Polynomial Equations over Finite, Discrete-Time Dynamical Systems*

Alberto Dennunzio[1], Valentina Dorigatti[1], Enrico Formenti[2],
Luca Manzoni[1], and Antonio E. Porreca[1]

[1] Dipartimento di Informatica, Sistemistica e Comunicazione
Università degli Studi di Milano-Bicocca
Viale Sarca 336/14, 20126 Milano, Italy
dennunzio@disco.unimib.it, v.dorigatti@campus.unimib.it,
luca.manzoni@disco.unimib.it, porreca@disco.unimib.it
[2] Universite Côte d'Azur, CNRS, I3S, France
enrico.formenti@unice.fr

Abstract. We introduce an algebraic approach for the analysis and composition of finite, discrete-time dynamical systems based on the category-theoretical operations of product and sum (coproduct). This allows us to define a semiring structure over the set of dynamical systems (modulo isomorphism) and, consequently, to express many decomposition problems in terms of polynomial equations. We prove that these equations are, in general, algorithmically unsolvable, but we identify a solvable subclass. Finally, we describe an implementation of the semiring operations for the case of finite cellular automata.

1 Introduction

Discrete dynamical systems are a formal tool widely used in applications to model real phenomena. Even if this formalism provides very interesting results, the overall theory is still a hot research topic. In this paper, we are going to adopt an abstraction of the formalism of (finite) discrete dynamical systems in order to provide general results which are valid for all the systems. The underlying idea is that in the abstract view one can find patterns that are simpler to study and precisely define and, in a second step, these patterns can be assembled to help studying complex particular cases. For example, consider the finite dynamical systems which are bijective. Their dynamics is represented by a graph which is made of disjoint cycles and which coincides with the graph of a permutation. Assume that from experimental data one knows that the phenomenon being modelled has a certain number of periodic orbits. Then, it is natural to wonder whether the observed system is composed of smaller parts and the overall behaviour has some variables. In our setting this translates into

* Enrico Formenti has been partially supported by PACA APEX FRI project. Luca Manzoni was partially supported by "Premio giovani talenti 2017" of Università degli Studi di Milano-Bicocca and Accademia dei Lincei.

the formulation of an equation on dynamical systems in which the unknowns multiply the expected patterns. Unfortunately, we prove that solving equations over dynamical systems is algorithmically infeasible in the general case, even in the case of polynomial equations (Theorem 1). However, if one of the two sides of the equations is constant, then the problem of finding the roots turns out to be in **NP** (Theorem 2). We believe it to actually be complete, and we suspect that its weaker versions are good candidates for the class of **NP**-intermediate problems. As a concrete example, we show that (finite) cellular automata are a subsemiring of the semiring **D** of (finite) discrete dynamical system and that, indeed, they are isomorphic to the whole **D**.

The paper is structured as follows. The next section introduces the formalism and basic concepts. It also provides a first example of a subsemiring (Proposition 1). Section 3 introduces the concept of equations over dynamical systems and the main results of the paper. Cellular automata and their subsemiring are introduced in Section 4. In the last section we draw our conclusions and provide several research directions for further developments.

2 The Semiring of Dynamical Systems

In this paper, a *(finite, discrete-time) dynamical system* is any pair (D, f) where D is a finite set of *states* and $f\colon D \to D$ is the *next-state function* which maps each state to the next one. We sometimes refer to (D, f) simply as D when the function f is implied by the context. We also allow $D = \varnothing$ as a legitimate set of states; in that case, f is necessarily the empty function.

Given a dynamical system, one can consider the graph of its dynamics $G(D, f)$ having the states D as vertices, and those edges $(x, y) \in D^2$ such that $f(x) = y$. A graph represents the dynamics of a dynamical system if and only if it is *functional*, *i.e.*, each vertex has outdegree exactly 1; since there is a bijection between dynamical systems and functional graphs, we sometimes refer interchangeably to a dynamical system and the graph of its dynamics.

Finite dynamical systems form a category **D** [3, p. 136], where arrows $(D, f) \to (E, g)$ are given by functions $\varphi\colon D \to E$ compatible with the two dynamics: $g \circ \varphi = \varphi \circ f$. This category has an initial object $\mathbf{0}$ (the empty dynamical system) and terminal objects $\mathbf{1}$ (any single-state dynamical system with the identity function). Furthermore, this category has products:

$$(D, f) \times (E, g) = (D \times E, f \times g) \qquad \text{where } (f \times g)(d, e) = (f(d), g(e))$$

which corresponds to the tensor product of the graphs of the dynamics, and coproducts (or sums):

$$(D, f) + (E, g) = (D \sqcup E, f + g) \qquad \text{where } (f + g)(x) = \begin{cases} f(x) & \text{if } x \in D \\ g(x) & \text{if } x \in E \end{cases}$$

which corresponds to the disjoint union of the graphs of the dynamics.

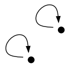
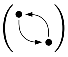
The product $D \times E$ defined above consists in the parallel, synchronous execution of the two dynamical systems D and E. The sum $D + E$ is the mutually exclusive alternative between the behaviour of D and the behaviour of E; the resulting dynamical system behaves as one of the two terms, depending on its initial state.

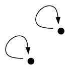
In this paper we are only interested in the dynamics of dynamical systems, irrespective of the precise nature of their states and their next-state functions. In other words, we consider dynamical systems having isomorphic graphs of their dynamics as identical. With this convention, the objects of the category $\mathbf{D}$ of finite dynamical systems are a countable set rather than a proper class, and the operations of sum (coproduct) and product give it a *commutative semiring* structure *with zero and identity* [2]. Indeed, as can be easily checked from the definitions above:

- $(\mathbf{D}, +)$ is a commutative monoid with neutral element $\mathbf{0}$,
- $(\mathbf{D}, \times)$ is a commutative monoid with neutral element $\mathbf{1}$,
- products distribute over sums: $x \times (y + z) = x \times y + x \times z$.

Notice that this semiring is not a ring, since no element (besides the trivial case of $\mathbf{0}$) possesses an additive inverse; furthermore, the only element invertible with respect to the product is trivially $\mathbf{1}$. This follows immediately from the fact that sum and product are monotonic with respect to the sizes of the dynamical systems. On the other hand, this same property guarantees us that $\mathbf{D}$ is an integral semiring, *i.e.*, there are no zero divisors.

While the graphs of the dynamics of the sum of two dynamical systems simply consist of the juxtaposition of the graphs of the two terms, the product generates more interesting results, as shown in Fig. 1. Just by looking at the Cayley table of the monoid $(\mathbf{D}, \times)$, we can already observe that the semiring $\mathbf{D}$ does not possess unique factorisations. Indeed, we have

 $\times$ $=$ $\Big($  $\Big)^2$

and both  and are irreducible (any nontrivial factorisation would otherwise appear, due to its size, in the Cayley table of Fig. 1).

Another interesting property of $\mathbf{D}$ is that it contains the semiring of the natural numbers, which is initial in the category of commutative semirings.

Proposition 1. *The semiring* $\mathbf{D}$ *contains a subsemiring* $\mathbf{N}$ *isomorphic to the natural numbers.*

Proof. For each $n \in \mathbb{N}$, let $\varphi(n) \in \mathbf{D}$ be the dynamical system consisting of exactly n fixed points (*i.e.*, the identity function over a set of n points), and let $\mathbf{N} = \varphi(\mathbb{N})$. Clearly $\mathbf{N}$ contains both $\mathbf{0} = \varphi(0)$ and $\mathbf{1} = \varphi(1)$. Given $\varphi(m), \varphi(n) \in \mathbf{N}$ we have $\varphi(m) + \varphi(n) = \varphi(m + n) \in \mathbf{N}$ and $\varphi(m) \times \varphi(n) = \varphi(n \times m) \in \mathbf{N}$. Finally, we have $\varphi(m) = \varphi(n)$ if and only if $m = n$. This means that φ is a semiring monomorphism, and that its image $\mathbf{N}$ is a subsemiring of $\mathbf{D}$ isomorphic to $\mathbb{N}$. $\square$

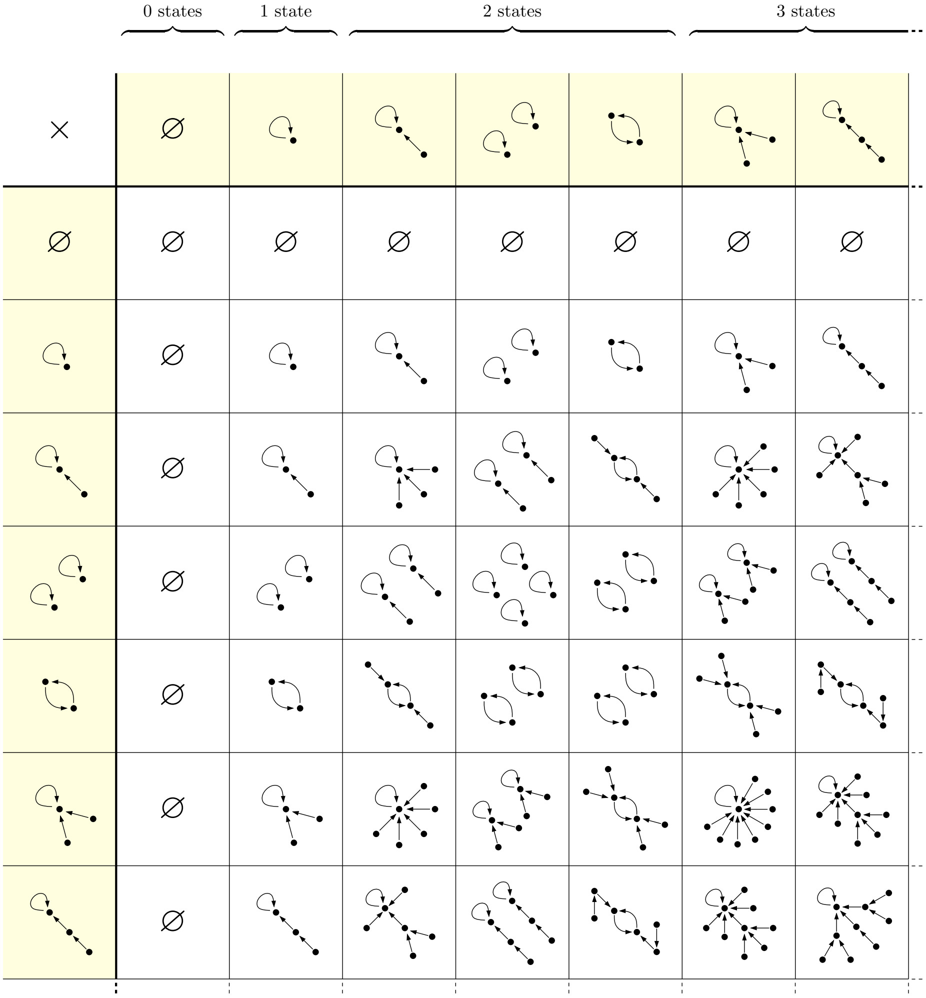


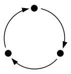
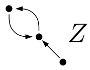
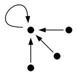
Fig. 1. A portion of the Cayley table of the commutative monoid $(\mathbf{D}, \times)$, including products of all dynamical systems with 0, 1, and 2 states, as well as some dynamical systems with 3 states, in increasing order of size (and arbitrary order among those with the same size).

Due to Proposition 1, in the following we will denote the subsemiring $\mathbf{N}$ of $\mathbf{D}$ simply by $\mathbb{N}$.

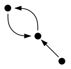
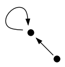
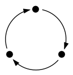
3 Polynomial Equations

Having equipped the dynamical systems $\mathbf{D}$ with a semiring algebraic structure allows us to formulate a number of problems in terms of polynomial equations. Recall that the polynomials over a commutative semiring are themselves a commutative semiring; in our case, we deal with polynomials over several variables $\mathbf{D}[X_1, \ldots, X_k]$.

One basic problem is to analyse a given dynamical system D in terms of smaller, simpler components. For instance, a solution to an equation of the form

 $X + Y^2 =$  $Z +$ 

allows us to express the (parametric) behaviour on the right-hand side in terms of a possibly different set of components combined as described on the left-hand side. One possible solution is

$X =$  $Y =$  $Z =$ 

In a ring R, by moving all terms on the left-hand side, any polynomial equation can be expressed as $p(\vec{X}) = 0$ with $\vec{X} = (X_1, \ldots, X_k)$ a set of variables and $p \in R[\vec{X}]$ a polynomial. In a proper semiring this is generally impossible, due to the lack of additive inverses; in our case, due to the above-mentioned monotonicity of + and × with respect to the sizes of dynamical systems, the equations of the form $p(\vec{X}) = \mathbf{0}$ are actually trivial, as they only admit the solution $\vec{X} = \vec{\mathbf{0}}$ when the constant term of p is null, and no solution otherwise. A general polynomial equation in $\mathbf{D}$ will then have the form $p(\vec{X}) = q(\vec{X})$ with $p, q \in \mathbf{D}[\vec{X}]$.

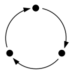
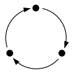
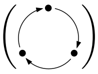
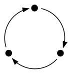
Given a set of variables $\vec{X} = (X_1, \ldots, X_k)$, a polynomial $p \in \mathbf{D}[\vec{X}]$, where the maximum degree of each variable is d, can be denoted by

$$p = \sum_{\vec{i} \in [0,d]^k} a_{\vec{i}} \vec{X}^{\vec{i}} \qquad \text{with } \vec{X}^{\vec{i}} = \prod_{j=1}^{k} X_j^{i_j}$$

Unfortunately, the algorithmic solution of polynomial equations over $\mathbf{D}$ turns out to be impossible by reduction from Hilbert's tenth problem [4]. This is not an immediate corollary of Proposition 1, since a polynomial equation over $\mathbb{N}$ might admit non-natural solutions in the larger semiring $\mathbf{D}$ of dynamical systems[3]; for

[3] While the existence of integer roots of a polynomial in $\mathbb{Z}[X]$ is undecidable, the existence of roots in the larger ring of real numbers is decidable, and the problem becomes even trivial for complex roots (due to the fundamental theorem of algebra).

instance, the equation $2X^2 = 3Y$ has the non-natural solution

$X =$  $Y = 2$  since $\Big($  $\Big)^2 = 3$ 

However, this equation obviously also has the natural solution $X = 3, Y = 6$ (uncoincidentally, these are the sizes of the dynamical systems of the previous solution). As we are going to show, this is actually a general property of equations over $\mathbb{N}$: by moving to the larger semiring $\mathbf{D}$ we might be able to find extra solutions, but only if there already exists a natural one.

Given a dynamical system $D \in \mathbf{D}$, let $|D|$ denote the size of its set of states.

Lemma 1. *The function* $|\cdot|\colon \mathbf{D} \to \mathbb{N}$ *is a semiring homomorphism.*

Proof. Clearly $|\mathbf{0}| = 0$ and $|\mathbf{1}| = 1$. Since sums and products in $\mathbf{D}$ respectively involve the disjoint union and the Cartesian product of the sets of states, we have $|D_1 + D_2| = |D_1| + |D_2|$ and $|D_1 \times D_2| = |D_1| \times |D_2|$. □

Lemma 2. *Let* $\vec{X} = (X_1, \dots, X_k)$ *be variables, let* $p, q \in \mathbb{N}[\vec{X}]$ *be polynomials, and suppose that* $p(\vec{D}) = q(\vec{D})$ *for some* $\vec{D} \in \mathbf{D}^k$*. Then, there exists* $\vec{n} \in \mathbb{N}^k$ *such that* $p(\vec{n}) = q(\vec{n})$*.*

Proof. Let $\vec{D} = (D_1, \dots, D_k) \in \mathbf{D}^k$ and suppose

$$p = \sum_{\vec{i} \in [0,d]^k} a_{\vec{i}} \vec{X}^{\vec{i}} \qquad\qquad q = \sum_{\vec{i} \in [0,d]^k} b_{\vec{i}} \vec{X}^{\vec{i}}$$

Since $p(\vec{D}) = q(\vec{D})$, we also have $|p(\vec{D})| = |q(\vec{D})|$, and since $|\cdot|$ is a semiring homomorphism (Lemma 1), this means that

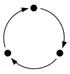
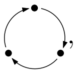
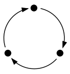
$$\sum_{\vec{i} \in [0,d]^k} a_{\vec{i}} |\vec{D}^{\vec{i}}| \quad = \quad \sum_{\vec{i} \in [0,d]^k} b_{\vec{i}} |\vec{D}^{\vec{i}}| \qquad \text{with } |\vec{D}^{\vec{i}}| = \prod_{j=1}^{k} |D_j|^{i_j}$$

or, in other words, that $p(|\vec{D}|) = q(|\vec{D}|)$, where $|\vec{D}| = (|D_1|, \dots, |D_k|)$. By letting $\vec{n} = |\vec{D}|$, the thesis follows. □

Since, by Proposition 1, every natural solution to a polynomial equation over $\mathbb{N}$ is also a dynamical system, we obtain that each equation over $\mathbb{N}$ has a solution in $\mathbf{D}$ if and only if it has a solution in $\mathbb{N}$. The latter is a variant of Hilbert's tenth problem [4], proving our problem also algorithmically unsolvable.

Theorem 1. *The problem of deciding whether a general polynomial equation over* $\mathbf{D}$ *admits a solution (and, by implication, finding one such solution when it is the case) is undecidable.* □

Remark 1. Notice that, although polynomial equations over $\mathbb{N}$ with solutions in $\mathbf{D}$ always admit a natural solution, this is not always the case for equations with more general coefficients; for instance

$X^2 = Y +$  has the solution $X =$ , $Y = 2$ 

but cannot have a solution with natural X, since X^2 would also be natural, while the right-hand side of the equation is never natural.

The equations become algorithmically solvable if one side is a constant, *i.e.*, if the equation has the form $p(\vec{X}) = D$ with $p \in \mathbf{D}[\vec{X}]$ and $D \in \mathbf{D}$. Indeed, in that case the size $|D|$ of the right-hand side of the equation allows us to perform a bounded search: due to the monotonicity of + and × with respect to the sizes of the dynamical system, each dynamical system of an assignment to $\vec{X}$ satisfying the equation (excluding any redundant variables which only appear with coefficient 0) has size at most $|D|$.

Assuming that the coefficients of the polynomials are given in input as explicit graphs, the value of each variable can be guessed in polynomial time by a nondeterministic Turing machine; the solution can then be checked by evaluating the polynomial on the left-hand side, with the caveat that we must halt and reject as soon as the partial result becomes larger than the right-hand side (this avoids a potentially exponential increase of the evaluated graph due to a polynomial of large degree). Finally, we need to check whether the evaluated left-hand side and the right-hand side of the equation are isomorphic, which can easily be performed by guessing an isomorphism between the two graphs. We can therefore conclude that

Theorem 2. *The problem of finding solutions of polynomial equations over* $\mathbf{D}$ *with a constant side is in* **NP**.

4 The Semiring of Cellular Automata

When dealing with a semiring, one interesting problem to tackle in order to understand its structure is to find its subsemirings. In the case of the semiring $\mathbf{D}$ specifically, it is also important to establish whether specific kinds of dynamical systems correspond to subsemirings or other subsets, such as ideals.

Let us consider finite, one-dimensional cellular automata (A, n, r, λ), where A is the alphabet of states, n the number of cells, r the radius and $\lambda \colon A^{2r+1} \to A$ the local rule; we also assume cyclic boundary conditions for simplicity.

The additive identity $\mathbf{0}$ of $\mathbf{D}$ has the empty graph as its dynamics; in terms of cellular automata this corresponds to length-0 automata. Notice that this is actually an equivalence class of automata, since any choice of A, r and λ generates this dynamics whenever $n = 0$.

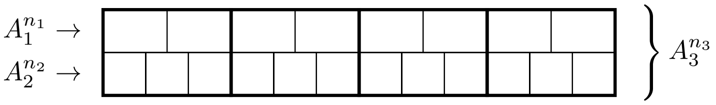
The multiplicative identity $\mathbf{1}$ of $\mathbf{D}$ has a dynamics consisting of a single fixed point. This dynamics is generated exactly by the cellular automata having $|A| = 1$, *i.e.*, exactly one state a, with any length n and radius r, and with the constant local rule $\lambda(a, \ldots, a) = a$.

Given two cellular automata $(A_1, n_1, r_1, \lambda_1)$ and $(A_2, n_2, r_2, \lambda_2)$ with global rule Λ_1 and Λ_2 respectively, their sum can be constructed as an automaton $(A_3, n_3, r_3, \lambda_3)$ with alphabet $A_3 = A_1^{n_1} \sqcup A_2^{n_2}$, i.e., the disjoint union of the global configurations of the two automata, length $n = 1$, radius $r = 0$ and local rule $\lambda_3 \colon A_3^1 \to A_3$ defined by

$$\lambda_3(c) = \begin{cases} \Lambda_1(c) & \text{if } c \in A_1^{n_1} \\ \Lambda_2(c) & \text{if } c \in A_2^{n_2} \end{cases}$$

Since $n = 1$, the local rule λ_3 is, in fact, identical to the global rule Λ_3, and this easily allows us to see that the dynamics of this automaton is the disjoint union of the dynamics of the terms of the sum, as required.

A configuration of the product of two cellular automata $(A_1, n_1, r_1, \lambda_1)$ and $(A_2, n_2, r_2, \lambda_2)$ is obtained by "laying side-by-side" the configurations of the two automata and grouping the cells together in order to obtain rectangular macro-cells:



The length of the product automaton is $n_3 = \gcd(n_1, n_2)$, with macro-cells consisting of $c_1 = n_1/n_3$ cells of the first automaton and $c_2 = n_2/n_3$ cells of the second; its alphabet is thus $A_3 = A_1^{n_1/n_3} \times A_2^{n_2/n_3}$. The radius can be computed by including the minimal number of macro-cells that suffices in order to include the neighbourhoods of the cells of the two automata being multiplied, as depicted in Figure 2. A neighbourhood of the first automaton is contained within a radius of $\lceil r_1/c_1 \rceil = \lceil \frac{r_1 n_3}{n_1} \rceil$ macro-cells, and a neighbourhood of the second within a radius of $\lceil r_2/c_2 \rceil = \lceil \frac{r_1 n_3}{n_2} \rceil$; by taking the maximum, in order to account for both original automata, we obtain

$$r_3 = \max\left(\left\lceil \frac{r_1 n_3}{n_1} \right\rceil, \left\lceil \frac{r_1 n_3}{n_2} \right\rceil\right) = \left\lceil \gcd(n_1, n_2) \times \max\left(\frac{r_1}{n_1}, \frac{r_2}{n_2}\right) \right\rceil.$$

Since finite cellular automata can generate the dynamics of the identity elements $\mathbf{0}$ and $\mathbf{1}$, and are closed under sum and product, they constitute a subsemiring of $\mathbf{D}$. Notice that, since any finite dynamical system (D, f) can be implemented as a length-1, radius-0 cellular automaton over the alphabet D, this semiring actually coincides with the whole semiring $\mathbf{D}$.

5 Conclusions

In this paper, we have presented a new abstract way of reasoning about finite discrete dynamical systems which is inspired by category theory. Introducing

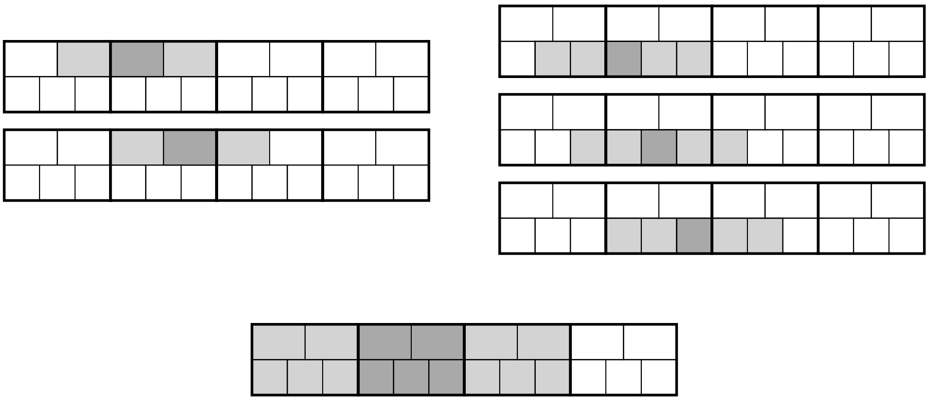


Fig. 2. If the two automata being multiplied have radius $r_1 = 1$ and $r_2 = 2$, respectively, then computing the next state of the dark grey micro-cell in the first (resp., second) row requires the states of the neighbouring cells in light grey, as shown in the top left (resp., top right) diagram. These are entirely contained in a neighbourhood of macro-cells of radius $r_3 = 1$ in the product automaton (bottom diagram).

the natural operations of addition and multiplication over dynamical systems provides an algebraic structure of semiring to the set of dynamical systems. This allowed to introduce classical formalisms for semirings like polynomials and lead to polynomial equations. We stress the importance of polynomial equations as a tool for the analysis of the dynamics of a system. Indeed, their solutions (if any) provide useful decompositions to further analyse the overall behaviour of the system.

Although solving general polynomial equations is algorithmically impracticable (see Theorem 1), the same problem turn out to be in **NP** in the case of polynomial equations in which the right-hand side is constant (see Theorem 2). Of course, this might still prove infeasible (if the problem turns out to be **NP**-complete, as expected) but it has the merit of being decidable. However, remark that, the proof of Theorem 2 essentially consists of two parts: guessing potential candidates and then checking if the two members of the equation are isomorphic. Now, consider the subsemiring **B** of **D** made by the dynamical systems which have a bijective next-state function. These systems are indeed permutations and for them the graph isomorphism problem can be solved in polynomial time (see [1]). It is therefore natural to ask for a polynomial time algorithm for this subsemiring. This subsemiring might be a good candidate for targeting polynomial time solving algorithms.

Another research direction naturally arises along the same line of thoughts. It consists in finding more significant subsemirings and their practical implications.

The exploration of polynomial equations in the general case has just started and most of the questions are still open. For example, can the number of solutions to a polynomial equation be tightly bounded? Is there any interesting decomposition theorem into irreducibles? What is precisely the role played by irreducibles *w.r.t.* the dynamical behaviour? Are they just a base for the limit set or can we extract more information?

References

1. Colbourn, C.J.: On testing isomorphism of permutation graphs. Networks 11(1), 13–21 (1981)
2. Hebisch, U., Weinert, H.J.: Semirings: Algebraic Theory and Applications in Computer Science. World Scientific (1998)
3. Lawvere, F.W., Schanuel, S.H.: Conceptual Mathematics, 2nd Edition: A First Introduction to Categories. Cambridge University Press (2009)
4. Matiyasevich, Y.: Hilbert's Tenth Problem. MIT Press (1993)