The algebra of a semigroup from Logic and Theoretical Computer Science

Peter M. Hines
Y.C.C.S.A. , Univ. York

Dept. of Mathematics
Semigroup Seminars

York – April 2020

Disclaimer:

These slides were the basis for a group discussion among the York mathematics semigroup theorists.

They should not be read as the record of a more formal presentation.

The overall topic:

An important monoid from logic & computer science

- Introduced in 1997 / 1998, in a PhD thesis on categorical logic (PMH97).
- Based on the symmetric inverse monoid on $\mathbb{N}$.
- A concrete example of some (very deep) abstract category theory & logic.
- No standard accepted name / notation:

> *"The endomorphism monoid of an idempotent self-dual object in a particle-style compact closed category".*

. . . let's call it $\mathfrak{R}$.

Motivation & Applications (I)

Notable **logical** / **computational** features of $\mathfrak{R}$

- Models the dynamics of logical deduction.
- A concrete model of *untyped lambda calculus*.
- Also models Turing machine dynamics.
- Based entirely on partial reversible functions.

Motivation & Applications (II)

Notable **categorical features** of $\mathfrak{R}$

- It has a **tensor**: $\_ \star \_ : \mathfrak{R} \times \mathfrak{R} \to \mathfrak{R}$
  satisfying all the *usual axioms* from category theory...
- It has a **closure** operator: $[\_ \to \_] : \mathfrak{R}^{op} \times \mathfrak{R} \to \mathfrak{R}$
  again, satisfying all the right axioms.

It is a monoidal closed monoid (i.e. single-object category)

Motivation & Applications (III)

As a consequence of **closure** and **having a single object**, it is a **reflexive** monoid:

— the monoid of an object isomorphic to its own function space.

Other known examples:

D. Scott's order-theoretic models of λ calculus (1972).
– see also, J. Lambek & P. Scott's C-monoids (1986).

Motivation & Applications (III)

It also has many other significant categorical properties:

1. Dualities
   (i.e. anti-isomorphisms $(\_)^* : \mathfrak{R}^{op} \to \mathfrak{R}$).
2. Frobenius algebras
3. (Categorical) compactness
4. Yang-Baxter operators
5. Traces
6. ...

Well-studied properties ...

traditionally associated with (Oxford-style) categorical quantum mechanics — although (for reasons to be explained) $\mathfrak{R}$ has never been interpreted in these terms.

Semigroup-theoretic properties

Not much known from a purely semigroup-theoretic viewpoint!

Some very basic properties that have commonly
been assumed for *many years* are in fact incorrect.

The actual situation is *more interesting*, but poorly understood!

A disclaimer

It appears harder to prove monoid-theoretic properties
than to prove facts about logical / categorical interpretations.

Even closure under composition is decidedly non-trivial.

What we do know(!)

We do recover embeddings of *interesting algebras*

- Thompson's groups $\mathcal{F}$ and $\mathcal{V}$.
- Nivat & Perot's polycyclic monoids
- Grigorchuk's group $\mathfrak{G}$
- The Temperley-Lieb algebra
- Lambek's pregroups
- ...

An important point

Given the ability to model universal computation, we expect to be able to find *any* computable monoids, but the above appear in a **structurally important** way.

The actual construction!

The starting point is $B(\mathbb{N})$, the monoid of partial injections on the natural numbers.

This is an inverse monoid:

Every $a \in B(\mathbb{N})$ has a **unique** generalised inverse $a^{\ddagger}$ satisfying

$$aa^{\ddagger}a = a \quad \text{and} \quad a^{\ddagger}aa^{\ddagger} = a^{\ddagger}$$

A key point:

uniqueness of generalised inverses

$\Leftrightarrow$

commutativity of idempotents.

Joins and partial orders

Inverse semigroups have a **natural partial order**:

$$a \leqslant b \quad \text{iff} \quad a = be \quad \text{for some } e^2 = e$$

$B(\mathbb{N})$ is also closed under arbitrary [1] joins of orthogonal elements.

A Reminder ...

An indexed set $\{f_j\}_{j \in J}$ is **orthogonal** iff

$$f_j^{\ddagger} f_i = 0 = f_j f_i^{\ddagger} \quad \forall i \neq j \in J$$

(i.e. f_i and f_j have disjoint domains & images).

[1] Not just finite – we are not working with Boolean inverse monoids

Matrices of inverse monoids

We are interested in inverse monoids of (2×2) matrices over the symmetric inverse monoid $B(\mathbb{N})$.

— equivalently, the symmetric inverse monoid on $\mathbb{N} \uplus \mathbb{N}$.

An alternative viewpoint

It is well-known that

$$\mathbb{N} \cong \mathbb{N} \uplus \mathbb{N}$$

(Hilbert's hotel / Cantor pairings, etc.) so we *could* just work with $B(\mathbb{N})$.

Doing so would obscure a lot of structure & make the algebra much more complex.

Matrix representations

Given an arrow $f \in B(\mathbb{N} \uplus \mathbb{N})$, we may write it as a (2×2) matrix over $B(\mathbb{N})$.

$$f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

by "taking projections".

A necessary and sufficient condition for matrix representations

The rook matrix condition

- Arrows in the same *row* have *disjoint images*.
- Arrows in the same *column* have *disjoint domains*.

Rook matrix conditions, explicitly

The **rook matrix** condition:

> *"Arrows in the same* row *have* disjoint images *and arrows in the same* column *have* disjoint domains*. "*

may be given algebraically

The rook conditions

This are equivalent to:

(disjoint images) $b^{\ddagger}a = 0 = d^{\ddagger}c$

(disjoint domains) $ca^{\ddagger} = 0 = db^{\ddagger}$

Composing matrices of partial injections

Given two such matrices, composition is given by the **usual formula**:

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea \vee fc & hd \vee gb \\ ga \vee hc & hd \vee gb \end{pmatrix}$$

- Multiplication is replaced by composition in $b(\mathbb{N})$,
- Addition is replaced by join w.r.t. the natural partial order.

Inverting matrices of partial injections

Taking generalised inverses also looks familiar!

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\ddagger} = \begin{pmatrix} a^{\ddagger} & c^{\ddagger} \\ b^{\ddagger} & d^{\ddagger} \end{pmatrix}$$

A direct analogy to the

"Reflect along the diagonal, and take adjoints"

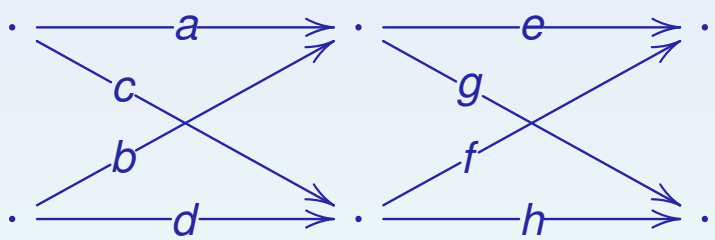
familiar from linear algebra.

Treating things graphically ...

Given rook matrices

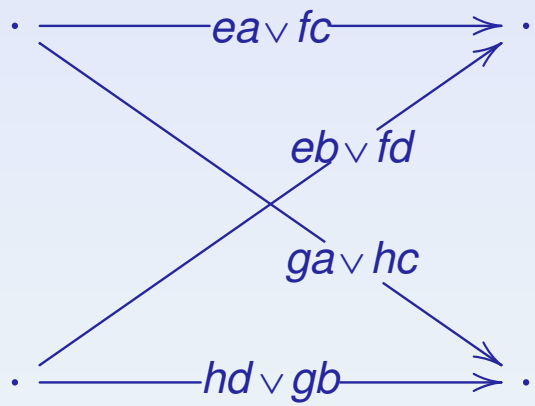
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in B(\mathbb{N} \uplus \mathbb{N})$$

let us draw these as digraphs:



Summing over paths ...

Matrix composition then becomes the standard ‘sum over paths from source to target’:



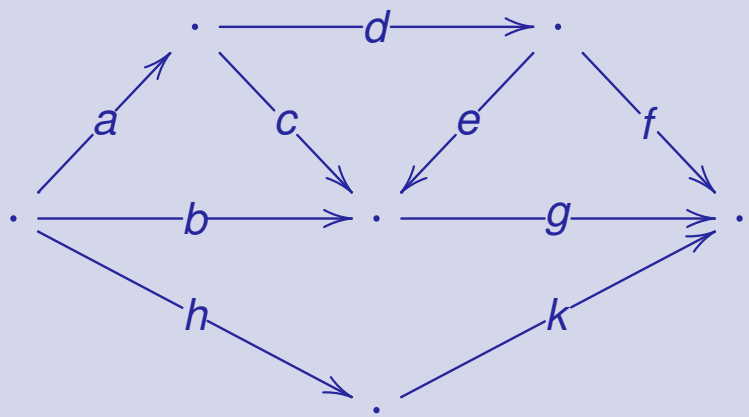
The motivation for the *rook matrix* condition is clear and ensures this is well-defined.

Rooks revisited (I)

The rook matrix conditions themselves can be treated graphically:

A reminder ...

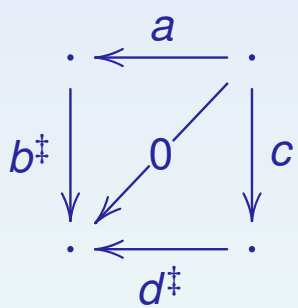
A diagram over a *category* or a *monoid* is said to **commute** iff all composites along paths with the same source and target are equal.

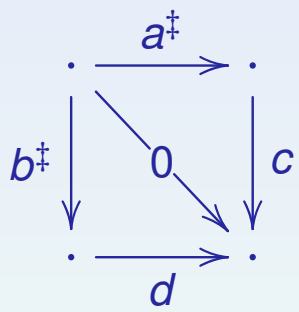


Rooks revisited (II)

Draw the rook conditions as commuting diagrams:

A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B(\mathbb{N} \uplus \mathbb{N})$ is a rook matrix iff the following two diagrams commute:

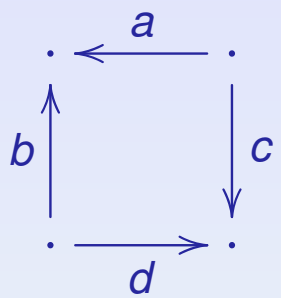




From a condition to a definition

Let us treat this as a *definition*:

A **rook square** is a diagram over $B(\mathbb{N})$



such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a rook matrix.

Rook squares are in 1:1 correspondence with elements of $B(\mathbb{N} \uplus \mathbb{N})$.

Simply drawing the digraph representation of matrices in a planar fashion.

Finally .. the monoid in question

Let us (finally!) define the monoid $\mathfrak{R}$ to have:

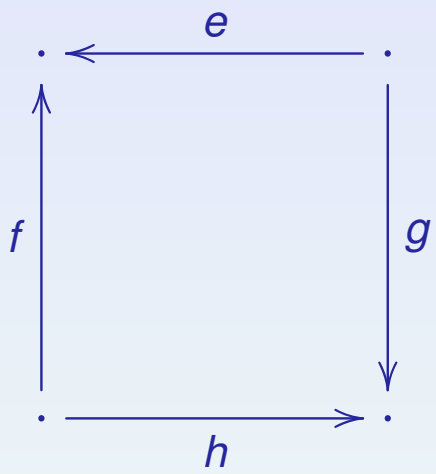
- As **elements**, all **rook squares** over $B(\mathbb{N})$.
- As **composition**, a **summing over paths** construction that preserves the 'rook squares' property.

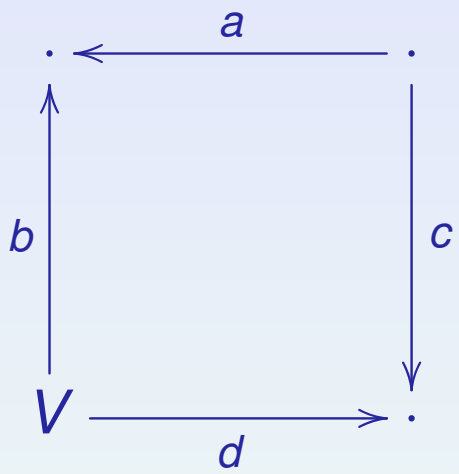
However, there are three possibilities for composing 4-tuples in a way that preserves the 'rook' property:

- The familiar 'matrix composition'.
- Two other less well known possibilities.

A ‘summing over paths’ construction

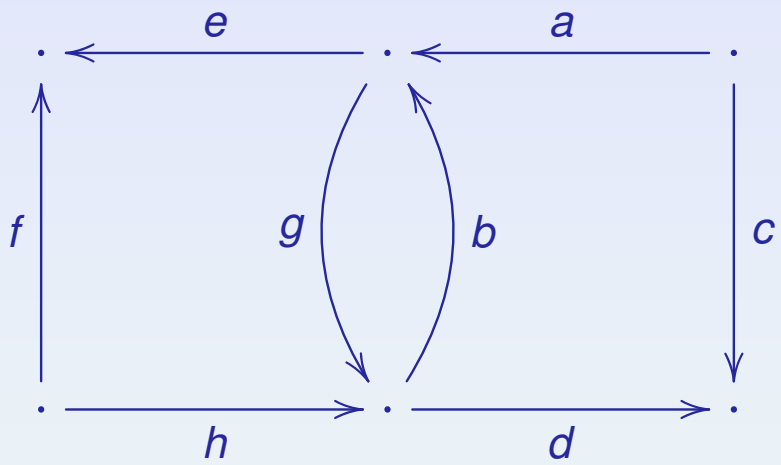
Consider two rook squares:





The ‘horizontal’ composition (I)

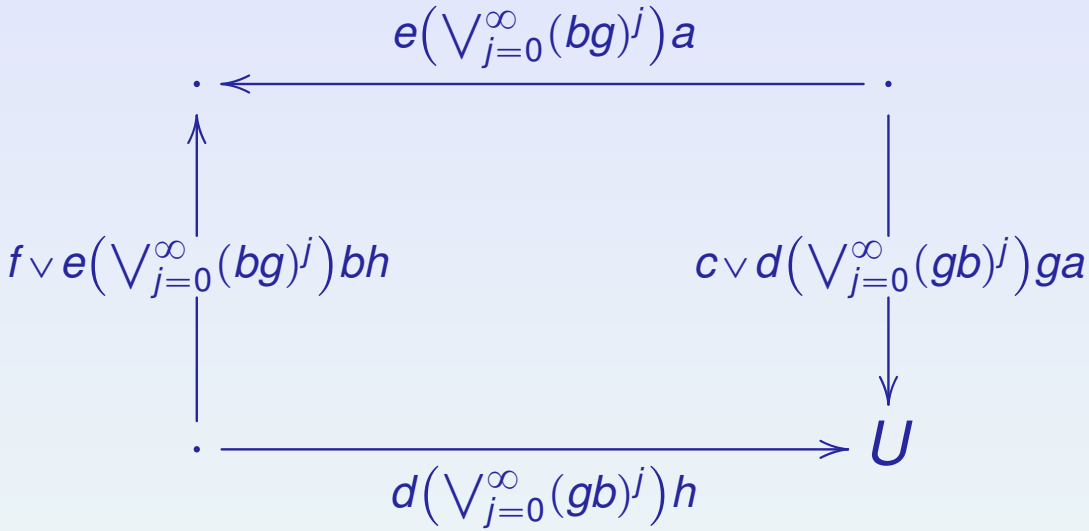
Let us paste these together along a common edge



and take the ‘join over paths’.

The ‘horizontal’ composition (II)

The intuition is simple ...



although we need some fairly complex (infinite) joins!

Some non-trivial results

With these elements, and this composition, we can show:

- All the above joins are well-defined.
- The result is also a rook square.
- This composition is associative.
- There is an identity element.

This is the monoid $\mathfrak{R}$

Where does this come from?

In 1996, two important categorical constructions were published:

- The **Int** construction of A. Joyal, R. Street, and D. Verity.
- The **GoI** construction of S. Abramsky.

These used very different conventions, but were gradually shown to be equivalent[2]

JSV gave the example of **relations on sets** —

PMH97 showed closure of **partial injections** & **rook squares** under the same composition and operations.

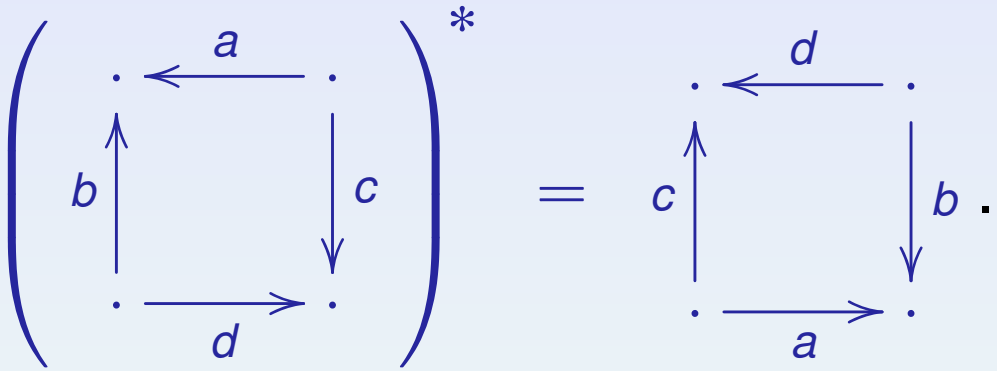
[2] (For category theorists – in the symmetric case ...)

Category theory, or algebra?

We have a categorical dual:

$$(\_)^* : \mathfrak{R}^{op} \to \mathfrak{R}$$

simply given by



This is an anti-isomorphism; however, it is *not* a generalised inverse.

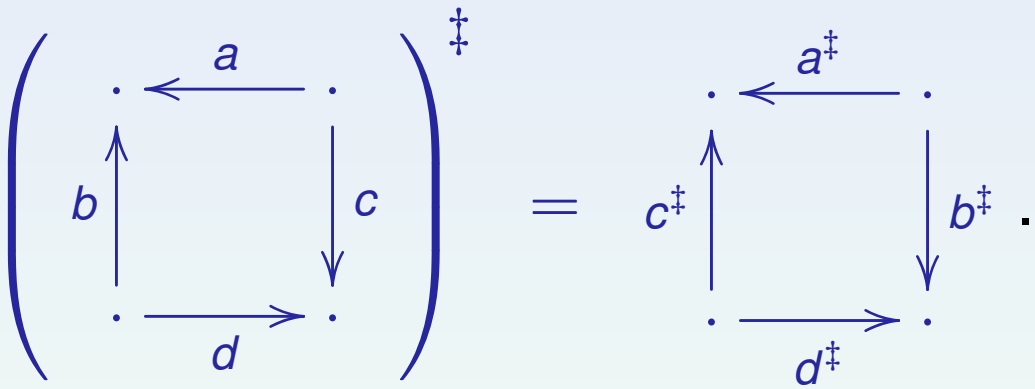
Do we have generalised inverses??

Is $\mathfrak{R}$ an inverse monoid?

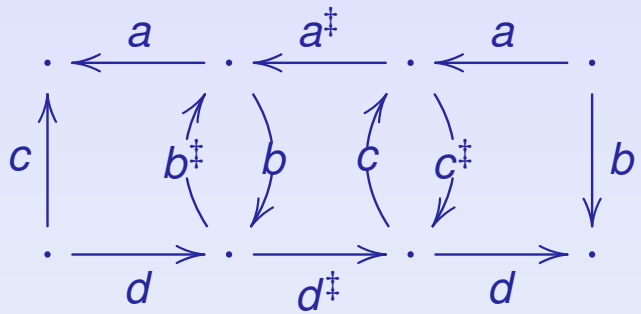
Recall the generalised inverse of a rook matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\ddagger} = \begin{pmatrix} a^{\ddagger} & c^{\ddagger} \\ b^{\ddagger} & d^{\ddagger} \end{pmatrix}$$

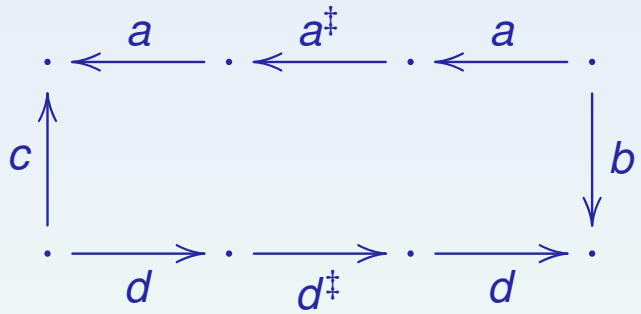
Making the obvious definition for rook squares:



Checking the defining conditions (I)

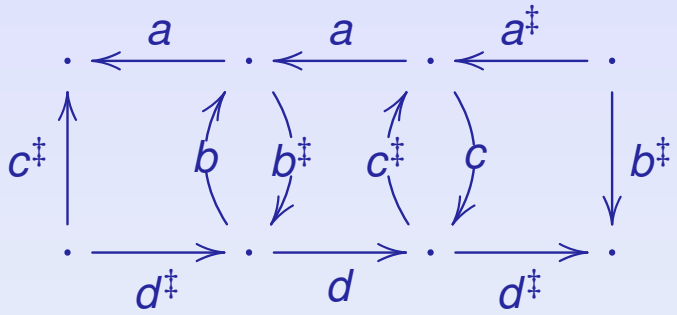


By the rook square conditions, this is:

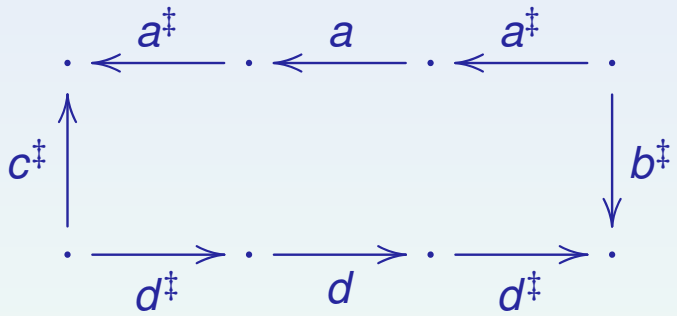


We recall that $aa^\ddagger a = a$ and $dd^\ddagger d = d$

Checking the defining conditions (II)



By the rook square conditions, this is:



We again recall that $a^\ddagger a a^\ddagger = a^\ddagger$ and $d^\ddagger d d^\ddagger = d^\ddagger$

The inverse and the dual

We have a **generalised inverse** anti-isomorphism

$$(\_)^{\ddagger} : \mathfrak{R} \to \mathfrak{R}$$

We also have the **categorical dual** anti-isomorphism

$$(\_)^{*} : \mathfrak{R} \to \mathfrak{R}$$

somewhat neatly, these commute with each other:

$$\left((\_)^{\ddagger}\right)^{*} = \left((\_)^{*}\right)^{\ddagger}$$

Is $\mathfrak{R}$ an inverse monoid?

If so, can we describe it as partial injections on some set?

Checking the defining conditions (III)

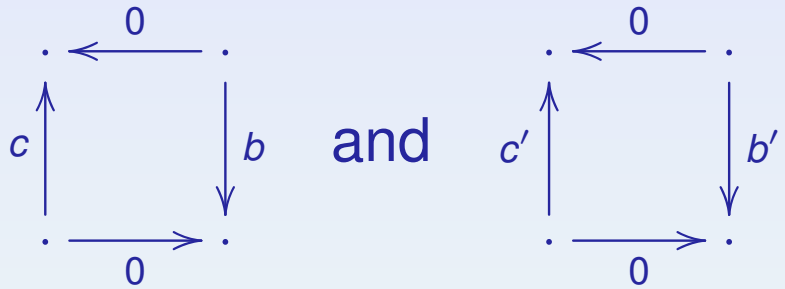
We have generalised inverses ... are they unique?

Equivalently, do all idempotents commute??

$\mathfrak{R}$ is not an inverse monoid

Lemma: Not all idempotents of $\mathfrak{R}$ commute.

Proof For arbitrary $b, b', c, c' \in B(\mathbb{N})$, the following are idempotent:



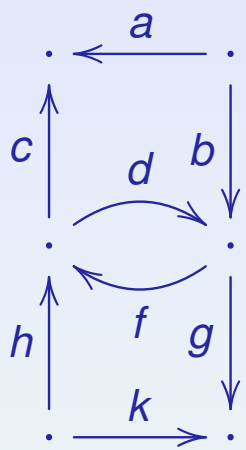
However, they commute precisely when $b = b$ and $c = c'$.

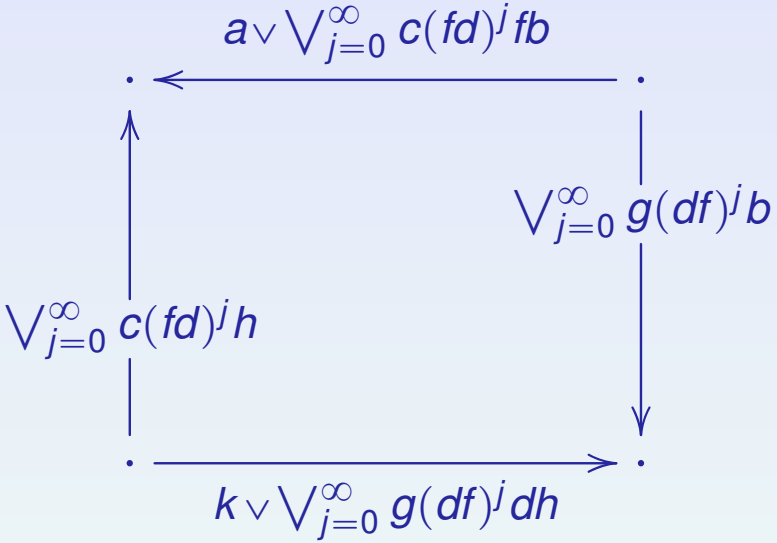
Corollary Generalised inverses are *not unique*.

We do have a more subtle form of uniqueness ...

The ‘vertical’ composition

We can also compose squares by pasting vertically:





A tale of two compositions

These are refered to in PMH97 as *horizontal* and *vertical* composition.

Let us denote them by:

$$\circ_h : \mathfrak{R} \times \mathfrak{R} \to \mathfrak{R} \quad \text{and} \quad \circ_v : \mathfrak{R} \times \mathfrak{R} \to \mathfrak{R}$$

respectively.

It is almost immediate that

$$(\mathfrak{R}, \circ_h) \;\cong\; (\mathfrak{R}, \circ_v)$$

Some historical perspective

Recall: In 1996, two important categorical constructions were published:

- The **Int** construction of A. Joyal, R. Street, and D. Verity.
- The **GoI** construction of S. Abramsky.

These *used very different conventions*.

horizontal & vertical compositions

Our $\circ_h$ and $\circ_v$ compositions correspond to the conventions of JSV and SA, respectively.

When working with $\mathfrak{R}$, it is more enlightening to treat them as **two distinct operations on the same structure!**

Back to uniqueness

- Generalised inverses in $\mathfrak{R}, \circ_h$ are **not unique**.
- Generalised inverses in $\mathfrak{R}, \circ_v$ are **not unique**.

What we do have:

Given a rook square S, then:

1. $S^\ddagger$ is a generalised inverse of S w.r.t. the horizontal composition.
2. $\left(S^\ddagger\right)^*$ is a generalised inverse of S w.r.t. the vertical composition.
3. $S^\ddagger$ is the **unique** rook square satisfying 1. and 2.

A ‘few’ questions

1. Is there a name for such monoids / generalised inverses?
2. What is the relationship between $\circ_h$ and $\circ_v$?

   They are not — as has been claimed — related by an interchange law.
3. What is the structure of the idempotents of $(\mathfrak{R}, \circ_h)$?
4. Which elements are idempotent w.r.t. both compositions?
5. Are the ‘group-like’ elements closed under composition?
6. Now we know that not all idempotents commute,
   can / should we take the quantum-like structures seriously?
7. What kind of purely semigroup-theoretic results can we prove ?
   – we don’t even know what Green’s relations look like!