A logic of Laurent streams

David Sprunger

Indiana University

April 26, 2015

Introduction

A formal power series $A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \cdots$ is **algebraic (over $\mathbb{F}_q[x]$)** means it is the root of some nonzero polynomial (in $\mathbb{F}_q[x][t]$). That is,

$$p_0 + p_1 \times A + p_2 \times A^2 + \cdots + p_n \times A^n = 0$$

for some $p_i \in \mathbb{F}_q[x]$ not all zero.

Introduction

A formal power series $A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \cdots$ is **algebraic (over $\mathbb{F}_q[x]$)** means it is the root of some nonzero polynomial (in $\mathbb{F}_q[x][t]$). That is,

$$p_0 + p_1 \times A + p_2 \times A^2 + \cdots + p_n \times A^n = 0$$

for some $p_i \in \mathbb{F}_q[x]$ not all zero.

A stream $a = (a_0, a_1, a_2, a_3, a_4, \ldots)$ is **q-automatic** means there is a finite automaton which will output a_n when run on the base q representation of n.

Introduction

A formal power series $A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \cdots$ is **algebraic (over $\mathbb{F}_q[x]$)** means it is the root of some nonzero polynomial (in $\mathbb{F}_q[x][t]$). That is,

$$p_0 + p_1 \times A + p_2 \times A^2 + \cdots + p_n \times A^n = 0$$

for some $p_i \in \mathbb{F}_q[x]$ not all zero.

A stream $a = (a_0, a_1, a_2, a_3, a_4, \ldots)$ is **q-automatic** means there is a finite automaton which will output a_n when run on the base q representation of n.

Theorem (Christol (1980))

A power series is algebraic over $\mathbb{F}_q[x]$ iff the stream of its coefficients is q-automatic.

Christol's theorem: questions

Christol's theorem: questions

1. So what?

Christol's theorem: questions

1. So what?

   Question 1: If A and B are two algebraic power series, is $C = a_0 b_0 + a_1 b_1 x + a_2 b_2 x^2 + \cdots$ algebraic?

Christol's theorem: questions

1. So what?

   Question 1: If A and B are two algebraic power series, is $C = a_0 b_0 + a_1 b_1 x + a_2 b_2 x^2 + \cdots$ algebraic?

   Question 2: If A is algebraic over $\mathbb{F}_q[x]$ and $\mathbb{F}_p[x]$, can we say anything interesting about it?

Christol's theorem: questions

1. So what?

   Question 1: If A and B are two algebraic power series, is $C = a_0 b_0 + a_1 b_1 x + a_2 b_2 x^2 + \cdots$ algebraic?

   Question 2: If A is algebraic over $\mathbb{F}_q[x]$ and $\mathbb{F}_p[x]$, can we say anything interesting about it?

2. An example?

Christol's theorem: questions

1. So what?

   Question 1: If A and B are two algebraic power series, is $C = a_0 b_0 + a_1 b_1 x + a_2 b_2 x^2 + \cdots$ algebraic?

   Question 2: If A is algebraic over $\mathbb{F}_q[x]$ and $\mathbb{F}_p[x]$, can we say anything interesting about it?

2. An example?

   $A = 1 + x + x^2 + x^3 + \cdots$ is algebraic over $\mathbb{F}_2[x]$, being the root of $1 + (x - 1) \times t$, and 2-automatic by a one-state machine.

Christol's theorem: questions

1. So what?

   Question 1: If A and B are two algebraic power series, is $C = a_0 b_0 + a_1 b_1 x + a_2 b_2 x^2 + \cdots$ algebraic?

   Question 2: If A is algebraic over $\mathbb{F}_q[x]$ and $\mathbb{F}_p[x]$, can we say anything interesting about it?

2. An example?

   $A = 1 + x + x^2 + x^3 + \cdots$ is algebraic over $\mathbb{F}_2[x]$, being the root of $1 + (x - 1) \times t$, and 2-automatic by a one-state machine.

3. Why again?

Christol's theorem: questions

1. So what?

   Question 1: If A and B are two algebraic power series, is $C = a_0 b_0 + a_1 b_1 x + a_2 b_2 x^2 + \cdots$ algebraic?

   Question 2: If A is algebraic over $\mathbb{F}_q[x]$ and $\mathbb{F}_p[x]$, can we say anything interesting about it?

2. An example?

   $A = 1 + x + x^2 + x^3 + \cdots$ is algebraic over $\mathbb{F}_2[x]$, being the root of $1 + (x - 1) \times t$, and 2-automatic by a one-state machine.

3. Why again?

   Coalgebra.

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:

$$\begin{aligned}
\mathtt{hd} &: \Sigma^\omega \to \Sigma & \mathtt{hd}(\sigma) &= \sigma_0 \\
\mathtt{tl} &: \Sigma^\omega \to \Sigma^\omega & \mathtt{tl}(\sigma) &= (\sigma_1, \sigma_2, \sigma_3, \ldots) \\
\pi_{a,b} &: \Sigma^\omega \to \Sigma^\omega & \pi_{a,b}(\sigma) &= (\sigma_a, \sigma_{a+b}, \sigma_{a+2b}, \ldots)
\end{aligned}$$

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.

For all $b > 0$, a $(\mathtt{hd}, \pi_{a,b})$-**bisimulation** is a relation $R \subseteq \Sigma^\omega \times \Sigma^\omega$ such that for all $(\sigma, \tau) \in R$ the following hold:

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

The case $b = 1$ is so commonly used we give it a special name. A $(\mathtt{hd}, \mathtt{tl})$-**bisimulation** is a relation $R \subseteq \Sigma^\omega \times \Sigma^\omega$ such that for all $(\sigma, \tau) \in R$ the following hold:

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

Theorem (Coinduction for streams)

Let Δ be the diagonal relation on Σ^ω. If R is a $(\mathtt{hd}, \pi_{a,b})$-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.

$[a] = (a, 0, 0, 0, \ldots)$
Corecursively, $[a]$ is the unique stream satisfying

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

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

$$\mathtt{hd}(X) = 0$$
$$\mathtt{tl}(X) = [1]$$

Power series form a ring, so let's give a ring structure to streams. If

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

then we want

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

Power series form a ring, so let's give a ring structure to streams. If

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

then we want

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

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

$$\mathtt{hd}(\sigma + \tau) = \mathtt{hd}(\sigma) + \mathtt{hd}(\tau)$$
$$\mathtt{tl}(\sigma + \tau) = \mathtt{tl}(\sigma) + \mathtt{tl}(\tau)$$

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

The (Cauchy) product of power series is given by

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

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

The (Cauchy) product of power series is given by

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

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

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

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

The (Cauchy) product of power series is given by

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

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

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

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

The (Cauchy) product of power series is given by

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

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

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

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

Let's prove some easy facts about stream operations using coinduction.

Fact 1 ([0] is the additive identity)

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

Proof.

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

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

And the tails stay in the relation:
$\mathtt{tl}([0] + \sigma) = \mathtt{tl}([0]) + \mathtt{tl}(\sigma) = [0] + \mathtt{tl}(\sigma)\ R\ \mathtt{tl}(\sigma)$. □

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:

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

The tails are (almost) related:

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

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:

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

The tails are (almost) related:

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

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:

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

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.*

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.*

We also could develop an analog to formal Laurent series (series with finitely many negative exponents).

Definition

A **Laurent stream** is $(\sigma, n) \in (\Sigma^\omega \times \mathbb{Z})/\equiv$, where $\equiv$ is the equivalence relation generated by $(\sigma, n) \equiv (\sigma \times X^m, n - m)$ for all $m \in \mathbb{N}$.

Theorem

If Σ is a field, then Laurent streams with associated $+$ and $\times$ operations is a field.

Algebraic and automatic streams

Definition

A stream σ is **algebraic** means there is $k \in \mathbb{N}$ and polynomial streams 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 any of the following equivalent conditions are satisfied:

1. There is a finite automaton which outputs σ_n when run on the base q representation of n.
2. K—the minimum set of streams containing σ and closed under applications of $\pi_{i,q}$ where $0 \leq i < q$—is finite.
3. $K = \{\pi_{i,q^k}(\sigma) : k \in \mathbb{N}, 0 \leq i < q^k\}$ is finite.

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

$$M = 01101001100101101001011001101001\ldots$$

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

$$\pi_{0,2}(M) = 0110100110010110\ldots = M$$
$$\pi_{1,2}(M) = 1001011001101001\ldots = \overline{M}$$
$$\pi_{0,2}(\overline{M}) = 1001011001101001\ldots = \overline{M}$$
$$\pi_{1,2}(\overline{M}) = 0110100110010110\ldots = M$$

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

$$M = 0110100110010110100101100110100\ldots$$
$$X^2 \times M = 0001101001100101101001011001101\ldots$$
$$([1] + X^2) \times M = 0111001111110011001100111111001\ldots$$

$$M^2 = 0010100010000010100000100010100\ldots$$
$$([1] + X + X^2 + X^3) \times M^2 = 0011001111110011001100111111001\ldots$$

"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

We'll need to be applying $\pi_{i,q}$ 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:

$$\pi_{i,q}(\sigma + \tau) = \pi_{i,q}(\sigma) + \pi_{i,q}(\tau)$$

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

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

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

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_3 + \sigma_1\tau_2 + \sigma_2\tau_1 + \sigma_3\tau_0, \ldots)$$

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

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

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_3 + \sigma_1\tau_2 + \sigma_2\tau_1 + \sigma_3\tau_0, \ldots)$$

That looks like the sum of two different stream products!

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

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

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_3 + \sigma_1\tau_2 + \sigma_2\tau_1 + \sigma_3\tau_0, \ldots)$$

That looks like the sum of two different stream products!

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

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

which implies

$$\pi_{1,2}(\sigma \times \tau) = (\sigma_0\tau_1 + \sigma_1\tau_0, \sigma_0\tau_3 + \sigma_1\tau_2 + \sigma_2\tau_1 + \sigma_3\tau_0, \ldots)$$

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 $\mathtt{tl}(\pi_{k,b}(\sigma)) = \pi_{k+b,b}(\sigma)$.

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 $\mathtt{tl}(\pi_{k,b}(\sigma)) = \pi_{k+b,b}(\sigma)$.

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 $b \neq 0$,

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

Proof.

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

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 $Nats = (1, 2, 3, 4, \ldots)$. Then $Nats^{(2)} = (1, 0, 2, 0, 3, 0, 4, 0, 5, 0, \ldots)$ and $Nats^{(3)} = (1, 0, 0, 2, 0, 0, 3, \ldots)$ 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 $(\mathrm{hd}, \pi_{i,q})$-bisimulation. The heads are equal:

$$\mathrm{hd}\left(\sum_{k=0}^{q-1} X^k \times (\pi_{k,q}(\sigma))^{(q)}\right) = \sum_{k=0}^{q-1} \mathrm{hd}(X^k) \cdot \mathrm{hd}(\pi_{k,q}(\sigma)^{(q)})$$
$$= \mathrm{hd}(\pi_{0,q}(\sigma)^{(q)}) = \mathrm{hd}(\sigma)$$

Proof.

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

$$\pi_{i,q}\left(\sum_{k=0}^{q-1} X^k \times (\pi_{k,q}(\sigma))^{(q)}\right) = \sum_{k=0}^{q-1} \pi_{i,q}(X^k \times (\pi_{k,q}(\sigma))^{(q)})$$

$$= \sum_{k=0}^{q-1}\left(\sum_{m=0}^{i} \pi_{m,q}(X^k) \times \pi_{i-m,q}(\pi_{k,q}(\sigma)^{(q)})\right.$$

$$\left. + \sum_{m=i+1}^{q-1} X \times \pi_{m,q}(X^k) \times \pi_{q+i-m,q}(\pi_{k,q}(\sigma)^{(q)})\right)$$

$$= \sum_{k=0}^{q-1}\left(\pi_{i,q}(X^k) \times \pi_{i-i,q}(\pi_{k,q}(\sigma)^{(q)}) + [0]\right)$$

$$= \sum_{k=0}^{q-1} \pi_{i,q}(X^k) \times \pi_{k,q}(\sigma) = [1] \times \pi_{i,q}(\sigma) = \pi_{i,q}(\sigma)$$

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 $\mathbb{F}_q[X] \Leftrightarrow \sigma$ 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, $\sigma^{(q)} = \sigma^q$.

(Quick reminder: $(1+x)^2 = 1 + 2x + x^2 = 1 + x^2$ in char 2.)

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 $\Leftarrow$ 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 $\tau = \tau^{(q)^0}, \tau^{(q)^1}, \ldots, \tau^{(q)^n} \in \text{span}(K^{(q)^{n+1}})$.

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 zero-degree coefficient [1] over a ring of characteristic q, then it is q-automatic.

Proof.

Suppose σ is q-splay dependent with zero-degree 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.

$$\pi_{i,q}\left(\sum_{j=0}^{t} k_j \times \sigma^{(q)^j}\right) = \pi_{i,q}\left(k_0 \times \sigma + \sum_{j=1}^{t} k_j \times \sigma^{(q)^j}\right)$$

$$= \pi_{i,q}\left(-\sum_{j=1}^{t} k_0 \times p_j \times \sigma^{(q)^j} + \sum_{j=1}^{t} k_j \times \sigma^{(q)^j}\right)$$

$$= \pi_{i,q}\left(\sum_{j=1}^{t} (k_j - k_0 \times p_j) \times \sigma^{(q)^j}\right)$$

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

□

To relax the assumption about $p_0 = [1]$, we just need to be able to divide by nonzero streams. Fortunately, Laurent streams allow us to do precisely this, from which we get the rest of the result.

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

Future work

Proof systems involving bisimulations typically focus on process calculi and have a lot of use in concurrent systems. Can we extend or develop new ones applicable to mathematical coalgebras?

Christol's theorem is a starting point in the algebraic theory of formal power series. Can we extend this method to further results in this vein?

Are there other identities involving other stream operations and projections?

Thanks!