The Černý Conjecture and Group Representations

Benjamin Steinberg

Carleton University

bsteinbg@math.carleton.ca

SATA September 4, 2008

Synchronizing Automata

- An automon $\mathscr{A} = (Q, \Sigma)$ is *synchronizing* if there exists $w \in \Sigma^*$ such that $|Qw| = 1$.
- Such a word w is called a *reset word*.

Conjecture (Černý '64)

A synchronizing automaton with n states admits a reset word of length at most $(n-1)^2$.

- The best known upper bound on the length of reset words is $\frac{n^3-n}{6}$, due to Pin based on a non-trivial combinatorial result of Frankl.
- One can obtain a bound of $\frac{n^3-n}{3}$ with straightforward methods.
- Improving a bound by a factor of 2 can be hard work!

Synchronizing Automata

- An automon $\mathscr{A} = (Q, \Sigma)$ is *synchronizing* if there exists $w \in \Sigma^*$ such that $|Qw| = 1$.
- Such a word w is called a *reset word*.

Conjecture (Černý '64)

A synchronizing automaton with n states admits a reset word of length at most $(n-1)^2$.

- The best known upper bound on the length of reset words is $\frac{n^3-n}{6}$, due to Pin based on a non-trivial combinatorial result of Frankl.
- One can obtain a bound of $\frac{n^3-n}{3}$ with straightforward methods.
- Improving a bound by a factor of 2 can be hard work!

Synchronizing Automata

- An automon $\mathscr{A} = (Q, \Sigma)$ is *synchronizing* if there exists $w \in \Sigma^*$ such that $|Qw| = 1$.
- Such a word w is called a *reset word*.

Conjecture (Černý '64)

A synchronizing automaton with n states admits a reset word of length at most $(n-1)^2$.

- The best known upper bound on the length of reset words is $\frac{n^3-n}{6}$, due to Pin based on a non-trivial combinatorial result of Frankl.
- One can obtain a bound of $\frac{n^3-n}{3}$ with straightforward methods.
- Improving a bound by a factor of 2 can be hard work!

Synchronizing Automata

- An automon $\mathscr{A} = (Q, \Sigma)$ is *synchronizing* if there exists $w \in \Sigma^*$ such that $|Qw| = 1$.
- Such a word w is called a *reset word*.

Conjecture (Černý '64)

A synchronizing automaton with n states admits a reset word of length at most $(n-1)^2$.

- The best known upper bound on the length of reset words is $\frac{n^3-n}{6}$, due to Pin based on a non-trivial combinatorial result of Frankl.
- One can obtain a bound of $\frac{n^3-n}{3}$ with straightforward methods.
- Improving a bound by a factor of 2 can be hard work!

Pin's Theorem

- The literature on Černý's conjecture consists of a vast array of partial results, the first of which was Pin's Theorem.
- If (Q, Σ) is an automaton, we view $\Sigma \subseteq T_Q$ (the semigroup of self-maps of Q).

Theorem (Pin '78)

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

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

Pin's Theorem

- The literature on Černý's conjecture consists of a vast array of partial results, the first of which was Pin's Theorem.
- If (Q, Σ) is an automaton, we view $\Sigma \subseteq T_Q$ (the semigroup of self-maps of Q).

Theorem (Pin '78)

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

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

Synchronizing Groups

- Motivated by the first part of Pin's Theorem, I defined in 2004 the notion of a synchronizing group.
- A group $G \subseteq S_n$ is called *synchronizing* if, for all non-permutations $t \in T_n$, the monoid $\langle G \cup t \rangle$ contains a constant map.
- 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 Neumann, Jan Saxl, Peter Cameron and Csaba Schneider.

Synchronizing Groups

- Motivated by the first part of Pin's Theorem, I defined in 2004 the notion of a synchronizing group.
- A group $G \subseteq S_n$ is called *synchronizing* if, for all non-permutations $t \in T_n$, the monoid $\langle G \cup t \rangle$ contains a constant map.
- 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 Neumann, Jan Saxl, Peter Cameron and Csaba Schneider.

Synchronizing Groups

- Motivated by the first part of Pin's Theorem, I defined in 2004 the notion of a synchronizing group.
- A group $G \subseteq S_n$ is called *synchronizing* if, for all non-permutations $t \in T_n$, the monoid $\langle G \cup t \rangle$ contains a constant map.
- 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 Neumann, Jan Saxl, Peter Cameron and Csaba Schneider.

Synchronizing Groups

- Motivated by the first part of Pin's Theorem, I defined in 2004 the notion of a synchronizing group.
- A group $G \subseteq S_n$ is called *synchronizing* if, for all non-permutations $t \in T_n$, the monoid $\langle G \cup t \rangle$ contains a constant map.
- 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 Neumann, Jan Saxl, Peter Cameron and Csaba Schneider.

Synchronizing Groups

- Motivated by the first part of Pin's Theorem, I defined in 2004 the notion of a synchronizing group.
- A group $G \subseteq S_n$ is called *synchronizing* if, for all non-permutations $t \in T_n$, the monoid $\langle G \cup t \rangle$ contains a constant map.
- 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 Neumann, Jan Saxl, Peter Cameron and Csaba Schneider.

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 $\mathscr{A} = (Q, \Sigma)$ be a synchronizing automaton on n states such that Σ contains a cyclic permutation of the states. Then $\mathscr{A}$ 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 $\mathscr{A} = (Q, \Sigma)$ be a synchronizing automaton on n states such that Σ contains a cyclic permutation of the states. Then $\mathscr{A}$ 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.

Černý Cayley Graphs

- Let G be a group of order n and Δ a generating set of G.
- The automaton (G, Δ) is called the *Cayley graph* of G with respect to Δ. 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, Δ) 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, Δ) 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 $(\mathbb{Z}, \{1\})$ 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 Δ a generating set of G.
- The automaton (G, Δ) is called the *Cayley graph* of G with respect to Δ. 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, Δ) 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, Δ) 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 $(\mathbb{Z}, \{1\})$ 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 Δ a generating set of G.
- The automaton (G, Δ) is called the *Cayley graph* of G with respect to Δ. 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, Δ) 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, Δ) 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 $(\mathbb{Z}, \{1\})$ 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 Δ a generating set of G.
- The automaton (G, Δ) is called the *Cayley graph* of G with respect to Δ. 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, Δ) 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, Δ) 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 $(\mathbb{Z}, \{1\})$ 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 Δ a generating set of G.
- The automaton (G, Δ) is called the *Cayley graph* of G with respect to Δ. 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, Δ) 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, Δ) 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 $(\mathbb{Z}, \{1\})$ 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, Δ) be a Cayley graph with $|G| = n > 1$.
- Define $\mathrm{diam}_\Delta(G)$ to be the least m so that any two states of (G, Δ) can be connected by a word of length at most m.
- $1 \leq \mathrm{diam}_\Delta(G) \leq n-1$.

Theorem (Rystsov '95)

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

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

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

Theorem (Rystsov '95)

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

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

Our Goal

- Recall Rystsov's bound is $1 + (n - 1 + \mathrm{diam}_\Delta(G))(n-2)$ 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 representation theory.

Our Goal

- Recall Rystsov's bound is $1 + (n - 1 + \mathrm{diam}_\Delta(G))(n - 2)$ 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 representation theory.

Representation Theory

- Fix a field K of characteristic 0 (usually $\mathbb{Q}$).
- All vector spaces V will be over K and finite dimensional.
- Fix a group G of order n.
- A *representation* of G is a homomorphism $\varphi\colon G \to GL(V)$ to the group of invertible linear transformations on V.
- $\dim V$ is called the *degree* of φ.
- $K^G = \{f\colon G \to K\}$ is a vector space of dimension n.
- $\lambda\colon G \to GL(K^G)$ given by

$$\lambda_g(f)(x) = f(xg)$$

is a representation of degree n called the *regular representation*.

Representation Theory

- Fix a field K of characteristic 0 (usually $\mathbb{Q}$).
- All vector spaces V will be over K and finite dimensional.
- Fix a group G of order n.
- A *representation* of G is a homomorphism $\varphi\colon G \to GL(V)$ to the group of invertible linear transformations on V.
- $\dim V$ is called the *degree* of φ.
- $K^G = \{f\colon G \to K\}$ is a vector space of dimension n.
- $\lambda\colon G \to GL(K^G)$ given by

$$\lambda_g(f)(x) = f(xg)$$

  is a representation of degree n called the *regular representation*.

Invariant Subspaces

- Let $\varphi\colon G \to GL(V)$ be a representation.
- $W \leq V$ is called a G-*invariant subspace* if $\varphi_g W \subseteq W$ all $g \in G$.
- 0 and V are the trivial G-invariant subspaces.
- For the regular representation $\lambda\colon G \to GL(K^G)$ there are two important invariant subspaces.
- The subspace V_1 of constant functions is G-invariant.
- If $f(x) = c$ all $x \in G$, then

$$\lambda_g f(x) = f(xg) = c$$

and so $\lambda_g f = f$. Thus V_1 is G-invariant.
- The space V_0 of all functions f so that $\sum_{x \in G} f(x) = 0$ is also G-invariant of dimension $n - 1$.

Invariant Subspaces

- Let $\varphi\colon G \to GL(V)$ be a representation.
- $W \leq V$ is called a *G-invariant subspace* if $\varphi_g W \subseteq W$ all $g \in G$.
- 0 and V are the trivial G-invariant subspaces.
- For the regular representation $\lambda\colon G \to GL(K^G)$ there are two important invariant subspaces.
- The subspace V_1 of constant functions is G-invariant.
- If $f(x) = c$ all $x \in G$, then

$$\lambda_g f(x) = f(xg) = c$$

and so $\lambda_g f = f$. Thus V_1 is G-invariant.
- The space V_0 of all functions f so that $\sum_{x \in G} f(x) = 0$ is also G-invariant of dimension $n - 1$.

Invariant Subspaces

- Let $\varphi\colon G \to GL(V)$ be a representation.
- $W \leq V$ is called a *G-invariant subspace* if $\varphi_g W \subseteq W$ all $g \in G$.
- 0 and V are the trivial G-invariant subspaces.
- For the regular representation $\lambda\colon G \to GL(K^G)$ there are two important invariant subspaces.
- The subspace V_1 of constant functions is G-invariant.
- If $f(x) = c$ all $x \in G$, then

$$\lambda_g f(x) = f(xg) = c$$

  and so $\lambda_g f = f$. Thus V_1 is G-invariant.
- The space V_0 of all functions f so that $\sum_{x \in G} f(x) = 0$ is also G-invariant of dimension $n - 1$.

Invariant Subspaces

- Let $\varphi\colon G \to GL(V)$ be a representation.
- $W \leq V$ is called a *G-invariant subspace* if $\varphi_g W \subseteq W$ all $g \in G$.
- 0 and V are the trivial G-invariant subspaces.
- For the regular representation $\lambda\colon G \to GL(K^G)$ there are two important invariant subspaces.
- The subspace V_1 of constant functions is G-invariant.
- If $f(x) = c$ all $x \in G$, then

$$\lambda_g f(x) = f(xg) = c$$

  and so $\lambda_g f = f$. Thus V_1 is G-invariant.
- The space V_0 of all functions f so that $\sum_{x\in G} f(x) = 0$ is also G-invariant of dimension $n-1$.

Irreducible Representations

- A representation $\varphi\colon G \to GL(V)$ is *irreducible* if it admits no non-trivial G-invariant subspaces.
- A degree 1 representation is obviously irreducible.
- Any representation can be uniquely expressed as a direct sum of irreducible representations (*irreps*).
- Every irrep appears as summand in the decomposition of the regular representation.
- The degree of any irrep is between 1 and $n-1$.

Definition

Define $m(G)$ to be the maximal degree of an irrep of G over $\mathbb{Q}$.

Irreducible Representations

- A representation $\varphi\colon G \to GL(V)$ is *irreducible* if it admits no non-trivial G-invariant subspaces.
- A degree 1 representation is obviously irreducible.
- Any representation can be uniquely expressed as a direct sum of irreducible representations (*irreps*).
- Every irrep appears as summand in the decomposition of the regular representation.
- The degree of any irrep is between 1 and $n-1$.

Definition

Define $m(G)$ to be the maximal degree of an irrep of G over $\mathbb{Q}$.

The Main Result

Theorem (BS)

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

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

In particular, if $\mathrm{diam}_\Delta(G)\leq m(G)$, then (G,Δ) 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, as irreps separate points.
- So we beat Rystsov's bound of $1+(n-1+\mathrm{diam}_\Delta(G))(n-2)$ in essentially all cases.

The Main Result

Theorem (BS)

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

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

In particular, if $\mathrm{diam}_\Delta(G) \leq m(G)$, then (G, Δ) 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, as irreps separate points.
- So we beat Rystsov's bound of $1 + (n - 1 + \mathrm{diam}_\Delta(G))(n-2)$ in essentially all cases.

The Main Result

Theorem (BS)

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

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

In particular, if $\mathrm{diam}_\Delta(G) \leq m(G)$, *then* (G, Δ) *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, as irreps separate points.
- So we beat Rystsov's bound of $1 + (n - 1 + \mathrm{diam}_\Delta(G))(n-2)$ in essentially all cases.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n - 1$, we achieve the Černý bound if and only if $\phi(n) = n - 1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n - 1$, we achieve the Černý bound if and only if $\phi(n) = n - 1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p-1)(q-1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n - 1$, we achieve the Černý bound if and only if $\phi(n) = n - 1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p-1)(q-1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n - 1$, we achieve the Černý bound if and only if $\phi(n) = n - 1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p-1)(q-1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n-1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n-1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n-1$, we achieve the Černý bound if and only if $\phi(n) = n-1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q-1+p-1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p-1)(q-1) \geq q-1+p-1$.
- So $(\mathbb{Z}_{pq}, \{p,q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n-1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n-1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n-1$, we achieve the Černý bound if and only if $\phi(n) = n-1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q-1+p-1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p-1)(q-1) \geq q-1+p-1$.
- So $(\mathbb{Z}_{pq}, \{p,q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n - 1$, we achieve the Černý bound if and only if $\phi(n) = n - 1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

Cyclic groups

- The regular representation of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$ where the generator acts by multiplication by x.
- $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$ (ζ_d is a primitive d^{th}-root of unity).
- So $m(\mathbb{Z}_n) = \phi(n)$.
- As $\mathrm{diam}_{\{1\}}(\mathbb{Z}) = n - 1$, we achieve the Černý bound if and only if $\phi(n) = n - 1$.
- In particular, we recover Pin's Theorem, but not Dubuc's Theorem (although we are very close).
- Suppose $p < q$ are odd primes and $n = pq$.
- Then $\mathrm{diam}_{\{p,q\}}(\mathbb{Z}_n) = q - 1 + p - 1$ ($\mathbb{Z}_n \cong \mathbb{Z}_q \times \mathbb{Z}_p$).
- $\phi(n) = (p - 1)(q - 1) \geq q - 1 + p - 1$.
- So $(\mathbb{Z}_{pq}, \{p, q\})$ is a Černý Cayley graph.

Direct Products of Cyclic Groups of Prime Order

- Let p be a prime.
- To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayely graph with respect to a basis Δ.
- $\mathrm{diam}_\Delta(\mathbb{Z}_p^k) = k(p-1)$.
- One can prove $m(\mathbb{Z}_p^k) = p-1$: each irrep factors through a map to $\mathbb{Z}_p$.
- 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, all $k \geq 1$.

Direct Products of Cyclic Groups of Prime Order

- Let p be a prime.
- To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayely graph with respect to a basis Δ.
- $\mathrm{diam}_\Delta(\mathbb{Z}_p^k) = k(p-1)$.
- One can prove $m(\mathbb{Z}_p^k) = p-1$: each irrep factors through a map to $\mathbb{Z}_p$.
- 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, all $k \geq 1$.

Direct Products of Cyclic Groups of Prime Order

- Let p be a prime.
- To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayely graph with respect to a basis Δ.
- $\mathrm{diam}_\Delta(\mathbb{Z}_p^k) = k(p-1)$.
- One can prove $m(\mathbb{Z}_p^k) = p-1$: each irrep factors through a map to $\mathbb{Z}_p$.
- 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, all $k \geq 1$.

Direct Products of Cyclic Groups of Prime Order

- Let p be a prime.
- To show that $\mathbb{Z}_p^k$ is a Černý group, it suffices to consider the Cayely graph with respect to a basis Δ.
- $\mathrm{diam}_\Delta(\mathbb{Z}_p^k) = k(p-1)$.
- One can prove $m(\mathbb{Z}_p^k) = p - 1$: each irrep factors through a map to $\mathbb{Z}_p$.
- 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, all $k \geq 1$.

Dihedral Groups

- Let D_n be the dihedral group of order $2n$ (symmetry group of a regular n-gon).
- Let Δ consist of a reflection and a rotation by $2\pi/n$.
- Then $\mathrm{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$. (Act on $\mathbb{Q}(\zeta_n)$ by having the reflection act as complex conjugation and the rotation act as multiplication by ζ_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.

Dihedral Groups

- Let D_n be the dihedral group of order $2n$ (symmetry group of a regular n-gon).
- Let Δ consist of a reflection and a rotation by $2\pi/n$.
- Then $\mathrm{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$. (Act on $\mathbb{Q}(\zeta_n)$ by having the reflection act as complex conjugation and the rotation act as multiplication by ζ_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.

Dihedral Groups

- Let D_n be the dihedral group of order $2n$ (symmetry group of a regular n-gon).
- Let Δ consist of a reflection and a rotation by $2\pi/n$.
- Then $\mathrm{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$. (Act on $\mathbb{Q}(\zeta_n)$ by having the reflection act as complex conjugation and the rotation act as multiplication by ζ_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.

Dihedral Groups

- Let D_n be the dihedral group of order $2n$ (symmetry group of a regular n-gon).
- Let Δ consist of a reflection and a rotation by $2\pi/n$.
- Then $\mathrm{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$. (Act on $\mathbb{Q}(\zeta_n)$ by having the reflection act as complex conjugation and the rotation act as multiplication by ζ_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.

Dihedral Groups

- Let D_n be the dihedral group of order $2n$ (symmetry group of a regular n-gon).
- Let Δ consist of a reflection and a rotation by $2\pi/n$.
- Then $\mathrm{diam}_\Delta(D_n) \leq \lceil \frac{n+1}{2} \rceil$.
- One can prove $m(D_n) = \phi(n)$. (Act on $\mathbb{Q}(\zeta_n)$ by having the reflection act as complex conjugation and the rotation act as multiplication by ζ_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 over $\mathbb{Q}$ 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 over $\mathbb{Q}$ 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 over $\mathbb{Q}$ 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 over $\mathbb{Q}$ 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 over $\mathbb{Q}$ 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.

Affine Groups

- Let p be a prime.
- The affine group $AG(1,p)$ is the group of all functions $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the form $f(x) = ax + b$ with $a \in \mathbb{Z}_p^*$ and $b \in \mathbb{Z}_p$.
- $AG(1,p) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^*$.
- It turns out $m(AG(1,p)) = p - 1$ (act on $\mathbb{Q}[\zeta_p]$), which is not in general larger than the diameter.

Theorem (BS)

Let Δ be a generating set for $AG(1,p)$ so that each translation can be represented by a word in Δ^* of length at most $p-1$. Then $(AG(1,p),\Delta)$ is a Černý Cayley graph. This applies in particular if Δ contains a translation.

Affine Groups

- Let p be a prime.
- The affine group $AG(1,p)$ is the group of all functions $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the form $f(x) = ax + b$ with $a \in \mathbb{Z}_p^*$ and $b \in \mathbb{Z}_p$.
- $AG(1,p) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^*$.
- It turns out $m(AG(1,p)) = p - 1$ (act on $\mathbb{Q}[\zeta_p]$), which is not in general larger than the diameter.

Theorem (BS)

Let Δ be a generating set for $AG(1,p)$ so that each translation can be represented by a word in Δ^* of length at most $p-1$. Then $(AG(1,p),\Delta)$ is a Černý Cayley graph. This applies in particular if Δ contains a translation.

Special Linear Groups

- 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 Δ 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.

Special Linear Groups

- 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 Δ 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.

Special Linear Groups

- 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 Δ 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.

Characters

- To estimate $m(SL(2,p))$ we make use of character theory.
- Let $\varphi\colon G \to GL(V)$ be a representation of G over $K \leq \mathbb{C}$.
- The *character* χ_φ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$.
- $\chi_\varphi(1)$ is the degree of φ (it is the trace of the identity map).
- A representation is determined up to isomorphism by its character.
- If $|G| = n$, then $\chi_\varphi(g)$ is a sum of n^{th}-roots of unity.
- The *character field* $\mathbb{Q}(\chi_\varphi)$ is the field extension of $\mathbb{Q}$ generated by the $\chi_\varphi(g)$ with $g \in G$.
- It is a finite Galois extension of $\mathbb{Q}$.

Characters

- To estimate $m(SL(2,p))$ we make use of character theory.
- Let $\varphi\colon G \to GL(V)$ be a representation of G over $K \leq \mathbb{C}$.
- The *character* χ_φ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$.
- $\chi_\varphi(1)$ is the degree of φ (it is the trace of the identity map).
- A representation is determined up to isomorphism by its character.
- If $|G| = n$, then $\chi_\varphi(g)$ is a sum of n^{th}-roots of unity.
- The *character field* $\mathbb{Q}(\chi_\varphi)$ is the field extension of $\mathbb{Q}$ generated by the $\chi_\varphi(g)$ with $g \in G$.
- It is a finite Galois extension of $\mathbb{Q}$.

Characters

- To estimate $m(SL(2,p))$ we make use of character theory.
- Let $\varphi\colon G \to GL(V)$ be a representation of G over $K \leq \mathbb{C}$.
- The *character* χ_φ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$.
- $\chi_\varphi(1)$ is the degree of φ (it is the trace of the identity map).
- A representation is determined up to isomorphism by its character.
- If $|G| = n$, then $\chi_\varphi(g)$ is a sum of n^{th}-roots of unity.
- The *character field* $\mathbb{Q}(\chi_\varphi)$ is the field extension of $\mathbb{Q}$ generated by the $\chi_\varphi(g)$ with $g \in G$.
- It is a finite Galois extension of $\mathbb{Q}$.

Characters

- To estimate $m(SL(2,p))$ we make use of character theory.
- Let $\varphi\colon G \to GL(V)$ be a representation of G over $K \leq \mathbb{C}$.
- The *character* χ_φ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$.
- $\chi_\varphi(1)$ is the degree of φ (it is the trace of the identity map).
- A representation is determined up to isomorphism by its character.
- If $|G| = n$, then $\chi_\varphi(g)$ is a sum of n^{th}-roots of unity.
- The *character field* $\mathbb{Q}(\chi_\varphi)$ is the field extension of $\mathbb{Q}$ generated by the $\chi_\varphi(g)$ with $g \in G$.
- It is a finite Galois extension of $\mathbb{Q}$.

Characters

- To estimate $m(SL(2,p))$ we make use of character theory.
- Let $\varphi\colon G \to GL(V)$ be a representation of G over $K \leq \mathbb{C}$.
- The *character* χ_φ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$.
- $\chi_\varphi(1)$ is the degree of φ (it is the trace of the identity map).
- A representation is determined up to isomorphism by its character.
- If $|G| = n$, then $\chi_\varphi(g)$ is a sum of n^{th}-roots of unity.
- The *character field* $\mathbb{Q}(\chi_\varphi)$ is the field extension of $\mathbb{Q}$ generated by the $\chi_\varphi(g)$ with $g \in G$.
- It is a finite Galois extension of $\mathbb{Q}$.

Characters

- To estimate $m(SL(2,p))$ we make use of character theory.
- Let $\varphi\colon G \to GL(V)$ be a representation of G over $K \leq \mathbb{C}$.
- The *character* χ_φ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$.
- $\chi_\varphi(1)$ is the degree of φ (it is the trace of the identity map).
- A representation is determined up to isomorphism by its character.
- If $|G| = n$, then $\chi_\varphi(g)$ is a sum of n^{th}-roots of unity.
- The *character field* $\mathbb{Q}(\chi_\varphi)$ is the field extension of $\mathbb{Q}$ generated by the $\chi_\varphi(g)$ with $g \in G$.
- It is a finite Galois extension of $\mathbb{Q}$.

Schur Index

- Let χ be an irreducible complex character of G and let $H = \mathrm{Gal}(\mathbb{Q}(\chi) : \mathbb{Q})$.
- So $|H| = [\mathbb{Q}(\chi) : \mathbb{Q}]$.
- For $h \in H$, define $h \cdot \chi$ by $h \cdot \chi(g) = h(\chi(g))$.
- There is a unique integer $m(\chi)$ (called the *Schur index* of χ) so that

$$\tilde{\chi} = m(\chi) \cdot \sum_{h \in H} h \cdot \chi$$

is an irreducible rational character of G.
- All irreducible rational characters of G are obtained this way.
- The Schur index is difficult to calculate.
- But the degree of $\tilde{\chi}$ is $\tilde{\chi}(1) = m(\chi) \cdot |H| \cdot \chi(1) \geq [\mathbb{Q}(\chi) : \mathbb{Q}]\chi(1)$.

Schur Index

- Let χ be an irreducible complex character of G and let $H = \mathrm{Gal}(\mathbb{Q}(\chi) : \mathbb{Q})$.
- So $|H| = [\mathbb{Q}(\chi) : \mathbb{Q}]$.
- For $h \in H$, define $h \cdot \chi$ by $h \cdot \chi(g) = h(\chi(g))$.
- There is a unique integer $m(\chi)$ (called the *Schur index* of χ) so that

$$\tilde{\chi} = m(\chi) \cdot \sum_{h \in H} h \cdot \chi$$

  is an irreducible rational character of G.
- All irreducible rational characters of G are obtained this way.
- The Schur index is difficult to calculate.
- But the degree of $\tilde{\chi}$ is $\tilde{\chi}(1) = m(\chi) \cdot |H| \cdot \chi(1) \geq [\mathbb{Q}(\chi) : \mathbb{Q}]\chi(1)$.

Schur Index

- Let χ be an irreducible complex character of G and let $H = \mathrm{Gal}(\mathbb{Q}(\chi) : \mathbb{Q})$.
- So $|H| = [\mathbb{Q}(\chi) : \mathbb{Q}]$.
- For $h \in H$, define $h \cdot \chi$ by $h \cdot \chi(g) = h(\chi(g))$.
- There is a unique integer $m(\chi)$ (called the *Schur index* of χ) so that

$$\tilde{\chi} = m(\chi) \cdot \sum_{h \in H} h \cdot \chi$$

  is an irreducible rational character of G.
- All irreducible rational characters of G are obtained this way.
- The Schur index is difficult to calculate.
- But the degree of $\tilde{\chi}$ is $\tilde{\chi}(1) = m(\chi) \cdot |H| \cdot \chi(1) \geq [\mathbb{Q}(\chi) : \mathbb{Q}]\chi(1)$.

Schur Index

- Let χ be an irreducible complex character of G and let $H = \mathrm{Gal}(\mathbb{Q}(\chi) : \mathbb{Q})$.
- So $|H| = [\mathbb{Q}(\chi) : \mathbb{Q}]$.
- For $h \in H$, define $h \cdot \chi$ by $h \cdot \chi(g) = h(\chi(g))$.
- There is a unique integer $m(\chi)$ (called the *Schur index* of χ) so that

$$\tilde{\chi} = m(\chi) \cdot \sum_{h \in H} h \cdot \chi$$

  is an irreducible rational character of G.
- All irreducible rational characters of G are obtained this way.
- The Schur index is difficult to calculate.
- But the degree of $\tilde{\chi}$ is $\tilde{\chi}(1) = m(\chi) \cdot |H| \cdot \chi(1) \geq [\mathbb{Q}(\chi) : \mathbb{Q}]\chi(1)$.

Schur Index

- Let χ be an irreducible complex character of G and let $H = \mathrm{Gal}(\mathbb{Q}(\chi) : \mathbb{Q})$.
- So $|H| = [\mathbb{Q}(\chi) : \mathbb{Q}]$.
- For $h \in H$, define $h \cdot \chi$ by $h \cdot \chi(g) = h(\chi(g))$.
- There is a unique integer $m(\chi)$ (called the *Schur index* of χ) so that

$$\tilde{\chi} = m(\chi) \cdot \sum_{h \in H} h \cdot \chi$$

  is an irreducible rational character of G.
- All irreducible rational characters of G are obtained this way.
- The Schur index is difficult to calculate.
- But the degree of $\tilde{\chi}$ is $\tilde{\chi}(1) = m(\chi) \cdot |H| \cdot \chi(1) \geq [\mathbb{Q}(\chi) : \mathbb{Q}]\chi(1)$.

Schur Index

- Let χ be an irreducible complex character of G and let $H = \mathrm{Gal}(\mathbb{Q}(\chi) : \mathbb{Q})$.
- So $|H| = [\mathbb{Q}(\chi) : \mathbb{Q}]$.
- For $h \in H$, define $h \cdot \chi$ by $h \cdot \chi(g) = h(\chi(g))$.
- There is a unique integer $m(\chi)$ (called the *Schur index* of χ) so that

$$\tilde{\chi} = m(\chi) \cdot \sum_{h \in H} h \cdot \chi$$

  is an irreducible rational character of G.
- All irreducible rational characters of G are obtained this way.
- The Schur index is difficult to calculate.
- But the degree of $\tilde{\chi}$ is $\tilde{\chi}(1) = m(\chi) \cdot |H| \cdot \chi(1) \geq [\mathbb{Q}(\chi) : \mathbb{Q}]\chi(1)$.

$m(SL(2,p))$

- Computation of the irreducible complex characters of $SL(2,p)$ go back to Frobenius and Schur.
- $SL(2,p)$ has irreducible complex characters χ_1 and χ_2 of degrees $p+1$ and $p-1$ (respectively) with respective character fields $\mathbb{Q}(\cos\frac{2\pi}{p-1})$ and $\mathbb{Q}(\cos\frac{2\pi}{p+1})$.
- If $n \geq 3$, then $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}] = \phi(n)/2$.
- Thus $m(SL(2,p)) \geq \max\left\{(p+1)\frac{\phi(p-1)}{2}, (p-1)\frac{\phi(p+1)}{2}\right\}$.
- 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.*

$m(SL(2,p))$

- Computation of the irreducible complex characters of $SL(2,p)$ go back to Frobenius and Schur.
- $SL(2,p)$ has irreducible complex characters χ_1 and χ_2 of degrees $p+1$ and $p-1$ (respectively) with respective character fields $\mathbb{Q}(\cos\frac{2\pi}{p-1})$ and $\mathbb{Q}(\cos\frac{2\pi}{p+1})$.
- If $n \geq 3$, then $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}] = \phi(n)/2$.
- Thus $m(SL(2,p)) \geq \max\left\{(p+1)^{\frac{\phi(p-1)}{2}}, (p-1)^{\frac{\phi(p+1)}{2}}\right\}$.
- 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.

$m(SL(2,p))$

- Computation of the irreducible complex characters of $SL(2,p)$ go back to Frobenius and Schur.
- $SL(2,p)$ has irreducible complex characters χ_1 and χ_2 of degrees $p+1$ and $p-1$ (respectively) with respective character fields $\mathbb{Q}(\cos\frac{2\pi}{p-1})$ and $\mathbb{Q}(\cos\frac{2\pi}{p+1})$.
- If $n \geq 3$, then $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}] = \phi(n)/2$.
- Thus $m(SL(2,p)) \geq \max\left\{(p+1)\frac{\phi(p-1)}{2}, (p-1)\frac{\phi(p+1)}{2}\right\}$.
- 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.

$m(SL(2,p))$

- Computation of the irreducible complex characters of $SL(2,p)$ go back to Frobenius and Schur.
- $SL(2,p)$ has irreducible complex characters χ_1 and χ_2 of degrees $p+1$ and $p-1$ (respectively) with respective character fields $\mathbb{Q}(\cos\frac{2\pi}{p-1})$ and $\mathbb{Q}(\cos\frac{2\pi}{p+1})$.
- If $n \geq 3$, then $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}] = \phi(n)/2$.
- Thus $m(SL(2,p)) \geq \max\left\{(p+1)\frac{\phi(p-1)}{2}, (p-1)\frac{\phi(p+1)}{2}\right\}$.
- 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.

$m(SL(2,p))$

- Computation of the irreducible complex characters of $SL(2,p)$ go back to Frobenius and Schur.
- $SL(2,p)$ has irreducible complex characters χ_1 and χ_2 of degrees $p+1$ and $p-1$ (respectively) with respective character fields $\mathbb{Q}(\cos\frac{2\pi}{p-1})$ and $\mathbb{Q}(\cos\frac{2\pi}{p+1})$.
- If $n \geq 3$, then $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}] = \phi(n)/2$.
- Thus $m(SL(2,p)) \geq \max\left\{(p+1)\frac{\phi(p-1)}{2}, (p-1)\frac{\phi(p+1)}{2}\right\}$.
- 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.

The Main Idea

- Let (G, Σ) be a synchronizing automaton containing the Cayley graph of (G, Δ).
- Our goal is to show that, for any $S \subsetneq G$, there exists $w \in \Sigma^*$ so that $|w| \leq n - m(G) + \mathrm{diam}_\Delta(G)$ and $|Sw^{-1}| > |S|$.
- With one letter we can "expand" a subset of size 1 to size 2.
- Then we expand $n-2$ times by words of length at most $n - m(G) + \mathrm{diam}_\Delta(G)$.
- This gives a reset word of length at most $1 + (n - m(G) + \mathrm{diam}_\Delta(G))(n-2)$.
- We do this by studying the tower $\{V_k\}$ of G-invariant subspace of the regular representation of G where

$$V_0 = G \cdot \chi_S \quad \text{and} \quad V_k = G \cdot \Sigma \cdot V_{k-1}.$$

The Main Idea

- Let (G, Σ) be a synchronizing automaton containing the Cayley graph of (G, Δ).
- Our goal is to show that, for any $S \subsetneq G$, there exists $w \in \Sigma^*$ so that $|w| \leq n - m(G) + \mathrm{diam}_\Delta(G)$ and $|Sw^{-1}| > |S|$.
- With one letter we can "expand" a subset of size 1 to size 2.
- Then we expand $n-2$ times by words of length at most $n - m(G) + \mathrm{diam}_\Delta(G)$.
- This gives a reset word of length at most $1 + (n - m(G) + \mathrm{diam}_\Delta(G))(n-2)$.
- We do this by studying the tower $\{V_k\}$ of G-invariant subspace of the regular representation of G where

$$V_0 = G \cdot \chi_S \quad \text{and} \quad V_k = G \cdot \Sigma \cdot V_{k-1}.$$

The Main Idea

- Let (G, Σ) be a synchronizing automaton containing the Cayley graph of (G, Δ).
- Our goal is to show that, for any $S \subsetneq G$, there exists $w \in \Sigma^*$ so that $|w| \leq n - m(G) + \mathrm{diam}_\Delta(G)$ and $|Sw^{-1}| > |S|$.
- With one letter we can "expand" a subset of size 1 to size 2.
- Then we expand $n-2$ times by words of length at most $n - m(G) + \mathrm{diam}_\Delta(G)$.
- This gives a reset word of length at most $1 + (n - m(G) + \mathrm{diam}_\Delta(G))(n-2)$.
- We do this by studying the tower $\{V_k\}$ of G-invariant subspace of the regular representation of G where

$$V_0 = G \cdot \chi_S \quad \text{and} \quad V_k = G \cdot \Sigma \cdot V_{k-1}.$$

The Main Idea

- Let (G, Σ) be a synchronizing automaton containing the Cayley graph of (G, Δ).
- Our goal is to show that, for any $S \subsetneq G$, there exists $w \in \Sigma^*$ so that $|w| \leq n - m(G) + \mathrm{diam}_\Delta(G)$ and $|Sw^{-1}| > |S|$.
- With one letter we can "expand" a subset of size 1 to size 2.
- Then we expand $n-2$ times by words of length at most $n - m(G) + \mathrm{diam}_\Delta(G)$.
- This gives a reset word of length at most $1 + (n - m(G) + \mathrm{diam}_\Delta(G))(n-2)$.
- We do this by studying the tower $\{V_k\}$ of G-invariant subspace of the regular representation of G where

$$V_0 = G \cdot \chi_S \quad \text{and} \quad V_k = G \cdot \Sigma \cdot V_{k-1}.$$

The Main Idea

- Let (G, Σ) be a synchronizing automaton containing the Cayley graph of (G, Δ).
- Our goal is to show that, for any $S \subsetneq G$, there exists $w \in \Sigma^*$ so that $|w| \leq n - m(G) + \mathrm{diam}_\Delta(G)$ and $|Sw^{-1}| > |S|$.
- With one letter we can "expand" a subset of size 1 to size 2.
- Then we expand $n-2$ times by words of length at most $n - m(G) + \mathrm{diam}_\Delta(G)$.
- This gives a reset word of length at most $1 + (n - m(G) + \mathrm{diam}_\Delta(G))(n-2)$.
- We do this by studying the tower $\{V_k\}$ of G-invariant subspace of the regular representation of G where

$$V_0 = G \cdot \chi_S \quad \text{and} \quad V_k = G \cdot \Sigma \cdot V_{k-1}.$$

The Main Idea

- Let (G, Σ) be a synchronizing automaton containing the Cayley graph of (G, Δ).
- Our goal is to show that, for any $S \subsetneq G$, there exists $w \in \Sigma^*$ so that $|w| \leq n - m(G) + \mathrm{diam}_\Delta(G)$ and $|Sw^{-1}| > |S|$.
- With one letter we can "expand" a subset of size 1 to size 2.
- Then we expand $n-2$ times by words of length at most $n - m(G) + \mathrm{diam}_\Delta(G)$.
- This gives a reset word of length at most $1 + (n - m(G) + \mathrm{diam}_\Delta(G))(n-2)$.
- We do this by studying the tower $\{V_k\}$ of G-invariant subspace of the regular representation of G where

$$V_0 = G \cdot \chi_S \quad \text{and} \quad V_k = G \cdot \Sigma \cdot V_{k-1}.$$

Open Questions

- 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?

Open Questions

- 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?

Open Questions

- 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?

Open Questions

- 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?

Open Questions

- 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?

The End

Thanks for your attention!