

BOOLEAN MONOMIAL DYNAMICAL SYSTEMS

OMAR COLÓN-REYES, REINHARD LAUBENBACHER, AND BODO PAREIGIS

ABSTRACT. An important problem in the theory of finite dynamical systems is to link the structure of a system with its dynamics. This paper contains such a link for a family of nonlinear systems over the field with two elements. For systems that can be described by monomials (including Boolean AND systems), one can obtain information about the limit cycle structure from the structure of the monomials. In particular, the paper contains a sufficient condition for a monomial system to have only fixed points as limit cycles. This condition depends on the cycle structure of the dependency graph of the system and can be verified in polynomial time.

1. INTRODUCTION

Finite dynamical systems are time-discrete dynamical systems on finite state sets. Well-known examples include cellular automata and Boolean networks, which have found broad applications in engineering, computer science, and, more recently, computational biology. (See, e.g., [K, AO, CS] for biological applications.) More general multi-state systems have been used in control theory [G, LB, M1, M2], the design and analysis of computer simulations [BR, BMR1, BMR2, LP2], and in computational biology as well [LS]. One underlying mathematical question that is common to many of these applications is how to analyze the dynamics of the models without actually enumerating all state transitions, since enumeration has exponential complexity in the number of model variables. The present paper is a contribution toward an answer to this question.

For our purposes, a finite dynamical system is a function $f : X \rightarrow X$, where X is a finite set [LP1]. Many applications assume X to be of the form k^n , where $n \geq 1$ and k is a finite field, often the field with two elements. In this paper we restrict ourselves to the case $X = k^n = \mathbb{F}_2^n$. The dynamics is generated by iteration of f , with the variables being updated simultaneously. In this paper we present a family of nonlinear systems for which the above question can be answered, that is, for which one can obtain information about the dynamics from the structure of the function. The answer is given in terms of properties of the dependency graph of the system, that is, the directed graph that represents the dependence of the coordinate functions of f on the other coordinates.

We assume that $f : k^n \rightarrow k^n$, $n \geq 1$, is a finite dynamical system. The dynamics of f is encoded in its *state space* $\mathcal{S}(f)$, which is a directed graph defined as follows. The vertices of $\mathcal{S}(f)$ are the 2^n elements of k^n . There is a directed edge $a \rightarrow b$ in $\mathcal{S}(f)$ if $f(a) = b$. In particular, a directed edge from a vertex to itself is admissible. That is, $\mathcal{S}(f)$ encodes all state transitions of f , and has the property that every vertex has out-degree exactly equal to 1. Each connected graph component of $\mathcal{S}(f)$ consists of a directed cycle, a so-called

Date: February 4, 2004.

1991 Mathematics Subject Classification. Primary 05C38; Secondary 68R10, 94C10.

The research in this paper was supported in part by Contract Nr. 78761-SOL-0343 from Los Alamos National Laboratory.

limit cycle, with a directed tree attached to each vertex in the cycle, consisting of the so-called *transients*.

Observe that f can be described in terms of its coordinate functions $f_i : k^n \rightarrow k$, that is, $f = (f_1, \dots, f_n)$. It is well known that, if k is any finite field with q elements and $g : k^n \rightarrow k$ is any set-theoretic function, then g can be represented by a polynomial in $k[x_1, \dots, x_n]$ [LN, p. 369]. This polynomial can be chosen uniquely so that any variable in it appears to a degree less than the number of elements in k . That is, for any g there is a unique $h \in k[x_1, \dots, x_n] / \langle x_i^q - x_i \mid i = 1, \dots, n \rangle$, such that $g(a) = h(a)$ for all $a \in k^n$. Consequently, any finite dynamical system over a finite field can be represented as a polynomial system. This is the point of view we take in this paper. For $q = 2$ this implies that every function can be represented by a square-free polynomial.

Observe further that any polynomial function over $k = \mathbb{F}_2$ with square-free monomials can be represented as a Boolean function, with multiplication corresponding to the logical AND, addition to the logical XOR, and negation as addition of the constant term 1. This implies that any finite dynamical system over \mathbb{F}_2 can be realized as a Boolean network. For a polynomial system $f = (f_1, \dots, f_n)$ the problem to be investigated then becomes one of drawing conclusions about the structure of the state space $\mathcal{S}(f)$ from the structure of the f_i . We first present a brief survey of existing results.

In the case of a linear system over an arbitrary finite field this question has a complete answer [H]. Let A be a matrix representation of a linear system $f : k^n \rightarrow k^n$. (That is, the f_i are linear polynomials without constant term.) Then the number of limit cycles and their length, as well as the structure of the transients, can be determined from the factorization of the characteristic polynomial of the matrix A . The structure of the limit cycles had been determined earlier by Elspas [E], and for affine systems by Milligan and Wilson [MW]. For nonlinear systems a very elegant general approach was proposed in [C]. A general nonlinear system can be embedded in a linear one, to which the author then applied techniques like in [E] to obtain the number and length of the limit cycles. The drawback of this method is that, if the nonlinear system has dimension n and the field has q elements, then the linear system has dimension q^n . It is also very difficult to see directly the effect of the specific nonlinear functions on the state space structure.

Very few results exist for general classes of nonlinear systems. Some facts about nonlinear one-dimensional cellular automata can be found in Wolfram's work [W]. For sequentially updated systems, there are some results in [BMR1]. For instance, it is shown there (Proposition 5) that sequentially updated Boolean NOR systems do not have any fixed points. In the one-dimensional case this problem has been studied extensively over the p -adic numbers, that is, the dynamics of univariate polynomials over \mathbf{Q}_p , viewed as a dynamical system. In particular, the case of monomials has been considered [KN], which are the focus of the present paper.

In this paper we focus on the class of nonlinear systems over $k = \mathbb{F}_2$ described by special types of polynomials, namely monomials. That is, we consider systems $f = (f_i)$, so that each f_i is a polynomial of the form $x_{i_1}x_{i_2} \cdots x_{i_r}$, or a constant equal to 0 or 1. This class includes all Boolean networks made up of AND functions. Associated to a general polynomial system one can construct its *dependency graph* $\mathcal{D}(f)$, whose vertices v_1, \dots, v_n correspond to the variables of the f_i . There is a directed arrow $v_i \rightarrow v_j$ if x_j appears in f_i . A special definition needs to be made to account for constant polynomials. For Boolean monomial systems the dependency graph in fact allows the unambiguous reconstruction of

the system. The main results of this paper show that in this case the cycle structure of the state space $\mathcal{S}(f)$ can be determined exclusively from the dependency graph $\mathcal{N}(f)$, that is, from the structure of the f_i . The key role is played by a numerical invariant associated to a strongly connected directed graph, that is, a graph in which there exists a walk (a directed path) between any two vertices. For such a graph one can define its *loop number* as the minimum of the distances of two walks from some vertex to itself. (The number is the same no matter which vertex is chosen.) It turns out that the dependency graph of a monomial system can be decomposed into strongly connected components whose loop numbers determine the structure of the limit cycles. If the loop number of every strongly connected component is one, then the state space has only fixed points as limit cycles, that is, f is a fixed point system.

2. PRELIMINARIES ON SYSTEMS AND DEPENDENCY GRAPHS

Let $f = (f_1, \dots, f_n) : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a Boolean monomial parallel update system, where the monomial functions are of the form

$$f_i = \alpha_i x_1^{\varepsilon_{1i}} \dots x_n^{\varepsilon_{ni}}$$

with $\alpha_i \in \{0, 1\}$ and $\varepsilon_{ji} \in \{0, 1\}$. If $\alpha_i = 0$ we set all $\varepsilon_{ji} = 0$. Let $f^m := f \circ f \circ \dots \circ f$ be the m -fold composition of the map f with itself. We write $f^m = (f^m_1, \dots, f^m_n)$. By definition we have

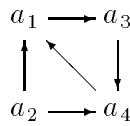
$$f^m_i = \alpha_i f^{m-1}_1^{\varepsilon_{1i}} \dots f^{m-1}_n^{\varepsilon_{ni}}.$$

Definition 2.1. With f we associate a digraph \mathcal{X} , called *dependency graph*, with vertex set $\{a_1, \dots, a_n, \varepsilon\}$. There is a directed edge from a_i to a_j if $\alpha_i = 1$ and x_j is a factor in f_i (i.e. $\varepsilon_{ji} = 1$). There is a directed edge from a_i to ε if $\alpha_i = 0$ (i.e. $f_i = 0$).

Observe that loops $a_i \rightarrow a_i$ are permitted. They occur if f_i has the factor x_i . If there is an edge $a_i \rightarrow \varepsilon$ ($f_i = 0$), then there is no edge $a_i \rightarrow a_j$ for any j . It is straightforward to see that the monomial system f is completely described by the dependency graph \mathcal{X} .

We give two simple examples:

Examples 2.2. (1) The system f given by the function $f = (x_3, x_1 \cdot x_4, x_4, x_1)$ has the following dependency graph



and the state space given in Figure 1.

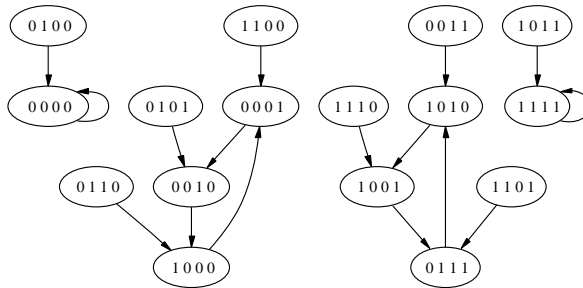
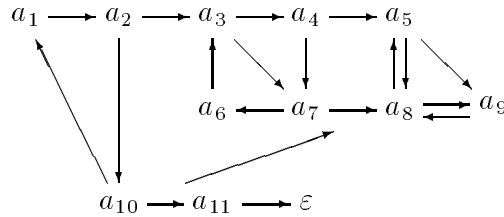


FIGURE 1. State space.

(2) The system f given by the function

$$f = (x_2, x_3x_{10}, x_4x_7, x_5x_7, x_8x_9, x_3, x_6x_8, x_5x_9, x_8, x_1x_8x_{11}, 0)$$

has the following dependency graph



Our theorems will show, that this system is a fixed point system, that is, all limit cycles are fixed points. In fact the state space of this system has 3 fixed points and 2048 nodes.

Proposition 2.3. *Let \mathcal{X} be the dependency graph of f and assume $f^m_i \neq 0$. There exists a walk $p : a_i \rightarrow a_j$ of length m in \mathcal{X} iff f^m_i contains the factor x_j .*

Proof. Assume that there are directed edges from a_i to a_{j_1}, \dots, a_{j_t} . Any walk leaving a_i goes through one of the a_{j_1}, \dots, a_{j_t} as a first step. So $f^m_i = \alpha_i f^{m-1}_{j_1} \dots f^{m-1}_{j_t}$. The claim now follows by induction and the observation that $x_j^2 = x_j$. For the converse observe that from

$$f^m_i = \alpha_i f^{m-1}_{j_1} \dots f^{m-1}_{j_t}$$

it follows that, if x_j is a factor of f^m_i it must also be a factor of some $f^{m-1}_{j_k}$. We can then again proceed by induction to get a walk of length m from a_i to a_j . \square

Corollary 2.4. *f^r_i is the product of all functions f^{r-s}_j for all walks $p : a_i \rightarrow a_j$ of length $s \leq r$.*

Proof. This follows by induction, as in Proposition 2.3. \square

Corollary 2.5. *If there is a walk $p : a_i \rightarrow a_j$ of length less than r , and if $f^1_j = f_j = 0$, then the function f^r_i is zero.*

3. THE STRUCTURE OF THE DEPENDENCY GRAPH

Definition 3.1. Let \mathcal{X} be the dependency graph of f .

- (1) We write $a \in \mathcal{X}$ for $a \in V_{\mathcal{X}} \setminus \{\varepsilon\}$.
- (2) For vertices $a, b \in \mathcal{X}$, we call a and b *strongly connected*, and write $a \sim b$, if and only if there is a walk $p : a \rightarrow b$ and a walk $q : b \rightarrow a$. Observe that there is always a walk of length zero (the empty walk) from a to a . Then $a \sim b$ is an equivalence relation on $V_{\mathcal{X}} \setminus \{\varepsilon\}$, called *strong equivalence*.
- (3) The equivalence class of $a \in \mathcal{X}$ is called a (*strongly*) *connected component* and is denoted by \bar{a} . Let $E(\mathcal{X})$ be the set of equivalence classes.
- (4) A vertex a with an edge $a \rightarrow \varepsilon$ is called a *zero*.
- (5) For $a, b \in \mathcal{X}$, let $p : a \rightarrow b$ be a walk. We denote the length of the walk p by $|p|$.

The smallest strongly connected components are described as follows. If $a_i \in \mathcal{X}$ is a vertex with $f_i = 1$ then there is by definition no edge originating in a_i , so a_i defines a one element strongly connected component which contains only the empty walk. The same holds in case $f_i = 0$, except that there is an edge $a_i \rightarrow \varepsilon$, but there is still only one walk, the empty walk, from a_i to a_i . If $f_i = x_i$, then a_i also defines a one element strongly connected

component, since there is no edge $a_i \rightarrow a_j$ for $j \neq i$. However, there are infinitely many closed walks $p_j : a_i \rightarrow a_i$, one for each length $|p_j| = j \in \mathbb{N}$.

Lemma 3.2. *Define $\bar{a} \leq \bar{b}$ iff there is a walk from a to b . Then $E(\mathcal{X})$ is a poset.*

Proof. Observe that, given $a, a' \in \bar{a}$ and $b, b' \in \bar{b}$, there is a walk from a to b if and only if there is a walk from a' to b' . If there is a walk from a to b and a walk from b to a , then a and b are strongly connected and thus $\bar{a} = \bar{b}$. \square

Observe that a_i defines a one point connected component \bar{a}_i if and only if $f_i = 0, 1$, or $f_i = x_i$.

This partial order will come up again in the discussion of glueing. It covers all the edges that do not occur in strongly connected components.

4. THE STATE SPACE OF A CONNECTED COMPONENT

In this section we will study strongly connected components. The study of the relations between connected components, that lead to the poset structure of $E(\mathcal{X})$ will be done in the next section. We first discuss three trivial cases.

Let $\mathcal{X} = \{a\}$ be a strongly connected component with a a zero. Then $f^m = 0$ for all $m \geq 1$. Let $\mathcal{X} = \{a\}$ be a strongly connected component with $f = 1$. Then $f^m = 1$ for all $m \geq 1$. If \mathcal{X} is the dependency graph of an arbitrary function $f : \mathbb{F}_2^r \rightarrow \mathbb{F}_2^r$ and if $a_i \in \mathcal{X}$ has a walk to a zero $a_j \rightarrow \varepsilon$ of length $n \geq 0$, then by Corollary 2.5 we have $f^{n+m}_i = 0$ for all $m \geq 1$.

Let \bar{a} be the strongly connected component of $a \in \mathcal{X}$. Assume there is a walk from a to a zero a_j in \mathcal{X} . Then there is an $n \geq 0$ such that $f^{n+m}_i = 0$ for all $a_i \in \bar{a}$ and all $m \geq 1$. In particular if \mathcal{X} is strongly connected and if $a_j \in \mathcal{X}$ is a zero, then f is a fixed point system with exactly one fixed point $(0, \dots, 0)$. So for the rest of section 4 we will assume that \mathcal{X} is strongly connected and we exclude the cases $f(x_1) = 1$ and $f(x_1) = 0$.

4.1. Loop numbers.

Definition 4.1. The *loop number* of $a \in \mathcal{X}$ is the minimum of all numbers $t \geq 1$ with $t = |p| - |q|$ for all closed walks $p, q : a \rightarrow a$. If there is no closed walk from a to a then we set the loop number to be zero. This last case occurs only if $\bar{a} = \{a\}$ and there is no edge from a to a (i.e. $f = 0, 1$, but we have excluded $f = 0$).

If there is a loop $p : a \rightarrow a$ then the loop number of a is $|pp| - |p| = 1$.

Let $a, b \in \mathcal{X}$. We show that the loop numbers of a and of b are equal. We get

Lemma 4.2. *The loop number is constant on any strongly connected \mathcal{X} , so the loop number of a strongly connected \mathcal{X} is a well defined number $\mathcal{L}(\mathcal{X})$.*

Proof. Let $p' : a \rightarrow b$ and $q' : b \rightarrow a$ be walks. Then $p'pq', p'qq' : b \rightarrow b$ are closed walks with $|p'pq'| - |p'qq'| = t$, so the loop number of b is less than or equal to the loop number of a . By symmetry the loop number is constant on \mathcal{X} . \square

Lemma 4.3. *Let the loop number of \mathcal{X} be t . Let $p' : a_i \rightarrow a_j$ and $q' : a_i \rightarrow a_j$ be walks. Then $|p'| - |q'| \in (t) \subseteq \mathbb{Z}$.*

Proof. Assume $|p'| > |q'|$ and let $|p'| - |q'| = rt + s$ with $0 \leq s < t$. We want to show $s = 0$. Let $p, q : a_i \rightarrow a_i$ be such that $|q| - |p| = t$. We have $r \geq 0$. Then

$$|p'p| - |q'q| = |p'| + |p| - |q'| - |q| = rt + s - t = (r - 1)t + s.$$

Hence there are walks $p'', q'' : a_i \rightarrow a_j$ with $|p''| - |q''| = s$. Let $p^* : a_j \rightarrow a_i$ be a walk. Then $|p^*p''| - |p^*q''| = s = 0$ because of the minimality of the loop number t . So $|p'| - |q'| \in (t)$. \square

Corollary 4.4. *Let the loop number of \mathcal{X} be t . Let $p : a \rightarrow a$ be a closed walk. Then $|p| \in (t)$.*

Proof. Im Lemma 4.3 take p and pp . \square

Proposition 4.5. *Let the loop number of \mathcal{X} be $t \geq 1$. For each $a, b \in \mathcal{X}$ there exists an $m \in \mathbb{N}$ and walks $p_i : a \rightarrow b$ of length $|p_i| = m + i \cdot t$ for all $i \in \mathbb{N}$.*

Proof. Let $p, q : a \rightarrow a$ be closed walks with $|q| - |p| = t$. By Corollary 4.4 $|p|$ is divisible by t . Let $r := |p|/t$. Let $p' : a \rightarrow b$ be a walk of length $s := |p'|$. Let $m := s + (r^2 - r)t$. Write $i \in \mathbb{N}$ as $i = jr + k$ with $0 \leq k < r$. Then the composition of walks

$$p'q^k p^{r-1+j-k} : a \rightarrow b$$

has length $|p'q^k p^{r-1+j-k}| = m + i \cdot t$. \square

Observe that the number m can be quite large. Even if we take p' to be a walk of minimal length and p, q of minimal length such that $|q| - |p| = t$, i.e. s and r minimal, we get $m = s + (r^2 - r)t$. This contributes to the lengths of transients in the state space.

4.2. Fixed points and cycles of strongly connected components.

Lemma 4.6. *For $a_i, a_j \in \mathcal{X}$ we define*

$$a_i \approx a_j : \iff \exists \text{ walk } p : a_i \rightarrow a_j \text{ with } |p| \in (t).$$

This is an equivalence relation, called loop equivalence.

Proof. We have $a_i \approx a_i$ with a walk of length zero and thus reflexivity. Transitivity is trivial. For symmetry let $a_i \approx a_j$, then there is a walk $p : a_i \rightarrow a_j$ with $|p| \in (t)$. Let $q : a_j \rightarrow a_i$ be any walk. Then $qp : a_i \rightarrow a_i$ is a walk with $|qp| = |q| + |p| \in (t)$ by Corollary 4.4, hence $|q| \in (t)$ and thus $a_j \approx a_i$. \square

Lemma 4.7. *There are exactly t loop equivalence classes in \mathcal{X} .*

Proof. Since there are walks starting in a_i for all lengths ≥ 0 , take a walk $a_i \rightarrow a_{i+1} \rightarrow \dots \rightarrow a_{i+t}$ of length t . The a_{i+j} , $j = 0, \dots, t-1$ are in different equivalence classes

$$\bar{a}_i, \bar{a}_{i+1}, \dots, \bar{a}_{i+t} = \bar{a}_i$$

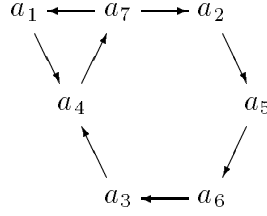
by Lemma 4.3. Every a_k is in one of these equivalence classes, since there is a walk $q : a_{i+t} \rightarrow a_k$ of length $|q| = rt + s$, so there is a walk $q' : a_{i+t} \rightarrow a_k$ of length $|q'| \in (t)$, hence $a_{i+t} \approx a_k$. \square

We may now label and enumerate the vertices of \mathcal{X} in the following way

$$(a_1, \dots, a_{i_1}), (a_{i_1+1}, \dots, a_{i_2}), \dots, (a_{i_{t-1}+1}, \dots, a_{i_t})$$

where each group $(a_{i_{j+1}}, \dots, a_{i_{j+1}})$ is a loop equivalence class and there is an edge $a_{i_j} \rightarrow a_{i_{j+1}}$ for all $j = 1, \dots, t-1$. If $s_j := i_j - i_{j-1}$ is the number of elements in each loop

class, then $\sum_{i=1}^t s_i = n$. The following example of a strongly connected dependency graph of loop number 3 should illuminate this enumeration of vertices $(a_1, a_2, a_3), (a_4, a_5), (a_6, a_7)$:



Corollary 4.8. *Let $a \in \mathcal{X}$ and let $\{a_1, \dots, a_u\}$ be the loop class of a (with $a_1 = a$). Then there is an $m \in \mathbb{N}$ such that for all $j = 1, \dots, u$ and all $i \in \mathbb{N}$ there is a walk $a \rightarrow a_j$ of length $(m+i)t$.*

Proof. Use Proposition 4.5 to obtain m_j and walks $p_{ij} : a \rightarrow a_j$ of lengths $m_j + it$ for all $i \in \mathbb{N}$ and all $j = 1, \dots, u$. By Lemma 4.3 each m_j is divisible by t . Take $m := \max\{m_1, \dots, m_u\}/t$. \square

Before we study the fixed points and cycles of an arbitrary connected dependency graph we look at a simple example.

Proposition 4.9. *The state space of a directed t -gon is isomorphic to the set of orbits of the action of the cyclic group of order t acting on \mathbb{F}_2^t , the t -dimensional hypercube, by cyclically exchanging the canonical basis vectors.*

Proof. The dynamical system f of a directed t -gon is $f(x_1, \dots, x_t) = (x_2, x_3, \dots, x_1)$. The states in the state space are elements of \mathbb{F}_2^t , and the action of f and the powers of f give an action of the cyclic group C_t on \mathbb{F}_2^t by cyclic exchange of the basis vectors. \square

Theorem 4.10. *Let \mathcal{X} be strongly connected with loop number $t \geq 1$ and n vertices. Let*

$$(a_1, \dots, a_{i_1}), (a_{i_1+1}, \dots, a_{i_2}), \dots, (a_{i_{t-1}+1}, \dots, a_{i_t})$$

be the enumeration of vertices of \mathcal{X} as described above. Then there is an m such that

$$f^{mt} = \underbrace{(y_1, \dots, y_1)}_{s_1 \text{ times}} \underbrace{(y_2, \dots, y_2)}_{s_2 \text{ times}} \dots \underbrace{(y_t, \dots, y_t)}_{s_t \text{ times}}$$

where $y_1 = x_1 \dots x_{i_1}$, $y_2 = x_{i_1+1} \dots x_{i_2}$, \dots , $y_t = x_{i_{t-1}+1} \dots x_{i_t}$.

Furthermore

$$\begin{aligned} f^{mt+1} &= \underbrace{(y_2, \dots, y_2)}_{s_1 \text{ times}} \underbrace{(y_3, \dots, y_3)}_{s_2 \text{ times}} \dots \underbrace{(y_1, \dots, y_1)}_{s_t \text{ times}} \\ &\vdots \\ f^{mt+j} &= \underbrace{(y_{j+1}, \dots, y_{j+1})}_{s_1 \text{ times}} \underbrace{(y_{j+2}, \dots, y_{j+2})}_{s_2 \text{ times}} \dots \underbrace{(y_j, \dots, y_j)}_{s_t \text{ times}} \end{aligned}$$

Proof. For each loop class c we use some m_c from Corollary 4.8 and compute the values $f^{m_c}_i$ for all i . By Proposition 2.3 we get $f^{m_c}_i = x_1 \dots x_u$ for all $i = 1, \dots, u$. If we use the maximum m of all such m_c , then we have the structure of f^{mt} .

To determine f^{mt+1}_i observe that for $i = 1, \dots, i_1$ there are walks $a_i \rightarrow a_j$ of length $mt + 1$ for all $a_j \in \{a_{i_1+1}, \dots, a_{i_2}\}$. By Lemma 4.3 no walk of length $mt + 1$ starting in a_i can end in a vertex different from these a_j . Hence $f^{mt+1}_i = y_2$ for all $i = 1, \dots, i_1$. The rest of the proof follows by induction. \square

This theorem allows us to give a complete description of the cycles in the state space of \mathcal{X} .

Corollary 4.11. *Let \mathcal{X} be as in Theorem 4.10. Then the subgraph of cycles in the state space of f is isomorphic to the state space of a directed t -gon, hence the set of orbits in the hypercube \mathbb{F}_2^t under the action of the cyclic group C_t .*

Proof. For every choice of arguments for the x_i we end up in the form of f^{mt} . Then f acts on these points by a cyclic permutation, which defines the various cycles in the state space. By reducing the number of y 's with the same subscript to one, we get the system (y_1, \dots, y_t) with the same cyclic action $g(y_1, \dots, y_n) = (y_2, y_3, \dots, y_1)$ and $g^j(y_1, \dots, y_n) = (y_{j+1}, y_{j+2}, \dots, y_j)$. This system arises from a directed t -gon. \square

Corollary 4.12. *Let \mathcal{X} be as in the Theorem.*

- (1) *The system f has fixed points $(0, \dots, 0)$ and $(1, \dots, 1)$.*
- (2) *The system f has limit cycles of all lengths dividing t .*
- (3) *The system f is a fixed point system if and only if the loop number of \mathcal{X} is 1.*

Example 2.2 (1) has two strongly connected components $\{a_2\}$ and $\{a_1, a_3, a_4\}$ with loop numbers 0 and 3 respectively. The second strongly connected component has two 3-cycles as well as two fixed points.

Example 2.2 (2) has four strongly connected components $\{a_1, a_2, a_{10}\}$, $\{a_3, a_4, a_6, a_7\}$, $\{a_5, a_8, a_9\}$, and $\{a_{11}\}$ with loop numbers 3, 1, 1, and 0 respectively. The second strongly connected component has two 3 cycles and two fixed points. The next two components have two fixed points each, and the last component has one fixed point. In both examples the strongly connected components of the systems are connected by further edges. So we have to investigate, how these additional edges effect the fixed point property.

4.3. The computation of loop numbers. In view of the importance of the loop number for determining if a system is a fixed point system, we describe some polynomial time algorithm to compute the loop number of a strongly connected component. Let A be the adjacency matrix of an arbitrary dependency graph \mathcal{X} with n vertices. Then the connected components can be read off the powers A, A^2, \dots, A^n of A by the fact that a vertex a_i is connected by a walk of length s to a vertex a_j iff the ij -th component of A^s is non-zero. The strongly connected component of a vertex a_i is obtained as follows: take the i -th row of all the matrices A^r , find all nonzero entries and determine the set $R(i)$ of associated js . Take the i -th column of all the matrices A^r , find all nonzero entries and determine the set $C(i)$ of associated js . Then $R(i) \cap C(i)$ is the set of indices j such that a_j is strongly connected with a_i .

Now we assume that \mathcal{X} is strongly connected and we exclude the cases $f(x_1) = 1$ and $f(x_1) = 0$. A closed walk $p : a_i \rightarrow a_i$ is called a *circuit* in \mathcal{X} if it has no repetitive vertices. A circuit has length at most n , so it can be read off the powers A, A^2, \dots, A^n of the adjacency matrix A . In contrast, closed walks may have arbitrarily large lengths.

Theorem 4.13. *Let X be a strongly connected graph. The loop number of \mathcal{X} is the greatest common divisor of the numbers i with $1 \leq i \leq n$, such that A^i has at least one non-zero diagonal entry.*

Proof. We first prove that the loop number of \mathcal{X} is the greatest common divisor of the lengths of all circuits of \mathcal{X} . The problem in proving this is, that the loop number cannot be represented in general as the difference of the lengths of two circuits.

Observe that a closed walk p can be decomposed into a number of circuits p_1, \dots, p_l sharing vertices.

Let d be the greatest common divisor of the lengths of all circuits of \mathcal{X} . Take a vertex $a \in \mathcal{X}$. Let p and q be closed walks through a representing the loop number $|p| - |q| = t$ of \mathcal{X} . We want to show $d = t$.

Decompose p and q into a number of circuits p_1, \dots, p_l and q_1, \dots, q_m . Then we get $|p| = |p_1| + \dots + |p_l|$ and $|q| = |q_1| + \dots + |q_m|$. Hence

$$|p_1| + \dots + |p_l| - |q_1| - \dots - |q_m| = t,$$

so that d divides t .

Now we show that t divides the length of each circuit in \mathcal{X} . Assume there is a circuit p' through $b \in \mathcal{X}$ whose length $s := |p'|$ is not divisible by t . There are walks $q_1 : a \rightarrow b$ and $q_2 : b \rightarrow a$. Let $r := |q_1| + |q_2|$ and let $t' := \gcd(r, s, t)$. Then t' can be written as $t' = \alpha t - \beta r - \gamma s$ with $\alpha, \gamma \geq 0$ and $\beta > 0$. So

$$|p'^\alpha| - |q_1^\alpha q_2^\alpha (q_1 q_2)^{\beta-1} (p')^\gamma q_1| = t',$$

i.e., we have constructed two closed walks whose lengths differ by t' . Hence $t' = t$ is the loop number of \mathcal{X} . Then $t' = t$ divides $s = |p'|$, a contradiction. Thus all lengths of circuits in \mathcal{X} are divisible by t , so that t divides d , hence $d = t$.

Now the length of all possible closed walks (of lengths $\leq n$) can be read of the non-zero diagonal entries of the powers of the adjacency matrix. These walks are composed, as above, of circuits, and their lengths are sums of the lengths of certain circuits. So the greatest common divisor of the numbers i , such that A^i has at least one non-zero diagonal entry is the greatest common divisor of the lengths of all circuits of \mathcal{X} . \square

5. GLUEING

Definition 5.1. Let \mathcal{X} and \mathcal{Y} be dependency graphs of functions $f : \mathbb{F}_2^r \rightarrow \mathbb{F}_2^r$ and $g : \mathbb{F}_2^s \rightarrow \mathbb{F}_2^s$, respectively. A *glueing* $\mathcal{X} \# \mathcal{Y}$ of \mathcal{Y} to \mathcal{X} consists of a digraph with vertices $V_{\mathcal{X}} \dot{\cup} V_{\mathcal{Y}}$ and edges $E_{\mathcal{X}} \dot{\cup} E_{\mathcal{Y}}$ (disjoint union), together with a set of additional directed edges from vertices in \mathcal{Y} to vertices in \mathcal{X} .

The function of $\mathcal{X} \# \mathcal{Y}$ is denoted by $f \# g : \mathbb{F}_2^{r+s} \rightarrow \mathbb{F}_2^{r+s}$.

Observe that \mathcal{X} is a subgraph of $\mathcal{X} \# \mathcal{Y}$ and that $f : \mathbb{F}_2^r \rightarrow \mathbb{F}_2^r$ is a quotient system of $f \# g : \mathbb{F}_2^{r+s} \rightarrow \mathbb{F}_2^{r+s}$.

We write elements in $\mathbb{F}_2^{r+s} = \mathbb{F}_2^r \times \mathbb{F}_2^s$ as pairs (α, β) with $\alpha = (\alpha_1, \dots, \alpha_r)$ and $\beta = (\beta_1, \dots, \beta_s)$. Similarly we write the variables for the function $f \# g$ as (x, y) with $x = (x_1, \dots, x_r)$ and $y = (y_1, \dots, y_s)$. Thus we can write the function $f \# g$ as

$$(f \# g)(x_1, \dots, x_r, y_1, \dots, y_s) = (f(x_1, \dots, x_r), h(x_1, \dots, x_r, y_1, \dots, y_s)),$$

with $f = (f_1, \dots, f_r)$ and $h = (h_1, \dots, h_s) = ((f \# g)_{r+1}, \dots, (f \# g)_{r+s})$.

We will use the poset $E(\mathcal{X})$ as in Lemma 3.2 together with the glueing procedure to study fixed point systems. We will discuss elements in $E(\mathcal{X})$ with no edges ($f = 0, 1$) separately. They are the strongly connected components of loop length 0.

Lemma 5.2. *Let $\mathcal{X} \# \mathcal{Y}$ be a fixed point system. Then \mathcal{X} is a fixed point system.*

Proof. This follows from the fact that f is a quotient system of $f \# g$. Indeed let $(\alpha, \beta) \in \mathbb{F}_2^{r+s}$. Let $m \in \mathbb{N}$ be such that $(f \# g)^m(\alpha, \beta) = (f \# g)^{m+1}(\alpha, \beta)$. Then we have $f^m(\alpha) = f^{m+1}(\alpha)$ so that f is a fixed point system. \square

Theorem 5.3. *Let \mathcal{X} be a fixed point system and let \mathcal{Y} be strongly connected of loop length ≥ 1 . Let $\mathcal{X}\#\mathcal{Y}$ be a glueing. The following are equivalent:*

- *The glueing $\mathcal{X}\#\mathcal{Y}$ is a fixed point system.*
- (1) *There is a vertex $a \in \mathcal{Y}$ that is connected with a walk to a zero in \mathcal{X} , or*
- (2) *\mathcal{Y} is a fixed point system.*

Proof. \Leftarrow : We use the notation introduced above. Assume that there is a vertex $a \in \mathcal{Y}$ that is connected with a walk to a zero in \mathcal{X} . Then all vertices of \mathcal{Y} are connected to a zero. By Corollary 2.5 we get an $n \in \mathbb{N}$ such that $(f\#g)^{n+m}_{r+i} = 0$ for all $m \geq 1$ and for all $i = 1, \dots, s$. Since f is a fixed point system we have $f^m = f^{m+1} = \dots$. So for a sufficiently large exponent m' the component \mathcal{Y} in $\mathcal{X}\#\mathcal{Y}$ can only contribute a fixed point $\beta = (0, \dots, 0)$. Hence $(f\#g)^{m'} = (f\#g)^{m'+1}$.

Let g be a fixed point system. Note that f is a subsystem of $f\#g$. Iterate $f\#g$ until the component on \mathcal{X} becomes constant:

$$(f\#g)^m(x, y) = (f^m(x), [(f\#g)^m]_{r+1}(x, y), \dots, [(f\#g)^m]_{r+s}(x, y)),$$

where

$$(f\#g)^{m+k}(x, y) = (f^m(x), ((f\#g)^{m+k})_{r+1}(x, y), \dots, (f\#g)^{m+k}_{r+s}(x, y)).$$

Set

$$(z_1, \dots, z_s) := ([(f\#g)^m]_{r+1}(x, y), \dots, [(f\#g)^m]_{r+s}(x, y)).$$

Then apply powers of $f\#g$ to $(f^m(x), (z_1, \dots, z_s))$ to get

$$(f\#g)^{m+1}(x, y) = (f^m(x), (f\#g)_{r+1}(f^m(x), z), \dots, (f\#g)_{r+s}(f^m(x), z)),$$

and

$$(f\#g)^{m+k}(x, y) = (f^m(x), (f\#g)^k_{r+1}(f^m(x), z), \dots, (f\#g)^k_{r+s}(f^m(x), z)).$$

So, for a fixed choice of x , the functions $(f\#g)_{r+1}, \dots, (f\#g)_{r+s}$, when viewed only as a function on elements from \mathbb{F}_2^s , are the functions g_1, \dots, g_s multiplied with certain factors from the fixed point $f^m(x)$. This defines a new system $h_x : \mathbb{F}_2^s \rightarrow \mathbb{F}_2^s$, so that

$$(f\#g)^k(f^m(x), z) = (f^m(x), h_x^k(z)). \quad (*)$$

If one of the factors taken from $f^m(x)$ is zero, then by Corollary 2.5 and by the fact that \mathcal{Y} is strongly connected, we get that h_x is a fixed point system with the only fixed point $\beta = (0, \dots, 0)$. If all of the factors taken from $f^m(x)$ are 1, then $h_x = g$ and hence is a fixed point system. So by (*) we see that $(f\#g)^k(f^m(x), z)$ ends in a fixed point for all choices of x and y .

\Rightarrow : Before we give the proof in this direction, we prove a Lemma. Let \mathcal{Z} be the dependency graph of an arbitrary Boolean monomial system. Decompose \mathcal{Z} into two parts, where \mathcal{Z}_0 is the glueing of all strongly connected components that allow a walk to a zero. Let \mathcal{Z}_1 be the glueing of all the other strongly connected components of \mathcal{Z} . Then there are no walks from any vertex in \mathcal{Z}_1 to any vertex in \mathcal{Z}_0 , so that \mathcal{Z} is a glueing of \mathcal{Z}_0 to \mathcal{Z}_1 .

Lemma 5.4. *Any system of the form \mathcal{Z}_1 has a fixed point $(1, \dots, 1)$.*

Proof. This is proved by induction on the number of connected components of \mathcal{Z}_1 . Assume that $\mathcal{Z}_1 = \mathcal{X}_1\#\mathcal{Y}$ where \mathcal{Y} is a connected component with no zero. We can assume that \mathcal{X}_1 has a fixed point $(1, \dots, 1)$. Observe that \mathcal{Y} belongs to the component $(\mathcal{X}\#\mathcal{Y})_1$ (not

connected to a zero) and \mathcal{Y} has a fixed point $(1, \dots, 1)$ by Corollary 4.12. So we get from the induction hypothesis that \mathcal{Z}_1 has also a fixed point $(1, \dots, 1)$. \square

Proof of Theorem continued. Now assume that $\mathcal{X}\#\mathcal{Y}$ is a fixed point system, and that no vertex of \mathcal{Y} is connected with a walk to a zero in \mathcal{X} . Now we use as initial state (x, y) for the system $f\#g$, with $x = (1, \dots, 1, 0, \dots, 0)$ (a fixed point of f), where the component $(1, \dots, 1)$ belongs to \mathcal{X}_1 and $(0, \dots, 0)$ belongs to \mathcal{X}_0 , and y arbitrary. Then, as discussed above, the system $h_x : \mathbb{F}_2^s \rightarrow \mathbb{F}_2^s$ coincides with $g : \mathbb{F}_2^s \rightarrow \mathbb{F}_2^s$. Since $f\#g$ is a fixed point system, the system g can also only contain fixed points and no proper limit cycles. Thus g is a fixed point system. \square

Theorem 5.5. *Let f be a fixed point system and let \mathcal{Y} be strongly connected of loop length 0. Let $\mathcal{X}\#\mathcal{Y}$ be a glueing. Then the system $f\#g$ corresponding to the glueing $\mathcal{X}\#\mathcal{Y}$ is a fixed point system.*

Proof. There are two cases: \mathcal{Y} is a one point component with $f_a = 1$ and the case that \mathcal{Y} is a one point component with $f_a = 0$. If $f_a = 0$, then there is no additional edge from $\mathcal{Y} = \{a\}$ to \mathcal{X} and thus $f\#g$ is a fixed point system with fixed points of the form $(\alpha, 0)$, where α is a fixed point of f . If $f_a = 1$ then any additional edge from $\mathcal{Y} = \{a\}$ to $a_i \in \mathcal{X}$ adds a factor to the last component, so that $f\#g = (f_1, \dots, f_n, x_{i_1} \dots x_{i_r})$. If $\alpha = (\alpha_1, \dots, \alpha_n)$ is a fixed point for f , i.e. $f(\alpha) = \alpha$ then $(f\#g)(\alpha, \beta) = (\alpha, \alpha_{i_1} \dots \alpha_{i_r})$ which is again a fixed point. So $f\#g$ is a fixed point system. \square

6. BOOLEAN MONOMIAL FIXED POINT SYSTEMS

In this section \mathcal{X} will be the digraph of an arbitrary Boolean monomial parallel update system.

Theorem 6.1. *Let \mathcal{X} be the digraph of $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. The following are equivalent:*

- (1) *The system $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is a fixed point system.*
- (2) *For every vertex $a \in \mathcal{X}$ one of the following holds*
 - (a) *a allows two closed walks $p, q : a \rightarrow a$ of length $|q| = |p| + 1$,*
 - (b) *a is connected with a walk to a zero, or*
 - (c) *there is no walk of length ≥ 1 from a to a .*

Proof. This is an immediate consequence of Theorem 5.3, Corollary 4.12 and the remarks at the beginning of section 4. \square

Definition 6.2. A system

$$f = (f_1, f_2, \dots, f_n) : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$$

is a *triangular system*, if each f_i is of the form

$$f_i = \alpha_i x_1^{\epsilon_{i1}} x_2^{\epsilon_{i2}} \dots x_i^{\epsilon_{ii}},$$

where $\alpha_i, \epsilon_{ij} \in \{0, 1\}$.

Corollary 6.3. *Every triangular system is a fixed point system.*

Proof. Let f be a triangular system with dependency graph \mathcal{X} . Then \mathcal{X} consists of the glueing of components with just one element. Therefore each component corresponds to a fixed point system, and by Theorem 5.3 we conclude that f is a fixed point system as well. \square

Corollary 6.4. *Let f be a system with dependency graph \mathcal{X} . Then f is a fixed point system if and only if every strongly connected component of \mathcal{X} either corresponds to a fixed point system or is connected by a walk to a zero in \mathcal{X} .*

Proof. This is an immediate consequence of Theorem 5.3. \square

Remark. The order in which we enumerate the variables does not really matter. We will certainly get the same state space up to isomorphism. Namely, if

$$f = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$

is a parallel update system and $\sigma \in S_n$ is a permutation, then

$$\sigma f = (f_{\sigma^{-1}(1)}(x_{\sigma(1)}, \dots, x_{\sigma(n)}), \dots, f_{\sigma^{-1}(n)}(x_{\sigma(1)}, \dots, x_{\sigma(n)}))$$

has a state space isomorphic to the state space of f . In particular, this defines a group action of S_n on the fixed point systems on n variables.

Theorem 6.5. *Let \mathcal{X} be the digraph of a fixed point system $f = (f_1, \dots, f_n)$. If there is no walk from a_i to a_j or if a_i or a_j have a walk of length greater than or equal to 1 to themselves, then $g := (f_1, \dots, x_i f_j, \dots, f_n)$ is a fixed point system.*

Proof. By Lemma 3.2 and the definition of glueing, \mathcal{X} is an iterated glueing of connected components: $\mathcal{X} = (\dots(\mathcal{X}_1 \# \mathcal{X}_2) \# \dots) \# \mathcal{X}_r$. By Corollary 6.4 the connected components \mathcal{X}_i are fixed point systems or they are connected by a directed path to a zero. The connected components that are fixed point systems then have loop number 0 or 1.

The multiplication of f_j with x_i introduces an extra edge $a_j \rightarrow a_i$ into the digraph \mathcal{X} , unless there is already a factor x_i in f_j , in which case the graph does not change. Let \mathcal{Y} be the digraph of g . We distinguish a number of cases.

Case 1: Suppose that a_i and a_j lie in the same component \mathcal{X}_s . If $i \neq j$, then \mathcal{X}_s has loop number 1 or is connected to a zero. So all components retain their properties responsible for \mathcal{Y} being a fixed point system. If $i = j$, then the loop number of \mathcal{X}_s becomes 1, so \mathcal{Y} is again a fixed point system.

Case 2: Let a_i lie in \mathcal{X}_s and $a_j \in \mathcal{X}_t$, and assume that there is no walk from \mathcal{X}_s to \mathcal{X}_t . If there is a walk from \mathcal{X}_t to \mathcal{X}_s then $\mathcal{X}_s \geq \mathcal{X}_t$ in the partial order of $E(\mathcal{X})$. The existence of an edge $a_j \rightarrow a_i$ does not change this property, so \mathcal{Y} is a fixed point system. If there is no walk from \mathcal{X}_t to \mathcal{X}_s , then we can extend the partial order of $E(\mathcal{X})$ to a total order such that $\mathcal{X}_s \geq \mathcal{X}_t$. Then the edge $a_j \rightarrow a_i$ does not change the order of the glueing, so \mathcal{Y} is a fixed point system.

Case 3: Let $a_i \in \mathcal{X}_s$ and $a_j \in \mathcal{X}_t$. Assume that there is a walk from \mathcal{X}_s to \mathcal{X}_t and thus a walk from a_i to a_j . By hypothesis we have two cases. Either there is a closed walk $a_i \rightarrow a_i$ of length greater than or equal to 1. Then the component \mathcal{X}_s has loop number 1. After inserting the edge $a_j \rightarrow a_i$ the two components \mathcal{X}_s and \mathcal{X}_t are joined into one connected component of loop number 1. All other components remain unchanged. So g is a fixed point system. Or there is a closed walk $a_j \rightarrow a_j$ of length greater than or equal to 1. Then the component \mathcal{X}_t has loop number 1. After inserting the edge $a_j \rightarrow a_i$ the two components \mathcal{X}_s and \mathcal{X}_t are joined again into one connected component of loop number 1. All other components remain unchanged. So g is again a fixed point system. \square

Corollary 6.6. *Let $f = (f_1, \dots, f_n)$ be a fixed point system and m a monomial. Then $mf = (mf_1, \dots, mf_n)$ is a fixed point system.*

Proof. It is sufficient to prove the corollary for the case where $m = x_i$ is a single variable. Consider first the system $(f_1, \dots, x_i f_i, \dots, f_n)$. As in the proof of the previous theorem we get an edge from a_i to a_i which can only change the loop number of the component of a_i to 1. So this system is again a fixed point system. Now we can apply Theorem 6.5 $n - 1$ times and get that $x_i f = (x_i f_1, \dots, x_i f_n)$ is a fixed point system. \square

REFERENCES

- [AO] Albert, R., and Othmer, H. G., The topology of the regulatory interactions predicts the expression pattern of the segment polarity genes in *Drosophila melanogaster*, *J. Theor. Biol.* **223**, 2003, 1–18.
- [BR] Barrett, C.L., and Reidys, C.M., Elements of a Theory of Simulation, I: Sequential CA Over Random Graphs, *Appl. Math. and Comput.* **98**, 1999, 241–259.
- [BMR1] Barrett, C.L., Mortveit, H.S., and Reidys, C.M., Elements of a Theory of Computer Simulation II: Sequential Dynamical Systems, *Appl. Math. and Comp.* **107** (2–3), 1999, 121–136.
- [BMR2] Barrett, C.L., Mortveit, H.S., and Reidys, C.M., Elements of a Theory of Computer Simulation III: Equivalence of SDS, *Appl. Math. and Comp.* **122**, 2001, 325–340.
- [CS] Celada, F., and Seiden, P.E., A computer model of cellular interactions in the immune system, *Immunol. Today* **13**, 1992, 56–62.
- [C] Cull, P., Linear analysis of switching nets, *Kybernetik* **8**, 1971, 31–39.
- [E] Elspas, Bernard, The Theory of Autonomous Linear Sequential Networks, *IRE Transactions on Circuit Theory*, **CT-6**, 1959, 45–60.
- [G] Germundsson, R., Gunnarsson, J., and Plantin, J., Symbolic algebraic discrete systems—applied to the JAS39 fighter aircraft, technical report, Linköping University, Linköping, Sweden, December, 1994.
- [H] Hernández Toledo, René A, Linear Finite Dynamical Systems, preprint, 2003.
- [K] Kauffman, S.A., Metabolic stability and epigenesis in randomly constructed genetic nets, *J. Theor. Biol.* **22**, 1969, 437–467.
- [KN] Khrennikov, A., and Nilsson, M., On the number of cycles of p -adic dynamical systems, *J. Number Theory* **90**, 2001, 255–264.
- [L] Laubenbacher, R., A computer algebra approach to biological systems, Proc. Intl. Symp. Symbolic and Alg. Comp., Philadelphia, Assoc. Comp. Mach., 2003.
- [LP1] Laubenbacher, R., and Pareigis, B., Equivalence relations on finite dynamical systems, *Adv. Applied Math.* **26**, 2001, 237–251.
- [LP2] Laubenbacher, R., and Pareigis, B., Decomposition and simulation of sequential dynamical systems, *Adv. Applied Math.* **30**, 2003, 655–678.
- [LS] Laubenbacher, R., and Stigler, B., A computational algebra approach to the reverse-engineering of gene regulatory networks, preprint, 2003.
- [LN] Lidl, R., and Niederreiter, H., *Finite Fields*, Encyclopedia of Math and its Appl. **20**, Cambridge University Press, London, 1997.
- [M1] Marchand, H., and LeBorgne, M., On the optimal control of polynomial dynamical systems over \mathbf{Z}/p , *Fourth workshop on Discrete Event Systems*, Cagliari, Italy, IEEE, 1998.
- [M2] Marchand, H., and LeBorgne, M., Partial order discrete event systems modeled as polynomial dynamical systems, IEEE Intl. Conf. on Control Applications, Trieste, Italy, 1998.
- [MW] Milligan, D.K., and Wilson, M.J.D., The behaviour of affine sequential Boolean networks, *Connection Science* **5**, 1993, 153–167.
- [W] Wolfram, S., *Cellular Automata and Complexity*, Westview Press, 1994.

VIRGINIA BIOINFORMATICS INSTITUTE, VIRGINIA TECH, BLACKSBURG, VA 24061-0477, USA

MATHEMATISCHES INSTITUT DER UNIVERSITÄT MÜNCHEN, GERMANY