Matrix mortality and the Pin-Černý Conjecture

Jorge Almeida\textsuperscript{1}  Benjamin Steinberg\textsuperscript{2}

\textsuperscript{1}University of Porto, \textsuperscript{2}Carleton University

bsteinbg@math.carleton.ca

http://www.mathstat.carleton.ca/~bsteinbg

DLT July 3, 2009
Synchronizing automata

- By an automaton $A = (Q, \Sigma)$, we understand a complete deterministic automaton with state set $Q$, input alphabet $\Sigma$ and no initial or final states.
- If $w \in \Sigma^*$, then the rank of $w$ is $rk(w) = |Qw|$.
- If $rk(w) = 1$, then $w$ is called a reset word.
- Define $rk(A) = \min\{rk(w) \mid w \in \Sigma^*\}$ (Pin).
- $A$ is synchronizing if $rk(A) = 1$, i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton $A$ of rank $r$ admits a word $w$ of length at most $(n - r)^2$ with $rk(w) = r$.

- The case $r = 1$ is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
By an automaton $\mathcal{A} = (Q, \Sigma)$, we understand a complete deterministic automaton with state set $Q$, input alphabet $\Sigma$ and no initial or final states.

- If $w \in \Sigma^*$, then the rank of $w$ is $\text{rk}(w) = |Qw|$.
- If $\text{rk}(w) = 1$, then $w$ is called a reset word.
- Define $\text{rk}(\mathcal{A}) = \min\{\text{rk}(w) \mid w \in \Sigma^*\}$ (Pin).
- $\mathcal{A}$ is synchronizing if $\text{rk}(\mathcal{A}) = 1$, i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton $\mathcal{A}$ of rank $r$ admits a word $w$ of length at most $(n - r)^2$ with $\text{rk}(w) = r$.

- The case $r = 1$ is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
By an automaton $\mathcal{A} = (Q, \Sigma)$, we understand a complete deterministic automaton with state set $Q$, input alphabet $\Sigma$ and no initial or final states.

- If $w \in \Sigma^*$, then the rank of $w$ is $\text{rk}(w) = |Qw|$.
- If $\text{rk}(w) = 1$, then $w$ is called a reset word.
- Define $\text{rk}(\mathcal{A}) = \min\{\text{rk}(w) \mid w \in \Sigma^*\}$ (Pin).
- $\mathcal{A}$ is synchronizing if $\text{rk}(\mathcal{A}) = 1$, i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton $\mathcal{A}$ of rank $r$ admits a word $w$ of length at most $(n - r)^2$ with $\text{rk}(w) = r$.

- The case $r = 1$ is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
By an automaton \( \mathcal{A} = (Q, \Sigma) \), we understand a complete deterministic automaton with state set \( Q \), input alphabet \( \Sigma \) and no initial or final states.

- If \( w \in \Sigma^* \), then the rank of \( w \) is \( \text{rk}(w) = |Qw| \).
- If \( \text{rk}(w) = 1 \), then \( w \) is called a reset word.
- Define \( \text{rk}(\mathcal{A}) = \min\{\text{rk}(w) \mid w \in \Sigma^*\} \) (Pin).

\( \mathcal{A} \) is synchronizing if \( \text{rk}(\mathcal{A}) = 1 \), i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton \( \mathcal{A} \) of rank \( r \) admits a word \( w \) of length at most \( (n - r)^2 \) with \( \text{rk}(w) = r \).

- The case \( r = 1 \) is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
By an automaton $A = (Q, \Sigma)$, we understand a complete deterministic automaton with state set $Q$, input alphabet $\Sigma$ and no initial or final states.

- If $w \in \Sigma^*$, then the rank of $w$ is $\text{rk}(w) = |Qw|$.
- If $\text{rk}(w) = 1$, then $w$ is called a reset word.
- Define $\text{rk}(A) = \min\{\text{rk}(w) \mid w \in \Sigma^*\}$ (Pin).
- $A$ is synchronizing if $\text{rk}(A) = 1$, i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton $A$ of rank $r$ admits a word $w$ of length at most $(n - r)^2$ with $\text{rk}(w) = r$.

- The case $r = 1$ is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
By an automaton \( \mathcal{A} = (Q, \Sigma) \), we understand a complete deterministic automaton with state set \( Q \), input alphabet \( \Sigma \) and no initial or final states.

- If \( w \in \Sigma^* \), then the rank of \( w \) is \( \text{rk}(w) = |Qw| \).
- If \( \text{rk}(w) = 1 \), then \( w \) is called a reset word.
- Define \( \text{rk}(\mathcal{A}) = \min\{\text{rk}(w) \mid w \in \Sigma^*\} \) (Pin).
- \( \mathcal{A} \) is synchronizing if \( \text{rk}(\mathcal{A}) = 1 \), i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton \( \mathcal{A} \) of rank \( r \) admits a word \( w \) of length at most \( (n - r)^2 \) with \( \text{rk}(w) = r \).

The case \( r = 1 \) is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
Synchronizing automata

By an automaton \( \mathcal{A} = (Q, \Sigma) \), we understand a complete deterministic automaton with state set \( Q \), input alphabet \( \Sigma \) and no initial or final states.

- If \( w \in \Sigma^* \), then the rank of \( w \) is \( \text{rk}(w) = |Qw| \).
- If \( \text{rk}(w) = 1 \), then \( w \) is called a reset word.
- Define \( \text{rk}(\mathcal{A}) = \min \{ \text{rk}(w) \mid w \in \Sigma^* \} \) (Pin).
- \( \mathcal{A} \) is synchronizing if \( \text{rk}(\mathcal{A}) = 1 \), i.e., it admits a reset word.

Conjecture (Černý-Pin)

An automaton \( \mathcal{A} \) of rank \( r \) admits a word \( w \) of length at most \((n - r)^2\) with \( \text{rk}(w) = r \).

The case \( r = 1 \) is due to Černý; the more general conjecture is a variation on an earlier conjecture of Pin.
Černý’s examples

- Černý showed that the shortest length reset word for the $n$-state synchronizing automaton with transitions

$$a = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 2 & 3 & \cdots & n \end{pmatrix}$$

is $(n - 1)^2$.

- The Černý automaton for $n = 4$:

- The word $b(a^3b)^2$ resets to state 2.
Černý’s examples

- Černý showed that the shortest length reset word for the $n$-state synchronizing automaton with transitions

$$a = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 2 & 3 & \cdots & n \end{pmatrix}$$

is $(n - 1)^2$.

- The Černý automaton for $n = 4$:

![Diagram of the Černý automaton for $n = 4$]

- The word $b(a^3b)^2$ resets to state 2.
Černý’s examples

- Černý showed that the shortest length reset word for the $n$-state synchronizing automaton with transitions

$$
a = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 2 & 3 & \cdots & n \end{pmatrix}
$$

is $(n - 1)^2$.
- The Černý automaton for $n = 4$:

- The word $b(a^3b)^2$ resets to state 2.
It is straightforward to obtain a cubic upper bound of $\frac{n^3-n}{3}$ on reset words for synchronizing automata.

The best known upper bound for the synchronizing case is $\frac{n^3-n}{6}$, which was proved by Pin modulo an extremal set theory result of Frankl.

Improving a bound by a factor of 2 can be hard work!

The lower bound of $(n - r)^2$ for rank $r$ is due to Pin.

Pin also has an analogous cubic upper bound for rank $r$.

Probabilistically speaking, all automata are synchronizing with reset word of length at most $2n$.

The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

There is no time to survey the whole literature here.
It is straightforward to obtain a cubic upper bound of \( \frac{n^3 - n}{3} \) on reset words for synchronizing automata.

The best known upper bound for the synchronizing case is \( \frac{n^3 - n}{6} \), which was proved by Pin modulo an extremal set theory result of Frankl.

Improving a bound by a factor of 2 can be hard work!

The lower bound of \((n - r)^2\) for rank \( r \) is due to Pin.

Pin also has an analogous cubic upper bound for rank \( r \).

Probabilistically speaking, all automata are synchronizing with reset word of length at most \( 2n \).

The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

There is no time to survey the whole literature here.
It is straightforward to obtain a cubic upper bound of \( \frac{n^3 - n}{3} \) on reset words for synchronizing automata.

The best known upper bound for the synchronizing case is \( \frac{n^3 - n}{6} \), which was proved by Pin modulo an extremal set theory result of Frankl.

Improving a bound by a factor of 2 can be hard work!

The lower bound of \((n - r)^2\) for rank \(r\) is due to Pin.

Pin also has an analogous cubic upper bound for rank \(r\).

Probabilistically speaking, all automata are synchronizing with reset word of length at most \(2n\).

The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

There is no time to survey the whole literature here.
It is straightforward to obtain a cubic upper bound of \( \frac{n^3-n}{3} \) on reset words for synchronizing automata.

The best known upper bound for the synchronizing case is \( \frac{n^3-n}{6} \), which was proved by Pin modulo an extremal set theory result of Frankl.

Improving a bound by a factor of 2 can be hard work!

The lower bound of \((n - r)^2\) for rank \(r\) is due to Pin.

Pin also has an analogous cubic upper bound for rank \(r\).

Probabilistically speaking, all automata are synchronizing with reset word of length at most 2\(n\).

The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

There is no time to survey the whole literature here.
It is straightforward to obtain a cubic upper bound of \( \frac{n^3-n}{3} \) on reset words for synchronizing automata.

The best known upper bound for the synchronizing case is \( \frac{n^3-n}{6} \), which was proved by Pin modulo an extremal set theory result of Frankl.

Improving a bound by a factor of 2 can be hard work!

The lower bound of \( (n - r)^2 \) for rank \( r \) is due to Pin.

Pin also has an analogous cubic upper bound for rank \( r \).

Probabilistically speaking, all automata are synchronizing with reset word of length at most \( 2n \).

The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

There is no time to survey the whole literature here.
Pin’s bounds

- It is straightforward to obtain a cubic upper bound of $\frac{n^3 - n}{3}$ on reset words for synchronizing automata.
- The best known upper bound for the synchronizing case is $\frac{n^3 - n}{6}$, which was proved by Pin modulo an extremal set theory result of Frankl.
- Improving a bound by a factor of 2 can be hard work!
- The lower bound of $(n - r)^2$ for rank $r$ is due to Pin.
- Pin also has an analogous cubic upper bound for rank $r$.
- Probabilistically speaking, all automata are synchronizing with reset word of length at most $2n$.
- The remainder of the Černý literature consists of a vast array of special, but interesting, cases.
- There is no time to survey the whole literature here.
Pin’s bounds

- It is straightforward to obtain a cubic upper bound of \( \frac{n^3 - n}{3} \) on reset words for synchronizing automata.

- The best known upper bound for the synchronizing case is \( \frac{n^3 - n}{6} \), which was proved by Pin modulo an extremal set theory result of Frankl.

- Improving a bound by a factor of 2 can be hard work!

- The lower bound of \( (n - r)^2 \) for rank \( r \) is due to Pin.

- Pin also has an analogous cubic upper bound for rank \( r \).

- Probabilistically speaking, all automata are synchronizing with reset word of length at most \( 2n \).

- The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

- There is no time to survey the whole literature here.
It is straightforward to obtain a cubic upper bound of \( \frac{n^3-n}{3} \) on reset words for synchronizing automata.

The best known upper bound for the synchronizing case is \( \frac{n^3-n}{6} \), which was proved by Pin modulo an extremal set theory result of Frankl.

Improving a bound by a factor of 2 can be hard work!

The lower bound of \((n - r)^2\) for rank \(r\) is due to Pin.

Pin also has an analogous cubic upper bound for rank \(r\).

Probabilistically speaking, all automata are synchronizing with reset word of length at most \(2n\).

The remainder of the Černý literature consists of a vast array of special, but interesting, cases.

There is no time to survey the whole literature here.
Some known results

The special cases treated so far tend to be of two sorts:

1. Combinatorial restrictions are imposed on the automata;
2. Algebraic restrictions are imposed on the transition monoid.

A key example of the first sort is the result of Dubuc that the Černý conjecture holds for circular automata: automata where one of the input letters cyclically permutes the state set.

Kari proved that if the underlying digraph of the automaton is Eulerian, then the Černý conjecture holds.

An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with aperiodic transition monoid with an upper bound of \( \frac{n(n - 1)}{2} \).

Rystsov showed that if the transition monoid is commutative, then the Černý conjecture holds with an upper bound of \( n - 1 \) (which is sharp).
Some known results

- The special cases treated so far tend to be of two sorts:
  1. **Combinatorial** restrictions are imposed on the automata;
  2. **Algebraic** restrictions are imposed on the transition monoid.

- A key example of the first sort is the result of Dubuc that the Černý conjecture holds for **circular automata**: automata where one of the input letters cyclically permutes the state set.

- Kari proved that if the underlying digraph of the automaton is **Eulerian**, then the Černý conjecture holds.

- An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with **aperiodic transition monoid** with an upper bound of $n(n - 1)/2$.

- Rystsov showed that if the transition monoid is commutative, then the Černý conjecture holds with an upper bound of $n - 1$ (which is sharp).
Some known results

- The special cases treated so far tend to be of two sorts:
  1. **Combinatorial** restrictions are imposed on the automata;
  2. **Algebraic** restrictions are imposed on the transition monoid.

- A key example of the first sort is the result of Dubuc that the Černý conjecture holds for **circular automata**: automata where one of the input letters cyclically permutes the state set.

- Kari proved that if the underlying digraph of the automaton is **Eulerian**, then the Černý conjecture holds.

- An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with **aperiodic** transition monoid with an upper bound of $\frac{n(n - 1)}{2}$.

- Rystsov showed that if the transition monoid is commutative, then the Černý conjecture holds with an upper bound of $n - 1$ (which is sharp).
Some known results

- The special cases treated so far tend to be of two sorts:
  1. **Combinatorial** restrictions are imposed on the automata;
  2. **Algebraic** restrictions are imposed on the transition monoid.

- A key example of the first sort is the result of Dubuc that the Černý conjecture holds for **circular automata**: automata where one of the input letters cyclically permutes the state set.

- Kari proved that if the underlying digraph of the automaton is **Eulerian**, then the Černý conjecture holds.

- An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with **aperiodic** transition monoid with an upper bound of \( n(n - 1)/2 \).

- Rystsov showed that if the transition monoid is commutative, then the Černý conjecture holds with an upper bound of \( n - 1 \) (which is sharp).
Some known results

- The special cases treated so far tend to be of two sorts:
  1. **Combinatorial** restrictions are imposed on the automata;
  2. **Algebraic** restrictions are imposed on the transition monoid.

- A key example of the first sort is the result of Dubuc that the Černý conjecture holds for **circular automata**: automata where one of the input letters cyclically permutes the state set.

- Kari proved that if the underlying digraph of the automaton is **Eulerian**, then the Černý conjecture holds.

- An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with **aperiodic** transition monoid with an upper bound of $n(n - 1)/2$.

- Rystsov showed that if the transition monoid is **commutative**, then the Černý conjecture holds with an upper bound of $n - 1$ (which is sharp).
Some known results

- The special cases treated so far tend to be of two sorts:
  1. **Combinatorial** restrictions are imposed on the automata;
  2. **Algebraic** restrictions are imposed on the transition monoid.

- A key example of the first sort is the result of Dubuc that the Černý conjecture holds for **circular automata**: automata where one of the input letters cyclically permutes the state set.

- Kari proved that if the underlying digraph of the automaton is **Eulerian**, then the Černý conjecture holds.

- An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with **aperiodic** transition monoid with an upper bound of \( n(n - 1)/2 \).

- Rystsov showed that if the transition monoid is **commutative**, then the Černý conjecture holds with an upper bound of \( n - 1 \) (which is sharp).
Some known results

- The special cases treated so far tend to be of two sorts:
  1. **Combinatorial** restrictions are imposed on the automata;
  2. **Algebraic** restrictions are imposed on the transition monoid.

- A key example of the first sort is the result of Dubuc that the Černý conjecture holds for **circular automata**: automata where one of the input letters cyclically permutes the state set.

- Kari proved that if the underlying digraph of the automaton is **Eulerian**, then the Černý conjecture holds.

- An important algebraic result is that of Trahtman establishing the Černý conjecture for automata with **aperiodic** transition monoid with an upper bound of \( n(n - 1)/2 \).

- Rystsov showed that if the transition monoid is **commutative**, then the Černý conjecture holds with an upper bound of \( n - 1 \) (which is sharp).
Representation theoretic approaches

- **Representation theory** is the study of algebraic objects using linear algebra.
- Many papers on Černý’s conjecture make use in some form or the other of representation theory without using the full strength of the subject.
- For instance, Dubuc’s paper on circular automata implicitly relies on properties of representations of cyclic groups.
- An approach using rational power series, pioneered by Béal, also relies on representation theory as representation theory lies in the foundations of weighted automata theory.
- Rystsov has a number of papers that make use of matrix representations to attack cases of the Černý conjecture.
- My goal is to explore representation theoretic approaches to the Černý conjecture.
Representation theoretic approaches

- **Representation theory** is the study of algebraic objects using linear algebra.
- Many papers on Černý's conjecture make use in some form or the other of representation theory without using the full strength of the subject.
- For instance, Dubuc's paper on circular automata implicitly relies on properties of representations of cyclic groups.
- An approach using rational power series, pioneered by Béal, also relies on representation theory as representation theory lies in the foundations of weighted automata theory.
- Rystsov has a number of papers that make use of matrix representations to attack cases of the Černý conjecture.
- My goal is to explore representation theoretic approaches to the Černý conjecture.
Representation theoretic approaches

- **Representation theory** is the study of algebraic objects using linear algebra.
- Many papers on Černý’s conjecture make use in some form or the other of representation theory without using the full strength of the subject.
- For instance, Dubuc’s paper on circular automata implicitly relies on properties of representations of cyclic groups.
- An approach using rational power series, pioneered by Béal, also relies on representation theory as representation theory lies in the foundations of weighted automata theory.
- Rystsov has a number of papers that make use of matrix representations to attack cases of the Černý conjecture.
- My goal is to explore representation theoretic approaches to the Černý conjecture.
Representation theory is the study of algebraic objects using linear algebra.

Many papers on Černý’s conjecture make use in some form or the other of representation theory without using the full strength of the subject.

For instance, Dubuc’s paper on circular automata implicitly relies on properties of representations of cyclic groups.

An approach using rational power series, pioneered by Béal, also relies on representation theory as representation theory lies in the foundations of weighted automata theory.

Rystsov has a number of papers that make use of matrix representations to attack cases of the Černý conjecture.

My goal is to explore representation theoretic approaches to the Černý conjecture.
Representation theoretic approaches

- **Representation theory** is the study of algebraic objects using linear algebra.
- Many papers on Černý’s conjecture make use in some form or the other of representation theory without using the full strength of the subject.
- For instance, Dubuc’s paper on circular automata implicitly relies on properties of representations of cyclic groups.
- An approach using rational power series, pioneered by Béal, also relies on representation theory as representation theory lies in the foundations of weighted automata theory.
- Rystsov has a number of papers that make use of matrix representations to attack cases of the Černý conjecture.
- My goal is to explore representation theoretic approaches to the Černý conjecture.
Representation theory is the study of algebraic objects using linear algebra.

Many papers on Černý’s conjecture make use in some form or the other of representation theory without using the full strength of the subject.

For instance, Dubuc’s paper on circular automata implicitly relies on properties of representations of cyclic groups.

An approach using rational power series, pioneered by Béal, also relies on representation theory as representation theory lies in the foundations of weighted automata theory.

Rystsov has a number of papers that make use of matrix representations to attack cases of the Černý conjecture.

My goal is to explore representation theoretic approaches to the Černý conjecture.
Theorem (Rystsov)

Suppose that it is true that, given a set $\Sigma \subseteq M_n(K)$ of $n \times n$ matrices over a field $K$ such that

1. $|\langle \Sigma \rangle| < \infty$
2. $0 \in \langle \Sigma \rangle$,

there is a word $w \in \Sigma^*$ of length at most $n^2$ representing the zero matrix. Then the Černý-Pin conjecture is true.

Unfortunately, Rystsov’s conjecture is false.

Paterson showed that it is undecidable whether the monoid generated by a finite subset of $M_3(\mathbb{Z})$ contains 0 (The Matrix Mortality Problem).

If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
Matrix mortality

**Theorem (Rystsov)**

*Suppose that it is true that, given a set $\Sigma \subseteq M_n(K)$ of $n \times n$ matrices over a field $K$ such that*

1. $|\langle \Sigma \rangle| < \infty$
2. $0 \in \langle \Sigma \rangle$,

*there is a word $w \in \Sigma^*$ of length at most $n^2$ representing the zero matrix. Then the Černý-Pin conjecture is true.*

- Unfortunately, Rystsov’s conjecture is false.
- Paterson showed that it is undecidable whether the monoid generated by a finite subset of $M_3(\mathbb{Z})$ contains 0 (The Matrix Mortality Problem).
- If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
Matrix mortality

**Theorem (Rystsov)**

Suppose that it is true that, given a set \( \Sigma \subseteq M_n(K) \) of \( n \times n \) matrices over a field \( K \) such that

1. \( |\langle \Sigma \rangle| < \infty \)
2. \( 0 \in \langle \Sigma \rangle \),

there is a word \( w \in \Sigma^* \) of length at most \( n^2 \) representing the zero matrix. Then the Černý-Pin conjecture is true.

- Unfortunately, Rystsov’s conjecture is false.
- Paterson showed that it is undecidable whether the monoid generated by a finite subset of \( M_3(\mathbb{Z}) \) contains \( 0 \) (The Matrix Mortality Problem).
- If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
Matrix mortality

Theorem (Rystsov)

Suppose that it is true that, given a set \( \Sigma \subseteq M_n(K) \) of \( n \times n \) matrices over a field \( K \) such that

1. \( |\langle \Sigma \rangle| < \infty \)
2. \( 0 \in \langle \Sigma \rangle \),

there is a word \( w \in \Sigma^* \) of length at most \( n^2 \) representing the zero matrix. Then the Černý-Pin conjecture is true.

- Unfortunately, Rystsov’s conjecture is false.
- Paterson showed that it is undecidable whether the monoid generated by a finite subset of \( M_3(\mathbb{Z}) \) contains 0 (The Matrix Mortality Problem).
- If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
Matrix mortality

Theorem (Rystsov)

Suppose that it is true that, given a set $\Sigma \subseteq M_n(K)$ of $n \times n$ matrices over a field $K$ such that

1. $|\langle \Sigma \rangle| < \infty$
2. $0 \in \langle \Sigma \rangle$,

there is a word $w \in \Sigma^*$ of length at most $n^2$ representing the zero matrix. Then the Černý-Pin conjecture is true.

- Unfortunately, Rystsov’s conjecture is false.
  - Paterson showed that it is undecidable whether the monoid generated by a finite subset of $M_3(\mathbb{Z})$ contains 0 (The Matrix Mortality Problem).
  - If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
Theorem (Rystsov)

Suppose that it is true that, given a set \( \Sigma \subseteq M_n(K) \) of \( n \times n \) matrices over a field \( K \) such that

1. \( |\langle \Sigma \rangle| < \infty \)
2. \( 0 \in \langle \Sigma \rangle \),

there is a word \( w \in \Sigma^* \) of length at most \( n^2 \) representing the zero matrix. Then the Černý-Pin conjecture is true.

- Unfortunately, Rystsov’s conjecture is false.
- Paterson showed that it is undecidable whether the monoid generated by a finite subset of \( M_3(\mathbb{Z}) \) contains 0 (The Matrix Mortality Problem).
- If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
Matrix mortality

Theorem (Rystsov)

Suppose that it is true that, given a set \( \Sigma \subseteq M_n(K) \) of \( n \times n \) matrices over a field \( K \) such that

1. \( |\langle \Sigma \rangle| < \infty \)
2. \( 0 \in \langle \Sigma \rangle \),

there is a word \( w \in \Sigma^* \) of length at most \( n^2 \) representing the zero matrix. Then the Černý-Pin conjecture is true.

- Unfortunately, Rystsov’s conjecture is false.
- Paterson showed that it is undecidable whether the monoid generated by a finite subset of \( M_3(\mathbb{Z}) \) contains \( 0 \) (The Matrix Mortality Problem).
- If Rystsov’s conjecture were true, then by considering reduction modulo primes this problem would be decidable.
The proof of Rystsov’s result uses only the field $\mathbb{F}_2$.

We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.

A monoid homomorphism $\rho: M \to M_n(\mathbb{Q})$ is called a representation of degree $n$.

A function $f: \mathbb{N} \to \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho: M \to M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.

Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$.

We say $f$ is a mortality function for a class of monoids $\mathcal{C}$ if it is a mortality function for all monoids in $\mathcal{C}$.

By a universal mortality function, we mean a mortality function for the class of all finite monoids.
Mortality functions

- The proof of Rystsov’s result uses only the field $\mathbb{F}_2$.
- We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.
- A monoid homomorphism $\rho: M \to M_n(\mathbb{Q})$ is called a representation of degree $n$.
- A function $f: \mathbb{N} \to \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho: M \to M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.
- Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$. 
- We say $f$ is a mortality function for a class of monoids $\mathcal{C}$ if it is a mortality function for all monoids in $\mathcal{C}$.
- By a universal mortality function, we mean a mortality function for the class of all finite monoids.
Mortality functions

- The proof of Rystsov’s result uses only the field $F_2$.
- We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.
- A monoid homomorphism $\rho : M \rightarrow M_n(\mathbb{Q})$ is called a representation of degree $n$.
- A function $f : \mathbb{N} \rightarrow \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho : M \rightarrow M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.
- Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$.
- We say $f$ is a mortality function for a class of monoids $C$ if it is a mortality function for all monoids in $C$.
- By a universal mortality function, we mean a mortality function for the class of all finite monoids.
The proof of Rystsov’s result uses only the field $\mathbb{F}_2$.

We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.

A monoid homomorphism $\rho : M \to M_n(\mathbb{Q})$ is called a representation of degree $n$.

A function $f : \mathbb{N} \to \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho : M \to M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.

Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$.

We say $f$ is a mortality function for a class of monoids $\mathcal{C}$ if it is a mortality function for all monoids in $\mathcal{C}$.

By a universal mortality function, we mean a mortality function for the class of all finite monoids.
The proof of Rystsov’s result uses only the field $\mathbb{F}_2$.

We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.

A monoid homomorphism $\rho : M \rightarrow M_n(\mathbb{Q})$ is called a representation of degree $n$.

A function $f : \mathbb{N} \rightarrow \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho : M \rightarrow M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.

Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$.

We say $f$ is a mortality function for a class of monoids $\mathcal{C}$ if it is a mortality function for all monoids in $\mathcal{C}$.

By a universal mortality function, we mean a mortality function for the class of all finite monoids.
Mortality functions

- The proof of Rystsov’s result uses only the field $\mathbb{F}_2$.
- We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.
- A monoid homomorphism $\rho: M \to M_n(\mathbb{Q})$ is called a representation of degree $n$.
- A function $f: \mathbb{N} \to \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho: M \to M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.
- Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$.
- We say $f$ is a mortality function for a class of monoids $\mathcal{C}$ if it is a mortality function for all monoids in $\mathcal{C}$.
- By a universal mortality function, we mean a mortality function for the class of all finite monoids.
Mortality functions

- The proof of Rystsov’s result uses only the field $\mathbb{F}_2$.
- We find it more convenient to work with the field $\mathbb{Q}$ of rational numbers.
- A monoid homomorphism $\rho : M \to M_n(\mathbb{Q})$ is called a representation of degree $n$.
- A function $f : \mathbb{N} \to \mathbb{N}$ is a mortality function for the monoid $M$ if, for all representations $\rho : M \to M_n(\mathbb{Q})$ with $0 \in \rho(M)$ and all generating sets $\Sigma$ for $M$, there exists $w \in \Sigma^*$ of length at most $f(n)$ such that $\rho(w) = 0$.
- Of course $f(n) = |M| - 1$ is a mortality function for a finite monoid $M$.
- We say $f$ is a mortality function for a class of monoids $\mathcal{C}$ if it is a mortality function for all monoids in $\mathcal{C}$.
- By a universal mortality function, we mean a mortality function for the class of all finite monoids.
A function $f : \mathbb{N} \rightarrow \mathbb{N}$ is superadditive if
\[ f(m) + f(n) \leq f(m + n). \]

The following result was inspired by Rystsov’s argument.

**Theorem (Almeida, BS)**

Let $A$ be an $n$-state automaton of rank $r$ with transition monoid $M$ and suppose that $f$ is a superadditive mortality function for $M$. Then there is a word of length at most $f(n - r)$ having rank $r$.

So if $n^2$ is a universal mortality function (which I don’t believe), then the Černý-Pin conjecture is true.

Almeida and I have obtained quadratic mortality bounds for a large class of monoids.

For this talk, we restrict our attention to a special case of our results.
A function $f : \mathbb{N} \to \mathbb{N}$ is superadditive if
\[ f(m) + f(n) \leq f(m + n). \]

The following result was inspired by Rystsov’s argument.

Theorem (Almeida, BS)

Let $A$ be an $n$-state automaton of rank $r$ with transition monoid $M$ and suppose that $f$ is a superadditive mortality function for $M$. Then there is a word of length at most $f(n - r)$ having rank $r$.

So if $n^2$ is a universal mortality function (which I don’t believe), then the Černý-Pin conjecture is true.

Almeida and I have obtained quadratic mortality bounds for a large class of monoids.

For this talk, we restrict our attention to a special case of our results.
A function $f : \mathbb{N} \rightarrow \mathbb{N}$ is superadditive if
\[ f(m) + f(n) \leq f(m + n). \]

The following result was inspired by Rystsov’s argument.

**Theorem (Almeida, BS)**

Let $\mathcal{A}$ be an $n$-state automaton of rank $r$ with transition monoid $M$ and suppose that $f$ is a superadditive mortality function for $M$. Then there is a word of length at most $f(n - r)$ having rank $r$.

So if $n^2$ is a universal mortality function (which I don’t believe), then the Černý-Pin conjecture is true.

Almeida and I have obtained quadratic mortality bounds for a large class of monoids.

For this talk, we restrict our attention to a special case of our results.
A function $f : \mathbb{N} \to \mathbb{N}$ is superadditive if
$$f(m) + f(n) \leq f(m + n).$$

The following result was inspired by Rystsov’s argument.

**Theorem (Almeida, BS)**

Let $A$ be an $n$-state automaton of rank $r$ with transition monoid $M$ and suppose that $f$ is a superadditive mortality function for $M$. Then there is a word of length at most $f(n - r)$ having rank $r$.

So if $n^2$ is a universal mortality function (which I don’t believe), then the Černý-Pin conjecture is true.

Almeida and I have obtained quadratic mortality bounds for a large class of monoids.

For this talk, we restrict our attention to a special case of our results.
A function \( f : \mathbb{N} \to \mathbb{N} \) is superadditive if
\[
  f(m) + f(n) \leq f(m + n).
\]
The following result was inspired by Rystsov’s argument.

**Theorem (Almeida, BS)**

Let \( \mathcal{A} \) be an \( n \)-state automaton of rank \( r \) with transition monoid \( M \) and suppose that \( f \) is a superadditive mortality function for \( M \).

Then there is a word of length at most \( f(n - r) \) having rank \( r \).

So if \( n^2 \) is a universal mortality function (which I don’t believe), then the Černý-Pin conjecture is true.

Almeida and I have obtained quadratic mortality bounds for a large class of monoids.

For this talk, we restrict our attention to a special case of our results.
A function $f : \mathbb{N} \to \mathbb{N}$ is superadditive if
\[ f(m) + f(n) \leq f(m + n). \]
The following result was inspired by Rystsov’s argument.

**Theorem (Almeida, BS)**

Let $\mathcal{A}$ be an $n$-state automaton of rank $r$ with transition monoid $M$ and suppose that $f$ is a superadditive mortality function for $M$. Then there is a word of length at most $f(n - r)$ having rank $r$.

So if $n^2$ is a universal mortality function (which I don’t believe), then the Černý-Pin conjecture is true.

Almeida and I have obtained quadratic mortality bounds for a large class of monoids.

For this talk, we restrict our attention to a special case of our results.
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let $A = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.
- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.
- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i \rho(a) = e_{i.a}$.
- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.
- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.
- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.
- Moreover, $V_0$ is invariant under $M$. 
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let $\mathcal{A} = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.
- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.
- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i \rho(a) = e_{i.a}$.
- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.
- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.
- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.
- Moreover, $V_0$ is invariant under $M$. 
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let $\mathcal{A} = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.
- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.
- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i \rho(a) = e_{i \cdot a}$.
- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.
- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.
- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.
- Moreover, $V_0$ is invariant under $M$. 
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let $\mathcal{A} = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.
- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.
- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i \rho(a) = e_i \cdot a$.
- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.
- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.
- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.
- Moreover, $V_0$ is invariant under $M$. 
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let \( \mathcal{A} = (Q, \Sigma) \) be an \( n \)-state automaton with transition monoid \( M \) and assume \( Q = \{1, \ldots, n\} \).
- Let \( e_1, \ldots, e_n \) be the standard basis of row vectors for \( \mathbb{Q}^n \).
- To each \( a \in \Sigma \), associate the linear transformation \( \rho(a) \) given by \( e_i \rho(a) = e_{i \cdot a} \).
- This induces an action of \( M \) on \( \mathbb{Q}^n \) by linear maps.
- Let \( V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\} \).
- \( V_0 \) is a hyperplane with basis \( \{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\} \), so it has dimension \( n - 1 \).
- Moreover, \( V_0 \) is invariant under \( M \).
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let $\mathcal{A} = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.
- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.
- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i\rho(a) = e_i \cdot a$.
- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.
- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.
- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.
- Moreover, $V_0$ is invariant under $M$. 
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.
- Let $\mathcal{A} = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.
- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.
- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i \rho(a) = e_i \cdot a$.
- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.
- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.
- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.
- Moreover, $V_0$ is invariant under $M$. 
A proof for the synchronizing case

- We outline a proof of the theorem for the synchronizing case, as it is much easier.

- Let $\mathcal{A} = (Q, \Sigma)$ be an $n$-state automaton with transition monoid $M$ and assume $Q = \{1, \ldots, n\}$.

- Let $e_1, \ldots, e_n$ be the standard basis of row vectors for $\mathbb{Q}^n$.

- To each $a \in \Sigma$, associate the linear transformation $\rho(a)$ given by $e_i \rho(a) = e_{i \cdot a}$.

- This induces an action of $M$ on $\mathbb{Q}^n$ by linear maps.

- Let $V_0 = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n \mid c_1 + \cdots + c_n = 0\} = \text{Span}\{e_i - e_j \mid 1 \leq i < j \leq n\}$.

- $V_0$ is a hyperplane with basis $\{e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n\}$, so it has dimension $n - 1$.

- Moreover, $V_0$ is invariant under $M$. 
We claim that $w \in \Sigma^*$ is a synchronizing word iff $\rho(w)|_{V_0} = 0$.

Indeed, $(e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w$.

So $\rho(w)$ annihilates $V_0$ iff $i \cdot w = j \cdot w$ for all $1 \leq i < j \leq n$.

But this occurs iff $|Q \cdot w| = 1$, i.e., $w$ is a reset word.

It now follows that if $f$ is a mortality function for $M$, then there is a reset word $w$ for $\mathcal{A}$ of length at most $f(n - 1)$.

Notice that for the synchronizing case the superadditivity of $f$ is not required.

Our argument for the Pin conjecture requires it.
We claim that $w \in \Sigma^*$ is a synchronizing word iff $\rho(w)|_{V_0} = 0$.

Indeed, $(e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w$.

So $\rho(w)$ annihilates $V_0$ iff $i \cdot w = j \cdot w$ for all $1 \leq i < j \leq n$.

But this occurs iff $|Q \cdot w| = 1$, i.e., $w$ is a reset word.

It now follows that if $f$ is a mortality function for $M$, then there is a reset word $w$ for $\mathcal{A}$ of length at most $f(n - 1)$.

Notice that for the synchronizing case the superadditivity of $f$ is not required.

Our argument for the Pin conjecture requires it.
We claim that $w \in \Sigma^*$ is a synchronizing word iff $\rho(w)|_{V_0} = 0$.

Indeed, $(e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w$.

So $\rho(w)$ annihilates $V_0$ iff $i \cdot w = j \cdot w$ for all $1 \leq i < j \leq n$.

But this occurs iff $|Q \cdot w| = 1$, i.e., $w$ is a reset word.

It now follows that if $f$ is a mortality function for $M$, then there is a reset word $w$ for $A$ of length at most $f(n - 1)$.

Notice that for the synchronizing case the superadditivity of $f$ is not required.

Our argument for the Pin conjecture requires it.
A proof for the synchronizing case II

- We claim that \( w \in \Sigma^* \) is a synchronizing word iff \( \rho(w)|_{V_0} = 0 \).
- Indeed, \( (e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w \).
- So \( \rho(w) \) annihilates \( V_0 \) iff \( i \cdot w = j \cdot w \) for all \( 1 \leq i < j \leq n \).
- But this occurs iff \( |Q \cdot w| = 1 \), i.e., \( w \) is a reset word.
- It now follows that if \( f \) is a mortality function for \( M \), then there is a reset word \( w \) for \( \mathcal{A} \) of length at most \( f(n - 1) \).
- Notice that for the synchronizing case the superadditivity of \( f \) is not required.
- Our argument for the Pin conjecture requires it.
We claim that $w \in \Sigma^*$ is a synchronizing word iff $\rho(w)|_{V_0} = 0$.

Indeed, $(e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w$.

So $\rho(w)$ annihilates $V_0$ iff $i \cdot w = j \cdot w$ for all $1 \leq i < j \leq n$.

But this occurs iff $|Q \cdot w| = 1$, i.e., $w$ is a reset word.

It now follows that if $f$ is a mortality function for $M$, then there is a reset word $w$ for $A$ of length at most $f(n - 1)$.

Notice that for the synchronizing case the superadditivity of $f$ is not required.

Our argument for the Pin conjecture requires it.
We claim that $w \in \Sigma^*$ is a synchronizing word iff $\rho(w)|_{V_0} = 0$.

Indeed, $(e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w$.

So $\rho(w)$ annihilates $V_0$ iff $i \cdot w = j \cdot w$ for all $1 \leq i < j \leq n$.

But this occurs iff $|Q \cdot w| = 1$, i.e., $w$ is a reset word.

It now follows that if $f$ is a mortality function for $M$, then there is a reset word $w$ for $A$ of length at most $f(n - 1)$.

Notice that for the synchronizing case the superadditivity of $f$ is not required.

Our argument for the Pin conjecture requires it.
We claim that $w \in \Sigma^*$ is a synchronizing word iff $\rho(w)|_{V_0} = 0$.

Indeed, $(e_i - e_j)\rho(w) = e_i \cdot w - e_j \cdot w$.

So $\rho(w)$ annihilates $V_0$ iff $i \cdot w = j \cdot w$ for all $1 \leq i < j \leq n$.

But this occurs iff $|Q \cdot w| = 1$, i.e., $w$ is a reset word.

It now follows that if $f$ is a mortality function for $M$, then there is a reset word $w$ for $A$ of length at most $f(n - 1)$.

Notice that for the synchronizing case the superadditivity of $f$ is not required.

Our argument for the Pin conjecture requires it.
Let $\rho : M \rightarrow M_n(\mathbb{Q})$ be a representation and put $V = \mathbb{Q}^n$.

A subspace $W \leq V$ is said to be $M$-invariant if $W \rho(M) \subseteq W$.

For example, $V_0$ from the above proof is an $M$-invariant subspace of $V$.

A representation is irreducible if $\{0\}$ and $V$ are the only $M$-invariant subspaces.

Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.

This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida,BS)**

Let $f$ be a superadditive function. Then $f$ is a mortality function for $M$ iff $f$ is a mortality function for each irreducible representation of $M$. 
Let $\rho: M \to M_n(\mathbb{Q})$ be a representation and put $V = \mathbb{Q}^n$.

A subspace $W \leq V$ is said to be $M$-invariant if $W\rho(M) \subseteq W$.

For example, $V_0$ from the above proof is an $M$-invariant subspace of $V$.

A representation is irreducible if $\{0\}$ and $V$ are the only $M$-invariant subspaces.

Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.

This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida,BS)**

Let $f$ be a superadditive function. Then $f$ is a mortality function for $M$ iff $f$ is a mortality function for each irreducible representation of $M$.
Let $\rho : M \to M_n(\mathbb{Q})$ be a representation and put $V = \mathbb{Q}^n$.

A subspace $W \leq V$ is said to be $M$-invariant if $W\rho(M) \subseteq W$.

For example, $V_0$ from the above proof is an $M$-invariant subspace of $V$.

A representation is irreducible if $\{0\}$ and $V$ are the only $M$-invariant subspaces.

Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.

This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida,BS)**

Let $f$ be a superadditive function. Then $f$ is a mortality function for $M$ iff $f$ is a mortality function for each irreducible representation of $M$. 
Let $\rho: M \rightarrow M_n(\mathbb{Q})$ be a representation and put $V = \mathbb{Q}^n$.

A subspace $W \leq V$ is said to be $M$-invariant if $W \rho(M) \subseteq W$.

For example, $V_0$ from the above proof is an $M$-invariant subspace of $V$.

A representation is irreducible if $\{0\}$ and $V$ are the only $M$-invariant subspaces.

Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.

This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida, BS)**

Let $f$ be a superadditive function. Then $f$ is a mortality function for $M$ iff $f$ is a mortality function for each irreducible representation of $M$. 
Let $\rho: M \to M_n(\mathbb{Q})$ be a representation and put $V = \mathbb{Q}^n$.

A subspace $W \leq V$ is said to be $M$-invariant if $W \rho(M) \subseteq W$.

For example, $V_0$ from the above proof is an $M$-invariant subspace of $V$.

A representation is irreducible if $\{0\}$ and $V$ are the only $M$-invariant subspaces.

Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.

This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida,BS)**

Let $f$ be a superadditive function. Then $f$ is a mortality function for $M$ iff $f$ is a mortality function for each irreducible representation of $M$. 
Let \( \rho : M \rightarrow M_n(\mathbb{Q}) \) be a representation and put \( V = \mathbb{Q}^n \).

A subspace \( W \leq V \) is said to be \( M \)-invariant if \( W \rho(M) \subseteq W \).

For example, \( V_0 \) from the above proof is an \( M \)-invariant subspace of \( V \).

A representation is irreducible if \( \{0\} \) and \( V \) are the only \( M \)-invariant subspaces.

Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.

This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida,BS)**

*Let \( f \) be a superadditive function. Then \( f \) is a mortality function for \( M \) iff \( f \) is a mortality function for each irreducible representation of \( M \).*
Let \( \rho: M \to M_n(\mathbb{Q}) \) be a representation and put \( V = \mathbb{Q}^n \).

- A subspace \( W \leq V \) is said to be \( M \)-invariant if \( W \rho(M) \subseteq W \).
- For example, \( V_0 \) from the above proof is an \( M \)-invariant subspace of \( V \).
- A representation is irreducible if \( \{0\} \) and \( V \) are the only \( M \)-invariant subspaces.
- Every representation can be ‘built up’ from irreducible representations in much the same way that every finite group can be ‘built up’ from finite simple groups.
- This allowed us to prove the following result by induction on the dimension.

**Theorem (Almeida,BS)**

Let \( f \) be a superadditive function. Then \( f \) is a mortality function for \( M \) iff \( f \) is a mortality function for each irreducible representation of \( M \).
Irreducible representations

There is a well-developed theory of irreducible representations of finite monoids due to Munn-Ponizovsky and further elaborated by Rhodes and Zalcstein.

In particular, the irreducible representations of a finite monoid $M$ can be constructed from the irreducible representations of its maximal subgroups.

The degrees of the irreducible representations are intimately connected to the Rees matrix representations of the principal factors of $M$, that is, the semigroups of the form $J^0$ with $J$ a regular $\mathcal{J}$-class of $M$. 
There is a well-developed theory of irreducible representations of finite monoids due to Munn-Ponizovsky and further elaborated by Rhodes and Zalcstein.

In particular, the irreducible representations of a finite monoid $M$ can be constructed from the irreducible representations of its maximal subgroups.

The degrees of the irreducible representations are intimately connected to the Rees matrix representations of the principal factors of $M$, that is, the semigroups of the form $J^0$ with $J$ a regular $\mathcal{J}$-class of $M$. 
There is a well-developed theory of irreducible representations of finite monoids due to Munn-Ponizovsky and further elaborated by Rhodes and Zalcstein.

In particular, the irreducible representations of a finite monoid $M$ can be constructed from the irreducible representations of its maximal subgroups.

The degrees of the irreducible representations are intimately connected to the Rees matrix representations of the principal factors of $M$, that is, the semigroups of the form $J^0$ with $J$ a regular $\mathcal{J}$-class of $M$. 
The case of DS

- A finite monoid belongs to the class DS if $e \in MaM \cap MbM$ implies $e \in MabM$ for all idempotents $e \in M$.
- Recall that $e$ is idempotent if $e^2 = e$.
- Equivalently, $M \in DS$ iff $M \times M$ cannot recognize the language $(ab)^*$.
- This class was introduced independently by Putcha and Schützenberger.
- Examples of monoids in DS include:
  - commutative monoids (obvious);
  - monoids satisfying an identity $x^m = x$ (Clifford);
  - monoids of upper triangular matrices over a finite field (Putcha).
- The variety DS appears frequently in the algebraic theory of automata.
A finite monoid belongs to the class $\text{DS}$ if $e \in MaM \cap MbM$ implies $e \in MabM$ for all idempotents $e \in M$.

Recall that $e$ is idempotent if $e^2 = e$.

Equivalently, $M \in \text{DS}$ iff $M \times M$ cannot recognize the language $(ab)^*$.

This class was introduced independently by Putcha and Schützenberger.

Examples of monoids in DS include:

- commutative monoids (obvious);
- monoids satisfying an identity $x^m = x$ (Clifford);
- monoids of upper triangular matrices over a finite field (Putcha).

The variety DS appears frequently in the algebraic theory of automata.
The case of DS

- A finite monoid belongs to the class **DS** if \( e \in MaM \cap MbM \) implies \( e \in MabM \) for all idempotents \( e \in M \).
- Recall that \( e \) is idempotent if \( e^2 = e \).
- Equivalently, \( M \in DS \) iff \( M \times M \) cannot recognize the language \((ab)^*\).
- This class was introduced independently by Putcha and Schützenberger.
- Examples of monoids in DS include:
  - commutative monoids (obvious);
  - monoids satisfying an identity \( x^m = x \) (Clifford);
  - monoids of upper triangular matrices over a finite field (Putcha).
- The variety DS appears frequently in the algebraic theory of automata.
The case of DS

- A finite monoid belongs to the class DS if \( e \in MaM \cap MbM \) implies \( e \in MabM \) for all idempotents \( e \in M \).
- Recall that \( e \) is idempotent if \( e^2 = e \).
- Equivalently, \( M \in DS \) iff \( M \times M \) cannot recognize the language \((ab)^*\).
- This class was introduced independently by Putcha and Schützenberger.
- Examples of monoids in DS include:
  - commutative monoids (obvious);
  - monoids satisfying an identity \( x^m = x \) (Clifford);
  - monoids of upper triangular matrices over a finite field (Putcha).
- The variety DS appears frequently in the algebraic theory of automata.
A finite monoid belongs to the class DS if \( e \in M a M \cap M b M \) implies \( e \in M a b M \) for all idempotents \( e \in M \).

Recall that \( e \) is idempotent if \( e^2 = e \).

Equivalently, \( M \in DS \) iff \( M \times M \) cannot recognize the language \((ab)^*\).

This class was introduced independently by Putcha and Schützenberger.

Examples of monoids in DS include:

- commutative monoids (obvious);
- monoids satisfying an identity \( x^m = x \) (Clifford);
- monoids of upper triangular matrices over a finite field (Putcha).

The variety DS appears frequently in the algebraic theory of automata.
A finite monoid belongs to the class \textbf{DS} if \( e \in MaM \cap MbM \) implies \( e \in MabM \) for all idempotents \( e \in M \).

Recall that \( e \) is \textbf{idempotent} if \( e^2 = e \).

Equivalently, \( M \in \text{DS} \) iff \( M \times M \) cannot recognize the language \((ab)^*\).

This class was introduced independently by Putcha and Schützenberger.

Examples of monoids in DS include:

- commutative monoids (obvious);
- monoids satisfying an identity \( x^m = x \) (Clifford);
- monoids of upper triangular matrices over a finite field (Putcha).

The variety DS appears frequently in the algebraic theory of automata.
The case of DS

- A finite monoid belongs to the class **DS** if $e \in MaM \cap MbM$ implies $e \in MabM$ for all idempotents $e \in M$.
- Recall that $e$ is **idempotent** if $e^2 = e$.
- Equivalently, $M \in \text{DS}$ iff $M \times M$ cannot recognize the language $(ab)^*$. 
- This class was introduced independently by Putcha and Schützenberger.
- **Examples of monoids in DS** include:
  - commutative monoids (obvious);
  - monoids satisfying an identity $x^m = x$ (Clifford);
  - monoids of upper triangular matrices over a finite field (Putcha).
- The variety DS appears frequently in the algebraic theory of automata.
A finite monoid belongs to the class \textbf{DS} if \( e \in MaM \cap MbM \) implies \( e \in MabM \) for all idempotents \( e \in M \).

Recall that \( e \) is \textit{idempotent} if \( e^2 = e \).

Equivalently, \( M \in \text{DS} \) iff \( M \times M \) cannot recognize the language \((ab)^*\).

This class was introduced independently by Putcha and Schützenberger.

Examples of monoids in DS include:

- commutative monoids (obvious);
- monoids satisfying an identity \( x^m = x \) (Clifford);
- monoids of upper triangular matrices over a finite field (Putcha).

The variety DS appears frequently in the algebraic theory of automata.
A finite monoid belongs to the class **DS** if \( e \in MaM \cap MbM \) implies \( e \in MabM \) for all idempotents \( e \in M \).

Recall that \( e \) is idempotent if \( e^2 = e \).

Equivalently, \( M \in DS \) iff \( M \times M \) cannot recognize the language \((ab)^*\).

This class was introduced independently by Putcha and Schützenberger.

Examples of monoids in DS include:
- commutative monoids (obvious);
- monoids satisfying an identity \( x^m = x \) (Clifford);
- monoids of upper triangular matrices over a finite field (Putcha).

The variety DS appears frequently in the algebraic theory of automata.
In previous work, we showed with Almeida, Margolis and Volkov that the Černý conjecture holds for automata with transition monoid in DS using representation theory.

Volkov asked in LATA 2008 whether the bound of \((n - 1)^2\) was tight for this class.

The main ingredient in our proof was the following result.

**Lemma (AMSV)**

If \(\rho: M \rightarrow M_n(\mathbb{Q})\) is an irreducible representation of a monoid in DS such that \(0 \in \rho(M)\) and \(\Sigma\) is a generating set for \(M\), then there is a letter \(a \in \Sigma\) with \(\rho(a) = 0\).

Consequently, \(f(n) = n\) is a superadditive mortality function for DS.
In previous work, we showed with Almeida, Margolis and Volkov that the Černý conjecture holds for automata with transition monoid in DS using representation theory.

Volkov asked in LATA 2008 whether the bound of \((n - 1)^2\) was tight for this class.

The main ingredient in our proof was the following result.

### Lemma (AMSV)

If \(\rho: M \to M_n(\mathbb{Q})\) is an irreducible representation of a monoid in DS such that \(0 \in \rho(M)\) and \(\Sigma\) is a generating set for \(M\), then there is a letter \(a \in \Sigma\) with \(\rho(a) = 0\).

Consequently, \(f(n) = n\) is a superadditive mortality function for DS.
In previous work, we showed with Almeida, Margolis and Volkov that the Černý conjecture holds for automata with transition monoid in DS using representation theory. Volkov asked in LATA 2008 whether the bound of \((n - 1)^2\) was tight for this class. The main ingredient in our proof was the following result.

**Lemma (AMSV)**

If \(\rho: M \rightarrow M_n(\mathbb{Q})\) is an irreducible representation of a monoid in DS such that \(0 \in \rho(M)\) and \(\Sigma\) is a generating set for \(M\), then there is a letter \(a \in \Sigma\) with \(\rho(a) = 0\).  

Consequently, \(f(n) = n\) is a superadditive mortality function for DS.
The case of DS II

- In previous work, we showed with Almeida, Margolis and Volkov that the Černý conjecture holds for automata with transition monoid in DS using representation theory.
- Volkov asked in LATA 2008 whether the bound of \((n - 1)^2\) was tight for this class.
- The main ingredient in our proof was the following result.

**Lemma (AMSV)**

If \(\rho: M \rightarrow M_n(\mathbb{Q})\) is an irreducible representation of a monoid in DS such that \(0 \in \rho(M)\) and \(\Sigma\) is a generating set for \(M\), then there is a letter \(a \in \Sigma\) with \(\rho(a) = 0\).

- Consequently, \(f(n) = n\) is a superadditive mortality function for DS.
In previous work, we showed with Almeida, Margolis and Volkov that the Černý conjecture holds for automata with transition monoid in DS using representation theory.

Volkov asked in LATA 2008 whether the bound of \((n - 1)^2\) was tight for this class.

The main ingredient in our proof was the following result.

**Lemma (AMSV)**

If \(\rho: M \rightarrow M_n(\mathbb{Q})\) is an irreducible representation of a monoid in DS such that \(0 \in \rho(M)\) and \(\Sigma\) is a generating set for \(M\), then there is a letter \(a \in \Sigma\) with \(\rho(a) = 0\).

Consequently, \(f(n) = n\) is a superadditive mortality function for DS.
The Černý-Pin conjecture for DS

Theorem (Almeida, BS)

If $A$ is an $n$-state, rank $r$ automaton with transition monoid in DS, then there is a word $w$ of length at most $n - r$ with $rk(w) = r$.

- This bound is easily seen to be sharp by considering automata over unary alphabets.
- For instance,

$$
\begin{array}{c}
\circ 1 \xrightarrow{a} \circ 2 \xrightarrow{a} \cdots \xrightarrow{a} \circ n
\end{array}
$$

is synchronizing with minimum length reset word $a^{n-1}$ and the transition monoid is commutative.
The Černý-Pin conjecture for DS

Theorem (Almeida, BS)

If $A$ is an $n$-state, rank $r$ automaton with transition monoid in DS, then there is a word $w$ of length at most $n - r$ with $rk(w) = r$.

- This bound is easily seen to be sharp by considering automata over unary alphabets.
- For instance,

\[
\begin{array}{c}
1 \xrightarrow{a} 2 \xrightarrow{a} \cdots \xrightarrow{a} n \\
\end{array}
\]

is synchronizing with minimum length reset word $a^{n-1}$ and the transition monoid is commutative.
The Černý-Pin conjecture for DS

Theorem (Almeida, BS)

If $A$ is an $n$-state, rank $r$ automaton with transition monoid in DS, then there is a word $w$ of length at most $n - r$ with $rk(w) = r$.

- This bound is easily seen to be sharp by considering automata over unary alphabets.
- For instance, 

$$
\begin{array}{cccc}
1 & \rightarrow & 2 & \rightarrow \\
& & \cdot & \\
& & \cdot & \\
& & \cdot & \\
& & \cdot & \\
& & \cdot & \\
& & \cdot & \\
\end{array}
$$

is synchronizing with minimum length reset word $a^{n-1}$ and the transition monoid is commutative.
The class EDS

- A finite monoid belongs to the class EDS if its idempotents generate a submonoid in DS.
- $\text{DS} \subseteq \text{EDS}$.
- Monoids with commuting idempotents (such as inverse monoids) belong to EDS.
- More generally, monoids whose idempotents form a submonoid belong to EDS.
- It is known that a monoid $M$ belongs to EDS iff it cannot recognize the language $\{a, b\}^* ab \{a, b\}^*$.
- Equivalently, EDS is the largest variety of monoids that cannot recognize all 2-testable languages.
The class EDS

- A finite monoid belongs to the class EDS if its idempotents generate a submonoid in DS.
- $DS \subseteq EDS$.
- Monoids with commuting idempotents (such as inverse monoids) belong to EDS.
- More generally, monoids whose idempotents form a submonoid belong to EDS.
- It is known that a monoid $M$ belongs to EDS iff it cannot recognize the language $\{a,b\}^*ab\{a,b\}^*$.
- Equivalently, EDS is the largest variety of monoids that cannot recognize all 2-testable languages.
A finite monoid belongs to the class EDS if its idempotents generate a submonoid in DS.

\[ DS \subseteq EDS. \]

Monoids with commuting idempotents (such as inverse monoids) belong to EDS.

More generally, monoids whose idempotents form a submonoid belong to EDS.

It is known that a monoid \( M \) belongs to EDS iff it cannot recognize the language \( \{a, b\}^*ab\{a, b\}^* \).

Equivalently, EDS is the largest variety of monoids that cannot recognize all 2-testable languages.
A finite monoid belongs to the class EDS if its idempotents generate a submonoid in DS.

DS ⊆ EDS.

Monoids with commuting idempotents (such as inverse monoids) belong to EDS.

More generally, monoids whose idempotents form a submonoid belong to EDS.

It is known that a monoid $M$ belongs to EDS iff it cannot recognize the language $\{a, b\}^*ab\{a, b\}^*$.

Equivalently, EDS is the largest variety of monoids that cannot recognize all 2-testable languages.
A finite monoid belongs to the class EDS if its idempotents generate a submonoid in DS.

\[ DS \subseteq EDS. \]

Monoids with commuting idempotents (such as inverse monoids) belong to EDS.

More generally, monoids whose idempotents form a submonoid belong to EDS.

It is known that a monoid \( M \) belongs to EDS iff it cannot recognize the language \( \{a, b\}^*ab\{a, b\}^* \).

Equivalently, EDS is the largest variety of monoids that cannot recognize all 2-testable languages.
A finite monoid belongs to the class EDS if its idempotents generate a submonoid in DS.

**DS \subseteq EDS.**

Monoids with commuting idempotents (such as inverse monoids) belong to EDS.

More generally, monoids whose idempotents form a submonoid belong to EDS.

It is known that a monoid $M$ belongs to EDS iff it cannot recognize the language $\{a, b\}^*ab\{a, b\}^*$.

Equivalently, EDS is the largest variety of monoids that cannot recognize all 2-testable languages.
The case of EDS

- Suppose that $M$ is a $\Sigma$-generated finite monoid.
- The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho: M \to M_n(\mathbb{Q})$ of $M$ a finite automaton $\mathcal{A}(\rho)$ over $\Sigma$.
- $0 \in \rho(M)$ iff $\mathcal{A}(\rho)$ is synchronizing with a sink state.
- The 0-words for the representation are precisely the reset words for the automaton.
- When $M \in \text{EDS}$, Almeida and I showed that $\mathcal{A}(\rho)$ has at most $n + 1$ states.
- Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m - 1)/2$ (and this bound is sharp).
- Consequently, $f(n) = n(n + 1)/2$ is a superadditive mortality function for EDS.
The case of EDS

- Suppose that $M$ is a $\Sigma$-generated finite monoid.
- The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho: M \rightarrow M_n(\mathbb{Q})$ of $M$ a finite automaton $A(\rho)$ over $\Sigma$.

- $0 \in \rho(M)$ iff $A(\rho)$ is synchronizing with a sink state.
- The 0-words for the representation are precisely the reset words for the automaton.
- When $M \in$ EDS, Almeida and I showed that $A(\rho)$ has at most $n + 1$ states.
- Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m - 1)/2$ (and this bound is sharp).
- Consequently, $f(n) = n(n + 1)/2$ is a superadditive mortality function for EDS.
The case of EDS

- Suppose that $M$ is a $\Sigma$-generated finite monoid.
- The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho : M \to M_n(\mathbb{Q})$ of $M$ a finite automaton $\mathcal{A}(\rho)$ over $\Sigma$.
- $0 \in \rho(M)$ iff $\mathcal{A}(\rho)$ is synchronizing with a sink state.
- The 0-words for the representation are precisely the reset words for the automaton.
- When $M \in EDS$, Almeida and I showed that $\mathcal{A}(\rho)$ has at most $n + 1$ states.
- Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m - 1)/2$ (and this bound is sharp).
- Consequently, $f(n) = n(n + 1)/2$ is a superadditive mortality function for EDS.
The case of EDS

- Suppose that $M$ is a $\Sigma$-generated finite monoid.
- The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho: M \to M_n(\mathbb{Q})$ of $M$ a finite automaton $A(\rho)$ over $\Sigma$.
- $0 \in \rho(M)$ iff $A(\rho)$ is synchronizing with a sink state.
- The 0-words for the representation are precisely the reset words for the automaton.
- When $M \in \text{EDS}$, Almeida and I showed that $A(\rho)$ has at most $n + 1$ states.
- Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m - 1)/2$ (and this bound is sharp).
- Consequently, $f(n) = n(n + 1)/2$ is a superadditive mortality function for EDS.
Suppose that $M$ is a $\Sigma$-generated finite monoid.

The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho: M \to M_n(\mathbb{Q})$ of $M$ a finite automaton $A(\rho)$ over $\Sigma$.

$0 \in \rho(M)$ iff $A(\rho)$ is synchronizing with a sink state.

The 0-words for the representation are precisely the reset words for the automaton.

When $M \in \text{EDS}$, Almeida and I showed that $A(\rho)$ has at most $n + 1$ states.

Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m - 1)/2$ (and this bound is sharp).

Consequently, $f(n) = n(n + 1)/2$ is a superadditive mortality function for EDS.
The case of EDS

- Suppose that $M$ is a $\Sigma$-generated finite monoid.
- The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho: M \to M_n(\mathbb{Q})$ of $M$ a finite automaton $A(\rho)$ over $\Sigma$.
- $0 \in \rho(M)$ iff $A(\rho)$ is synchronizing with a sink state.
- The 0-words for the representation are precisely the reset words for the automaton.
- When $M \in \text{EDS}$, Almeida and I showed that $A(\rho)$ has at most $n + 1$ states.
- Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m - 1)/2$ (and this bound is sharp).
- Consequently, $f(n) = n(n + 1)/2$ is a superadditive mortality function for EDS.
The case of EDS

- Suppose that $M$ is a $\Sigma$-generated finite monoid.
- The Rhodes-Zalcstein theory allows us to associate to each irreducible representation $\rho: M \to M_n(\mathbb{Q})$ of $M$ a finite automaton $A(\rho)$ over $\Sigma$.
- $0 \in \rho(M)$ iff $A(\rho)$ is synchronizing with a sink state.
- The 0-words for the representation are precisely the reset words for the automaton.
- When $M \in \text{EDS}$, Almeida and I showed that $A(\rho)$ has at most $n+1$ states.
- Rystsov showed that, for $m$-state synchronizing automata with sink state, there is a synchronizing word of length at most $m(m-1)/2$ (and this bound is sharp).
- Consequently, $f(n) = n(n+1)/2$ is a superadditive mortality function for EDS.
The Černý-Pin conjecture for EDS

**Theorem (Almeida, BS)**

If $\mathcal{A}$ is an $n$-state, rank $r$ automaton with transition monoid in EDS, then there is a word $w$ of length at most

$$\frac{(n - r)(n - r + 1)}{2}$$

with $\text{rk}(w) = r$.

- The bound of $n(n - 1)/2$ is sharp for the Černý conjecture.
- Rystsov has an example of an $n$-state synchronizing automaton with minimal length reset word of length $n(n - 1)/2$ whose transition monoid has commuting idempotents.
- Our method works much more generally than for EDS.
- For instance $n(n + 1)/2$ is a mortality function for $M_k(\mathbb{F}_q)$ and the partial transformation monoids $PT_k$. 
The Černý-Pin conjecture for EDS

Theorem (Almeida, BS)

If $A$ is an $n$-state, rank $r$ automaton with transition monoid in EDS, then there is a word $w$ of length at most

$$\frac{(n - r)(n - r + 1)}{2}$$

with $\text{rk}(w) = r$.

- The bound of $n(n - 1)/2$ is sharp for the Černý conjecture.
- Rystsov has an example of an $n$-state synchronizing automaton with minimal length reset word of length $n(n - 1)/2$ whose transition monoid has commuting idempotents.
- Our method works much more generally than for EDS.
- For instance $n(n + 1)/2$ is a mortality function for $M_k(\mathbb{F}_q)$ and the partial transformation monoids $PT_k$. 
The Černý-Pin conjecture for EDS

Theorem (Almeida, BS)

If \( \mathcal{A} \) is an \( n \)-state, rank \( r \) automaton with transition monoid in EDS, then there is a word \( w \) of length at most

\[
\frac{(n - r)(n - r + 1)}{2}
\]

with \( \text{rk}(w) = r \).

- The bound of \( n(n - 1)/2 \) is sharp for the Černý conjecture.
- Rystsov has an example of an \( n \)-state synchronizing automaton with minimal length reset word of length \( n(n - 1)/2 \) whose transition monoid has commuting idempotents.
- Our method works much more generally than for EDS.
- For instance \( n(n + 1)/2 \) is a mortality function for \( M_k(\mathbb{F}_q) \) and the partial transformation monoids \( PT_k \).
The Černý-Pin conjecture for EDS

**Theorem (Almeida, BS)**

If \( \mathcal{A} \) is an \( n \)-state, rank \( r \) automaton with transition monoid in EDS, then there is a word \( w \) of length at most

\[
\frac{(n - r)(n - r + 1)}{2}
\]

with \( \text{rk}(w) = r \).

- The bound of \( n(n - 1)/2 \) is sharp for the Černý conjecture.
- Rystsov has an example of an \( n \)-state synchronizing automaton with minimal length reset word of length \( n(n - 1)/2 \) whose transition monoid has commuting idempotents.
- Our method works much more generally than for EDS.
- For instance \( n(n + 1)/2 \) is a mortality function for \( M_k(\mathbb{F}_q) \) and the partial transformation monoids \( PT_k \).
The Černý-Pin conjecture for EDS

Theorem (Almeida, BS)

If $A$ is an $n$-state, rank $r$ automaton with transition monoid in EDS, then there is a word $w$ of length at most

$$\frac{(n - r)(n - r + 1)}{2}$$

with $rk(w) = r$.

- The bound of $n(n - 1)/2$ is sharp for the Černý conjecture.
- Rystsov has an example of an $n$-state synchronizing automaton with minimal length reset word of length $n(n - 1)/2$ whose transition monoid has commuting idempotents.
- Our method works much more generally than for EDS.
- For instance $n(n + 1)/2$ is a mortality function for $M_k(\mathbb{F}_q)$ and the partial transformation monoids $PT_k$. 
Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.

On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.

If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.

So if we can remove the dependence on the number of generators, we are done.

The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.

For the irreducible case, the number of generators is irrelevant.

So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
A universal mortality function

- Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.

- On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.

- If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.

- So if we can remove the dependence on the number of generators, we are done.

- The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.

- For the irreducible case, the number of generators is irrelevant.

- So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
A universal mortality function

- Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.
- On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.
- If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.
- So if we can remove the dependence on the number of generators, we are done.
- The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.
- For the irreducible case, the number of generators is irrelevant.
- So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
A universal mortality function

- Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.
- On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.
- If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.
- So if we can remove the dependence on the number of generators, we are done.
- The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.
- For the irreducible case, the number of generators is irrelevant.
- So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.

On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.

If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.

So if we can remove the dependence on the number of generators, we are done.

The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.

For the irreducible case, the number of generators is irrelevant.

So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
A universal mortality function

- Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.

- On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.

- If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.

- So if we can remove the dependence on the number of generators, we are done.

- The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.

- For the irreducible case, the number of generators is irrelevant.

- So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
A universal mortality function

- Given the undecidability of the Matrix Mortality Problem for $3 \times 3$ integer matrices, it is not altogether clear that a universal mortality function exists.
- On the other hand, Simon/Mandel and Jacob independently proved that there is a recursive bound on the order of a finite $k$-generated submonoid of $M_n(\mathbb{Q})$.
- If a monoid $M$ contains 0, then 0 can be represented by a word of length $|M| - 1$.
- So if we can remove the dependence on the number of generators, we are done.
- The results of Simon/Mandel and Jacob rely on the solution to the Burnside problem for matrix semigroups.
- For the irreducible case, the number of generators is irrelevant.
- So by working a little harder to get a superadditive bound in the irreducible case, we proved the following theorem.
A universal mortality function II

Theorem (Almeida, BS)

The function

\[ f(n) = \begin{cases} 
1 & n = 1 \\
(2n - 1)^{n^2} - 1 & n > 1 
\end{cases} \]

is a superadditive universal mortality function.

- We know this upper bound is not tight.
- The best lower bound we have is \( n^2 \).
- For aperiodic monoids, we can now prove \( 2^n - 1 \) is a mortality function (the article in the Proceedings has \( 2^{n^2} - 1 \)).
Theorem (Almeida, BS)

The function

\[
f(n) = \begin{cases} 
1 & n = 1 \\
(2n - 1)^{n^2} - 1 & n > 1 
\end{cases}
\]

is a superadditive universal mortality function.

- We know this upper bound is not tight.
- The best lower bound we have is \( n^2 \).
- For aperiodic monoids, we can now prove \( 2^n - 1 \) is a mortality function (the article in the Proceedings has \( 2^{n^2} - 1 \)).
Theorem (Almeida, BS)

The function

\[
f(n) = \begin{cases} 
1 & n = 1 \\
(2n - 1)^{n^2} - 1 & n > 1 
\end{cases}
\]

is a superadditive universal mortality function.

- We know this upper bound is not tight.
- The best lower bound we have is \( n^2 \).
- For aperiodic monoids, we can now prove \( 2^n - 1 \) is a mortality function (the article in the Proceedings has \( 2^{n^2} - 1 \)).
Theorem (Almeida, BS)

The function

\[
f(n) = \begin{cases} 
1 & n = 1 \\
(2n - 1)n^2 - 1 & n > 1 
\end{cases}
\]

is a superadditive universal mortality function.

- We know this upper bound is not tight.
- The best lower bound we have is \( n^2 \).
- For aperiodic monoids, we can now prove \( 2^n - 1 \) is a mortality function (the article in the Proceedings has \( 2^{n^2} - 1 \)).
And Now For Something Completely Different
A Larch...
And Now For Something Completely Different

A Larch...
And Now For Something Completely Different

A Larch...
Now I want to focus on some aspects of Černý’s conjecture related to Pin and Dubuc’s theorems.

This part of the talk is not in the Proceedings and is my own work.

Theorem (Pin ’78)

Let $\mathcal{A} = (Q, \Sigma)$ be a synchronizing automaton so that $|Q|$ is a prime $p$ and some element of $\Sigma$ cyclically permutes $Q$. Then:

1. $\mathcal{A}$ is synchronizing if and only if $\Sigma$ contains a non-permutation;
2. In this case, $\mathcal{A}$ has a reset word of length at most $(p - 1)^2$. 

Now I want to focus on some aspects of Černý’s conjecture related to Pin and Dubuc’s theorems.

This part of the talk is not in the Proceedings and is my own work.

**Theorem (Pin '78)**

Let $\mathcal{A} = (Q, \Sigma)$ be a synchronizing automaton so that $|Q|$ is a prime $p$ and some element of $\Sigma$ cyclically permutes $Q$. Then:

1. $\mathcal{A}$ is synchronizing if and only if $\Sigma$ contains a non-permutation;
2. In this case, $\mathcal{A}$ has a reset word of length at most $(p - 1)^2$. 
Now I want to focus on some aspects of Černý’s conjecture related to Pin and Dubuc’s theorems.

This part of the talk is not in the Proceedings and is my own work.

**Theorem (Pin ’78)**

Let $\mathcal{A} = (Q, \Sigma)$ be a synchronizing automaton so that $|Q|$ is a prime $p$ and some element of $\Sigma$ cyclically permutes $Q$. Then:

1. $\mathcal{A}$ is synchronizing if and only if $\Sigma$ contains a non-permutation;
2. In this case, $\mathcal{A}$ has a reset word of length at most $(p - 1)^2$. 

<table>
<thead>
<tr>
<th>Theorem (Pin ’78)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{A} = (Q, \Sigma)$ be a synchronizing automaton so that $</td>
</tr>
<tr>
<td>1. $\mathcal{A}$ is synchronizing if and only if $\Sigma$ contains a non-permutation;</td>
</tr>
<tr>
<td>2. In this case, $\mathcal{A}$ has a reset word of length at most $(p - 1)^2$.</td>
</tr>
</tbody>
</table>
Now I want to focus on some aspects of Černý’s conjecture related to Pin and Dubuc’s theorems.

This part of the talk is not in the Proceedings and is my own work.

**Theorem (Pin ’78)**

Let $A = (Q, \Sigma)$ be a synchronizing automaton so that $|Q|$ is a prime $p$ and some element of $\Sigma$ cyclically permutes $Q$. Then:

1. $A$ is synchronizing if and only if $\Sigma$ contains a non-permutation;

2. In this case, $A$ has a reset word of length at most $(p - 1)^2$. 

---

**Pin’s Theorem**
Now I want to focus on some aspects of Černý’s conjecture related to Pin and Dubuc’s theorems.

This part of the talk is not in the Proceedings and is my own work.

**Theorem (Pin ’78)**

Let $A = (Q, \Sigma)$ be a synchronizing automaton so that $|Q|$ is a prime $p$ and some element of $\Sigma$ cyclically permutes $Q$. Then:

1. $A$ is synchronizing if and only if $\Sigma$ contains a non-permutation;
2. In this case, $A$ has a reset word of length at most $(p - 1)^2$. 
Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group. A permutation group $G \subseteq S_n$ is called synchronizing if, for all non-permutations $t$ of $\{1, \ldots, n\}$, the automaton $(\{1, \ldots, n\}, G \cup \{t\})$ is synchronizing. Pin’s Theorem implies that cyclic groups of prime order are synchronizing. It is easy to see that 2-transitive groups are synchronizing. With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results. João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation. Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group. A permutation group $G \subseteq S_n$ is called synchronizing if, for all non-permutations $t$ of $\{1, \ldots, n\}$, the automaton $(\{1, \ldots, n\}, G \cup \{t\})$ is synchronizing.

Pin’s Theorem implies that cyclic groups of prime order are synchronizing.

It is easy to see that 2-transitive groups are synchronizing.

With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results.

João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation.

Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Synchronizing groups

Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group.

A permutation group $G \subseteq S_n$ is called synchronizing if, for all non-permutations $t$ of $\{1, \ldots, n\}$, the automaton $(\{1, \ldots, n\}, G \cup \{t\})$ is synchronizing.

Pin’s Theorem implies that cyclic groups of prime order are synchronizing.

It is easy to see that 2-transitive groups are synchronizing.

With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results.

João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation.

Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group.

A permutation group \( G \subseteq S_n \) is called synchronizing if, for all non-permutations \( t \) of \( \{1, \ldots, n\} \), the automaton \( (\{1, \ldots, n\}, G \cup \{t\}) \) is synchronizing.

Pin’s Theorem implies that cyclic groups of prime order are synchronizing.

It is easy to see that 2-transitive groups are synchronizing.

With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results.

João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation.

Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group.

A permutation group $G \subseteq S_n$ is called synchronizing if, for all non-permutations $t$ of $\{1, \ldots, n\}$, the automaton $(\{1, \ldots, n\}, G \cup \{t\})$ is synchronizing.

Pin’s Theorem implies that cyclic groups of prime order are synchronizing.

It is easy to see that 2-transitive groups are synchronizing.

With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results.

João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation.

Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group.

A permutation group $G \subseteq S_n$ is called synchronizing if, for all non-permutations $t$ of $\{1, \ldots, n\}$, the automaton $(\{1, \ldots, n\}, G \cup \{t\})$ is synchronizing.

Pin’s Theorem implies that cyclic groups of prime order are synchronizing.

It is easy to see that 2-transitive groups are synchronizing.

With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results.

João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation.

Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Synchronizing groups

- Motivated by the first part of Pin’s Theorem, I defined in 2004 the notion of a synchronizing group.
- A permutation group $G \subseteq S_n$ is called synchronizing if, for all non-permutations $t$ of $\{1, \ldots, n\}$, the automaton $(\{1, \ldots, n\}, G \cup \{t\})$ is synchronizing.
- Pin’s Theorem implies that cyclic groups of prime order are synchronizing.
- It is easy to see that 2-transitive groups are synchronizing.
- With Arnold, I proved synchronizing groups are primitive and gave a sufficient condition for a group to be synchronizing in terms of representation theory that covers the above results.
- João Araújo independently came up with the notion in 2006 and found a beautiful group theoretic reformulation.
- Synchronizing groups have recently received quite a bit of attention from prominent group theorists including Peter Cameron, Peter Neumann and Jan Saxl.
Dubuc extended the second part of Pin’s Theorem to arbitrary automata containing a cyclic permutation via an ingenious linear algebraic argument.

**Theorem (Dubuc ’98)**

Let $\mathcal{A} = (Q, \Sigma)$ be a synchronizing automaton on $n$ states such that $\Sigma$ contains a cyclic permutation of the states. Then $\mathcal{A}$ has a reset word of length at most $(n - 1)^2$.

The results of Dubuc and Pin make it natural to consider more general groups than cyclic groups.
Dubuc’s Theorem

- Dubuc extended the second part of Pin’s Theorem to arbitrary automata containing a cyclic permutation via an ingenious linear algebraic argument.

**Theorem (Dubuc ’98)**

Let $A = (Q, \Sigma)$ be a synchronizing automaton on $n$ states such that $\Sigma$ contains a cyclic permutation of the states. Then $A$ has a reset word of length at most $(n - 1)^2$.

- The results of Dubuc and Pin make it natural to consider more general groups than cyclic groups.
Dubuc extended the second part of Pin’s Theorem to arbitrary automata containing a cyclic permutation via an ingenious linear algebraic argument.

Theorem (Dubuc ’98)

Let $\mathcal{A} = (Q, \Sigma)$ be a synchronizing automaton on $n$ states such that $\Sigma$ contains a cyclic permutation of the states. Then $\mathcal{A}$ has a reset word of length at most $(n - 1)^2$.

The results of Dubuc and Pin make it natural to consider more general groups than cyclic groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.

The automaton $(G, \Delta)$ is called the Cayley graph of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.

Let us say that an automaton $\mathcal{A}$ contains the Cayley graph $(G, \Delta)$ if $\mathcal{A} = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $\mathcal{A}$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a Černý Cayley graph if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let's say $G$ is a Černý group if all its Cayley graphs are Černý Cayley graphs.

Dubuc's theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.

The automaton $(G, \Delta)$ is called the **Cayley graph** of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.

Let us say that an automaton $\mathcal{A}$ **contains** the Cayley graph $(G, \Delta)$ if $\mathcal{A} = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $\mathcal{A}$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a **Černý Cayley graph** if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let's say $G$ is a **Černý group** if all its Cayley graphs are Černý Cayley graphs.

Dubuc's theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.

The automaton $(G, \Delta)$ is called the Cayley graph of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.

Let us say that an automaton $\mathcal{A}$ contains the Cayley graph $(G, \Delta)$ if $\mathcal{A} = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $\mathcal{A}$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a Černý Cayley graph if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let’s say $G$ is a Černý group if all its Cayley graphs are Černý Cayley graphs.

Dubuc’s theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.

The automaton $(G, \Delta)$ is called the Cayley graph of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.

Let us say that an automaton $A$ contains the Cayley graph $(G, \Delta)$ if $A = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $A$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a Černý Cayley graph if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let’s say $G$ is a Černý group if all its Cayley graphs are Černý Cayley graphs.

Dubuc’s theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.

The automaton $(G, \Delta)$ is called the **Cayley graph** of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.

Let us say that an automaton $\mathscr{A}$ **contains** the Cayley graph $(G, \Delta)$ if $\mathscr{A} = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $\mathscr{A}$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a **Černý Cayley graph** if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let’s say $G$ is a **Černý group** if all its Cayley graphs are Černý Cayley graphs.

Dubuc’s theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Černý Cayley graphs

- Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.
- The automaton $(G, \Delta)$ is called the Cayley graph of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.
- Let us say that an automaton $A$ contains the Cayley graph $(G, \Delta)$ if $A = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.
- So $A$ is obtained from the Cayley graph by adding new transitions but no new states.
- Call $(G, \Delta)$ a Černý Cayley graph if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.
- Let’s say $G$ is a Černý group if all its Cayley graphs are Černý Cayley graphs.
- Dubuc’s theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.
- Cyclic groups of prime power order are Černý groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$. The automaton $(G, \Delta)$ is called the **Cayley graph** of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G, \ a \in \Sigma$.

Let us say that an automaton $\mathcal{A}$ contains the Cayley graph $(G, \Delta)$ if $\mathcal{A} = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $\mathcal{A}$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a **Černý Cayley graph** if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let’s say $G$ is a **Černý group** if all its Cayley graphs are Černý Cayley graphs.

Dubuc’s theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Let $G$ be a group of order $n$ and $\Delta$ a generating set of $G$.

The automaton $(G, \Delta)$ is called the **Cayley graph** of $G$ with respect to $\Delta$. A typical transition is of the form $g \xrightarrow{a} ga$ with $g \in G$, $a \in \Sigma$.

Let us say that an automaton $A$ **contains** the Cayley graph $(G, \Delta)$ if $A = (G, \Sigma)$ where $\Delta \subseteq \Sigma$.

So $A$ is obtained from the Cayley graph by adding new transitions but no new states.

Call $(G, \Delta)$ a **Černý Cayley graph** if every synchronizing automaton containing it has a reset word of length at most $(n - 1)^2$.

Let’s say $G$ is a **Černý group** if all its Cayley graphs are Černý Cayley graphs.

Dubuc’s theorem says that $(\mathbb{Z}_n, \{1\})$ is a Černý Cayley graph.

Cyclic groups of prime power order are Černý groups.
Rystsov’s Theorem

- The above notion was implicitly considered by Rystsov.
- In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order $n$ admits a reset word of length $\leq 2(n - 1)^2$.
- He proved in fact a slightly better result.
- Let $(G, \Delta)$ be a Cayley graph with $|G| = n > 1$.
- Define $\text{diam}_\Delta(G)$ to be the least $m$ so that any two states of $(G, \Delta)$ can be connected by a word of length at most $m$.
- $1 \leq \text{diam}_\Delta(G) \leq n - 1$.

**Theorem (Rystsov ’95)**

A synchronizing automaton containing the Cayley graph $(G, \Delta)$ has a reset word of length at most $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$.

- $(n - 1)^2 = 1 + n(n - 2)$. 
Rystsov’s Theorem

- The above notion was implicitly considered by Rystsov.
- In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order $n$ admits a reset word of length $\leq 2(n - 1)^2$.
- He proved in fact a slightly better result.
- Let $(G, \Delta)$ be a Cayley graph with $|G| = n > 1$.
- Define $\text{diam}_\Delta(G)$ to be the least $m$ so that any two states of $(G, \Delta)$ can be connected by a word of length at most $m$.
- $1 \leq \text{diam}_\Delta(G) \leq n - 1$.

**Theorem (Rystsov '95)**

A synchronizing automaton containing the Cayley graph $(G, \Delta)$ has a reset word of length at most $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$.

- $(n - 1)^2 = 1 + n(n - 2)$. 

27/38
The above notion was implicitly considered by Rystsov.

In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order \( n \) admits a reset word of length \( \leq 2(n - 1)^2 \).

He proved in fact a slightly better result.

Let \( (G, \Delta) \) be a Cayley graph with \( |G| = n > 1 \).

Define \( \text{diam}_\Delta(G) \) to be the least \( m \) so that any two states of \( (G, \Delta) \) can be connected by a word of length at most \( m \).

\[ 1 \leq \text{diam}_\Delta(G) \leq n - 1. \]

### Theorem (Rystsov ’95)

A synchronizing automaton containing the Cayley graph \( (G, \Delta) \) has a reset word of length at most \( 1 + (n - 1 + \text{diam}_\Delta(G))(n - 2) \).

\[ (n - 1)^2 = 1 + n(n - 2). \]
The above notion was implicitly considered by Rystsov.

In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order $n$ admits a reset word of length $\leq 2(n - 1)^2$.

He proved in fact a slightly better result.

Let $(G, \Delta)$ be a Cayley graph with $|G| = n > 1$.

- Define $\text{diam}_\Delta(G)$ to be the least $m$ so that any two states of $(G, \Delta)$ can be connected by a word of length at most $m$.
- $1 \leq \text{diam}_\Delta(G) \leq n - 1$.

**Theorem (Rystsov '95)**

A synchronizing automaton containing the Cayley graph $(G, \Delta)$ has a reset word of length at most $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$.

$(n - 1)^2 = 1 + n(n - 2)$. 
Rystsov’s Theorem

- The above notion was implicitly considered by Rystsov.
- In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order \( n \) admits a reset word of length \( \leq 2(n - 1)^2 \).
- He proved in fact a slightly better result.
- Let \((G, \Delta)\) be a Cayley graph with \(|G| = n > 1\).
- Define \( \text{diam}_\Delta(G) \) to be the least \( m \) so that any two states of \((G, \Delta)\) can be connected by a word of length at most \( m \).
- \( 1 \leq \text{diam}_\Delta(G) \leq n - 1 \).

**Theorem (Rystsov ’95)**

A synchronizing automaton containing the Cayley graph \((G, \Delta)\) has a reset word of length at most \( 1 + (n - 1 + \text{diam}_\Delta(G))(n - 2) \).

\[(n - 1)^2 = 1 + n(n - 2).\]
Rystsov’s Theorem

- The above notion was implicitly considered by Rystsov.
- In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order $n$ admits a reset word of length $\leq 2(n - 1)^2$.
- He proved in fact a slightly better result.
- Let $(G, \Delta)$ be a Cayley graph with $|G| = n > 1$.
- Define $\text{diam}_\Delta(G)$ to be the least $m$ so that any two states of $(G, \Delta)$ can be connected by a word of length at most $m$.
- $1 \leq \text{diam}_\Delta(G) \leq n - 1$.

**Theorem (Rystsov ’95)**

A synchronizing automaton containing the Cayley graph $(G, \Delta)$ has a reset word of length at most $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$.

- $(n - 1)^2 = 1 + n(n - 2)$. 
Rystsov’s Theorem

- The above notion was implicitly considered by Rystsov.
- In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order $n$ admits a reset word of length $\leq 2(n - 1)^2$.
- He proved in fact a slightly better result.
- Let $(G, \Delta)$ be a Cayley graph with $|G| = n > 1$.
- Define $\text{diam}_\Delta(G)$ to be the least $m$ so that any two states of $(G, \Delta)$ can be connected by a word of length at most $m$.
- $1 \leq \text{diam}_\Delta(G) \leq n - 1$.

**Theorem (Rystsov ’95)**

A synchronizing automaton containing the Cayley graph $(G, \Delta)$ has a reset word of length at most

$$1 + (n - 1 + \text{diam}_\Delta(G))(n - 2).$$

- $(n - 1)^2 = 1 + n(n - 2)$. 

Rystsov’s Theorem

- The above notion was implicitly considered by Rystsov.
- In 1995, he proved a synchronizing automaton containing the Cayley graph of a group of order $n$ admits a reset word of length $\leq 2(n - 1)^2$.
- He proved in fact a slightly better result.
- Let $(G, \Delta)$ be a Cayley graph with $|G| = n > 1$.
- Define $\text{diam}_\Delta(G)$ to be the least $m$ so that any two states of $(G, \Delta)$ can be connected by a word of length at most $m$.
- $1 \leq \text{diam}_\Delta(G) \leq n - 1$.

Theorem (Rystsov ’95)

A synchronizing automaton containing the Cayley graph $(G, \Delta)$ has a reset word of length at most $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$.

- $(n - 1)^2 = 1 + n(n - 2)$. 
Recall Rystsov’s bound is $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$ and $(n - 1)^2 = 1 + n(n - 2)$.

So Rystsov’s bound only achieves the Černý bound when the diameter is 1, i.e., all non-trivial elements of $G$ belong to the generating set.

We aim to improve his bound so that in many cases we achieve the Černý bound.

Even when we do not achieve the Černý bound with our main result, our techniques often suffice to establish a family of Cayley graphs is Černý.

Our results lead to several new families of Černý groups.

Our main tool is still representation theory.
• Recall Rystsov’s bound is $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$ and $(n - 1)^2 = 1 + n(n - 2)$.

• So Rystsov’s bound only achieves the Černý bound when the diameter is 1, i.e., all non-trivial elements of $G$ belong to the generating set.

• We aim to improve his bound so that in many cases we achieve the Černý bound.

• Even when we do not achieve the Černý bound with our main result, our techniques often suffice to establish a family of Cayley graphs is Černý.

• Our results lead to several new families of Černý groups.

• Our main tool is still representation theory.
Our goal

- Recall Rystsov’s bound is \( 1 + (n - 1 + \text{diam}_\Delta(G))(n - 2) \) and \( (n - 1)^2 = 1 + n(n - 2) \).
- So Rystsov’s bound only achieves the Černý bound when the diameter is 1, i.e., all non-trivial elements of \( G \) belong to the generating set.
- We aim to improve his bound so that in many cases we achieve the Černý bound.
- Even when we do not achieve the Černý bound with our main result, our techniques often suffice to establish a family of Cayley graphs is Černý.
- Our results lead to several new families of Černý groups.
- Our main tool is still representation theory.
Recall Rystsov’s bound is $1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)$ and $(n - 1)^2 = 1 + n(n - 2)$.

So Rystsov’s bound only achieves the Černý bound when the diameter is 1, i.e., all non-trivial elements of $G$ belong to the generating set.

We aim to improve his bound so that in many cases we achieve the Černý bound.

Even when we do not achieve the Černý bound with our main result, our techniques often suffice to establish a family of Cayley graphs is Černý.

Our results lead to several new families of Černý groups.

Our main tool is still representation theory.
Recall Rystsov’s bound is \(1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)\) and \((n - 1)^2 = 1 + n(n - 2)\).

So Rystsov’s bound only achieves the Černý bound when the diameter is 1, i.e., all non-trivial elements of \(G\) belong to the generating set.

We aim to improve his bound so that in many cases we achieve the Černý bound.

Even when we do not achieve the Černý bound with our main result, our techniques often suffice to establish a family of Cayley graphs is Černý.

Our results lead to several new families of Černý groups.

Our main tool is still representation theory.
Our goal

- Recall Rystsov’s bound is \( 1 + (n - 1 + \text{diam}_\Delta(G))(n - 2) \) and \((n - 1)^2 = 1 + n(n - 2)\).
- So Rystsov’s bound only achieves the Černý bound when the diameter is 1, i.e., all non-trivial elements of \( G \) belong to the generating set.
- We aim to improve his bound so that in many cases we achieve the Černý bound.
- Even when we do not achieve the Černý bound with our main result, our techniques often suffice to establish a family of Cayley graphs is Černý.
- Our results lead to several new families of Černý groups.
- Our main tool is still representation theory.
Irreducible representations of groups

- We shall call an irreducible representation of a group an \textit{irrep}.
- For groups, an arbitrary representation is a direct sum of irreps, which is not the case for monoids.
- If $|G| = n$, then the degree of any irrep is between 1 and $n - 1$.

\textbf{Definition}

For a finite group $G$, define $m(G)$ to be the maximal degree of an irrep of $G$ over $\mathbb{Q}$.

- $1 \leq m(G) \leq |G| - 1$. 
We shall call an irreducible representation of a group an \textit{irrep}.

For groups, an arbitrary representation is a direct sum of irreps, which is not the case for monoids.

If $|G| = n$, then the degree of any irrep is between 1 and $n - 1$.

\textbf{Definition}

For a finite group $G$, define $m(G)$ to be the maximal degree of an irrep of $G$ over $\mathbb{Q}$.

$1 \leq m(G) \leq |G| - 1.$
We shall call an irreducible representation of a group an \textit{irrep}.

For groups, an arbitrary representation is a direct sum of irreps, which is not the case for monoids.

If $|G| = n$, then the degree of any irrep is between 1 and $n - 1$.

\begin{definition}
For a finite group $G$, define $m(G)$ to be the maximal degree of an irrep of $G$ over $\mathbb{Q}$.
\end{definition}

$1 \leq m(G) \leq |G| - 1$. 
Irreducible representations of groups

- We shall call an irreducible representation of a group an irrep.
- For groups, an arbitrary representation is a direct sum of irreps, which is not the case for monoids.
- If $|G| = n$, then the degree of any irrep is between 1 and $n - 1$.

**Definition**

For a finite group $G$, define $m(G)$ to be the maximal degree of an irrep of $G$ over $\mathbb{Q}$.

- $1 \leq m(G) \leq |G| - 1$. 
We shall call an irreducible representation of a group an irrep.

For groups, an arbitrary representation is a direct sum of irreps, which is not the case for monoids.

If $|G| = n$, then the degree of any irrep is between 1 and $n - 1$.

**Definition**

For a finite group $G$, define $m(G)$ to be the maximal degree of an irrep of $G$ over $\mathbb{Q}$.

$1 \leq m(G) \leq |G| - 1$. 
The main result

**Theorem (BS)**

Let \((G, \Delta)\) be a Cayley graph of a group of order \(n\). Then any synchronizing automaton containing \((G, \Delta)\) admits a reset word of length at most

\[
1 + (n - m(G) + \text{diam}_\Delta(G))(n - 2).
\]

In particular, if \(\text{diam}_\Delta(G) \leq m(G)\), then \((G, \Delta)\) is a Černý Cayley graph.

- The last statement follows since \((n - 1)^2 = 1 + n(n - 2)\).
- \(m(G) = 1\) iff \(G \cong \mathbb{Z}_2^k\) for some \(k\).
- So we beat Rystsov's bound of
  \[
  1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)
  \]
  in essentially all cases.
The main result

**Theorem (BS)**

Let \((G, \Delta)\) be a Cayley graph of a group of order \(n\). Then any synchronizing automaton containing \((G, \Delta)\) admits a reset word of length at most

\[
1 + (n - m(G) + \text{diam}_\Delta(G))(n - 2).
\]

In particular, if \(\text{diam}_\Delta(G) \leq m(G)\), then \((G, \Delta)\) is a Černý Cayley graph.

- The last statement follows since \((n - 1)^2 = 1 + n(n - 2)\).
- \(m(G) = 1\) iff \(G \cong \mathbb{Z}_2^k\) for some \(k\).
- So we beat Rystsov’s bound of \(1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)\) in essentially all cases.
The main result

**Theorem (BS)**

Let \((G, \Delta)\) be a Cayley graph of a group of order \(n\). Then any synchronizing automaton containing \((G, \Delta)\) admits a reset word of length at most

\[
1 + (n - m(G) + \text{diam}_{\Delta}(G))(n - 2).
\]

In particular, if \(\text{diam}_{\Delta}(G) \leq m(G)\), then \((G, \Delta)\) is a Černý Cayley graph.

- The last statement follows since \((n - 1)^2 = 1 + n(n - 2)\).
- \(m(G) = 1\) iff \(G \cong \mathbb{Z}_2^k\) for some \(k\).
- So we beat Rystsov’s bound of \(1 + (n - 1 + \text{diam}_{\Delta}(G))(n - 2)\) in essentially all cases.
The main result

**Theorem (BS)**

Let \((G, \Delta)\) be a Cayley graph of a group of order \(n\). Then any synchronizing automaton containing \((G, \Delta)\) admits a reset word of length at most

\[
1 + (n - m(G) + \text{diam}_\Delta(G))(n - 2).
\]

In particular, if \(\text{diam}_\Delta(G) \leq m(G)\), then \((G, \Delta)\) is a Černý Cayley graph.

- The last statement follows since \((n - 1)^2 = 1 + n(n - 2)\).
- \(m(G) = 1\) iff \(G \cong \mathbb{Z}_2^k\) for some \(k\).
- So we beat Rystsov’s bound of
  \[
  1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)
  \]
  in essentially all cases.
The main result

**Theorem (BS)**

Let \((G, \Delta)\) be a Cayley graph of a group of order \(n\). Then any synchronizing automaton containing \((G, \Delta)\) admits a reset word of length at most

\[
1 + (n - m(G) + \text{diam}_\Delta(G))(n - 2).
\]

In particular, if \(\text{diam}_\Delta(G) \leq m(G)\), then \((G, \Delta)\) is a Černý Cayley graph.

- The last statement follows since \((n - 1)^2 = 1 + n(n - 2)\).
- \(m(G) = 1\) iff \(G \cong \mathbb{Z}_2^k\) for some \(k\).
- So we beat Rystsov’s bound of
  \[
  1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)
  \]
  in essentially all cases.
The main result

**Theorem (BS)**

Let \((G, \Delta)\) be a Cayley graph of a group of order \(n\). Then any synchronizing automaton containing \((G, \Delta)\) admits a reset word of length at most

\[
1 + (n - m(G) + \text{diam}_\Delta(G))(n - 2).
\]

In particular, if \(\text{diam}_\Delta(G) \leq m(G)\), then \((G, \Delta)\) is a Černý Cayley graph.

- The last statement follows since \((n - 1)^2 = 1 + n(n - 2)\).
- \(m(G) = 1\) iff \(G \cong \mathbb{Z}_2^k\) for some \(k\).
- So we beat Rystsov’s bound of
  \[
  1 + (n - 1 + \text{diam}_\Delta(G))(n - 2)
  \]
  in essentially all cases.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}\{1\}(\mathbb{Z}_n) = n - 1$.
- So we achieve the Černý bound iff $\phi(n) = n - 1$.
- This occurs iff $n$ is prime.
- In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
- This does not follow from Dubuc’s result.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}\{1\}(\mathbb{Z}_n) = n - 1$.
- So we achieve the Černý bound iff $\phi(n) = n - 1$.
- This occurs iff $n$ is prime.
- In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
- This does not follow from Dubuc’s result.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}_{\{1\}}(\mathbb{Z}_n) = n - 1$.
  - So we achieve the Černý bound iff $\phi(n) = n - 1$.
  - This occurs iff $n$ is prime.
- In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
  - Suppose $p < q$ are odd primes and $n = pq$.
  - Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
  - $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
  - So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
  - This does not follow from Dubuc’s result.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}_1(\mathbb{Z}_n) = n - 1$.
- So we achieve the Černý bound iff $\phi(n) = n - 1$.
  - This occurs iff $n$ is prime.
  - In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
  - Suppose $p < q$ are odd primes and $n = pq$.
  - Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
  - $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
  - So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
  - This does not follow from Dubuc’s result.
Cyclic groups

- One can prove \( m(\mathbb{Z}_n) = \phi(n) \) (Euler’s function).
- The irrep comes from the action of \( \mathbb{Z}_n \) on \( \mathbb{Q}(\zeta_n) \) (\( \zeta_n \) a primitive \( n^{th} \)-root of unity) by multiplication by \( \zeta_n \).
- Of course, \( \text{diam}_{\{1\}}(\mathbb{Z}_n) = n - 1 \).
- So we achieve the Černý bound iff \( \phi(n) = n - 1 \).
- This occurs iff \( n \) is prime.
  - In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
  - Suppose \( p < q \) are odd primes and \( n = pq \).
  - Then \( \text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1 \) (\( \mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p \)).
  - \( \phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1 \).
  - So \( (\mathbb{Z}_{pq}, \{p,q\}) \) is a Černý Cayley graph.
  - This does not follow from Dubuc’s result.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}_1(\mathbb{Z}_n) = n - 1$.
- So we achieve the Černý bound iff $\phi(n) = n - 1$.
- This occurs iff $n$ is prime.
- In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
  - Suppose $p < q$ are odd primes and $n = pq$.
  - Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
  - $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
  - So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
  - This does not follow from Dubuc’s result.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}_1(\mathbb{Z}_n) = n - 1$.
- So we achieve the Černý bound iff $\phi(n) = n - 1$.
- This occurs iff $n$ is prime.
- In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
  - Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
  - $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
  - So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
  - This does not follow from Dubuc’s result.
One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).

The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.

Of course, ${\rm diam}_{\{1\}}(\mathbb{Z}_n) = n - 1$.

So we achieve the Černý bound iff $\phi(n) = n - 1$.

This occurs iff $n$ is prime.

In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).

Suppose $p < q$ are odd primes and $n = pq$.

Then $diam_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).

$\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.

So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

This does not follow from Dubuc’s result.
One can prove \( m(\mathbb{Z}_n) = \phi(n) \) (Euler’s function).

The irrep comes from the action of \( \mathbb{Z}_n \) on \( \mathbb{Q}(\zeta_n) \) (\( \zeta_n \) a primitive \( n^{th} \)-root of unity) by multiplication by \( \zeta_n \).

Of course, \( \text{diam}_{\{1\}}(\mathbb{Z}_n) = n - 1 \).

So we achieve the Černý bound iff \( \phi(n) = n - 1 \).

This occurs iff \( n \) is prime.

In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).

Suppose \( p < q \) are odd primes and \( n = pq \).

Then \( \text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1 \) (\( \mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p \)).

\( \phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1 \).

So \( (\mathbb{Z}_{pq}, \{p, q\}) \) is a Černý Cayley graph.

This does not follow from Dubuc’s result.
Cyclic groups

- One can prove $m(\mathbb{Z}_n) = \phi(n)$ (Euler’s function).
- The irrep comes from the action of $\mathbb{Z}_n$ on $\mathbb{Q}(\zeta_n)$ ($\zeta_n$ a primitive $n^{th}$-root of unity) by multiplication by $\zeta_n$.
- Of course, $\text{diam}_1(\mathbb{Z}_n) = n - 1$.
- So we achieve the Černý bound iff $\phi(n) = n - 1$.
- This occurs iff $n$ is prime.
- In particular, our method recovers Pin’s Theorem, but not Dubuc’s Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\text{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.
- This does not follow from Dubuc’s result.
Let $p$ be a prime.

To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayley graph with respect to a basis $\Delta$.

$\text{diam}_\Delta(\mathbb{Z}_p^k) = k(p - 1)$.

One can prove $m(\mathbb{Z}_p^k) = p - 1$.

Our bound therefore is not strong enough when $k > 1$.

Nonetheless we can prove:

**Theorem (BS)**

The group $\mathbb{Z}_p^k$ is a Černý group for $p$ prime and all $k \geq 1$. 
Let $p$ be a prime.

To show that $\mathbb{Z}^k_p$ is a Černý group, it suffices to consider the Cayley graph with respect to a basis $\Delta$.

- $\text{diam}_\Delta(\mathbb{Z}^k_p) = k(p - 1)$.
- One can prove $m(\mathbb{Z}^k_p) = p - 1$.
- Our bound therefore is not strong enough when $k > 1$.

Nonetheless we can prove:

**Theorem (BS)**

The group $\mathbb{Z}^k_p$ is a Černý group for $p$ prime and all $k \geq 1$. 
Let $p$ be a prime.

To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayley graph with respect to a basis $\Delta$.

$\text{diam}_\Delta(\mathbb{Z}_p^k) = k(p - 1)$.

One can prove $m(\mathbb{Z}_p^k) = p - 1$.

Our bound therefore is not strong enough when $k > 1$. Nonetheless we can prove:

**Theorem (BS)**

The group $\mathbb{Z}_p^k$ is a Černý group for $p$ prime and all $k \geq 1$. 
Let $p$ be a prime.

To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayley graph with respect to a basis $\Delta$.

$\text{diam}_\Delta(\mathbb{Z}_p^k) = k(p - 1)$.

One can prove $m(\mathbb{Z}_p^k) = p - 1$.

Our bound therefore is not strong enough when $k > 1$.

Nonetheless we can prove:

**Theorem (BS)**

The group $\mathbb{Z}_p^k$ is a Černý group for $p$ prime and all $k \geq 1$.
Let $p$ be a prime.

To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayley graph with respect to a basis $\Delta$.

$diam_{\Delta}(\mathbb{Z}_p^k) = k(p - 1)$.

One can prove $m(\mathbb{Z}_p^k) = p - 1$.

Our bound therefore is not strong enough when $k > 1$.

Nonetheless we can prove:

**Theorem (BS)**

The group $\mathbb{Z}_p^k$ is a Černý group for $p$ prime and all $k \geq 1$. 
Let $p$ be a prime.

To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayley graph with respect to a basis $\Delta$.

- $\text{diam}_\Delta(\mathbb{Z}_p^k) = k(p - 1)$.
- One can prove $m(\mathbb{Z}_p^k) = p - 1$.
- Our bound therefore is not strong enough when $k > 1$.

Nonetheless we can prove:

**Theorem (BS)**

*The group $\mathbb{Z}_p^k$ is a Černý group for $p$ prime and all $k \geq 1$.***
Let $D_n$ be the dihedral group of order $2n$ (the symmetry group of a regular $n$-gon).

Let $\Delta$ consist of a reflection and a rotation by $2\pi/n$.

Then $\text{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.

One can prove $m(D_n) = \phi(n)$.

If $n = p^a q^b$ where $p \leq q$ are odd primes, then one verifies that $\lceil \frac{n+1}{2} \rceil \leq \phi(n)$ and so we obtain a Černý Cayley graph.

Theorem (BS)

Let $p$ be an odd prime. Then $D_p$ and $D_{p^2}$ are Černý groups.
Let $D_n$ be the dihedral group of order $2n$ (the symmetry group of a regular $n$-gon).

Let $\Delta$ consist of a reflection and a rotation by $2\pi/n$.

Then $\text{diam}_\Delta(D_n) \leq \left\lceil \frac{n+1}{2} \right\rceil$.

One can prove $m(D_n) = \phi(n)$.

If $n = p^a q^b$ where $p \leq q$ are odd primes, then one verifies that $\left\lceil \frac{n+1}{2} \right\rceil \leq \phi(n)$ and so we obtain a Černý Cayley graph.

Theorem (BS)

Let $p$ be an odd prime. Then $D_p$ and $D_{p^2}$ are Černý groups.
Let $D_n$ be the dihedral group of order $2n$ (the symmetry group of a regular $n$-gon).

Let $\Delta$ consist of a reflection and a rotation by $2\pi/n$.

Then $\text{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.

One can prove $m(D_n) = \phi(n)$.

If $n = p^a q^b$ where $p \leq q$ are odd primes, then one verifies that $\lceil \frac{n+1}{2} \rceil \leq \phi(n)$ and so we obtain a Černý Cayley graph.

**Theorem (BS)**

Let $p$ be an odd prime. Then $D_p$ and $D_{p^2}$ are Černý groups.
- Let $D_n$ be the dihedral group of order $2n$ (the symmetry group of a regular $n$-gon).
- Let $\Delta$ consist of a reflection and a rotation by $2\pi/n$.
- Then $\text{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$.
- If $n = p^aq^b$ where $p \leq q$ are odd primes, then one verifies that $\lceil \frac{n+1}{2} \rceil \leq \phi(n)$ and so we obtain a Černý Cayley graph.

**Theorem (BS)**

Let $p$ be an odd prime. Then $D_p$ and $D_{p^2}$ are Černý groups.
Dihedral groups

- Let $D_n$ be the dihedral group of order $2n$ (the symmetry group of a regular $n$-gon).
- Let $\Delta$ consist of a reflection and a rotation by $2\pi/n$.
- Then $\text{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$.
- If $n = p^a q^b$ where $p \leq q$ are odd primes, then one verifies that $\lceil \frac{n+1}{2} \rceil \leq \phi(n)$ and so we obtain a Černý Cayley graph.

**Theorem (BS)**

Let $p$ be an odd prime. Then $D_p$ and $D_{p^2}$ are Černý groups.
Let $D_n$ be the dihedral group of order $2n$ (the symmetry group of a regular $n$-gon).

Let $\Delta$ consist of a reflection and a rotation by $2\pi/n$.

Then $\text{diam}_{\Delta}(D_n) \leq \lceil \frac{n+1}{2} \rceil$.

One can prove $m(D_n) = \phi(n)$.

If $n = p^a q^b$ where $p \leq q$ are odd primes, then one verifies that $\lceil \frac{n+1}{2} \rceil \leq \phi(n)$ and so we obtain a Černý Cayley graph.

**Theorem (BS)**

Let $p$ be an odd prime. Then $D_p$ and $D_{p^2}$ are Černý groups.
Symmetric groups

- It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.
- The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.
- Thus $m(S_n)^2 p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.
- $p_n \sim \frac{\exp\left(\pi \sqrt{2n/3}\right)}{4n\sqrt{3}}$ and $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.
- Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.
- With Coxeter-Moore generators $(1 \ 2), (2 \ 3), \ldots, (n-1 \  n)$, the diameter is $\binom{n}{2}$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.
- With the generating set $(1 \ 2), (1 \ 2 \cdots n)$, the diameter of $S_n$ is at most $\binom{n}{2}(n + 1)$ and so we again get a Černý Cayley graph for $n$ large enough.
Symmetric groups

- It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.
- The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.
- Thus $m(S_n)^2 p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.
- $p_n \sim \frac{\exp\left(\frac{\pi \sqrt{2n/3}}{4n \sqrt{3}}\right)}{4n \sqrt{3}}$ and $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.
- Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.
- With Coxeter-Moore generators $(1 \ 2), (2 \ 3), \ldots, (n-1 \ n)$, the diameter is $\left(\frac{n}{2}\right)$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.
- With the generating set $(1 \ 2), (1 \ 2 \cdots n)$, the diameter of $S_n$ is at most $\left(\frac{n}{2}\right)(n + 1)$ and so we again get a Černý Cayley graph for $n$ large enough.
Symmetric groups

- It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.
- The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.
- Thus $m(S_n)^2 p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.
- $p_n \sim \frac{\exp\left(\frac{\pi \sqrt{2n/3}}{4n\sqrt{3}}\right)}{4n\sqrt{3}}$ and $n! \sim \sqrt{2\pi n \left(\frac{n}{e}\right)^n}$.
- Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.
- With Coxeter-Moore generators $(1 \ 2), (2 \ 3), \ldots, (n-1 \ n)$, the diameter is $\binom{n}{2}$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.
- With the generating set $(1 \ 2), (1 \ 2 \ \cdots \ n)$, the diameter of $S_n$ is at most $\binom{n}{2}(n+1)$ and so we again get a Černý Cayley graph for $n$ large enough.
Symmetric groups

- It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.
- The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.
- Thus $m(S_n)^2 p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.
- $p_n \sim \frac{\exp\left(\frac{\pi \sqrt{2n/3}}{4n \sqrt{3}}\right)}{n!}$ and $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.
- Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.
- With Coxeter-Moore generators $(1\,2), (2\,3), \ldots, (n-1\,n)$, the diameter is $\binom{n}{2}$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.
- With the generating set $(1\,2), (1\,2 \cdots n)$, the diameter of $S_n$ is at most $\binom{n}{2}(n+1)$ and so we again get a Černý Cayley graph for $n$ large enough.
Symmetric groups

- It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.
- The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.
- Thus $m(S_n)^2 p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.
- $p_n \sim \frac{\exp\left(\pi \sqrt{2n/3}\right)}{4n\sqrt{3}}$ and $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.

Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.

- With Coxeter-Moore generators $(1\ 2), (2\ 3), \ldots, (n-1\ n)$, the diameter is $\binom{n}{2}$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.

- With the generating set $(1\ 2), (1\ 2\ \cdots\ n)$, the diameter of $S_n$ is at most $\binom{n}{2}(n+1)$ and so we again get a Černý Cayley graph for $n$ large enough.
It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.

The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.

Thus $m(S_n)^2p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.

$p_n \sim \frac{\exp\left(\pi \sqrt{2n/3}\right)}{4n\sqrt{3}}$ and $n! \sim \sqrt{2\pi n \left(\frac{n}{e}\right)^n}$.

Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.

With Coxeter-Moore generators $(1 \ 2), (2 \ 3), \ldots, (n-1 \ n)$, the diameter is $\binom{n}{2}$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.

With the generating set $(1 \ 2), (1 \ 2 \ \ldots \ n)$, the diameter of $S_n$ is at most $\binom{n}{2}(n+1)$ and so we again get a Černý Cayley graph for $n$ large enough.
Symmetric groups

- It is known that the symmetric group $S_n$ has $p_n$ irreducible representations where $p_n$ is the number of partitions of $n$.
- The sum of the squares of the degrees of the irreps of $S_n$ is $n!$.
- Thus $m(S_n)^2 p_n \geq n!$, i.e., $m(S_n) \geq \sqrt{n!/p_n}$.
- $p_n \sim \frac{\exp\left(\frac{\pi \sqrt{2n/3}}{4n\sqrt{3}}\right)}{4n\sqrt{3}}$ and $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.
- Therefore, $m(S_n)$ grows extremely quickly as a function of $n$.
- With Coxeter-Moore generators $(1 \ 2), (2 \ 3), \ldots, (n-1 \ n)$, the diameter is $\binom{n}{2}$ [think “Bubble Sort”] and so we obtain a Černý Cayley graph for $n$ large enough.
- With the generating set $(1 \ 2), (1 \ 2 \ \cdots \ n)$, the diameter of $S_n$ is at most $\binom{n}{2}(n+1)$ and so we again get a Černý Cayley graph for $n$ large enough.
Let $p$ be a prime.

$SL(2, p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{Z}_p, ad - bc = 1 \right\}$.

A standard generating set $\Delta$ for $SL(2, p)$ consists of the matrices

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.
\]

The diameter with this generating set is no more than $3p - 2$.

Estimating $m(SL(2, p))$ is a bit more complicated.
Let $p$ be a prime.

$SL(2, p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc = 1 \right\}.$

A standard generating set $\Delta$ for $SL(2, p)$ consists of the matrices

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$

The diameter with this generating set is no more than $3p - 2$.

Estimating $m(SL(2, p))$ is a bit more complicated.
Let $p$ be a prime.

$SL(2, p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc = 1 \right\}$.

A standard generating set $\Delta$ for $SL(2, p)$ consists of the matrices

$$
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.
$$

The diameter with this generating set is no more than $3p - 2$.

Estimating $m(SL(2, p))$ is a bit more complicated.
Let $p$ be a prime.

$$SL(2, p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc = 1 \right\}.$$  

A standard generating set $\Delta$ for $SL(2, p)$ consists of the matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$  

The diameter with this generating set is no more than $3p - 2$.

Estimating $m(SL(2, p))$ is a bit more complicated.
Let $p$ be a prime.

$SL(2, p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc = 1 \right\}$.

A standard generating set $\Delta$ for $SL(2, p)$ consists of the matrices

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

The diameter with this generating set is no more than $3p - 2$.

Estimating $m(SL(2, p))$ is a bit more complicated.
In the group theory literature there is much more detailed information about representations over $\mathbb{C}$ than over $\mathbb{Q}$.

Schur index theory allows one to use Galois theory in order to understand irreps over $\mathbb{Q}$ in terms of irreps over $\mathbb{C}$.

Via these methods, we computed

$$m(SL(2, p)) \geq \max \left\{ (p + 1) \frac{\phi(p-1)}{2}, (p - 1) \frac{\phi(p+1)}{2} \right\}.$$ 

The diameter of the Cayley graph of $SL(2, p)$ with our generators was at most $3p - 2$.

**Theorem (BS)**

Let $p \geq 17$ be a prime. Then the Cayley graph of $SL(2, p)$ with respect to the generators $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ is a Černý Cayley graph.
In the group theory literature there is much more detailed information about representations over $\mathbb{C}$ than over $\mathbb{Q}$.

Schur index theory allows one to use Galois theory in order to understand irreps over $\mathbb{Q}$ in terms of irreps over $\mathbb{C}$.

Via these methods, we computed

$$m(SL(2, p)) \geq \max \left\{ (p + 1) \frac{\phi(p-1)}{2}, (p - 1) \frac{\phi(p+1)}{2} \right\}.$$

The diameter of the Cayley graph of $SL(2, p)$ with our generators was at most $3p - 2$.

**Theorem (BS)**

Let $p \geq 17$ be a prime. Then the Cayley graph of $SL(2, p)$ with respect to the generators $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ is a Černý Cayley graph.
In the group theory literature there is much more detailed information about representations over $\mathbb{C}$ than over $\mathbb{Q}$.

Schur index theory allows one to use Galois theory in order to understand irreps over $\mathbb{Q}$ in terms of irreps over $\mathbb{C}$.

Via these methods, we computed
\[
m(SL(2, p)) \geq \max \left\{ (p + 1) \frac{\phi(p-1)}{2}, (p - 1) \frac{\phi(p+1)}{2} \right\}.
\]

The diameter of the Cayley graph of $SL(2, p)$ with our generators was at most $3p - 2$.

Theorem (BS)

Let $p \geq 17$ be a prime. Then the Cayley graph of $SL(2, p)$ with respect to the generators
\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}
\] is a Černý Cayley graph.
In the group theory literature there is much more detailed information about representations over $\mathbb{C}$ than over $\mathbb{Q}$.

Schur index theory allows one to use Galois theory in order to understand irreps over $\mathbb{Q}$ in terms of irreps over $\mathbb{C}$.

Via these methods, we computed

$$m(SL(2, p)) \geq \max \left\{ (p + 1) \frac{\phi(p-1)}{2}, (p - 1) \frac{\phi(p+1)}{2} \right\}.$$

The diameter of the Cayley graph of $SL(2, p)$ with our generators was at most $3p - 2$.

**Theorem (BS)**

Let $p \geq 17$ be a prime. Then the Cayley graph of $SL(2, p)$ with respect to the generators

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

is a Černý Cayley graph.
In the group theory literature there is much more detailed information about representations over $\mathbb{C}$ than over $\mathbb{Q}$.

Schur index theory allows one to use Galois theory in order to understand irreps over $\mathbb{Q}$ in terms of irreps over $\mathbb{C}$.

Via these methods, we computed
\[ m(SL(2, p)) \geq \max \left\{ (p + 1) \frac{\phi(p-1)}{2}, (p - 1) \frac{\phi(p+1)}{2} \right\}. \]

The diameter of the Cayley graph of $SL(2, p)$ with our generators was at most $3p - 2$.

**Theorem (BS)**

Let $p \geq 17$ be a prime. Then the Cayley graph of $SL(2, p)$ with respect to the generators $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ is a Černý Cayley graph.
A number of questions remain open.

- Is every cyclic group a Černý group?
- Is every abelian group a Černý group?
- Is every dihedral group a Černý group?
- Is every group a Černý group?
A number of questions remain open.

- Is every cyclic group a Černý group?
- Is every abelian group a Černý group?
- Is every dihedral group a Černý group?
- Is every group a Černý group?
A number of questions remain open.

- Is every cyclic group a Černý group?
- Is every abelian group a Černý group?
- Is every dihedral group a Černý group?
- Is every group a Černý group?
A number of questions remain open.
Is every cyclic group a Černý group?
Is every abelian group a Černý group?
Is every dihedral group a Černý group?
Is every group a Černý group?
A number of questions remain open.

Is every cyclic group a Černý group?

Is every abelian group a Černý group?

Is every dihedral group a Černý group?

Is every group a Černý group?
Vielen Dank für Ihre Aufmerksamkeit!