

Projections of stream convolution products and a proof of Christol's Theorem

David Sprunger

Indiana University

April 1, 2015

Introduction

Power series are studied as algebraic objects:

$$A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \dots$$

Streams are studied as coalgebraic objects:

$$a = (a_0, a_1, a_2, a_3, a_4, \dots)$$

Christol's theorem is a bridge between these two perspectives, which characterizes some distinguished power series as some distinguished streams.

Outline:

- 1 Give coalgebraic definitions for algebraic operations on power series
- 2 Prove some new facts about power series using coalgebraic methods
- 3 Use these facts to prove Christol's theorem

Coalgebra for streams

Σ is a set and Σ^ω is the set of all streams with entries in that set. We define some functions:

$$\begin{aligned} \text{hd} : \Sigma^\omega &\rightarrow \Sigma & \text{hd}(\sigma) &= \sigma_0 \\ \pi_{a,b} : \Sigma^\omega &\rightarrow \Sigma^\omega & \pi_{a,b}(\sigma) &= (\sigma_a, \sigma_{a+b}, \sigma_{a+2b}, \dots) \\ \text{tl} : \Sigma^\omega &\rightarrow \Sigma^\omega & \text{tl} &= \pi_{1,1} \end{aligned}$$

Corecursion (for streams) allows us to define streams by specifying the heads and the tails (or heads and π 's) of the streams.

Coinduction (for streams) allows us to decide two streams are equal based on the fact that they are related by a bisimulation.

Why do we care about streams?

Some famous streams, defined corecursively:

$$0 \quad \begin{array}{l} \text{hd}(0) = 1 \\ \text{tl}(0) = 0 \end{array} \quad \Bigg|$$

Why do we care about streams?

Some famous streams, defined corecursively:

$$O \quad \begin{array}{l} \text{hd}(O) = 1 \\ \text{tl}(O) = O \end{array} \quad \Bigg| \quad O = (1, 1, 1, \dots)$$

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$
P	$\text{hd}(P) = 1$ $\text{tl}(P) = 2 \cdot P$	

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$
P	$\text{hd}(P) = 1$ $\text{tl}(P) = 2 \cdot P$	$P = (1, 2, 4, 8, \dots)$

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$
P	$\text{hd}(P) = 1$ $\text{tl}(P) = 2 \cdot P$	$P = (1, 2, 4, 8, \dots)$
M	$\text{hd}(M) = 0$ $\pi_{0,2}(M) = M$ $\pi_{1,2}(M) = \overline{M}$	

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$
P	$\text{hd}(P) = 1$ $\text{tl}(P) = 2 \cdot P$	$P = (1, 2, 4, 8, \dots)$
M	$\text{hd}(M) = 0$ $\pi_{0,2}(M) = M$ $\pi_{1,2}(M) = \overline{M}$	$M = (0, 1, 1, 0, 1, 0, 0, 1, \dots)$

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$
P	$\text{hd}(P) = 1$ $\text{tl}(P) = 2 \cdot P$	$P = (1, 2, 4, 8, \dots)$
M	$\text{hd}(M) = 0$ $\pi_{0,2}(M) = M$ $\pi_{1,2}(M) = \overline{M}$	$M = (0, 1, 1, 0, 1, 0, 0, 1, \dots)$
C	$\text{hd}(C) = 1$ $\text{tl}(C) = C \times C$	

Why do we care about streams?

Some famous streams, defined corecursively:

O	$\text{hd}(O) = 1$ $\text{tl}(O) = O$	$O = (1, 1, 1, \dots)$
N	$\text{hd}(N) = 1$ $\text{tl}(N) = O + N$	$N = (1, 2, 3, \dots)$
P	$\text{hd}(P) = 1$ $\text{tl}(P) = 2 \cdot P$	$P = (1, 2, 4, 8, \dots)$
M	$\text{hd}(M) = 0$ $\pi_{0,2}(M) = M$ $\pi_{1,2}(M) = \overline{M}$	$M = (0, 1, 1, 0, 1, 0, 0, 1, \dots)$
C	$\text{hd}(C) = 1$ $\text{tl}(C) = C \times C$	$C = (1, 1, 2, 5, 14, \dots)$

A (hd, tl) -**bisimulation** is a relation $R \subseteq \Sigma^\omega \times \Sigma^\omega$ such that for all $(\sigma, \tau) \in R$ the following hold:

- 1) $\text{hd}(\sigma) = \text{hd}(\tau)$, and
- 2) $(\text{tl}(\sigma), \text{tl}(\tau)) \in R$.

For all $b > 1$, a $(\text{hd}, \pi_{a,b})$ -**bisimulation** is a relation $R \subseteq \Sigma^\omega \times \Sigma^\omega$ such that for all $(\sigma, \tau) \in R$ the following hold:

- 1) $\text{hd}(\sigma) = \text{hd}(\tau)$, and
- 2) for all $0 \leq a < b$, we have $(\pi_{a,b}(\sigma), \pi_{a,b}(\tau)) \in R$.

Theorem (Coinduction for streams)

Let Δ be the diagonal relation on Σ^ω . If R is a (hd, tl) -bisimulation or a $(\text{hd}, \pi_{a,b})$ -bisimulation, then $R \subseteq \Delta$. In particular, if $(\sigma, \tau) \in R$ where R is a bisimulation, then $\sigma = \tau$.

Streams and power series

There are two special power series: constant series and x .

$$[a] = (a, 0, 0, 0, \dots)$$

Another way to think of this is with a coalgebraic definition. $[a]$ is the unique stream satisfying:

$$\text{hd}([a]) = a$$

$$\text{tl}([a]) = [0]$$

$X = (0, 1, 0, 0, 0, \dots)$ is the unique stream satisfying

$$\text{hd}(X) = 0$$

$$\text{tl}(X) = [1]$$

Power series form a ring, so let's give a ring structure to streams. That means we need an addition and a multiplication operation. If

$$\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots)$$

$$\tau = (\tau_0, \tau_1, \tau_2, \tau_3, \dots)$$

then we want

$$\sigma + \tau = (\sigma_0 + \tau_0, \sigma_1 + \tau_1, \sigma_2 + \tau_2, \sigma_3 + \tau_3, \dots)$$

Power series form a ring, so let's give a ring structure to streams. That means we need an addition and a multiplication operation. If

$$\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots)$$

$$\tau = (\tau_0, \tau_1, \tau_2, \tau_3, \dots)$$

then we want

$$\sigma + \tau = (\sigma_0 + \tau_0, \sigma_1 + \tau_1, \sigma_2 + \tau_2, \sigma_3 + \tau_3, \dots)$$

We can give this a coalgebraic definition: $\sigma + \tau$ satisfies

$$\text{hd}(\sigma + \tau) = \text{hd}(\sigma) + \text{hd}(\tau)$$

$$\text{tl}(\sigma + \tau) = \text{tl}(\sigma) + \text{tl}(\tau)$$

$$\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots)$$

$$\tau = (\tau_0, \tau_1, \tau_2, \tau_3, \dots)$$

The (Cauchy) product of power series is given by

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

$$\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots)$$

$$\tau = (\tau_0, \tau_1, \tau_2, \tau_3, \dots)$$

The (Cauchy) product of power series is given by

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

This also has a standard coalgebraic definition: $\sigma \times \tau$ satisfies

$$\text{hd}(\sigma \times \tau) = \text{hd}(\sigma) \cdot \text{hd}(\tau)$$

$$\text{tl}(\sigma \times \tau) = [\text{hd}(\sigma)] \times \text{tl}(\tau) + \text{tl}(\sigma) \times \tau$$

$$\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots)$$

$$\tau = (\tau_0, \tau_1, \tau_2, \tau_3, \dots)$$

The (Cauchy) product of power series is given by

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

This also has a standard coalgebraic definition: $\sigma \times \tau$ satisfies

$$\text{hd}(\sigma \times \tau) = \text{hd}(\sigma) \cdot \text{hd}(\tau)$$

$$\text{tl}(\sigma \times \tau) = [\text{hd}(\sigma)] \times \text{tl}(\tau) + \text{tl}(\sigma) \times \tau$$

$$\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_3, \dots)$$

$$\tau = (\tau_0, \tau_1, \tau_2, \tau_3, \dots)$$

The (Cauchy) product of power series is given by

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

This also has a standard coalgebraic definition: $\sigma \times \tau$ satisfies

$$\text{hd}(\sigma \times \tau) = \text{hd}(\sigma) \cdot \text{hd}(\tau)$$

$$\text{tl}(\sigma \times \tau) = [\text{hd}(\sigma)] \times \text{tl}(\tau) + \text{tl}(\sigma) \times \tau$$

(We also throw in integer exponentiation as shorthand for repeated multiplication.)

Let's prove some easy facts about stream operations using the coinductive proof principle.

Fact 1 ($[0]$ is the additive identity)

If σ is a stream, then $[0] + \sigma = \sigma$.

Proof.

By (hd, tl) -bisimulation where $R = \{([0] + \sigma, \sigma) : \sigma \in \Sigma^\omega\}$.

The heads match: $\text{hd}([0] + \sigma) = \text{hd}([0]) + \text{hd}(\sigma) = \text{hd}(\sigma)$.

And the tails stay in the relation:

$\text{tl}([0] + \sigma) = \text{tl}([0]) + \text{tl}(\sigma) = [0] + \text{tl}(\sigma) R \text{tl}(\sigma)$. □

Fact 2 (\times left distributes over $+$)

If σ , τ , and ρ are streams, then $\sigma \times \tau + \sigma \times \rho = \sigma \times (\tau + \rho)$.

Proof.

By bisimulation with $R = \{(\sigma \times \tau + \sigma \times \rho, \sigma \times (\tau + \rho)) : \sigma, \tau, \rho \in \Sigma^\omega\}$.

The heads are equal:

$$\begin{aligned} \text{hd}(\sigma \times \tau + \sigma \times \rho) &= \text{hd}(\sigma) \cdot \text{hd}(\tau) + \text{hd}(\sigma) \cdot \text{hd}(\rho) \\ &= \text{hd}(\sigma) \cdot (\text{hd}(\tau) + \text{hd}(\rho)) = \text{hd}(\sigma \times (\tau + \rho)) \end{aligned}$$

The tails are (almost) related:

$$\begin{aligned} \text{tl}(\sigma \times \tau + \sigma \times \rho) &= \text{tl}(\sigma \times \tau) + \text{tl}(\sigma \times \rho) \\ &= [\text{hd}(\sigma)] \times \text{tl}(\tau) + \text{tl}(\sigma) \times \tau + [\text{hd}(\sigma)] \times \text{tl}(\rho) + \text{tl}(\sigma) \times \rho \\ &= [\text{hd}(\sigma)] \times \text{tl}(\tau) + [\text{hd}(\sigma)] \times \text{tl}(\rho) + \text{tl}(\sigma) \times \tau + \text{tl}(\sigma) \times \rho \\ R? &[\text{hd}(\sigma)] \times (\text{tl}(\tau) + \text{tl}(\rho)) + \text{tl}(\sigma) \times (\tau + \rho) \end{aligned}$$

Fact 2 (\times left distributes over $+$)

If σ , τ , and ρ are streams, then $\sigma \times \tau + \sigma \times \rho = \sigma \times (\tau + \rho)$.

Proof.

By bisimulation with $R = \{(\sigma \times \tau + \sigma \times \rho, \sigma \times (\tau + \rho)) : \sigma, \tau, \rho \in \Sigma^\omega\}$.

The heads are equal:

$$\begin{aligned} \text{hd}(\sigma \times \tau + \sigma \times \rho) &= \text{hd}(\sigma) \cdot \text{hd}(\tau) + \text{hd}(\sigma) \cdot \text{hd}(\rho) \\ &= \text{hd}(\sigma) \cdot (\text{hd}(\tau) + \text{hd}(\rho)) = \text{hd}(\sigma \times (\tau + \rho)) \end{aligned}$$

The tails are (almost) related:

$$\begin{aligned} \text{tl}(\sigma \times \tau + \sigma \times \rho) &= \text{tl}(\sigma \times \tau) + \text{tl}(\sigma \times \rho) \\ &= [\text{hd}(\sigma)] \times \text{tl}(\tau) + \text{tl}(\sigma) \times \tau + [\text{hd}(\sigma)] \times \text{tl}(\rho) + \text{tl}(\sigma) \times \rho \\ &= [\text{hd}(\sigma)] \times \text{tl}(\tau) + [\text{hd}(\sigma)] \times \text{tl}(\rho) + \text{tl}(\sigma) \times \tau + \text{tl}(\sigma) \times \rho \\ R? &[\text{hd}(\sigma)] \times (\text{tl}(\tau) + \text{tl}(\rho)) + \text{tl}(\sigma) \times (\tau + \rho) \end{aligned}$$

Let's try again with a stronger coinduction hypothesis.

Proof.

By bisimulation with $R =$

$$\left\{ \left(\sum_{i=1}^k \sigma_i \times \tau_i + \sigma_i \times \rho_i, \sum_{i=1}^k \sigma_i \times (\tau_i + \rho_i) \right) : k \in \mathbb{N}, \sigma_i, \tau_i, \rho_i \in \Sigma^\omega \right\}.$$

The heads are equal.

The tails are related:

$$\begin{aligned} \sum \text{tl}(\sigma \times \tau + \sigma \times \rho) &= \sum \text{tl}(\sigma \times \tau) + \text{tl}(\sigma \times \rho) \\ &= \sum [\text{hd}(\sigma)] \times \text{tl}(\tau) + \text{tl}(\sigma) \times \tau + [\text{hd}(\sigma)] \times \text{tl}(\rho) + \text{tl}(\sigma) \times \rho \\ &= \sum [\text{hd}(\sigma)] \times \text{tl}(\tau) + [\text{hd}(\sigma)] \times \text{tl}(\rho) + \sum \text{tl}(\sigma) \times \tau + \text{tl}(\sigma) \times \rho \\ R \sum [\text{hd}(\sigma)] \times (\text{tl}(\tau) + \text{tl}(\rho)) + \sum \text{tl}(\sigma) \times (\tau + \rho) \end{aligned}$$

□

Fast forwarding, we could prove the following theorem:

Theorem (Rutten, 2005)

If Σ is a ring, then Σ^ω with the induced stream operations $+$ and \times is also a ring, where $[0]$ and $[1]$ are the respective identities.

This ring could be denoted $\Sigma[[x]]$.

Algebraic and automatic streams

A **polynomial** is a stream that is eventually 0. One way to generate them is with the BNF grammar

$$P ::= [a] \mid X \mid P + P \mid P \times P \mid P^k$$

Definition

A stream σ is **algebraic** means there is $k \in \mathbb{N}$ and polynomials p_i , not all $[0]$, such that $\sum_{i=0}^k p_i \times \sigma^i = [0]$

Definition

A stream σ is **q -automatic** means the set $K = \{\pi_{i,q^k}(\sigma) : k \in \mathbb{N}, 0 \leq i < q^k\}$ is finite.

Christol's theorem says a stream is q -automatic iff it is algebraic over \mathbb{F}_q .

The Thue-Morse sequence is a famous 2-automatic stream.

$$M = 01101001100101101001011001101001 \dots$$

It is 2-automatic because its 2-kernel is finite:

$$\pi_{0,2}(M) = 0110100110010110 \dots = M$$

$$\pi_{1,2}(M) = 1001011001101001 \dots = \overline{M}$$

$$\pi_{0,2}(\overline{M}) = 1001011001101001 \dots = \overline{M}$$

$$\pi_{1,2}(\overline{M}) = 0110100110010110 \dots = M$$

The Thue-Morse stream is also algebraic over $\mathbb{F}_2[X]$!

$$M = 01101001100101101001011001101001 \dots$$

$$X^2 \times M = 00011010011001011010010110011010 \dots$$

$$([1] + X^2) \times M = 01110011111100110011001111110011 \dots$$

$$M^2 = 00101000100000101000001000101001 \dots$$

$$([1] + X + X^2 + X^3) \times M^2 = 00110011111100110011001111110011 \dots$$

“Therefore” $X + ([1] + X^2) \times M + ([1] + X + X^2 + X^3) \times M^2 = [0]$

M and \overline{M} are “finitely definable” in two senses. They are two solutions to the (coalgebraic) specification:

$$\sigma = \mathbf{zip}(\sigma, \tau)$$

$$\tau = \mathbf{zip}(\tau, \sigma)$$

And also the only solutions to the (algebraic) polynomial in $\mathbb{F}_2[X][\sigma]$:

$$X + (1 + X)^2 \times \sigma + (1 + X)^3 \times \sigma^2 = 0$$

Solutions to zip specifications like the above are known to be exactly the automatic streams, and solutions to polynomials like the above are by definition the algebraic streams.

Projections of stream products

Part of Christol's theorem will involve showing an algebraic stream is automatic, so we'll need to be applying $\pi_{a,b}$ to algebraic streams to check the kernel is finite. It's simple to figure out what π will do to constant streams, X , and sums:

$$\pi_{a,b}(\sigma + \tau) = \pi_{a,b}(\sigma) + \pi_{a,b}(\tau)$$

The difficulty is with projections of stream products. Our key result will describe $\pi_{a,b}(\sigma \times \tau)$ generically.

Let's start with an example. If we write $\sigma = (\sigma_0, \sigma_1, \sigma_2, \dots)$ and $\tau = (\tau_0, \tau_1, \tau_2, \dots)$, then from earlier we had:

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

Let's start with an example. If we write $\sigma = (\sigma_0, \sigma_1, \sigma_2, \dots)$ and $\tau = (\tau_0, \tau_1, \tau_2, \dots)$, then from earlier we had:

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

That looks like the sum of two different stream products!

Let's start with an example. If we write $\sigma = (\sigma_0, \sigma_1, \sigma_2, \dots)$ and $\tau = (\tau_0, \tau_1, \tau_2, \dots)$, then from earlier we had:

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

That looks like the sum of two different stream products!

Let's start with an example. If we write $\sigma = (\sigma_0, \sigma_1, \sigma_2, \dots)$ and $\tau = (\tau_0, \tau_1, \tau_2, \dots)$, then from earlier we had:

$$\sigma \times \tau = (\sigma_0\tau_0, \sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_2 + \sigma_1\tau_1 + \sigma_2\tau_0, \dots)$$

That looks like the sum of two different stream products! So based on these first terms we'd say

$$\pi_{1,2}(\sigma \times \tau) = \pi_{0,2}(\sigma) \times \pi_{1,2}(\tau) + \pi_{1,2}(\sigma) \times \pi_{0,2}(\tau)$$

After doing some more examples, we come to the conjecture that

$$\pi_{a,b}(\sigma \times \tau) = \sum_{k=0}^a \pi_{k,b}(\sigma) \times \pi_{a-k,b}(\tau) + \sum_{k=a+1}^{b-1} X \times \pi_{k,b}(\sigma) \times \pi_{b+a-k,b}(\tau)$$

for all $0 \leq a < b$.

After doing some more examples, we come to the conjecture that

$$\pi_{a,b}(\sigma \times \tau) = \sum_{k=0}^a \pi_{k,b}(\sigma) \times \pi_{a-k,b}(\tau) + \sum_{k=a+1}^{b-1} X \times \pi_{k,b}(\sigma) \times \pi_{b+a-k,b}(\tau)$$

for all $0 \leq a < b$.

Unfortunately, the coinduction doesn't go through—we need a stronger coinduction hypothesis to deal with things like $\tau 1(\pi_{k,b}(\sigma)) = \pi_{k+b,b}(\sigma)$.

So try some more examples where $b \leq a$. That leads to a conjecture that

$$\pi_{a,b}(\sigma \times \tau) = \sum_{k=0}^a \pi_{k,b}(\sigma) \times \pi_{a-k,b}(\tau) - \sum_{k=b}^a X \times \pi_{k,b}(\sigma) \times \pi_{b+a-k,b}(\tau).$$

for all $b \leq a$.

Putting everything together, we get the following:

Theorem

For all streams σ and τ and all $a, b \in \mathbb{N}$ with $b \neq 0$,

$$\begin{aligned} \pi_{a,b}(\sigma \times \tau) &= \sum_{k=0}^a \pi_{k,b}(\sigma) \times \pi_{a-k,b}(\tau) + \sum_{k=a+1}^{b-1} X \times \pi_{k,b}(\sigma) \times \pi_{b+a-k,b}(\tau) \\ &\quad - \sum_{k=b}^a X \times \pi_{k,b}(\sigma) \times \pi_{b+a-k,b}(\tau) \end{aligned}$$

Proof.

By (hd, t1)-bisimulation. It's a straightfoward, albeit long, calculation involving properties of t1, like $\text{t1}(\sigma + \tau) = \text{t1}(\sigma) + \text{t1}(\tau)$ or the formula for $\text{t1}(\sigma \times \tau)$. □

The q -splay operator

We introduce a new unary operator: the q -splay operator. $\sigma^{(q)}$ is defined to be the unique stream satisfying

$$\pi_{0,q}(\sigma^{(q)}) = \sigma$$

$$\pi_{i,q}(\sigma^{(q)}) = [0], \text{ for all } 0 < i < q$$

Let $Nats = (1, 2, 3, 4, \dots)$. Then $Nats^{(2)} = (1, 0, 2, 0, 3, 0, 4, 0, 5, 0, \dots)$ and $Nats^{(3)} = (1, 0, 0, 2, 0, 0, 3, \dots)$ are examples of q -splays.

Some q -splay lemmas

Lemma (Reassemblage)

For all streams σ , $\sigma = \sum_{k=0}^{q-1} X^k \times (\pi_{k,q}(\sigma))^{(q)}$.

Proof.

By $(\text{hd}, \pi_{i,q})$ -bisimulation. The heads are equal:

$$\begin{aligned} \text{hd} \left(\sum_{k=0}^{q-1} X^k \times (\pi_{k,q}(\sigma))^{(q)} \right) &= \sum_{k=0}^{q-1} \text{hd}(X^k) \cdot \text{hd}(\pi_{k,q}(\sigma))^{(q)} \\ &= \text{hd}(\pi_{0,q}(\sigma))^{(q)} = \text{hd}(\sigma) \end{aligned}$$



Proof.

The derivatives are related. For $0 \leq i < q$:

$$\begin{aligned}
 \pi_{i,q} \left(\sum_{k=0}^{q-1} X^k \times (\pi_{k,q}(\sigma))^{(q)} \right) &= \sum_{k=0}^{q-1} \pi_{i,q}(X^k \times (\pi_{k,q}(\sigma))^{(q)}) \\
 &= \sum_{k=0}^{q-1} \left(\sum_{m=0}^i \pi_{m,q}(X^k) \times \pi_{i-m,q}(\pi_{k,q}(\sigma))^{(q)} \right. \\
 &\quad \left. + \sum_{m=i+1}^{q-1} X \times \pi_{m,q}(X^k) \times \pi_{q+i-m,q}(\pi_{k,q}(\sigma))^{(q)} \right) \\
 &= \sum_{k=0}^{q-1} \left(\pi_{i,q}(X^k) \times \pi_{i-i,q}(\pi_{k,q}(\sigma))^{(q)} + [0] \right) \\
 &= \sum_{k=0}^{q-1} \pi_{i,q}(X^k) \times \pi_{k,q}(\sigma) = [1] \times \pi_{i,q}(\sigma) = \pi_{i,q}(\sigma)
 \end{aligned}$$

Lemma (Partial cancel)

If $\sigma, \tau \in \Sigma^\omega$ and $0 \leq i < q$, then $\pi_{i,q}(\sigma \times \tau^{(q)}) = \pi_{i,q}(\sigma) \times \tau$.

Proof.

$$\begin{aligned}
 \pi_{i,q}(\sigma \times \tau^{(q)}) &= \sum_{k=0}^i \pi_{k,q}(\sigma) \times \pi_{i-k,q}(\tau^{(q)}) \\
 &\quad + \sum_{k=i+1}^{q-1} X \times \pi_{k,q}(\sigma) \times \pi_{q+i-k,q}(\tau^{(q)}) \\
 &= \pi_{i,q}(\sigma) \times \pi_{i-i,q}(\tau^{(q)}) \\
 &= \pi_{i,q}(\sigma) \times \tau
 \end{aligned}$$



Christol's theorem

Fix a prime q . We assume from here on that we're working with $\Sigma = \mathbb{F}_q$. The proof of Christol's theorem will take the form of two equivalences:

σ is algebraic over $\mathbb{F}_q \Leftrightarrow \sigma$ is q -splay dependent $\Leftrightarrow \sigma$ is q -automatic.

For all $n \in \mathbb{N}$, define $\sigma^{(q)^n} = \begin{cases} \sigma & \text{if } n = 0 \\ (\sigma^{(q)^{n-1}})^{(q)} & \text{if } n > 0. \end{cases}$

A stream σ is **q -splay dependent** means there are polynomials p_i , not all $[0]$, such that $\sum_{i=0}^k p_i \times \sigma^{(q)^i} = [0]$.

Proposition (Frobenius)

For all streams σ in characteristic q , $\sigma^{(q)} = \sigma^q$.

Proposition (Ore's theorem)

A stream σ is algebraic iff there are polynomials p_i , not all $[0]$, such that

$$\sum_{i=0}^k p_i \times \sigma^{q^i} = [0]$$

Corollary

For all streams σ in characteristic q , σ is algebraic iff σ is q -splay dependent.

Proposition (dependent \Leftrightarrow automatic)

If a stream $\sigma \in \Sigma^\omega$ is q -automatic, then it is q -splay dependent.

Proof.

Suppose σ is q -automatic, and let $K = \ker(\sigma)$. We know $|K| < \infty$. For each $n \in \mathbb{N}$, $\tau \in K$, we claim $\tau = \tau^{(q)^0}, \tau^{(q)^1}, \dots, \tau^{(q)^n} \in \text{span}(K^{(q)^{n+1}})$.

The Reassemblage Lemma is the $n = 0$ case.

For our induction step, we assume for all $\tau \in K$ we can write

$\tau^{(q)^n} = \sum p_i \times \kappa_i^{(q)^{n+1}}$ where $\kappa_i \in K$. Taking the q -splay of both sides

yields $\tau^{(q)^{n+1}} = \sum p_i^{(q)} \times \kappa_i^{(q)^{n+2}}$, so for all $\tau \in K$ we have

$\tau^{(q)^{n+1}} \in \text{span}(K^{(q)^{n+2}})$. This also shows that

$\text{span}(K^{(q)^{n+1}}) \subseteq \text{span}(K^{(q)^{n+2}})$, so we have completed our induction.

This gives us the q -splay dependency by taking $n = |K|$. □

Proposition (dependent(*) \Rightarrow automatic)

If a stream $\sigma \in \Sigma^\omega$ is q -splay dependent with leading coefficient [1] over a ring of characteristic q , then it is q -automatic.

Proof.

Suppose σ is q -splay dependent with leading coefficient [1], so

$\sum_{j=0}^t p_j \times \sigma^{(q)^j} = [0]$ where the p_j are polynomial, and $p_0 = [1]$. Let

$D = \max_{j \in [0, t]} (\deg(p_j))$ We consider

$$H = \left\{ \sum_{j=0}^t k_j \times \sigma^{(q)^j} : k_j \text{ polynomial, } \deg(k_j) < D \text{ and } k_t = 0 \right\}$$

and show H is closed under applications of $\pi_{i,q}$ with $0 \leq i < q$.

Proof.

Let's apply $\pi_{i,q}$ to a typical element of H .

$$\begin{aligned}
 \pi_{i,q} \left(\sum_{j=0}^t k_j \times \sigma^{(q)^j} \right) &= \pi_{i,q} \left(k_0 \times \sigma + \sum_{j=1}^t k_j \times \sigma^{(q)^j} \right) \\
 &= \pi_{i,q} \left(- \sum_{j=1}^t k_0 \times p_j \times \sigma^{(q)^j} + \sum_{j=1}^t k_j \times \sigma^{(q)^j} \right) \\
 &= \pi_{i,q} \left(\sum_{j=1}^t (k_j - k_0 \times p_j) \times \sigma^{(q)^j} \right) \\
 &= \sum_{j=1}^t \pi_{i,q}(k_j - k_0 \times p_j) \times \sigma^{(q)^{j-1}} = \sum_{j=0}^{t-1} \pi_{i,q}(k_{j+1} - k_0 \times p_{j+1}) \times \sigma^{(q)^j}
 \end{aligned}$$

□

To relax the assumption about $p_0 = [1]$, we just need to be able to divide by nonzero streams. To do this in the world of power series, one usually passes to the field of formal Laurent series. (Power series where you're allowed finitely many negative degree terms.) There is an analogous way to do this in streams via Laurent streams.

With this done, we've shown a stream is q -splay dependent iff it is q -automatic. Hence, we've proven Christol's theorem!

Thanks!