# Two problems on completely reachable automata

Road coloring problem and Don's conjecture

Yinfeng Zhu

Ural Federal University

1340-е заседание семинара “Алгебраические системы”

16 декабря 2023 г.

# Deterministic finite automata

A deterministic finite automata (DFA) is a triple $\mathcal{A} = (Q, \Sigma, \delta)$ where

- $Q$ is a finite set, called the state set;
- $\Sigma$ is a finite set, called the input alphabet;
- $\delta : Q \times \Sigma \to Q$ is a map, called the transition function.

$\Sigma^*$ stands for the set of all words over $\Sigma$ including the empty word $\epsilon$. The function $\delta$ extends to a function $Q \times \Sigma^* \to Q$ (still denoted by $\delta$) via the the following recursion: For every $q \in Q$, we set

$$\delta(q, \epsilon) = q$$
$$\delta(q, wa) = \delta(\delta(q, w), a)$$

for all $w \in \Sigma^*$ and $a \in \Sigma$.
To simplify the notation, we often write $q.w$ for $\delta(q, w)$ and $P.w$ for $\{\delta(q, w) : q \in P\}$.

# Deterministic finite automata

A deterministic finite automata (DFA) is a triple $\mathcal{A} = (Q, \Sigma, \delta)$ where

- $Q$ is a finite set, called the state set;
- $\Sigma$ is a finite set, called the input alphabet;
- $\delta : Q \times \Sigma \to Q$ is a map, called the transition function.

$\Sigma^*$ stands for the set of all words over $\Sigma$ including the empty word $\epsilon$. The function $\delta$ extends to a function $Q \times \Sigma^* \to Q$ (still denoted by $\delta$) via the the following recursion: For every $q \in Q$, we set

$$\begin{aligned} \delta(q, \epsilon) &= q \\ \delta(q, wa) &= \delta(\delta(q, w), a) \end{aligned}$$

for all $w \in \Sigma^*$ and $a \in \Sigma$.

To simplify the notation, we often write $q.w$ for $\delta(q, w)$ and $P.w$ for $\{\delta(q, w) : q \in P\}$.

# Deterministic finite automata

A deterministic finite automata (DFA) is a triple $\mathcal{A} = (Q, \Sigma, \delta)$ where

- $Q$ is a finite set, called the state set;
- $\Sigma$ is a finite set, called the input alphabet;
- $\delta : Q \times \Sigma \to Q$ is a map, called the transition function.

$\Sigma^*$ stands for the set of all words over $\Sigma$ including the empty word $\epsilon$. The function $\delta$ extends to a function $Q \times \Sigma^* \to Q$ (still denoted by $\delta$) via the the following recursion: For every $q \in Q$, we set

$$\delta(q, \epsilon) = q$$
$$\delta(q, wa) = \delta(\delta(q, w), a)$$

for all $w \in \Sigma^*$ and $a \in \Sigma$.
To simplify the notation, we often write $q.w$ for $\delta(q, w)$ and $P.w$ for $\{\delta(q, w) : q \in P\}$.

# Completely reachable automata

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a DFA.

- A non-empty subset $P \subseteq Q$ is reachable in $\mathcal{A}$ if $P = Q.w$ for some word $w \in \Sigma^*$.
- A DFA is completely reachable if every non-empty set of its states is reachable.
- A DFA is synchronizing if there exists a reachable singleton set $\{x\} \subseteq Q$.

# Completely reachable automata

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a DFA.

- A non-empty subset $P \subseteq Q$ is reachable in $\mathcal{A}$ if $P = Q.w$ for some word $w \in \Sigma^*$.
- A DFA is completely reachable if every non-empty set of its states is reachable.
- A DFA is synchronizing if there exists a reachable singleton set $\{x\} \subseteq Q$.

# Completely reachable automata

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a DFA.

- A non-empty subset $P \subseteq Q$ is reachable in $\mathcal{A}$ if $P = Q.w$ for some word $w \in \Sigma^*$.
- A DFA is completely reachable if every non-empty set of its states is reachable.
- A DFA is synchronizing if there exists a reachable singleton set $\{x\} \subseteq Q$.

# Digraph

A digraph is a quadruple $G = (V, E, i, t)$ where $V, E$ are non-empty sets and $i, t : E \to V$.

- The elements in $V$ are called vertices;
- the elements of $E$ are called edges;

for an edge $e \in E$,

- the vertex $i(e)$ is called the initial vertex of $e$;
- the vertex $t(e)$ is called the terminal vertex of $e$.

# Digraph

A digraph is a quadruple $G = (V, E, i, t)$ where $V, E$ are non-empty sets and $i, t : E \to V$.

- The elements in $V$ are called vertices;
- the elements of $E$ are called edges;

for an edge $e \in E$,

- the vertex $i(e)$ is called the initial vertex of $e$;
- the vertex $t(e)$ is called the terminal vertex of $e$.

# Neighbours and degrees

Let $v$ be a vertex in a digraph $G$.

- The out-neighbour of $v$ is the set $\{i(e) : t(e) = v, e \in E\}$, denoted $N_+(v)$.
- The in-neighbour of $v$ is the set $\{t(e) : i(e) = v, e \in E\}$, denoted $N_-(v)$.
- For a subset $U \in V$,
  - write $N_+(U)$ for the set $\{u : N_+(u), u \in U\}$;
  - write $N_-(U)$ for the set $\{u : N_-(u), u \in U\}$.
- The out-degree of $v$ is the number of edges whose initial vertex is $v$, denoted $d_+(v)$.
- The in-degree of $v$ is the number of edges whose terminal vertex is $v$, denoted $d_-(v)$.

# Neighbours and degrees

Let $v$ be a vertex in a digraph $G$.

- The out-neighbour of $v$ is the set $\{i(e) : t(e) = v, e \in E\}$, denoted $N_+(v)$.
- The in-neighbour of $v$ is the set $\{t(e) : i(e) = v, e \in E\}$, denoted $N_-(v)$.
- For a subset $U \in V$,
  - write $N_+(U)$ for the set $\{u : N_+(u), u \in U\}$;
  - write $N_-(U)$ for the set $\{u : N_-(u), u \in U\}$.
- The out-degree of $v$ is the number of edges whose initial vertex is $v$, denoted $\mathrm{d}_+(v)$.
- The in-degree of $v$ is the number of edges whose terminal vertex is $v$, denoted $\mathrm{d}_-(v)$.

# Neighbours and degrees

Let $v$ be a vertex in a digraph $G$.

- The out-neighbour of $v$ is the set $\{i(e) : t(e) = v, e \in E\}$, denoted $N_+(v)$.
- The in-neighbour of $v$ is the set $\{t(e) : i(e) = v, e \in E\}$, denoted $N_-(v)$.
- For a subset $U \in V$,
  - write $N_+(U)$ for the set $\{u : N_+(u), u \in U\}$;
  - write $N_-(U)$ for the set $\{u : N_-(u), u \in U\}$.
- The out-degree of $v$ is the number of edges whose initial vertex is $v$, denoted $\mathrm{d}_+(v)$.
- The in-degree of $v$ is the number of edges whose terminal vertex is $v$, denoted $\mathrm{d}_-(v)$.

# Road colorings

For a set $X$, write $\mathcal{P}(X)$ for the power set of $X$.

A road coloring of a finite digraph $G = (V, E, i, t)$ is a function $\alpha : E \to \mathcal{P}(\Sigma)$ such that for every vertex $v \in V$, the family of sets

$$\{\alpha(e) : t(e) = v, e \in E\}$$

forms a partition of $\Sigma$.

# Automata from road colorings

Let $\alpha : E \to \mathcal{P}(\Sigma)$ be a road coloring of $G$.
Define $\mathcal{A}(G, \alpha)$ to the automaton $(V, \Sigma, \delta)$ such that for every $v \in V$ and $a \in \Sigma$,

$$v.a = t(e)$$

where $e$ is the arc such that $i(e) = v$ and $a \in \alpha(e)$.
The road coloring $\alpha$

- is called a sychronizing coloring if $\mathcal{A}(G, \alpha)$ is a synchronizing automata;
- is called a completely reachable coloring if $\mathcal{A}(G, \alpha)$ is a completely reachable automata.

# Automata from road colorings

Let $\alpha : E \to \mathcal{P}(\Sigma)$ be a road coloring of $G$.
Define $\mathcal{A}(G, \alpha)$ to the automaton $(V, \Sigma, \delta)$ such that for every $v \in V$ and $a \in \Sigma$,

$$v.a = t(e)$$

where $e$ is the arc such that $i(e) = v$ and $a \in \alpha(e)$.
The road coloring $\alpha$

- is called a sychronizing coloring if $\mathcal{A}(G, \alpha)$ is a synchronizing automata;
- is called a completely reachable coloring if $\mathcal{A}(G, \alpha)$ is a completely reachable automata.

# Automata from road colorings

Let $\alpha : E \to \mathcal{P}(\Sigma)$ be a road coloring of $G$.
Define $\mathcal{A}(G, \alpha)$ to the automaton $(V, \Sigma, \delta)$ such that for every $v \in V$ and $a \in \Sigma$,

$$v.a = t(e)$$

where $e$ is the arc such that $i(e) = v$ and $a \in \alpha(e)$.
The road coloring $\alpha$

- is called a sychronizing coloring if $\mathcal{A}(G, \alpha)$ is a synchronizing automata;
- is called a completely reachable coloring if $\mathcal{A}(G, \alpha)$ is a completely reachable automata.

# Trahtman's Road Coloring Theorem

- The period of a strongly connected digraph $G$ is the greatest common divisor of the lengths of its cycles, denoted $p(G)$.
- A digraph is called aperiodic if its period equals 1.

### Theorem (Trahtman[1], 2009)

*Let $G = (V, E, i, t)$ be a strongly connected digraph and $d = \max\{\mathrm{d}_+(v), v \in V\}$. The following are equivalent.*

1. *The digraph $G$ admits a synchronizing coloring.*
2. *The digraph $G$ admits a synchronizing coloring with $d$ colors.*
3. *The digraph $G$ is aperiodic.*

[1] A. N. Trahtman (2009). "The road coloring problem". B: *Israel J. Math.* 172, c. 51—60. ISSN: 0021-2172,1565-8511.

# Completely reachable colorings

**Theorem (Z., 2023+)**

*A digraph $G = (V, E, i, t)$ admits a completely reachable coloring if and only if*

1. *$G$ is strongly connected,*
2. *$G$ is aperiodic,*
3. *for every subset $U \subseteq V$, $|U| \leq |N_{-}(U)|$.*

**Theorem (Z., 2023+)**

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

# Completely reachable colorings

**Theorem (Z., 2023+)**

*A digraph $G = (V, E, i, t)$ admits a completely reachable coloring if and only if*

1. *$G$ is strongly connected,*
2. *$G$ is aperiodic,*
3. *for every subset $U \subseteq V$, $|U| \leq |N_{-}(U)|$.*

**Theorem (Z., 2023+)**

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

# Cyclic Decomposition Theorem

### Theorem (Cyclic Decomposition Theorem)

*Let $G$ be a strongly connected digraph of period $p$. The vertex set can be partition into $p$ sets $\{C_i : i \in \mathbb{Z}_p\}$ such that $N_+(C_i) = C_{i+1}$ for every $i \in \mathbb{Z}_p$.*
*Moreover, for each vertex $v \in C_j$ for some $j$, there exists a positive integer $k$ such that*

$$N_-^k(v) = \underbrace{N_-(\cdots N_-(}_{k} v)) = C_j.$$

# Hall's Marriage Theorem

A bipartite graph $H = (X, Y, E)$ is a triple, where $X$, $Y$ are two nonempty sets and $E \subseteq X \times Y$.

The elements in $X \cup Y$ are vertices and the elements in $E$ are edges. A $X$-perfect matching of $H$ is a matching, a set of disjoint edges, which covers every vertex in $X$. For $U \subseteq X$, the neighborhood of $U$ is the set $\{w : (u, w) \in E, u \in U\}$, denoted $N(U)$.

**Theorem (Hall's Marriage Theorem)**

*Let $H = (X, Y, E)$ be a bipartite graph. There exists an $X$-perfect matching if and only if for every subset $U \subseteq X$, we have $|U| \leq N(U)$.*

# Hall's Marriage Theorem

A bipartite graph $H = (X, Y, E)$ is a triple, where $X, Y$ are two nonempty sets and $E \subseteq X \times Y$.

The elements in $X \cup Y$ are vertices and the elements in $E$ are edges. A $X$-perfect matching of $H$ is a matching, a set of disjoint edges, which covers every vertex in $X$.

For $U \subseteq X$, the neighborhood of $U$ is the set $\{w : (u, w) \in E, u \in U\}$, denoted $N(U)$.

**Theorem (Hall's Marriage Theorem)**

*Let $H = (X, Y, E)$ be a bipartite graph. There exists an $X$-perfect matching if and only if for every subset $U \subseteq X$, we have $|U| \leq N(U)$.*

# Hall's Marriage Theorem

A bipartite graph $H = (X, Y, E)$ is a triple, where $X, Y$ are two nonempty sets and $E \subseteq X \times Y$.
The elements in $X \cup Y$ are vertices and the elements in $E$ are edges. A $X$-perfect matching of $H$ is a matching, a set of disjoint edges, which covers every vertex in $X$.
For $U \subseteq X$, the neighborhood of $U$ is the set $\{w : (u, w) \in E, u \in U\}$, denoted $N(U)$.

**Theorem (Hall's Marriage Theorem)**

*Let $H = (X, Y, E)$ be a bipartite graph. There exists an $X$-perfect matching if and only if for every subset $U \subseteq X$, we have $|U| \leq N(U)$.*

# Hall's Marriage Theorem

A bipartite graph $H = (X, Y, E)$ is a triple, where $X, Y$ are two nonempty sets and $E \subseteq X \times Y$.
The elements in $X \cup Y$ are vertices and the elements in $E$ are edges. A $X$-perfect matching of $H$ is a matching, a set of disjoint edges, which covers every vertex in $X$.
For $U \subseteq X$, the neighborhood of $U$ is the set $\{w : (u, w) \in E, u \in U\}$, denoted $N(U)$.

**Theorem (Hall's Marriage Theorem)**

*Let $H = (X, Y, E)$ be a bipartite graph. There exists an $X$-perfect matching if and only if for every subset $U \subseteq X$, we have $|U| \leq N(U)$.*

# The proof

**Theorem (Z., 2023+)**

*A digraph $G = (V, E, i, t)$ admits a completely reachable coloring if and only if*

1. *$G$ is strongly connected,*
2. *$G$ is aperiodic,*
3. *for every subset $U \subseteq V$, $|U| \leq |N_-(U)|$.*

# The proof

"⇒":

- Let $\alpha$ be a completely reachable coloring of $G$ and its color set is $\Sigma$. The corresponding autoaton is $\mathcal{A}(G, \alpha) = (V, \Sigma, \delta)$.
- For every two vertices $u, v$, by completely reachability, there exists a word $w$ such that $V.w = \{u\}$ and then $\delta(v, w) = u$. Then there exists a walk in $G$ from $v$ to $u$.
- By Cyclic Decomposition Theorem, the vertex set $V$ can be partitioned into $p$ sets $\{C_i : i \in \mathbb{Z}_p\}$ such that $N_+(C_i) = C_{i+1}$ for every $i \in \mathbb{Z}_p$.
- Then for any word $w \in \Sigma^*$ and $i \in \mathbb{Z}_p$, $V.w \cap C_i \neq \emptyset$. Since every singleton set is reachable. we have $p = 1$.
- For a non-empty subset $U \subseteq V$, take a word $w = w'a \in \Sigma^*$ such that $V.w = U$. Let $W$ be the set $V.w'$. Then

$$|U| \leq |W| \leq |N_-(U)|.$$

# The proof

"$\Rightarrow$":

- Let $\alpha$ be a completely reachable coloring of $G$ and its color set is $\Sigma$. The corresponding autoaton is $\mathcal{A}(G, \alpha) = (V, \Sigma, \delta)$.
- For every two vertices $u, v$, by completely reachability, there exists a word $w$ such that $V.w = \{u\}$ and then $\delta(v, w) = u$. Then there exists a walk in $G$ from $v$ to $u$.
- By Cyclic Decomposition Theorem, the vertex set $V$ can be partitioned into $p$ sets $\{C_i : i \in \mathbb{Z}_p\}$ such that $N_+(C_i) = C_{i+1}$ for every $i \in \mathbb{Z}_p$.
- Then for any word $w \in \Sigma^*$ and $i \in \mathbb{Z}_p$, $V.w \cap C_i \neq \emptyset$. Since every singleton set is reachable. we have $p = 1$.
- For a non-empty subset $U \subseteq V$, take a word $w = w'a \in \Sigma^*$ such that $V.w = U$. Let $W$ be the set $V.w'$. Then

$$|U| \leq |W| \leq |N_-(U)|.$$

# The proof

"$\Rightarrow$":

- Let $\alpha$ be a completely reachable coloring of $G$ and its color set is $\Sigma$. The corresponding autoaton is $\mathcal{A}(G, \alpha) = (V, \Sigma, \delta)$.
- For every two vertices $u, v$, by completely reachability, there exists a word $w$ such that $V.w = \{u\}$ and then $\delta(v, w) = u$. Then there exists a walk in $G$ from $v$ to $u$.
- By Cyclic Decomposition Theorem, the vertex set $V$ can be partitioned into $p$ sets $\{C_i : i \in \mathbb{Z}_p\}$ such that $N_+(C_i) = C_{i+1}$ for every $i \in \mathbb{Z}_p$.
- Then for any word $w \in \Sigma^*$ and $i \in \mathbb{Z}_p$, $V.w \cap C_i \neq \emptyset$. Since every singleton set is reachable. we have $p = 1$.
- For a non-empty subset $U \subseteq V$, take a word $w = w'a \in \Sigma^*$ such that $V.w = U$. Let $W$ be the set $V.w'$. Then

$$|U| \leq |W| \leq |N_-(U)|.$$

# The proof

"⇒":

- Let $\alpha$ be a completely reachable coloring of $G$ and its color set is $\Sigma$. The corresponding autoaton is $\mathcal{A}(G,\alpha) = (V, \Sigma, \delta)$.
- For every two vertices $u, v$, by completely reachability, there exists a word $w$ such that $V.w = \{u\}$ and then $\delta(v, w) = u$. Then there exists a walk in $G$ from $v$ to $u$.
- By Cyclic Decomposition Theorem, the vertex set $V$ can be partitioned into $p$ sets $\{C_i : i \in \mathbb{Z}_p\}$ such that $N_+(C_i) = C_{i+1}$ for every $i \in \mathbb{Z}_p$.
- Then for any word $w \in \Sigma^*$ and $i \in \mathbb{Z}_p$, $V.w \cap C_i \neq \emptyset$. Since every singleton set is reachable. we have $p = 1$.
- For a non-empty subset $U \subseteq V$, take a word $w = w'a \in \Sigma^*$ such that $V.w = U$. Let $W$ be the set $V.w'$. Then

$$|U| \leq |W| \leq |N_-(U)|.$$

# The proof

"$\Rightarrow$":

- Let $\alpha$ be a completely reachable coloring of $G$ and its color set is $\Sigma$. The corresponding autoaton is $\mathcal{A}(G, \alpha) = (V, \Sigma, \delta)$.
- For every two vertices $u, v$, by completely reachability, there exists a word $w$ such that $V.w = \{u\}$ and then $\delta(v, w) = u$. Then there exists a walk in $G$ from $v$ to $u$.
- By Cyclic Decomposition Theorem, the vertex set $V$ can be partitioned into $p$ sets $\{C_i : i \in \mathbb{Z}_p\}$ such that $N_+(C_i) = C_{i+1}$ for every $i \in \mathbb{Z}_p$.
- Then for any word $w \in \Sigma^*$ and $i \in \mathbb{Z}_p$, $V.w \cap C_i \neq \emptyset$. Since every singleton set is reachable. we have $p = 1$.
- For a non-empty subset $U \subseteq V$, take a word $w = w'a \in \Sigma^*$ such that $V.w = U$. Let $W$ be the set $V.w'$. Then

$$|U| \leq |W| \leq |N_-(U)|.$$

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

"$\Leftarrow$":

- Define $H$ to be the bipartite graph $H = (V_1, V_2, E_H)$ such that $V_1 = V_2 = V$ and $(u, v) \in E_H$ if there exists $e \in E$ such that $i(e) = u$ and $t(e) = v$.
- Observe that for every non-empty subset $U \subseteq V_1$, then $|U| \leq |N(U)|$.

Let $W$ be a non-empty subset of $V_1$. Let $H'$ be the induced subgraph of $H$ on $W \cup N(W)$. By the Hall's Marriage Theorem, there exists a $W$-perfect matching $M$ in $H'$.

Now we can define a function $f_W : V_2 \to V_1$ as following:

1. for $y \in V_2$ which is covered by edge $(x, y) \in M$, set $f_W(y) = x$;
2. for $y \in N(W)$ which is not covered by the matching $M$, set $f_W(y)$ to be an arbitrary vertex in $W \cap N(y)$.
3. for $y \in V_2 \setminus N(W)$, set $f_W(y)$ to be an arbitrary vertex in $N(y)$.

It is clear that $W = f_W(N(W))$.

# The proof, cont'd

Now we construct a road coloring $\alpha : E \to \mathcal{P}(\Sigma)$, where $\Sigma = \mathcal{P}(V) \setminus \{\emptyset\}$ by setting

$$\alpha(e) = \{U : f_U(t(e)) = i(e), \emptyset \neq U \subseteq V\}.$$

Let $\mathcal{A} = (V, \Sigma, \delta) = \mathcal{A}(G, \alpha)$. Note that for every non-empty subset $U$, we have

$$\delta(N_-(U), U) = U.$$

- Let $U_0$ be an arbitrary non-empty subset of $V$, define $U_i = N_-(U_{i-1})$ for all positive integer $i$.
- Since $G$ is strongly connected and aperiodic, by Cyclic Decomposition Theorem, there exists an integer $k$ such that $U_k = V$.
- Then $U_0 = \delta(V, U_{k-1}U_{k-2} \cdots U_1 U_0)$.
- Hence $\mathcal{A}$ is completely reachable and $G$ admits a completely reachable coloring.

# The proof, cont'd

Now we construct a road coloring $\alpha : E \to \mathcal{P}(\Sigma)$, where $\Sigma = \mathcal{P}(V) \setminus \{\emptyset\}$ by setting

$$\alpha(e) = \{U : f_U(t(e)) = i(e), \emptyset \neq U \subseteq V\}.$$

Let $\mathcal{A} = (V, \Sigma, \delta) = \mathcal{A}(G, \alpha)$. Note that for every non-empty subset $U$, we have

$$\delta(N_{-}(U), U) = U.$$

- Let $U_0$ be an arbitrary non-empty subset of $V$, define $U_i = N_{-}(U_{i-1})$ for all positive integer $i$.
- Since $G$ is strongly connected and aperiodic, by Cyclic Decomposition Theorem, there exists an integer $k$ such that $U_k = V$.
- Then $U_0 = \delta(V, U_{k-1}U_{k-2} \cdots U_1 U_0)$.
- Hence $\mathcal{A}$ is completely reachable and $G$ admits a completely reachable coloring.

# The proof, cont'd

Now we construct a road coloring $\alpha : E \to \mathcal{P}(\Sigma)$, where $\Sigma = \mathcal{P}(V) \setminus \{\emptyset\}$ by setting

$$\alpha(e) = \{U : f_U(t(e)) = i(e), \emptyset \neq U \subseteq V\}.$$

Let $\mathcal{A} = (V, \Sigma, \delta) = \mathcal{A}(G, \alpha)$. Note that for every non-empty subset $U$, we have

$$\delta(N_{-}(U), U) = U.$$

- Let $U_0$ be an arbitrary non-empty subset of $V$, define $U_i = N_{-}(U_{i-1})$ for all positive integer $i$.
- Since $G$ is strongly connected and aperiodic, by Cyclic Decomposition Theorem, there exists an integer $k$ such that $U_k = V$.
- Then $U_0 = \delta(V, U_{k-1}U_{k-2} \cdots U_1 U_0)$.
- Hence $\mathcal{A}$ is completely reachable and $G$ admits a completely reachable coloring.

# The proof, cont'd

Now we construct a road coloring $\alpha : E \to \mathcal{P}(\Sigma)$, where $\Sigma = \mathcal{P}(V) \setminus \{\emptyset\}$ by setting

$$\alpha(e) = \{U : f_U(t(e)) = i(e), \emptyset \neq U \subseteq V\}.$$

Let $\mathcal{A} = (V, \Sigma, \delta) = \mathcal{A}(G, \alpha)$. Note that for every non-empty subset $U$, we have

$$\delta(N_-(U), U) = U.$$

- Let $U_0$ be an arbitrary non-empty subset of $V$, define $U_i = N_-(U_{i-1})$ for all positive integer $i$.
- Since $G$ is strongly connected and aperiodic, by Cyclic Decomposition Theorem, there exists an integer $k$ such that $U_k = V$.
- Then $U_0 = \delta(V, U_{k-1}U_{k-2}\cdots U_1U_0)$.
- Hence $\mathcal{A}$ is completely reachable and $G$ admits a completely reachable coloring.

# The proof, cont'd

Now we construct a road coloring $\alpha : E \to \mathcal{P}(\Sigma)$, where $\Sigma = \mathcal{P}(V) \setminus \{\emptyset\}$ by setting

$$\alpha(e) = \{U : f_U(t(e)) = i(e), \emptyset \neq U \subseteq V\}.$$

Let $\mathcal{A} = (V, \Sigma, \delta) = \mathcal{A}(G, \alpha)$. Note that for every non-empty subset $U$, we have

$$\delta(N_-(U), U) = U.$$

- Let $U_0$ be an arbitrary non-empty subset of $V$, define $U_i = N_-(U_{i-1})$ for all positive integer $i$.
- Since $G$ is strongly connected and aperiodic, by Cyclic Decomposition Theorem, there exists an integer $k$ such that $U_k = V$.
- Then $U_0 = \delta(V, U_{k-1}U_{k-2} \cdots U_1 U_0)$.
- Hence $\mathcal{A}$ is completely reachable and $G$ admits a completely reachable coloring.

# The proof, cont'd

Now we construct a road coloring $\alpha : E \to \mathcal{P}(\Sigma)$, where $\Sigma = \mathcal{P}(V) \setminus \{\emptyset\}$ by setting

$$\alpha(e) = \{U : f_U(t(e)) = i(e), \emptyset \neq U \subseteq V\}.$$

Let $\mathcal{A} = (V, \Sigma, \delta) = \mathcal{A}(G, \alpha)$. Note that for every non-empty subset $U$, we have

$$\delta(N_-(U), U) = U.$$

- Let $U_0$ be an arbitrary non-empty subset of $V$, define $U_i = N_-(U_{i-1})$ for all positive integer $i$.
- Since $G$ is strongly connected and aperiodic, by Cyclic Decomposition Theorem, there exists an integer $k$ such that $U_k = V$.
- Then $U_0 = \delta(V, U_{k-1}U_{k-2} \cdots U_1 U_0)$.
- Hence $\mathcal{A}$ is completely reachable and $G$ admits a completely reachable coloring.

## Theorem (Z., 2023+)

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

Proof for $k = 2$:

- Let $G = (V, E, i, t)$ be a digraph such that
  1. $|V|$ is an odd prime number;
  2. for every vertex $v$, $\mathrm{d}_+(v) = 2$;
  3. there exist vertice $x$ and $y$ such that $\mathrm{d}_-(x) = 1$, $\mathrm{d}_-(y) = 3$ and $\mathrm{d}_-(z) = 2$, for each $z \in V \setminus \{x, y\}$.
- Then $G$ admits a completely reachable coloring if and only if $G$ has a hamitonian cycle.
- To determine whether or not such a given graph $G$ has a hamitonian cycle is NP-complelte. (Our proof is obtained from the proof in this paper[2] with some small modification.)

[2] J. Plesník (1979). "The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two". B: *Inform. Process. Lett.* 8.4, c. 199—201. ISSN: 0020-0190,1872-6119.

## Theorem (Z., 2023+)

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

Proof for $k = 2$:

- Let $G = (V, E, i, t)$ be a digraph such that
  1. $|V|$ is an odd prime number;
  2. for every vertex $v$, $d_+(v) = 2$;
  3. there exist vertice $x$ and $y$ such that $d_-(x) = 1$, $d_-(y) = 3$ and $d_-(z) = 2$, for each $z \in V \setminus \{x, y\}$.
- Then $G$ admits a completely reachable coloring if and only if $G$ has a hamitonian cycle.
- To determine whether or not such a given graph $G$ has a hamitonian cycle is NP-complelte. (Our proof is obtained from the proof in this paper[2] with some small modification.)

---

[2] J. Plesník (1979). "The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two". B: *Inform. Process. Lett.* 8.4, c. 199—201. ISSN: 0020-0190,1872-6119.

## Theorem (Z., 2023+)

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

Proof for $k = 2$:

- Let $G = (V, E, i, t)$ be a digraph such that
  1. $|V|$ is an odd prime number;
  2. for every vertex $v$, $d_+(v) = 2$;
  3. there exist vertice $x$ and $y$ such that $d_-(x) = 1$, $d_-(y) = 3$ and $d_-(z) = 2$, for each $z \in V \setminus \{x, y\}$.
- Then $G$ admits a completely reachable coloring if and only if $G$ has a hamitonian cycle.
- To determine whether or not such a given graph $G$ has a hamitonian cycle is NP-complelte. (Our proof is obtained from the proof in this paper[2] with some small modification.)

[2] J. Plesník (1979). "The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two". B: *Inform. Process. Lett.* 8.4, c. 199—201. ISSN: 0020-0190,1872-6119.

## Theorem (Z., 2023+)

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

Proof for $k = 2$:

- Let $G = (V, E, i, t)$ be a digraph such that
  1. $|V|$ is an odd prime number;
  2. for every vertex $v$, $\mathrm{d}_+(v) = 2$;
  3. there exist vertice $x$ and $y$ such that $\mathrm{d}_-(x) = 1$, $\mathrm{d}_-(y) = 3$ and $\mathrm{d}_-(z) = 2$, for each $z \in V \setminus \{x, y\}$.
- Then $G$ admits a completely reachable coloring if and only if $G$ has a hamitonian cycle.
- To determine whether or not such a given graph $G$ has a hamitonian cycle is NP-complelte. (Our proof is obtained from the proof in this paper[2] with some small modification.)

---

[2] J. Plesník (1979). "The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two". B: *Inform. Process. Lett.* 8.4, c. 199—201. ISSN: 0020-0190,1872-6119.

## Theorem (Z., 2023+)

*Let $k \geq 2$ be a fixed integer. To determine a given digraph $G = (V, E, i, t)$ whether or not it admits a completely reachable with $k$ colors is NP-complete.*

Proof for $k = 2$:

- Let $G = (V, E, i, t)$ be a digraph such that
  1. $|V|$ is an odd prime number;
  2. for every vertex $v$, $\mathrm{d}_+(v) = 2$;
  3. there exist vertice $x$ and $y$ such that $\mathrm{d}_-(x) = 1$, $\mathrm{d}_-(y) = 3$ and $\mathrm{d}_-(z) = 2$, for each $z \in V \setminus \{x, y\}$.
- Then $G$ admits a completely reachable coloring if and only if $G$ has a hamitonian cycle.
- To determine whether or not such a given graph $G$ has a hamitonian cycle is NP-complelte. (Our proof is obtained from the proof in this paper[2] with some small modification.)

---

[2] J. Plesník (1979). "The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two". B: *Inform. Process. Lett.* 8.4, c. 199—201. ISSN: 0020-0190,1872-6119.

# Problems

Let $f : \mathbb{N} \to \mathbb{N}$.

1. For a given digarph $G$ with $n$ vertices, is there a polynomial-time algorithm to determine whether $G$ admits a completely reachable coloring which uses $f(n)$ colors?
2. For a given digraph $G$ which admits a completely reachable coloring, can we find one completely reachable coloring in polynomial time?

# Don's Conjecture

Henk Don[3] conjecture that if in a DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq n(n - |S|)$.

If Don's Conjecture is true, it implies the famous Černý Conjecture: If $\mathcal{A}$ is a sychronizing DFA with $n$ states, then there exists a signleton set is reachable by a word of length $\leq (n-1)^2$.

François Gonze and Raphaël Jungers[4] constructed a series of $n$-state automata with a distinguished subset $S$ of $\lfloor \frac{n}{2} \rfloor$ such that if $n \geq 6$ then the shortest word that reaches $S$ is greater than $\frac{2^n}{n}$.

[3] Henk Don (2016). "The Černý conjecture and 1-contracting automata". В: *Electron. J. Combin.* 23.3, Paper 3.12, 10. ISSN: 1077-8926.

[4] François Gonze и Raphaël M. Jungers (2019). "Hardly reachable subsets and completely reachable automata with 1-deficient words". В: *J. Autom. Lang. Comb.* 24.2-4, с. 321—342. ISSN: 1430-189X,2567-3785.

# Don's Conjecture

Henk Don[3] conjecture that if in a DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq n(n - |S|)$.
If Don's Conjecture is true, it implies the famous Černý Conjecture: If $\mathcal{A}$ is a sychronizing DFA with $n$ states, then there exists a signleton set is reachable by a word of length $\leq (n-1)^2$.
François Gonze and Raphaël Jungers[4] constructed a series of $n$-state automata with a distinguished subset $S$ of $\lfloor \frac{n}{2} \rfloor$ such that if $n \geq 6$ then the shortest word that reaches $S$ is greater than $\frac{2^n}{n}$.

[3] Henk Don (2016). "The Černý conjecture and 1-contracting automata". B: *Electron. J. Combin.* 23.3, Paper 3.12, 10. ISSN: 1077-8926.

[4] François Gonze и Raphaël M. Jungers (2019). "Hardly reachable subsets and completely reachable automata with 1-deficient words". B: *J. Autom. Lang. Comb.* 24.2-4, c. 321—342. ISSN: 1430-189X,2567-3785.

# Don's Conjecture

Henk Don[3] conjecture that if in a DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq n(n - |S|)$.
If Don's Conjecture is true, it implies the famous Černý Conjecture: If $\mathcal{A}$ is a sychronizing DFA with $n$ states, then there exists a signleton set is reachable by a word of length $\leq (n-1)^2$.
François Gonze and Raphaël Jungers[4] constructed a series of $n$-state automata with a distinguished subset $S$ of $\lfloor \frac{n}{2} \rfloor$ such that if $n \geq 6$ then the shortest word that reaches $S$ is greater than $\frac{2^n}{n}$.

[3] Henk Don (2016). "The Černý conjecture and 1-contracting automata". В: *Electron. J. Combin.* 23.3, Paper 3.12, 10. ISSN: 1077-8926.

[4] François Gonze и Raphaël M. Jungers (2019). "Hardly reachable subsets and completely reachable automata with 1-deficient words". В: *J. Autom. Lang. Comb.* 24.2-4, с. 321—342. ISSN: 1430-189X,2567-3785.

# Don's Conjecture for completely reachable automata

The restriction of the conjecture to completely reachable automata is still an open problem.

### Conjecture

*If in a completely reachable DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq n(n - |S|)$.*

### Theorem (Robert Ferens and Marek Szykuła[5], 2023)

*If in a completely reachable DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq 2n(n - |S|)$.*

[5] Robert Ferens и Marek Szykuł a (2023). "Completely reachable automata: a polynomial algorithm and quadratic upper bounds". В: *50th International Colloquium on Automata, Languages, and Programming*. Т. 261. LIPIcs. Leibniz Int. Proc. Inform. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, Art. No. 59, 17. ISBN: 978-3-95977-278-5.

# Don's Conjecture for completely reachable automata

The restriction of the conjecture to completely reachable automata is still an open problem.

### Conjecture

*If in a completely reachable DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq n(n - |S|)$.*

### Theorem (Robert Ferens and Marek Szykuła[5], 2023)

*If in a completely reachable DFA with $n$ states, some subset $S$ of states is reachable, then $S$ is reachable by a word of length $\leq 2n(n - |S|)$.*

---

[5] Robert Ferens и Marek Szykuł a (2023). "Completely reachable automata: a polynomial algorithm and quadratic upper bounds". В: *50th International Colloquium on Automata, Languages, and Programming*. Т. 261. LIPIcs. Leibniz Int. Proc. Inform. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, Art. No. 59, 17. ISBN: 978-3-95977-278-5.

# Binary completely reachable automata

- DFAs with two letters are called binary.
- For $n \geq 3$, an $n$-state binary completely reachable automaton is circular, that is, one of the letters acts as a circular permutation.
- For an $n$-state binary completely reachable automaton DFA $\mathcal{A} = (Q, \Sigma, \delta)$, we will assume $Q = \mathbb{Z}_n$, $\Sigma = \{a, b\}$ and for all $q \in Q$, $q.b = q \oplus 1$, where $\oplus$ stands for addition modulo $n$.
- Observe that $|Q \setminus Q.a| = 1$. We will also assume that $\{0\} = Q \setminus Q.a$.

# Binary completely reachable automata

- DFAs with two letters are called binary.
- For $n \geq 3$, an $n$-state binary completely reachable automaton is circular, that is, one of the letters acts as a circular permutation.
- For an $n$-state binary completely reachable automaton DFA $\mathcal{A} = (Q, \Sigma, \delta)$, we will assume $Q = \mathbb{Z}_n$, $\Sigma = \{a, b\}$ and for all $q \in Q$, $q.b = q \oplus 1$, where $\oplus$ stands for addition modulo $n$.
- Observe that $|Q \setminus Q.a| = 1$. We will also assume that $\{0\} = Q \setminus Q.a$.

# Binary completely reachable automata

- DFAs with two letters are called binary.
- For $n \geq 3$, an $n$-state binary completely reachable automaton is circular, that is, one of the letters acts as a circular permutation.
- For an $n$-state binary completely reachable automaton DFA $\mathcal{A} = (Q, \Sigma, \delta)$, we will assume $Q = \mathbb{Z}_n$, $\Sigma = \{a, b\}$ and for all $q \in Q$, $q.b = q \oplus 1$, where $\oplus$ stands for addition modulo $n$.
- Observe that $|Q \setminus Q.a| = 1$. We will also assume that $\{0\} = Q \setminus Q.a$.

# Binary completely reachable automata

- DFAs with two letters are called binary.
- For $n \geq 3$, an $n$-state binary completely reachable automaton is circular, that is, one of the letters acts as a circular permutation.
- For an $n$-state binary completely reachable automaton DFA $\mathcal{A} = (Q, \Sigma, \delta)$, we will assume $Q = \mathbb{Z}_n$, $\Sigma = \{a, b\}$ and for all $q \in Q$, $q.b = q \oplus 1$, where $\oplus$ stands for addition modulo $n$.
- Observe that $|Q \setminus Q.a| = 1$. We will also assume that $\{0\} = Q \setminus Q.a$.

# Binary completely reachable automata

- DFAs with two letters are called binary.
- For $n \geq 3$, an $n$-state binary completely reachable automaton is circular, that is, one of the letters acts as a circular permutation.
- For an $n$-state binary completely reachable automaton DFA $\mathcal{A} = (Q, \Sigma, \delta)$, we will assume $Q = \mathbb{Z}_n$, $\Sigma = \{a, b\}$ and for all $q \in Q$, $q.b = q \oplus 1$, where $\oplus$ stands for addition modulo $n$.
- Observe that $|Q \setminus Q.a| = 1$. We will also assume that $\{0\} = Q \setminus Q.a$.

# Standardized automata

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a binary completely reachable automaton. The automata $\mathcal{A}$ is called standardized, if there exists a state $r \neq 0$ such that $0.a = r.a$.

Let $H_1$ be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $\{0.a^k : 1 \leq k \leq n\}$.

- [David Casas and Mikhail Volkov[6], 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 = (\mathbb{Z}_n, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 \cong (\mathbb{Z}_{n/2}, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. For a non-empty subset $S \subseteq \mathbb{Z}_n$, $S$ is reachable by a word of length $\leq n(n - |S|) + n - 1$.

[6] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations*. arXiv: 2311.00077 [cs.FL].

# Standardized automata

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a binary completely reachable automaton. The automata $\mathcal{A}$ is called standardized, if there exists a state $r \neq 0$ such that $0.a = r.a$.
Let $H_1$ be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $\{0.a^k : 1 \leq k \leq n\}$.

- [David Casas and Mikhail Volkov[6], 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 = (\mathbb{Z}_n, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 \cong (\mathbb{Z}_{n/2}, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. For a non-empty subset $S \subseteq \mathbb{Z}_n$, $S$ is reachable by a word of length $\leq n(n - |S|) + n - 1$.

[6] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations.* arXiv: 2311.00077 [cs.FL].

# Standardized automata

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a binary completely reachable automaton. The automata $\mathcal{A}$ is called standardized, if there exists a state $r \neq 0$ such that $0.a = r.a$.
Let $H_1$ be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $\{0.a^k : 1 \leq k \leq n\}$.

- [David Casas and Mikhail Volkov[6], 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 = (\mathbb{Z}_n, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 \cong (\mathbb{Z}_{n/2}, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. For a non-empty subset $S \subseteq \mathbb{Z}_n$, $S$ is reachable by a word of length $\leq n(n - |S|) + n - 1$.

[6] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations*. arXiv: 2311.00077 [cs.FL].

# Standardized automata

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a binary completely reachable automaton. The automata $\mathcal{A}$ is called standardized, if there exists a state $r \neq 0$ such that $0.a = r.a$.
Let $H_1$ be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $\{0.a^k : 1 \leq k \leq n\}$.

- [David Casas and Mikhail Volkov[6], 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 = (\mathbb{Z}_n, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 \cong (\mathbb{Z}_{n/2}, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. For a non-empty subset $S \subseteq \mathbb{Z}_n$, $S$ is reachable by a word of length $\leq n(n - |S|) + n - 1$.

[6] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations*. arXiv: 2311.00077 [cs.FL].

# Standardized automata

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a binary completely reachable automaton. The automata $\mathcal{A}$ is called standardized, if there exists a state $r \neq 0$ such that $0.a = r.a$.
Let $H_1$ be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $\{0.a^k : 1 \leq k \leq n\}$.

- [David Casas and Mikhail Volkov[6], 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 = (\mathbb{Z}_n, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. If $H_1 \cong (\mathbb{Z}_{n/2}, \oplus)$ then $\mathcal{A}$ fulfills Don's Conjecture.
- [Z., 2023+] Let $\mathcal{A}$ be a standardized automata. For a non-empty subset $S \subseteq \mathbb{Z}_n$, $S$ is reachable by a word of length $\leq n(n - |S|) + n - 1$.

[6] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations*. arXiv: 2311.00077 [cs.FL].

# Expandable

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be an $n$-state DFA and $S$ a subset of $Q$.

- A word $w$ over $\Sigma$ expands $S$ if there exists a set $R$ such that $R.w = S$ and $|R| > |S|$.
- A proper non-empty subset of $Q$ is said to be $k$-expandable if it can be expanded by a word of length at most $k$.
- If every proper non-empty subset of $Q$ is $n$-expandable, then the DFA $\mathcal{A}$ fulfills Don's Conjecture.
- There exists a standradized DFA and a subset of states such that the subset is not $n$-expandable in the DFA.

# Expandable

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be an $n$-state DFA and $S$ a subset of $Q$.

- A word $w$ over $\Sigma$ expands $S$ if there exists a set $R$ such that $R.w = S$ and $|R| > |S|$.
- A proper non-empty subset of $Q$ is said to be $k$-expandable if it can be expanded by a word of length at most $k$.
- If every proper non-empty subset of $Q$ is $n$-expandable, then the DFA $\mathcal{A}$ fulfills Don's Conjecture.
- There exists a standradized DFA and a subset of states such that the subset is not $n$-expandable in the DFA.

# Expandable

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be an $n$-state DFA and $S$ a subset of $Q$.

- A word $w$ over $\Sigma$ expands $S$ if there exists a set $R$ such that $R.w = S$ and $|R| > |S|$.
- A proper non-empty subset of $Q$ is said to be $k$-expandable if it can be expanded by a word of length at most $k$.
- If every proper non-empty subset of $Q$ is $n$-expandable, then the DFA $\mathcal{A}$ fulfills Don's Conjecture.
- There exists a standradized DFA and a subset of states such that the subset is not $n$-expandable in the DFA.

# Expandable

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be an $n$-state DFA and $S$ a subset of $Q$.

- A word $w$ over $\Sigma$ expands $S$ if there exists a set $R$ such that $R.w = S$ and $|R| > |S|$.
- A proper non-empty subset of $Q$ is said to be $k$-expandable if it can be expanded by a word of length at most $k$.
- If every proper non-empty subset of $Q$ is $n$-expandable, then the DFA $\mathcal{A}$ fulfills Don's Conjecture.
- There exists a standradized DFA and a subset of states such that the subset is not $n$-expandable in the DFA.

# Expandable

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be an $n$-state DFA and $S$ a subset of $Q$.

- A word $w$ over $\Sigma$ expands $S$ if there exists a set $R$ such that $R.w = S$ and $|R| > |S|$.
- A proper non-empty subset of $Q$ is said to be $k$-expandable if it can be expanded by a word of length at most $k$.
- If every proper non-empty subset of $Q$ is $n$-expandable, then the DFA $\mathcal{A}$ fulfills Don's Conjecture.
- There exists a standradized DFA and a subset of states such that the subset is not $n$-expandable in the DFA.

# A sequence of subgroups

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a standardized DFA. For a subgroup $H$ of $(\mathbb{Z}_n, \oplus)$, define $U(\mathcal{A}, H) = \{i \in \{1, \ldots, \frac{n}{|H|} - 1\} : H.a^k \cap (H \oplus i) \neq \emptyset, k \geq 1\}$.

Since $\mathcal{A}$ is completely reachable, $U(\mathcal{A}, H)$ is non-empty.

- Define $H_0$ to the trivial subgroup of $(\mathbb{Z}_n, \oplus)$.
- For an integer $i \geq 1$ such that $H_{i-1} \neq (\mathbb{Z}_n, \oplus)$, define $H_i$ to be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $H_{i-1} \cup U(\mathcal{A}, H_{i-1})$.
- We obtain a sequence of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = (\mathbb{Z}_n, \oplus).$$

- Observe that $\ell \leq \Omega(n)$, where $\Omega(n)$ is the number of prime factors of $n$ with multiplicity.

# A sequence of subgroups

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a standardized DFA. For a subgroup $H$ of $(\mathbb{Z}_n, \oplus)$, define $U(\mathcal{A}, H) = \{i \in \{1, \ldots, \frac{n}{|H|} - 1\} : H.a^k \cap (H \oplus i) \neq \emptyset, k \geq 1\}$.
Since $\mathcal{A}$ is completely reachable, $U(\mathcal{A}, H)$ is non-empty.

- Define $H_0$ to the trivial subgroup of $(\mathbb{Z}_n, \oplus)$.
- For an integer $i \geq 1$ such that $H_{i-1} \neq (\mathbb{Z}_n, \oplus)$, define $H_i$ to be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $H_{i-1} \cup U(\mathcal{A}, H_{i-1})$.
- We obtain a sequence of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = (\mathbb{Z}_n, \oplus).$$

- Observe that $\ell \leq \Omega(n)$, where $\Omega(n)$ is the number of prime factors of $n$ with multiplicity.

# A sequence of subgroups

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a standardized DFA. For a subgroup $H$ of $(\mathbb{Z}_n, \oplus)$, define $U(\mathcal{A}, H) = \{i \in \{1, \dots, \frac{n}{|H|} - 1\} : H.a^k \cap (H \oplus i) \neq \emptyset, k \geq 1\}$.
Since $\mathcal{A}$ is completely reachable, $U(\mathcal{A}, H)$ is non-empty.

- Define $H_0$ to the trivial subgroup of $(\mathbb{Z}_n, \oplus)$.
- For an integer $i \geq 1$ such that $H_{i-1} \neq (\mathbb{Z}_n, \oplus)$, define $H_i$ to be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $H_{i-1} \cup U(\mathcal{A}, H_{i-1})$.
- We obtain a sequence of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = (\mathbb{Z}_n, \oplus).$$

- Observe that $\ell \leq \Omega(n)$, where $\Omega(n)$ is the number of prime factors of $n$ with multiplicity.

# A sequence of subgroups

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a standardized DFA. For a subgroup $H$ of $(\mathbb{Z}_n, \oplus)$, define $U(\mathcal{A}, H) = \{i \in \{1, \ldots, \frac{n}{|H|} - 1\} : H.a^k \cap (H \oplus i) \neq \emptyset, k \geq 1\}$.
Since $\mathcal{A}$ is completely reachable, $U(\mathcal{A}, H)$ is non-empty.

- Define $H_0$ to the trivial subgroup of $(\mathbb{Z}_n, \oplus)$.
- For an integer $i \geq 1$ such that $H_{i-1} \neq (\mathbb{Z}_n, \oplus)$, define $H_i$ to be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $H_{i-1} \cup U(\mathcal{A}, H_{i-1})$.
- We obtain a sequence of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = (\mathbb{Z}_n, \oplus).$$

- Observe that $\ell \leq \Omega(n)$, where $\Omega(n)$ is the number of prime factors of $n$ with multiplicity.

# A sequence of subgroups

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a standardized DFA. For a subgroup $H$ of $(\mathbb{Z}_n, \oplus)$, define $U(\mathcal{A}, H) = \{i \in \{1, \ldots, \frac{n}{|H|} - 1\} : H.a^k \cap (H \oplus i) \neq \emptyset, k \geq 1\}$.
Since $\mathcal{A}$ is completely reachable, $U(\mathcal{A}, H)$ is non-empty.

- Define $H_0$ to the trivial subgroup of $(\mathbb{Z}_n, \oplus)$.
- For an integer $i \geq 1$ such that $H_{i-1} \neq (\mathbb{Z}_n, \oplus)$, define $H_i$ to be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $H_{i-1} \cup U(\mathcal{A}, H_{i-1})$.
- We obtain a sequence of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = (\mathbb{Z}_n, \oplus).$$

- Observe that $\ell \leq \Omega(n)$, where $\Omega(n)$ is the number of prime factors of $n$ with multiplicity.

# A sequence of subgroups

Let $\mathcal{A} = (\mathbb{Z}_n, \{a, b\}, \delta)$ be a standardized DFA. For a subgroup $H$ of $(\mathbb{Z}_n, \oplus)$, define $U(\mathcal{A}, H) = \{i \in \{1, \ldots, \frac{n}{|H|} - 1\} : H.a^k \cap (H \oplus i) \neq \emptyset, k \geq 1\}$.
Since $\mathcal{A}$ is completely reachable, $U(\mathcal{A}, H)$ is non-empty.

- Define $H_0$ to the trivial subgroup of $(\mathbb{Z}_n, \oplus)$.
- For an integer $i \geq 1$ such that $H_{i-1} \neq (\mathbb{Z}_n, \oplus)$, define $H_i$ to be the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by $H_{i-1} \cup U(\mathcal{A}, H_{i-1})$.
- We obtain a sequence of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = (\mathbb{Z}_n, \oplus).$$

- Observe that $\ell \leq \Omega(n)$, where $\Omega(n)$ is the number of prime factors of $n$ with multiplicity.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k)+n-1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|)+n-1$ such that $\mathbb{Z}_n.w' = S$.

# Outline of our proof

## Theorem (Z., 2023+)

*Let $\mathcal{A} = (\mathbb{Z}_n, \Sigma, \delta)$ be a standardized automata. For a non-empty subset $S$, $S$ is reachable by a word of length $\leq n(n-k) + n - 1$.*

There are some minor differences between the real proof and the following outline.

Outline of our proof:

- Write $q_i$ for $\frac{n}{|H_i|}$. Let $S \subseteq \mathbb{Z}_n$. And define $m(S)$ be the integer $m$ such that $S$ is not a union of $H_m$-cosets and is a union of $H_{m-1}$-cosets.
- There exists a word $w$ of length $\leq q_{m(S)-1}$ such that $R.w = S$ and either $|R| > |S|$ or $m(R) < m(S)$.
- Moreover, if $0 \notin S$, then we can improve the estimate of the length of $w$ to $|w| \leq q_{m(S)-1} - q_{m(S)} + 1$.
- Then, for every non-empty proper subset $S$, there exists an expanding word for $S$ of length $\leq n + m(S)$.
- By connecting some expanding words, we can get a word $w'$ of length $\leq n(n-|S|) + n - 1$ such that $\mathbb{Z}_n.w' = S$.

# Restricted Cayley digraph

Let $k$ be a positive integer. Write $[k]$ for $\{1, \ldots, k\}$.

- A [k]-graded set $(X, f)$ is a set $X$ together with a function $f : X \to [k]$.
- Let $X$ be a subset of a group $G$, the Cayley digraph of $G$ with respect to $X$, denoted $\mathrm{Cay}(G, X)$, has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X\}$ as its edge set.
- If $G = \mathbb{Z}_n$ is a cyclic group and $(X, f)$ is $[k]$-graded set, the restricted Cayley digraph $\mathcal{R}(G, X, f)$ of $\mathbb{Z}_n$ with respect to $(X, f)$ has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X, g + f(x) \leq n\}$ as its edge set.

Lemma

*Let $G = (\mathbb{Z}_n, \oplus)$. Let $(X, f)$ be a $[k]$-graded set. If $f$ is a surjective map, then the strongly connected components of $\mathcal{R}(G, X, f)$ have the cosets of $\langle X \rangle$ as their vertex sets.*

This lemma is a corollary of [Proposition 5,[7]].

[7] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations.* arXiv: 2311.00077 [cs.FL].

# Restricted Cayley digraph

Let $k$ be a positive integer. Write $[k]$ for $\{1, \ldots, k\}$.

- A $[k]$-graded set $(X, f)$ is a set $X$ together with a function $f : X \to [k]$.
- Let $X$ be a subset of a group $G$, the Cayley digraph of $G$ with respect to $X$, denoted $\mathrm{Cay}(G, X)$, has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X\}$ as its edge set.
- If $G = \mathbb{Z}_n$ is a cyclic group and $(X, f)$ is $[k]$-graded set, the restricted Cayley digraph $\mathcal{R}(G, X, f)$ of $\mathbb{Z}_n$ with respect to $(X, f)$ has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X, g + f(x) \leq n\}$ as its edge set.

## Lemma

*Let $G = (\mathbb{Z}_n, \oplus)$. Let $(X, f)$ be a $[k]$-graded set. If $f$ is a surjective map, then the strongly connected components of $\mathcal{R}(G, X, f)$ have the cosets of $\langle X \rangle$ as their vertex sets.*

This lemma is a corollary of [Proposition 5,[7]].

[7] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations.* arXiv: 2311.00077 [cs.FL].

# Restricted Cayley digraph

Let $k$ be a positive integer. Write $[k]$ for $\{1, \ldots, k\}$.

- A $[k]$-graded set $(X, f)$ is a set $X$ together with a function $f : X \to [k]$.
- Let $X$ be a subset of a group $G$, the Cayley digraph of $G$ with respect to $X$, denoted $\mathrm{Cay}(G, X)$, has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X\}$ as its edge set.
- If $G = \mathbb{Z}_n$ is a cyclic group and $(X, f)$ is $[k]$-graded set, the restricted Cayley digraph $\mathcal{R}(G, X, f)$ of $\mathbb{Z}_n$ with respect to $(X, f)$ has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X, g + f(x) \leq n\}$ as its edge set.

**Lemma**

*Let $G = (\mathbb{Z}_n, \oplus)$. Let $(X, f)$ be a $[k]$-graded set. If $f$ is a surjective map, then the strongly connected components of $\mathcal{R}(G, X, f)$ have the cosets of $\langle X \rangle$ as their vertex sets.*

This lemma is a corollary of [Proposition 5,[7]].

[7] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations.* arXiv: 2311.00077 [cs.FL].

# Restricted Cayley digraph

Let $k$ be a positive integer. Write $[k]$ for $\{1, \ldots, k\}$.

- A $[k]$-graded set $(X, f)$ is a set $X$ together with a function $f : X \to [k]$.
- Let $X$ be a subset of a group $G$, the Cayley digraph of $G$ with respect to $X$, denoted $\mathrm{Cay}(G, X)$, has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X\}$ as its edge set.
- If $G = \mathbb{Z}_n$ is a cyclic group and $(X, f)$ is $[k]$-graded set, the restricted Cayley digraph $\mathcal{R}(G, X, f)$ of $\mathbb{Z}_n$ with respect to $(X, f)$ has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X, g + f(x) \leq n\}$ as its edge set.

## Lemma

*Let $G = (\mathbb{Z}_n, \oplus)$. Let $(X, f)$ be a $[k]$-graded set. If $f$ is a surjective map, then the strongly connected components of $\mathcal{R}(G, X, f)$ have the cosets of $\langle X \rangle$ as their vertex sets.*

This lemma is a corollary of [Proposition 5,[7]].

[7] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations.* arXiv: 2311.00077 [cs.FL].

# Restricted Cayley digraph

Let $k$ be a positive integer. Write $[k]$ for $\{1, \dots, k\}$.

- A $[k]$-graded set $(X, f)$ is a set $X$ together with a function $f : X \to [k]$.
- Let $X$ be a subset of a group $G$, the Cayley digraph of $G$ with respect to $X$, denoted $\mathrm{Cay}(G, X)$, has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X\}$ as its edge set.
- If $G = \mathbb{Z}_n$ is a cyclic group and $(X, f)$ is $[k]$-graded set, the restricted Cayley digraph $\mathcal{R}(G, X, f)$ of $\mathbb{Z}_n$ with respect to $(X, f)$ has $G$ as its vertex set and $\{(g, gx) : g \in G, x \in X, g + f(x) \leq n\}$ as its edge set.

## Lemma

*Let $G = (\mathbb{Z}_n, \oplus)$. Let $(X, f)$ be a $[k]$-graded set. If $f$ is a surjective map, then the strongly connected components of $\mathcal{R}(G, X, f)$ have the cosets of $\langle X \rangle$ as their vertex sets.*

This lemma is a corollary of [Proposition 5,[7]].

[7] David Casas и Mikhail V. Volkov (2023). *Don's conjecture for binary completely reachable automata: an approach and its limitations.* arXiv: 2311.00077 [cs.FL].

## Lemma

*Let $\mathcal{A}$ is a standardize DFA. Let $S$ be proper non-empty subset of $\mathbb{Z}_n$. Then there exists a word $w$ of length $\leq q_{m(S)-1}$ satisfying one of the following conditions:*

1. $|R| > |S|$;
2. $0 \notin R$ *and* $H_{m-1} \cap R = \neq \emptyset$ *which imply* $m(R) < m(S)$.

Proof:

- Set $G := (\mathbb{Z}_n, \oplus)/H_{m-1}$, $X = \{H_{m-1} \oplus j : j \in U(\mathcal{A}, H_{m-1})\}$ and $f(H_{m-1} \oplus j)$ to be the least integer $k$ such that $H_{m-1}.a^k \cap (H_{m-1} \oplus j) \neq \emptyset$.
- In $\mathcal{R}(G, X, f)$, there exists a strongly connected component $C = H_m \oplus t$ such that $C \cap S \notin \{\emptyset, C\}$. (Regard $C$ and $S$ as sets of $H_{m-1}$-cosets.)
- Take two vertices $L = H_{m-1} \oplus p \in C \setminus S$ and $L' = H_{m-1} \oplus p' \in C \cap S$ such that $(L, L')$ is an edge of $\mathcal{R}(G, X, f)$.
- One can check that $a^{f(H_{m-1} \oplus (p'-p))} b^p$ is a word satisfying our requirements.

## Lemma

*Let $\mathcal{A}$ is a standardize DFA. Let $S$ be proper non-empty subset of $\mathbb{Z}_n$. Then there exists a word $w$ of length $\leq q_{m(S)-1}$ satisfying one of the following conditions:*

1. $|R| > |S|$;
2. $0 \notin R$ *and* $H_{m-1} \cap R =\neq \emptyset$ *which imply* $m(R) < m(S)$.

Proof:

- Set $G := (\mathbb{Z}_n, \oplus)/H_{m-1}$, $X = \{H_{m-1} \oplus j : j \in U(\mathcal{A}, H_{m-1})\}$ and $f(H_{m-1} \oplus j)$ to be the least integer $k$ such that $H_{m-1}.a^k \cap (H_{m-1} \oplus j) \neq \emptyset$.
- In $\mathcal{R}(G, X, f)$, there exists a strongly connected component $C = H_m \oplus t$ such that $C \cap S \notin \{\emptyset, C\}$. (Regard $C$ and $S$ as sets of $H_{m-1}$-cosets.)
- Take two vertices $L = H_{m-1} \oplus p \in C \setminus S$ and $L' = H_{m-1} \oplus p' \in C \cap S$ such that $(L, L')$ is an edge of $\mathcal{R}(G, X, f)$.
- One can check that $a^{f(H_{m-1} \oplus (p'-p))} b^p$ is a word satisfying our requirements.

## Lemma

*Let $\mathcal{A}$ is a standardize DFA. Let $S$ be proper non-empty subset of $\mathbb{Z}_n$. Then there exists a word $w$ of length $\leq q_{m(S)-1}$ satisfying one of the following conditions:*

1. $|R| > |S|$;
2. $0 \notin R$ *and* $H_{m-1} \cap R =\neq \emptyset$ *which imply* $m(R) < m(S)$.

Proof:

- Set $G := (\mathbb{Z}_n, \oplus)/H_{m-1}$, $X = \{H_{m-1} \oplus j : j \in U(\mathcal{A}, H_{m-1})\}$ and $f(H_{m-1} \oplus j)$ to be the least integer $k$ such that $H_{m-1}.a^k \cap (H_{m-1} \oplus j) \neq \emptyset$.
- In $\mathcal{R}(G, X, f)$, there exists a strongly connected component $C = H_m \oplus t$ such that $C \cap S \notin \{\emptyset, C\}$. (Regard $C$ and $S$ as sets of $H_{m-1}$-cosets.)
- Take two vertices $L = H_{m-1} \oplus p \in C \setminus S$ and $L' = H_{m-1} \oplus p' \in C \cap S$ such that $(L, L')$ is an edge of $\mathcal{R}(G, X, f)$.
- One can check that $a^{f(H_{m-1} \oplus (p'-p))} b^p$ is a word satisfying our requirements.

## Lemma

*Let $\mathcal{A}$ is a standardize DFA. Let $S$ be proper non-empty subset of $\mathbb{Z}_n$. Then there exists a word $w$ of length $\leq q_{m(S)-1}$ satisfying one of the following conditions:*

1. $|R| > |S|$;
2. $0 \notin R$ *and* $H_{m-1} \cap R = \neq \emptyset$ *which imply* $m(R) < m(S)$.

Proof:

- Set $G := (\mathbb{Z}_n, \oplus)/H_{m-1}$, $X = \{H_{m-1} \oplus j : j \in U(\mathcal{A}, H_{m-1})\}$ and $f(H_{m-1} \oplus j)$ to be the least integer $k$ such that $H_{m-1}.a^k \cap (H_{m-1} \oplus j) \neq \emptyset$.
- In $\mathcal{R}(G, X, f)$, there exists a strongly connected component $C = H_m \oplus t$ such that $C \cap S \notin \{\emptyset, C\}$. (Regard $C$ and $S$ as sets of $H_{m-1}$-cosets.)
- Take two vertices $L = H_{m-1} \oplus p \in C \setminus S$ and $L' = H_{m-1} \oplus p' \in C \cap S$ such that $(L, L')$ is an edge of $\mathcal{R}(G, X, f)$.
- One can check that $a^{f(H_{m-1} \oplus (p' - p))} b^p$ is a word satisfying our requirements.

## Lemma

*Let $\mathcal{A}$ is a standardize DFA. Let $S$ be proper non-empty subset of $\mathbb{Z}_n$. Then there exists a word $w$ of length $\leq q_{m(S)-1}$ satisfying one of the following conditions:*

1. $|R| > |S|$;
2. $0 \notin R$ *and* $H_{m-1} \cap R =\neq \emptyset$ *which imply* $m(R) < m(S)$.

Proof:

- Set $G := (\mathbb{Z}_n, \oplus)/H_{m-1}$, $X = \{H_{m-1} \oplus j : j \in U(\mathcal{A}, H_{m-1})\}$ and $f(H_{m-1} \oplus j)$ to be the least integer $k$ such that $H_{m-1}.a^k \cap (H_{m-1} \oplus j) \neq \emptyset$.
- In $\mathcal{R}(G, X, f)$, there exists a strongly connected component $C = H_m \oplus t$ such that $C \cap S \notin \{\emptyset, C\}$. (Regard $C$ and $S$ as sets of $H_{m-1}$-cosets.)
- Take two vertices $L = H_{m-1} \oplus p \in C \setminus S$ and $L' = H_{m-1} \oplus p' \in C \cap S$ such that $(L, L')$ is an edge of $\mathcal{R}(G, X, f)$.
- One can check that $a^{f(H_{m-1} \oplus (p'-p))} b^p$ is a word satisfying our requirements.

In the case that $0 \notin S$ and $H_{m(S)} \cap S \neq \emptyset$,

- Consider $S.b^{q_m - 1}$.
- Applying the arguments in the last slides for $S.b^{q_m-1}$, we can obtain a word $a^{f(H_{m-1} \oplus (p'-p))} b^p$ satisfying our requirements with respect to $S.b^{q_m-1}$.
- We can prove that $p \geq q_m - 1$. So the word $a^{f(H_{m-1} \oplus (p'-p))} b^{p-q_m+1}$ satifies our requirements with respect to $S$ and its length is at most $q_{m-1} - q_m + 1$.

In the case that $0 \notin S$ and $H_{m(S)} \cap S \neq \emptyset$,

- Consider $S.b^{q_m - 1}$.
- Applying the arguments in the last slides for $S.b^{q_m-1}$, we can obtain a word $a^{f(H_{m-1} \oplus (p'-p))} b^p$ satisfying our requirements with respect to $S.b^{q_m-1}$.
- We can prove that $p \geq q_m - 1$. So the word $a^{f(H_{m-1} \oplus (p'-p))} b^{p-q_m+1}$ satifies our requirements with respect to $S$ and its length is at most $q_{m-1} - q_m + 1$.

In the case that $0 \notin S$ and $H_{m(S)} \cap S \neq \emptyset$,

- Consider $S.b^{q_m-1}$.
- Applying the arguments in the last slides for $S.b^{q_m-1}$, we can obtain a word $a^{f(H_{m-1} \oplus (p'-p))} b^p$ satisfying our requirements with respect to $S.b^{q_m-1}$.
- We can prove that $p \geq q_m - 1$. So the word $a^{f(H_{m-1} \oplus (p'-p))} b^{p-q_m+1}$ satifies our requirements with respect to $S$ and its length is at most $q_{m-1} - q_m + 1$.

Using the above lemma successively, we obtain

$$S_k \xrightarrow{w_{k-1}} S_{k-1} \xrightarrow{w_{k-2}} \cdots \xrightarrow{w_1} S_1 \xrightarrow{w_0} S_0 = S$$

such that $|S_k| > |S|$ and

$$|w_0| \leq q_{m(S_0)-1}$$
$$|w_i| \leq q_{m(S_i)-1} - q_{m(S_i)} + 1 \qquad \text{for every } i \in [k-1].$$

Since $m(S_i) - 1 \geq m(S_{i+1})$, we have $q_{m(S_i)-1} \leq q_{m(S_{i+1})}$ for all $i > 0$.
Let $u = w_{k-1} \cdots w_2 w_1$. Hence we have $|u| \leq q_{m(S_{k-1})} + k - 1 \leq n + m(S)$.
We say that the word $u$ "meet" a subgroup $H_m$ if there exists $S_i$ such that $m(S_i) = m$.
It is clear that $|u| \leq n +$ (the number of subgroups met by $u$) $- 1$.

Using the above lemma successively, we obtain

$$S_k \xrightarrow{w_{k-1}} S_{k-1} \xrightarrow{w_{k-2}} \cdots \xrightarrow{w_1} S_1 \xrightarrow{w_0} S_0 = S$$

such that $|S_k| > |S|$ and

$$\begin{aligned} |w_0| &\leq q_{m(S_0)-1} \\ |w_i| &\leq q_{m(S_i)-1} - q_{m(S_i)} + 1 \qquad \text{for every } i \in [k-1]. \end{aligned}$$

Since $m(S_i) - 1 \geq m(S_{i+1})$, we have $q_{m(S_i)-1} \leq q_{m(S_{i+1})}$ for all $i > 0$.
Let $u = w_{k-1} \cdots w_2 w_1$. Hence we have $|u| \leq q_{m(S_{k-1})} + k - 1 \leq n + m(S)$.
We say that the word $u$ "meet" a subgroup $H_m$ if there exists $S_i$ such that $m(S_i) = m$.
It is clear that $|u| \leq n +$ (the number of subgroups met by $u$) $- 1$.

Using the above lemma successively, we obtain

$$S_k \xrightarrow{w_{k-1}} S_{k-1} \xrightarrow{w_{k-2}} \cdots \xrightarrow{w_1} S_1 \xrightarrow{w_0} S_0 = S$$

such that $|S_k| > |S|$ and

$$|w_0| \leq q_{m(S_0)-1}$$
$$|w_i| \leq q_{m(S_i)-1} - q_{m(S_i)} + 1 \qquad \text{for every } i \in [k-1].$$

Since $m(S_i) - 1 \geq m(S_{i+1})$, we have $q_{m(S_i)-1} \leq q_{m(S_{i+1})}$ for all $i > 0$.
Let $u = w_{k-1} \cdots w_2 w_1$. Hence we have $|u| \leq q_{m(S_{k-1})} + k - 1 \leq n + m(S)$.
We say that the word $u$ "meet" a subgroup $H_m$ if there exists $S_i$ such that $m(S_i) = m$.
It is clear that $|u| \leq n +$ (the number of subgroups met by $u$) $- 1$.

Using the above lemma successively, we obtain

$$S_k \xrightarrow{w_{k-1}} S_{k-1} \xrightarrow{w_{k-2}} \cdots \xrightarrow{w_1} S_1 \xrightarrow{w_0} S_0 = S$$

such that $|S_k| > |S|$ and

$$|w_0| \leq q_{m(S_0)-1}$$
$$|w_i| \leq q_{m(S_i)-1} - q_{m(S_i)} + 1 \qquad \text{for every } i \in [k-1].$$

Since $m(S_i) - 1 \geq m(S_{i+1})$, we have $q_{m(S_i)-1} \leq q_{m(S_{i+1})}$ for all $i > 0$.
Let $u = w_{k-1} \cdots w_2 w_1$. Hence we have $|u| \leq q_{m(S_{k-1})} + k - 1 \leq n + m(S)$.
We say that the word $u$ "meet" a subgroup $H_m$ if there exists $S_i$ such that $m(S_i) = m$.
It is clear that $|u| \leq n +$ (the number of subgroups met by $u$) $- 1$.

Using the above lemma successively, we obtain

$$S_k \xrightarrow{w_{k-1}} S_{k-1} \xrightarrow{w_{k-2}} \cdots \xrightarrow{w_1} S_1 \xrightarrow{w_0} S_0 = S$$

such that $|S_k| > |S|$ and

$$\begin{aligned} |w_0| &\leq q_{m(S_0)-1} \\ |w_i| &\leq q_{m(S_i)-1} - q_{m(S_i)} + 1 \qquad \text{for every } i \in [k-1]. \end{aligned}$$

Since $m(S_i) - 1 \geq m(S_{i+1})$, we have $q_{m(S_i)-1} \leq q_{m(S_{i+1})}$ for all $i > 0$.
Let $u = w_{k-1} \cdots w_2 w_1$. Hence we have $|u| \leq q_{m(S_{k-1})} + k - 1 \leq n + m(S)$.
We say that the word $u$ "meet" a subgroup $H_m$ if there exists $S_i$ such that $m(S_i) = m$.
It is clear that $|u| \leq n +$ (the number of subgroups met by $u$) $- 1$.

Using the above lemma successively, we obtain

$$S_k \xrightarrow{w_{k-1}} S_{k-1} \xrightarrow{w_{k-2}} \cdots \xrightarrow{w_1} S_1 \xrightarrow{w_0} S_0 = S$$

such that $|S_k| > |S|$ and

$$|w_0| \leq q_{m(S_0)-1}$$
$$|w_i| \leq q_{m(S_i)-1} - q_{m(S_i)} + 1 \qquad \text{for every } i \in [k-1].$$

Since $m(S_i) - 1 \geq m(S_{i+1})$, we have $q_{m(S_i)-1} \leq q_{m(S_{i+1})}$ for all $i > 0$.
Let $u = w_{k-1} \cdots w_2 w_1$. Hence we have $|u| \leq q_{m(S_{k-1})} + k - 1 \leq n + m(S)$.
We say that the word $u$ "meet" a subgroup $H_m$ if there exists $S_i$ such that $m(S_i) = m$.
It is clear that $|u| \leq n +$ (the number of subgroups met by $u$) $- 1$.

Using arguments in the last slides successively, we obtain

$$R_k \xrightarrow{u_{k-1}} R_{k-1} \xrightarrow{u_{k-2}} \cdots \xrightarrow{u_1} R_1 \xrightarrow{u_0} R_0 = S \tag{1}$$

where $R_k = \mathbb{Z}_n$ and $|R_i| > |R_{i-1}|$.

For every subgroup $H_m$, only at most $\frac{n}{|H_m|}$ words in $\{u_0, \ldots, u_{k-1}\}$ meet $H_m$. Then

$$\sum_{i=0}^{k-1} |u_i| \leq n(n - |S|) + \sum_{j=1}^{\ell} \frac{n}{|H_m|} \leq n(n - |S|) + n - 1.$$

Using arguments in the last slides successively, we obtain

$$R_k \xrightarrow{u_{k-1}} R_{k-1} \xrightarrow{u_{k-2}} \cdots \xrightarrow{u_1} R_1 \xrightarrow{u_0} R_0 = S \tag{1}$$

where $R_k = \mathbb{Z}_n$ and $|R_i| > |R_{i-1}|$.
For every subgroup $H_m$, only at most $\frac{n}{|H_m|}$ words in $\{u_0, \ldots, u_{k-1}\}$ meet $H_m$. Then

$$\sum_{i=0}^{k-1} |u_i| \leq n(n - |S|) + \sum_{j=1}^{\ell} \frac{n}{|H_m|} \leq n(n - |S|) + n - 1.$$

Using arguments in the last slides successively, we obtain

$$R_k \xrightarrow{u_{k-1}} R_{k-1} \xrightarrow{u_{k-2}} \cdots \xrightarrow{u_1} R_1 \xrightarrow{u_0} R_0 = S \tag{1}$$

where $R_k = \mathbb{Z}_n$ and $|R_i| > |R_{i-1}|$.
For every subgroup $H_m$, only at most $\frac{n}{|H_m|}$ words in $\{u_0, \ldots, u_{k-1}\}$ meet $H_m$. Then

$$\sum_{i=0}^{k-1} |u_i| \leq n(n - |S|) + \sum_{j=1}^{\ell} \frac{n}{|H_m|} \leq n(n - |S|) + n - 1.$$

# Thank you

Спасибо