D_2)^k \times (D_2)^m \simeq (D_2)^n$.

As to we (c), it turns out that the lattices CG are up to isomorphism exactly the lattices $\mathcal{L}(E, cl)$ where (E, cl) is a combinatorial geometry (3.1). What is more, these lattices are exactly the atomistic upper semimodular lattices. In [W4, Thm.4] a short matroid-theoretic proof of a result of Dilworth is given: Every upper semi-modular L admits a *cover preserving* embedding into a suitable lattice CG (the *necessity* of L being upper semimodular is clear). Many people's favorite lattice CG (e.g. Rota's and mine) is the lattice $\mathrm{Part}(S)$ of all set partitions of a set S. If we identity set partitions with equivalence relations θ in the usual way then the partial ordering of $\mathrm{Part}(S)$ is this: $\theta \leq \theta'$ if and only if $a\theta b$ implies $a\theta' b$. See also 5.5.

An obvious class of type (b) lattices are the *coordinatizable* lattices $PG \simeq \mathrm{Sub}(F^n)$, i.e. subspace lattices of F-vector spaces. Albeit not[24] every PG is coordinatizable, by a result of Birkhoff the lattices PG nevertheless nicely coincide with the subspace lattices of what is called *projective geometries.* Of course, the latter are special types of combinatorial geometries (E, cl) and "subspace" just means "flat". In fact $cl = cl_J$ with $J = J(PG)$, see Section 3. A projective geometry (E, cl) is *nondegenerate* if its lattice $PG = \mathcal{L}(E, cl)$ is directly irreducible. For instance, each nondegenerate projective geometry with $d(PG) = 3$ is called *projective plane* and can be viewed as a set E of "points" and a set of at least 3-element "lines" $\ell \subseteq E$ such that these properties hold: Any two distinct points are simultaneously contained in exactly one line (as in familiar Euclidean geometry), and dually any two distinct lines intersect in exactly one point (thus no two lines are "parallel" in *contrast* to Euclidean geometry).

All of this relates to *2-distributive* lattices which are defined by the identity

$$(18) \qquad a \wedge (b \vee c \vee d) \;=\; (a \wedge (b \vee c)) \;\vee\; (a \wedge (b \vee d)) \;\vee\; (a \wedge (c \vee d)).$$

One readily checks (try?) that no lattice $PG = \mathrm{Sub}(F^3)$ satisfies (18), and so no (isomorphic copy of) $\mathrm{Sub}(F^3)$ can occur as sublattice in a 2-distributive lattice. Conversely and more subtle, each modular lattice L that violates (18) must contain some directly irreducible length three

[24] However, by a famous 1965 Theorem of Vehlen-Young PG is coordinatizable whenever $d(PG) \geq 4$.

PG as sublattice[25] (even as interval).

5.1.1 The fundamental theorem of projective geometry

Each vector space automorphism $f : F^m \to F^m$ yields (verify) a lattice automorphism ϕ : $\mathrm{Sub}(F^m) \to \mathrm{Sub}(F^m)$ if we set $\phi(X) := \{f(x) : x \in X\}$. Conversely, is *each* lattice automorphism ϕ on $\mathrm{Sub}(F^m)$ "linearly induced" by a suitable vector space automorphism f in the sense that $\phi(X) = \{f(x) : x \in X\}$ for all $X \in \mathrm{Sub}(F^m)$? The Fundamental Theorem of Projective Geometry (FTPG) states that this is true for many[26] types of fields provided that $m \geq 3$. A lot of effort has gone to adapt the FTPG to suitable R-modules $H \neq F^m$, e.g. having many direct summands.

The "degenerate" case $m = 2$ actually generalizes neatly from vector spaces to R-modules H with $d(\mathrm{Sub}(H)) = 2$ that are otherwise unrestricted. First observe that $\mathrm{Sub}(H) \simeq M_n$ where possibly n is an infinite cardinal. Up to a trivial exception, it turns out [W12] that for $n \leq 4$ *every* lattice automorphism $\phi : \mathrm{Sub}(H) \xrightarrow{\sim} \mathrm{Sub}(H)$ (which amounts to an arbitrary permutation of the atoms) is induced by a module automorphism $f : H \xrightarrow{\sim} H$ while for $n \geq 5$ there always is some ϕ which is not.[27]

Article [W9] looks at the FTPG in the "trivial direction" from $H \to H$ to $\mathrm{Sub}(H) \to \mathrm{Sub}(H)$, but with a twist. That is, suppose $f : H \to H$ is bijective and *R-homogeneous* (so $f(\lambda a) = \lambda f(a)$) but *not* necessarily additive (so $f(a+b) \neq f(a)+f(b)$). Under what extra provisos does f induce a lattice automorphism $\phi : \mathrm{Sub}(H) \to \mathrm{Sub}(H)$?

5.2 Groups, modules, and universal algebras

We collect a few facts about groups, modules and universal algebras. Some relate directly to my research, others constitute the backdrop for later sections.

5.2.1. Some properties of groups G are nicely reflected in their subgroup lattices. For instance for $|G| < \infty$ it holds that:

G is cyclic $\Leftrightarrow$ $\mathrm{Sub}(G)$ is distributive (Ore 1938, " $\Rightarrow$ " is easy)

G is supersoluble $\Leftrightarrow$ $\mathrm{Sub}(G)$ is Jordan-Dedekind

Many groups G, for instance Abelian or Hamiltonian[28] ones, have a modular lattice $\mathrm{Sub}(G)$, but no group-theoretic characterization of modularity is known. Akin to 5.1.1, the question of

[25] This fits well our characterization of distributive (= 1-distributive) lattices in terms of M_n's, which are exactly the directly irreducible length two PG's. Which ones are coordinatizable? We emphasize that (18) is a much weaker restriction than (7).

[26] We omit details. Suffice it to say that it works for $F = \mathbb{R}$, and it works for *every* field F if one is willing to trade the linearity of f for semi-linearity.

[27] It seems that even for the special case of vector spaces $H = F^2$ the stated fact was only known for *commutative* fields F; see [W12] for details. Recall also footnote 23 about M_4, M_5.

[28] A non Abelian group G is *Hamiltonian* if each subgroup is normal. More generally, a universal algebra A is *Hamiltonian* if every subalgebra is a congruence class of a suitable congruence. My only "pure"(uncluttered by anything else) universal algebra article is about these matters [GW]. My second-purest is [W2]: As is well

when lattice isomorphisms $\mathrm{Sub}(G) \xrightarrow{\sim} \mathrm{Sub}(G)$ are induced by group isomorphisms $G \xrightarrow{\sim} G$, is prominent in [Sch].

Recall that a group G is *simple* if G and $\{1\}$ are its sole *normal* subgroups. The classification of all simple finite groups, and thus to large extent *all finite* groups, is considered the biggest collaborative triumph of humankind so far. If one proceeds according to the cardinality $n = |G|$ then $n = 16$ is the first hard case. Although it was settled about 200 years ago, there does not seem to be an exposition that is based on as little prerequisites as [W11].

5.2.2. For a module $H = {}_RH$ to be *simple* means that $\{0\}$ and H are its only submodules. It is *indecomposable* if $H = K_1 \oplus K_2$ implies $K_1 = H$ or $K_2 = H$. Of course simple implies indecomposable. If $\dim(\mathrm{Sub}(H)) < \infty$ then clearly H is a direct sum of indecomposable submodules. One calls H *semisimple* if it is the sum of some (equivalently: all) simple submodules. Since each atomistic modular $f\ell$-lattice is complemented (5.1), each submodule K_1 of a semisimple module H has a complement K_2, i.e. $H = K_1 \oplus K_2$.

Recall that each R-module H really boils down to a "linear representation" of its ring R in that $r \mapsto (x \mapsto rx)$ is a ring homomorphism $\alpha : R \to \mathrm{End}(V, +)$, where $\mathrm{End}(V, +)$ is the endomorphism ring of the Abelian group $(V, +)$ underlying H. If α is injective then H is called *faithful*. One says that R is of *finite representation type* if up to isomorphism there are only finitely many indecomposable R-modules of finite length. This framework also accommodates linear representations of groups (even semi-groups) if one lets $R = F[G]$ be the group algebra over a field F. In this case $(V, +)$ is promoted to a F-vector space and each element of R (in particular of G) is associated with a vector space automorphism $V \xrightarrow{\sim} V$. However, structures different from rings, groups, semigroups, for which one seeks linear representations, need not fit the module framework.

The more general framework is the one of additive categories [S]. Without going into details, we note that semisimplicity and indecomposability remain central concepts on this level. Mentioned "structures" include Lie algebras, quivers, posets, or modular lattices. The latter two will be discussed in 5.4.

5.2.3. As a gentle introduction to universal algebra we recommend [BS]. Recall that a *congruence* (*relation*) on a universal algebra A is an equivalence relation $\theta \in \mathrm{Part}(A)$ which is compatible with the operations of A. It gives rise to a *quotient algebra* A/θ. The family $\mathrm{Con}(A)$ of all congruences is a sublattice of $\mathrm{Part}(A)$. For modules H one has $\mathrm{Con}(H) \simeq \mathrm{Sub}(H)$, for groups G only[29] $\mathrm{Con}(G) \simeq \mathrm{Sub}_N(G) := \{X \in \mathrm{Sub}(G) : X \text{ normal}\}$, and for arbitrary algebras A there may be next to no relation between the lattices $\mathrm{Con}(A)$ and $\mathrm{Sub}(A)$. Usually $\mathrm{Con}(A)$ is more important. Solving a problem of Ralph McKenzie (stated in [B]), the modularity of $\mathrm{Con}(A)$ can be settled in polynomial time [HW2]. If $\mathrm{Con}(A) = \{\bot, \top\}$ then A is called *simple*. That is consistent with the corresponding notions in 5.2.1 and 5.2.2.

Any student taking an algebra course hears about direct products of groups or vector spaces, but not necessarily of *subdirect* products which are far more useful. A subalgebra A of a direct

known, each identity that holds in an algebra A carries over to A/θ. Peter Pálfy had shown that modularity or distributivity even carries over from $\mathrm{Sub}(A)$ to $\mathrm{Sub}(A/\theta)$. In [W2] this is generalized twofold: Instead of $\mathrm{Sub}(A)$ the framework (6) suffices, and distributivity and modularity are special cases of certain *meet-weak* identities.

[29] That $\mathrm{Sub}_N(G)$ also is a *modular* sublattice of the usually nonmodular lattice $\mathrm{Sub}(G)$ is harder to see than the modularity of $\mathrm{Sub}(H)$.

product of algebras $A_1 \times A_2 \times \cdots \times A_n$ is called a *subdirect product* if for each $i \in [n]$ and each $b \in A_i$ there is at least one tuplet $(a_1, \cdots, b, \cdots a_n) \in A$. This gives rise to congruences $\theta_1, \cdots, \theta_n$ such that $\theta_1 \wedge \cdots \wedge \theta_n = \perp$, and conversely congruences which meet in $\perp$ yield a subdirect product. The irredundant subdirect decomposition of any algebra A correspond to the irredundant meet representations of $\perp \in \mathrm{Con}(A)$ (see also 2.1). Note that "simple $\Rightarrow$ subdirectly irreducible" but not conversely.

A *variety* is a class $\mathcal{V}$ of algebras of the same type (say all of them semigroups) which is closed under taking quotients, subalgebras, and direct products. The *free* n-generated algebra $\mathcal{FV}(n)$ in any variety $\mathcal{V}$ is the unique member of $\mathcal{V}$ with the property that every n-generated $A \in \mathcal{V}$ is a quotient $A = \mathcal{FV}(n)/\theta$.

The above remarks indicate how deeply universal algebra is linked to lattice theory. Of course lattices L are not just tools for algebras, they are themselves algebras. In fact, they are particularly nice in that $\mathrm{Con}(L)$ is always distributive. One consequence is that lattice varieties are more user-friendly. In particular the smallest variety $\mathcal{V}(L_0)$ that contains a given finite lattice L_0 is *locally finite* in the sense that every finitely generated member $L \in \mathcal{V}(L_0)$ is finite, and $\mathcal{V}(L_0)$ boils down[30] to the class $\mathcal{V}'$ of all subdirect products of quotients of sublattices of L_0. That may sound awkward but it readily implies[31] that $\mathcal{V}(D_2)$ is the variety $\mathcal{D}$ of all distributive lattices, and it forces (why?) that each member of $\mathcal{V}(M_3)$ is a subdirect product of M_3's and D_2's. Recall from 4.4.1 that $FD(n) \in \mathcal{D}$ generalizes to $FD(P) \in \mathcal{D}$. The variety $\mathcal{M}$ of all modular lattices is not locally finite; e.g. $|FM(3)| = 28$ (Dedekind) but $|FM(4)| = \infty$. The lattices $FM(P)$ mentioned in 4.4.1 will reoccur in 5.4.1.

5.3 Lower bounding $j(L)$ in a finite modular lattice

In this section all lattices L are finite. Generalizing the distributive case, by a famous result of Dilworth each modular L still satisfies $j(L) = m(L)$. We shall exhibit a lower bound for $j(L)$ in terms of $d(L)$ and $s(L)$ below that is much harder to establish than Theorem 3.

For starters, it turns out that $\mathrm{Con}(L)$ is not just distributive (5.2.3) but Boolean of length $s(L) := d(\mathrm{Con}(L)) \leq d(L)$. What is more:

$$L \text{ simple } \Leftrightarrow\ L \text{ subdirectly irreducible } \Leftrightarrow\ L \text{ directly irreducible } \Leftrightarrow\ s(L) = 1.$$

The letter s indicates that $s(L)$ gives the number of subdirectly irreducible factors of L. Correcting a mistake in [HW1] the following is shown in [W6]:

(19) $\qquad j(L) \quad \geq \quad 2d(L) - s(L).$

For all distributive lattices $L = D$ the inequality (19) is sharp[32] but also for M_3 (check) and many others, as we shall see. A *line-top* is defined as an element x all of whose lower covers

[30] For finite algebras A_0 which are not lattices one only has $\mathcal{V}' \subsetneq \mathcal{V}(A_0)$; however, $\mathcal{V}(A_0)$ is locally finite also in this case.

[31] Clearly $\mathcal{V}(D_2) \subseteq D$. Conversely, the only subdirectly irreducible member of $\mathcal{D}$ is D_2 because for each at least 3-element $D \in \mathcal{D}$ any $a \in D \setminus \{\perp, \top\}$ yields a subdirect decomposition of D via $x \mapsto (a \wedge x, a \vee x)$. Thus $\mathcal{D} \subseteq \mathcal{V}(D_2)$.

[32] This follows from $d(D) = j(D) = s(D)$ where the first $=$ is Theorem 3 and the second $=$ is because for distributive D the $s(D)$ many co-atoms θ_p of $\mathrm{Con}(D)$ correspond to its join-irreducibles $p \in J(D)$. Namely,

$x_1, \cdots, x_n$ number to $n \geq 3$ and are such that the interval $[x_1 \wedge \cdots \wedge x_n, x]$ is isomorphic to M_n. A crucial technical tool for each modular lattice L is a certain geometric structure, called *base of lines*[33], that consists of $J(L)$ as point set and of suitable "lines" $\ell \subseteq J(L)$ that partition $J(L)$ in $s(L)$ many "connected components". These lines are usually not unique but for each line-top exactly one of "its" lines is picked. Further details below. If $i(L)$ is the number of line-tops (in particular $i(D) = 0$ in the distributive case) then

(20) $\qquad i(L) \;\; \geq \;\; d(L) - s(L).$

The potential 2-distributivity (see 5.1) of L amounts to a certain "local acyclicity" of all its bases of lines, which in turn yields

(21) $\qquad j(L) \;\; \geq \;\; i(L) + d(L).$

Observe that (21) betters (19) (in view of (20)). For instance, $L = \text{Sub}(GF(2)^3)$ isn't 2-distributive, and indeed $7 \not\geq 7 + 3$. If there is local acyclicity, there must be (global) acyclicity which presumingly is better still. Indeed, all *acyclic*[34] modular lattices L improve upon (20) in that

(22) $\qquad i(L) \;\; = \;\; d(L) - s(L).$

For instance, (22) becomes $1 = 2 - 1$ for $L = M_n$. Finally, if L is 3-*acyclic*[35] in the sense of being acyclic with all line-tops having $n = 3$, then (21) is sharp and therefore also (19) (using (22)).

In any modular L a *line* is defined as a subset $\ell \subseteq J(L)$ which has $|\ell| \geq 3$ and is maximal with respect to the property that all $p \neq q$ in ℓ yield the *same* join $p \vee q = x$. The kind of elements x arising are exactly the previously defined line-tops. For instance, for $x \in L_3$ in Figure 4 one corresponding line is $\{8, 10, 11, 12\}$ (another would be $\{8, 9, 11, 12\}$). A line for the line-top $y \in L_3$ is $\{4, 9, 10\}$ and ditto for the line-tops z, u. The arising base of lines has $s(L_3) = 3$ connected components (one of which is $\{2\}$, corresponding to a subdirect factor D_2). The lattice L_3 is acyclic. If we drop 11 or 12, it becomes 3-acyclic and thus (19) is sharp: $11 = 2 \cdot 7 - 3$.

---

because each p is *join-prime* in the sense that ($x \vee y \geq p \Rightarrow x \geq p$ or $y \geq p$) for all $x, y \in D$, one checks that $[p, \top]$ and $D \setminus [p, \top]$ are the classes of a congruence θ_p on D.

[33]They generalize the projective geometries of 5.1 in congenial ways. Although bases of lines are rooted in the "Dreiecksmatroide" of [W1], their enhancement to a level fit for proving the arithmetic relations (19) to (22) must be credited to Herrmann. On the other hand, much of the representation theory component of [HW1] (outlined in 5.4) was established in [W1] by merely using the Dreiecksmatroid concept. See also 5.8.

[34]By definition acyclicity means that in some base of lines (equivalently: all base of lines) there occurs no cycle of lines (in the obvious sense).

[35]It is also handy to call a lattice *locally* 3-*acyclic* if it is locally acyclic and all line-tops have $n = 3$. These names slightly differ from the ones in [HW1]; e.g. our "3-acyclic" is just "acylcic".

Fig. 4

5.4 Modular lattices of finite representation type

Let V be a finite-dimensional F-vector space. With the backdrop of 5.2.2 we define a (F*-linear*) *representation* of a modular lattice L as a homomorphism $\phi : L \to \mathrm{Sub}(V)$ with $\phi(\bot) = \{0\}$ and $\phi(\top) = V$. Two representations $\phi_1 : L \to \mathrm{Sub}(V_1)$ and $\phi_2 : L \to \mathrm{Sub}(V_2)$ are *isomorphic*[36] if there is a vector space isomorphism $f : V_1 \stackrel{\sim}{\to} V_2$ such that $f(\phi_1(a)) = \phi_2(a)$ for all $a \in L$. The (external) *direct sum* $\phi_1 \oplus \phi_2 \oplus \cdots \oplus \phi_m$ of representations is defined in the obvious way (how?). A representation $\phi : L \to \mathrm{Sub}(V)$ is *non-simple* if there is a (cherry-picked!) nonzero subspace $V_1 \subsetneqq V$ such that $a \mapsto \phi(a) \cap V_1$ is a representation $L \to \mathrm{Sub}(V_1)$. And ϕ is *decomposable* if there is a decomposition $V = V_1 \oplus V_2$ such that $\phi(a) = (V_1 \cap \phi(a)) \oplus (V_2 \cap \phi(a))$ for all $a \in L$. In this case $\phi_i : L \to \mathrm{Sub}(V_i) : a \mapsto V_i \cap \phi(a)$ is a representation of L $(i = 1, 2)$ and ϕ is isomorphic to $\phi_1 \oplus \phi_2$ (check). See [P] for an example of a non-simple representation which is however indecomposable. A representation ϕ is *faithful* if it is injective, and of course is *cover preserving* (cp) if $x \prec y$ implies $\phi(x) \prec \phi(y)$. The following is easy to see and similar to [P, Lemma 2.3]:

(23) If L is finite and subdirectly irreducible then every cover preserving representation is faithful (clear) and indecomposable.

In accordance with general representation theory (5.2.2) we say that L is of *finite representation type* if there are only finitely many nonisomorphic indecomposable representations. It's handy to call the representation type *subdirectly driven* if $\phi(L)$ is subdirectly irreducible for all indecomposable representations ϕ.

The following is shown in [HW1]: Let $\mathcal{MD}_2$ be the class of finite 2-distributive modular lattices. Each $L \in \mathcal{MD}_2$ has a faithful representation over every field F. More specifically, if F is large enough one gets a faithful cp embedding (this was shown by other means by Jónsson-Nation

[36] Note that this relates to "linearly induced" from 5.1.1.

in 1986). If faithful cp representations over *all* fields F are required, it's exactly the locally 3-acyclic lattices that comply. For instance, all modular lattices which admit a cp embedding into a partition lattice (see 5.5) are locally 3-acyclic. The lattices $L \in \mathcal{MD}_2$ of finite representation type are exactly the 3-acyclic ones. Any such L is semisimple, i.e. each representation ϕ of L is a sum of simple representations. Specifically, L is subdirectly driven in the extra pleasant manner that for each subdirectly irreducible factor L/θ there is a unique indecomposable representation $\phi : L \to \mathrm{Sub}(V)$ such that $\phi(L) \simeq L/\theta$ is a *cp* sublattice of Sub(V).

5.4.1 A linear representation of a *poset* P is defined [S, p.31] as a merely *monotone* map $\phi : P \to \mathrm{Sub}(V)$. While the representation theory of arbitrary (non-free) lattices cannot be reduced to the (historically first) representation theory of posets, it works the other way around, at least in principle. Namely, the representations of any finite poset P correspond in obvious ways to the representations of the *lattice* $L = FM(P)$ which however (5.2.3) can be infinite and highly complex even for small P. Nevertheless, the following can be said. Define

$$\mathcal{K}_1 \;:=\; \{P \text{ finite poset}:\ |FM(P)| < \infty\}$$

$$\mathcal{K}_2 \;:=\; \{P \text{ finite poset}:\ FM(P) \text{ (equivalently : } P) \text{ has finite representation type}\}$$

$$\mathcal{K}_3 \;:=\; \{P \text{ finite poset}:\ FM(P) \text{ has subdirectly driven representation type}\}$$

Not at all obvious, it turns out that $\mathcal{K}_1 \subseteq \mathcal{K}_2 \subseteq \mathcal{K}_3$. In order to flesh things out a bit we e.g. write $\mathbf{1}+\mathbf{2}+\mathbf{5}$ for the poset which is a disjoint union of chains of cardinality 1,2,5. That generalizes our previous notation in that (say) $FM(4) = FM(\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1})$. Then:

- By a result of Wille 1973 one has $P \in \mathcal{K}_1$ iff P has neither $\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}$ nor $\mathbf{1}+\mathbf{2}+\mathbf{2}$ as subposet. In this case $FM(P)$ is in fact in $\mathcal{V}(M_3)$ and thus 3-acyclic.
- One has $P \in \mathcal{K}_2$ iff P has none of these as subposets: $\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}$, $\mathbf{2}+\mathbf{2}+\mathbf{2}$, $\mathbf{1}+\mathbf{2}+\mathbf{5}$, $\mathbf{1}+\mathbf{3}+\mathbf{3}$, $\mathbf{4}+\mathbf{Z_4}$ (where $\mathbf{Z_4} = \{z_1, z_2, z_3, z_4,\ z_1 < z_2 > z_3 < z_4\}$). For instance $\mathbf{1}+\mathbf{2}+\mathbf{2} \in \mathcal{K}_2 \setminus \mathcal{K}_1$ and $FM(\mathbf{1}+\mathbf{2}+\mathbf{2})$ is a subdirect product of D_2's, M_3's and certain PG's of length three (see 5.1).
- Most prominently $\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1} \in \mathcal{K}_3 \setminus \mathcal{K}_2$. Its (infintely many) indecomposable representations have been classified in a famous 1970 paper of Gelfand-Ponomarev. Major strides to understand matters in lattice-theoretic terms were made in [H].
- For instance $P := \mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1}+\mathbf{1} \notin \mathcal{K}_3$ because by [P, p.48] there is a indecomposable representation $\phi : FM(P) \to \mathrm{Sub}(V)$ such that $\phi(FM(P))$ is subdirectly *reducible* of cardinality 15. This is reminiscent of the M_4, M_5 dichotomy.

We mention in passing that incidence algebras over P (which we view from another angle in 5.7) are of utter importance in [S].

5.5 Cover preserving embeddings into partition lattices

All lattices L are finite in 5.5. Recall the definitions of PG and CG from 5.1. Whereas in 5.4 we had embeddings $L \to PG$, here we turn to embeddings $L \to CG$. The first L is forced to be modular, but by a theorem of Dilworth the second L can be *any* lattice. The nicest lattices CG are the lattices $\text{Part}(S)$ of all set partitions (= equivalence relations) of a set S. Pudlak and Tuma solved a long standing problem by showing that each lattice L in fact embeds into $\text{Part}(S)$, thus topping Dilworth's CG embedding theorem. Trouble is, their proof requires S to have super-exponential cardinality with respect to $d(L)$.

I felt therefore challenged to find lattices L that embed in the most economic way, i.e. with $|S| = d(L) - 1$ (why?). Of course that forces *cp-embeddings* and hence (see 5.1) upper semimodular lattices L. Having acquired some skills with *modular* lattices L (bases of lines, etc.) I focused on them from the outset. Some sufficient and some necessary conditions (not quite matching but almost) for the cp embeddability of L were obtained in [W4]. Suffice it to say that by mere cardinality arguments no nondegenerate projective plane PG, nor M_4 is cp embeddable into $\text{Part}(S)$. Therefore L is necessarily *locally* 3-acyclic, but it can feature quite sophisticated accumulations of (global) cyles.

5.6 Cyclic modules and rays

Here follow three facts about *cyclic* R-modules P, i.e. of type $P = Rx$ for some $x \in P$. Firstly, it is easy to see (try) that each join irreducible member P of any lattice $\text{Sub}({}_R H)$ is cyclic. Secondly, if $\text{Sub}(H)$ is distributive of finite length then H must be cyclic as well.[37]

Thirdly, a fixed R-module H_0 is a *ray* if for each R-module H' each R-homogeneous map $f : H_0 \to H'$ (i.e. $f(\lambda a) = \lambda f(a)$) must be additive (i.e. $f(a + b) = f(a) + f(b)$). Trivial but important, each cyclic module is a ray (try). Here is a weak kind of converse: For a ray H_0 each join irreducible submodule $P \in \text{Sub}(H_0)$ is not just cyclic itself but must be *strictly* contained in a cyclic submodule [MW]. In particular, a ray H_0 with $\text{Sub}(H_0) \simeq M_n$ must be cyclic. Here are three further problems addressed in [MW]:

(a) Characterize the rays among specific classes $\mathcal{H}$ of modules.
(b) Find rings R for which "ray $\Rightarrow$ cyclic".
(c) Characterize the Fuchs-Maxson-Pilz (FMP) rings, i.e. those R for which *every* R-module is a ray.

In brief, (a) is settled for the class $\mathcal{H}$ of all semisimple modules, (b) e.g. holds for left perfect local rings. As to (c), this is Carl Maxson's quest. Based on previous work of Fuchs, Maxson and Pilz, it is shown in [MW, p.127] that *among* the semiperfect rings, the FMP-rings are exactly the full matrix rings over fields. This leads us naturally to the next topic.

5.7 A machine for producing non-isomorphic incidence algebras

For any fixed field F consider the set R_1 of all 8×8-matrices A with component $A_{i,j} = 0$ whenever the (i, j)-entry of the $(0, F)$-*pattern* in Figure 5(ii) is zero (thus say $A_{2,5} = 0$). Otherwise $A_{i,j} \in F$ can be arbitrary. Clearly R_1 is closed under addition. Also R_1 is closed under multiplication

[37] This was known. A quick proof is given in [MW]. Other than for groups, for finite length modules only the direction "distributive $\Rightarrow$ cyclic" holds.

because the binary relation on the index set [8] defined by

$$i \sim j :\Leftrightarrow \text{ (the } (i,j) - \text{entry in Figure 5(ii) is } F),$$

is transitive. Furthermore R_1 contains the identity matrix since $\sim$ is reflexive. Any such ring R of $n \times n$ matrices spawned by a transitive, reflexive relation $\sim$ on $[n]$ is called a *structural matrix ring* over F. If additionally $\sim$ is antisymmetric, $\sim$ becomes a partial order[38] relation $\leq$ on $P = [n]$, and one calls R the *incidence algebra* over the poset $(P, \leq)$.

As one readily verifies, applying any fixed permutation $\pi \in S_n$ simulateously to the rows and columns of the $(0,F)$-pattern of R yields a usually much different $(0,F)$-pattern whose corresponding incidence algebra R' is however isomorphic to R. The reader may enjoy to check that R_1 (defined by Figure 5(ii)) is isomorphic to R_2 (defined by Figure 5(iii)) by virtue of the permutation $\pi_0 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 8 & 2 & 1 & 7 & 6 & 3 \end{pmatrix}$.

(i)

Q_1 fixed	Q_3 free
0	Q_2 fixed

(ii)

$$\left[\begin{array}{ccccc|ccc}
F & F & F & 0 & 0 & F & F & 0 \\
0 & F & F & 0 & 0 & F & F & 0 \\
0 & 0 & F & 0 & 0 & F & 0 & 0 \\
0 & 0 & 0 & F & 0 & 0 & F & F \\
0 & 0 & 0 & F & F & 0 & F & F \\ \hline
0 & 0 & 0 & 0 & 0 & F & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & F & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & F & F
\end{array}\right]$$

(iii)

$$\left[\begin{array}{ccccc|ccc}
F & F & F & 0 & 0 & F & 0 & 0 \\
0 & F & F & 0 & 0 & F & 0 & 0 \\
0 & 0 & F & 0 & 0 & F & 0 & 0 \\
0 & 0 & 0 & F & 0 & F & F & F \\
0 & 0 & 0 & F & F & F & F & F \\ \hline
0 & 0 & 0 & 0 & 0 & F & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & F & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & F & F
\end{array}\right]$$

Fig. 5

By a 1970 result[39] of Richard Stanley the converse holds as well: Whenever $R \simeq R'$, there is at least one $\pi \in S_n$ by which the two defining $(0,F)$-patterns are linked. This begs the question (doesn't it?) for a machinery that precludes the existence of linking permutations π and thus spawns nonisomorphic incidence algebras at liberty. Here comes one way to do it. Subdivide the $n \times n$ grid into four quadrants Q_1, Q_2, Q_3, Q_4 as follows (Figure 5(i)). The lower left Q_4 is zero. For $i = 1, 2$ let Q_i be the $(0,F)$-pattern of the incidence algebra of an arbitrary but fixed poset P_i. The quadrant Q_3 is a free "plug-in" $(0,F)$-pattern, but it needs to be admissible[40] in the sense that the overall $(0,F)$-pattern yields an incidence algebra $R = R(Q_3)$ in the first place. The pair of posets (P_1, P_2) may or may not satisfy a certain *IF-condition*. It is shown in [W15, Thm.2] that the following statements are equivalent:

(a) Distinct plug-ins $Q_3 \neq Q_3'$ always yield *nonisomorphic* rings $R(Q_3)$ and $R(Q_3')$.
(b) (P_1, P_2) satisfies the IF-condition.

[38] Of course this $\leq$ is not to be confused with the natural order on $[n]$.

[39] A short and very different proof based on a forgotten 1964 paper of R.E. Johnson and the distributivity of the lattice $\mathrm{Sub}({}_R F^n)$ is given in [W15]. Similar matters for $n \times n$ *structural* matrix rings R, inspired by conversations with Leon van Wyk, are pursued in [ABW]. For instance, the shape of the (non-distributive) lattice $\mathrm{Sub}({}_R F^m)$ is investigated when R somehow (necessarily *not* by matrix multiplication) acts upon F^m when $m \neq n$.

[40] It's easy to explicitly describe the admissible plug-ins. In fact, all of them can be compactly generated using POE with suitable wildcards.

For instance, the underlying $(\overline{P}_1, \overline{P}_2)$ in (ii) and (iii) does not satisfy the IF-condition. That's why π_0 above could exist. It turns out that among many other possibilities each pair of *chains* (P_1, P_2) satisfies the IF-condition. Thus if Q_1 and Q_2 in (ii) and (iii) are replaced by upper diagonal matrices (i.e. having F's on and above the main diagonal) then the two overall $(0, F)$-patterns would define two nonisomorphic incidence algebras.

5.8 How it all began: Infinite-dimensional quadratic spaces

For us[41] a *quadratic space* (V, Φ) is a F-vector space V which is equipped with a skew-symmetric bilinear form $\Phi : V \times V \to F$, i.e. $\Phi(y, x) = -\Phi(x, y)$. For any subset $X \subseteq V$ its *orthogonal* is defined as $X^\perp := \{y \in V : \ (\forall x \in X)\ \Phi(x, y) = 0\}$. It is easily seen (try) that (i) $X \subseteq Y \Rightarrow X^\perp \supseteq Y^\perp$, and that the *bi-orthogonal* $X^{\perp\perp} := (X^\perp)^\perp$ satisfies (ii) $X^{\perp\perp} \supseteq X$. In fact $X \mapsto X^{\perp\perp}$ is a closure operator; idempotency follows from $X^{\perp\perp\perp} = X^\perp$ which is a consequence of (i) and (ii). Furthermore $X^\perp$ always is a subspace of E and $(X + Y)^\perp = X^\perp \cap Y^\perp$, while solely $(X \cap Y)^\perp \supseteq X^\perp + Y^\perp$.

A vector space automorphism $f : V \xrightarrow{\sim} V$ is an *isometry* if $\Phi(f(x), f(y)) = \Phi(x, y)$ for all $x, y \in V$. Two subspaces X, Y, of V are called *congruent* (not to be confused with the notion from 5.2) if there is an isometry $f : V \xrightarrow{\sim} V$ with $f(X) = Y$. Notice that $f(X) = Y$ implies $f(X^\top) = Y^\top$ whence $f(X \cap X^\perp) = Y \cap Y^\perp$, whence say $f((X \cap X)^\perp + X^{\perp\perp}) = (Y \cap Y^\perp) + Y^{\perp\perp}$ and so forth. More specifically, defining the *radical* of a subspace U as $\operatorname{rad} U = U \cap U^\top$, the generated *quadratic lattice* $Q_0[X]$ is a quotient of the free object FQ_0 in a suitable variety (5.2.3) of "quadratic lattices":

[41] In reality some additional technical conditions need to hold.

Fig. 6

By the comments above it is clear that the index-preserving (ip) isomorphy of the quadratic lattices $Q_0[X]$ and $Q_0[Y]$ is *necessary* for the subspaces $X, Y \subseteq E$ to be congruent. Here ip means that e.g.

$$\dim(X^{\top\top}/X) = 73 \quad \text{implies} \quad \dim(Y^{\top\top}/Y) = 73.$$

As proven in [G], if $\dim(E) \le \aleph_0$ (i.e. E has countable dimension), then the stated condition is *sufficient* as well.[42] If $\dim(E) = \aleph_1$ then besides $X \mapsto X^{\perp\perp}$ a more subtle closure operator $X \mapsto \sigma_1(X)$ derived from Φ enters the definition of a similar quadratic lattices $Q_1[X]$. We mention that $\sigma_1(X) \subseteq X^{\top\top}$ and that σ_1 is topological, i.e. satisfies $(C04)$ in section 3. The ip isomorphy $Q_1[X] \simeq Q_1[Y]$ is again sufficient and necessary for the congruence of X and Y. Things can be pushed to higher dimensions due to Gross' Lattice Method which works as long as dim$E) \le \aleph_{\omega_1}$ and the concerned lattices are finite and distributie. Here $|FQ_0| = 14$ (Kaplansky), $|FQ_1| = 30$ (Bäni) and $|FQ_2| = 88$ (Gross), and all three lattices are distributive.

[42] If $\dim(E) < \aleph_0$ then quadratic lattices can be dispensed with altogether due to a Theorem of Witt which states that the isometry of X and Y is necessary and sufficient for their congruence. In fact it was exactly the failure of Witt's Theorem in dimension $\aleph_0$ which prompted Gross to invent his Lattice Method: In brief, the required isometry $f : V \xrightarrow{\sim} V$ that maps X upon Y is constructed by heeding the fine structure of the relevant quadratic lattice. This was perhaps the crown of several original ideas of Gross to push quadratic forms from finite to infinite (even uncountable) dimensions. Previously uncountable quadratic space theory was all but restricted to Hilbert space theory. Herbert Gross passed away, much too early, in 1989. The monograph [KKW] is dedicated to his memory.

For $\dim(E) = \aleph_3$ the lattice $Q_3[X]$ can have up to $|FQ_3| = 957$ elements and need not be distributive (Gross, Lomecky, Schuppli). Nevertheless, in my thesis [W1] I showed that Gross' Lattice Method can be adapted. The state of affairs for $\aleph_4$ remains open (though $|FQ_4| = \infty$ is known) but for $\dim(E) = \aleph_5$ I found subspaces $X, Y \subseteq E$ which are *not* congruent despite the fact that $Q_5[X]$ and $Q_5[Y]$ are ip isomorphic (of cardinality 32). This somewhat damaged the reputation of the Lattice Method as a panacea.

The reason why X and Y cannot be matched by an isometry is that there is not even a *linear* automorphism $V \xrightarrow{\sim} V$ that maps $Q_5[X]$ upon $Q_5[Y]$. This prompted me to drop the distracting quadratic form Φ and focus on linear matters in half of [W1]; see 5.4. The occurence of a mischievious sublattice M_5 in $Q_5[X] \simeq Q_5[Y]$ also led to [W12], see 5.1.1.

If one keeps the lattices finite and distributive in the Lattice Method one can focus instead on the dimension bound of (E, Φ). In my thesis I extended $\aleph_{\omega_1}$ to the first weakly inaccessible cardinal, which exposed me to quite a bit of axiomatic set theory. While another pupil of Gross (my colleague Otmar Spinas) became a successful set theorist, I returned to finite structures after my thesis.

6 The asymptotic number of binary codes

Previous versions of this manuscript had section 6 subsumed under either "Combinatorial geometries" or "Modularity". This is because the switch from binary matroids (3.1) to binary codes (defined below) boils down to a change of perspective on the *same* underlying 0, 1-matrices. As to modularity, this concerns the lattices $L(\pi)$ below. Eventually I decided that my biggest[43] achievement [W10] deserves a section on its own.

Binary codes are used to encode and transmit information all over the earth, within our solar system (most recently to and from Juno which is on its way to Jupiter), and quite likely in other solar systems as well. Formally a (linear) *binary code* X of length N is a subspace of the vector space $GF(2)^n$, where (recall) $GF(2) = \{0, 1\}$ is the two element field. For two binary vectors $v, w \in GF(2)^n$ the (*Hamming*) *distance* is the number of positions i in which they differ:

$$d(v, w) \quad := \quad |\{1 \le i \le n : \ v_i \ne w_i\}|.$$

Ideally a binary code X of fixed length n should satisfy two conflicting properties; it should be large while maintaining a high minimum distance

$$md(X) \quad := \quad \min\{d(x, y) : x, y \in X, x \ne y\}.$$

This and other properties do not change when a fixed permutation $\pi \in S_n$ is applied to all codewords of X, resulting in some new binary code X^π. For instance, if $\pi \in S_3$ is the cyclic

[43] This is by traditional standards whereby those articles are best which solve *other* people's problems; of course taking into account both the difficulty of the problem and the standing of the problem-poser. More details being given throughout this manuscript, my (and my co-authors' Adaricheva and Herrmann) served problem-posers were Welsh, Edelman-Jamison, Coyle-Shmulevich, Burris, and Rival. My other articles (like most published articles) "just" advance knowledge in more or less useful directions by settling one's *own* (taylor-made) problems. If I take as criterion citation count, total work required, or the interval between the first and last research done for an article (regardless of year-long pauses), the crown goes to [W5], [W4], [W14] respectively.

permutation $1 \mapsto 2 \mapsto 3 \mapsto 1$ then say

$$X = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}$$

results in

$$X^\pi = \{(0,0,0),(1,0,0),(0,0,1),(1,0,1)\}.$$

Two binary codes X and X' of the same length n are called *equivalent* if $X' = X^\pi$ for some permutation π. Let $b(n)$ be the number of equivalence classes of binary codes of length n. Ad hoc one verifies $b(1) = 2$, $b(2) = 4$, $b(3) = 8$ (try), and it continues as expected: $b(4) = 16$, $b(5) = 32$. However, $b(n) \neq 2^n$ in general:

$$\begin{array}{lcl} b(6) & = & 68 \\ b(7) & = & 148 \\ b(8) & = & 342 \\ b(9) & = & 848 \\ b(10) & = & 2297 \\ b(25) & = & 58638266023262502962716 \end{array}$$

(google $A076766$, which will give you one of Sloane's integer sequences)

An explicit formula for $b(n)$ seems impossible but letting $G(n,2)$ be the number of subspaces of $GF(2)^n$ it is clear that $b(n) \leq G(n,2)/n!$ since each equivalence class of subspaces has cardinality at most $n!$. Less trivial, in 2005 I found that asymptotically $b(n) \approx G(n,2)/n!$ thereby settling a problem posed by Dominic Welsh in 1969 [Ox, Problem 14.5.4]. In fact one has the stronger result [W10] that

$$(24) \quad (1 + 2^{-\frac{n}{2}+2\log n+1.2499})\frac{G(n,2)}{n!} \quad \leq \quad b(n) \quad \leq \quad (1 + 2^{-\frac{n}{2}+2\log n+1.2501})\frac{G(n,2)}{n!}$$

for all sufficiently large n. As to a formula for $G(n,2)$, one has $G(n,2) = \sum_{k=0}^{n} G(n,2,k)$ where $G(n,2,k)$ is the so-called *Gauss coefficient* that counts the number of k-dimensional subspaces of $GF(2)^n$. Many features of Gauss coefficients, including their asymptotic behaviour, were long known, but not so the asymptotic behaviour of the *sum* $G(n,2)$ it seems. Using a recursive formula of J. Goldman and Gian-Carlo Rota,[44] i.e.

$$(25) \quad G(n+1,2) \quad = \quad 2G(n,2) + (2^n - 1)G(n-1,2) \quad (n \geq 1)$$

and a hint from Andrew Barbour concerning Cauchy-sequences did the trick. It turned out that $G(n,2)$ grows slightly different[45] for even and for odd numbers. Specifically,

$$(26) \quad G(2n,2) \approx (7.371969\cdots)2^{n^2/4}, \qquad G(2n+1,2) \approx (7.371949\cdots)2^{n^2/4}$$

The proof of (24) hinges on the possibility (using [BF]) to get lower and upper bounds for the size of the sublattices $L(\pi) \subseteq \mathrm{Sub}(GF(2)^n)$ of all T_π-invariant subspaces, where $T_\pi : GF(2)^n \to$

[44] I am privileged to have known well Gian-Carlo Rota, one of the founders of modern combinatorics, who in 1989 was eager to learn as mush as possible about modular lattices from a (then) nobody like me.

[45] That is why 1.2499 and 1.2501 in (24) *cannot* be replaced by $1.25 - \varepsilon$ and $1.25 + \varepsilon$ for fixed $\varepsilon > 0$. Stavros Kousidis proved in September 2011 that the two constants $7.37\cdots$ in (26) can be given in a closed form that involves the Jacobi theta functions. His article is on the ar$X$iv.

$GF(2)^n$ is the linear operator induced by the $n!$ many permutations π. The minimal polynomial of T_π plays a crucial rôle.

References

[AW] K. Adaricheva, M. Wild, Realization of abstract convex geometries by point configurations, *European Journal of Combinatorics* 31 (2010) 379-400.

[ABW] M. Akkurt, G.P. Barker, M. Wild, Structural matrix rings and their lattices of invariant subspaces, *Linear Algebra and its Applications* 394 (2005) 25-38.

[B] S. Burris, Computers and universal algebra: some directions, *Algebra Universalis* 34 (1995) 61-71.

[BF] L. Brickmann, P.A. Fillmore, The invariant subspace lattice of a linear transformation, *Canad. J. Math.* 19 (1967) 810-822.

[BS] S. Burris, H.P. Sankappanavar, A course in universal algebra, The Millenium Edition, freely available on the web.

[EJ] P.H. Edelman, R. Jamison, The theory of convex geometries, *Geometriae Dedicata* 19 (1985) 247-274.

[FW] H. Fripertinger, M. Wild, A catalogue of regular matroids of cardinality at most fifteen, submitted.

[GR] J. Goldman, G.C. Rota, The number of subspaces of a vector space, *Recent Progress in Combinatorics*, p.75-83, Academic Press 1969.

[GW] V. Gould, M. Wild, Every Hamiltonian variety has the congruence extension property – a short proof, *Algebra Universalis* 26 (1989) 187-188.

[G] H. Gross, Quadratic forms in infinite dimensional vector space, *Progress in Mathematics 1*, Birkhäuser 1979.

[H] C. Herrmann, Rahmen und erzeugende Quadrupel in modularen Verbänden, *Algebra Universalis* 14 (1982) 357-387.

[HW1] C. Herrmann, M. Wild, Acyclic modular lattices and their representations, *Journal of Algebra* 136 (1991) 17-36.

[HW2] C. Herrmann, M. Wild, A polynomial algorithm for testing congruence modularity, *International Journal of Algebra and Computation* 6 (1996) 379-387.

[KKW] H.A. Keller, U.M. Künzi, M. Wild (eds.) Orthogonal geometry in infinite dimensional vector spaces, (book in memoriam of Herbert Gross), *Bayreuther Mathematicshe Schriften*, Heft 53 (1998), 326p.

[M] D. Maier, The theory of relational databases, Computer Science Press 1983.

[MW] C.J. Maxson, M. Wild, When are homogeneous functions linear? A lattice point of view, *Results in Mathematics* 47 (2005) 122-129.

[Ox] J.G. Oxley, *Matroid Theory*, Oxford University Press 1992.

[P] W. Pogunktke, Zerlegung von S-Verbänden, *Mathematische Zeitschrift* 142 (1975) 47-65.

[RW] C. Rohwer, M. Wild, LULU-theory, idempotent stack filters, and the mathematics of vision of Marr, *Advances in Imaging and Electron Physics* 146 (2007) 57-162.

[Sch] R. Schmidt, *Subgroup lattices of groups*, De Gruyter 1994.

[S] D. Simson, *Linear representations of partially ordered sets and vector space categories*, Gordon and Breach Science Publishers 1992.

[WW] S. Wagner, M. Wild, Partitioning the hypercube Q_n into n isomorphic edge-disjoint trees, submitted.

[W1] M. Wild, Dreieckverbände, Lineare und quadratische Darstellungstheorie, PhD thesis, University of Zurich 1987.

[W2] M. Wild, Join epimorphisms which preserve certain lattice identities, *Algebra Universalis* 27 (1990) 398-410.

[W3] M. Wild, Cover preserving order embeddings into Boolean lattices, *Order* 9 (1992) 209-232.

[W4] M. Wild, Cover preserving embedding of modular lattices into partition lattices, *Discrete Mathematics* 112 (1993) 204-244.

[W5] M. Wild, A theory of finite closure spaces based on implications, *Advances in Mathematics* 108 (1994) 118-139.

[W6] M. Wild, The minimal number of join irreducibles of a finite modular lattice, *Algebra Universalis* 35 (1996) 113-123.

[W7] M. Wild, Optimal implicational bases for finite modular lattices, *Quaestiones Mathematicae* 23 (2000) 153-161.

[W8] M. Wild, Idempotent and co-idempotent stack filters and min-max operators, *Theoretical Computer Science* 299 (2003) 603-631.

[W9] M. Wild, Homogeneous bijections that induce automorphisms of the submodule lattice, *Communications in Algebra* 33 (2005) 2649-2661.

[W10] M. Wild, The asymptotic number of binary codes and binary matroids, *SIAM Journal on Discrete Mathematics* 19 (2005) 691-699.

[W11] M. Wild, The groups of order sixteen made easy, *American Mathematical Monthly* 112 (2005) 20-31.

[W12] M. Wild, The fundamental theorem of projective geometry for an arbitrary length two module, *Rocky Mountain Journal of Mathematics* 36 (2006) 2075-2080.

[W13] M. Wild, Generating all cycles, chordless cycles and Hamiltonian cycles with the princple of exclusion, *Journal of Discrete Algorithms* 6 (2008) 93-102.

[W14] M. Wild, Weakly submodular rank functions, supermatroids, and the flat lattice of a distributive supermatroid, *Discrete Mathematics* 308 (2008) 999-1017.

[W15] M. Wild, Incidence algebras that are uniquely determined by their zero-nonzero matrix pattern, *Linear Algebra and its Application* 430 (2009) 1007-1016.

[W16] M. Wild, Compactly generating all satisfying truth assignments of a Horn formula, to appear in *Journal on satisfiability, Boolean modeling and computation.*

[W17] M. Wild, Counting or producing all fixed cardinality transversals, submitted.

[W18] M. Wild, Computing the output distribution and selection probabilities of a stack filter from the DNF of its positive Boolean function, submitted. In the ar$X$iv.