Expansive Automata Networks

Journées SDA2 2019

F. Bridoux, M. Gadouleau, *G. Theyssier*

Institut de mathématiques de Marseille
(CNRS, Université Aix-Marseille)

juin 2019

Automata Networks

$$F : Q^n \to Q^n$$

- Q finite alphabet
- $n \in \mathbb{N}$

Automata Networks

$$F : Q^n \to Q^n$$

- Q finite alphabet
- $n \in \mathbb{N}$

- dynamically: all orbits are ultimately periodic

Automata Networks

$$F : Q^n \to Q^n$$

- Q finite alphabet
- $n \in \mathbb{N}$

- dynamically: all orbits are ultimately periodic

- yes but Q^n has some structure!
- $x = (x_1, \dots, x_n)$

Dependency Graph

- given $F : Q^n \to Q^n$
- define digraph $G_F = (\{1, \cdots, n\}, E)$ by

$$(i, j) \in E \Leftrightarrow \begin{cases} \exists x, y : F(x)_i \neq F(y)_i \\ \text{with } x \text{ and } y \text{ differing only at coordinate } j \end{cases}$$

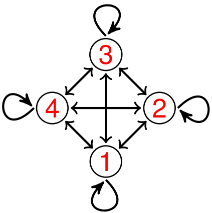
Dependency Graph

- given $F : Q^n \to Q^n$
- define digraph $G_F = (\{1, \cdots, n\}, E)$ by

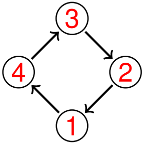
$$(i, j) \in E \Leftrightarrow \begin{cases} \exists x, y : F(x)_i \neq F(y)_i \\ \text{with } x \text{ and } y \text{ differing only at coordinate } j \end{cases}$$

- examples:

  - $F = 0 \cdots 0 \leftrightarrow 1 \cdots 1$
  - $G_F =$



  - $F(x)_k = x_{k+1 \bmod n}$
  - $G_F =$



Automata Networks Theory

Automata Networks Theory

Robert' Theorem

If G_F is acyclic then F is nilpotent (F^n is constant).

Feedback bound

$$\left|\{x : F(x) = x\}\right| \leq |Q|^{\nu(G_F)}$$

$\nu(G_F) =$ size of minimal feedback vertex set

Automata Networks Theory

Robert' Theorem

If G_F is acyclic then F is nilpotent (F^n is constant).

Feedback bound

$$\Big|\{x : F(x) = x\}\Big| \leq |Q|^{\nu(G_F)}$$

$\nu(G_F) =$ size of minimal feedback vertex set

- many refinements using signed graphs, e.g.:

Automata Networks Theory

Robert' Theorem

If G_F is acyclic then F is nilpotent (F^n is constant).

Feedback bound

$$\big|\{x : F(x) = x\}\big| \leq |Q|^{\nu(G_F)}$$

$\nu(G_F) =$ size of minimal feedback vertex set

- many refinements using signed graphs, e.g.:

Thomas' first rule

If G_F has no positive cycle then F has at most one fixed point.

Positive feedback bound

$\big|\{x : F(x) = x\}\big| \leq |Q|^{\nu^+(G_F)}$

Classical Expansiveness

- (X, d) compact metric space

Classical Expansiveness

- (X, d) compact metric space
- a dynamical system (F, X) is expansive if

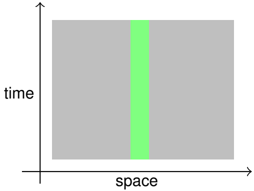
$$\exists\epsilon : x \neq y \Rightarrow \exists t, d(F^t(x), F^t(y)) > \epsilon$$

Classical Expansiveness

- (X, d) compact metric space
- a dynamical system (F, X) is expansive if

$$\exists \epsilon : x \neq y \Rightarrow \exists t, d(F^t(x), F^t(y)) > \epsilon$$

- a cellular automaton $F : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ is expansive if



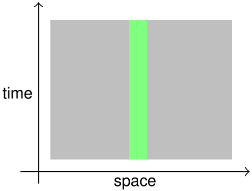
observing the trace of an orbit determines the whole orbit.

Classical Expansiveness

- (X, d) compact metric space
- a dynamical system (F, X) is expansive if

$$\exists \epsilon : x \neq y \Rightarrow \exists t, d(F^t(x), F^t(y)) > \epsilon$$

- a cellular automaton $F : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ is expansive if



observing the trace of an orbit determines the whole orbit.

- observability in automata networks

Expansive Automata Networks

Expansive Automata Networks

- F expansive if for all i

$$x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$$

Expansive Automata Networks

- F expansive if for all i

$$x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$$

- trace $\tau_i : x \mapsto (F(x)_i, F^2(x)_i, F^3(x)_i, \ldots)$
- F expansive $\Leftrightarrow \tau_i$ injective for all i

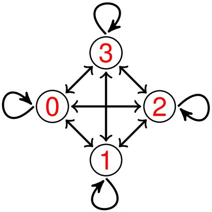
Expansive Automata Networks

- F expansive if for all i

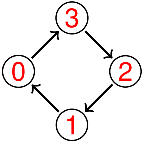
$$x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$$

- trace $\tau_i : x \mapsto (F(x)_i, F^2(x)_i, F^3(x)_i, \dots)$
- F expansive $\Leftrightarrow \tau_i$ injective for all i

- $F = 0 \cdots 0 \leftrightarrow 1 \cdots 1$



- $F(x)_k = x_{k+1 \bmod n}$



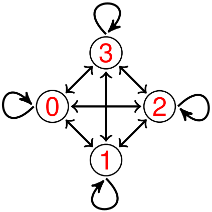
Expansive Automata Networks

- F expansive if for all i

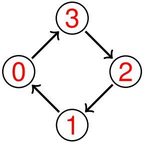
$$x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$$

- trace $\tau_i : x \mapsto (F(x)_i, F^2(x)_i, F^3(x)_i, \ldots)$
- F expansive $\Leftrightarrow$ τ_i injective for all i

- $F = 0 \cdots 0 \leftrightarrow 1 \cdots 1$



- $F(x)_k = x_{k+1 \bmod n}$



- variations on the definition

Expansion time

- $x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$
- but how large must be t?

Expansion time

- $x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$
- but how large must be t?
- $\tau_i^t : x \mapsto (F(x)_i, \ldots, F^t(x)_i)$
- **expansion time** of F:

$$T(F) = \min\{t : \tau_i^t \text{ injective for all } i\}$$

Expansion time

- $x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$
- but how large must be t?
- $\tau_i^t : x \mapsto (F(x)_i, \ldots, F^t(x)_i)$
- **expansion time** of F:

$$T(F) = \min\{t : \tau_i^t \text{ injective for all } i\}$$

Proposition

1. for any expansive F: $n \leq T(F) \leq |Q|^n$

Expansion time

- $x \neq y \Rightarrow \exists t > 0 : F^t(x)_i \neq F^t(y)_i$
- but how large must be t?
- $\tau_i^t : x \mapsto (F(x)_i, \ldots, F^t(x)_i)$
- **expansion time** of F:

$$T(F) = \min\{t : \tau_i^t \text{ injective for all } i\}$$

Proposition

1. for any expansive F: $n \leq T(F) \leq |Q|^n$
2. $(\forall n)$ there is F with $T(F) = |Q|^n - |Q| - 1$

- twisted lexicographic order:

$$00 \to 01 \to 02 \to 10 \to 11 \to 12 \to 20 \to 22 \to 21 \to 00$$

Linear networks

- $Q = \mathbb{F}_q$ finite field and Q^n vectorial space
- $F : Q^n \to Q^n$ can be a linear map

Linear networks

- $Q = \mathbb{F}_q$ finite field and Q^n vectorial space
- $F : Q^n \to Q^n$ can be a linear map

F linear and expansive $\Rightarrow$ expansion time is n.

Linear networks

- $Q = \mathbb{F}_q$ finite field and Q^n vectorial space
- $F : Q^n \to Q^n$ can be a linear map

F linear and expansive $\Rightarrow$ expansion time is n.

- Then τ_i^n is a linear bijective map:

$$\tau_i^n = \begin{pmatrix} M_{1,i} & \cdots & M_{n,i} \\ \vdots & \cdots & \vdots \\ M_{1,i}^n & \cdots & M_{n,i}^n \end{pmatrix}$$

  where $F^t = (M_{i,j}^t)$
- for F linear:

F expansive $\Leftrightarrow$ $det(\tau_i^n) \neq 0$ for all i

Graphs allowing expansiveness

- for which G is there F expansive with $G_F = G$?

$$\begin{tikzcd} 0 \arrow[loop left] \arrow[r, leftrightarrow] & 1 \arrow[r, leftrightarrow] & 2 \\ & 3 & \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r, leftrightarrow] & 1 \arrow[r, leftrightarrow] & 2 \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[loop left] \arrow[r, leftrightarrow] & 1 \arrow[r, leftrightarrow] & 2 \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r, leftrightarrow] & 1 \arrow[r, leftrightarrow] & 2 \arrow[r, leftrightarrow] & 3 \end{tikzcd}$$

Graphs allowing expansiveness

- necessary condition 1: G strongly connected

Graphs allowing expansiveness

- necessary condition 1: G strongly connected
- necessary condition 2: $|N^+(S)| \geq |S|$ for all $S \subseteq V$

Graphs allowing expansiveness

- necessary condition 1: G strongly connected
- necessary condition 2: $|N^+(S)| \geq |S|$ for all $S \subseteq V$

Hall's mariage theorem

condition 2 $\Leftrightarrow$ G partitioned into disjoint cycles.

Graphs allowing expansiveness

- necessary condition 1: G strongly connected
- necessary condition 2: $|N^+(S)| \geq |S|$ for all $S \subseteq V$

Hall's mariage theorem

condition 2 $\Leftrightarrow$ G partitioned into disjoint cycles.

- G is *admissible* if it verifies cond. 1 and 2

Theorem

There exists F expansive with $G_F = G \Leftrightarrow G$ admissible

Graphs allowing expansiveness

- necessary condition 1: G strongly connected
- necessary condition 2: $|N^+(S)| \geq |S|$ for all $S \subseteq V$

Hall's mariage theorem

condition 2 $\Leftrightarrow$ G partitioned into disjoint cycles.

- G is *admissible* if it verifies cond. 1 and 2

Theorem

There exists F expansive with $G_F = G \Leftrightarrow G$ admissible

- robust to slight variations in the definition of expansiveness

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = G$ is expansive.

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = G$ is expansive.

- F expansive $\Leftrightarrow det(\tau_i^n) \neq 0$ for all i

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = G$ is expansive.

- F expansive $\Leftrightarrow$ $det(\tau_i^n) \neq 0$ for all i
- view F as matrix $(X_{i,j})$ where $X_{i,j}$ are formal variables
- $X_{i,j} = 0 \Leftrightarrow (i,j) \in G$

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = G$ is expansive.

- F expansive $\Leftrightarrow$ $det(\tau_i^n) \neq 0$ for all i
- view F as matrix $(X_{i,j})$ where $X_{i,j}$ are formal variables
- $X_{i,j} = 0 \Leftrightarrow (i, j) \in G$
- then $det(\tau_i^n) \in \mathbb{F}_q[X_{i,j}]$

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = G$ is expansive.

- F expansive $\Leftrightarrow$ $det(\tau_i^n) \neq 0$ for all i
- view F as matrix $(X_{i,j})$ where $X_{i,j}$ are formal variables
- $X_{i,j} = 0 \Leftrightarrow (i,j) \in G$
- then $det(\tau_i^n) \in \mathbb{F}_q[X_{i,j}]$

Schwartz–Zippel lemma

$P \in \mathbb{F}_q[X_1, \ldots, X_k]$, non-zero, total degree d, then:

$$Pr(P(a_1, \ldots, a_k) = 0) \leq \frac{d}{|\mathbb{F}_q|}$$

for $a_1, \ldots, a_k$ chosen uniformly independently in $\mathbb{F}_q$.

Proof of the Theorem

- probabilistic proof, we actually show for any admissible G:

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = G$ is expansive.

- F expansive $\Leftrightarrow$ $det(\tau_i^n) \neq 0$ for all i
- view F as matrix $(X_{i,j})$ where $X_{i,j}$ are formal variables
- $X_{i,j} = 0 \Leftrightarrow (i,j) \in G$
- then $det(\tau_i^n) \in \mathbb{F}_q[X_{i,j}]$

Schwartz–Zippel lemma

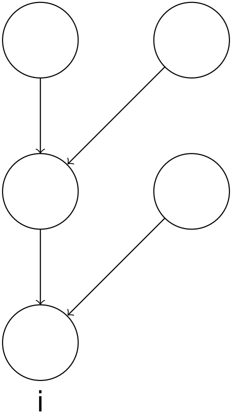
$P \in \mathbb{F}_q[X_1, \ldots, X_k]$, non-zero, total degree d, then:

$$Pr(P(a_1, \ldots, a_k) = 0) \leq \frac{d}{|\mathbb{F}_q|}$$

for $a_1, \ldots, a_k$ chosen uniformly independently in $\mathbb{F}_q$.

Proof of the Theorem

$$det(\tau_i^n) = \sum_{\sigma}(-1)^{s(\sigma)} \prod_{t=1}^{n} (\tau_i^n)_{\sigma(t),t}$$



Lower bounds on Q

- $E(Q, G)$: set of expansive F with alphabet Q and $G_F = G$

Lower bounds on Q

- $E(Q, G)$: set of expansive F with alphabet Q and $G_F = G$

Theorem

For any Q there is an admissible G such that $E(Q, G) = \emptyset$.

Lower bounds on Q

- $E(Q, G)$: set of expansive F with alphabet Q and $G_F = G$

Theorem

For any Q there is an admissible G such that $E(Q, G) = \emptyset$.

- $n \sim q^{q^{q^2}}$ where $q = |Q|$
- q^2 is sufficient for **linear** networks

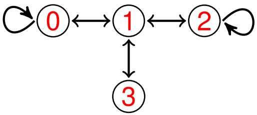
Lower bounds on Q

- $E(Q,G)$: set of expansive F with alphabet Q and $G_F = G$

Theorem

For any Q there is an admissible G such that $E(Q,G) = \emptyset$.

- $n \sim q^{q^{q^2}}$ where $q = |Q|$
- q^2 is sufficient for **linear** networks



$$q \equiv 2 \mod 4$$

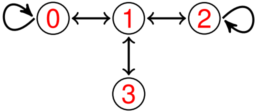
Lower bounds on Q

- $E(Q, G)$: set of expansive F with alphabet Q and $G_F = G$

Theorem

For any Q there is an admissible G such that $E(Q, G) = \emptyset$.

- $n \sim q^{q^{q^2}}$ where $q = |Q|$
- q^2 is sufficient for **linear** networks

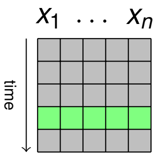


$q \equiv 2 \mod 4$

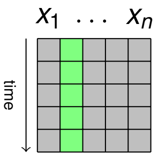
Open

Upper-bound on Q for all admissible graphs of fixed degree d?

Super-expansiveness

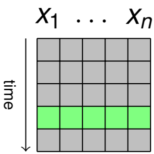


bijective

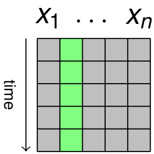


expansive in time *n*

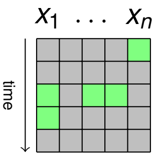
Super-expansiveness



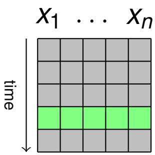
bijective



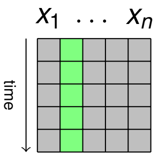
expansive in time n



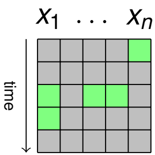
Super-expansiveness



bijective

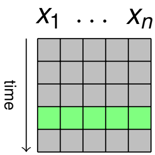


expansive in time n

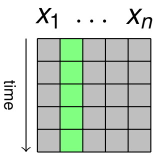


- $O = \big((i_1, t_1), \dots, (i_n, t_n)\big)$
- $\tau_O = x \mapsto \big(F^{t_1}(x)_{i_1}, \dots, F^{t_n}(x)_{i_n}\big)$

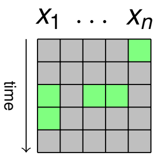
Super-expansiveness



bijective



expansive in time n



- $O = \big((i_1, t_1), \dots, (i_n, t_n)\big)$
- $\tau_O = x \mapsto \big(F^{t_1}(x)_{i_1}, \dots, F^{t_n}(x)_{i_n}\big)$

Definition

F super-expansive if τ_O injective for any O of length n.

Super-expansiveness

- F super-expansive $\Rightarrow$ G_F complete graph

Super-expansiveness

- F super-expansive $\Rightarrow G_F$ complete graph

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = K_n$ is super-expansive.

- same kind of proof

Super-expansiveness

- F super-expansive $\Rightarrow G_F$ complete graph

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = K_n$ is super-expansive.

- same kind of proof
- **Bonus!** a MDS code:

$$\{x_1 \cdots x_n F(x)_1 \cdots F(x)_n \cdots F^n(x)_1 \cdots F^n(x)_n : (x_i) \in Q^n\}$$

Super-expansiveness

- F super-expansive $\Rightarrow G_F$ complete graph

Theorem

For large $\mathbb{F}_q$ a random linear F with $G_F = K_n$ is super-expansive.

- same kind of proof
- **Bonus!** a MDS code:

$$\left\{x_1 \cdots x_n F(x)_1 \cdots F(x)_n \cdots F^n(x)_1 \cdots F^n(x)_n : (x_i) \in Q^n\right\}$$

- Singleton bound: $\#\text{words} \leq q^{\text{length}-\text{distance}+1}$
- In our case: $q^n \leq q^{n^2-(n^2-n+1)+1}$

Going further

- expansion frequency
- block-sequential update schedules
- link with other “topological” properties
- observability in general