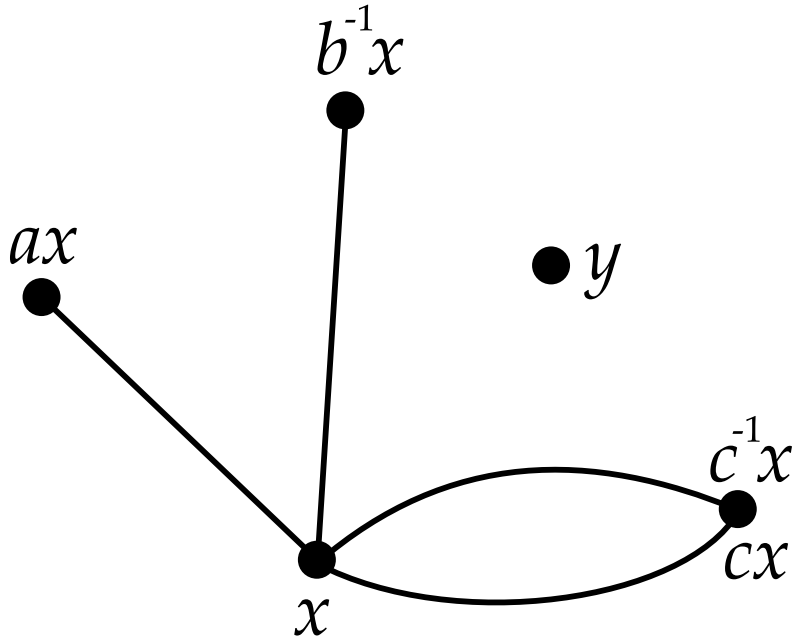
Joint Mathematics Meetings (Jan 2005)

Random Cayley Graphs and the Second Eigenvalue Problem

Po-Shen Loh, Caltech Graduate

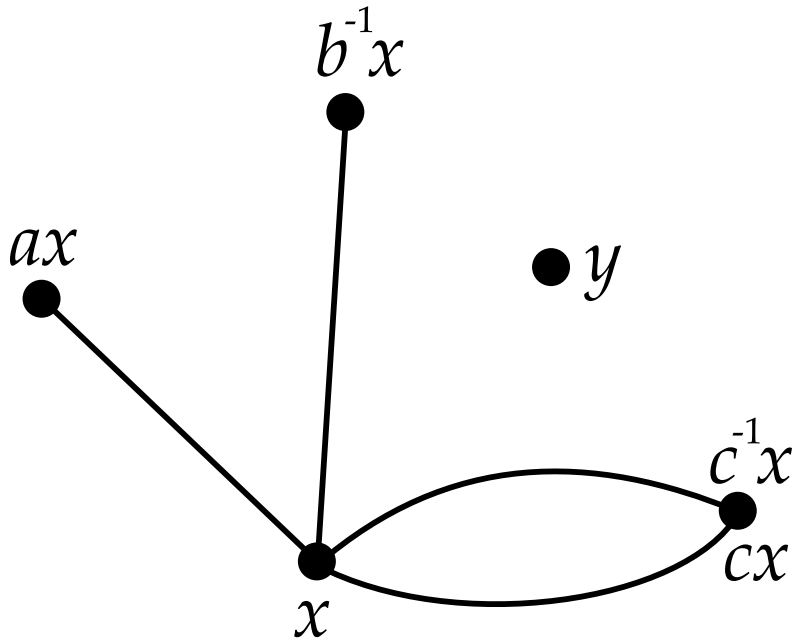
Advisor: Leonard Schulman, Caltech Computer Science

Cayley (multi-)graph



- $X(G, S)$
- a, b, and c are in $S \sqcup S^{-1}$
- There is no t in $S \sqcup S^{-1}$ for which $y = tx$

Adjacency matrix



	x
ax	1
$b^{-1}x$	1
y	0
cx	2

Normalized adjacency matrix; functionals

- $N := |S|$
- Normalized adj. matrix is $\frac{1}{2N} A$
- M has spectrum $|x_1| \geq |x_2| \geq \cdots \geq |x_n|$
  $\lambda(M) := |x_1|$
  $\mu(M) := |x_2|$

Results

Theorem 1 *(Alon/Roichman, 1994)*

For any $\epsilon > 0$*, there exists* $c > 0$ *such that for any fixed* G*,*
$\mathrm{E}[\mu(X(G,S))] < (1 + o(1))\epsilon$*, where* $|S| = N = c \log |G|$.

Results

Theorem 1 *(Alon/Roichman, 1994)*

For any $\epsilon > 0$*, there exists* $c > 0$ *such that for any fixed* G*,*
$\mathrm{E}[\mu(X(G,S))] < (1+o(1))\epsilon$*, where* $|S| = N = c\log|G|$.

Theorem 2 *(Loh/Schulman, 2004)*

$N = c\log D(G)$ *will do, with the same* c.

Results

Theorem 1 *(Alon/Roichman, 1994)*

For any $\epsilon > 0$*, there exists* $c > 0$ *such that for any fixed* G*,*
$\mathrm{E}[\mu(X(G,S))] < (1 + o(1))\epsilon$*, where* $|S| = N = c \log |G|$.

Theorem 2 *(Loh/Schulman, 2004)*

$N = c \log D(G)$ *will do, with the same* c.

Conjecture 1 *(Loh/Schulman, 2004)*

$N = O(\log R(G))$ *is sufficient.*

From eigenvalues to random walks

M has real spectrum and $\lambda(M) = 1$:

$$\mu(M) \leq \left(\mathrm{Tr}(M^{2m}) - 1\right)^{1/2m}$$

From eigenvalues to random walks

M has real spectrum and $\lambda(M) = 1$:

$$\mu(M) \leq \left(\mathrm{Tr}(M^{2m}) - 1\right)^{1/2m}$$

Jensen's inequality:

$$\mathrm{E}[\mu(X(G,S))] \leq \mathrm{E}\left[\left(\mathrm{Tr}(A^{2m}) - 1\right)^{1/2m}\right] \leq \left(\mathrm{E}[\mathrm{Tr}(A^{2m})] - 1\right)^{1/2m}$$

Process RW

(1) Choose a random word of length $2m$ from the free monoid on the N letters $\{a_1, a_2, \ldots, a_N\}$

$$a_2 a_5 a_5^{-1} a_1^{-1} a_7 a_3$$

Process RW

(1) Choose a random word of length $2m$ from the free monoid on the N letters $\{a_1, a_2, \ldots, a_N\}$ $\quad a_2 a_5 a_5^{-1} a_1^{-1} a_7 a_3$

(2) Reduce the word in the free group by iteratively canceling adjacent pairs $\quad a_2 a_1^{-1} a_7 a_3$

Process RW

(1) Choose a random word of length $2m$ from the free monoid on the N letters $\{a_1, a_2, \ldots, a_N\}$ $\quad a_2 a_5 a_5^{-1} a_1^{-1} a_7 a_3$

(2) Reduce the word in the free group by iteratively canceling adjacent pairs $\quad a_2 a_1^{-1} a_7 a_3$

(3) Randomly assign group elements (from G) to the letters that appear in the remaining word, and evaluate the product in G.

Process RW

(1) Choose a random word of length $2m$ from the free monoid on the N letters $\{a_1, a_2, \ldots, a_N\}$ $\quad a_2 a_5 a_5^{-1} a_1^{-1} a_7 a_3$

(2) Reduce the word in the free group by iteratively canceling adjacent pairs $\quad a_2 a_1^{-1} a_7 a_3$

(3) Randomly assign group elements (from G) to the letters that appear in the remaining word, and evaluate the product in G.

$$\mathrm{E}[\mathrm{Tr}(A^{2m})] = G \cdot \Pr(\textbf{RW} \mapsto 1)$$

Events

(A)

(B)

(C) Neither of A or B, but (3) yields $1 \in G$.

$$\Pr(\textbf{RW} \mapsto 1) \leq \Pr(A) + \Pr(B) + \Pr(C)$$

Events

Let $M := 2m\left(1 - \frac{\log\log 2m}{\log 2m}\right)$.

(A) Step (2) produces a word ω shorter than M.

(B) Not A, and every letter that appears in the ω appears at least twice.

(C) Neither of A or B, but (3) yields $1 \in G$.

$$\Pr(\textbf{RW} \mapsto 1) \leq \Pr(A) + \Pr(B) + \Pr(C)$$

Bounds for A, B, C

(shorter than M) $\quad \Pr(A) \leq$

(no singletons) $\quad \Pr(B) \leq$

(has singleton, yields 1) $\quad \Pr(C) \leq 1/G$

For C: $\quad \omega = X\alpha Y$

Bounds for A, B, C

Recall $M = 2m\left(1 - \frac{\log\log 2m}{\log 2m}\right)$.

(shorter than M)	$\Pr(A)$	$\leq$	$2^{2m}(2/N)^{m\log\log 2m/\log 2m}$
(no singletons)	$\Pr(B)$	$\leq$	$2^{M}(m/N)^{M/2}$
(has singleton, yields 1)	$\Pr(C)$	$\leq$	$1/G$

For C: $\omega = X\alpha Y$

Simplification

Recall $M = 2m\left(1 - \frac{\log\log 2m}{\log 2m}\right)$.

$$\begin{array}{rrcl} \text{(shorter than } M\text{)} & \Pr(A) & \leq & 2^{2m}(2/N)^{m\log\log 2m/\log 2m} \\ \text{(no singletons)} & \Pr(B) & \leq & 2^{M}(m/N)^{M/2} \\ \text{(has singleton, yields 1)} & \Pr(C) & \leq & 1/G \end{array}$$

Setting $2m := (\log G)/b$ and $N := c\log G$:

$$\left(\mathrm{E}[\mathrm{Tr}(A^{2m})] - 1\right)^{1/2m} \leq (1+o(1))\left(e^{b}\sqrt{\frac{2}{bc}}\right)$$

Group Algebra $\mathbb{C}[G]$

	x
ax	1
$b^{-1}x$	1
y	0
cx	2

Vector space with basis indexed by G.

$$T := S \sqcup S^{-1}$$

$$\alpha := \sum_{t \in T} \frac{1}{|T|} t$$

Group representations

$\rho : G \longrightarrow \mathbb{C}^{D \times D}$, unitary matrices

- $\rho(xy) = \rho(x)\rho(y)$
- $\rho(x^{-1}) = \rho(x)^{-1}$

Group representations

$\rho : G \longrightarrow \mathbb{C}^{D \times D}$, unitary matrices

- $\rho(xy) = \rho(x)\rho(y)$
- $\rho(x^{-1}) = \rho(x)^{-1}$

Reducible: isomorphic (exists uniform change of basis) to

$$\begin{pmatrix} A_x & 0 \\ 0 & B_x \end{pmatrix}$$

Special properties

$$\rho_1 \equiv 1 \qquad \rho_r(1) = I_{d_r}$$

Special properties

$$\rho_1 \equiv 1 \qquad \rho_r(1) = I_{d_r}$$

$$\chi_r(x) = \mathrm{Tr}(\rho_r(x))$$

$$\sum_{x \in G} \chi_r(x) = 0 \quad \text{for nontrivial irreducibles}$$

Special properties

$$\rho_1 \equiv 1 \qquad \rho_r(1) = I_{d_r}$$

$$\chi_r(x) = \mathrm{Tr}(\rho_r(x))$$

$$\sum_{x \in G} \chi_r(x) = 0 \quad \text{for nontrivial irreducibles}$$

$$\sum_{r=1}^{R} d_r^2 = G$$

Fourier transform

$$\mathcal{F} \quad : \quad \mathbb{C}[G] \xrightarrow{\sim} \bigoplus_{r=1}^{R} \mathcal{M}_r$$

Fourier transform

$$\mathcal{F} \quad : \quad \mathbb{C}[G] \xrightarrow{\sim} \bigoplus_{r=1}^{R} \mathcal{M}_r$$

$$\mathcal{F} \quad : \quad \sum_{x \in G} a_x x \longmapsto \bigoplus_{r=1}^{R} \left(\sum_{x \in G} a_x \rho_r(x) \right)$$

Fourier transform

$$\mathcal{F} \quad : \quad \mathbb{C}[G] \xrightarrow{\sim} \bigoplus_{r=1}^{R} \mathcal{M}_r$$

$$\mathcal{F} \quad : \quad \sum_{x \in G} a_x x \longmapsto \bigoplus_{r=1}^{R} \left(\sum_{x \in G} a_x \rho_r(x) \right)$$

$$\mathcal{F}(\alpha) \quad = \quad \begin{pmatrix} \Psi_1 & 0 & \dots & 0 \\ 0 & \Psi_2 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & \Psi_R \end{pmatrix}, \qquad \Psi_r := \sum_{t \in T} \frac{1}{|T|} \rho_r(t)$$

From μ to λ

$$\Psi_1 = \sum_{t \in T} \frac{1}{|T|} \rho_1(t)$$

$$\mu \begin{pmatrix} \Psi_1 & 0 & \dots & 0 \\ 0 & \Psi_2 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & \Psi_R \end{pmatrix} = \lambda \begin{pmatrix} \Psi_2 & \dots & 0 \\ . & \dots & . \\ 0 & \dots & \Psi_R \end{pmatrix}$$

From eigenvalues to traces

M has real spectrum:

$$\lambda(M) \leq \left(\mathrm{Tr}(M^{2m})\right)^{1/2m}$$

From eigenvalues to traces

M has real spectrum:

$$\lambda(M) \leq \left(\mathrm{Tr}(M^{2m})\right)^{1/2m}$$

Jensen's inequality:

$$\mathrm{E}[\mu(X(G,S))] \leq \mathrm{E}\left[\left(\mathrm{Tr}(A_0^{2m})\right)^{1/2m}\right] \leq \left(\mathrm{E}[\mathrm{Tr}(A_0^{2m})]\right)^{1/2m}$$

Swap order of summation

$$\sum_{r=2}^{R} \mathrm{Tr}(\Psi_r^{2m}) \quad = \quad \sum_{r=2}^{R} \mathrm{Tr}\left(\frac{1}{|T|} \sum_{t \in T} \rho_r(t) \right)^{2m}$$

Swap order of summation

$$\begin{aligned}\sum_{r=2}^{R} \mathrm{Tr}(\Psi_r^{2m}) &= \sum_{r=2}^{R} \mathrm{Tr}\left(\frac{1}{|T|}\sum_{t\in T}\rho_r(t)\right)^{2m} \\ &= \frac{1}{|T|^{2m}}\sum_{r=2}^{R}\left(\sum_{t_1,t_2,\ldots,t_{2m}\in T}\chi_r(t_1t_2\cdots t_{2m})\right)\end{aligned}$$

Swap order of summation

$$\begin{aligned}
\sum_{r=2}^{R} \mathrm{Tr}(\Psi_r^{2m}) &= \sum_{r=2}^{R} \mathrm{Tr}\left(\frac{1}{|T|}\sum_{t\in T}\rho_r(t)\right)^{2m} \\
&= \frac{1}{|T|^{2m}}\sum_{r=2}^{R}\left(\sum_{t_1,t_2,\ldots,t_{2m}\in T}\chi_r(t_1t_2\cdots t_{2m})\right) \\
&= \frac{1}{|T|^{2m}}\sum_{r=2}^{R}\sum_{g\in G}\chi_r(g)N_g
\end{aligned}$$

Swap order of summation

$$\begin{aligned}
\sum_{r=2}^{R} \mathrm{Tr}(\Psi_r^{2m}) &= \sum_{r=2}^{R} \mathrm{Tr}\left(\frac{1}{|T|}\sum_{t\in T}\rho_r(t)\right)^{2m} \\
&= \frac{1}{|T|^{2m}}\sum_{r=2}^{R}\left(\sum_{t_1,t_2,\ldots,t_{2m}\in T}\chi_r(t_1t_2\cdots t_{2m})\right) \\
&= \frac{1}{|T|^{2m}}\sum_{r=2}^{R}\sum_{g\in G}\chi_r(g)N_g \\
\mathrm{Re}\,\mathrm{E}[\mathrm{Tr}(A^{2m})] &= \frac{1}{|T|^{2m}}\sum_{g\in G}\mathrm{E}[N_g]\sum_{r=2}^{R}\mathrm{Re}\,\chi_r(g),
\end{aligned}$$

Process RW, revisited

$$\frac{\mathrm{E}[N_g]}{|T|^{2m}} = \Pr(\textbf{RW} \mapsto g)$$

Process RW, revisited

$$\frac{\mathrm{E}[N_g]}{|T|^{2m}} = \Pr(\textbf{RW} \mapsto g)$$

$$\sum_{g \in G} \Pr(\textbf{RW} \mapsto g) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$= \sum_{g \in G} \Pr(\textbf{RW} \mapsto g \text{ and } A \cup B) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$+ \sum_{g \in G} \Pr(\textbf{RW} \mapsto g \text{ and } \overline{A \cup B}) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

Process RW, revisited

$$\frac{\mathrm{E}[N_g]}{|T|^{2m}} = \Pr(\textbf{RW} \mapsto g)$$

$$\sum_{g \in G} \Pr(\textbf{RW} \mapsto g) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$= \sum_{g \in G} \Pr(\textbf{RW} \mapsto g \text{ and } A \cup B) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$+ \sum_{g \in G} \frac{1}{G} \Pr(\overline{A \cup B}) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

Process RW, revisited

$$\frac{\mathrm{E}[N_g]}{|T|^{2m}} = \Pr(\textbf{RW} \mapsto g)$$

$$\sum_{g \in G} \Pr(\textbf{RW} \mapsto g) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$= \sum_{g \in G} \Pr(\textbf{RW} \mapsto g \text{ and } A \cup B) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$+ \sum_{r=2}^{R} \frac{1}{G} \Pr(\overline{A \cup B}) \sum_{g \in G} \operatorname{Re} \chi_r(g)$$

Process RW, revisited

$$\frac{\mathrm{E}[N_g]}{|T|^{2m}} = \Pr(\textbf{RW} \mapsto g)$$

$$\sum_{g \in G} \Pr(\textbf{RW} \mapsto g) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$= \sum_{g \in G} \Pr(\textbf{RW} \mapsto g \text{ and } A \cup B) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$+ \sum_{r=2}^{R} \frac{1}{G} \Pr(\overline{A \cup B}) \sum_{g \in G} \operatorname{Re} \chi_r(g)$$

Process RW, revisited

$$\frac{\mathrm{E}[N_g]}{|T|^{2m}} = \Pr(\textbf{RW} \mapsto g)$$

$$\sum_{g \in G} \Pr(\textbf{RW} \mapsto g) \sum_{r=2}^{R} \operatorname{Re} \chi_r(g)$$

$$\leq \sum_{g \in G} \Pr(\textbf{RW} \mapsto g \text{ and } A \cup B) D(G)$$

$$+ \sum_{r=2}^{R} \frac{1}{G} \Pr(\overline{A \cup B}) \sum_{g \in G} \operatorname{Re} \chi_r(g)$$

Comparison with Alon/Roichman

L/S: $(\Pr(A) + \Pr(B)) \cdot D(G)$

Comparison with Alon/Roichman

A/R:
$$G \cdot (\Pr(A) + \Pr(B) + \Pr(C)) - 1$$
$$\leq \quad (\Pr(A) + \Pr(B)) \cdot G$$

L/S:
$$(\Pr(A) + \Pr(B)) \cdot D(G)$$

Comparison with Alon/Roichman

A/R: $$G \cdot (\Pr(A) + \Pr(B) + \Pr(C)) - 1$$
$$\leq \quad (\Pr(A) + \Pr(B)) \cdot G$$

L/S: $$(\Pr(A) + \Pr(B)) \cdot D(G)$$

Recall: $M = 2m\left(1 - \frac{\log\log 2m}{\log 2m}\right)$,

(shorter than M) $$\Pr(A) \leq 2^{2m}(2/N)^{m \log\log 2m/\log 2m}$$

(no singletons) $$\Pr(B) \leq 2^{M}(m/N)^{M/2}$$

Simplification, revisited

Recall $M = 2m\left(1 - \frac{\log\log 2m}{\log 2m}\right)$.

$$\begin{array}{rrcl} \text{(shorter than } M\text{)} & \Pr(A) & \leq & 2^{2m}(2/N)^{m\log\log 2m/\log 2m} \\ \text{(no singletons)} & \Pr(B) & \leq & 2^{M}(m/N)^{M/2} \\ \text{(has singleton, yields 1)} & \Pr(C) & \leq & 1/G \end{array}$$

Setting $2m := (\log D(G))/b$ and $N := c\log D(G)$:

$$((\Pr(A) + \Pr(B)) \cdot D(G))^{1/2m} \leq (1 + o(1))\left(e^b\sqrt{\frac{2}{bc}}\right)$$

Future work

$$\sum_{g\in G} \Pr(\textbf{RW} \mapsto g) \sum_{r=2}^{R} \operatorname{Re}\chi_r(g)$$

$$= \sum_{g\in G} \Pr(\textbf{RW} \mapsto g \text{ and } A\cup B) \sum_{r=2}^{R} \operatorname{Re}\chi_r(g)$$

$$+ \sum_{g\in G} \Pr(\textbf{RW} \mapsto g \text{ and } \overline{A\cup B}) \sum_{r=2}^{R} \operatorname{Re}\chi_r(g)$$

Acknowledgements

- Marshall family
- Caltech Summer Undergraduate Research Fellowship office
- Caltech Mathematics Department