Monoids, Categories & Monotone Partial Injections

Why Computer Scientists should know and love Inverse Semigroup Theory

peter.hines@york.ac.uk
Peter Hines — University of York

Some motivation ...

This talk is about some **inverse semigroup theory**

closely associated with **theoretical computer science.**

It is not a C.S. talk as such – hopefully the structures used are of interest for their own sake!

We will take a bottom-up approach.

A relevant quotation

"Many reversible functional programming languages, as well as categorical models thereof, come equipped with a tacit assumption of totality, a property that is neither required nor necessarily desirable".

Axelsen & Kaarsgaard (2016 ... to appear)

A sample question

Fixed point operators are important in many fields of computer science, from lambda calculus to functional programming.

Can we introduce fixed points into models of reversible *functional programming?*

A disclaimer

We may or may not reach the final destination

but there is a lot of fun stuff on the way

However, the answer is YES

Our categorical setting

We work with the prototypical inverse category **pInj** of *partial injections on sets*.

Wagner-Preston in the the multi-object case

- (R. Cockett 2002)
  Every *small inverse category* has a representation within the category **pInj**.
- (C. Heunen 2013)
  The same holds for *locally small inverse categories*.

The basics ...

We will be mixing order theory & partial injections.

By analogy with Kleene equality

In a poset $(P, \leqslant_P)$, we write $a \lesssim_P b$ for

"$a \leqslant_P b$ provided both a and b are defined".

A partial injection $f : (P, \leqslant) \to (Q, \leqslant)$ is **monotone (mono.)** when

$$a \leqslant b \Rightarrow f(a) \lesssim f(b)$$

Denote the mono.s from P to Q by $\mathbf{mono}(P, Q)$

A word of warning!

Monotone partial injections form categories / monoids

— *these are not generally inverse categories / monoids.*

The generalised inverse of a monotone partial injection is not, in general, monotone.

Obvious example:

The natural numbers with distinct partial orderings.

Consider some non-zero

$$f \in \mathbf{mono}((\mathbb{N}, =), (\mathbb{N}, \leqslant))$$

Then f^{-1} is monotone precisely when $f = 1_{\{x\}}$, for some $x \in \mathbb{N}$.

From the inverse semigroup viewpoint:

We may consider several interesting subsets of monotone partial injections.

- $\{f : A \to B : f^{-1} \in \textbf{mono}(B, A)\} \subseteq \textbf{mono}(A, B)$
- $\{f : A \to B : dom(f) \text{ is a chain.}\} \subseteq \textbf{mono}(A, B)$
- $\{f : A \to B : \forall\ a \perp a' \in dom(f),\ f(a) \perp f(a')\} \subseteq \textbf{mono}(A, B)$

These all coincide with $\textbf{mono}(\mathbf{A}, \mathbf{B})$ itself when A, B are *countable, totally ordered sets*.

As the obvious example, consider $\mathbb{N}$, with the usual ordering.

Denote the set of monotone partial injections on $\mathbb{N}$ by

$$\mathbf{mono}(\mathbb{N},\mathbb{N}) \leqslant \mathbf{pInj}(\mathbb{N},\mathbb{N})$$

This set is closed under composition and generalised inverse and contains all partial identities, so forms an inverse monoid.

A boolean inverse monoid?

mono$(\mathbb{N}, \mathbb{N})$ is **not** a boolean inverse monoid:

$$a(n) = \begin{cases} n+1 & n \text{ even} \\ \perp & n \text{ odd} \end{cases} \quad , \quad b(n) = \begin{cases} \perp & n \text{ even} \\ n-1 & n \text{ odd} \end{cases}$$

$a \perp b \in$ **mono**$(\mathbb{N}, \mathbb{N})$, but $a \vee b$ is definitely not monotone.

Closure under joins of orthogonal elements fails!

A Σ-monoid structure nevertheless

An indexed family $\{a_j\}_{j\in J} \subseteq \mathbf{mono}(\mathbb{N},\mathbb{N})$ is **summable** iff

$\forall i \neq j \in J$,

- $a_i \perp a_j$
- $a_i \bigvee a_j \in \mathbf{pInj}(\mathbb{N},\mathbb{N})$ is monotone,

in which case, their sum is:

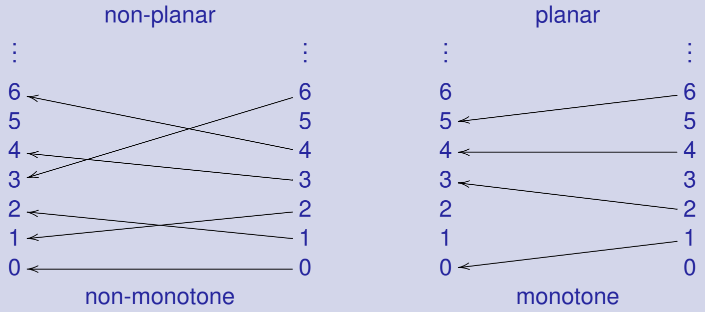
$$\sum_{j\in J} a_j \overset{def.}{=} \bigvee_{j\in J} a_j \in \mathbf{mono}(\mathbb{N},\mathbb{N}).$$

We have a Σ-monoid structure, together with (infinite) distributivity — as used by E. Haghverdi (2000)

Some intuition ...

Think of monotone partial injections on $\mathbb{N}$ as ‘planar diagrams’.

Monotonicity as planarity for partial injections on $\mathbb{N}$



Why planarity?

1. The **quantum Jones polynomial** algorithm (Aharanov, Jones, Landau)
   - A QM algorithm for computing Jones polynomials at $e^{\frac{2k\pi i}{5}}$
   - Classically, a (presumably) $P\#$ problem.
   - Based on the *Temperley-Lieb algebra*
     "Knot theory without crossings" – L. Kaufmann.
2. **Lambek pregroups** (From categorical linguistics)
   - Becoming used in Natural Language Processing
   - Diagrams determined by *planarity & acyclicity*.
3. **Complexity theory** (Planarity provides bounds to complexity).
   - *Matchgates and classical simulation of quantum circuits*
     – R. Jozsa, A. Miyake
   - Restricting swap gates allows for *efficient classical simulation* of QM circuits.
4. . . .

First ... some simple theory!

Initial & final idempotents

Viewed graphically, the following is straightforward:

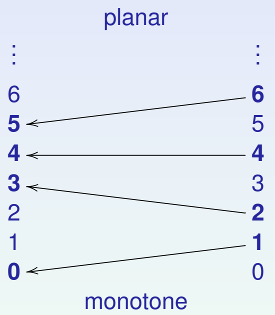
Every $f \in mono(\mathbb{N}, \mathbb{N})$ is uniquely determined by its initial & final idempotents.

$dom(f), im(f) \subseteq \mathbb{N}$ are increasing sequences with bottom elements.

Initial & final idempotents

Viewed graphically, the following is straightforward:

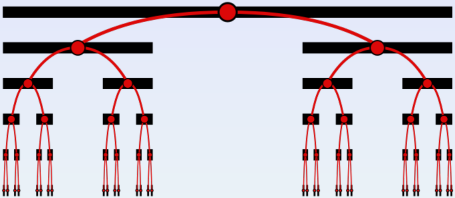
Every $f \in mono(\mathbb{N}, \mathbb{N})$ is uniquely determined by its initial & final idempotents.



$dom(f), im(f) \subseteq \mathbb{N}$ are increasing sequences with bottom elements.

An equivalent viewpoint

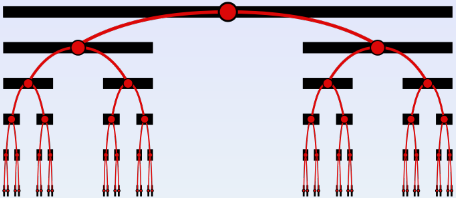
Every monotone partial bijection is uniquely determined by a pair of points of the Cantor set $\mathfrak{C}$.



Formally, one-sided countably infinite strings over $\{0, 1\}$, or equivalently, $\mathfrak{C} = \textbf{Fun}(\mathbb{N}, \{0, 1\})$.

What we will not do!

We all know: the Cantor set is isomorphic to two copies of the Cantor set.



Why *pairs* of points?

Working with single points, rather than pairs of points, would obscure the intuition.

Formalising a little more ...

Given $E \subseteq \mathbb{N}$, denote the indicator function for membership by

$$ind_E(n) = \begin{cases} 1 & n \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Abusing notation slightly: given $e^2 = e = 1_E \in mono(\mathbb{N}, \mathbb{N})$, we write $Ind_e : \mathbb{N} \rightarrow \{0, 1\}$.

A trivial observation:

For arbitrary partial injections $f \in \mathbf{pInj}(\mathbb{N}, \mathbb{N})$,

$$\sum_{n=0}^{\infty} ind_{ff^{-1}}(n) = \sum_{n=0}^{\infty} ind_{f^{-1}f}(n) \in \mathbb{N} \cup \{\infty\}$$

A few simple definitions

A pair of Cantor points $(d, c) \in \mathfrak{C} \times \mathfrak{C}$ is **balanced** when

$$\sum_{j=0}^{\infty} d(j) \; = \; \sum_{j=0}^{\infty} c(j) \; \in \; \mathbb{N} \cup \{\infty\}$$

We denote the set of balanced Cantor points by $\mathfrak{B} \subseteq \mathfrak{C} \times \mathfrak{C}$.

There is a $1:1$ correspondence $\mathfrak{B} \; \equiv \; \mathbf{mono}(\mathbb{N}, \mathbb{N})$.

Giving this explicitly:

Balanced Cantor pairs $\equiv$ monotone partial injections

- $\Leftarrow$ Given $f \in \mathbf{mono}(\mathbb{N},\mathbb{N})$, the balanced pair is:

$$\left(Ind_{ff^{-1}}, Ind_{f^{-1}f}\right) \in \mathfrak{B}$$

- $\Rightarrow$ Given $(t,s) \in \mathfrak{B}$, define $m_{(t,s)} \in \mathbf{mono}(\mathbb{N},\mathbb{N})$ by

$$m_{(t,s)}(n) = \begin{cases} \perp & s(n) = 0 \\ min_{x\in\mathbb{N}}\left\{\sum_{j=0}^{x} t(j) = \sum_{j=0}^{n} s(j)\right\} & s(n) = 1 \end{cases}$$

An illustration:

A balanced pair of Cantor points:

$$t = 1001110 \ , \ s = 0110101\ldots$$

$n =$	0	1	2	3	4	5	6	...
$s(n) =$	0	1	1	0	1	0	1	...
$t(n) =$	1	0	0	1	1	1	0	...

An illustration:

A balanced pair of Cantor points:

$$t = 1001110 \quad , \quad s = 0110101\ldots$$

$n =$	0	1	2	3	4	5	6	...
$s(n) =$	0	1	1	0	1	0	1	...
$\sum_{j\leqslant n} s(j) =$	0	1	2	2	3	3	4	...
$\sum_{j\leqslant n} t(j) =$	1	1	1	2	3	4	4	...
$t(n) =$	1	0	0	1	1	1	0	...

A monoid operation on balanced pairs?

There exists some operation

$$\cdot : \mathfrak{B} \times \mathfrak{B} \to \mathfrak{B}$$

such that $(\mathfrak{B}, \cdot) \;\cong\; \textbf{mono}(\mathbb{N}, \mathbb{N})$.

What does this look like?

Normal forms (I)

A monotone partial injection is **reducing** when $\forall x \in \mathbb{N}$,

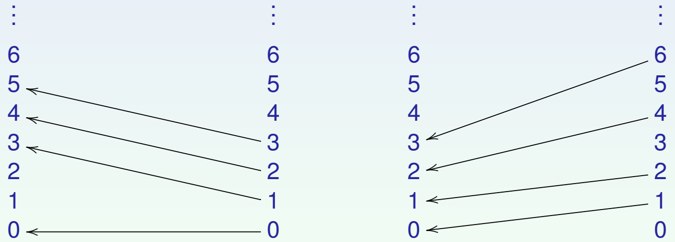
$$Ind_{ff^{-1}}(x) = 1 \Rightarrow Ind_{ff^{-1}}(k) = 1 \ \forall k \leqslant x$$

Dually, it is **expanding** when $\forall x \in \mathbb{N}$,

$$Ind_{f^{-1}f}(x) = 1 \ \Rightarrow \ Ind_{f^{-1}f}(k) = 1 \ \forall k \leqslant x$$

An illustrative example:

Expanding **Reducing**



Cantor points as reducing / expanding arrows

Reducing (resp. expanding) arrows are uniquely determined by their initial (resp. final) idempotents.

Given $c \in \mathfrak{C}$, define $Red_c \in \mathbf{mono}(\mathbb{N}, \mathbb{N})$ by

$$Red_c(n) = \begin{cases} \perp & n = 0 \\ \sum_{j=0}^{n} c(n) - 1 & n = 1 \end{cases}$$

Dually, define $Exp_c \in \mathbf{mono}(\mathbb{N}, \mathbb{N})$ by

$$Exp_c = Red_c^{-1}$$

Normal forms (II)

Given an arbitrary monotone partial injection $f \in \mathbf{mono}(\mathbb{N}, \mathbb{N})$, then the balanced pair $(t, s) = (Ind_{ff^{-1}}, Ind_{f^{-1}f}) \in \mathfrak{B}$ is the unique balanced pair satisfying

$$f = Exp_t Red_s$$

(The only non-trivial point is uniqueness, which follows since (t, s) is required to be balanced).

By considering normal forms (or directly)

Given $(v, u), (t, s) \in \mathfrak{B}$, 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, $x(n) = v(n).u(k).t(k) \in \{0, 1\}$,

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

The generalised inverse is immediate: $(t, s)^{-1} \ = \ (s.t)$.

This gives$(\mathfrak{B}, \cdot) \ \cong$ **mono**$(\mathbb{N}, \mathbb{N})$ as required.

Duals and self-encodings

Recall the complement / dual operation on the Cantor set:

$$c^{\perp}(n) \ = \ c(n) + 1 \ (mod\ 2) \ \ \forall\ c \in \mathfrak{C}$$

E.g. $c = 0100101\ldots$ has complement $c^{\perp} = 1011010\ldots$.

A key definition

A Cantor point $c \in \mathfrak{C}$ is **dual-balanced** when $(c, c^{\perp})$ is a balanced pair.

$$\sum_{\alpha=0}^{\infty} c(\alpha) \ = \ \infty \ = \ \sum_{\alpha=0}^{\infty} c^{\perp}(\alpha)$$

Question: Topologically / graphically, what does the set of such points look like?

Composing / inverting ??

Basic properties:

The set of balanced pairs of the form $(c, c^\perp)$ is:

- closed under generalised inverse: $(c, c^\perp)^{-1} \ = \ (c^\perp, c)$
- decidedly not closed under composition!

$$(c, c^\perp)(c, c^\perp) \ = \ \mathbf{0} \in \mathbf{mono}(\mathbb{N}, \mathbb{N})$$

Dual-balanced Cantor points correspond to

Riffle Shuffles of two countably infinite decks of cards.

Credit: Johnny Blood Photography

How to shuffle (infinite) decks of cards

- Cards from Deck A and Deck B are placed one-by-one onto a single stack.
- At each step, a single card is taken from the bottom[1] of either A or B, and placed on top of the stack.

D.-B. Cantor points provide instructions

At step j, take the next card from Deck $\begin{cases} A & c(j) = 0 \\ B & c(j) = 1 \end{cases}$

[1] **Important:** *deals* as opposed to *shuffles* are antimonotone!

Shuffles, threads & races

In theoretical / practical C.S. ‘shuffles’ are studied in parallel processing.

- Two or more threads require processor time to perform a series of tasks.
- The ‘shuffle’ describes the actual order in which these tasks are executed.
- This is important whenever ‘race conditions’ occur.

Studying *infinite shuffles* is needed when we consider *non-terminating processes*.

$(c, c^\perp) \in \mathfrak{B}$ ensures fair play!

The Dual-Balanced condition on the Cantor point

$$\sum_{j=0}^{\infty} c(j) = \infty = \sum_{j=0}^{\infty} c^\perp(j)$$

ensures that no cards are 'withheld' in the process.

The alternating Cantor point

$$a(n) = n \ (mod\ 2)$$

gives the *'perfect riffle shuffle'*.

From D.-B. Cantor points to Young Tableaux

There is an obvious correspondence between

1. D.-B. Cantor points,
2. (∞, ∞) Young tableaux.

$$c = 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ \ldots \in \mathfrak{C}$$

$c(n) = 0$	1	3	5	8	9	...
$c(n) = 1$	0	2	4	6	7	...

The obvious question:

What about **standard** Young tableaux?

We first need some standard inverse semigroup theory.

D.-B. Cantor points as inverse monoids

Proposition: D.-B. Cantor points uniquely determine effective representations of Nivat & Perrot's *polycyclic monoid* P_2 as inverse submonoids of $\mathbf{mono}(\mathbb{N}, \mathbb{N})$.

Recall – the polycyclic monoid P_2

- Two generators, $\{p, q\}$
- Relations:

$$pq^{-1} = 0 = q^{-1}p \text{ and } pp^{-1} = 1 = qq^{-1}$$

Useful fact: polycyclic monoids are *congruence-free*.

Monotone representations of P_2

Let $c \in \mathfrak{C}$ be dual-balanced. Looking at normal forms,

$$Exp_c Red_{c^\perp} \;=\; (c, c^\perp) \quad \text{and} \quad (c^\perp, c) = Exp_{c^\perp} Red_c$$

By construction, $Red_c Exp_c \;=\; 1_{\mathbb{N}} \;=\; Red_{c^\perp} Exp_{c^\perp}$.

By definition, of $(\ )^\perp : C \to C$,

$$c(n) = 0 \iff c^\perp(n) = 1$$

and so

$$Red_c Exp_{c^\perp} \;=\; 0_{\mathbb{N}} \;=\; Red_{c^\perp} Exp_c$$

The assignment $p \mapsto Red_c$, $q \to Red_{c^\perp}$ gives a monotone representation of P_2.

Such representations are effective, since $dom(p) \cup dom(q) = \mathbb{N}$.

As always ... an example

For the *alternating Cantor point*, or *perfect riffle shuffle*,

$$a(n) = n \ (mod\ 2) \quad \text{or } a = 010101010101\ldots$$

we derive the representation of P_2 corresponding to the Cantor pairing:

$$p^{-1}(x) = 2x \quad \text{and} \quad q^{-1}(x) = 2x + 1$$

On to Standard Young tableaux

In **standard** Young tableaux, the cells are well-ordered both *horizontally* and *vertically*.

x	a
y	b

$$\begin{array}{ccc} x & -\leqslant- & a \\ \rotatebox{-90}{$\leqslant$} & & \rotatebox{-90}{$\leqslant$} \\ b & -\leqslant- & y \end{array}$$

Which dual-balanced Cantor points / riffle shuffles / representations of P_2 satisfy such conditions?

Ballot sequences & monoids

A (binary) **ballot sequence** is an element $w \in \{0,1\}^*$ where, for *every* prefix u of w,

$$\#1s \text{ in } u \;\leqslant\; \#0s \text{ in } u$$

Denote the set of all finite ballot sequences by *Ballot* — this forms a submonoid of $\{0,1\}^*$.

By contradiction: Consider $v, w \in Ballot$ such that $vw \notin Ballot$. Then there exists some prefix u of vw satisfying $\#0s$ in $u < \#1s$ in u. As $v \in Ballot$, u is not a prefix of v, so $u = vl$, for some prefix l of w. However, $\#0s$ in $v \geqslant \#1s$ in v. Therefore, $\#1s$ in $l \geqslant \#0s$ in l, contradicting the assumption that $w \in Ballot$.

A (binary) **ballot sequence** is an element $w \in \{0,1\}^*$ where, for *every* prefix u of w,

$$\#1s \text{ in } u \;\leqslant\; \#0s \text{ in } u$$

Denote the set of all finite ballot sequences by $Ballot$
— this forms a submonoid of $\{0,1\}^*$.

By contradiction: Consider $v, w \in Ballot$ such that $vw \notin Ballot$. Then there exists some prefix u of vw satisfying $\#0s$ in $u < \#1s$ in u. As $v \in Ballot$, u is not a prefix of v, so $u = vl$, for some prefix l of w. However, $\#0s$ in $v \geqslant \#1s$ in v. Therefore, $\#1s$ in $l \geqslant \#0s$ in l, contradicting the assumption that $w \in Ballot$.

A surprisingly simple monoid

Ballot sequences are *very heavily studied*

... but only in combinatorics!

Proposition The monoid of binary ballot sequences is not finitely generated.

By contradiction: Assume a finite generating set G for $Ballot \leqslant \{0,1\}^*$. As G is finite, the longest contiguous string of $1s$ in any member of G is bounded by some finite $K \in \mathbb{N}$. No composite of members of G can account for the ballot sequence $0^{K+1}1^{K+1}$.

A **non-minimal** generating set is given by $\{0^{n+k}1^n\}_{(n,k)\in\mathbb{N}\times\mathbb{N}}$

Boring monoid – interesting embedding

To see that this set is non-minimal:

$$(0^x 1^0)(0^y 1^z) \; = \; 0^{x+y} 1^z$$

Consider the submonoid where

"*All non-empty sequences contain* 1*.*"

This submonoid:

- has minimal generating set $\{0^{n+k+1} 1^{n+1}\}_{(n,k) \in \mathbb{N} \times \mathbb{N}}$
- is the free monoid on its generating set.

We derive an embedding of free monoids:

$$ufe : (\mathbb{N} \times \mathbb{N})^* \rightarrow \{0, 1\}^*$$

From the finite to the infinite:

A Cantor point $c \in \mathbb{C}$ is **ballot** provided

$$\sum_{j=0}^{N} c(j) \leqslant \sum_{j=0}^{N} c^{\perp}(j) \ \forall N \in \mathbb{N}$$

Denote the ballot Cantor points by $\mathfrak{C}_{\mathfrak{B}}$.

(Standard example: the alternating Cantor point).

" Every finite prefix is a member of the Ballot monoid"

Question:

How do such Cantor points behave under the usual meet and join?

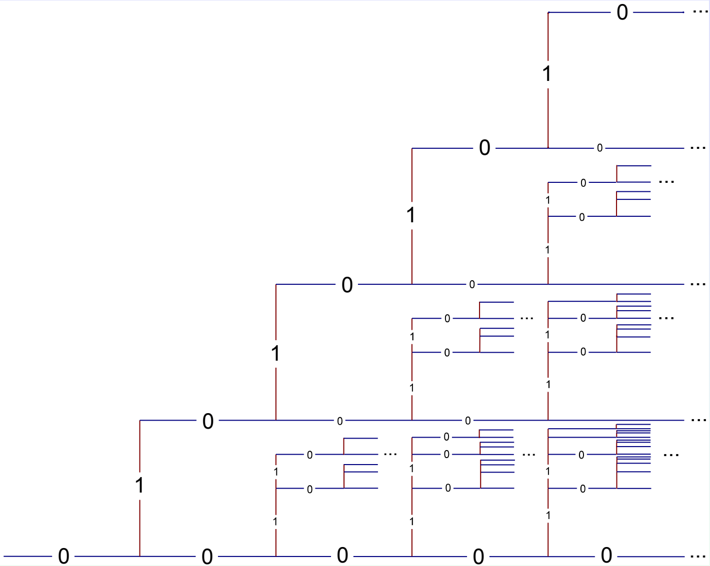
The ballot Scott domain

Key properties:

- There is no top element & they are **not** closed under the join $(c \vee d)(n) \ = \ max\{c(n), d(n)\}$.
- They **are** closed under the meet, $(c \wedge d)(n) \ = \ c(n)d(n)$
- There is a bottom element $z(n) = 0$, for all $n \in \mathbb{N}$.
- The supremum of every chain $c_0 \leqslant c_1 \leqslant c_2 \leqslant \ldots$ is also in $\mathfrak{C}_{\mathfrak{B}}$
- There is a notion of **compact element**: $c \in \mathfrak{C}_{\mathfrak{B}}$ is compact iff $\sum_{j=0}^{\infty} c(j) < \infty$
- Every element is the supremum of a chain of compact elements.

There is also a nice diagrammatic representation:

The ballot Cantor points



Combining two properties:

Let us remove the compact points!

A **dual-balanced ballot** Cantor point $c \in \mathfrak{C}$ satisfies:

- $\sum_{j=0}^{\infty} c(j) = \sum_{j=0}^{\infty} c^{\perp}(j)$
- $\sum_{j=0}^{N} c(j) \leqslant \sum_{j=0}^{N} c^{\perp}(j)$.

There is a 1:1 correspondence:

DBB Cantor points $\equiv$ Standard (∞, ∞) Young tableaux

The ballot property in C.S.

Recall the intuition of

Shuffles $\equiv$ order of execution of threads

The ballot property rules out:

"We have executed more tasks from thread B than thread A"

Canonical example:

- Thread A tasks push data onto a stack.
- Thread B tasks remove data from a stack.

The ballot condition ensures that we are never trying to remove data from an empty stack.

The ballot property in C.S.

Recall the intuition of

$$\text{Shuffles} \equiv \text{order of execution of threads}$$

The ballot property rules out:

"We have executed more tasks from thread B than thread A"

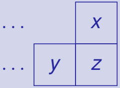
Canonical example:

- Thread A tasks push data onto a stack.
- Thread B tasks remove data from a stack.

The ballot condition ensures that we are never trying to remove data from an empty stack.

Another interpretation

As card-shuffling:

The only way we can see: 

with $z \leqslant x$ is when

"More cards have been laid from Deck B than from Deck A"

As DBB Cantor points are dual-balanced, they uniquely determine representations of P_2, as monotone partial injections on $\mathbb{N}$.

Call these **standard monotone representations.**

Fun & games with polycyclic monoids

A very standard result **N. & P. (1970)**

There exists an embedding of P_∞ into P_2.

Recall:

The infinite-generator polycyclic monoid P_∞ has generating set $\{p_j\}_{j\in\mathbb{N}}$, with relations $p_j p_k^{-1} = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases}$

The embedding is given by

$$p_j \mapsto pq^j \quad , \quad p_j^{-1} \mapsto q^{-j}p^{-1}$$

Straightforward to check that the required relations are satisfied!

Polycyclic monoids as bijections

A slightly lesser-known result **H.& L. (... a while back)**

Representations of P_∞ within **pInj**$(\mathbb{N}, \mathbb{N})$ correspond to injections

$$\mathbb{N} \times \mathbb{N} \hookrightarrow \mathbb{N}$$

which are bijections when the representation is effective

A very simple construction

For a given representation, we define

$$\Psi(x, y) \ = \ p_x^{-1}(y) \ \ \forall (x, y) \in \mathbb{N} \times \mathbb{N}$$

A worked example:

Let's do this for the *standard monotone representation* determined by the *alternating Cantor point* $a \in \mathfrak{C}$.

$$p^{-1}(n) = 2n \quad \text{and} \quad q^{-1}(n) = 2n+1$$

Expanding out, we get

$$\Psi_a(x,y) \;=\; q^{-x}p^{-1}(y) \;=\; 2^{x+1}y + 2^x - 1$$

A bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

The infinite perfect shuffle

x \ $y =$	0	1	2	3	4	5	$\dots$
0	0	2	4	6	8	10	$\dots$
1	1	5	9	13	17	21	$\dots$
2	3	11	19	27	35	43	$\dots$
3	7	23	39	55	71	87	$\dots$
4	15	47	79	111	143	175	$\dots$
5	31	94	159	223	287	351	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

A few observations:

Simple observations

- This table contains every natural number.
- Both rows and columns appear to be well-ordered

  — an $(\infty, \infty, \infty, \ldots)$ standard Young tableaux?
- There seems to be some ‘underlying fractal structure’ ...

More practically — how easy is it to perform this shuffle?

Deep fractal structure ??

On the n^{th} step, we play from Deck x:

	$\cdots$ $Deck_4$	$Deck_3$	$Deck_2$	$Deck_1$	$Deck_0$
$n = 1$					•
$n = 2$				•	
$n = 3$					•
$n = 4$			•		
$n = 5$					•
$n = 6$				•	
$n = 7$					•
$n = 8$		•			
$n = 9$					•
$n = 10$				•	
$n = 11$					•
$n = 12$			•		
$n = 13$					•
$n = 14$				•	
$n = 15$					•
$n = 16$	•				

This looks kind of familiar!

	…	2^4	2^3	2^2	2^1	2^0
$n = 1$						1
$n = 2$					1	0
$n = 3$					1	1
$n = 4$				1	0	0
$n = 5$				1	0	1
$n = 6$				1	1	0
$n = 7$				1	1	1
$n = 8$			1	0	0	0
$n = 9$			1	0	0	1
$n = 10$			1	0	1	0
$n = 11$			1	0	1	1
$n = 12$			1	1	0	0
$n = 13$			1	1	0	1
$n = 14$			1	1	1	0
$n = 15$			1	1	1	1
$n = 16$		1	0	0	0	0

Performing the perfect infinite riffle

A very simple rule

1. Count in binary ...
2. What is the **most significant bit** that has just changed?
3. Play a card from that deck!

peter.hines@york.ac.uk
Peter Hines — University of York

The standard Young property

It is straightforward that **rows** and **columns** are well-ordered:

k	m
l	

$k = \Psi_a(x, y)$ for some $(x, y) \in \mathbb{N} \times \mathbb{N}$.

- $l = 2k + 1 \;>\; k$
- $m = k + 2^{y+1} \;>\; k$.

They also contain all natural numbers.

Claim These properties follow generally from:

1. The fact that representations of P_2 are *monotone* (since they are derived from DB Cantor points).
2. The ballot property on these Cantor points.

A quick outline

Let $c \in \mathfrak{C}$ be a dual-balanced ballot Cantor point. This determines an effective monotone representation $P_2 \stackrel{c}{\hookrightarrow} \mathbf{pInj}(\mathbb{N}, \mathbb{N})$ which corresponds to an (∞, ∞) Young tableau:

$p^{-1}(0)$	$p^{-1}(1)$	$p^{-1}(2)$	$p^{-1}(3)$	$p^{-1}(4)$	$\ldots$
$q^{-1}(0)$	$q^{-1}(1)$	$q^{-1}(2)$	$q^{-1}(3)$	$q^{-1}(4)$	$\ldots$

By the ballot property, $p^{-1}(n) \leqslant q^{-1}(n)$, so this is *standard*.

A quick outline (cont.)

By the same properties, $q^{-k}(n) < q^{-(k+1)}(n)$, so the following table is has well-ordered rows and columns:

$p^{-1}(0)$	$p^{-1}(1)$	$p^{-1}(2)$	$p^{-1}(3)$	$p^{-1}(4)$	$\ldots$
$q^{-1}p^{-1}(0)$	$q^{-1}p^{-1}(1)$	$q^{-1}p^{-1}(2)$	$q^{-1}p^{-1}(3)$	$q^{-1}p^{-1}(4)$	$\ldots$
$q^{-2}p^{-1}(0)$	$q^{-2}p^{-1}(1)$	$q^{-2}p^{-1}(2)$	$q^{-2}p^{-1}(3)$	$q^{-2}p^{-1}(4)$	$\ldots$
$q^{-3}p^{-1}(0)$	$q^{-3}p^{-1}(1)$	$q^{-3}p^{-1}(2)$	$q^{-3}p^{-1}(3)$	$q^{-3}p^{-1}(4)$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Finally, as q^{-1} is monotone and $q^{-1}(x) > p^{-1}(x)$, we deduce that

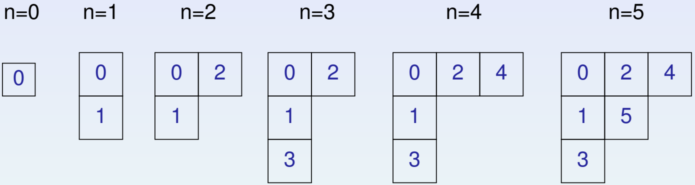
$$\bigcap_{j=0}^{\infty} q^{-1}(\mathbb{N}) = \varnothing$$

and so the embedding of P_∞ is effective.

From the infinite to the finite

Each $(\infty, \infty, \infty, \ldots)$ standard Young tableau can be written as a consistent sequence of finite standard Young tableaux.

For the alternating Cantor point:



Generators of irreducible representations of symmetric groups

. . . or just a complicated way of counting in binary?

Thinking more categorically

From counting in binary to categorical models

of fixed points for reversible computing.

Thinking categorically ...

An old result (H. & L.):

Every effective representation of P_2 within $\mathbf{pInj}(\mathbb{N}, \mathbb{N})$ determines a (semi-) monoidal tensor on this monoid.

The construction: For all partial bijections $f, g \in \mathbf{pInj}(\mathbb{N}, \mathbb{N})$, we take

$$f \star g \ = \ p^{-1}fp \vee q^{-1}fq$$

Explaining terms!

A **monoidal tensor** on a category $\mathcal{C}$ is a functor,

$$(\_ \otimes \_) : \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$$

satisfying *additional properties*.

Functoriality implies:

1. **Identities are preserved . . .**

$$1_X \otimes 1_Y \ = \ 1_{X \otimes Y}$$

2. **. . . as is composition:**

$$(f \otimes g)(h \otimes k) \ = \ (fh \otimes gk)$$

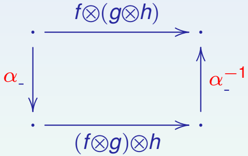
About those additional properties ...

1. There exists a **unit object** I satisfying

$$A \otimes I \;\cong\; A \;\cong\; I \otimes A$$

for all objects A.

2. The tensor $\_ \otimes \_$ is **associative** up to a (well-behaved) family of isomorphisms:



It is **strict** when $f \otimes (g \otimes h) = (f \otimes g) \otimes h$.

A semi- suffices

A **semi-monoidal** category satisfies the exioms for a monoidal category, except perhaps for the existence of a unit object.

Some standard results

1. We can freely adjoin a unit object to any semi-monoidal category.
2. At the unit object (i.e. in the monoid $\mathcal{C}(I, I)$)
   - The tensor and composition coincide.
   - The monoid $C(I, I)$ is thus (E.-H. argument) abelian.

We are working with monoids (single-object categories)

— things become uninteresting if our unique object is the unit.

Semi-monoidal monoids:

A semi-monoidal monoid consists of:

- A single-object category (i.e. a **monoid**) $\mathcal{M}$
- A **monoid homomorphism**

$$\_ \star \_ : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$$

- An invertible **associativity** element $\alpha \in \mathcal{M}$ satisfying:

$$\alpha(f \otimes (g \otimes h)) = ((f \otimes g) \otimes h)\alpha$$

- **MacLane's coherence condition**

$$\alpha^2 = (\alpha \star 1)\alpha(1 \star \alpha)$$

A concrete example (H. & L.)

Based on the alternating Cantor point $a(n) = n + 1 \ (mod\ 2)$, we have:

- **The monoid**: **pInj**$(\mathbb{N}, \mathbb{N})$
- **The tensor**

$$(f \star g)(n) = \begin{cases} 2f\left(\frac{n}{2}\right) & n\ (mod\ 2) = 0 \\ 2g\left(\frac{n-1}{2}\right) + 1 & n\ (mod\ 2) = 1 \end{cases}$$

- **The associativity element**:

$$\alpha(n) = \begin{cases} 2n & n\ (mod\ 2) = 0, \\ n+1 & n\ (mod\ 4) = 1, \\ \frac{n-1}{2} & n\ (mod\ 4) = 3. \end{cases}$$

Dealing with associativity:

A consequence of M.V.L. (2004)

The group of isomorphisms generated by:

$$\alpha(n) = \begin{cases} 2n & n \ (mod\ 2) = 0, \\ n+1 & n \ (mod\ 4) = 1, \\ (n-1)/2 & n \ (mod\ 4) = 3. \end{cases}$$

$$(1 \star \alpha)(n) = \begin{cases} n & n \ (mod\ 2) = 0, \\ 2n-1 & n \ (mod\ 4) = 1, \\ n+2 & n \ (mod\ 8) = 3, \\ (n-1)/2 & n \ (mod\ 8) = 7. \end{cases}$$

generate a copy of Thompson's group $\mathcal{F}$

... as used by V. Shpilrain, A. Ushakov in their public-key cryptographic protocol.

Can we please have a simpler example?

Can we chose a different effective representation of P_2 so that associativity becomes strict?

$$f \star (g \star h) \;=\; (f \star h) \star h$$

How about if we relax conditions on the ballot property / monotonicity / effectiveness / etc. ?

A no-go result

Proposition: In *any* semi-monoidal monoid $(\mathcal{M}, \star)$,

$$(\_ \star \_) : \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M} \text{ is strictly associative}$$
$$\Longleftrightarrow$$
$$\text{The unique object of } \mathcal{M} \text{ is the unit object.}$$

Proof $(\Leftarrow)$ *(Standard Theory ...)*

The complicated direction!

(Proof) $(\Leftarrow)$

Some useful theory ...

An alternative characterization of unit objects given by:

A. Saavedra (1972), J. Kock (2008), A. Joyal, J. Kock (2011)

In the monoid case, these state:

The unique object of $(\mathcal{M}, \star)$ *is a unit object precisely when*

$$(1 \star \_), (\_ \star 1) : \mathcal{M} \to \mathcal{M}$$

are isomorphisms.

Is it because I is strict?

Assume $\star$ is strictly associative, and define the injective monoid homomorphism:

$$\eta = (1 \star \_ \star 1) : \mathcal{M} \hookrightarrow \mathcal{M}$$

Define a semi-monoidal tensor on its image, by, for all $\eta(r), \eta(s) \in \eta(\mathcal{M})$

$$\eta(r) \odot \eta(s) = 1 \star (r \star s) \star 1$$

By construction, $(\mathcal{M}, \star) \cong (\eta(\mathcal{M}), \odot)$.

The final step

By definition, for all $\eta(f) \in \eta(\mathcal{M})$,

$$\begin{aligned} 1 \odot \eta(f) &= 1 \star (1 \star f) \star 1 \\ &= 1 \star 1 \star f \star 1 \\ &= 1 \star f \star 1 \\ &= \eta(f) \end{aligned}$$

Thus $1 \odot \_ \; = \; Id_{\eta(\mathcal{M})} \; = \; \_ \odot 1$.

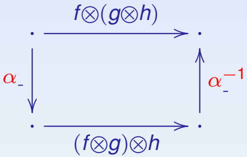
The unique object of $(\eta(\mathcal{M}), \odot)$ is a unit object.

However, $(\eta(\mathcal{M}), \odot) \;\cong\; (\mathcal{M}, \star)$.

Thus the unique object of $\mathcal{M}$ is a unit object. $\mathcal{M}$ is an abelian monoid, and $\_ \star \_$ is simply composition.

A categorical reason why P_2 is congruence-free & $\mathcal{F}$ has no non-abelian quotients.

We are stuck dealing with non-strict associativity



However, dealing with it is *not complex*, despite appearances.

Another example

Let's look at another tensor on $\mathbf{pInj}(\mathbb{N}, \mathbb{N})$

One tensor is never enough!

- Start with the alternating Cantor point

$$a = 010101010\ldots$$

or *any* DBB Cantor point.

- This determines a *standard monotone representation* of P_2 within $\mathbf{pInj}(\mathbb{N}, \mathbb{N})$.

- Via the N. & P embedding $P_\infty \hookrightarrow P_2$,

$$p_j \mapsto pq^j \quad \forall j \in \mathbb{N}$$

this in turn determines an effective embedding of P_∞.

- This is equivalent to a bijection $\Psi_a : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, given by

$$\Psi_a(x, y) = p_x^{-1}(y) \quad \forall (x, y) \in \mathbb{N} \times \mathbb{N}$$

One tensor is never enough!

- Start with the alternating Cantor point

$$a = 010101010\ldots$$

  or *any* DBB Cantor point.

- This determines a *standard monotone representation* of P_2 within $\mathbf{pInj}(\mathbb{N}, \mathbb{N})$.

- Via the N. & P embedding $P_\infty \hookrightarrow P_2$,

$$p_j \mapsto pq^j \quad \forall j \in \mathbb{N}$$

  this in turn determines an effective embedding of P_∞.

- This is equivalent to a bijection $\Psi_a : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, given by

$$\Psi_a(x, y) = p_x^{-1}(y) \quad \forall (x, y) \in \mathbb{N} \times \mathbb{N}$$

One tensor is never enough!

- Start with the alternating Cantor point

$$a = 010101010\ldots$$

or *any* DBB Cantor point.

- This determines a *standard monotone representation* of P_2 within $\mathbf{pInj}(\mathbb{N}, \mathbb{N})$.

- Via the N. & P embedding $P_\infty \hookrightarrow P_2$,

$$p_j \mapsto pq^j \quad \forall j \in \mathbb{N}$$

this in turn determines an effective embedding of P_∞.

- This is equivalent to a bijection $\Psi_a : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, given by

$$\Psi_a(x, y) = p_x^{-1}(y) \quad \forall (x, y) \in \mathbb{N} \times \mathbb{N}$$

One tensor is never enough!

- Start with the alternating Cantor point

$$a = 010101010\dots$$

or *any* DBB Cantor point.

- This determines a *standard monotone representation* of P_2 within $\mathbf{pInj}(\mathbb{N}, \mathbb{N})$.

- Via the N. & P embedding $P_\infty \hookrightarrow P_2$,

$$p_j \mapsto pq^j \quad \forall j \in \mathbb{N}$$

this in turn determines an effective embedding of P_∞.

- This is equivalent to a bijection $\Psi_a : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, given by

$$\Psi_a(x, y) = p_x^{-1}(y) \quad \forall (x, y) \in \mathbb{N} \times \mathbb{N}$$

Another H.-L. result

We define a tensor using the bijection $\Psi_c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by:

$$u \otimes v \ = \ \Psi_c(u \times v)\Psi_c^{-1} \quad \forall u, v \in \mathbf{pInj}(\mathbb{N}, \mathbb{N})$$

We may prove this is a semi-monoidal tensor by:

- Direct calculations (tedious)
- Categorical methods (abstract nonsense)

Unwinding the definitions:

$$u \otimes v \ = \ \bigvee_{j=0}^{\infty} p_{u(j)}^{-1} \ v \ p_j \ = \ \bigvee_{j=0}^{\infty} q^{-u(j)} p^{-1} \ v \ pq^j$$

Another H.-L. result

We define a tensor using the bijection $\Psi_c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by:

$$u \otimes v \ = \ \Psi_c(u \times v)\Psi_c^{-1} \quad \forall u, v \in \mathbf{pInj}(\mathbb{N}, \mathbb{N})$$

We may prove this is a semi-monoidal tensor by:

- Direct calculations (tedious)
- Categorical methods (abstract nonsense)

Unwinding the definitions:

$$u \otimes v \ = \ \bigvee_{j=0}^{\infty} p_{u(j)}^{-1} \ v \ p_j \ = \ \bigvee_{j=0}^{\infty} q^{-u(j)} p^{-1} \ v \ pq^j$$

A quick check ...

Checking the Saavedra / Kock / Joyal conditions for units:

The endomorphisms $(1 \otimes \_), (\_ \otimes 1) : \mathbf{pInj}(\mathbb{N}, \mathbb{N}) \rightarrow \mathbf{pInj}(\mathbb{N}, \mathbb{N})$

- are injective monoid homomorphisms.
- are not isomorphisms!

Some previous work ...

These operations (in heavily disguised form!) were used by J.-Y. Girard's GoI series (1989 onwards).

Using Girard's notation, define $?(f) = (f \otimes 1)$ and $!(f) = (1 \otimes f)$.

A quick check ...

Checking the Saavedra / Kock / Joyal conditions for units:

The endomorphisms $(1 \otimes \_), (\_ \otimes 1) : \mathbf{pInj}(\mathbb{N}, \mathbb{N}) \to \mathbf{pInj}(\mathbb{N}, \mathbb{N})$

- are injective monoid homomorphisms.
- are not isomorphisms!

Some previous work ...

These operations (in heavily disguised form!) were used by J.-Y. Girard's GoI series (1989 onwards).

Using Girard's notation, define $?(f) = (f \otimes 1)$ and $!(f) = (1 \otimes f)$.

Writing things explicitly (I)

Let's look at $(1 \otimes \_)$.

$$!(f) \;=\; (1 \otimes f) \;=\; \Psi(1 \times f)\Psi^{-1}$$

From the definition of Ψ,

$$!(f) \;=\; \bigvee_{j=0}^{\infty} p_j^{-1} \; f \; p_j$$

In terms of P_2, rather than P_∞,

$$!(f) \;=\; \bigvee_{j=0}^{\infty} q^{-j} p^{-1} \; f \; p q^j$$

Writing things explicitly (II)

Alternatively, consider $(\_ \otimes 1)$.

$$?(f) \;=\; (f \otimes 1) \;=\; \Psi(f \times 1)\Psi^{-1}$$

From the definition of Ψ,

$$?(f) \;=\; \bigvee_{j=0}^{\infty} p_{f(j)}^{-1}\, p_j$$

In terms of P_2, rather than P_∞,

$$?(f) \;=\; \bigvee_{j=0}^{\infty} q^{-f(j)} p^{-1}\, pq^j$$

Interacting tensors (I)

How do $\_ \star \_$ and $?(\ )$ interact??

By direct calculation:

$$
\begin{aligned}
0\star ?(f) &= p^{-1}0p \ \vee \ q^{-1}?(f)q \\
&= q^{-1}\left(\bigvee_{j=0}^{\infty} q^{-f(j)}p^{-1}pq^{j}\right) q \\
&= \bigvee_{j=0}^{\infty} q^{-(f(j)+1)}p^{-1}pq^{(j+1)} \\
&= \\
&= ?(succ.f.succ^{-1})
\end{aligned}
$$

Where $succ(n) = n+1$ is the successor function.

A simple shift operation on the action of $?(f)$.

Interacting tensors (II)

How do $\_ \star \_$ and $!(\_)$ interact??

By direct calculation:

$$
\begin{aligned}
f \star !(f) &= p^{-1} f p \ \vee \ q^{-1} !(f) q \\
&= p^{-1} f p \ \vee \ q^{-1} \left(\bigvee_{j=0}^{\infty} q^{-j} p^{-1} f p q^{j} \right) q \\
&= p^{-1} f p \vee \left(\bigvee_{j=1}^{\infty} q^{-j} p^{-1} f p q^{j} \right) \\
&= !(f)
\end{aligned}
$$

The homomorphism $1 \otimes \_$ provides right fixed points for $\_ \star \_$.

More generally

In general, what is the interaction between $\_ \star \_$ and $\_ \otimes \_$?

An extremely subtle interaction, determined by:

1. N. & P.'s embedding $P_\infty \hookrightarrow P_2$.
2. Countability of $\mathbb{N}$.
3. The ballot property & monotonicity.
4. Categorical distributivity.
5. ...

Are we nearly there yet ??

We still haven't found what we're looking for

We have exhibited: **fixed points for a tensor**.

What is needed: **fixed points for functional application.**

The two are related in a fundamental way,
in *monoidal closed categories*.

Fortunately: There is a construction (JSV96,SA96) of (well-behaved) monoidal closed categories that preserves such fixed points.

This is of course(!) applicable to **pInj** and related categories.

A little bit of advertising ...

For this to work in general, we need:

- (Semi-)monoidal equivalences between categories & monoids.
- A related coherence theorem / strictification procedure.

(PMH 2016) *Journal of Homotopy & Related Structures* ... to appear.

Even more fortunately ...

That belongs in the realm of **category theory**

rather than **(inverse) semigroup theory**.

Although inverse categories

– particularly **pInj** *–*

provide particularly neat examples !