On the Dynamics of Bounded-Degree Automata Networks

Julio Aracena[4], Florian Bridoux[3], Maximilien Gadouleau[5], Pierre Guillon[1],
Kévin Perrot[2], Adrien Richard[3], and Guillaume Theyssier[1]

[1] Aix-Marseille Université, CNRS, I2M UMR7373, Marseille, France
[2] Aix-Marseille Université, Univ. Toulon, CNRS, LIS UMR7020, Marseille, France
[3] Univ. Côte d'Azur, CNRS, I3S UMR 7271, Sophia Antipolis, France
[4] Departamento de Matemáticas, Universidad de Concepción, Chile
[5] Department of Computer Science, Durham University, Durham, UK

Abstract. Automata networks can be seen as bare finite dynamical systems, but their growing theory has shown the importance of the underlying communication graph of such networks. This paper tackles the question of what dynamics can be realized up to isomorphism if we suppose that the communication graph has bounded degree. We prove several negative results about parameters like the number of fixed points or the rank. We also show that we can realize with degree 2 a dynamics made of a single fixed point and a cycle gathering all other configurations. However, we leave open the embarrassingly simple question of whether a dynamics consisting of a single cycle can be realized with bounded degree, although we prove that it is impossible when the network is supposed centralized, and that realizing precisely a Gray code map is impossible with bounded degree. Finally we give bounds on the complexity of the problem of recognizing such dynamics.

1 Introduction

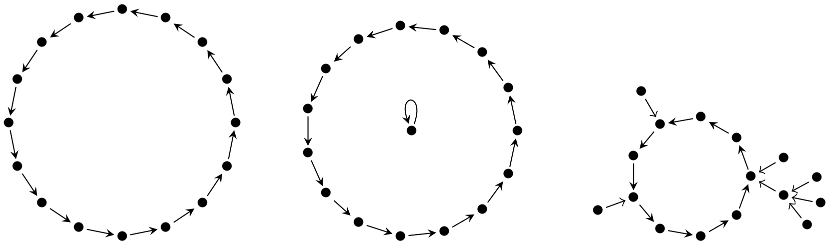
TODO: complete/adapt with new results : Theorems 2, 3, 4, 5, 6

TODO: better review of existing litterature

TODO: better blabla

One possible definition for a boolean automata network is simply a self-map $F : \{0,1\}^n \to \{0,1\}^n$. This definition forgets about the computational aspect of the model, which consists, through a dual point of view, in a set of n automata linked by some arcs, each holding a bit that they can update depending on that of their incoming neighbors.

As a model of computation generalizing finite cellular automata, this communication graph is quite relevant, and it is natural to constrain it, in particular the possible degrees: a small degree indeed represents simple local computations, whereas a complete communication graph can yield any dynamics $F : \{0,1\}^n \to \{0,1\}^n$. The minimal communication graph, often called interaction graph, plays an important role in automata network theory (see[6] for a



(a) a cycle of length 2^n.

(b) a cycle of length 2^n-1 and an isolated vertex.

(c) a cycle of length 2^n-C and a size-C forest plugged to it.

Fig. 1. Three examples of dynamics on 2^4 configurations.

survey). It was already established that some dynamics require high degree, and even a dense communication graph [1].

In this paper, we address the question of how restrictions on the communication graph, and in particular bounding its degrees, can impose restrictions on the possible dynamics. For instance, in Figure 1, one can see three (families of) graphs representing possible dynamics. Which are the ones that can be realized by communication graphs with small degree?

In Section 3, we establish bounds on different parameters of the dynamics depending on the degree of communication graphs. This in particular allows to show that the family of dynamics from Figure 1(c) cannot be realized with a bounded-degree communication graph. In Section 4, we give some constructions using feedback shift registers, which allow in particular to realize dynamics of the type from Figure 1(b) with communication graphs of degree 2. Finally, in Section 6, we give upper and lower bounds for the computational complexity of recognizing dynamics that can be realized with a bounded-degree communication graph.

However, we leave open the question about the minimum degree necessary to realize dynamics from Figure 1(a). Prior to this work, J. Aracena and A. Zapata formulated the conjecture that such dynamics requires unbounded degree. This also appears in [2] with various intermediate results.

2 Definitions and notations

Consider a finite alphabet Q with $q = |Q|$ symbols. Without loss of generality, $Q = \{0, \dots, q-1\}$. Consider also a set $V = \{1, \dots, n\}$ of n *nodes*. A *configuration* $x = (x_i)_{i \in V} \in Q^V$ is a function $V \to Q$. For every $U \subseteq V$, we denote $x_U : U \to Q$ the restriction of x to U, *i.e.*, $(x_U)_i = x_i$ for every $i \in U$. Given a *pattern* $u \in Q^U$, we define the *cylinder* $[u] = \{x \in Q^V : x_U = u\}$.

An *automata network* (AN) is a map $F : Q^V \to Q^V$. It can be represented as a *dynamics graph*, like those from Figure 1, by linking each configuration x to its image $F(x)$. This graph is denoted by $\mathcal{D}(F)$. Two ANs are called isomorphic if their dynamics graphs are isomorphic. A configuration x such that $F(x) = x$ is called a fixed point, and the number of fixed points of F is denoted $\mathrm{fp}(F)$. The *rank* of F is its number of images and is denoted by $\mathrm{rk}(F)$. The set of ANs with alphabet of size q and with n nodes is denoted $\mathcal{F}(n, q)$.

A *communication graph* for F is a graph over vertex set V such that for every $i \in V$, and every $x, x' \in Q^V$ which agree over the in-neighborhood $N^-(i) \subseteq V$ of i, we have $F(x)_i = F(x')_i$. In other words, the value $F(x)_i$ is updated thanks to a local function $f_i : Q^V \to Q$ which depends only on the values $x_{N^-(i)}$. For $U \subseteq V$, we may also denote $f_U(x) = F(x)_U$. The *interaction graph* of F, denoted $G(F)$, is the minimal communication graph of F. Its *degree* is the maximum in-degree of a vertex in $G(F)$. By extension, the *degree* of F is the degree of its interaction graph. We denote by $\mathcal{F}(n, q, d)$ the set of ANs from $\mathcal{F}(n, q)$ with degree at most d.

KP: was $F(x)_{N^-(i)} = F(x')_{N^-(i)}$

A first remark is that if $u \in Q^{N^-(i)}$, then $|[u]| = 2^{n-|N^-(i)|} = 2^{n-d}$ if the in-degree of i in the communication graph is d.

Another remark which will be useful is the following lemma.

Lemma 1. *Consider $F \in \mathcal{F}(n, q, d)$ and $U \subseteq V$ with $|U| \leq \lfloor n/d \rfloor$. Then for any pattern $u \in Q^U$, $\left|F^{-1}([u])\right|$ is a multiple of $q^{n-|U|d}$.*

Proof. Since the degree of $G(F)$ is upper-bounded by d, f_U only depends of $Y = \bigcup_{i \in U} N^-(i)$, so that $|Y| \leq |U|\, d$. In other words, for every $x \in Q^U$ such that $f_U(x) = u$, we have $f_U([x_Y]) = \{u\}$. Hence, $\left|F^{-1}([u])\right| = \left|\{v \in Q^Y \mid f_U([v]) = u\}\right| q^{n-|Y|}$. Since $|Y| \leq |U|\, d$, this is a multiple of $q^{n-|U|d}$. □

3 Non-local dynamics

Here we prove that some dynamics are intrinsically non-local in the sense that they cannot be realized by bounded-degree networks, even up to isomorphism.

The identity AN on Q^V ($F(x) = x$ for all x) has q^n fixed points and degree 1. Our first result shows that if $G(F)$ has bounded degree and F is not the identity, then the number of fixed points of F cannot be close to q^n.

Proposition 1. *Let $F \in \mathcal{F}(n, q, d)$ with $\mathrm{fp}(F) < q^n$. Then $\mathrm{fp}(F) \leq q^n - q^{n-d}$.*

Proof. Since F is not the identity map, there exist $i \in V$ and $x \in Q^V$ such that $f_i(x) \neq x_i$. There are two cases. If $i \notin N^-(i)$, then every pattern $u \in Q^{V \setminus \{i\}}$ admits two extensions $y, y' \in [u]$, with $y_i \neq y'_i$, but $f_i(y) = f_i(y')$, so that at most one of them is a fixed point. Hence, $\mathrm{fp}(F) \leq q^n - q^{n-1} \leq q^n - q^{n-d}$. On the other hand, if $i \in N^-(i)$, then let $u = x_{N^-(i)}$; for every configuration $y \in [u]$, $f_i(y) = f_i(x) \neq x_i = y_i$ and y is not a fixed point. Therefore, $\mathrm{fp}(F) \leq q^n - |[u]| \leq q^n - q^{n-d}$. □

Remark 1. The bound from the previous lemma is tight: indeed let $F(x) = x$ if $x_{1,\dots,d} \neq 0^d$ and $\pi x_1 x_{2,\dots,n}$ otherwise, where π is a derangement of Q. Then F is an AN of degree d with $q^n - q^{n-d}$ fixed points. Alternatively, consider the graph

G on $\{1,\dots,n\}$ with arcs $\{(i,i) : i \in \{1,\dots,n\}\} \cup \{(i,1) : i \in \{2,\dots,d\}\}$. Then G has degree d and following [**?**, Theorem 3], there is an AN with interaction graph G and exactly $q^n - q^{n-d}$ fixed points (namely, F given above).

Proposition 1 can be generalised to the powers of F. First, note that if $F \in \mathcal{F}(q,n,d)$ then $F^k \in \mathcal{F}(q,n,d^k)$ for every $k \geq 1$ (because from $G(F)$ of degree $\leq d$ we obtain a communication graph for F^k by putting an edge for each path of length k). By combining this remark and Proposition 1, we obtain that, if $\mathrm{fp}(F^k) < q^n$ then $\mathrm{fp}(F^k) \leq q^n - q^{n-d^k}$.

As an application, we can easily find bijections without fixed points that force large communication degrees. Suppose for instance that the dynamics of $F \in \mathcal{F}(2,n)$ consists of $2^{n-1} - 2$ limit cycles of length 2 and one limit cycle of length 4. Then F^2 has exactly $2^n - 4$ fixed points. Denoting by d the degree of $G(F)$, we obtain that $2^n - 4 = \mathrm{fp}(F^2) \leq 2^n - 2^{n-d^2}$ and thus $d \geq \sqrt{n-2}$.

Remark 2. The number of nonisomorphic bijective ANs is $p(q^n)$ (where p is the partition function), which is asymptotically given by the Hardy-Ramanujan formula (see [**?**]):

$$p(q^n) \sim \frac{1}{4q^n\sqrt{3}} \exp(\pi\sqrt{2q^n/3}).$$

However, there are only $(q^{q^d})^n$ AN with degree $\leq d$. So few bijective AN have a realization with bounded degree.

Our second result shows that if $G(F)$ has bounded degree and F is not a bijection, then the rank of F cannot be close to q^n. In [2], it is shown that certain dynamics with rank $q^n - 1$ can only be realised by ANs of degree n. In particular, we generalise this result by showing that all dynamics with rank $q^n - 1$ require degree n.

Theorem 1. *Let $F \in \mathcal{F}(n,q,d)$ with $rk(F) < q^n$. Then $rk(F) \leq q^n - 2$ for $d = n-1$ and $rk(F) \leq q^n - \frac{n}{d+1}$ for $d < n-1$.*

Theorem 1 states AN dynamics cannot be close to bijective without being bijective. In particular, the family of dynamics depicted in Figure 1(c) is impossible to realize with bounded-degree ANs. However, Theorem 1 fails among bijective ANs of fixed degree, such as the dynamics depicted in Figure 1(c), as we will see in Section 4.

To prove the theorem, we need as simple witnessing lemma.

Lemma 2. *If $Y \subset Q^V$ with $|Y| \leq n$, and $x \in Q^V \setminus Y$, then there exists $U \subset V$ with $|U| \leq |Y|$ and $[x_U] \cap Y = \emptyset$.*

Proof. Let us prove the statement by induction on Y. If $Y = \emptyset$, the trivial cylinder with $U = \emptyset$ is suitable. Now, let Y and x be such that there exists $U \subset V$ with $|U| \leq |Y|$ and $[x_U] \cap Y = \emptyset$. Let us prove the statement for $Y \sqcup \{y\}$, where $y \in Q^V \setminus (Y \sqcup \{x\})$. Since $x \neq y$, there exists $i \in V$ such that $x_i \neq y_i$. Note that $|U \cup \{i\}| \leq |U| + 1 \leq |Y| + 1$. Hence $[x_{U\cup\{i\}}] \subset [x_U]$; by induction hypothesis, it does not intersect Y. Moreover, $[x_{U\cup\{i\}}] \subset [x_{\{i\}}] \not\ni y$. It results that $[x_{U\cup\{i\}}] \cap (Y \sqcup \{y\}) = \emptyset$. □

For $F \in \mathcal{F}(n,q)$ and $k \in \mathbb{N}$, let us define $Y_k = \left|F^{-1}(y)\right| = k\}$. We also note $Y_{\geq \ell} = \bigcup_{k \geq \ell} Y_k$. Remark that $Q^V = Y_{\geq 0}$, and that $\sum_{k \in \mathbb{N}} k \, |Y_k| = q^n$, so that $q^n - \mathrm{rk} F = |Y_0| \geq |Y_{\geq 2}| \geq |Y_0| \max_{Y_k \neq \emptyset} k$. Clearly, $\mathrm{rk}(F) < q^n \iff |Y_0| > 0 \iff |Y_{\geq 2}| > 0$.

Lemma 3. *Let $F \in \mathcal{F}(n,q)$. If $|Y|_0 \geq 1$ and $|Y_{\geq 2}| \leq \lfloor n/d \rfloor$, then $|Y_0| \geq q^{n - |Y_{\geq 2}| d}$.*

Proof. Let $x \in Y_0$. Since $x \notin Y_{\geq 2}$, Lemma 2 gives some $U \subset Q^V$ such that $|U| \leq |Y_{\geq 2}| \leq \lfloor n/d \rfloor$ and $[x_u] \cap Y_{\geq 2} = \emptyset$. One can write $\left|F^{-1}([x_U])\right|$ as $\left|F^{-1}([x_U] \cap Y_0)\right| + \left|F^{-1}([x_U] \setminus Y_0)\right|$. The first term is 0, by definition of Y_0, and the second is $|[x_U] \setminus Y_0|$, by nonintersection with $Y_{\geq 2}$. Since $x \in [x_U] \cap Y_0$, $\left|F^{-1}([x_U])\right| = |[x_U] \setminus Y_0| < q^{n-|U|}$. On the other hand, Lemma 1 allows to write $\left|F^{-1}([x_U])\right|$ as $\alpha q^{n-|U|d}$, for some $\alpha \in \mathbb{N}$. Since $\alpha q^{n-|U|d} < q^{n-|U|}$, we get that $\alpha \leq q^{|U|(d-1)} - 1$. Putting things together, $|[x_U] \setminus Y_0| = \left|F^{-1}([x_U])\right| \leq (q^{|U|(d-1)} - 1) q^{n-|U|d} = |[x_U]| - q^{n-|U|d}$. We get that $|Y_0| \geq |[x_U]| - |[x_U] \setminus Y_0| \geq q^{n-|U|d} \geq q^{n - |Y_{\geq 2}| d}$. □

Proof (of Theorem 1). If $\mathrm{rk}(F) < q^n$, then $|Y_0| \geq 1$. If $|Y_{\geq 2}| > \lfloor n/d \rfloor$, then $|Y_0| \geq |Y_{\geq 2}| > \lfloor n/d \rfloor$ and we are done. Otherwise, Lemma 3 gives that $|Y_0| \geq q^{n - |Y_{\geq 2}| d} \geq q^{n - |Y_0| d}$. Hence, $\log_q |Y_0| \geq n - |Y_0| \, d$ and $(d+1) \, |Y_0| \geq \log_q |Y_0| + |Y_0| \, d \geq n$ (because $|Y_0| \geq \log_q |Y_0|$ when $|Y_0| \geq 1$). □

Here is another application of Lemma 1.

Proposition 2. *Let $F \in \mathcal{F}(n,q,d)$ such that F is not constant. Then the number of preimages of any configuration is upper-bounded by $q^n - q^{n-d}$.*

Proof. Let $y \in Q^V$. Let us prove that $|F^{-1}(y)| \leq q^n - q^{n-d}$. Since F is not constant, there exists $z \in F(Q^V)$ such that $z_i \neq y_i$ for some $i \in V$. Since $F^{-1}([z_i]) \neq \emptyset$, by Lemma 1, $|F^{-1}([z_i])| \geq q^{n-d}$. Furthermore, since $F^{-1}([z_i]) \cap F^{-1}(y) = \emptyset$, we conclude $|F^{-1}(y)| \leq q^n - q^{n-d}$. □

It is tight because we can have $F(x) = 0^n$ if $x_{1,\dots,d} \neq 0^d$ and 10^{n-1} otherwise.

4 Realization results

4.1 Feedback shift registers

In this section, we are interested in realizing examples of AN with *almost degree* 1, *i.e.*, whose all but one nodes have degree at most 1.

We use the following important tool. Let $g : Q^n \to Q$, and $F_g : Q^n \to Q^n$ be the corresponding *feedback shift register* (FSR), that is, $F_g(x) = F_g(x_1, \dots, x_n) = (x_2, \dots, x_n, g(x))$. $G(F_g)$ is thus obtained from the path $1 \to 2 \to \cdots \to n$ by adding an arc from i to n whenever g depends on input i: it has almost degree 1.

The *de Bruijn graph* of order n over the alphabet Q has vertex set $V = Q^n$ and arc set $E = \{(au, ub) : a, b \in Q, u \in Q^{n-1}\}$.

Proposition 3 ([?]). *For any n and any $1 \leq k \leq q^n$, the de Bruijn graph of order n admits a cycle of length k.*

Proposition 4. *For any n and any $1 \leq k \leq q^n$, there exists $F : Q^n \to Q^n$ with almost degree 1 and whose maximum limit cycle has length k.*

Proof. Consider some cycle C of length k in the de Bruijn graph of order n over Q, given by Proposition 3, and the feedback shift register F_g, where

$$g(x) = \begin{cases} b & \text{if } x = au \text{ and } au \to ub \in C; \\ 0 & \text{otherwise.} \end{cases}$$

F_g has almost degree 1, and has the cycle C in its dynamics. To conclude the proof, it is sufficient to observe that the dynamics on the complement of C consists in adding 0 at node n and shifting node $i+1$ to node i for $i < n$. Therefore, the only possible cycle created by this part of the dynamics is possibly the fixed point $0 \cdots 0$. □

4.2 Construction of near-Hamiltonian dynamics with in-degree 2

We say $F : Q^V \to Q^V$ is near-Hamiltonian if it has one fixed point and a cycle of length $q^n - 1$. In this section, we let q be a prime power and $Q = \mathrm{GF}(q)$ be the finite field of order q. We can then construct a near-Hamiltonian AN $F : \mathrm{GF}(q)^n \to \mathrm{GF}(q)^n$ with an interaction graph of maximum in-degree 2.

KP: the second one was $\mathrm{GF}(q)^m$

Theorem 2. *For any prime power q and any $n \geq 2$, there exists a near-Hamiltonian AN in $\mathcal{F}(n, q, 2)$.*

Proof. Let $\mathrm{GF}(q^n)$ be generated by the primitive polynomial $P(\xi) = \sum_{i=0}^{n-1} p_i \xi^i$ and let α be a root of $P(\xi)$, i.e. a primitive element of $\mathrm{GF}(q^n)$. We then identify $\mathrm{GF}(q^n)$ and $\mathrm{GF}(q)^n$ as follows:

$$x = (x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(q)^n \sim \beta = x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} \in \mathrm{GF}(q^n).$$

Then

$$F(x) = \alpha x$$

is near-Hamiltonian: 0 is a fixed point, and since $\mathrm{GF}(q^n)^*$ is a cyclic group generated by α, we have the cycle $1 \mapsto \alpha \mapsto \cdots \mapsto \alpha^{q^n-2} \mapsto \alpha^{q^n-1} = 1$.

For any $\beta \in \mathrm{GF}(q^m)$, we have

$$\begin{aligned}\alpha\beta &= \alpha \sum_{j=0}^{m-1} x_j \alpha^j \\ &= \sum_{j=0}^{m-2} x_j \alpha^{j+1} + x_{m-1}\alpha^m \\ &= \sum_{i=0}^{m-1} x_{i-1}\alpha^i + x_{m-1} \sum_{i=0}^{m-1} (-p_i)\alpha^i \\ &= \sum_{i=0}^{m-1} (x_{i-1} - p_i x_{m-1})\alpha^i.\end{aligned}$$

The local functions are then given by

$$f_i(x) = x_{i-1} - p_i x_{m-1},$$

(with $x_{-1} = 0$), hence F has degree 2. □

Example 1. Let $q = 2$, $n = 3$, $P(\xi) = \xi^3 + \xi + 1$. Then $\alpha^3 = \alpha + 1$, and

$$\mathrm{GF}(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\}$$

(and $\alpha^7 = 1$). We identify $\mathrm{GF}(2)^3$ and $\mathrm{GF}(2^3)$ as follows:

$$\begin{aligned}000 &\sim 0 \\ 100 &\sim 1 \\ 010 &\sim \alpha \\ 001 &\sim \alpha^2 \\ 110 &\sim \alpha + 1 = \alpha^3 \\ 011 &\sim \alpha^2 + \alpha = \alpha^4 \\ 111 &\sim \alpha^2 + \alpha + 1 = \alpha^5 \\ 101 &\sim \alpha^2 + 1 = \alpha^6.\end{aligned}$$

Then F is given as follows:

$$0 \mapsto 0, \quad 1 \mapsto \alpha \mapsto \alpha^2 \mapsto \alpha^3 \mapsto \alpha^4 \mapsto \alpha^5 \mapsto \alpha^6 \mapsto 1,$$

or from a Boolean network point of view:

$$000 \mapsto 000, \quad 100 \mapsto 010 \mapsto 001 \mapsto 110 \mapsto 011 \mapsto 111 \mapsto 101 \mapsto 100.$$

In terms of local functions, we have

$$\begin{aligned}f_0(x) &= x_2 \\ f_1(x) &= x_0 + x_2 \\ f_2(x) &= x_1.\end{aligned}$$

4.3 Rank $q^n - 2$ with $d = 2n/3$

We have shown in Theorem 1 that rank $q^n - 1$ required degree n. For rank $q^n - 2$, however, the bound only yields $d \geq n/2 - 1$; we now prove that we can achieve $d = \lceil \frac{2}{3} n \rceil$.

Theorem 3. *For all $n \geq 3$ and all odd $q \geq 3$, there exists an AN in $\mathcal{F}(n, q, d = \lceil \frac{2}{3} n \rceil)$ with rank $q^n - 2$.*

Proof. First, we consider the case $n = 3$ and $d = 2$. Let $q \geq 3$ be odd and $Q = \mathbb{Z}_q$. The local functions of F are given as follows.

$$f_1(x_1, x_3) = \begin{cases} x_1 & \text{if } x_1 \geq 2 \\ (x_1 + x_3) \mod 2 & \text{if } x_1 \in \{0, 1\}, \end{cases}$$

$$f_2(x_1, x_2) = \begin{cases} x_2 & \text{if } x_1 \geq 2 \\ (x_1 + x_2) \mod q & \text{if } x_1 \in \{0, 1\}, x_2 \neq 0 \\ 1 & \text{if } x_1 x_2 = 00 \\ 0 & \text{if } x_1 x_2 = 10, \end{cases}$$

$$f_3(x_2, x_3) = \begin{cases} x_3 & \text{if } x_2 \neq 0 \\ (x_3 + 1) \mod q & \text{if } x_2 = 0. \end{cases}$$

For instance, for $q = 3$ we obtain:

x	$F(x)$	x	$F(x)$	x	$F(x)$
000	011	100	101	200	201
001	112	101	002	201	202
002	010	102	100	202	200
010	010	110	120	210	210
011	111	111	021	211	211
012	012	112	122	212	212
020	020	120	100	220	220
021	121	121	001	221	221
022	022	122	102	222	222

We now search for collisions. One can easily check the following two collisions:

$$F(0, 0, q - 1) = F(0, 1, 0), \tag{1}$$

$$F(1, 0, q - 1) = F(1, q - 1, 0). \tag{2}$$

We now prove that those are the only collisions. Suppose $a = a_1 a_2 a_3$ and $b = b_1 b_2 b_3$ are two distinct configurations, say $q^2 a_1 + q a_2 + a_3 < q^2 b_1 + q b_2 + b_3$, such that $F(a) = F(b)$. We proceed by a case analysis.

1. $b_1 \geq 2$.
   Then $f_1(a) = f_1(b) \geq 2$, hence $a_1 = f_1(a) = f_1(b) = b_1 \geq 2$. Moreover, $f_2(a) = a_2 = f_2(b) = b_2$. Thus $a_2 = b_2$ and $a_3 \neq b_3$, which yields $f_3(a) \neq f_3(b)$, which is the desired contradiction.

2. $a_1 = 0$, $b_1 = 1$.
   Since $f_2(a) = f_2(b)$, we obtain $a_2 \in \{2, \dots, q-1\}$ and $b_2 = a_2 - 1 \in \{1, \dots, q-2\}$. Since $f_3(a) = f_3(b)$ and $a_2, b_2 \neq 0$, we obtain $a_3 = b_3$. But then $f_1(a) = a_3 \mod 2 \neq (b_3 + 1) \mod 2 = f_3(b)$, which is the desired contradiction.
3. $a_1 = b_1 = 0$.
   First, we have $a_2 \neq b_2$, since otherwise $a_2 = b_2$ and $a_3 \neq b_3$ thus $f_3(a) \neq f_3(b)$. Now, since $f_2(a) = f_2(b)$, we obtain $a_2 = 0$ and $b_2 = 1$. Then $(a_3 + 1) \mod q = f_3(a) = f_3(b) = b_3$ and $a_3 \mod 2 = f_1(a) = f_1(b) = b_3 \mod 2$; those two constraints are both satisfied only if $a_3 = q - 1$ and $b_3 = 0$. Therefore a and b are the collision in (1).
4. $a_1 = b_1 = 1$.
   Again, we have $a_2 \neq b_2$, hence $a_2 = 0$ and $b_2 = q - 1$. By the same reasoning as above, we obtain $a_3 = q - 1$ and $b_3 = 0$. Therefore a and b are the collision in (2).

Having proved the case $n = 3$, we now move on to the case where $n = 3\ell$ for some $\ell \geq 1$. Let q be odd and let $k = q^\ell$ be odd as well. Consider $F \in \mathcal{F}(k, 3, 2)$ as described above. By identifying $\mathbb{Z}_k$ with $(\mathbb{Z}_q)^\ell$, we obtain a network $\tilde{F} \in \mathcal{F}(q, n = 3\ell, d = 2\ell)$ of rank $k^3 - 2 = q^n - 2$.

We now deal with the other case, say $n = 3\ell + r$ for some $r \in \{1, 2\}$; write $[n] = L \cup R$ with $L = \{1, \dots, 3\ell\}$ and $R = \{3\ell + 1, \dots, n\}$. Let $\tilde{F} \in F(q, 3\ell, 2\ell)$ of rank $q^{3\ell} - 2$ as above. Then let $\hat{F} \in F(q, n = 3\ell + r, d = 2\ell + r)$ choose between the identity function on L or $\tilde{F}$, depending on the control bits in R:

KP: second line of $\hat{f}_L(x)$ it was $\tilde{f}(x_L)$ instead of $\tilde{F}(x_L)$

$$\hat{f}_L(x) = \begin{cases} x_L & \text{if } x_R \neq 0 \\ \tilde{F}(x_L) & \text{if } x_R = 0 \end{cases}$$
$$\hat{f}_R(x) = x_R.$$

Then $\hat{F}(x) = \hat{F}(y)$ for some $x \neq y$ if and only if $x_R = y_R = 0$ and x_L and y_L collide: $\tilde{F}(x_L) = \tilde{F}(y_L)$. Thus there are only two collisions. □

5 Further negative results for the Boolean case

In this section, we consider the case of $q = 2$ and $d = 2$. This is an interesting case, as the only balanced functions $f_i : \{0,1\}^2 \to \{0,1\}$ on two variables are affine. Therefore, any permutation in $\mathcal{F}(n, q = 2, d = 2)$ must be affine. This algebraic restriction leads to strong dynamical restrictions, as seen below.

5.1 Non-existence of Boolean Hamiltonian with degree 2

We call an AN $F : Q^V \to Q^V$ Hamiltonian if its dynamics consists of a single cycle of length q^n. We prove that $\mathcal{F}(n, 2, 2)$ does not contain any Hamiltonian AN (for $n \geq 3$). We use a result that can be applied to any affine AN.

Theorem 4. *If F is an affine AN over $\mathrm{GF}(q)^n$ with $n \geq 3$, then it is not Hamiltonian.*

Proof. Computer search settles the case where $n = 3$ and $q = 2$. We now assume $(n, q) \neq (3, 2)$, which is equivalent to $n \leq q^{n-2}$.

Let F be affine, i.e. $F(x) = Ax + v$ for some matrix $A \in \mathrm{GF}(q)^{n \times n}$ and some vector $v \in \mathrm{GF}(q)^n$. For the sake of contradiction, suppose F is Hamiltonian. Denoting $k = q^n$, we have

$$F^k(x) = A^k x + (A^{k-1} + A^{k-2} + \cdots + A + I)v = x,$$

hence $A^k = I$.

Let $B = A - I$. Since A and $-I$ commute, we have $B^k = A^k + (-I)^k$ [8, Theorem 1.46] and hence $B^k = A^k + (-1)^k I = A^k - I = 0$. Thus B is nilpotent and by simple linear algebra, $B^n = 0$. Since $n \leq q^{n-2}$, we have $B^{q^{n-2}} = 0$, and hence $A^{q^{n-2}} = I$.

Thus $F^{q^{n-2}}(x) = x + u$ for some vector u and

$$F^{q^{n-1}}(x) = x + qu = x,$$

which contradicts the fact that F is Hamiltonian. □

Corollary 1. *Let $q = 2$ and $n \geq 3$. If F is Hamiltonian, then F has degree at least 3.*

Proof. Suppose F is Hamiltonian of degree 2. All the local functions of F are balanced, hence F is affine, which contradicts Theorem 4. □

5.2 Upper bound on the rank

We can significantly refine the bound in Theorem 1 for the case $q = 2$, $d = 2$.

Proposition 5. *Suppose $F \in \mathcal{F}(n, 2, 2)$ with $rk(F) < 2^n$. Then $rk(F) \leq 2^n - 2^{n-2}$.*

Proof. Suppose F is a non-bijective AN in $\mathcal{F}(n, 2, 2)$. First, if all its local functions are balanced, then F is affine, hence $\mathrm{rk}(F) \leq 2^{n-1} < 2^n - 2^{n-2}$. Second, if the local function $f_v(x_u, x_v)$ is not balanced, then there exists $b \in \{0, 1\}$ such that $|f_v^{-1}(b)| \geq 3$. Let $A = \{x : x_{uv} \in f_v^{-1}(b)\}$ and $B = \{x : x_v = b\}$. Denoting $\bar{A} = \{0, 1\}^V \setminus A$, we obtain

$$|f(\{0,1\}^V)| \leq |f(A)| + |f(\bar{A})| \leq |B| + |\bar{A}| \leq 2^{n-1} + 2^{n-2} = 2^n - 2^{n-2}.$$

□

Remark 3. This bound is also tight. Indeed, let $F \in \mathcal{F}(n, 2, 2)$ be defined by $f_1(x_1, x_2) = x_1 \wedge x_2$ and $f_i(x) = x_i$ otherwise. Then $F(\{0, 1\}^V) = \{x \in \{0, 1\}^V : x_1 x_2 \neq 10\}$ so that $\mathrm{rk}(F) = 2^n - 2^{n-2}$.

5.3 Hamiltonian dynamics on centralized interaction graphs

To be more concise in the following, we use the following notations: $x + y$ on configurations to mean addition modulo 2 componentwise, e_i the configuration equal to 1 at node i and 0 elsewhere. We also denote $[n] = \{1, 2, \dots, n\}$.

Aracena and Zapata conjectured that for all $n \geq 3$, if $F \in \mathcal{F}(n, 2)$ is Hamiltonian, then F has degree n. Equivalently, there is no Hamiltonian function in $\mathcal{F}(n, 2, d)$ when $d < n$. Actually, we need to impose $n \geq 3$ since the function $F \in \mathcal{F}(2, 2)$ defined by $F(x_1, x_2) = (x_2, x_1 + 1)$ is Hamiltonian and belongs to $\mathcal{F}(2, 2, 1)$. In this section, we prove the conjecture under the assumption that $G(F)$ is *centralized*, that is, $G(F)$ has a node whose deletion leaves the graph acyclic. In the following, we abusively say that F is centralized when $G(F)$ is. Note that FSRs are centralized networks. So we will prove that there is no centralized Hamiltonian function in $\mathcal{F}(n, 2, d)$ when $d < n$. We actually prove something stronger.

Theorem 5. *Let $F \in \mathcal{F}(n, 2, d)$ be a centralized bijection. If $n \geq 3$ and $d < n$, then F has an even number of limit cycles.*

The main tool is a swap operation on F, taken from [4], defined (in our setting) as follows. Given distinct $x, y \in \{0, 1\}^n$, let $(x \leftrightarrow y)$ the permutation of $\{0, 1\}^n$ that swaps x and y: $(x \leftrightarrow y)(x) = y$, $(x \leftrightarrow y)(y) = x$ and $(x \leftrightarrow y)(z) = z$ for all $z \neq x, y$. Given $F \in \mathcal{F}(n, 2)$, we say that $F' = F \circ (x \leftrightarrow y)$ is a *swap* of F. Let $p(F) \in \{0, 1\}$ be the parity of the number of limit cycles in F, and suppose that F is a bijection. Then F' is a bijection and the swap operation changes the parity of the number of limit cycles: $p(F') \neq p(F)$. Indeed, let C_x and C_y be the limit cycles of F containing x and y, respectively, and let ℓ and ℓ' be the numbers of limit cycles in F and F', respectively. Clearly every limit cycle of F distinct from C_x, C_y is also a limit cycle of F'. Then, we have two cases. First, if $C_x = C_y$, then the swap operation splits this limit cycle into two limit cycles so that $\ell' = \ell + 1$; see Figure 2(a) for an illustration. Second, if $C_x \neq C_y$, then the swap operation joins the two limit cycles into one limit cycle so that $\ell' = \ell - 1$; see Figure 2(b) for an illustration. Thus in any case $p(F) \neq p(F')$.

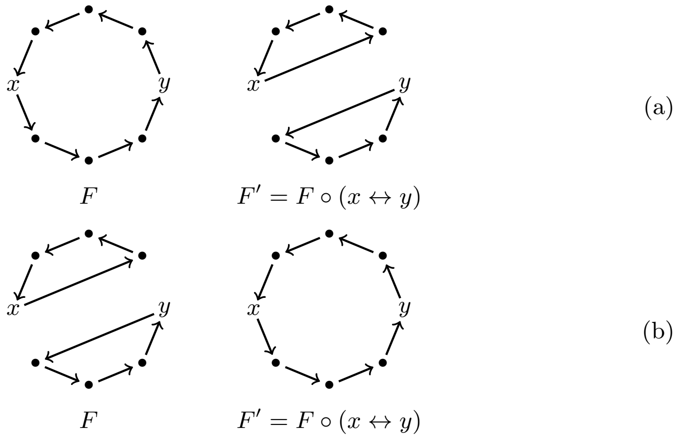
More generally, for $k \geq 1$, we say that F' is a *k-swap* of F if there exists configurations $x^1, y^1, \dots, x^k, y^k$, with $x^i \neq y^i$ for all $1 \leq i \leq n$, such that

$$F' = F \circ (x^1 \leftrightarrow y^1) \circ \cdots \circ (x^k \leftrightarrow y^k).$$

By convention, the 0-swap of F is F itself. The k-swap operation preserves the bijectivity, and since each individual swap changes the parity of the number of limit cycles, we obtain the following lemma.

Lemma 4. *Let $F \in \mathcal{F}(n, 2)$ be a bijection, and let F' be a k-swap of F. Then $p(F) = p(F')$ if and only if k is even.*

In [4], Fredricksen gives a survey of Hamiltonian FSRs and, given a bijective FSR $F \in \mathcal{F}(n, 2)$, the swap operation is used to connect $p(F)$ and the *weight*



F $\quad F' = F \circ (x \leftrightarrow y)$

F $\quad F' = F \circ (x \leftrightarrow y)$

Fig. 2. Illustration of the swap operation.

of F defined (in our setting) as the number $w(F)$ of configurations $x \in \{0,1\}^n$ such that $x_n < F_1(x)$. Let $\sigma \in F(n,2)$ be the *circular shift*, defined by

$$\sigma(x) = (x_n, x_1, \dots, x_{n-1}).$$

Fredricksen proves that σ is a $w(F)$-swap of F. He also says, without proof, that $p(\sigma) = 0$. From these two properties and Lemma 4, we obtain that $p(F)$ is the parity of $w(F)$. An unmentioned and easy to prove consequence is that if node 1 has in-degree at most $n-1$ in $G(F)$, then $w(F)$ is even (this will be generalized in Lemma 9) and thus F has an even number of limit cycles: this proves Theorem 5 (and thus Aracena-Zapata's conjecture) for FSRs.

In addition to this simple observation, our contribution is an extension of the mentioned results to centralized networks, giving Theorem 5. We start by giving a simple proof that σ has an even number of limit cycles (when $n \geq 3$), which already used the swap technic.

Lemma 5. *For all $n \geq 3$, we have $p(\sigma) = 0$.*

Proof. Let $\bar\sigma \in \mathcal{F}(n,2)$ defined by $\bar\sigma(x) = \sigma(x) + e_1$. Since $\sigma(x+y) = \sigma(x) + \sigma(y)$ we have, $\bar\sigma^2(x) = \sigma(\bar\sigma(x)) + e_1 = \sigma(\sigma(x) + e_1) + e_1 = \sigma^2(x) + \sigma(e_1) + e_1$. More generally, for all $k \geq 1$,

$$\bar\sigma^k(x) = \sigma^k(x) + \sigma^{k-1}(e_1) + \cdots + \sigma^0(e_1).$$

In particular, since σ^n is the identity, we have

$$\bar\sigma^n(x) = x + \sigma^{n-1}(e_1) + \cdots + \sigma^0(e_1) = x + e_n + e_{n-1} + \cdots + e_1 = x + 1,$$

so $\bar\sigma^n$ is the negation. Suppose that $\bar\sigma$ has exactly r limit cycles, with length $c_1, \dots, c_r$. Since $\bar\sigma^n$ is the negation, $\bar\sigma^{2n}$ is the identity. Thus $\bar\sigma$ is a bijection and each c_i divides $2n$ but not n. Let $\alpha \geq 0$ be the integer such $n/2^\alpha$ is odd; since $n \geq 3$ we have $n > \alpha + 1$. The fact that c_i divides $2n$ but not n means that $c_i = 2^{\alpha+1} q_i$ for some odd integer q_i. Since $\bar{\sigma}$ is a bijection, we have

$$2^{\alpha+1} \sum_{i=1}^{r} q_i = \sum_{i=1}^{r} \ell_i = 2^n$$

and thus $q_1 + \cdots + q_r = 2^{n-\alpha-1} \geq 2$. Since every q_i is odd we deduce that r is even, that is, $p(\bar{\sigma}) = 0$. Let X be the set of configurations $x \in \{0,1\}^n$ with $x_n = 0$, and let $x^1, \dots, x^k$ be an enumeration of X, so $k = 2^{n-1}$. Let F be the k-swap of $\bar{\sigma}$ defined by

$$F = \bar{\sigma} \circ (x^1 \leftrightarrow x^1 + e_n) \circ \cdots \circ (x^k \leftrightarrow x^k + e_n).$$

For all $x \in X$ we have $\sigma(x + e_n) = \sigma(x) + e_1$; hence $F(x) = \bar{\sigma}(x + e_n) = \sigma(x + e_n) + e_1 = \sigma(x)$ and $F(x + e_n) = \bar{\sigma}(x) = \sigma(x) + e_1 = \sigma(x + e_n)$. Thus $F = \sigma$ is a k-swap of $\bar{\sigma}$ and since k is even, by Lemma 4, $p(\sigma) = p(\bar{\sigma}) = 0$. $\square$

We now extend the notion of weight to the centralized case. We need the following property.

Lemma 6. *If $F \in \mathcal{F}(n,2)$ is a centralized bijection, then $G(F)$ is Hamiltonian.*

Proof. Let $F \in \mathcal{F}(n,2)$ be a bijection. Gadouleau proves in [5] that $G(F)$ contains a spanning subgraph which is a disjoint union of cycles. In $G(F)$, this spanning subgraph necessarily consists of a single cycle, and thus $G(F)$ is Hamiltonian. $\square$

Let $F \in \mathcal{F}(n,2)$ be a centralized bijection, and let C be a Hamiltonian cycle in $G(F)$. Let $i \in [n]$ and let j its in-neighbor in C. We denote by $w_i(F,C)$ the number of configurations $x \in \{0,1\}^n$ such that $x_j < F_i(x)$, and we set

$$w(F,C) = \sum_{i=1}^{n} w_i(F,C).$$

Note that if F is a FSR, there is a unique Hamiltonian cycle C (whose vertices are $1, 2 \dots, n$ in order) and since $w_i(F,C) = 0$ for all $i \neq 1$, we have $w(F) = w_1(F,C) = w(F,C)$ and we recover the previous definition.

Let $\sigma^C \in \mathcal{F}(n,2)$ defined by: for all $i \in [n]$ and $x \in \{0,1\}^n$, $\sigma^C_i(x) = x_j$ where j is the in-neighbor of i in C. Obviously, σ^C is isomorphic to σ and has thus an even number of limit cycles, and $\sigma^C = \sigma$ when the vertices of C are $1, 2, \dots, n$ in order. That σ is a $w(F)$-swap of a bijective FSR F is then generalized as follows.

Lemma 7. *Let $F \in \mathcal{F}(n,2)$ is a centralized bijection and let C be a Hamiltonian cycle of $G(F)$. Then σ^C is a $w(F,C)$-swap of F.*

Proof. Suppose without loss that the vertices of C are $1, 2, \ldots, n$ in order, so that $\sigma^C = \sigma$. For all $i \in [n]$ and $x \in \{0,1\}^n$, we have

$$w_i(F,C) = 0 \;\Rightarrow\; F_i(x) = x_{i-1} \tag{3}$$

where x_0 means x_n. Indeed, let X be the set of $x \in \{0,1\}^n$ with $x_{i-1} = 0$. Since $w_i(F,C) = 0$, if $x_{i-1} = 0$ then $F_i(x) = 0$. Hence $X \subseteq F_i^{-1}(0)$. Since F is a bijection we have $|F_i^{-1}(0)| = |F_i^{-1}(1)| = 2^{n-1}$ and since $|X^0| = 2^{n-1}$ we deduce that $F_i^{-1}(0) = X$. Consequently, if $x_{i-1} = 1$ then $F_i(x) = 1$. This proves (3).

We now prove, by induction on $w(F)$, that σ is a $w(F,C)$-swap of F. If $w(F,C) = 0$ then $F = \sigma$ by (3). This prove the base case. For the induction, suppose that $w(F) > 0$. Since each node i in $G(F)$ with $w_i(F,C) = 0$ is, by (3), of in-degree one, and since $G(F)$ is centralized, there is a node i with $w_i(F,C) > 0$ whose deletion leaves $G(F)$ acyclic. Suppose, without loss, that this node is node 1. Then 1 is the unique out-neighbor of n since otherwise there is a cycle which does not contain node 1. We deduce that, for all $x \in \{0,1\}^n$,

$$F(x + e_n) = F(x) + e_1. \tag{4}$$

Indeed, since 1 is the unique out-neighbor of n, $F(x+e_n)$ and $F(x)$ differ at most in component 1, and since F is a bijection this forces $F(x+e_n) = F(x) + e_1$. Let $y \in \{0,1\}^n$ such that $y_n < F_1(y)$, which exists since $w_1(F,C) > 0$, and let

$$F' = F \circ (y \leftrightarrow y + e_n).$$

Then $F'(y) = F(y+e_n) = F(y) + e_1$, and thus $F'_1(y) = 0$. Furthermore, $F'(y + e_n) = F(y) = F(y+e_n) + e_1$ and for all $x \in \{0,1\}^n$ with $x \neq y, y+e_n$ we have $F'(x) = F(x)$. Hence $G(F')$ has an arc from n to 1, and since $F'_i = F_i$ for all $i \neq 1$ we deduce that C is contained in $G(F')$, and that $w(F',C) = w(F,C) - 1$. By induction, σ is a $w(F',C)$-swap of F' and since F' is a 1-swap F we deduce that σ is a $w(F,C)$-swap of F. □

Putting things together we obtain the following.

Lemma 8. *Let $F \in \mathcal{F}(n,2)$ be a centralized bijection and let C be a Hamiltonian cycle of $G(F)$. Then $p(F)$ is the parity of $w(F,C)$.*

Proof. By Lemma 7, σ^C is a $w(F,C)$-swap of F. Since σ^C is isomorphic to σ, by Lemma 5 we have $p(\sigma^C) = p(\sigma) = 0$. By Lemma 4 $p(F) = 0$ if and only $w(F,C)$ is even. Thus $p(F)$ is the parity of $w(F,C)$. □

To conclude, we need the following easy lemma.

Lemma 9. *Let $F \in \mathcal{F}(n,2,d)$ be a centralized bijection and let C be a Hamiltonian cycle of $G(F)$. If $d < n$ then $w(F,C)$ is even.*

Proof. Suppose that $d < n$. Let $i \in [n]$ and j its in-neighbor in C. Let X be the set of $x \in \{0,1\}^n$ with $x_j < F_i(x)$. Thus $|X| = w_i(F,C)$. Since $d < n$, there exists $k \in [n]$ such that $G(F)$ has no arc from k to i. Let $x \in X$. Since there is an arc from j to i we have $k \neq j$ thus $(x+e_k)_j = 0$, and since there is no arc from k to i we have $F_i(x+e_k) = F_i(x) = 1$, thus $x+e_k \in X$. We deduce that $x \in X$ if and only if $x+e_k \in X$, which proves that $|X| = w_i(F,C)$ is even. Thus each $w_i(F,C)$ is even, and so is $w(F,C)$. □

The proof of Theorem 5 is now straightforward.

Proof (of Theorem 5). Let $F \in \mathcal{F}(n,2,d)$ be a centralized bijection. By Lemma 6, $G(F)$ has a Hamiltonian cycle C. If $d < n$ then $w(F,C)$ is even by Lemma 9 and thus $p(F) = 0$ by Lemma 8. □

Theorem 5 suggests the following strengthening of Aracena-Zapata's conjecture: if $F \in \mathcal{F}(n,2,d)$ is bijective and $d < n$, then F has an even number of limit cycles.

5.4 Gray codes

A *Gray code* is an enumeration of the configurations in $\{0,1\}^n$ such that two successive configurations differ in one component, and such that the first and last ones also differ in one component. Gray codes are well known structures with many applications [9]. In our setting, a Gray code is a Hamiltonian function $F \in \mathcal{F}(n,2)$ such that, for all $x \in \{0,1\}^n$, x and $F(x)$ differ in one component. In this section, we prove the following.

Theorem 6. *If $\mathcal{F}(n,2,d)$ contains a Gray code then $d \geq \log n$.*

This provides a proof, for gray codes, of the following weaker form of Aracena-Zapata's conjecture: for any fixed d, if n is large enough, then $\mathcal{F}(n,2,d)$ has no Hamiltonian function.

For the proof we need the following definitions. Let $\delta(x,y)$ be the *Hamming distance* between x and y, that is, the number of $i \in [n]$ such that $x_i \neq y_i$. Given $F \in \mathcal{F}(n,2)$ we set

$$\delta(F) = \sum_{x \in \{0,1\}^n} \delta(x, F(x)).$$

So if F is a Gray code then $\delta(F) = 2^n$. Given $i \in [n]$, let us say that F_i is a *trivial component* of F if F_i is constant or $F_i(x) = x_i$ for all $x \in \{0,1\}^n$. For instance, if F is a bijection with an odd number of limit cycles, then F has no trivial component.

Lemma 10. *Let $0 < \epsilon \leq 1$ and $F \in \mathcal{F}(n,2)$ without trivial component. If $\delta(F) \leq n^{(1-\epsilon)}2^n$ then $G(F)$ has at least $\epsilon n \log n$ arcs.*

Proof. Suppose that $\delta(F) \leq n^{(1-\epsilon)}2^n$. Let N_i be the in-neighbors of i in $G(F)$ and $d_i = |N_i|$ its in-degree. Let X_i be the set of $x \in \{0,1\}^n$ with $F_i(x) \neq x_i$. Note that X_i is non-empty since otherwise F_i is a trivial component. Note also that

$$\sum_{i=1}^{n} |X_i| = \delta(F) \leq n^{(1-\epsilon)}2^n. \tag{5}$$

If $i \notin N_i$ then, for all $x \in \{0,1\}^n$, we have $F_i(x) = F_i(x + e_i)$ thus exactly one of $x, x + e_i$ belongs to X_i, and thus $|X_i| = 2^{n-1} \geq 2^{n-d_i}$ since $d_i \geq 1$ (because F_i is not constant). Suppose that $i \in N_i$, and let $x \in X_i$. For any y with $y_{N_i} = x_{N_i}$ we have $y_i = x_i \neq F_i(x) = F_i(y)$ so $y \in X_i$, and we deduce that $|X_i| \geq 2^{n-d_i}$. Thus in any case

$$d_i \geq n - \log |X_i|.$$

Hence the number e of arcs in $G(F)$ is

$$e = \sum_{i=1}^{n} d_i \geq n^2 - \sum_{i=1}^{n} \log |X_i| = n^2 - \log \Big(\prod_{i=1}^{n} |X_i| \Big).$$

Using the AM-GM inequality and then (5) we have

$$\prod_{i=1}^{n} |X_i| \leq \left(\frac{\sum_{i=1}^{n} |X_i|}{n} \right)^n \leq \left(\frac{n^{(1-\epsilon)} 2^n}{n} \right)^n = 2^{n^2 - \epsilon n \log n}.$$

We deduce that

$$e \geq n^2 - \log(2^{n^2 - \epsilon n \log n}) = \epsilon n \log n.$$

□

Proof (of Theorem 6). Let $F \in \mathcal{F}(n,2,d)$ be a Gray code. Since F has no trivial component, and since $\delta(F) = 2^n$, by Lemma 10 (applied with $\epsilon = 1$), $G(F)$ has at least $n \log n$ arcs, and thus the average in-degree is $\log n \leq d$. □

6 Complexity of recognizing bounded-degree dynamics

Fix d and q, and consider the following decision problem called BDD (bounded-degree dynamics): given $F \in \mathcal{F}(n,q)$ represented by Boolean circuits, is there some $F' \in \mathcal{F}(n,q,d)$ such that $\mathcal{D}(F)$ and $\mathcal{D}(F')$ are isomorphic?

Theorem 7. *The problem BDD is in PSPACE for every d, q, and co-NP-hard for any $q \geq 2$ and $d \geq 1$.*

Proof. For the upper bound, a naive algorithm solving BDD consists in guessing $F' \in \mathcal{F}(n,q,d)$ (whose size is polynomial in F thanks to the bounded-degree condition) and checking that $\mathcal{D}(F)$ and $\mathcal{D}(F')$ are isomorphic. Given that planar graph isomorphism is computable with a LOGSPACE Turing machine M [3] and that $\mathcal{D}(F)$ and $\mathcal{D}(F')$ are at most exponentially larger than the input (Boolean circuit for F), we can test isomorphism of $\mathcal{D}(F)$ and $\mathcal{D}(F')$ in PSPACE by simulating each reading step of the read-only input tape of M by an evaluation of circuit in polynomial time (testing $F(x) = y$ is the same as testing the presence of the corresponding arc in $\mathcal{D}(F)$). This gives an algorithm in NP with an oracle in PSPACE, *i.e.*, an algorithm in the complexity class PSPACE.

For the co-NP-hardness we reduce from UNSAT. Given a propositional formula ϕ on p variables $v_1, \ldots, v_p$, we construct $F \in \mathcal{F}(n,q)$ on $|V| = p + d$

automata, with $P = \{v_1, \dots, v_p\}$, $D = \{t_1, \dots, t_d\}$ and $V = P \cup D$. Let $Q = \{0, \dots, q-1\}$, and for $x \in Q^V$, consider the valuation $\theta(x_P)$ sending each 0 to false and other symbols to true. Set the local functions to be the identity $f_i(x) = x_i$ for every $i \in V \setminus \{t_d\}$, and:

$$f_{t_d}(x) = \begin{cases} x_{t_d} + 1 \mod q & \text{if } x_D = a^d \text{ and } \phi(\theta(x_P)), \\ x_{t_d} & \text{otherwise.} \end{cases}$$

If ϕ is unsatisfiable, then t_d depends only on D and F has degree d, hence it is a positive instance of BDD. Otherwise, F is not the identity, and it has:

- $(q^d - 1)q^p = q^n - q^{n-d}$ fixed points with $x_D \neq a^d$,
- at least one additional fixed point with $x_D = a^d$ and $\theta(x_P)$ satisfying ϕ.

Proposition 1 then implies that it is a negative instance of BDD. □

If we drop the isomorphism condition from the above problem, we get another one called BDIG (bounded-degree interaction graph): given $F \in \mathcal{F}(n, q)$ represented by Boolean circuits, is there some $F' \in \mathcal{F}(n, q, d)$ such that $\mathcal{D}(F) = \mathcal{D}(F')$? or, equivalently, is the degree of the interaction graph of F bounded by d?

Theorem 8. *The problem BDIG is co-NP-complete.*

Proof. The lower bound is given by the same reduction as in the proof of Theorem 7. For the upper bound, a simple co-NP algorithm consists in guessing an automaton $i \in V$, $d+1$ configurations $x^1, \dots, x^{d+1}$, and $d+1$ distinct automata $i_1, \dots, i_{d+1}$, then checking for each $j \in \{1, \dots, d+1\}$ that $f_i(x^j) \neq f_i(x^j + e_{i_j})$. For each j, it checks whether x^j witnesses the effective dependency of i on automaton i_j. It is possible to guess $d+1$ such witnesses if and only if the interaction graph of F has degree at least $d+1$. □

7 Acknowledgments

This work was supported by ECOS-ANID project C19E02 between France and Chile, ANR-18-CE40-0002 FANs, HORIZON-MSCA-2022-SE-01 101131549 ACANCOS, and STIC AmSud CAMA 22-STIC-02 (Campus France MEAE). The authors thank Anahí Gajardo, Diego Maldonado, and Christopher Thraves, who participated in elaborating some ideas for the presented results. Figure 1 is built with Ti*k*Z library OODGraph.

References

1. Florian Bridoux, Kévin Perrot, Aymeric Picard Marchetto, and Adrien Richard. Interaction graphs of isomorphic automata networks I: Complete digraph and minimum in-degree. *Journal of Computer and System Sciences*, 138:103458, 2023.
2. Arturo Antonio Zapata Cortés. Dinámicas hamiltonianas en redes booleanas. Master's thesis, Universidad de Concepción, 2022.

3. Samir Datta, Nutan Limaye, Prajakta Nimbhorkar, Thomas Thierauf, and Fabian Wagner. Planar Graph Isomorphism is in Log-Space. In Manindra Agrawal, Lance Fortnow, Thomas Thierauf, and Christopher Umans, editors, *Algebraic Methods in Computational Complexity*, volume 9421 of *Dagstuhl Seminar Proceedings (DagSemProc)*, pages 1–32, Dagstuhl, Germany, 2010. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.
4. Harold Fredricksen. A survey of full length nonlinear shift register cycle algorithms. *SIAM Review*, 24(2):195–221, 1982.
5. Maximilien Gadouleau. On the rank and periodic rank of finite dynamical systems. *Electronic journal of combinatorics.*, 25(3):P3, 2018.
6. Maximilien Gadouleau. On the influence of the interaction graph on a finite dynamical system. *Natural Computing*, 19(1):15–28, feb 2019.
7. Tony Grubman, Y Ahmet Şekercioğlu, and David R Wood. Partitioning de Bruijn graphs into fixed-length cycles for robot identification and tracking. *Discrete Applied Mathematics*, 213:101–113, 2016.
8. Rudolf Lidl and Harald Niederreiter. *Finite Fields.* Cambridge University Press, 1996.
9. Carla Savage. A survey of combinatorial gray codes. *SIAM review*, 39(4):605–629, 1997.