Is Babai afraid of spiders?

Nick Gill (OU)

July 4, 2011

Joint with Helfgott (ENS); Bamberg, Royle, Seress, Spiga (UWA).

Babai's conjecture

For G a group, S a set of generators of G, write $\Gamma(G, S)$ for the **Cayley graph of G with respect to S.**

Babai's conjecture

For G a group, S a set of generators of G, write $\Gamma(G, S)$ for the **Cayley graph of G with respect to S.**

Conjecture (Babai)

There exists $c > 0$ such that, for G a finite simple group, and $S \subseteq G$ a set of generators, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

Babai's conjecture

For G a group, S a set of generators of G, write $\Gamma(G,S)$ for the **Cayley graph of G with respect to S.**

Conjecture (Babai)

There exists $c > 0$ such that, for G a finite simple group, and $S \subseteq G$ a set of generators, we have

$$\mathrm{diam}(\Gamma(G,S)) \leq (\log|G|)^c.$$

This has been proved for G a finite group of Lie type of bounded rank. The conjecture is open for groups of Lie type of unbounded rank, and for the alternating groups.

A result of Babai-Beals-Seress

From here on $G = A_n$, and S is a set of generators for G.

A result of Babai-Beals-Seress

From here on $G = A_n$, and S is a set of generators for G.
For $g \in A_n$ write $\mathrm{supp}(g)$ for the set of elements in $[1, n]$ that are moved by g.

A result of Babai-Beals-Seress

From here on $G = A_n$, and S is a set of generators for G.
For $g \in A_n$ write $\mathrm{supp}(g)$ for the set of elements in $[1, n]$ that are moved by g.

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (\frac{1}{3} - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

A result of Babai-Beals-Seress

From here on $G = A_n$, and S is a set of generators for G.
For $g \in A_n$ write $\mathrm{supp}(g)$ for the set of elements in $[1, n]$ that are moved by g.

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (\frac{1}{3} - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

We prove this by showing that we can write all elements of G as words (in elements of S) of length $\leq (\log |G|)^c \sim n^c$. (Stirling's formula)

The proof of BBS' result

1. We consider a lazy random walk on $\Gamma(G, S)$; we obtain *mixing elements h* as words of length n^4;

The proof of BBS' result

1. We consider a lazy random walk on $\Gamma(G, S)$; we obtain *mixing elements* h as words of length n^4;
2. We show that $\mathbb{E}(\mathrm{supp}([g, g^h])) < \mathrm{supp}(g)\frac{1}{1+\sqrt{\epsilon}} = (\frac{1}{3} - \epsilon)n\frac{1}{1+\sqrt{\epsilon}}$;

The proof of BBS' result

1. We consider a lazy random walk on $\Gamma(G,S)$; we obtain *mixing elements h* as words of length n^4;
2. We show that $\mathbb{E}(\mathrm{supp}([g,g^h])) < \mathrm{supp}(g)\frac{1}{1+\sqrt{\epsilon}} = (\frac{1}{3}-\epsilon)n\frac{1}{1+\sqrt{\epsilon}}$;
3. We repeat the previous step $\log_{1+\sqrt{\epsilon}}((\frac{1}{3}-\epsilon)n)$ times, to get a word of length n^e that is a 3-cycle (here e depends only on ϵ);

The proof of BBS' result

1. We consider a lazy random walk on $\Gamma(G,S)$; we obtain *mixing elements h* as words of length n^4;
2. We show that $\mathbb{E}(\mathrm{supp}([g,g^h])) < \mathrm{supp}(g)\frac{1}{1+\sqrt{\epsilon}} = (\frac{1}{3}-\epsilon)n\frac{1}{1+\sqrt{\epsilon}}$;
3. We repeat the previous step $\log_{1+\sqrt{\epsilon}}((\frac{1}{3}-\epsilon)n)$ times, to get a word of length n^e that is a 3-cycle (here e depends only on ϵ);
4. We conjugate by elements of A at most $\frac{1}{3}n(n-1)(n-2)$ times to get all 3-cycles as words of length n^{e+3};

The proof of BBS' result

1. We consider a lazy random walk on $\Gamma(G,S)$; we obtain *mixing elements* h as words of length n^4;
2. We show that $\mathbb{E}(\mathrm{supp}([g,g^h])) < \mathrm{supp}(g)\frac{1}{1+\sqrt{\epsilon}} = (\frac{1}{3}-\epsilon)n\frac{1}{1+\sqrt{\epsilon}}$;
3. We repeat the previous step $\log_{1+\sqrt{\epsilon}}((\frac{1}{3}-\epsilon)n)$ times, to get a word of length n^e that is a 3-cycle (here e depends only on ϵ);
4. We conjugate by elements of A at most $\frac{1}{3}n(n-1)(n-2)$ times to get all 3-cycles as words of length n^{e+3};
5. All elements of G can be written as a product of n 3-cycles, i.e. as words of length n^{e+4} in elements of S.

The proof of BBS' result

1. We consider a lazy random walk on $\Gamma(G, S)$; we obtain *mixing elements h* as words of length n^4;
2. We show that $\mathbb{E}(\mathrm{supp}([g, g^h])) < \mathrm{supp}(g)\frac{1}{1+\sqrt{\epsilon}} = (\frac{1}{3} - \epsilon)n\frac{1}{1+\sqrt{\epsilon}}$;
3. We repeat the previous step $\log_{1+\sqrt{\epsilon}}((\frac{1}{3} - \epsilon)n)$ times, to get a word of length n^e that is a 3-cycle (here e depends only on ϵ);
4. We conjugate by elements of A at most $\frac{1}{3}n(n-1)(n-2)$ times to get all 3-cycles as words of length n^{e+3};
5. All elements of G can be written as a product of n 3-cycles, i.e. as words of length n^{e+4} in elements of S.

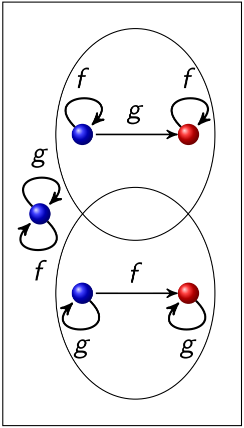
QED

An improvement to $\frac{1}{2} - \epsilon$

Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.

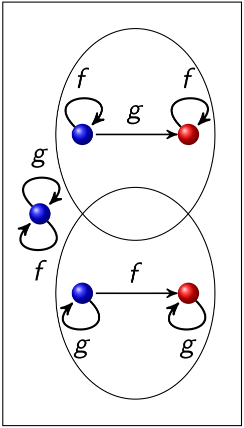
An improvement to $\frac{1}{2} - \epsilon$

Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



An improvement to $\frac{1}{2} - \epsilon$

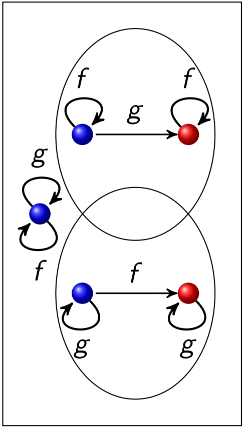
Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



- $|\mathrm{supp}(g)| = |\mathrm{supp}(f)| = \delta n$;

An improvement to $\frac{1}{2} - \epsilon$

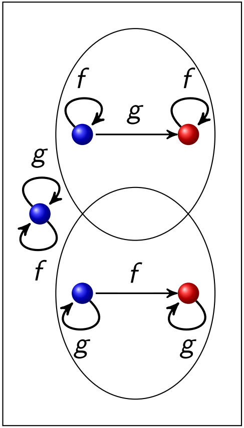
Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



- $|\,\mathrm{supp}(g)| = |\,\mathrm{supp}(f)| = \delta n$;
- $|(\mathrm{supp}(g) \cup \mathrm{supp}(f))| = (2\delta - \delta^2)n$;

An improvement to $\frac{1}{2} - \epsilon$

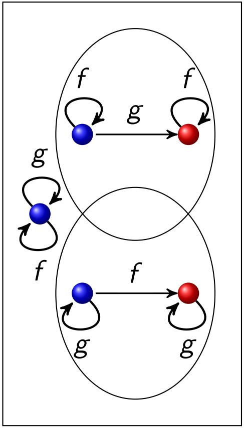
Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



- $|\mathrm{supp}(g)| = |\mathrm{supp}(f)| = \delta n$;
- $|(\mathrm{supp}(g) \cup \mathrm{supp}(f))| = (2\delta - \delta^2)n$;
- The number of blue nodes in $\mathrm{supp}(g)$ is $[\delta(1-\delta)^2]n$;

An improvement to $\frac{1}{2} - \epsilon$

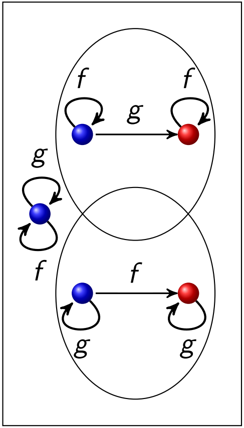
Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



- $|\mathrm{supp}(g)| = |\mathrm{supp}(f)| = \delta n$;
- $|(\mathrm{supp}(g) \cup \mathrm{supp}(f))| = (2\delta - \delta^2)n$;
- The number of blue nodes in $\mathrm{supp}(g)$ is $[\delta(1-\delta)^2]n$;
- The number of blue nodes in $\mathrm{supp}(f)$ is $[\delta(1-\delta)^2]n$;

An improvement to $\frac{1}{2} - \epsilon$

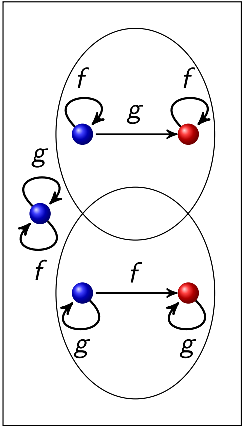
Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



- $|\mathrm{supp}(g)| = |\mathrm{supp}(f)| = \delta n$;
- $|(\mathrm{supp}(g) \cup \mathrm{supp}(f))| = (2\delta - \delta^2)n$;
- The number of blue nodes in $\mathrm{supp}(g)$ is $[\delta(1-\delta)^2]n$;
- The number of blue nodes in $\mathrm{supp}(f)$ is $[\delta(1-\delta)^2]n$;
- Thus $[g, f]$ fixes $[1 - (2\delta - \delta^2) + 2\delta(1-\delta)^2]n$ nodes.

An improvement to $\frac{1}{2} - \epsilon$

Write $f = g^h$ and let us show that $[g, f] = gfg^{-1}f^{-1}$ has smaller support than g whenever $\mathrm{supp}(g) < \frac{1}{2} - \epsilon$.



- $|\mathrm{supp}(g)| = |\mathrm{supp}(f)| = \delta n$;
- $|(\mathrm{supp}(g) \cup \mathrm{supp}(f))| = (2\delta - \delta^2)n$;
- The number of blue nodes in $\mathrm{supp}(g)$ is $[\delta(1-\delta)^2]n$;
- The number of blue nodes in $\mathrm{supp}(f)$ is $[\delta(1-\delta)^2]n$;
- Thus $[g, f]$ fixes $[1 - (2\delta - \delta^2) + 2\delta(1-\delta)^2]n$ nodes.
- This is more than $(1-\delta)n$ nodes if and only if $\delta < \frac{1}{2}$.

What have we got?

We have a theorem!

What have we got?

We have a theorem!

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (\frac{1}{2} - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

What have we got?

We have a theorem!

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (\frac{1}{2} - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

We did this by showing that $[g, f]$ has smaller support than g on the average.

What have we got?

We have a theorem!

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (\frac{1}{2} - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

We did this by showing that $[g, f]$ has smaller support than g on the average.

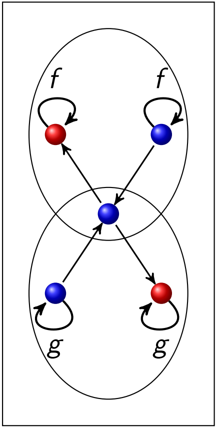
Can we do better? Why stick with $[g, f]$? What about other words?

The word $[g, f]^3$

The word $[g, f]^3$ fixes everything that $[g, f]$ fixes, plus more...

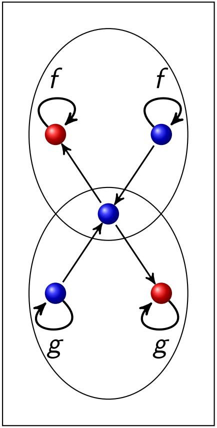
The word $[g, f]^3$

The word $[g, f]^3$ fixes everything that $[g, f]$ fixes, plus more...



The word $[g, f]^3$

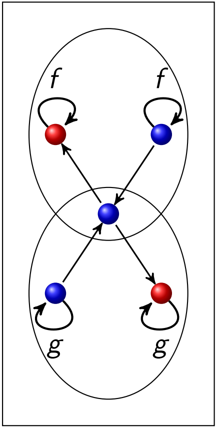
The word $[g, f]^3$ fixes everything that $[g, f]$ fixes, plus more...



- We get extra blue nodes to a value of $[3\delta^2(1-\delta)^4]n$;

The word $[g, f]^3$

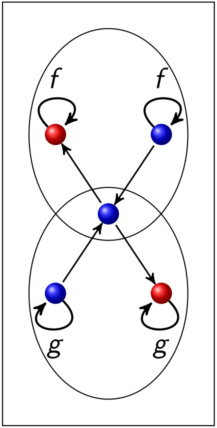
The word $[g, f]^3$ fixes everything that $[g, f]$ fixes, plus more...



- We get extra blue nodes to a value of $[3\delta^2(1-\delta)^4]n$;
- Thus $[g, f]^3$ fixes $[1-(2\delta-\delta^2)+2\delta(1-\delta)^2+3\delta^2(1-\delta)^4]n$ nodes.

The word $[g, f]^3$

The word $[g, f]^3$ fixes everything that $[g, f]$ fixes, plus more...



- We get extra blue nodes to a value of $[3\delta^2(1-\delta)^4]n$;
- Thus $[g, f]^3$ fixes $[1-(2\delta-\delta^2)+2\delta(1-\delta)^2+3\delta^2(1-\delta)^4]n$ nodes.
- This is more than $(1-\delta)n$ nodes if and only if $\delta < 0.568$.

The current world record

If we use the word $([g, h][g^{-1}, h])^k$, where k is a big integer, then we can produce improvements provided $\delta < 0.64242$.

The current world record

If we use the word $([g,h][g^{-1},h])^k$, where k is a big integer, then we can produce improvements provided $\delta < 0.64242$.

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (0.64242 - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G,S)) \leq (\log |G|)^c.$$

The current world record

If we use the word $([g, h][g^{-1}, h])^k$, where k is a big integer, then we can produce improvements provided $\delta < 0.64242$.

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (0.64242 - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G, S)) \leq (\log |G|)^c.$$

It would appear that this is as good as it gets, i.e. there is a constant $x < 1$ above which we cannot decrease support. The reason appears to be hidden in classical work of Manning.

The current world record

If we use the word $([g,h][g^{-1},h])^k$, where k is a big integer, then we can produce improvements provided $\delta < 0.64242$.

Theorem

For $\epsilon > 0$, there exists $c > 0$ such that if S contains an element g such that $|\mathrm{supp}(g)| < (0.64242 - \epsilon)n$, we have

$$\mathrm{diam}(\Gamma(G,S)) \leq (\log|G|)^c.$$

It would appear that this is as good as it gets, i.e. there is a constant $x < 1$ above which we cannot decrease support. The reason appears to be hidden in classical work of Manning.
We conclude that...

BABAI IS NOT AFRAID OF SPIDERS.