Graphical regular representations of groups of prescribed valency

Binzhou Xia

University of Melbourne

AAC01 Sydney

König's conjecture

In the interplay of group theory with some other branches of mathematics, a typical question is whether a given group can be represented as the group of symmetries of certain mathematical object.

König's conjecture

In the interplay of group theory with some other branches of mathematics, a typical question is whether a given group can be represented as the group of symmetries of certain mathematical object.

As to graphs, the problem of whether a group can be represented as the automorphism group of a graph was considered at a very early stage of graph theory.

König's conjecture

In the interplay of group theory with some other branches of mathematics, a typical question is whether a given group can be represented as the group of symmetries of certain mathematical object.

As to graphs, the problem of whether a group can be represented as the automorphism group of a graph was considered at a very early stage of graph theory.

A graph Γ ia a pair (V, E), where V is a set and E is a set of 2-subsets of V. Elements of V are the vertices and elements of E are the edges.

König's conjecture

In the interplay of group theory with some other branches of mathematics, a typical question is whether a given group can be represented as the group of symmetries of certain mathematical object.

As to graphs, the problem of whether a group can be represented as the automorphism group of a graph was considered at a very early stage of graph theory.

A graph Γ ia a pair (V, E), where V is a set and E is a set of 2-subsets of V. Elements of V are the vertices and elements of E are the edges. An automorphism of Γ ia a permutation of V that preserves E. All the automorphisms form the automorphism group of Γ, denoted $\mathrm{Aut}(\Gamma)$.

König's conjecture

In the interplay of group theory with some other branches of mathematics, a typical question is whether a given group can be represented as the group of symmetries of certain mathematical object.

As to graphs, the problem of whether a group can be represented as the automorphism group of a graph was considered at a very early stage of graph theory.

A graph Γ ia a pair (V, E), where V is a set and E is a set of 2-subsets of V. Elements of V are the vertices and elements of E are the edges. An automorphism of Γ ia a permutation of V that preserves E. All the automorphisms form the automorphism group of Γ, denoted $\mathrm{Aut}(\Gamma)$.

König conjectured in his 1936 book "Theorie der endlichen und unendlichen Graphen', the first textbook on the field of graph theory, that every finite group is the automorphism group of a finite graph.

König's conjecture

In the interplay of group theory with some other branches of mathematics, a typical question is whether a given group can be represented as the group of symmetries of certain mathematical object.

As to graphs, the problem of whether a group can be represented as the automorphism group of a graph was considered at a very early stage of graph theory.

A graph Γ ia a pair (V, E), where V is a set and E is a set of 2-subsets of V. Elements of V are the vertices and elements of E are the edges. An automorphism of Γ ia a permutation of V that preserves E. All the automorphisms form the automorphism group of Γ, denoted $\mathrm{Aut}(\Gamma)$.

König conjectured in his 1936 book "Theorie der endlichen und unendlichen Graphen', the first textbook on the field of graph theory, that every finite group is the automorphism group of a finite graph.

Frucht's theorem

- König's conjecture was proved by Frucht in 1939[1].

[1] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.*, 6 (1939), 239–250.

Frucht's theorem

- König's conjecture was proved by Frucht in 1939[1].
- In 1949, Frucht[2] proved a stronger version stating that every finite group is the automorphism group of a cubic graph (every vertex is adjacent to exactly three vertices).

[1] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.*, 6 (1939), 239–250.

[2] R. Frucht, Graphs of degree three with a given abstract group, *Canadian J. Math.*, 1 (1949), 365–378.

Frucht's theorem

- König's conjecture was proved by Frucht in 1939[1].
- In 1949, Frucht[2] proved a stronger version stating that every finite group is the automorphism group of a cubic graph (every vertex is adjacent to exactly three vertices).
- In 1957, Sabidussi[3] proved that for all integers $k \geqslant 3$, every finite group is the automorphism group of a k-valent graph (every vertex is adjacent to exactly k vertices).

[1] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.*, 6 (1939), 239–250.

[2] R. Frucht, Graphs of degree three with a given abstract group, *Canadian J. Math.*, 1 (1949), 365–378.

[3] G. Sabidussi, Graphs with given group and given graph-theoretical properties, *Canadian J. Math.*, 9 (1957), 515–525.

Frucht's theorem

- König's conjecture was proved by Frucht in 1939[1].
- In 1949, Frucht[2] proved a stronger version stating that every finite group is the automorphism group of a cubic graph (every vertex is adjacent to exactly three vertices).
- In 1957, Sabidussi[3] proved that for all integers $k \geqslant 3$, every finite group is the automorphism group of a k-valent graph (every vertex is adjacent to exactly k vertices).

In the above theorems, the group may not act transitively on the vertex set and may not have the same order as the graph.

[1] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.*, 6 (1939), 239–250.

[2] R. Frucht, Graphs of degree three with a given abstract group, *Canadian J. Math.*, 1 (1949), 365–378.

[3] G. Sabidussi, Graphs with given group and given graph-theoretical properties, *Canadian J. Math.*, 9 (1957), 515–525.

Graphic regular representation

Graphic regular representation

A graph Γ is called a graphic regular representation (GRR) of a group G if $\mathrm{Aut}(\Gamma) \cong G$ acts regularly on the vertex set of Γ.

Graphic regular representation

A graph Γ is called a graphic regular representation (GRR) of a group G if $\mathrm{Aut}(\Gamma) \cong G$ acts regularly on the vertex set of Γ.

After considerable work by many authors, Godsil at the end of 1970's[4] was able to determine which finite groups have a GRR.

[4] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, pp. 221–239, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.

Graphic regular representation

A graph Γ is called a graphic regular representation (GRR) of a group G if $\mathrm{Aut}(\Gamma) \cong G$ acts regularly on the vertex set of Γ.

After considerable work by many authors, Godsil at the end of 1970's[4] was able to determine which finite groups have a GRR.

However, a Sabidussi-like theorem concerning GRRs of a prescribed valency is still far out of reach

[4] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, pp. 221–239, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.

Graphic regular representation

A graph Γ is called a graphic regular representation (GRR) of a group G if $\mathrm{Aut}(\Gamma) \cong G$ acts regularly on the vertex set of Γ.

After considerable work by many authors, Godsil at the end of 1970's[4] was able to determine which finite groups have a GRR.

However, a Sabidussi-like theorem concerning GRRs of a prescribed valency is still far out of reach — even for a Frucht-like theorem on cubic GRRs[5].

[4] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, pp. 221–239, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.

[5] H. S. M. Coxeter, R. Frucht and D. L. Powers, *Zero-symmetric graphs*, trivalent graphical regular representations of groups, Academic Press, New York-London, 1981.

Graphic regular representation

A graph Γ is called a graphic regular representation (GRR) of a group G if $\mathrm{Aut}(\Gamma) \cong G$ acts regularly on the vertex set of Γ.

After considerable work by many authors, Godsil at the end of 1970's[4] was able to determine which finite groups have a GRR.

However, a Sabidussi-like theorem concerning GRRs of a prescribed valency is still far out of reach — even for a Frucht-like theorem on cubic GRRs[5].

In 2002, Fang, Li, Wang and Xu[6] conjectured that every finite nonabelian simple group has a cubic GRR and tetravalent GRR.

[4] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, pp. 221–239, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.

[5] H. S. M. Coxeter, R. Frucht and D. L. Powers, *Zero-symmetric graphs*, trivalent graphical regular representations of groups, Academic Press, New York-London, 1981.

Graphic regular representation

A graph Γ is called a graphic regular representation (GRR) of a group G if $\mathrm{Aut}(\Gamma) \cong G$ acts regularly on the vertex set of Γ.

After considerable work by many authors, Godsil at the end of 1970's[4] was able to determine which finite groups have a GRR.

However, a Sabidussi-like theorem concerning GRRs of a prescribed valency is still far out of reach — even for a Frucht-like theorem on cubic GRRs[5].

In 2002, Fang, Li, Wang and Xu[6] conjectured that every finite nonabelian simple group has a cubic GRR and tetravalent GRR.

[4] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, pp. 221–239, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.

[5] H. S. M. Coxeter, R. Frucht and D. L. Powers, *Zero-symmetric graphs*, trivalent graphical regular representations of groups, Academic Press, New York-London, 1981.

[6] X. G. Fang, C. H. Li, J. Wang and M. Y. Xu, On cubic Cayley graphs of finite simple groups, *Discrete Math.*, 244 (2002), no. 1-3, 67–75.

Cayley graph

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.
- $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.
- $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.
- Let R be the right regular representation. Then $R(G)$ is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$.

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.
- $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.
- Let R be the right regular representation. Then $R(G)$ is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$.
- Conversely, a graph whose automorphism group has a subgroup G regular on the vertex set is isomorphic to a Cayley graph of G.

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.
- $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.
- Let R be the right regular representation. Then $R(G)$ is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$.
- Conversely, a graph whose automorphism group has a subgroup G regular on the vertex set is isomorphic to a Cayley graph of G.

Thus a GRR of a group G is a Cayley graph of G with smallest possible automorphism group:

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.
- $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.
- Let R be the right regular representation. Then $R(G)$ is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$.
- Conversely, a graph whose automorphism group has a subgroup G regular on the vertex set is isomorphic to a Cayley graph of G.

Thus a GRR of a group G is a Cayley graph of G with smallest possible automorphism group:

$\mathrm{Cay}(G, S)$ is a GRR of G iff $\mathrm{Aut}(\mathrm{Cay}(G, S)) = R(G)$.

Cayley graph

Given a group G and an inverse-closed subset S of $G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S is the graph with vertex set G and edge set $\{\{x, sx\} \mid x \in G,\ s \in S\}$.

- $\mathrm{Cay}(G, S)$ is $|S|$-valent.
- $\mathrm{Cay}(G, S)$ is connected if and only if S generates G.
- Let R be the right regular representation. Then $R(G)$ is a subgroup of $\mathrm{Aut}(\mathrm{Cay}(G, S))$.
- Conversely, a graph whose automorphism group has a subgroup G regular on the vertex set is isomorphic to a Cayley graph of G.

Thus a GRR of a group G is a Cayley graph of G with smallest possible automorphism group:

$\mathrm{Cay}(G, S)$ is a GRR of G iff $\mathrm{Aut}(\mathrm{Cay}(G, S)) = R(G)$.

In this case, S is a generating set of G.

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs:

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs: every finite nonbelian simple group has a cubic GRR.

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs: every finite nonbelian simple group has a cubic GRR.

- The alternating group A_n with $n \geqslant 5$ has a cubic GRR (Godsil 1983).

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs: every finite nonbelian simple group has a cubic GRR.

- The alternating group A_n with $n \geqslant 5$ has a cubic GRR (Godsil 1983).
- The Suzuki group ${}^2\mathrm{B}_2(q)$ with $q = 2^{2c+1} \geqslant 8$ has a cubic GRR (Fang-Li-Wang-Xu 2002).

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs: every finite nonbelian simple group has a cubic GRR.

- The alternating group A_n with $n \geqslant 5$ has a cubic GRR (Godsil 1983).
- The Suzuki group ${}^2\mathrm{B}_2(q)$ with $q = 2^{2c+1} \geqslant 8$ has a cubic GRR (Fang-Li-Wang-Xu 2002).
- The 2-dimensional projective special linear group $\mathrm{PSL}_2(q)$ with $q \geqslant 4$ has a cubic GRR iff $q \neq 7$ (Fang-X. 2016).

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs: every finite nonbelian simple group has a cubic GRR.

- The alternating group A_n with $n \geqslant 5$ has a cubic GRR (Godsil 1983).
- The Suzuki group ${}^2\mathrm{B}_2(q)$ with $q = 2^{2c+1} \geqslant 8$ has a cubic GRR (Fang-Li-Wang-Xu 2002).
- The 2-dimensional projective special linear group $\mathrm{PSL}_2(q)$ with $q \geqslant 4$ has a cubic GRR iff $q \neq 7$ (Fang-X. 2016). In particular, $\mathrm{PSL}_2(7)$ is a counterexample to the Fang-Li-Wang-Xu conjecture.

Cubic GRRs of finite simple groups

The Fang-Li-Wang-Xu conjecture on cubic GRRs: every finite nonbelian simple group has a cubic GRR.

- The alternating group A_n with $n \geqslant 5$ has a cubic GRR (Godsil 1983).
- The Suzuki group ${}^2\mathrm{B}_2(q)$ with $q = 2^{2c+1} \geqslant 8$ has a cubic GRR (Fang-Li-Wang-Xu 2002).
- The 2-dimensional projective special linear group $\mathrm{PSL}_2(q)$ with $q \geqslant 4$ has a cubic GRR iff $q \neq 7$ (Fang-X. 2016). In particular, $\mathrm{PSL}_2(7)$ is a counterexample to the Fang-Li-Wang-Xu conjecture.

Conjecture (Fang-X. 2016)

There are only finitely many finite nonabelian simple groups that have no cubic GRR.

More on cubic GRRs of $\mathrm{PSL}_2(q)$

More on cubic GRRs of $\mathrm{PSL}_2(q)$

If $\mathrm{Cay}(G,S)$ is a cubic GRR of G, then S either consists of three involutions or contains exactly one involution.

More on cubic GRRs of $\mathrm{PSL}_2(q)$

If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S either consists of three involutions or contains exactly one involution.

Theorem (Fang-X. 2016)

More on cubic GRRs of $\mathrm{PSL}_2(q)$

If $\mathrm{Cay}(G,S)$ is a cubic GRR of G, then S either consists of three involutions or contains exactly one involution.

Theorem (Fang-X. 2016)

Let $G=\mathrm{PSL}_2(q)$ with $q\geqslant 4$.

More on cubic GRRs of $\mathrm{PSL}_2(q)$

If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S either consists of three involutions or contains exactly one involution.

Theorem (Fang-X. 2016)

Let $G = \mathrm{PSL}_2(q)$ with $q \geqslant 4$.

(a) If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S is a set of three involutions.

More on cubic GRRs of $\mathrm{PSL}_2(q)$

If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S either consists of three involutions or contains exactly one involution.

Theorem (Fang-X. 2016)

Let $G = \mathrm{PSL}_2(q)$ with $q \geqslant 4$.

(a) If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S is a set of three involutions.

(b) If $q \neq 7$, then there exists three involutions x, y and z in G such that $\mathrm{Cay}(G, \{x, y, z\})$ is a cubic GRR of G.

More on cubic GRRs of $\mathrm{PSL}_2(q)$

If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S either consists of three involutions or contains exactly one involution.

Theorem (Fang-X. 2016)

Let $G = \mathrm{PSL}_2(q)$ with $q \geqslant 4$.

(a) If $\mathrm{Cay}(G, S)$ is a cubic GRR of G, then S is a set of three involutions.

(b) If $q \neq 7$, then there exists three involutions x, y and z in G such that $\mathrm{Cay}(G, \{x, y, z\})$ is a cubic GRR of G.

(c) There exist involutions x and y in G such that the probability for a randomly chosen involution z to make $\mathrm{Cay}(G, \{x, y, z\})$ a cubic GRR of G tends to 1 as q tends to infinity.

Spiga's conjectures

Inspired by our work, Spiga recently posed the following conjectures:

Spiga's conjectures

Inspired by our work, Spiga recently posed the following conjectures:

Conjecture (Spiga 2017)

Spiga's conjectures

Inspired by our work, Spiga recently posed the following conjectures:

Conjecture (Spiga 2017)

(i) Except for a finite number of cases, every finite nonabelian simple group G contains three involutions x, y and z such that $\mathrm{Cay}(G, \{x, y, z\})$ is a cubic GRR of G.

Spiga's conjectures

Inspired by our work, Spiga recently posed the following conjectures:

Conjecture (Spiga 2017)

(i) Except for a finite number of cases, every finite nonabelian simple group G contains three involutions x, y and z such that $\mathrm{Cay}(G, \{x, y, z\})$ is a cubic GRR of G.

(ii) Except for a finite number of cases and for the groups $\mathrm{PSL}_2(q)$, every finite nonabelian simple group G contains an element x and an involution y such that $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ is a cubic GRR of G.

Spiga's conjectures

Inspired by our work, Spiga recently posed the following conjectures:

Conjecture (Spiga 2017)

(i) Except for a finite number of cases, every finite nonabelian simple group G contains three involutions x, y and z such that $\mathrm{Cay}(G, \{x, y, z\})$ is a cubic GRR of G.

(ii) Except for a finite number of cases and for the groups $\mathrm{PSL}_2(q)$, every finite nonabelian simple group G contains an element x and an involution y such that $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ is a cubic GRR of G.

(iii) The proportion of cubic Cayley graphs (up to isomorphism) over a finite nonabelian simple group G that are GRRs tends to 1 as $|G|$ tends to infinity.

My result

Theorem (X. 2017+)

My result

Theorem (X. 2017+)

Let G be a finite simple group of Lie type of rank at least 9. Then there exists an element x of prime order in G such that the probability for a random involution y in G to make $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ a cubic GRR of G tends to 1 as $|G|$ tends to infinity.

My result

Theorem (X. 2017+)

Let G be a finite simple group of Lie type of rank at least 9. Then there exists an element x of prime order in G such that the probability for a random involution y in G to make $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ a cubic GRR of G tends to 1 as $|G|$ tends to infinity.

- The theorem gives an affirmative answer to Spiga's conjecture (ii) for finite simple groups of Lie type of rank at least 9, and also gives evidence for Spiga's conjecture (iii).

My result

Theorem (X. 2017+)

Let G be a finite simple group of Lie type of rank at least 9. Then there exists an element x of prime order in G such that the probability for a random involution y in G to make $\mathrm{Cay}(G, \{x, x^{-1}, y\})$ a cubic GRR of G tends to 1 as $|G|$ tends to infinity.

- The theorem gives an affirmative answer to Spiga's conjecture (ii) for finite simple groups of Lie type of rank at least 9, and also gives evidence for Spiga's conjecture (iii).
- The theorem implies that there are at most finitely many finite simple groups of Lie type of rank at least 9 that have no cubic GRR, which reduces the verification of our conjecture "Only finitely many finite nonabelian simple groups have no cubic GRR" to finite simple groups of Lie type of rank at most 8.

A byproduct

A byproduct

Let G be a finite simple group of Lie type of rank at least 9.

A byproduct

Let G be a finite simple group of Lie type of rank at least 9. According to the theorem, there exists an element x of prime order in G such that the probability for a random involution y in G to make $\{x, y\}$ a generating set of G tends to 1 as $|G|$ tends to infinity.

A byproduct

Let G be a finite simple group of Lie type of rank at least 9. According to the theorem, there exists an element x of prime order in G such that the probability for a random involution y in G to make $\{x, y\}$ a generating set of G tends to 1 as $|G|$ tends to infinity.

- By a classic result of Liebeck and Shalev, most finite nonabelian simple groups can be generated by an involution and an element of order three[7].

[7] M. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Ann. of Math. (2)*, 144 (1996), no. 1, 77–125.

A byproduct

Let G be a finite simple group of Lie type of rank at least 9. According to the theorem, there exists an element x of prime order in G such that the probability for a random involution y in G to make $\{x, y\}$ a generating set of G tends to 1 as $|G|$ tends to infinity.

- By a classic result of Liebeck and Shalev, most finite nonabelian simple groups can be generated by an involution and an element of order three[7].
- Recently, King proved that every finite nonabelian simple group can be generated by an involution and an element of prime order[8].

[7] M. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Ann. of Math. (2)*, 144 (1996), no. 1, 77–125.

[8] C. S. H. King, Generation of finite simple groups by an involution and an element of prime order, *J. Algebra* 478 (2017), 153–173.

A byproduct

Let G be a finite simple group of Lie type of rank at least 9. According to the theorem, there exists an element x of prime order in G such that the probability for a random involution y in G to make $\{x, y\}$ a generating set of G tends to 1 as $|G|$ tends to infinity.

- By a classic result of Liebeck and Shalev, most finite nonabelian simple groups can be generated by an involution and an element of order three[7].
- Recently, King proved that every finite nonabelian simple group can be generated by an involution and an element of prime order[8].

The byproduct is an asymptotic version of King's result.

[7] M. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Ann. of Math. (2)*, 144 (1996), no. 1, 77–125.

[8] C. S. H. King, Generation of finite simple groups by an involution and an element of prime order, *J. Algebra* 478 (2017), 153–173.

Thank you for listening!