Three undergraduate research experiences in abstract algebra

Peter Jipsen

Chapman University

AMS Fall Western Sectional Meeting
UC Riverside, California, USA

November 10, 2019

Outline

- Nathan Lawless, 2013
  - **Generating modular lattices**
- Eyad Kurd-Misto and James Wimberley, 2015
  - **Boolean semilattices**
- Sarah Alexander and Nadia Upegui, 2017
  - **Separation algebras and effect algebras**
- Some observations

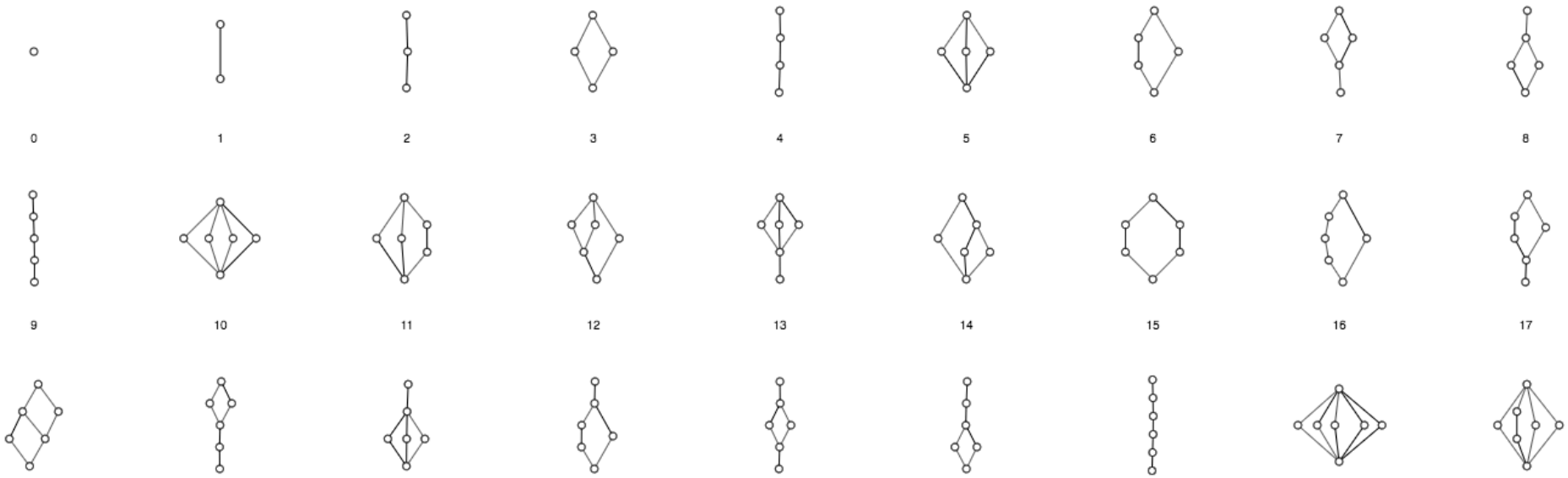
Lattices

A research project with Nathan Lawless.

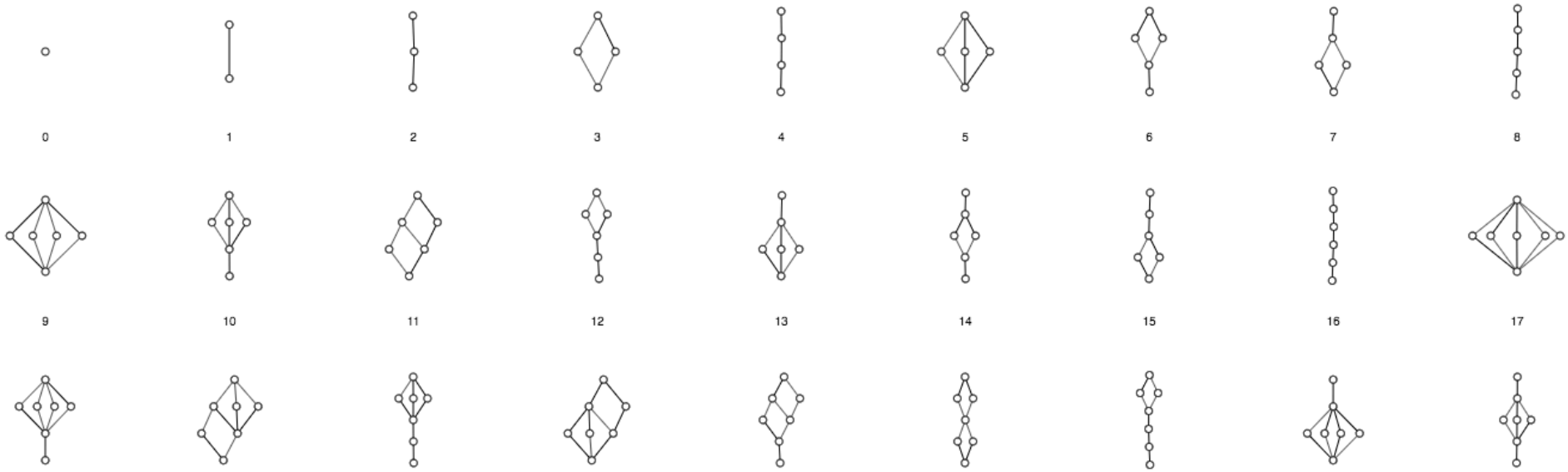
A **lattice** is a set L with two binary operations $\wedge, \vee$ that are

associative	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	$(x \vee y) \vee z = x \vee (y \vee z)$
commutative	$x \wedge y = y \wedge x$	$x \vee y = y \vee x$
absorptive	$(x \wedge y) \vee x = x$	$(x \vee y) \wedge x = x$

Elements in a lattice are **partially ordered** by $x \leq y \iff x \wedge y = x$.



Lattices versus modular lattices



Modular Lattices

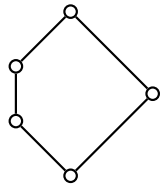
- A **modular lattice** M is a lattice that satisfies the modular law for all $x, y, z \in M$:

$$x \geq z \text{ implies } x \wedge (y \vee z) = (x \wedge y) \vee z$$

or equivalently:

$$x \wedge [y \vee (x \wedge z))] = (x \wedge y) \vee (x \wedge z).$$

- An alternative way to view modular lattices is by **Dedekind's Theorem**: *L is a nonmodular lattice iff N_5 can be embedded into L.*



N_5

  - Examples of modular lattices are:
    - Lattices of subspaces of vector spaces.
    - Lattices of ideals of a ring.
    - Lattices of normal subgroups of a group.

Our Objective

We wanted to come up with an algorithm to efficiently generate all finite modular lattices of a given size n up to isomorphism.

Why is this important?

1. Providing a tool for generation of modular lattices and related structures.
2. The generated modular lattices can provide evidence for conjectures and/or counterexamples.
3. Discovering new structural properties of modular lattices.

Generating Finite Lattices

Heitzig and Reinhold [2000] developed an **orderly algorithm** to enumerate all finite lattices and used it to count the number of lattices up to size 18. To explain their algorithm, we give some definitions related to posets and lattices:

- We say that b is a **cover** of a if $a < b$ and there is no element c such that $a < c < b$, and denote this by $a \prec b$.
- We say an element is an **atom** if it covers the bottom element.
- We call $\uparrow A = \{x \in L \mid a \leq x \text{ for some } a \in A\}$ the **upper set** of A.
- An **antichain** is a subset of L in which any two elements in the subset are incomparable.
- The set of all maximal elements in L is called the first level of L ($Lev_1(L)$). The **(m+1)-th level** of L can be recursively defined by $lev_{m+1}(L) = Lev_1(L - \bigcup_{i=1}^{m} Lev_i(L))$.

Counting Finite Lattices (continued)

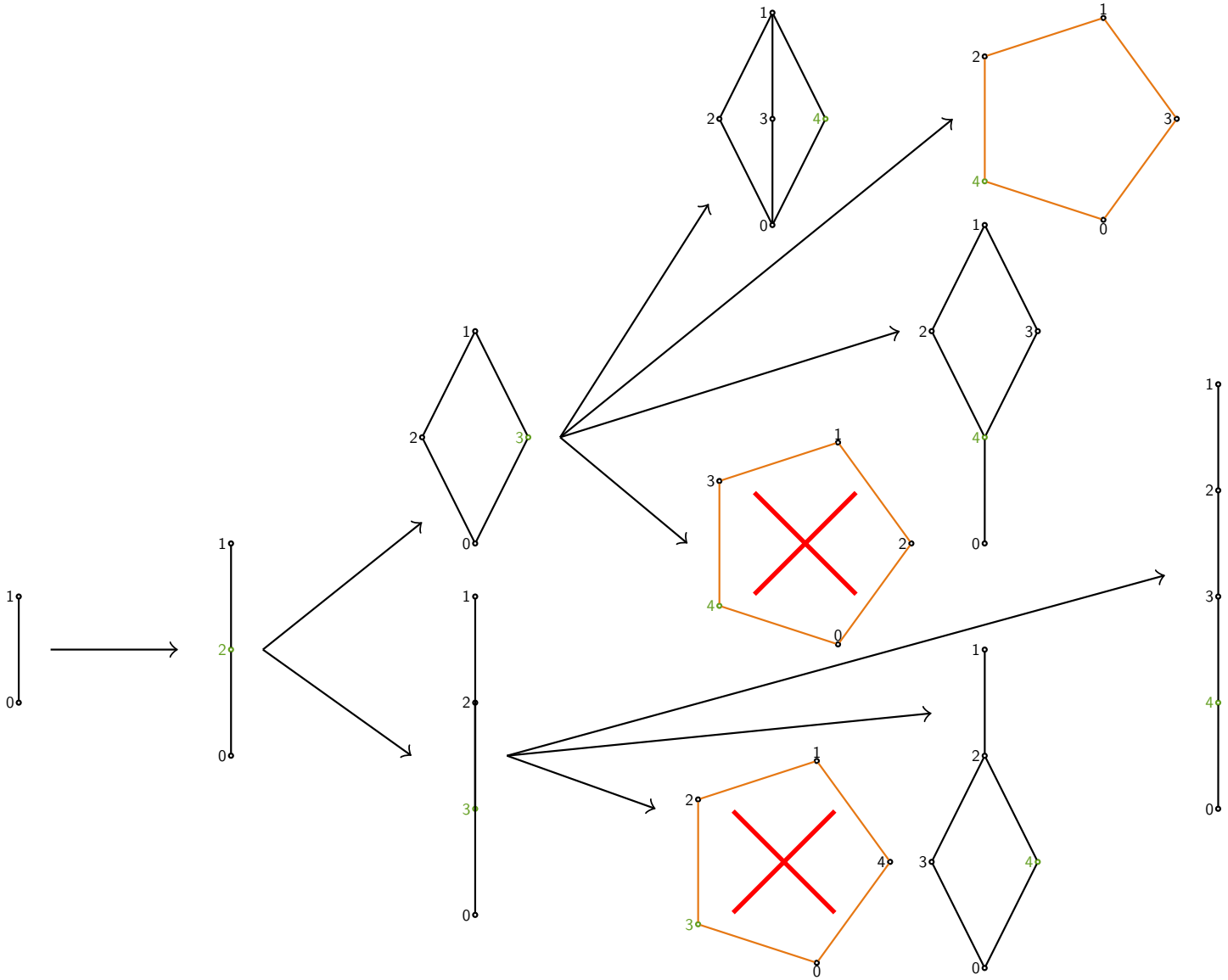
Let A be an antichain of a lattice L. If A satisfies A1, we call it a **lattice-antichain**.

(A1) For any $a, b \in \uparrow A$, $a \wedge b \in \uparrow A \cup \{0\}$.

$\boldsymbol{L^A}$ is constructed from L by adding an atom which is covered by all elements in A. If A satisfies A1, then L^A is a lattice. (Heitzig, 2000).

A recursive algorithm can be formulated that generates for a given natural number $n \geq 2$ exactly all canonical lattices up to n elements starting with the two element lattice:

```
next_lattice(integer m, canonical m-lattice L)
begin
    if m < n then
        for each lattice-antichain A of L do
            if L^A is a canonical lattice then
                next_lattice (m + 1, L^A)
    if m = n then output L
```


1
0
1
2
0
1
2
3
0
1
2
3
4
0
1
2
3
4
0
1
2
3
4
0
1
2
3
4
0
1
2
3
4
0
1
2
3
4
0
1
2
3
4
0

Dealing with Isomorphisms

- In order to select one isomorphic copy, a weight is defined for each lattice. If a lattice has the lowest weight among all it's permutations, it is considered canonical.
- However, this is an expensive check since it requires checking all permutations for each lattice (with some restrictions).
- The algorithm runtime can be improved by introducing a *canonical path extension*, introduced by McKay (1998):
  - We only use one arbitrary representative of each orbit in the lattice antichains of L.
  - When L^A is generated, we perform a "canonical deletion". If L is automorphic to the generated lattice, we consider L^A canonical.

Counting Finite Lattices: Semimodular Lattices

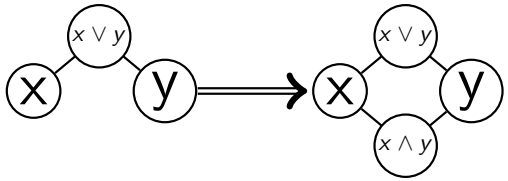
This algorithm can be modified such that when a lattice of size n is generated, the algorithm checks if it is (semi)modular.

Since semimodular and modular lattices are a very small fraction of all lattices, we present some results to reduce the search space of the algorithm. Here, $Lev_k(L)$ and $Lev_{k-1}(L)$ denote the bottom and second bottom levels of L respectively.

- **Semimodular Lattices Theorem:** When generating semimodular lattices, for a lattice L, we only consider antichains A which satisfy **A1** and all of the following conditions:
  (A2) $A \subseteq Lev_{k-1}(L)$ or $A \subseteq Lev_k(L)$.
  (A3) If $A \subseteq Lev_k(L)$, there are no atoms in $Lev_{k-1}(L)$.
  (A4) For all $x, y \in A$, x and y have a common cover.

Counting Finite Lattices: Modular Lattices

- **Modular Lattices Theorem:** When generating modular lattices, for a lattice L, we only consider antichains A which satisfy **A1-4** and **(A5)** If $A \subseteq Lev_k(L)$, $Lev_{k-1}(L)$ satisfies lower semimodularity
  (ie: for all $x, y \in Lev_{k-1}(L)$, $x, y \prec x \vee y$ implies $x \wedge y \prec x, y$)



Runtime Analysis

- Calculation of modular lattices of size n takes approximatelly 5.5 times the time used to generate all modular lattices of size $n-1$.
- In order to reach higher numbers, the algorithm was parallelized using Message Passing Interface (MPI).
- Approximately **2 weeks** were required to calculate all modular lattices of size 24 running the algorithm in parallel on 64 CPUs. It is estimated it would have taken **6 month** with the serial version.

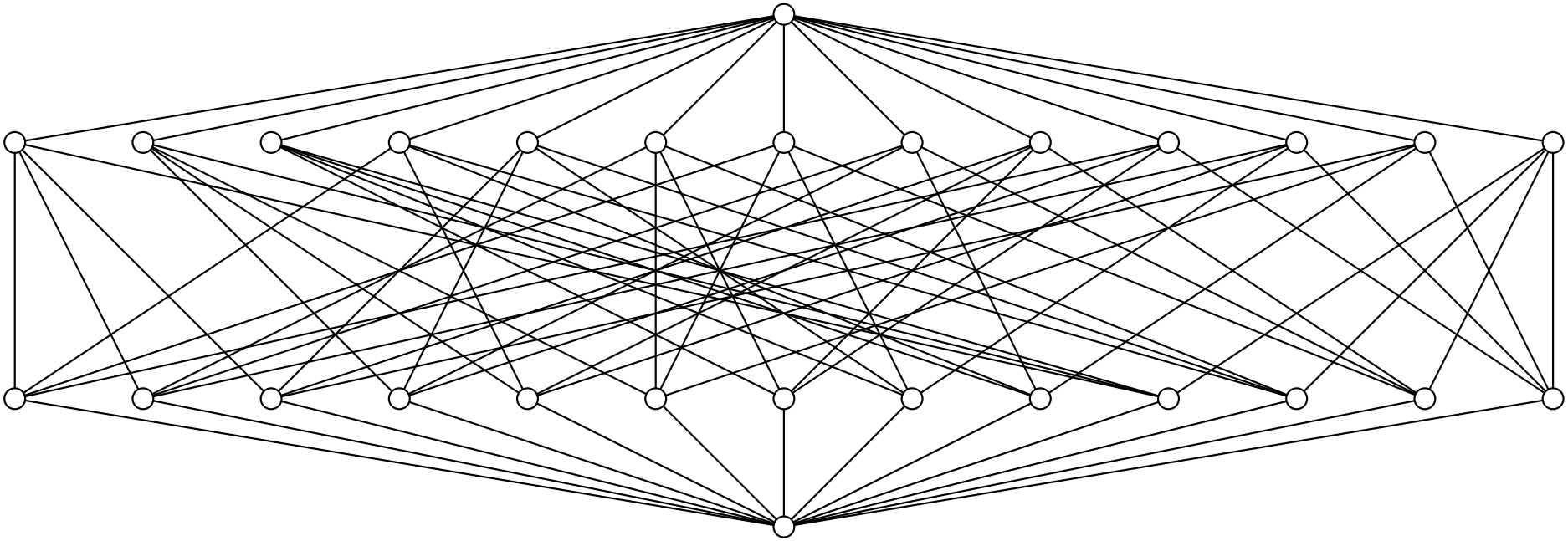
Results

n	# Lattices	# Semimod. Latt.	# Mod. Latt.
3	1	**1**	1
4	2	**2**	2
5	5	**4**	4
6	15	**8**	8
7	53	**17**	16
8	222	**38**	34
9	1 078	**88**	72
10	5 994	**212**	157
11	37 622	**530**	343
12	262 776	**1376**	766

Results

n	# Lattices	# Semimod. Latt.	# Mod. Latt.
3	1	**1**	1
4	2	**2**	2
5	5	**4**	4
6	15	**8**	8
7	53	**17**	16
8	222	**38**	34
9	1 078	**88**	72
10	5 994	**212**	157
11	37 622	**530**	343
12	262 776	**1376**	766
13	2 018 305	**3 693**	**1 718**
14	16 873 364	**10 232**	**3 899**
15	152 233 518	**29 231**	**8 898**
16	1 471 613 387	**85 906**	**20 475**
17	15 150 569 446	**259 291**	**47 321**
18	165 269 824 761	**802 308**	**110 024**
19	**1 901 910 625 578**	**2 540 635**	**256 791**
20	–	**8 220 218**	**601 991**
21	–	**27 134 483**	**1 415 768**
22	–	**91 258 141**	**3 340 847**
23	–	–	**7 904 700**
24	–	–	**18 752 942**

Modular lattice of subspaces of $\mathbb{F}_3^3$



Semilattices and Boolean Algebras

A research project with **Eyad Kurd-Misto** and **James Wimberley**.

A **semilattice** $\langle S, \cdot \rangle$ is a set S with an operation $\cdot$ that satisfies

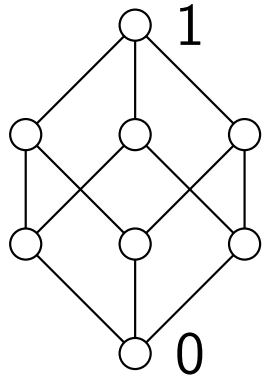
$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad x \cdot y = y \cdot x \qquad x \cdot x = x,$$

known as **associativity**, **commutativity** and **idempotence**.

A **Boolean algebra** $\langle B, \wedge, \vee, \neg, 0, 1 \rangle$ is a lattice with a complement operation $\neg$, a bottom element 0, and a top element 1, such that

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee \neg x = 1 \qquad x \wedge \neg x = 0$$



Groupoids and Boolean Groupoids

A **groupoid** $\langle G, \cdot \rangle$ is a set with a binary operation $\cdot$

A **Boolean groupoid** is an algebra of the form $\langle B, \wedge, \vee, \neg, \cdot, 0, 1 \rangle$ such that $\langle B, \wedge, \vee, \neg, 0, 1 \rangle$ is a Boolean algebra and $\cdot$ is a binary operation satisfying:

$$x \cdot 0 = 0 \cdot x = 0$$
$$x \cdot (y \vee z) = (x \cdot y) \vee (x \cdot z)$$
$$(x \vee y) \cdot z = (x \cdot z) \vee (y \cdot z)$$

It is **integral** if $x \cdot y = 0 \implies x = 0$ or $y = 0$.

For a groupoid $\mathbf{G} = \langle G, \cdot \rangle$, define the **complex algebra** $\mathbf{G}^+ = \langle \mathcal{P}(G), \cap, \cup, \neg, \cdot, \emptyset, G \rangle$. Then $\mathbf{G}^+$ is an integral Boolean groupoid.

Idempotent Boolean Groupoids

Theorem 1. *Every integral square-increasing Boolean groupoid* **B** *is isomorphic to a subalgebra of a complex algebra of an idempotent groupoid* **G**. *If* **B** *is finite* **G** *will be finite and if* **B** *is commutative we can choose* **G** *to be commutative.*

Example.

$\cdot$	a	b
a	$a \vee b$	$a \vee b$
b	$a \vee b$	b

B

$\hookrightarrow$

$\cdot$	a_0	a_1	a_2	b_0	b_1	b_2
a_0	a_0	b_0	b_2	a_0	b_0	b_2
a_1	b_0	a_1	b_1	b_0	a_1	b_1
a_2	b_2	b_1	a_2	b_2	b_1	a_2
b_0	a_0	b_0	b_2	b_0	b_0	b_2
b_1	b_0	a_1	b_1	b_0	b_1	b_1
b_2	b_2	b_1	a_2	b_2	b_1	b_2

G

Figure 1: An integral comm. square-increasing Boolean groupoid **B** and the corresponding commutative idempotent groupoid **G**.

Boolean Semilattices

A **Boolean semilattice** is a Boolean groupoid satisfying the additional axioms:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad x \cdot y = y \cdot x \qquad x \leq x \cdot x$$

A Boolean semilattice **B** is **representable** if there exists a semilattice **S** such that **B** is isomorphic to a subalgebra of $\mathbf{S}^{+}$.

Representations

Lemma 2. *Let* $\mathbf{A}$ *be a finite representable Boolean semilattice.*

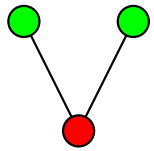
Then every semilattice representing $\mathbf{A}$ *is infinite if and only if there exist disjoint* $x, y \in A$ *such that* $x \vee y \leq x \cdot y$. ($a =$ ●, $b =$ ●).

$\cdot$	a	b
a	a	a
b	a	b

$\mathbf{A}_1$

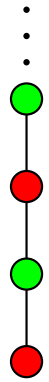
$\cdot$	a	b
a	a	a
b	a	1

$\mathbf{A}_2$



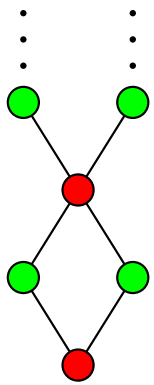
$\cdot$	a	b
a	a	1
b	1	b

$\mathbf{A}_3$



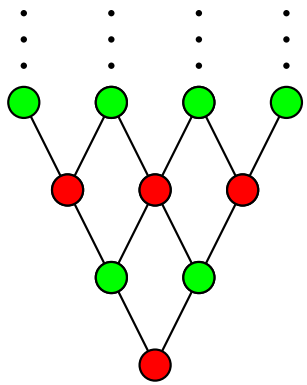
$\cdot$	a	b
a	a	1
b	1	1

$\mathbf{A}_4$



$\cdot$	a	b
a	1	1
b	1	1

$\mathbf{A}_5$



Representations (continued)

Representable Boolean semilattices satisfy the following axioms:

1. $x \wedge y \cdot 1 \leq x \cdot y$
2. $x(x \cdot y \wedge \neg x) \leq x^2 \vee (x \cdot y \wedge \neg x)^2$
3. $u \leq y \cdot z \implies x \cdot u \leq (x \cdot z \wedge v) \cdot y \vee (x \cdot z \wedge \neg v) \cdot u$
4. $x \cdot y \leq x \vee y \implies x^2 \wedge y^2 \leq x \cdot y$

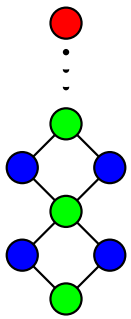
Representations (continued)

Theorem 3. *There are 79 Boolean semilattices with 8 elements that satisfy axioms 1-4. Of these, 72 are known to be representable.*

It is an open problem whether the remaining 7 are representable. Here we only show a few representations.

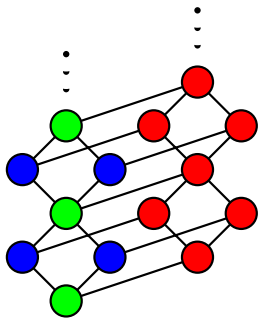
$\cdot$	a	b	c
a	a	b	c
b		b	$b \vee c$
c			$b \vee c$

$\mathbf{B}_1$



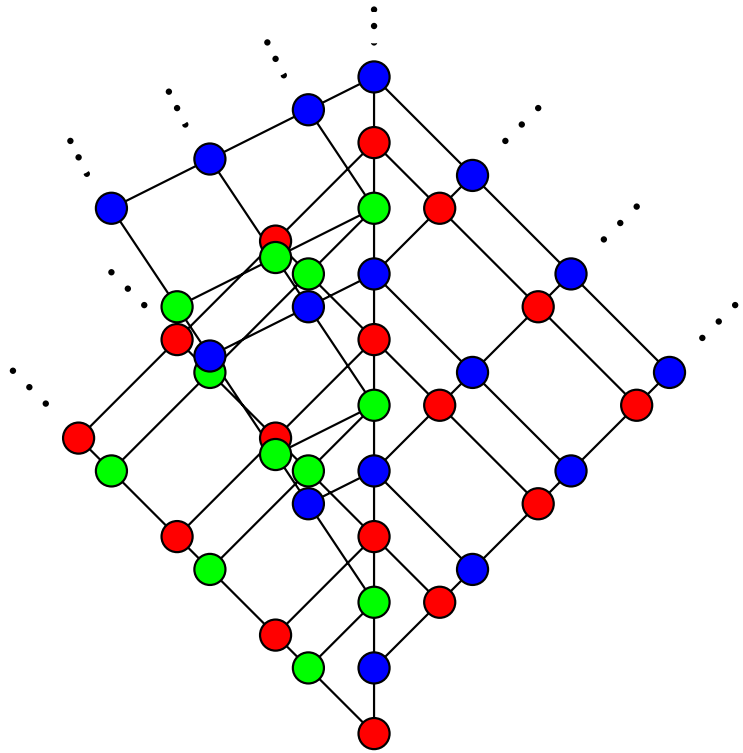
$\cdot$	a	b	c
a	a	$b \vee c$	$b \vee c$
b		b	$b \vee c$
c			$b \vee c$

$\mathbf{B}_{13}$



$\cdot$	a	b	c
a	a	1	1
b		b	1
c			c

$\mathbf{B}_{40}$



Results

Assume $\mathbf{A}, \mathbf{B}$ are complete and atomic Boolean semilattices with sets of atoms $\{a_i : i \in I\}$ and $\{b_j : j \in J\}$ respectively, and that $\mathbf{A}$ is representable by a semilattice $S_{\mathbf{A}}$, and $\mathbf{B}$ is representable by a semilattice $S_{\mathbf{B}}$.

Theorem 4. (Tensor product of $\mathbf{A}, \mathbf{B}$). *Let $\mathbf{A} \otimes \mathbf{B}$ be the algebra that has atoms $\{(a_i, b_j) : i \in I, j \in J\}$ and define*

$$(a, b) \cdot (c, d) = \vee\{(u, v) : 0 \prec u \leq a \cdot^{\mathbf{A}} c, 0 \prec v \leq b \cdot^{\mathbf{B}} d\}$$

Then $S_{\mathbf{A}} \times S_{\mathbf{B}}$ is a representation of $\mathbf{A} \otimes \mathbf{B}$.

Theorem 5. (Ordinal sum of $\mathbf{A}, \mathbf{B}$). *Let $\mathbf{C} = \mathbf{A} \oplus \mathbf{B}$ be the algebra with atoms $\{a_i : i \in I\} \cup \{b_j : j \in J\}$ and define*

$$a_i \cdot^{\mathbf{C}} a_j = a_i \cdot^{\mathbf{A}} a_j \qquad b_i \cdot^{\mathbf{C}} b_j = b_i \cdot^{\mathbf{B}} b_j$$

$$a_i \cdot^{\mathbf{C}} b_j = b_j \cdot^{\mathbf{C}} a_i = a_i$$

for all $i \in I$ and $j \in J$. Then the ordinal sum $S_{\mathbf{A}} \oplus S_{\mathbf{B}}$ is a representation of $\mathbf{A} \oplus \mathbf{B}$.

Summary of second project

We solved an open problem of Cliff Bergman (2015).

In particular we showed that every (finite) integral square-increasing Boolean groupoid is representable by a (finite) idempotent groupoid.

Using a computer program, we showed that there are 79 Boolean semilattices with 8 elements that satisfy the currently known axioms of representable Boolean semilattices.

We found semilattice representations for 72 of them.

The research produced three theorems about constructions that preserve representability.

What is a Partial Algebra?

A research project with **Sarah Alexander** and **Nadia Upegui**.

- A **partial operation** g of arity n on a set A is a function from a subset $D(g)$ of A^n to A.
- A **partial algebra** is a pair $\mathbf{A} = (A, \mathcal{F}^{\mathbf{A}})$ where A is a set and $\mathcal{F}^{\mathbf{A}}$ is a set of operations on A containing at least one partial operation.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	-
2	2	3	-	-
3	3	-	-	-

Separation Algebras

A **separation algebra** (or SA) $\mathbf{A} = (A, +, 0)$ is a partial algebra such that for all $x, y, z \in A$

$$\begin{aligned}
\text{(canc)} \quad & x + y \text{ defined and } x + y = x + z \implies y = z \\
\text{(comm)} \quad & x + y \text{ defined} \implies x + y = y + x \\
\text{(asso)} \quad & (x + y) + z \text{ defined} \implies (x + y) + z = x + (y + z) \\
\text{(iden)} \quad & x + 0 = x
\end{aligned}$$

In short, it is a **cancellative commutative partial monoid**.

Separation algebras are **naturally pre-ordered** by

$$x \leq y \quad \iff \quad \exists w \; x + w = y$$

Any abelian group is a (total) separation algebra ($\leq$ relates all elements).

Generalized Effect Algebras

$(\mathbb{N}, +, 0)$ is another (total) separation algebra.

A **generalized effect algebra** (or GEA) $\mathbf{A} = (A, +, 0)$ is a separation algebra such that for all $x, y \in A$ we have

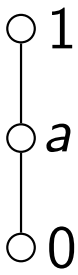
(positivity) $x + y = 0 \implies x = 0 = y$

GEAs are natually **partially** ordered by

$$x \leq y \quad \iff \quad \exists w \; x + w = y$$

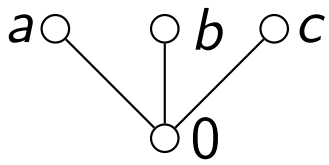
Examples of GE-Algebras

An effect algebra of size 3



$+$	0	a	1
0	0	a	1
a	a	1	$-$
1	1	$-$	$-$

A GEA of size 4



$+$	0	a	b	c
0	0	a	b	c
a	a	$-$	$-$	$-$
b	b	$-$	$-$	$-$
c	c	$-$	$-$	$-$

Why Study Effect Algebras?

Effect algebras have applications in the foundations of **quantum mechanics** and in **probability theory**.

D. J. Foulis and M. K. Bennett [1994]:

If a quantum-mechanical system $\mathcal{S}$ is represented in the usual way by a Hilbert space $\mathcal{H}$, then a self-adjoint operator A on $\mathcal{H}$ such that $\mathbf{0} \leq \mathbf{A} \leq \mathbf{1}$ corresponds to an **effect** for $\mathcal{S}$. Effects are of significance in representing **unsharp** measurements or observations on the system $\mathcal{S}$, and effect valued measures play an important role in stochastic quantum mechanics.

Why Study Separation Algebras?

Let **A** be a separation algebra and for $X, Y \subseteq A$ define $X * Y = \{x + y \mid x \in X, y \in Y\}$, the complex lifting of $+$.

The complex algebra $(\mathcal{P}(A), \cup, \cap, \neg, \emptyset, A, *, \mathrel{-\!\!*}, \{0\})$ is a complete and atomic Boolean algebra with a separating conjunction $*$ and a residual $X \mathrel{-\!\!*} Y = \{z \in A \mid X * \{z\} \subseteq Y\}$.

This is a **Boolean bunched implication algebra**.

In logical form, Boolean bunched implication logic is used in **separation logic** to reason about pointer structures and concurrency of programs.

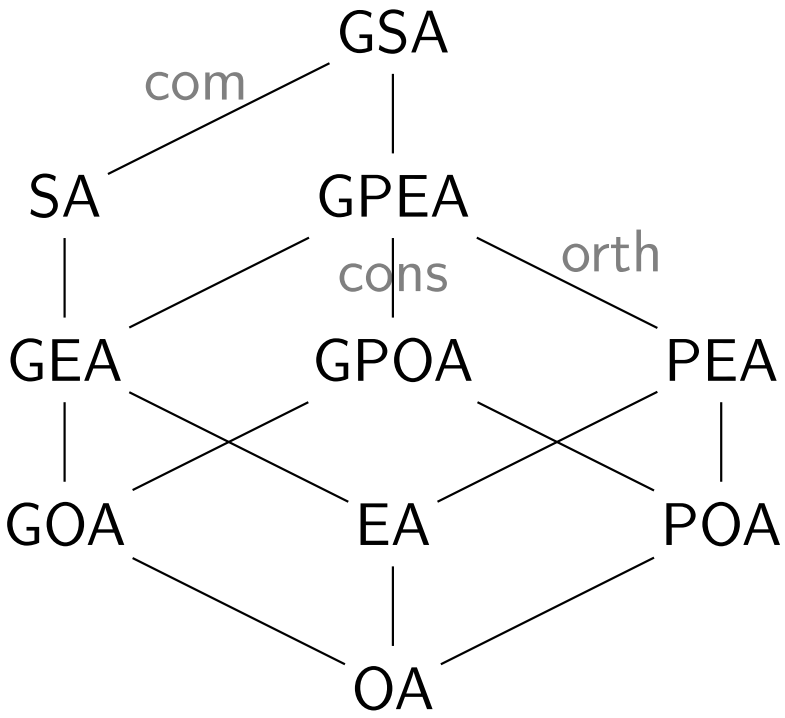
Concrete examples of separation algebras arise from modeling a memory heap as partial functions f from $\mathbb{N}$ (addresses) to V (values).

$f * g$ is defined and $= f \cup g \quad \iff \quad D(f) \cap D(g) = \emptyset.$

Subclasses and Expansions of GPE-algebras

Adding combinations of three independent axioms creates subclasses:

(com) $x + y = y + x$ (**commutative**)
(orth) $x + y = 1 \iff y = x^{\sim} \iff x = y^{-}$ (**orthocomplement**)
(cons) $x + x$ defined $\implies x = 0$ (**consistent**)



G = Generalized, S = Separation, P = Pseudo, E = Effect, O = Ortho

From Separation Algebras to Effect Algebras

An element v is **invertible** if there exists w such that $vw = e = wv$

A^* denotes the set of invertible elements of a GS-algebra $\mathbf{A}$.

The inverse of v, if it exists, is unique and is denoted by v^{-1}.

Lemma

Let $\mathbf{A}$ *be a generalized separation algebra. Then*

1. A^* *is the bottom equivalence class* $[e]$ *of the poset* $A/{\equiv} = (\{[x] : x \in A\}, \leq)$,
2. $\mathbf{A}^* = (A^*, \cdot, e, ^{-1})$ *is a (total) group and is a closed subalgebra of* $\mathbf{A}$,
3. $x \equiv y$ *holds if and only if* $x \in yA^*$, *and*
4. $\equiv$ *is the identity relation if and only if* e *is the only invertible element.*

From Separation Algebras to Effect Algebras

Every separation algebra can be collapsed in a unique way to a largest generalized effect algebra.

Hence a substantial part of the structure theory of separation algebras is covered by results about generalized effect algebras.

Theorem

For a GS-algebra $\mathbf{A}$,

1. *the relation* $\equiv$ *is a closed congruence,*
2. $\mathbf{A}/\equiv$ *is a GPE-algebra,*
3. *the congruence classes of* $\equiv$ *all have the same cardinality, and*
4. *if* $h : \mathbf{A} \to \mathbf{B}$ *is a homomorphism and* $\mathbf{B}$ *is a GPE-algebra then there exists a unique homomorphism* $g : \mathbf{A}/\equiv \to \mathbf{B}$ *such that* $g \circ \gamma = h$ *(where* $\gamma : \mathbf{A} \to \mathbf{A}/\equiv$ *is the canonical homomorphism* $\gamma(x) = [x]$*).*

From abelian groups and effect algebras to separation algebras

Theorem

Let $\mathbf{G}$ *be an abelian group and* $\mathbf{B}$ *a GE-algebra.*
Then $\mathbf{A} = \mathbf{G} \times \mathbf{B}$ *is a separation algebra with* $\mathbf{A}^* = \mathbf{G} \times \{e\}$.

Similarly the product of a group and a GPE-algebra is a GS-algebra.

Proof.

The product of separation algebras is again a separation algebra since this class of algebras is defined by quasi-identities.
The element $(g, e) \in A$ has inverse (g^{-1}, e).
Now let $b \in B$. If (g, b) has an inverse (h, c) then $bc = e$, hence by positivity of B we have $b = e$.
Therefore $\mathbf{A}^* = \mathbf{G} \times \{e\}$. □

Counting Effect algebras and Separation algebras

n	OA	POA	GOA	EA	PEA	GPOA	GEA	SA	GPEA	GSA
2	1	1	1	1	1	1	1	2	1	2
3	0	0	1	1	1	1	2	3	2	3
4	1	1	2	3	3	2	5	8	5	8
5	0	1	2	4	5	3	12	13	13	14
6	1	2	4	10	12	7	35	39	42	48
7	0	2	8	14	19	19	119	120	171	172
8	2	5	18	40	52	68	496	507	1020	1037
9	0	4	42	60	84	466	2699	2703	11742	11749
10	2	10	156	172	240	8740	21888	21905	322918	
11	0	9	834	282	418		292496	292497		

Table: Number of partial algebras in each class

O = Ortho, P = Pseudo, G = Generalized, E = Effect, S = Separation

Some observations

Some observations

- There are open research problems in abstract algebra accessible to undergraduates.

Some observations

- There are open research problems in abstract algebra accessible to undergraduates.
- In classical areas (groups, rings, fields) it is difficult to find open problems where there is chance of success.

Some observations

- There are open research problems in abstract algebra accessible to undergraduates.
- In classical areas (groups, rings, fields) it is difficult to find open problems where there is chance of success.
- Weaken the axioms slightly and consider problems about finite structures.

Some observations

- There are open research problems in abstract algebra accessible to undergraduates.
- In classical areas (groups, rings, fields) it is difficult to find open problems where there is chance of success.
- Weaken the axioms slightly and consider problems about finite structures.
- Ordered structures allow for nice diagrams where one can discover ideas.

Some observations

- There are open research problems in abstract algebra accessible to undergraduates.
- In classical areas (groups, rings, fields) it is difficult to find open problems where there is chance of success.
- Weaken the axioms slightly and consider problems about finite structures.
- Ordered structures allow for nice diagrams where one can discover ideas.
- Computational methods can be very useful.

Some observations

- There are open research problems in abstract algebra accessible to undergraduates.
- In classical areas (groups, rings, fields) it is difficult to find open problems where there is chance of success.
- Weaken the axioms slightly and consider problems about finite structures.
- Ordered structures allow for nice diagrams where one can discover ideas.
- Computational methods can be very useful.
- Automated theorem provers like Prover9/Mace4 are helpful (no programming needed).

References

S. Alexander, P. Jipsen and N. Upegui, **On the structure of generalized effect algebras and separation algebras**, in proc. 17th Int. Conference on Relational and Algebraic Methods in Computer Science (RAMiCS), Groningen, Netherlands, LNCS Vol 11194, Springer (2018), 148–165

P. Jipsen, M. E. Kurd-Misto and J. Wimberley, **On the representation of Boolean magmas and Boolean semilattices**, in Outstanding Contributions to Logic by Hajnal Andréka and Istvan Németi, Springer (to appear)

P. Jipsen and N. Lawless, **Generating all finite modular lattices of a given size**, Algebra Universalis, 74(3) (2015), 253–264

Thanks!