Combinatorics of Discrete Dynamical Systems

Yinfeng Zhu
Shanghai Jiao Tong University

Joint with Yaokun Wu and Zeying Xu

International Workshop on Algebraic Combinatorics at AHU
October 31, 2016

Higher order inhomogenous DDS

Let t be a positive integer. Let S be a set and let $\mathcal{F}$ be a collection of t-variable maps from S^t to S. The pair $(S, \mathcal{F})$ is called an order-t discrete dynamical system (t-DDS).

- initial states: $x = (x_1, x_2, \ldots, x_t) \in S^t$;
- dynamical mechanism: $F = (f_1, f_2, \ldots) \in \mathcal{F}^{\mathbb{N}}$;
- a trajectory determined by (x, F): $\mathbb{X} = (x_1, x_2, \ldots) \in S^{\mathbb{N}}$, where

$$x_{i+t} = f_i(x_i, x_{i+1}, \ldots, x_{i+t-1}), \forall i \in \mathbb{N}\,.$$

Higher order inhomogenous DDS

Let t be a positive integer. Let S be a set and let $\mathcal{F}$ be a collection of t-variable maps from S^t to S. The pair $(S, \mathcal{F})$ is called an order-t discrete dynamical system (t-DDS).

- initial states: $x = (x_1, x_2, \ldots, x_t) \in S^t$;
- dynamical mechanism: $F = (f_1, f_2, \ldots) \in \mathcal{F}^{\mathbb{N}}$;
- a trajectory determined by (x, F): $\mathbb{X} = (x_1, x_2, \ldots) \in S^{\mathbb{N}}$, where

$$x_{i+t} = f_i(x_i, x_{i+1}, \ldots, x_{i+t-1}), \forall i \in \mathbb{N}.$$

The phase space of $(S, \mathcal{F})$ is an arc-labelled digraph with

- vertex set S^t;
- arc set $\{(x_1, \ldots, x_t) \xrightarrow{f} (x_2, \ldots, x_t, f(x_1, \ldots, x_t)) : x_i \in S, f \in \mathcal{F}\}$,

and will be denoted by $\mathcal{PS}_{\mathcal{F}}$. One-sided infinite walks in the phase space are just all trajectories in $(S, \mathcal{F})$.

Morkov operator

Let $t \in \mathbb{N}$ and K be a finite set. Write $\mathrm{Set}_K := 2^K \setminus \{\emptyset\}$. Let f be a map from K^t to Set_K. It can be graphically represented by its De Bruijn form Γ_f, a digraph with vertex set K^t and arc set

$$\{(x_1, \ldots, x_t) \to (x_2, \ldots, x_{t+1}) : x_{t+1} \in f(x_1, \ldots, x_t)\}.$$

Morkov operator

Let $t \in \mathbb{N}$ and K be a finite set. Write $\mathrm{Set}_K := 2^K \setminus \{\emptyset\}$. Let f be a map from K^t to Set_K. It can be graphically represented by its De Bruijn form Γ_f, a digraph with vertex set K^t and arc set

$$\{(x_1, \dots, x_t) \to (x_2, \dots, x_{t+1}) : x_{t+1} \in f(x_1, \dots, x_t)\}.$$

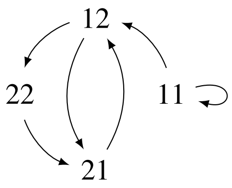
The map f induces a map M_f from Set_K^t to Set_K, called the Morkov operator associated to f, such that

$$\mathrm{M}_f(A_1, \dots, A_t) = \bigcup_{x \in A_1 \times \cdots \times A_t} f(x).$$

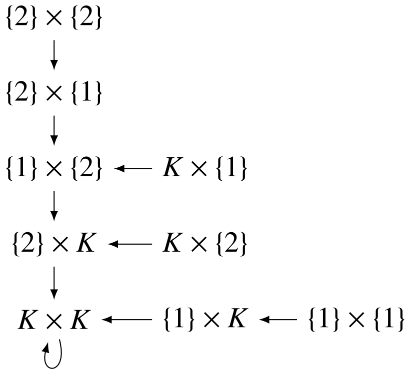
Let $\mathcal{F}$ be a finite collection of maps from K^t to Set_K. We define $\mathrm{M}_{\mathcal{F}}$ to be the multi-set $\{\mathrm{M}_f : f \in \mathcal{F}\}$.

Example

$t = 2, K = \{1, 2\}$



Γ_f



$\mathcal{PS}_{\mathrm{M}_f}$

Figure: The De Bruijn form Γ_f and the phase space $\mathcal{PS}_{\mathrm{M}_f}$.

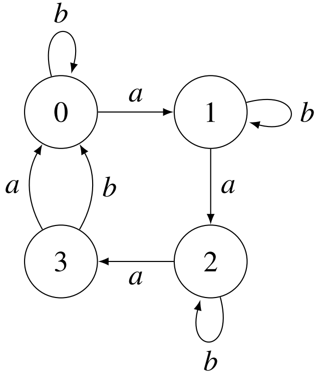
(t, r, k)-EBDDS

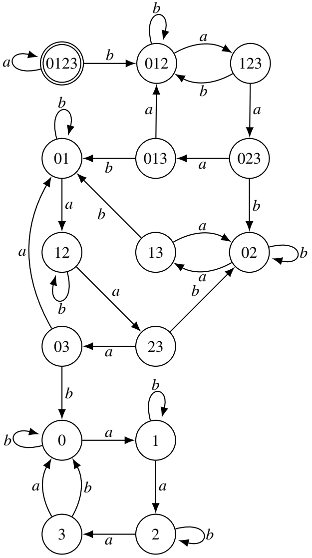
Let $t, r, k \in \mathbb{N}$. Let K be a set of size k and let $\mathcal{F}$ be a collection of r maps from K^t to Set_K. The pair $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$ is called a (t, r, k)-essential Boolean-linear discrete dynamincal systems or, simply, a (t, r, k)-EBDDS.

Convention:

- In the case that $\mathcal{F} = \{f\}$, we write $(\mathrm{Set}_K, \mathrm{M}_f)$ for $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$.
- For $a = (a_1, \ldots, a_t) \in K^t$, we write $\{a\}$ for $\{a_1\} \times \cdots \times \{a_t\}$.

Černý automata as a $(1, 2, k)$-EBDDS





Černý Conjecture

Let $r, k \in \mathbb{N}$. Let K be a set of size k and let $\mathcal{F}$ be a set of r maps from K to Set_K.

If every element from $\mathcal{F}$ is indeed a map from K to $\binom{K}{1}$ and there exists a walk from K to a singleton set in $\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}$, we call the $(1, r, k)$-EBDDS $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$ a synchronizing automaton.

Černý Conjecture

Let $r, k \in \mathbb{N}$. Let K be a set of size k and let $\mathcal{F}$ be a set of r maps from K to Set_K.

If every element from $\mathcal{F}$ is indeed a map from K to $\binom{K}{1}$ and there exists a walk from K to a singleton set in $\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}$, we call the $(1, r, k)$-EBDDS $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$ a synchronizing automaton.

Conjecture (Černý, 1964)

Let $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$ be a synchronizing $(1, r, k)$-EBDDS. Then there exists a walk W from K to a singleton set in $\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}$ with length at most $(k-1)^2$.

Primitive exponent

A (t,r,k)-EBDDS $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$ is primitive if every long enough walk in $\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}$ ends at K^t.

For a primitive (t,r,k)-EBDDS $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$, the primitive exponent is the minimum non-negative integer T such that every length-T walk in $\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}$ ends at K^t, which we denote by $\mathrm{g}(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$.

We use $\gamma(t,r,k)$ to denote the maximum number in the set

$$\{\,\mathrm{g}(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}}) : \ (\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}}) \text{ is a primitive } (t,r,k)\text{-EBDDS}\}.$$

Maximum primitive exponents of $(1, r, k)$-EBDDS

Theorem (Wielandt, 1959)

$$\gamma(1,1,k) = \begin{cases} (k-1)^2+1, & \textit{if } k \geq 2; \\ (k-1)^2 = 0, & \textit{if } k = 1. \end{cases}$$

Maximum primitive exponents of $(1, r, k)$-EBDDS

Theorem (Wielandt, 1959)

$$\gamma(1,1,k) = \begin{cases} (k-1)^2+1, & \textit{if } k \geq 2; \\ (k-1)^2 = 0, & \textit{if } k = 1. \end{cases}$$

Theorem (Cohen, Sellers, 1982)

$$\gamma(1, 2^k - 2, k) = 2^k - 2,$$

Maximum primitive exponents of $(1, r, k)$-EBDDS

Theorem (Wielandt, 1959)

$$\gamma(1,1,k) = \begin{cases} (k-1)^2+1, & \textit{if } k \geq 2; \\ (k-1)^2 = 0, & \textit{if } k = 1. \end{cases}$$

Let $r(k)$ be minimum positive integer r such that

$$\gamma(1,r,k) = 2^k - 2.$$

Theorem (Cohen, Sellers, 1982)

$$\gamma(1, 2^k-2, k) = 2^k - 2,$$

Maximum primitive exponents of $(1, r, k)$-EBDDS

Theorem (Wielandt, 1959)

$$\gamma(1,1,k) = \begin{cases} (k-1)^2+1, & \textit{if } k \geq 2; \\ (k-1)^2 = 0, & \textit{if } k = 1. \end{cases}$$

Let $r(k)$ be minimum positive integer r such that

$$\gamma(1,r,k) = 2^k - 2.$$

Theorem (Cohen, Sellers, 1982)

$$\gamma(1, 2^k-2, k) = 2^k - 2,$$

namely,

$$r(k) \leq 2^k - 2.$$

Maximum primitive exponents of $(1, r, k)$-EBDDS, cont'd

Theorem (Wu, Z., 2015)

$$\gamma(1, k, k) = 2^k - 2,$$

or, equivalently,

$$r(k) \leq k.$$

Note that

$$\gamma(1, 1, k) \leq \gamma(1, 2, k) \leq \cdots \\ \leq \gamma(1, r(k) - 1, k) < \gamma(1, r(k), k) = \gamma(1, r(k) + 1, k) = \cdots = 2^k - 2.$$

Question

Does it hold that $\gamma(1, i, k) < \gamma(1, i + 1, k)$ for all $i \in [1, r(k) - 1]$?

In the spirit of Černý

Conjecture (Wu, Xu, Z., 2016)

Let $(\mathrm{Set}_K, \mathrm{M}_{\mathcal{F}})$ *be a primitive* $(1, r, k)$*-EBDDS. For any* $A, B \in \mathrm{Set}_K$*, it holds*

$$\mathrm{DIST}_{\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}}(A, B) \leq |B|k^r$$

as long as A *can reach* B *in* $\mathcal{PS}_{\mathrm{M}_{\mathcal{F}}}$*.*

Remark

If this conjecture is correct, then for every $k \geq 2$ *we can obtain*

$$r(k) \geq \lceil \frac{\log_2(2^k - 2)}{\log_2 k} \rceil - 1.$$

Maximum primitive exponents of $(t, 1, k)$-EBDDS

- $\gamma(2, 1, 1) = 1$.
- $\gamma(2, 1, 2) = 7$.
- $\gamma(2, 1, 3) = 23$.

Theorem (Wu, Xu, Z., 2016+)

For $k \geq 4$,

$$\gamma(2, 1, k) \geq (2k - 1)^2 + 1. \quad (1)$$

Maximum primitive exponents of $(t, 1, k)$-EBDDS

- $\gamma(2,1,1) = 1$.
- $\gamma(2,1,2) = 7$.
- $\gamma(2,1,3) = 23$.

Theorem (Wu, Xu, Z., 2016+)

For $k \geq 4$,

$$\gamma(2,1,k) \geq (2k-1)^2 + 1. \tag{1}$$

Conjecture (Wu, Xu, Z., 2016+)

Equality holds in (1) *for all $k \geq 4$.*

Maximum primitive exponents of $(t, 1, k)$-EBDDS

- $\gamma(2, 1, 1) = 1$.
- $\gamma(2, 1, 2) = 7$.
- $\gamma(2, 1, 3) = 23$.

Theorem (Wu, Xu, Z., 2016+)

For $k \geq 4$*,*

$$\gamma(2, 1, k) \geq (2k - 1)^2 + 1. \tag{1}$$

Conjecture (Wu, Xu, Z., 2016+)

Equality holds in (1) *for all* $k \geq 4$*.*

Theorem (Chen, Wu, 2016+)

$$k^t \leq \gamma(t, 1, k) \leq t(k - 1)(k^t - 1) + 1.$$

Strong connectivity of $(t, 1, k)$-EBDDS

Let $(\mathrm{Set}_K, \mathrm{M}_f)$ be a $(t, 1, k)$-EBDDS.

For $a, b \in K^t$, we define $\mathcal{RI}_f(a, b)$ to be the set

$$\{i \geq 0 : \ b \in \mathrm{M}_f^i(\{a\})\}$$

and call it the set of reachable indices of f from a to b.

We call $(\mathrm{Set}_K, \mathrm{M}_f)$ strongly connected if $\mathcal{RI}_f(a, b) \neq \emptyset$ for all $a, b \in K^t$.

Diameter of $(t, 1, k)$-EBDDS

Let $(\mathrm{Set}_K, \mathrm{M}_f)$ be a strongly connected $(t, 1, k)$-EBDDS.
For all $a, b \in K^t$, we define the distance from a to b:

$$\mathrm{DIST}_f(a, b) = \min\left\{i : \ i \in \mathcal{RI}_f(a, b)\right\}.$$

The diameter of $(\mathrm{Set}_K, \mathrm{M}_f)$:

$$\mathrm{DIA}(f) = \max\left\{\mathrm{DIST}_f(a, b) : \ a, b \in K^t\right\}.$$

Diameter of $(t, 1, k)$-EBDDS

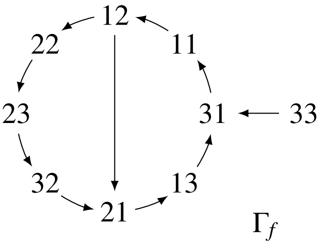
Let $(\mathrm{Set}_K, \mathrm{M}_f)$ be a strongly connected $(t, 1, k)$-EBDDS.
For all $a, b \in K^t$, we define the distance from a to b:

$$\mathrm{DIST}_f(a, b) = \min \left\{ i : \ i \in \mathcal{RI}_f(a, b) \right\}.$$

The diameter of $(\mathrm{Set}_K, \mathrm{M}_f)$:

$$\mathrm{DIA}(f) = \max \left\{ \mathrm{DIST}_f(a, b) : \ a, b \in K^t \right\}.$$

Note that $\mathrm{DIA}(f)$ may be larger than k^t when $t \geq 2$.



$$\mathrm{DIA}(f) = \mathrm{DIST}_f((2, 2), (3, 3)) = 15 > 3^2.$$

$$\mathbb{X} = (\{2\}, \{2\}, \{3\}, \{2\}, \{1\}, \{3\}, \{1\}, \{1\}, \{2\}, \{1, 2\}, \{3\}, \{1, 2\}, \{1\}, \{2, 3\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\} \cdots)$$

Maximum diameter of $(t, 1, k)$-EBDDS

- $\mathrm{D}_{t,k} :=$
  $\max\left\{\mathrm{DIA}(f) : (\mathrm{Set}_K, \mathrm{M}_f) \text{ is a strongly connected } (t,1,k)\text{-EBDDS}\right\}.$

Maximum diameter of $(t, 1, k)$-EBDDS

- $\mathrm{D}_{t,k} :=$
  $\max\left\{\mathrm{DIA}(f) : (\mathrm{Set}_K, \mathrm{M}_f)\right.$ is a strongly connected $(t, 1, k)$-EBDDS$\left.\right\}$.

- $\mathrm{D}_{2,2} = 4$ and $\mathrm{D}_{2,3} = 15$.

Theorem (Wu, Xu, Z., 2016+)

For $k \geq 5$,

$$\mathrm{D}_{2,k} \geq \begin{cases} 2k^2, & \text{if } k \text{ is odd,} \\ 2k^2 - k + 1, & \text{if } k \text{ is even.} \end{cases}$$

Conjecture (Wu, Xu, Z., 2016+)

$$\lim_{k\to\infty} \frac{\mathrm{D}_{2,k}}{k^2} = 2.$$

Cyclic classes

Let $(\mathrm{Set}_K, \mathrm{M}_f)$ be a strongly connected $(t, 1, k)$-EBDDS. We say $a, b \in K^t$ are equivalent in the relation $\sim_{\mathrm{M}_f}$ if there exists $N > 0$ such that

$$\mathrm{M}_f^N(\{a\}) = \mathrm{M}_f^N(\{b\}).$$

Let $C_f := K^t / \sim_{\mathrm{M}_f}$. Each equivalent class of $\sim_{\mathrm{M}_f}$ is called a cyclic class of $(\mathrm{Set}_K, \mathrm{M}_f)$. We define the period of $(\mathrm{Set}_K, \mathrm{M}_f)$ to be the number of equivalent classes and denote it by $\mathrm{per}(f)$.

Cyclic classes, Cont'd

Theorem (Wu, Xu, Z., 2016+)

Let $(\mathrm{Set}_K, \mathrm{M}_f)$ *be a strongly connected* $(t, 1, k)$*-EBDDS. Then the following hold:*

(i) $\mathrm{per}(f) = \gcd(\mathcal{RI}_f(a, a))$ *for all* $a \in K^t$.

(ii) *Let* $\overline{\mathrm{M}_f} : C_f \to C_f$ *such that*

$$\overline{\mathrm{M}_f}([a]) = [b],$$

where $b \in \mathrm{M}_f(\{a\})$ *and* $a, b \in K^t$. *Then the transformation semigroup generated by* $\overline{\mathrm{M}_f}$ *is the cyclic group* $\mathbb{Z}_{\mathrm{per}(f)}$.

Cyclic classes, Cont'd

Theorem (Wu, Xu, Z., 2016+)

Let $(\mathrm{Set}_K, \mathrm{M}_f)$ *be a strongly connected* $(t, 1, k)$*-EBDDS. Then the following hold:*

(i) $\mathrm{per}(f) = \gcd(\mathcal{RI}_f(a, a))$ *for all* $a \in K^t$*.*

(ii) *Let* $\overline{\mathrm{M}_f} : C_f \to C_f$ *such that*

$$\overline{\mathrm{M}_f}([a]) = [b],$$

where $b \in \mathrm{M}_f(\{a\})$ *and* $a, b \in K^t$*. Then the transformation semigroup generated by* $\overline{\mathrm{M}_f}$ *is the cyclic group* $\mathbb{Z}_{\mathrm{per}(f)}$*.*

Theorem (Wu, Xu, Z., 2016+)

Let $(\mathrm{Set}_K, \mathrm{M}_f)$ *be a* $(t, 1, k)$*-EBDDS. Then* $(\mathrm{Set}_K, \mathrm{M}_f)$ *is primitive if and only if* $(\mathrm{Set}_K, \mathrm{M}_f)$ *is strongly connected and has period one.*

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N}$

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N}$ $\qquad \mathcal{P}(2) = \mathbb{N} \setminus \{2,3,5,6,7\}$

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N} \supsetneq \mathcal{P}(2) = \mathbb{N} \setminus \{2,3,5,6,7\}$

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N} \supsetneq \mathcal{P}(2) = \mathbb{N} \setminus \{2,3,5,6,7\} \supsetneq \mathcal{P}(3)$.

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N} \supsetneq \mathcal{P}(2) = \mathbb{N} \setminus \{2,3,5,6,7\} \supsetneq \mathcal{P}(3)$.
- For any $t \in \mathbb{N}$, we have $|\mathbb{N} \setminus \mathcal{P}(t)| < \infty$.

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N} \supsetneq \mathcal{P}(2) = \mathbb{N} \setminus \{2,3,5,6,7\} \supsetneq \mathcal{P}(3)$.
- For any $t \in \mathbb{N}$, we have $|\mathbb{N} \setminus \mathcal{P}(t)| < \infty$.

	$t = 1$	$t = 2$	$t = 3$	$t = 4$	$t \geq 5$
$\mathcal{P}(t) \cap [1, 2t+3]$	$[1, 2t+3]$	$\{1, 2t\}$	$\{1, 2t+2\}$	$\{1, 2t\}$	$\{1\}$

Sets of periods

Let $\mathcal{P}(t,k)$ be the set of positive integers which can be the period of a strongly connected $(t,1,k)$-EBDDS and let $\mathcal{P}(t) = \bigcup_{k\in\mathbb{N}} \mathcal{P}(t,k)$.

- $\mathcal{P}(1) = \mathbb{N} \supsetneq \mathcal{P}(2) = \mathbb{N} \setminus \{2,3,5,6,7\} \supsetneq \mathcal{P}(3)$.
- For any $t \in \mathbb{N}$, we have $|\mathbb{N} \setminus \mathcal{P}(t)| < \infty$.

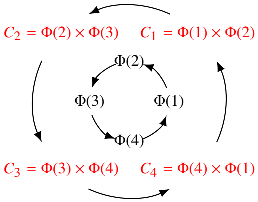
	$t=1$	$t=2$	$t=3$	$t=4$	$t \geq 5$
$\mathcal{P}(t) \cap [1, 2t+3]$	$[1, 2t+3]$	$\{1, 2t\}$	$\{1, 2t+2\}$	$\{1, 2t\}$	$\{1\}$

Conjecture (Wu, Xu, Z., 2016+)

$$\mathcal{P}(1) \supsetneqq \mathcal{P}(2) \supsetneqq \mathcal{P}(3) \supsetneqq \cdots$$

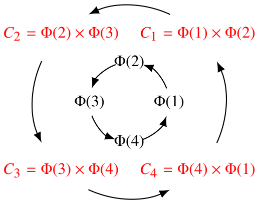
Cyclic decomposition

Let $t, k, p \in \mathbb{N}$ and K be a set of size k.
Let Φ be a map from $\mathbb{Z}_p$ to Set_K.
Let $C_i := \Phi(i) \times \cdots \times \Phi(i + t - 1)$ for all $i \in \mathbb{Z}_p$.
We call Φ a cyclic decomposition of (K^t, t) with period $\mathrm{per}(\Phi) = p$ if $\{C_i\}_{i \in \mathbb{Z}_p}$ form a partition of K^t.



Cyclic decomposition

Let $t, k, p \in \mathbb{N}$ and K be a set of size k.
Let Φ be a map from $\mathbb{Z}_p$ to Set_K.
Let $C_i := \Phi(i) \times \cdots \times \Phi(i + t - 1)$ for all $i \in \mathbb{Z}_p$.
We call Φ a cyclic decomposition of (K^t, t) with period $\mathrm{per}(\Phi) = p$ if $\{C_i\}_{i \in \mathbb{Z}_p}$ form a partition of K^t.

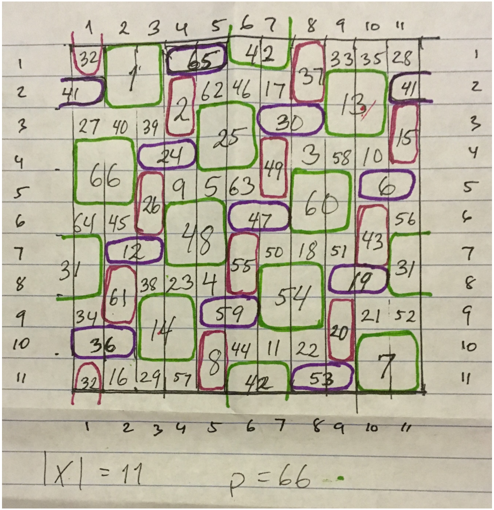


Theorem (Wu, Xu, Z., 2016+)

For any positive integer p, $p \in \mathcal{P}(t, k)$ if and only if there exists a cyclic decomposition Φ of (K^t, t) with $|K| = k$ and $\mathrm{per}(\Phi) = p$.

Examples of cyclic decomposition

- De Bruijn sequences
- An example from Bill Martin



A question

Question

Let t, k, p be three positive integers and let K be a set of size k. What is the number of different cyclic decompositions of (K^t, t) with period p?

A conjecture on expansion property

Conjecture (Wu, Xu, Z., 2016)

Let k be an integer larger than 3. Let A be a $k \times k$ primitive Boolean matrix with primitive exponent p. Let $\sigma(A)$ be the number of entries of A which equals 1.

- *If $\sigma(A) > k^2 - 4k + 7$, then*

$$\sigma(A) < \sigma(A^2) < \cdots < \sigma(A^p) = k^2.$$

- *If $\sigma(A) > k^2 - 5k + 10$, then*

$$\sigma(A) \leq \sigma(A^2) \leq \cdots \leq \sigma(A^p) = k^2.$$

THANK YOU!