Expansive Automata Networks

The Automata Factory 3

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

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

November 2020

Automata networks

- graph $G = (V, E)$
- alphabet $Q = \{0, \dots q-1\}$
- configurations $x \in Q^V$
- transition maps $f_v : Q^{N_v} \to Q$

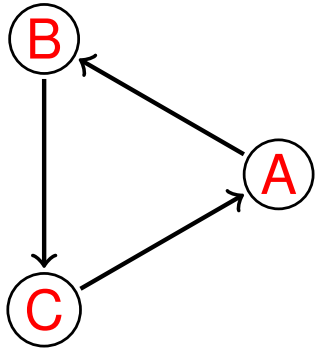
Automata networks

- graph $G = (V, E)$
- alphabet $Q = \{0, \dots q-1\}$
- configurations $x \in Q^V$
- transition maps $f_v : Q^{N_v} \to Q$
- global map : $F : Q^V \to Q^V$ with $F(x)_v = f_v(x)$

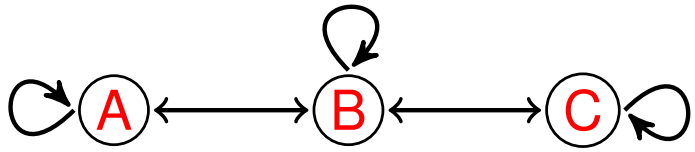
Automata networks

- graph $G = (V, E)$
- alphabet $Q = \{0, \dots q-1\}$
- configurations $x \in Q^V$
- transition maps $f_v : Q^{N_v} \to Q$
- global map : $F : Q^V \to Q^V$ with $F(x)_v = f_v(x)$

Example 1

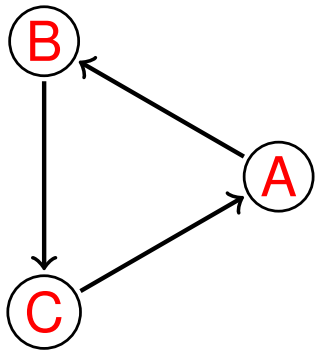


Example 2

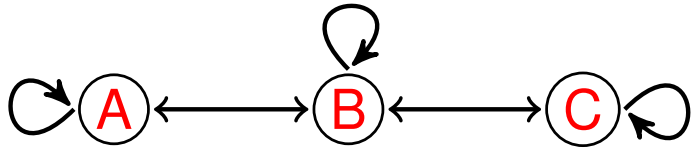


with $Q = \{0, 1\}$ and $f_v(x) = \sum_{i \in N_v} x_i \bmod 2$

Examples



	A	B	C
t=0	1	0	0
t=1	0	1	0
t=2	0	0	1
t=3	1	0	0



	A	B	C
t=0	1	0	0
t=1	1	1	0
t=2	0	0	1
t=3	0	1	1
t=4	1	0	0

Finite dynamical systems

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

Finite dynamical systems

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

- dynamically: all orbits are ultimately periodic

Finite dynamical systems

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

- dynamically: all orbits are ultimately periodic

- yes but Q^n has some structure!
- $x = (x_1, \ldots, x_n)$
- $(0, 0, \ldots, 0)$ is closer to $(1, 0, \ldots, 0)$ than $(1, \ldots, 1)$

Finite dynamical systems

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

- dynamically: all orbits are ultimately periodic

- yes but Q^n has some structure!
- $x = (x_1, \ldots, x_n)$
- $(0, 0, \ldots, 0)$ is closer to $(1, 0, \ldots, 0)$ than $(1, \ldots, 1)$

$\rightsquigarrow$ **a 'topological dynamics' point of view**

Classical Expansiveness

- (X, d) compact metric space

Classical Expansiveness

- (X, d) compact metric space
- a dynamical system (F, X) is expansive if $\exists \epsilon > 0$

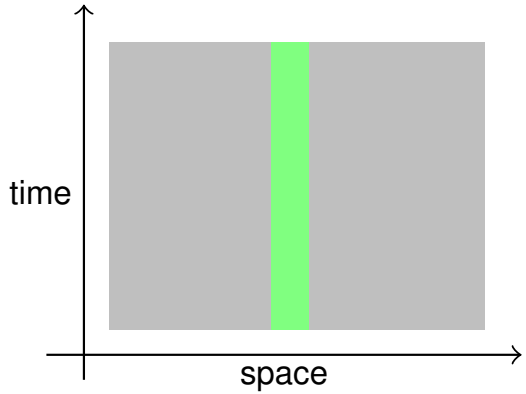
$$\forall x, y \in X : x \neq y \Rightarrow \exists t,\ d(F^t(x), F^t(y)) \geq \epsilon$$

Classical Expansiveness

- (X, d) compact metric space
- a dynamical system (F, X) is expansive if $\exists \epsilon > 0$

$$\forall x, y \in X : x \neq y \Rightarrow \exists t,\ d(F^t(x), F^t(y)) \geq \epsilon$$

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



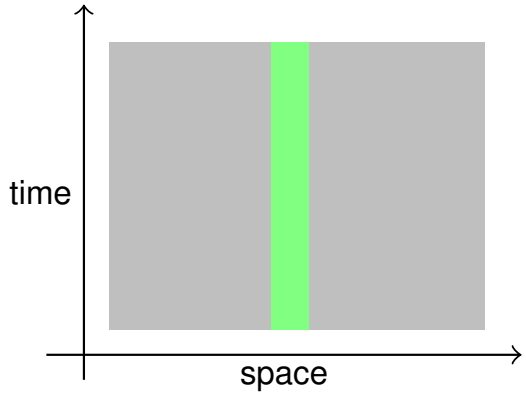
partial observation of an orbit determines the whole orbit

Classical Expansiveness

- (X, d) compact metric space
- a dynamical system (F, X) is expansive if $\exists \epsilon > 0$

$$\forall x, y \in X : x \neq y \Rightarrow \exists t,\ d(F^t(x), F^t(y)) \geq \epsilon$$

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



partial observation of an orbit determines the whole orbit

- $\rightsquigarrow$ observability in control theory

Expansive Automata Networks

Expansive Automata Networks

- F expansive if for all v

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

Expansive Automata Networks

- F expansive if for all v

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

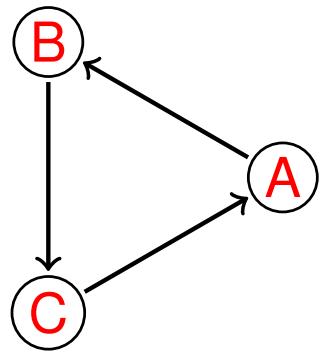
- **trace** $\tau_v : x \mapsto (F(x)_v, F^2(x)_v, F^3(x)_v, \ldots)$
- F **expansive** $\Leftrightarrow$ τ_v **injective for all** v

Expansive Automata Networks

- F expansive if for all v

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

- **trace** $\tau_v : x \mapsto (F(x)_v, F^2(x)_v, F^3(x)_v, \ldots)$
- F **expansive** $\Leftrightarrow$ τ_v **injective for all** v
- expansive $\Rightarrow$ bijective
- example:



Expansion time

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

Expansion time

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

- $\tau_v^t : x \mapsto (F(x)_v, \ldots, F^t(x)_v)$
- **expansion time** of F:

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

Expansion time

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

- $\tau_v^t : x \mapsto (F(x)_v, \ldots, F^t(x)_v)$
- **expansion time** of F:

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

Proposition

(n = number of nodes)

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

Expansion time

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

- $\tau_v^t : x \mapsto (F(x)_v, \ldots, F^t(x)_v)$
- **expansion time** of F:

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

Proposition

(n = number of nodes)

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

Exponential expansion time

Lexicographic order

1. 0 0 0
2. 0 0 1
3. 0 1 0
4. 0 1 1
5. 1 0 0
6. 1 0 1
7. 1 1 0
8. 1 1 1

Exponential expansion time

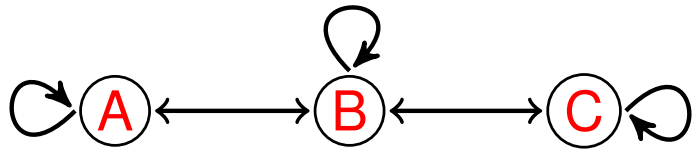
	Lexicographic order	**Twisted** lexicographic order
1	0 0 0	0 0 0
2	0 0 1	0 0 1
3	0 1 0	0 1 0
4	0 1 1	0 1 1
5	1 0 0	1 1 0
6	1 0 1	1 1 1
7	1 1 0	1 0 1
8	1 1 1	1 0 0

Exponential expansion time

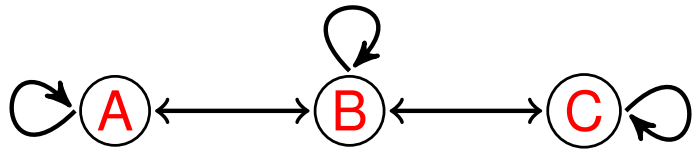
	Lexicographic order	**Twisted** lexicographic order
1	0 0 0	0 0 0
2	0 0 1	0 0 1
3	0 1 0	0 1 0
4	0 1 1	0 1 1
5	1 0 0	1 1 0
6	1 0 1	1 1 1
7	1 1 0	1 0 1
8	1 1 1	1 0 0

- **twisted** version is expansive
- T(**twisted**) = 5

Back to example 1

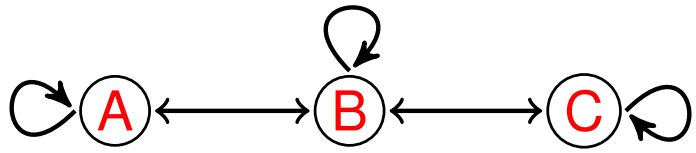


Back to example 1



- bijective but **not** expansive
  - $F(101) = 101$
  - $F(000) = 000$
  - τ_B not injective

Back to example 1



- bijective but **not** expansive
  - $F(101) = 101$
  - $F(000) = 000$
  - τ_B not injective

- because of the update rules or because of the graph?
- something special for this kind of rules?

Linear networks

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

Linear networks

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

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

- Then τ_v^n is a linear bijective map:

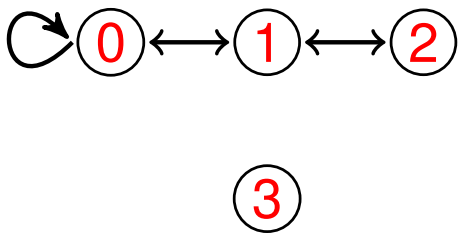
$$\tau_v^n = \begin{pmatrix} M_{1,v} & \cdots & M_{n,v} \\ \vdots & \cdots & \vdots \\ M_{1,v}^n & \cdots & M_{n,v}^n \end{pmatrix}$$

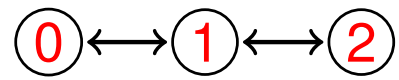
  where $F^t = (M_{i,j}^t)$
- for F linear:

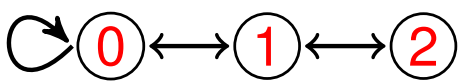
F expansive $\Leftrightarrow$ $det(\tau_v^n) \neq 0$ for all v

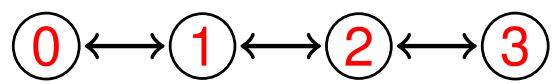
Graphs allowing expansiveness

- take any graph G
- can we define local rules f_v s.t. F is expansive?









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

G admissible **IFF** exists F expansive defined on G

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

G admissible **IFF** exists F expansive defined on G

- 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 on 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 on G is expansive.

- F expansive $\Leftrightarrow$ $det(\tau_v^n) \neq 0$ for all v

Proof of the Theorem

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

Theorem

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

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

Proof of the Theorem

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

Theorem

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

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

Proof of the Theorem

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

Theorem

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

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

Schwartz–Zippel lemma

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

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

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

Proof of the Theorem

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

Theorem

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

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

Schwartz–Zippel lemma

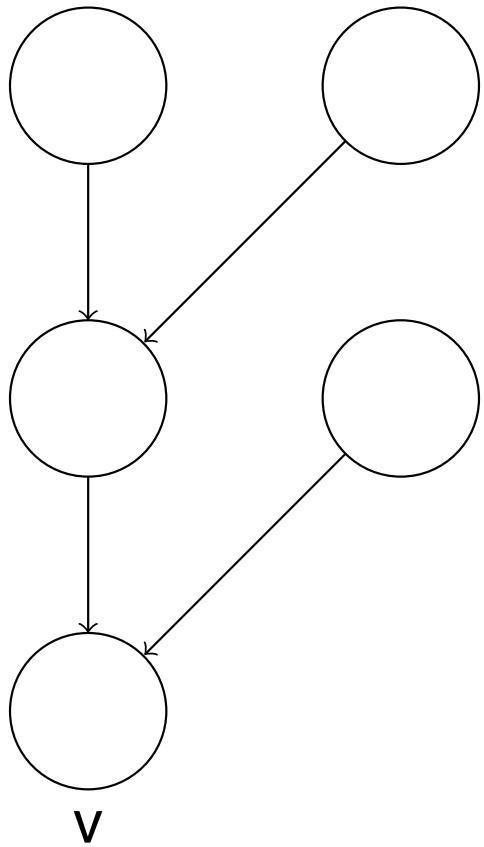
$P \in \mathbb{F}_q[X_1, \ldots, X_k]$, non-zero, total degree d, then:

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

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

Proof of the Theorem

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



Deciding expansiveness

- for linear networks, enough to compute a determinant
- general case?

Deciding expansiveness

- for linear networks, enough to compute a determinant
- general case?

- Decision problem **EXPAN**
  - *input:* automata network F (given via Boolean circuits)
  - *question:* is F expansive?

Deciding expansiveness

- for linear networks, enough to compute a determinant
- general case?

- Decision problem **EXPAN**
  - *input:* automata network F (given via Boolean circuits)
  - *question:* is F expansive?

Theorem

EXPAN is PSPACE-complete

Deciding expansiveness

- for linear networks, enough to compute a determinant
- general case?

- Decision problem **EXPAN**
  - *input:* automata network F (given via Boolean circuits)
  - *question:* is F expansive?

Theorem

EXPAN is PSPACE-complete

Open

Is (positive) expansivity decidable on cellular automata?

PSPACE-hardness ingredients

- reduction from QBF (Quantified Boolean Formula):
  $\Psi = \forall x_1 \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$

PSPACE-hardness ingredients

- reduction from QBF (Quantified Boolean Formula):
  $\Psi = \forall x_1 \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$

- brute force algorithm: nested loops
  - loop L_1 on x_1 (loop L_2 on x_2 (loop L_3 on x_3)))

PSPACE-hardness ingredients

- reduction from QBF (Quantified Boolean Formula):
  $\Psi = \forall x_1 \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$

- brute force algorithm: nested loops
  - loop L_1 on x_1 (loop L_2 on x_2 (loop L_3 on x_3)))
  - L_1: Ψ true if $\Psi(x_1) = \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$ true twice

PSPACE-hardness ingredients

- reduction from QBF (Quantified Boolean Formula):
  $\Psi = \forall x_1 \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$

- brute force algorithm: nested loops
  - loop L_1 on x_1 (loop L_2 on x_2 (loop L_3 on x_3)))
  - L_1: Ψ true if $\Psi(x_1) = \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$ true twice
  - L_2: $\Psi(x_1)$ true if $\Psi(x_1, x_2)$ true at least once

PSPACE-hardness ingredients

- reduction from QBF (Quantified Boolean Formula):
  $\Psi = \forall x_1 \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$

- brute force algorithm: nested loops
  - loop L_1 on x_1 (loop L_2 on x_2 (loop L_3 on x_3)))
  - L_1: Ψ true if $\Psi(x_1) = \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$ true twice
  - L_2: $\Psi(x_1)$ true if $\Psi(x_1, x_2)$ true at least once
  - L_3: $\Psi(x_1, x_3)$ true if $\phi(x_1, x_2, x_3)$ true twice

PSPACE-hardness ingredients

- reduction from QBF (Quantified Boolean Formula):
  $\Psi = \forall x_1 \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$

- brute force algorithm: nested loops
  - loop L_1 on x_1 (loop L_2 on x_2 (loop L_3 on x_3)))
  - L_1: Ψ true if $\Psi(x_1) = \exists x_2 \forall x_3 \phi(x_1, x_2, x_3)$ true twice
  - L_2: $\Psi(x_1)$ true if $\Psi(x_1, x_2)$ true at least once
  - L_3: $\Psi(x_1, x_3)$ true if $\phi(x_1, x_2, x_3)$ true twice

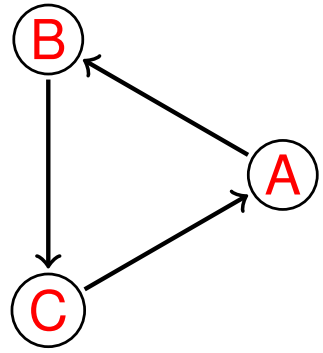
- all done by enumerating and counting
- **expansive counter** $\approx$ twisted lexicographic order

PSPACE-hardness construction

- layered construction

TEST
counter 1
counter 2
counter 3
x_1
x_2
x_3
instruction counter

TEST layer

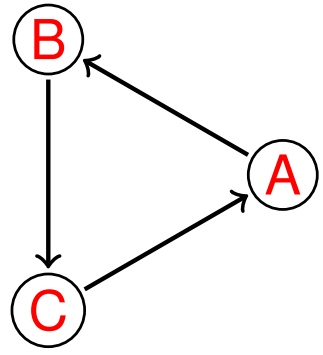


PSPACE-hardness construction

- layered construction

TEST
counter 1
counter 2
counter 3
x_1
x_2
x_3
instruction counter

TEST layer



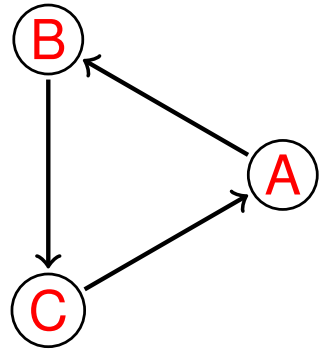
- bottom (blue part) always expansive
- construction expansive **IFF** test layer rotated at each cycle

PSPACE-hardness construction

- layered construction

TEST
counter 1
counter 2
counter 3
x_1
x_2
x_3
instruction counter

TEST layer



- bottom (blue part) always expansive
- construction expansive **IFF** test layer rotated at each cycle
- counter check trick: bad initialization $\Rightarrow$ rotate test layer
- Ψ true: rotate test layer
- Ψ false: do not rotate

Lower bounds on Q

- $E(Q, G)$: set of expansive F on graph G with alphabet Q

Lower bounds on Q

- $E(Q, G)$: set of expansive F on graph G with alphabet Q

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 on graph G with alphabet Q

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

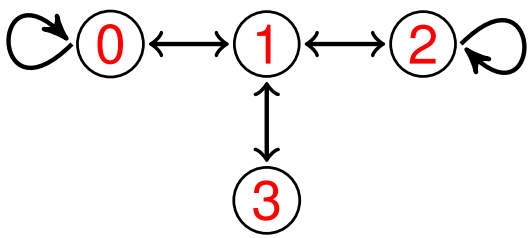
Lower bounds on Q

- $E(Q, G)$: set of expansive F on graph G with alphabet Q

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



$q \equiv 2 \mod 4$

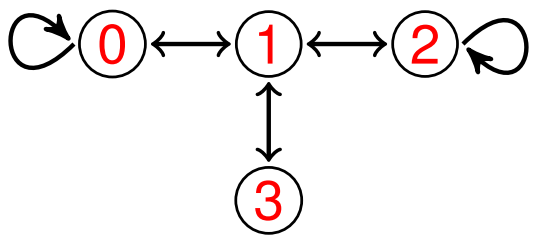
Lower bounds on Q

- $E(Q, G)$: set of expansive F on graph G with alphabet Q

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

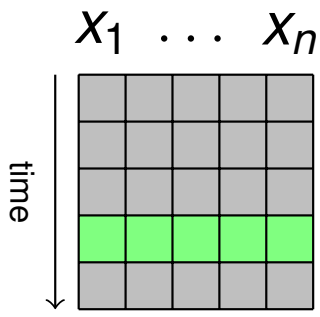


$q \equiv 2 \mod 4$

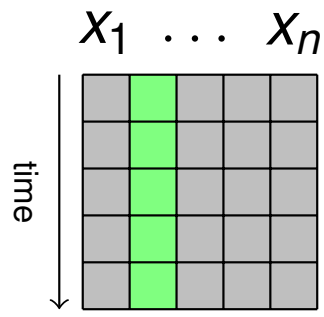
Open

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

Super-expansiveness

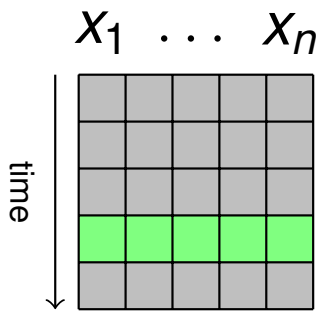


bijective

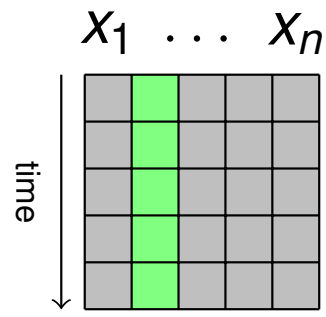


expansive in time n

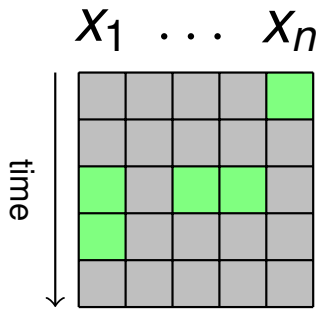
Super-expansiveness



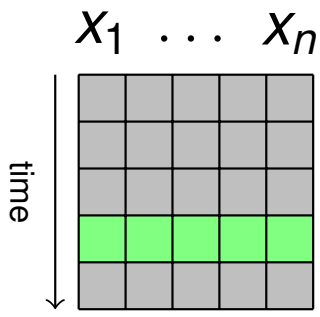
bijective



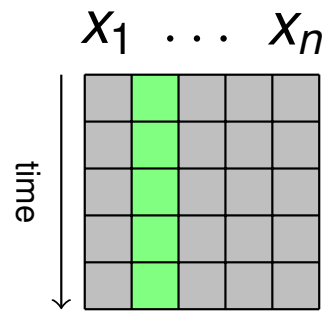
expansive in time n



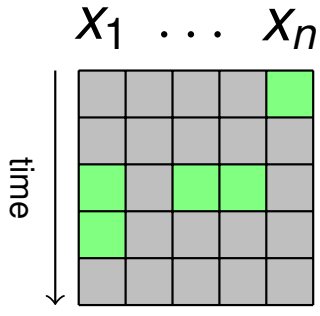
Super-expansiveness



bijective

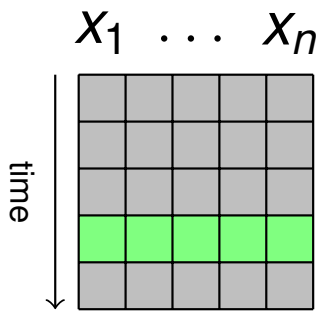


expansive in time n

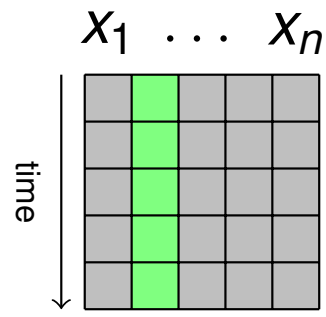


- $O = \big((v_1, t_1), \ldots, (v_n, t_n)\big)$
- $\tau_O = x \mapsto \big(F^{t_1}(x)_{v_1}, \ldots, F^{t_n}(x)_{v_n}\big)$

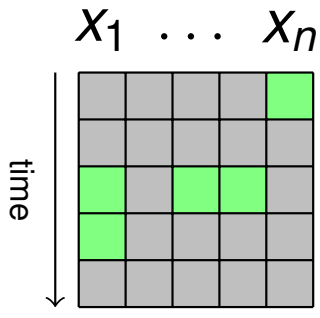
Super-expansiveness



bijective



expansive in time n



- $O = ((v_1, t_1), \ldots, (v_n, t_n))$
- $\tau_O = x \mapsto \left(F^{t_1}(x)_{v_1}, \ldots, F^{t_n}(x)_{v_n}\right)$

Definition

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

Super-expansiveness

- F super-expansive on $G \Rightarrow$ G complete graph

Super-expansiveness

- F super-expansive on $G \Rightarrow G$ complete graph

Theorem

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

- same kind of proof

Super-expansiveness

- F super-expansive on $G \Rightarrow G$ complete graph

Theorem

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

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

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

Super-expansiveness

- F super-expansive on $G \Rightarrow G$ complete graph

Theorem

For large $\mathbb{F}_q$ a random linear F on $G = K_n$ 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

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