Elementary arithmetic as semigroup & category theory

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

Dept. of Mathematics
Semigroup Seminars

York – June 2020

The overall topic:

Treating elementary arithmetic as inverse semigroup theory
via the theory of (monotone) partial injections,
and transformations of Cantor space.

One outcome :

Interesting (new?) inverse monoids that generalise

Nivat & Perot's **Polycyclic Monoids**
(a.k.a. the logicians' *dynamical algebra*)

in a natural way.

Disclaimer : These slides have been updated following the talk, in order to correct some attributions / references.

Practical motivation (I)

A follow-up to a talk given at

International Conference on Mathematics,
Engineering, & Technology
(ICoMET Jan. 2020 — Sukkur, Pakistan)

on practical & useful applications of inverse semigroup theory.

Applied inverse semigroup theory??

Modeling security holes due to Race Conditions
via representations of polycyclic monoids
as *monotone partial injections* on $\mathbb{N}$

Based on a very practical application :
"**Hacking Starbucks for unlimited free coffee**" – Egor Homakov

Practical motivation (II)

Today's topic appears to give a route towards:

provably post-quantum cryptography

Post-quantum crypto. searches for protocols that are *believed* not to be susceptible to attacks by quantum computers.

A more general / ambitious aim :

Can *prove* certain problems are necessarily immune to quantum attacks?

Not the subject of today's talk ...

Category theory

Not a prerequisite of the rest of the talk!

Everything in this talk is very strongly categorical

- This is based on treating the natural numbers $\mathbb{N}$ as a category.
- Many categorical properties are vast generalisations of properties of $\mathbb{N}$.
- Semigroup-theoretic constructions, and category-theoretic constructions often coincide.

I will do my best to hide the category theory

The natural numbers as a category (I)

Treating $\mathbb{N}$ as a category :

- Objects – these are $\{0, 1, 2, 3, \ldots\}$
- Arrows – there is a unique arrow $a \rightarrow b$ iff $a \leqslant b$.

$(\mathbb{N}, \_ \times \_, \_ + \_)$ is a distributive category :

- Two **monoidal tensors** $(\_ + \_)$ and $(\_ \times \_)$
- satisfying a distributive law

The natural numbers as a category (II)

Treating $\mathbb{N}$ as a category :

- Objects – these are $\{0, 1, 2, 3, \ldots\}$
- Arrows – there is a unique arrow $a \to b$ iff $a \leqslant b$.

As pointed out in

> *"Metric spaces, generalised logics & closed categories" – W. Lawvere (1972)*

We have **monoidal closure** :

- $(\mathbb{N}, \_ + \_)$ is monoidal closed
- The **internal hom** functor $[\_ \to \_]$ is given by **monus**

$$x \stackrel{\bullet}{-} y \; = \; \begin{cases} x - y & x \geqslant y, \\ 0 & \text{otherwise.} \end{cases}$$

The natural numbers as a category (III)

Treating $\mathbb{N}$ as a category :

- Objects – these are $\{0, 1, 2, 3, \ldots\}$
- Arrows – there is a unique arrow $a \rightarrow b$ iff $a \leqslant b$.

We have categorical traces

- Both $(\mathbb{N}, \_ \times \_)$ and $(\mathbb{N}, \_ + \_)$ are **traced**.
- The trace of $(\mathbb{N}, \_ \times \_)$ is

$$Tr^u(x) = \begin{cases} \frac{x}{u} & x \ (mod\ u) = 0 \\ \perp & \text{otherwise.} \end{cases}$$

- The trace of $(\mathbb{N}, \_ + \_)$ is

$$Tr^u(x) = \begin{cases} x - u & x \geqslant u \\ \perp & \text{otherwise.} \end{cases}$$

The Category Theory

is now over ...

... at least, explicitly!

Our starting point :

Recall $\mathcal{I}(\mathbb{N})$, the inverse monoid of partial injections on the natural numbers.

- Every $a \in \mathcal{I}(\mathbb{N})$ has a **unique** generalised inverse $a^\ddagger$ satisfying
$$aa^\ddagger a = a \quad \text{and} \quad a^\ddagger aa^\ddagger = a^\ddagger$$

- Uniqueness of generalised inverses $\Leftrightarrow$ commutativity of idempotents.
- Idempotents are simply partial identities.
- $aa^\ddagger$ and $a^\ddagger a$ are partial identities on the *domain* and *image* of a, called the **initial** and **final idempotents**.

An interesting submonoid

Let us consider $m\mathcal{I}(\mathbb{N})$ — the submonoid of *monotone* partial injections.

$$x \leqslant y \;\Rightarrow\; f(x) \leqslant f(y) \quad \forall x, y \in dom(f)$$

Basic properties :

1. $\mathbb{N}$ is totally ordered $\Rightarrow$

   $m\mathcal{I}(\mathbb{N})$ is an inverse monoid

2. $\mathbb{N}$ is well-ordered $\Rightarrow$

   Every element $f \in m\mathcal{I}(\mathbb{N})$ is uniquely determined by its initial and final idempotents, $f^\ddagger f$ and $ff^\ddagger$.

In particular, 2. is a very strong property!

A straightforward corollary ...

The kind of results that are immediate :

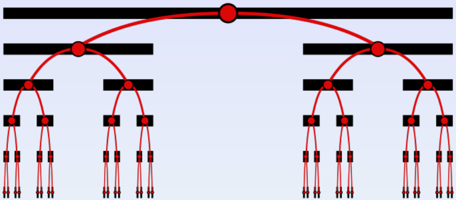
Let S be a (0-)bisimple inverse submonoid of $m\mathcal{I}(\mathbb{N})$.

As every element $f \in m\mathcal{I}(\mathbb{N})$ is uniquely determined by its initial and final idempotents,

S is uniquely determined by its lattice of idempotents $E(S)$.

From $m\mathcal{I}(\mathbb{N})$ to Cantor space

Elements of $m\mathcal{I}(\mathbb{N})$ correspond to pairs of points of Cantor space $\mathfrak{C}$.



Formally, one-sided infinite strings over $\{0, 1\}$,

$$c = 0100101101\ldots$$

or equivalently, functions from $c : \mathbb{N} \to \{0, 1\}$.

Idempotents as Cantor points

Elements of $m\mathcal{I}(\mathbb{N})$ are in bijective correspondence with **balanced pairs** of Cantor points.

i.e. pairs (c_d, c_a) satisfying :

$$\sum_{r=0}^{\infty} c_a(r) = \sum_{r=0}^{\infty} c_d(r) \quad \in \mathbb{N} \cup \{\infty\}$$

Given $e^2 = e \in m\mathcal{I}(\mathbb{N})$, consider its indicator function

$$c_e(n) = \begin{cases} 1 & \exists e(n) \\ 0 & \text{otherwise.} \end{cases}$$

as a point of Cantor space.

For arbitrary $a \in m\mathcal{I}(\mathbb{N})$, we have **initial** and **final Cantor points**, $c_{f^\ddagger f}$ and $c_{ff^\ddagger}$, which are balanced, since f is partial injective.

A composition on balanced Cantor pairs

Given balanced Cantor points $(v,u),(t,s)$, define a composition by:

$$(x,w) \;=\; (v,u) \;\cdot\; (t,s)$$

where $w(n) = s(n).u(j).t(j) \in \{0,1\}$,

$$j = min_{j\in\mathbb{N}} \left\{ \sum_{\alpha=0}^{j} t(\alpha) = \sum_{\alpha=0}^{n} s(\alpha) \right\}$$

and similarly, $x(n) = v(n).u(k).t(k) \in \{0,1\}$,

$$k = min_{k\in\mathbb{N}} \left\{ \sum_{\alpha=0}^{k} u(\alpha) = \sum_{\alpha=0}^{n} v(\alpha) \right\}$$

Another digression ...

what we could, but will not do!

Fun & games with Fractals

The Cantor set $\mathfrak{C}$ is
– by construction –
isomorphic to two copies of itself.

Why **pairs** of Cantor points?

Using the Cantor pairing

Given a Cantor point, $c : \mathbb{N} \to \{0, 1\}$ form two new Cantor points

$$c_a, c_d : \mathbb{N} \to \{0, 1\}$$

by looking at its behaviour on the odd & even numbers respectively.

$$c_a(r) \; = \; c(2r) \quad \text{and} \quad c_d(r) \; = \; c(2r + 1)$$

Elements of $m\mathcal{I}(\mathbb{N})$ as Cantor points

There is a bijective correspondence between :

- Monotone partial injections on $\mathbb{N}$ (i.e. elements of $m\mathcal{I}(\mathbb{N})$)
- Cantor points satisfying

$$\sum_{r=0}^{\infty} c(2r) = \sum_{r=0}^{\infty} c(2r+1)$$

Fun exercise: Write down the composition of such Cantor points!

Cantor's is not the only pairing

More generally, we can use *any* pairing[1] $\phi : \mathbb{N} \cong \mathbb{N} \uplus \mathbb{N}$ to determine a bijection $\Phi : \mathfrak{C} \cong \mathfrak{C} \times \mathfrak{C}$.

Note the "logarithmic" effect

Bijections on the natural numbers $\mathbb{N} \cong \mathbb{N} \uplus \mathbb{N}$

Uniquely determine / are determined by

Bijections on the Cantor set $\mathfrak{C} \cong \mathfrak{C} \times \mathfrak{C}$

There is – of course !(..) – a great deal of category theory behind this.

[1] We prefer *monotone* pairings – expressible as pairs of monotone partial injections.

End of digression

Back to the inverse semigroup theory

... which, nevertheless, remains closely connected to the category theory.

A simple arithmetic starting point :

Addition on $\mathbb{N}$ is monotone.
We 'curry' this to get a family of partial injections :

$$\{add_a(n) = n + a\}_{a \in \mathbb{N}} \subseteq m\mathcal{I}(\mathbb{N})$$

along with their generalised inverses

$$add_a^\ddagger(n) = \begin{cases} n - a & n \geqslant a, \\ \perp & \text{otherwise.} \end{cases}$$

For category theorists

- add_a is the functor $a \oplus \_ : nat \to nat$,
- $add_a^\ddagger$ is a categorical trace.

What submonoid of $m\mathcal{I}(\mathbb{N})$ is generated by these elements?

A well-known monoid

Not a surprise to anybody!

An un-needed reminder ...

The bicyclic inverse monoid **B** has a single generator, and a single relation:

$$\mathcal{B} = \langle s \ : \ ss^{\ddagger} = 1 \rangle$$

The bisimple submonoid of $m\mathcal{I}(\mathbb{N})$ uniquely specified by the idempotents $\{1_{\mathbb{N}+a} \ : \ a \in \mathbb{N}\}$.

From idempotents to arrows

Every pair of idempotents $(1_{\mathbb{N}+b}, 1_{\mathbb{N}+a})$ uniquely specifies an element

$$(b,a) \ = \ add_b add_a^\ddagger \in m\mathcal{I}(\mathbb{N})$$

"The unique monotone partial injection that maps $\mathbb{N}+a$ to $\mathbb{N}+b$"

This corresponds to the normal form for **B**, with composition

$$(d,c)(b,a) \ = \ \left(d + [b \overset{\bullet}{-} c], [c \overset{\bullet}{-} b] + a\right)$$

Successor is not the only generator

Question : *For fixed $x > 0 \in \mathbb{N}$, which inverse monoid is generated by add_x ?*

A clue: self-embeddings of B

The homomorphism $self_k : \mathcal{B} \hookrightarrow \mathcal{B}$, defined by its action on the unique generator as $s \mapsto s^k$, is a self-embedding, for all $k > 0$.

Unsurprising Answer : *Yet another copy of* **B**.

How may we map between these embeddings?

Self-embeddings of **B**

For all $k > 0$, define the injection $\eta_k : \mathcal{B} \rightarrow m\mathcal{I}(\mathbb{N})$ by

$$\eta_k(s) \;=\; add_k^{\ddagger}$$

For all $k > 0$, we have a commuting diagram :

$$\begin{tikzcd} \mathcal{B} \arrow[rr, "self_k"] \arrow[dr, "\eta_k"'] & & \mathcal{B} \arrow[dl, "\eta_1"] \\ & m\mathcal{I}(\mathbb{N}) & \end{tikzcd}$$

together with the inclusions

$$\eta_y(\mathcal{B}) \;\subseteq\; \eta_x(\mathcal{B}) \quad \text{iff} \quad y \ (mod\ x) = 0$$

An (inverse) category of inverse monoids :

Let us apply the notions of **partiality** and **reversibility** to mappings between monoids.

A **partial embedding** $f : M \to N$ of inverse monoids is a a partial injective function on underlying sets, satisfying

1. $f(1_M) = 1_N$
2. $a, b \in dom(f) \;\Rightarrow\; ab \in dom(f)$
3. $a \in dom(f) \;\Rightarrow\; a^\ddagger \in dom(f)$
4. $f^\ddagger$ also satisfies 2. and 3.

The class of all inverse monoids, with this notion of homomorphism, forms an inverse category *pIMMs*.

"Partial Inverse Monoid Monics"

A multiplicity of monoids

A fun game to play :

1. Start with an inverse monoid X.
2. Consider its endomorphism monoid $X^{(1)} = pIMMs(X, X)$
   ...this is also an inverse monoid.
3. Repeat the process : $X^{(n+1)} = pIMMs(X^{(n)}, X^{(n)})$

Derive a countable set of inverse monoids $\{X^{(j)}\}_{j \in \mathbb{N}}$.

A non-trivial question

Define Ω_X to be the full subcategory of *pIMMs* whose objects are $\{X^{(j)}\}_{j \in \mathbb{N}}$.

What can we say about the structure of this?

Can we ever have $X^{(i)} \simeq X^{(j)}$, for $i \neq j$?

We can prove a few facts about
this construction, applied to the bicyclic monoid.

There exists an embedding of the bicyclic monoid into its own endomorphism monoid

$$\mathcal{B} \hookrightarrow \mathcal{B}^{(1)} = \mathit{pIMMs}(\mathcal{B}, \mathcal{B})$$

This is given by : $s^{\ddagger} \mapsto \mathit{self}_1 \in \mathcal{B}^{(1)}$.

As a corollary, $\mathcal{B}$ is a retract of $\mathcal{B}^{(n)}$, for all $n \in \mathbb{N}$.

Back to concrete monoids!

We can consider partial embeddings of $m\mathcal{I}(\mathbb{N})$ that map $\eta_j(\mathcal{B})$ to $\eta_k(\mathcal{B})$

None of these can be inner automorphisms.

How about on the semi-lattice of idempotents?

Recall : Each submonoid $\eta_j(\mathcal{B}) \subseteq m\mathcal{I}(\mathbb{N})$ is uniquely determined by its (distinct) idempotents.

Claim : Yes, whenever $j = 0 \ (mod\ k)$.

Moving from elements to idempotents

The simple (key) case :

$$
\begin{tikzcd}
\mathcal{B} & E(\mathcal{B}) \arrow[l, hook'] \arrow[r, hook] & \mathcal{B} \arrow[d, "\eta_1"] \\
m\mathcal{I}(\mathbb{N}) \arrow[from=1-1, d, "\eta_k"'] \arrow[rr, "times_k^{\ddagger}(\ )times_k"'] & & m\mathcal{I}(\mathbb{N})
\end{tikzcd}
$$

Where $times_k$ is given by currying multiplication $times_k = k \times \_$ and its generalised inverse is :

$$
times_k^{\ddagger}(n) \ = \begin{cases} \frac{n}{k} & n \ (mod\ k) = 0 \\ \\ \perp & \text{otherwise.} \end{cases}
$$

Ceci n'est pas un monoïde bicyclic

Consider the inverse submonoid of $m\mathcal{I}(\mathbb{N})$ generated by $\{times_n\}_{n>0\in\mathbb{N}}$.

Question : "Which inverse monoid is this?"

Euclid proved this is not finitely generated!

A minimal generating set is given by

$$\{times_p \ : \ p \text{ is prime.}\} \subseteq m\mathcal{I}(\mathbb{N})$$

Idempotents and elements

- The **idempotents** are the partial identities : $1_{a\mathbb{N}}$ for all $a > 0 \in \mathbb{N}$
- Composition of idempotents is simply:

$$1_{a\mathbb{N}} 1_{b\mathbb{N}} = 1_{lcm(a,b)\mathbb{N}}$$

- The arrows are, for all $a, b > 0 \in \mathbb{N}$,

  "The unique monotone partial injection that maps $a\mathbb{N}$ onto $b\mathbb{N}$, and is undefined elsewhere."

  This is given by $[b, a] = times_b times_a^\ddagger$.
- Composition?

By either :

1. Elementary number theory, or
2. The 'composing Cantor pairs' formulæ

we may give composition explicitly, as

$$[d, c][b, a] \;=\; \left[d \times \frac{lcm(c, b)}{b} \;,\; \frac{lcm(b, c)}{c} \times a \right]$$

This looks familiar(!)

An interesting special case :

$$\left[p^d, p^c\right]\left[p^b, p^a\right] \;=\; \left[p^{d+(b \dot{-} c)}, p^{(c \dot{-} b)+a}\right]$$

for fixed $p \in \mathbb{N}^+$

An inverse monoid

"On the foundations of inverse monoids & algebras"
J. Leech (1998)

- Underlying set $\mathbb{N}^+ \times \mathbb{N}^+$, with composition given by

$$[d,c][b,a] \;=\; \left[d \times \frac{lcm(c,b)}{b} \;,\; \frac{lcm(b,c)}{c} \times a \right]$$

Basic properties :

- Identity is $[1,1]$.
- Generalised inverses given by $[b,a]^\ddagger = [a,b]$.
- Minimal generating set given by $\{[1,p] : \; p \text{ is prime.}\}$.
- $E(\mathcal{T}) \;\cong\; (\mathbb{N}^+, lcm(\;,\;))$.

A general construction :

J. Leech called this monoid P.

— we will use $\mathcal{T}$, to avoid confusion with the (upcoming) polycyclic monoids.

For category theorists ...

Consider $\mathcal{T}$ to be :

the result of applying some 'bicyclic construction'

to the category $(\mathbb{N}, \_ \times \_)$, instead of $(\mathbb{N}, \_ + \_)$.

Open Question : How general can this be made?

Self-embeddings of $\mathcal{T}$

There is an obvious $\mathbb{N}^+$-indexed family of self-embeddings :

$$Self_n([b,a]) \ = \ \left[b^n, a^n\right] \ \ \forall [b,a] \in \mathcal{T}$$

These satisfy familiar properties ...

$$Self_m Self_n = Self_{m\times n}$$

Within the inverse category pIMMs of partial embeddings, we also have their generalised inverses

$$Self_n^\ddagger \in pIMMs(\mathcal{T},\mathcal{T})$$

Similarly to the bicyclic monoid ...

Perhaps unsurprisingly, we have a reflexivity property

$$\mathcal{T} \ \hookrightarrow \ pIMMs(\mathcal{T},\mathcal{T})$$

so $\mathcal{T}$ is a retract of every object of $\Omega_{\mathcal{T}}$.

Embedding $\mathcal{B}$ into $\mathcal{T}$

For all $n > 1 \in \mathbb{N}$, there exists an embedding $n^{(\text{-})}\mathcal{B} :\hookrightarrow \mathcal{T}$.

This is best defined on normal forms, by $(a, b) \mapsto [n^a, n^b]$.

Recall :

$$\left[n^d, n^c\right]\left[n^b, n^a\right] = \left[n^{d+(b \dot{-} c)}, n^{(c \dot{-} b)+a}\right]$$

These embeddings have generalised inverses within *pIMMs*, that we denote $log_n : \mathcal{T} \to \mathcal{B}$.

An eternal recurrence ?

We could carry on, and look at :

The inverse submonoid of $m\mathcal{I}(\mathbb{N})$ generated by $\{(\ )^n \ : n \in \mathbb{N}^+\}$

...and continue indefinitely ...

To do so would be to miss something interesting on the way!

Une generalisation des monoïdes polycyclique ?

Nivat & Perot famously introduced the *polycyclic monoids* as,

"A generalisation of the bicyclic monoid" (1972)

Can we derive polycylic monoids by in a similar way?

Recall :

Given a set X, the polycyclic monoid P_X is the inverse monoid generated by X, with relations

$$xy^{\ddagger} = \begin{cases} 1 & x = y \\ 0 & \text{otherwise.} \end{cases}$$

Not quite! Instead, we a monoid arising from 'combining' $\mathcal{B}$ and $\mathcal{T}$ that generalises them in a natural way.

$\mathcal{T}$ and $\mathcal{B}$, Combined

We work in the concrete settings of $m\mathcal{I}(\mathbb{N})$.
For all $a > b \in \mathbb{N}$, we define

$$R^{\ddagger}_{a,b}(n) \; = \; an + b \quad \forall n \in \mathbb{N}$$

with generalised inverse given by

$$R_{a,b}(n) \; = \; \begin{cases} \frac{n-a}{b} & n \; (mod \; b) = a \\ \\ \perp & \text{otherwise.} \end{cases}$$

This gives $R^{\ddagger}_{c,d} R_{a,b}$ as the unique monotone partial injection with

- Domain : $a\mathbb{N} + b$
- Image : $c\mathbb{N} + d$

The monoid $\mathcal{TBC}$

Denote by $\mathcal{TBC}$ the inverse submonoid of $m\mathcal{I}(\mathbb{N})$ generated by

$$\{ R_{a,b} \ : \ a > b \in \mathbb{N} \} \subseteq m\mathcal{I}(\mathbb{N})$$

.

Some claims :

1. $\mathcal{TBC}$ contains a copy of $\mathcal{T}$ (and hence a copy of $\mathcal{B}$).
2. $\mathcal{TBC}$ contains a copy of every finite polycyclic monoid.
3. Elements of $\mathcal{TBC}$ have normal form :

$$\{R^{\ddagger}_{c,d} R_{a,b} \ : \ c > d, a > b \in \mathbb{N}\} \cup \{0\}$$

Some simple properties :

As a very basic identity,

$$R_{c,d}R_{a,b} \;=\; R_{ac,ad+b} \quad \forall c > d, a > b \in \mathbb{N}$$

As a simple corollary,

$$R_{x,0}R_{y,0} \;=\; R_{xy,0}$$

giving a natural embedding $T \hookrightarrow \mathcal{TBC}$.

Embedding f.g. polycyclic monoids

Embedding P_a into $\mathcal{TBC}$

Fix arbitrary $a > 1$, and consider the subset

$$\{R_{a,0}, R_{a,1}, \ldots, R_{a,a-1}\}$$

Direct calculations give, for all $n \in \mathbb{N}$:

$$R_{a,b'} R^{\ddagger}_{a,b}(n) = \begin{cases} n & b = b' \\ \perp & b \neq b' \end{cases}$$

since $n \ (mod\ a) = b \quad \Rightarrow \quad n \ (mod\ a) \neq b'$ for all $b \neq b'$.

An embedding of the a**-generator polycyclic monoid** into $\mathcal{TBC}$.

Note this is a **strong embedding**, since $\bigcup_{b=0}^{n-1} dom\,(R_{a,b}) \ = \ dom(I)$.

Normal forms?

We need to show :

Normal forms are closed under composition. The composite

$$\left(R^{\ddagger}_{r,s} R_{p,q} \right) \left(R^{\dagger}_{c,d} R_{a,b} \right)$$

is of the form $R^{\ddagger}_{v,w} R_{t,u}$.

(Ideally, give explicit formulæ for $x > y, u > v \in \mathbb{N}$*).*

The key case :

We first do this for idempotents – this leads to the general formula.

The idempotent $R^{\ddagger}_{a,b} R_{a,b}$ is the partial identity on $a\mathbb{N} + b$.

From basic number theory :

Undergraduate modular arithmetic :

The Chinese Remainder Theorem allows us to compute

$$a\mathbb{N} + b \ \cap \ c\mathbb{N} + d \ = \ x\mathbb{N} + y$$

when a and c are co-prime.

The **extended** CRT allows us to work generally.
There are two cases : $a\mathbb{N} + b \ \cap \ c\mathbb{N} + d$ is

1. $lcm(a,c)\mathbb{N} + y$ when

$$(b \dot{-} d) + (d \dot{-} b) \ \in \ gcd(a,c)\mathbb{N}$$

2. $\emptyset$ otherwise.

A formula for composition

With a 'little' more work

$$\left(R^{\ddagger}_{r,s}R_{p,q}\right)\left(R^{\dagger}_{c,d}R_{a,b}\right) \ =$$

$$\begin{cases} R^{\ddagger}_{v,w}R_{t,u} & (q \stackrel{\bullet}{-} d) + (d \stackrel{\bullet}{-} q) \ \in \ gcd(p,c)\mathbb{N} \\ 0 & \text{otherwise.} \end{cases}$$

Should we so wish ..

we may give $R^{\ddagger}_{v,w}R_{t,u}$ explicitly.

Via repeated applications of CRT

When the composite is non-zero :

$$R^{\ddagger}_{(r,s)} R_{(p,q)} R^{\ddagger}_{(c,d)} R_{(a,b)} \;=\; R^{\ddagger}_{v,w} R_{t,u}$$

with coefficients given by :

- $v = \frac{r.lcm(c,p)}{p}$
- $w = r\left(\frac{x-q}{p}\right) + s$
- $t = \frac{a.lcm(c,p)}{c}$
- $u = a\left(\frac{x-d}{c}\right) + b$

where x is the solution to

$$lcm(c,p)\mathbb{N} + x \;=\; p\mathbb{N} + q \;\cap\; c\mathbb{N} + d$$

given by the extended Chinese Remainder Theorem

A purely abstract $\mathcal{TBC}$?

We can now give $\mathcal{TBC}$ as an abstract inverse monoid :

- Underlying set : $\{((c,d),(a,b) \ : \ d < c, \ b < a \in \mathbb{N}\}$
- Identity : $((1,0),(1,0))$,
- Generalised inverses : $((c,d),(a,b))^\ddagger \ = \ ((a,b),(c,d))$,
- Idempotents : $((a,b),(a,b))$
- Composition : *something non-trivial ...*

Sometimes, representation within $m\mathcal{I}(\mathbb{N})$ is better!

Why the interest ?

What is appealing about $\mathcal{TBC}$ in terms of

logic / computability / foundations ?

We are actually interested in a monoid derived from $\mathcal{TBC}$

Joins and partial orders

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

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

In $\mathcal{I}(\mathbb{N})$, this is simply set-theoretic inclusion.

$\mathcal{I}(\mathbb{N})$ is also closed under arbitrary 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).

Joins of orthogonal monotone elements?

Consider the orthogonal monotone partial injections :

$$R^{\ddagger}_{2,0}R_{3,0} \quad , \quad R^{\ddagger}_{4,1}R_{3,1} \quad , \quad R^{\ddagger}_{4,3}R_{3,2}$$

Their join is a *bijection* on $\mathbb{N}$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots \\ 1 & 3 & 2 & 5 & 7 & 4 & 9 & 11 & 6 & \ldots \end{pmatrix}$$

…but not the unique *monotone* bijection on $\mathbb{N}$.

Historical background

The above bijection is found in unpublished 1932 notes of Collatz (creator of the famous "$3n+1$ problem"). It is the basis of a –still unsolved– problem now called "the original Collatz conjecture".

Piece-wise monotone partial injections

Consider an inverse monoid $X \subseteq m\mathcal{I}(\mathbb{N}) \subseteq \mathcal{I}(\mathbb{N})$.

The set of all *finite* joins (within $\mathcal{I}(\mathbb{N})$)
of orthogonal elements is an inverse monoid.

Call this the piecewise-monotone closure of X, denoted pmX.

The real object of interest is $pm\mathcal{TBC}$.

Possibly relevant :

- J. Conway (1972) " Unpredictable Iterations"
- E. Lehtonen (2008) "Two undecidable variants of Collatz's problem"
- A. Caraiani (2010) "Multiplicative semigroups related to the $3x + 1$ problem"