Factorisation in the semiring of Finite Dynamical Systems

https://arxiv.org/abs/2210.11270

Émile Naquin and Maximilien Gadouleau

Department of Computer Science, Durham University

York Semigroup
2022-10-26

Outline

Outline

Introduction to FDSs

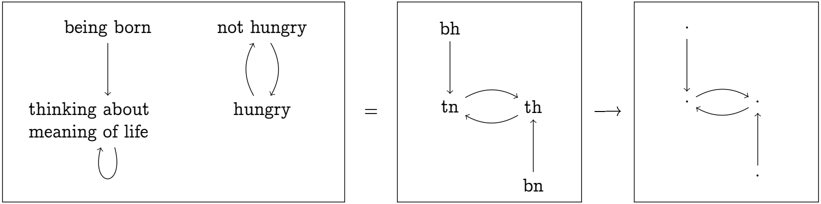
Three problems related to product decomposition

Using infinite trees

Outlook

Context 1

Consider the “philosopher” system:



We do not know the internal logic, but we can make the difference between two different internal states of the grey-box.

The main problem is to determine how to “break down” this into smaller subsystems.

Context 2

We consider finite, deterministic, discrete-time dynamical systems (FDS).

Two natural operations (Dennunzio et al. 18):

- Sum: two independent systems, a trajectory is completely contained in the system it starts in.
- Product: two independent systems, running in parallel.

Semiring of FDSs, formally

An FDS is a mapping $A : S_A \to S_A$, where S_A is finite.

We consider FDSs up to equivalence: $A \cong B$ if and only if there exists $\phi : S_A \to S_B$ with $A\phi = \phi B$.
Then $\mathbb{D}$ is the set of equivalence classes, i.e. of functional graphs.

We can then always assume that S_A and S_B are disjoint for all $A \neq B$.

Sum: $C = A + B$ with $S_C = S_A \cup S_B$ and

$$C(x) = \begin{cases} A(x) & \text{if } x \in S_A \\ B(x) & \text{if } x \in S_B. \end{cases}$$

Product: $D = AB$ with $S_D = S_A \times S_B$ and

$$D(a, b) = (A(a), B(b)).$$

Basic semiring/semigroup results

$\mathbb{D}$ with sum and product forms a semiring with

- additive identity the empty map $\varnothing : \emptyset \to \emptyset$;
- multiplicative identity the fixpoint C_1.

The sum semigroup is too easy, so we focus on product for now.

The product semigroup is $\mathcal{J}$-trivial, the only regular element is the identity.

It contains $\mathbb{N}$, $\mathbb{N}[X]$, $\mathbb{N}[X, Y]$, etc.

Outline

Introduction to FDSs

Three problems related to product decomposition

Using infinite trees

Outlook

Three problems

Let $A \in \mathbb{D}$. We consider three ways of "breaking down" A into smaller subsystems.

1. Factorisation: Is A reducible, i.e. are there B, C with $|B|, |C| < |A|$ such that $A = BC$? Is the factorisation into irreducibles unique?
2. Division: given B and A a multiple of B, what is (are?) C such that $A = BC$?
3. Root: What B satisfy(ies) $B^k = A$?

For each problem, there is an algebraic question (what?) and an algorithmic one (how?).

Non-unique factorisation

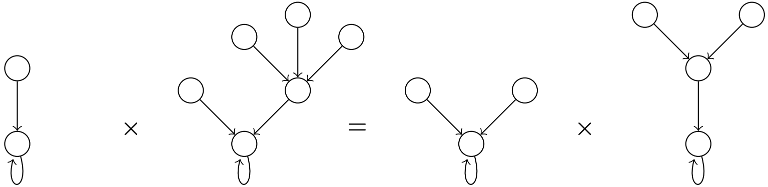
Factorisation into irreducible FDSs is not unique: e.g.

$$C_2 \times C_2 = 2C_1 \times C_2.$$

In fact, more generally we have

$$C_a C_b = \mathrm{lcm}(a, b)\, C_{\gcd(a,b)}.$$

The same problem arises for dendrons, i.e. connected FDSs with a fixpoint:



Irreducible and prime FDSs

(Dorigatti 17) Almost all FDSs are irreducible, i.e.

$$\frac{|\{\text{irreducible FDSs of size } n\}|}{|\{\text{FDSs of size } n\}|} \to 1.$$

An FDS A is prime if

$$A \mid BC \implies A \mid B \text{ or } A \mid C.$$

Currently, no prime FDSs are known!
(Couturier 21) gives some necessary conditions for primality.

Our results

Today I will focus on three results from (Naquin, Gadouleau 22).

Say A is cancellative if $AX = AY \implies X = Y$ for all X, Y.

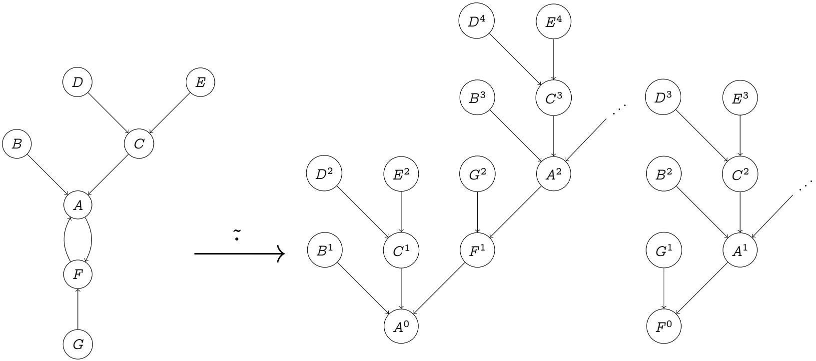
1. Theorem: (Cancellativity with connected FDSs)
   For any FDS A, $AX = AY \implies X = Y$ whenever X and Y are both connected.
2. Theorem: (Classification of cancellative FDSs)
   A is cancellative iff it has a fixpoint.
3. Theorem: (Unicity of k-th roots)
   For any $k \geq 1$ and $B, C \in \mathbb{D}$, $B^k = C^k \implies B = C$.

We will go through the main tool to prove these results, and use it to prove the first one.

Outline

Products on (possibly infinite) trees

Our strategy is to recast product problems about FDSs into similar problems for infinite trees and forests. We do so thanks to the unrolling construction below.



Its unrolling $\widetilde{S}$

An FDS S

Product on trees

The product on trees is done level by level.

We then have $\widetilde{AB} = \widetilde{A}\widetilde{B}$.

The main result is then that the semigroup of infinite trees is cancellative.
Theorem: If T_1, T_2, T_3 are infinite trees, then
$T_1 T_2 = T_1 T_3 \implies T_2 = T_3$.

Note that (Doré et al 22) also introduce the unrollings, and prove the same cancellativitity result for trees, but they use a different proof and use it for different ends.

Application

Theorem: If $AX = AY$ with X, Y connected, then $X = Y$.

Lemma: If X, Y are connected and have the same periodic part, then $\widetilde{X} = \widetilde{Y} \implies X = Y$.

Proof of Theorem:

1. X and Y have the same periodic part.
   The periodic part of X is C_x, that of Y is C_y. Let A have n periodic points, then $AX = AY$ has $nx = ny$ periodic points, thus $x = y$.
2. Then

$$AX = AY \implies \widetilde{AX} = \widetilde{AY} \implies \tilde{A}\tilde{X} = \tilde{A}\tilde{Y} \implies \tilde{X} = \tilde{Y} \implies X = Y$$

A semiring consequence

Theorem: A is cancellative iff it has a fixpoint.

Corollary: Let $P(X) = \sum_{i=0}^{d} P_i X^i$ be a polynomial in $\mathbb{D}[X]$. If P_1 has a fixpoint, then P is injective.

Idea of proof: Without loss, $P_0 = 0$. Suppose $P(A) = P(B)$ and define

$$D = \sum_{i=1}^{d} P_i \sum_{j=0}^{i-1} A^{i-1-j} B^j.$$

Then $D = P_1 + Q$ has a fixpoint and $AD = BD$, thus $A = B$.

Outline

Outlook

Some interesting open problems:

1. Which polynomials are injective? This would be the major result in terms of "unicity of decomposition."
2. Complexity of (simple) problems, notably division of permutations.
3. Are there any prime FDSs? I conjecture that there aren't any!

We need more algebra:

1. Classical problems/results from semirings?
2. Using Grothendieck group, ring, field of fractions, etc.