Golden Gates, Ramanujan Complexes and Ramanujan Digraphs

Ori Parzanchevski, Hebrew University of Jerusalem

Expanders and Extractors, Simons Institute, Berkeley 2017

Ramanujan graphs

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.

Ramanujan graphs

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

Ramanujan graphs

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

$$Spec\left(Adj|_{L^2(T_k)}\right) = \left[-2\sqrt{k-1}, 2\sqrt{k-1}\right].$$

Ramanujan graphs

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

$$Spec\left(Adj|_{L^2(T_k)}\right) = \left[-2\sqrt{k-1}, 2\sqrt{k-1}\right].$$

- A k-regular graph is Ramanujan if the nontrivial spectrum is contained in $Spec\left(Adj|_{L^2(T_k)}\right)$.

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

$$Spec\left(Adj|_{L^2(T_k)}\right) = \left[-2\sqrt{k-1}, 2\sqrt{k-1}\right].$$

- A k-regular graph is Ramanujan if the nontrivial spectrum is contained in $Spec\left(Adj|_{L^2(T_k)}\right)$.
- Every k-regular graph is a quotient of T_k by a group of isometries.

Ramanujan graphs

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

$$Spec\left(Adj|_{L^2(T_k)}\right) = \left[-2\sqrt{k-1}, 2\sqrt{k-1}\right].$$

- A k-regular graph is Ramanujan if the nontrivial spectrum is contained in $Spec\left(Adj|_{L^2(T_k)}\right)$.
- Every k-regular graph is a quotient of T_k by a group of isometries.
- Lubotzky-Phillips-Sarnak '88: for $p \equiv 1 \pmod 4$, endow the $(p+1)$-regular tree with an arithmetic structure.

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

$$Spec\left(Adj|_{L^2(T_k)}\right) = \left[-2\sqrt{k-1}, 2\sqrt{k-1}\right].$$

- A k-regular graph is Ramanujan if the nontrivial spectrum is contained in $Spec\left(Adj|_{L^2(T_k)}\right)$.
- Every k-regular graph is a quotient of T_k by a group of isometries.
- Lubotzky-Phillips-Sarnak '88: for $p \equiv 1 \pmod 4$, endow the $(p+1)$-regular tree with an arithmetic structure.
- Ramanujan, Petersson, Selberg, Satake...:

  Arithmetic quotients of geometric objects behave nicely.

Ramanujan graphs

- A k-regular graph G is an expander if the nontrivial eigenvalues of Adj_G are small.
- "Trivial" - constant eigenfunction, or constant on 2-partition.
- How small is small?
- Alon-Boppana: the best one can hope for is the L^2-spectrum of the k-regular tree:

$$Spec\left(Adj|_{L^2(T_k)}\right) = \left[-2\sqrt{k-1}, 2\sqrt{k-1}\right].$$

- A k-regular graph is Ramanujan if the nontrivial spectrum is contained in $Spec\left(Adj|_{L^2(T_k)}\right)$.
- Every k-regular graph is a quotient of T_k by a group of isometries.
- Lubotzky-Phillips-Sarnak '88: for $p \equiv 1 \pmod 4$, endow the $(p+1)$-regular tree with an arithmetic structure.
- Ramanujan, Petersson, Selberg, Satake...:

  Arithmetic quotients of geometric objects behave nicely.
- LPS: Ramanujan quotients of T_{p+1}.

Unitary similitudes group

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^* A = I\} \quad \text{where } i = \sqrt{-1}$$

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$.

Unitary similitudes group

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^* A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^*A = \lambda I \;\; \left(\lambda \in R^\times\right)\right\}_{/R^\times}.$$

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^* A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^* A = \lambda I \;\; (\lambda \in R^\times)\right\}_{/R^\times}.$$

- $PGU_2(\mathbb{R}) = PU(2)$ (if $A^* A = \lambda I$ then $\frac{A}{\sqrt{\lambda}} \in U(2)$).

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^*A = \lambda I \;\; (\lambda \in R^\times)\right\}_{/R^\times}.$$

- $PGU_2(\mathbb{R}) = PU(2)$ (if $A^*A = \lambda I$ then $\frac{A}{\sqrt{\lambda}} \in U(2)$).
- $R = \mathbb{Z}\left[\frac{1}{5}\right] = \left\{\frac{n}{5^\ell} \,\middle|\, n \in \mathbb{Z}, 5 \in \mathbb{N}\right\}$.

Unitary similitudes group

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^*A = \lambda I \;\; (\lambda \in R^\times)\right\}_{/R^\times}.$$

- $PGU_2(\mathbb{R}) = PU(2)$ (if $A^*A = \lambda I$ then $\frac{A}{\sqrt{\lambda}} \in U(2)$).
- $R = \mathbb{Z}\left[\frac{1}{5}\right] = \left\{\frac{n}{5^\ell} \,\middle|\, n \in \mathbb{Z}, 5 \in \mathbb{N}\right\}$.

$$\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$$

Unitary similitudes group

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^*A = \lambda I \;\; (\lambda \in R^\times)\right\}_{/R^\times}.$$

- $PGU_2(\mathbb{R}) = PU(2)$ (if $A^*A = \lambda I$ then $\frac{A}{\sqrt{\lambda}} \in U(2)$).
- $R = \mathbb{Z}\left[\frac{1}{5}\right] = \left\{\frac{n}{5^\ell} \,\middle|\, n \in \mathbb{Z}, 5 \in \mathbb{N}\right\}$.

$$\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$$

since $\begin{pmatrix} 2+i & \\ & 2-i \end{pmatrix}^* \begin{pmatrix} 2+i & \\ & 2-i \end{pmatrix} = \begin{pmatrix} 5 & \\ & 5 \end{pmatrix}$

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \ldots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^*A = \lambda I \;\; (\lambda \in R^\times)\right\}_{/R^\times}.$$

- $PGU_2(\mathbb{R}) = PU(2)$ (if $A^*A = \lambda I$ then $\frac{A}{\sqrt{\lambda}} \in U(2)$).
- $R = \mathbb{Z}\left[\frac{1}{5}\right] = \left\{\frac{n}{5^\ell} \,\middle|\, n \in \mathbb{Z}, 5 \in \mathbb{N}\right\}$.

$$\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$$

since $\begin{pmatrix} 2+i & \\ & 2-i \end{pmatrix}^* \begin{pmatrix} 2+i & \\ & 2-i \end{pmatrix} = \begin{pmatrix} 5 & \\ & 5 \end{pmatrix}$ and $5 \in \mathbb{Z}\left[\frac{1}{5}\right]^\times$.

- Unitary group over ring R:

$$U_2(R) = \{A \in M_{2\times 2}(R[i]) \mid A^*A = I\} \quad \text{where } i = \sqrt{-1}$$

- $U_2(\mathbb{R}) = U(2)$. Think about $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{F}_p, \dots$
- Nicer to look at the group of unitary similitudes:

$$PGU_2(R) = \left\{A \in M_{2\times 2}(R[i]) \,\middle|\, A^*A = \lambda I \;\; (\lambda \in R^\times)\right\}_{/R^\times}.$$

- $PGU_2(\mathbb{R}) = PU(2)$ (if $A^*A = \lambda I$ then $\frac{A}{\sqrt{\lambda}} \in U(2)$).
- $R = \mathbb{Z}\left[\frac{1}{5}\right] = \left\{\frac{n}{5^\ell} \,\middle|\, n \in \mathbb{Z}, 5 \in \mathbb{N}\right\}$.

$$\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$$

since $\left(\begin{smallmatrix} 2+i & \\ & 2-i \end{smallmatrix}\right)^* \left(\begin{smallmatrix} 2+i & \\ & 2-i \end{smallmatrix}\right) = \left(\begin{smallmatrix} 5 & \\ & 5 \end{smallmatrix}\right)$ and $5 \in \mathbb{Z}\left[\frac{1}{5}\right]^\times$.

- Think of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$ as all $A \in M_2(\mathbb{Z}[i])$ with $A^*A = 5^n I$, $n \in \mathbb{N}$.

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$.

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \mid A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- So, $Cay(\Gamma_2, S)$ is a 6-regular tree.

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \mid A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- So, $Cay(\Gamma_2, S)$ is a 6-regular tree.
- For any $q \neq 2, 5$,

$$\Gamma_{2q} := \{A \in M_2(\mathbb{Z}[i]) \mid A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{2q}\} \leq \Gamma_2$$

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- So, $Cay(\Gamma_2, S)$ is a 6-regular tree.
- For any $q \neq 2, 5$,

$$\Gamma_{2q} := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{2q}\} \leq \Gamma_2,$$

and $X^{5,q} := \Gamma_{2q} \backslash Cay(\Gamma_2, S)$ is the LPS Ramanujan graph.

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- So, $Cay(\Gamma_2, S)$ is a 6-regular tree.
- For any $q \neq 2, 5$,

$$\Gamma_{2q} := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{2q}\} \leq \Gamma_2,$$

and $X^{5,q} := \Gamma_{2q} \backslash Cay(\Gamma_2, S)$ is the LPS Ramanujan graph.
- In fact, $\Gamma_{2q} \trianglelefteq \Gamma_2$, so

$$X^{5,q} = \Gamma_{2q} \backslash Cay(\Gamma_2, S) = Cay\left({}^{\Gamma_2}/_{\Gamma_{2q}}, S\right)$$

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \mid A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- So, $Cay(\Gamma_2, S)$ is a 6-regular tree.
- For any $q \neq 2, 5$,

$$\Gamma_{2q} := \{A \in M_2(\mathbb{Z}[i]) \mid A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{2q}\} \leq \Gamma_2,$$

and $X^{5,q} := \Gamma_{2q} \backslash Cay(\Gamma_2, S)$ is the LPS Ramanujan graph.
- In fact, $\Gamma_{2q} \trianglelefteq \Gamma_2$, so

$$X^{5,q} = \Gamma_{2q} \backslash Cay(\Gamma_2, S) = Cay\left({}^{\Gamma_2}/_{\Gamma_{2q}}, S\right)$$

Actually, ${}^{\Gamma_2}/_{\Gamma_{2q}} \cong$ to either $PGL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$.

- Theorem (LPS):

$$S = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \right\}$$

generate a free subgroup of $PGU_2\left(\mathbb{Z}\left[\frac{1}{5}\right]\right)$. Which group?

$$\Gamma_2 := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 2\}$$

- So, $Cay(\Gamma_2, S)$ is a 6-regular tree.
- For any $q \neq 2, 5$,

$$\Gamma_{2q} := \{A \in M_2(\mathbb{Z}[i]) \,|\, A^*A = 5^n I,\ A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{2q}\} \leq \Gamma_2,$$

and $X^{5,q} := \Gamma_{2q} \backslash Cay(\Gamma_2, S)$ is the LPS Ramanujan graph.
- In fact, $\Gamma_{2q} \trianglelefteq \Gamma_2$, so

$$X^{5,q} = \Gamma_{2q} \backslash Cay(\Gamma_2, S) = Cay\left({}^{\Gamma_2}/_{\Gamma_{2q}}, S\right)$$

Actually, ${}^{\Gamma_2}/_{\Gamma_{2q}} \cong$ to either $PGL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$.
- Uses Ramanujan-Petersson conjecture (Eichler/Weyl/Deligne), Functoriality (Jacquet-Langlands).

Other p

Other p

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8\,(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z})\,.$$

Other p

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8\,(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z})\,.$$

- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^* A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z}).$$

- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^*A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$

and $1/8$ of them are $\equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \pmod 2$;

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8(p+1)$ solutions to
$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z}).$$
- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives
$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^*A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$
and $1/8$ of them are $\equiv \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \pmod 2$; Denote them by S_p.

Other p

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z}).$$

- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^*A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$

and $1/8$ of them are $\equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \pmod 2$; Denote them by S_p.

- For example,

$$S_5 = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\}$$

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8\,(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z})\,.$$

- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^*A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$

and $1/8$ of them are $\equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \pmod 2$; Denote them by S_p.

- For example,

$$S_5 = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\}$$

- LPS: $Cay\left(\langle S_p \rangle, S_p\right)$ is a $(p+1)$-regular tree.

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8\,(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z})\,.$$

- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^*A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$

and $1/8$ of them are $\equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \pmod 2$; Denote them by S_p.

- For example,

$$S_5 = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\}$$

- LPS: $Cay\left(\langle S_p \rangle, S_p\right)$ is a $(p+1)$-regular tree.
- Chiu '92 ($p = 2$)

- Jacobi's four-square theorem: if $p \equiv 1 \pmod 4$, there are $8\,(p+1)$ solutions to

$$a^2 + b^2 + c^2 + d^2 = p \qquad (a, b, c, d \in \mathbb{Z})\,.$$

- Write $\alpha = a + bi$, $\beta = c + di$. Each solution gives

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right), \qquad A^* A = \left(|\alpha|^2 + |\beta|^2\right) \cdot I = p \cdot I$$

and $1/8$ of them are $\equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \pmod 2$; Denote them by S_p.

- For example,

$$S_5 = \left\{ \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\}$$

- LPS: $Cay\left(\langle S_p \rangle, S_p\right)$ is a $(p+1)$-regular tree.
- Chiu '92 ($p = 2$), Davidoff-Sarnak-Valette '03 ($p \equiv 3 \pmod 4$).

Quantum compiling

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$.

Quantum compiling

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$. Replaces $\mathbb{F}_2$.

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$. Replaces $\mathbb{F}_2$.
- Quantum gate = matrices in $PU(2)$.

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$. Replaces $\mathbb{F}_2$.
- Quantum gate = matrices in $PU(2)$.
- Basic problem: Find gates $A_1, \ldots, A_r \in PU(2)$ which topologically generate $PU(2)$.

Quantum compiling

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$. Replaces $\mathbb{F}_2$.
- Quantum gate = matrices in $PU(2)$.
- Basic problem: Find gates $A_1, \ldots, A_r \in PU(2)$ which topologically generate $PU(2)$.
- Harder: Find efficient gates:
  for any $M \in PU(2)$ and $\varepsilon > 0$, there is a short circuit in A_i in the ε-neighborhood of M.

Quantum compiling

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$. Replaces $\mathbb{F}_2$.
- Quantum gate = matrices in $PU(2)$.
- Basic problem: Find gates $A_1, \ldots, A_r \in PU(2)$ which topologically generate $PU(2)$.
- Harder: Find efficient gates:
  for any $M \in PU(2)$ and $\varepsilon > 0$, there is a short circuit in A_i in the ε-neighborhood of M.
- Hardest: Find such a short circuit, given $\{A_i\}, M, \varepsilon$.

Quantum compiling

- Qubit: element of $\mathbb{C}^2/\mathbb{C}^\times$. Replaces $\mathbb{F}_2$.
- Quantum gate = matrices in $PU(2)$.
- Basic problem: Find gates $A_1, \ldots, A_r \in PU(2)$ which topologically generate $PU(2)$.
- Harder: Find efficient gates:
  for any $M \in PU(2)$ and $\varepsilon > 0$, there is a short circuit in A_i in the ε-neighborhood of M.
- Hardest: Find such a short circuit, given $\{A_i\}, M, \varepsilon$.
- Nice to have: good growth rate. E.g. if $\{A_i\}$ have no relations, there are r^ℓ circuits with ℓ gates.

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$

  is actually a free group sitting inside $PU(2)$.

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$

  is actually a free group sitting inside $PU(2)$.
- V-gates (Bocharov-Gurevich-Svore '13):

$$\langle S_5 \rangle = \left\langle \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\rangle$$

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$

  is actually a free group sitting inside $PU(2)$.
- V-gates (Bocharov-Gurevich-Svore '13):

$$\langle S_5 \rangle = \left\langle \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\rangle$$

- Excellent growth rate ($6 \cdot 5^{\ell-1}$ circuits of length ℓ).

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$

  is actually a free group sitting inside $PU(2)$.
- V-gates (Bocharov-Gurevich-Svore '13):

$$\langle S_5 \rangle = \left\langle \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\rangle$$

- Excellent growth rate ($6 \cdot 5^{\ell-1}$ circuits of length ℓ).
- Compiling: e.g. $M = \begin{pmatrix} -2373 - 4484i & -4716 + 922i \\ 2092 + 4326i & -5011 + 792i \end{pmatrix}$

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,
$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$
is actually a free group sitting inside $PU(2)$.
- V-gates (Bocharov-Gurevich-Svore '13):
$$\langle S_5 \rangle = \left\langle \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\rangle$$
- Excellent growth rate ($6 \cdot 5^{\ell-1}$ circuits of length ℓ).
- Compiling: e.g. $M = \begin{pmatrix} -2373 - 4484i & -4716 + 922i \\ 2092 + 4326i & -5011 + 792i \end{pmatrix}$
satisfies $M^* M = 5^{11} \cdot I$ and $M \equiv I \pmod 5$, so $M \in \langle S_5 \rangle$.

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\tfrac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$

  is actually a free group sitting inside $PU(2)$.
- V-gates (Bocharov-Gurevich-Svore '13):

$$\langle S_5 \rangle = \left\langle \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\rangle$$

- Excellent growth rate ($6 \cdot 5^{\ell-1}$ circuits of length ℓ).
- Compiling: e.g. $M = \begin{pmatrix} -2373 - 4484i & -4716 + 922i \\ 2092 + 4326i & -5011 + 792i \end{pmatrix}$
  satisfies $M^* M = 5^{11} \cdot I$ and $M \equiv I \pmod 5$, so $M \in \langle S_5 \rangle$.
- Decompose M as a circuit in S_5 by navigating the tree $Cay(\langle S_5 \rangle, S_5)$.

- Since $S_p \subseteq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \subseteq PGU_2(\mathbb{R}) = PU(2)$,

$$\langle S_p \rangle = \left\{ A \in PGU_2\left(\mathbb{Z}\left[\tfrac{1}{p}\right]\right) \,\middle|\, A \equiv I \pmod 2 \right\}$$

  is actually a free group sitting inside $PU(2)$.
- V-gates (Bocharov-Gurevich-Svore '13):

$$\langle S_5 \rangle = \left\langle \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}^{\pm 1} \right\rangle$$

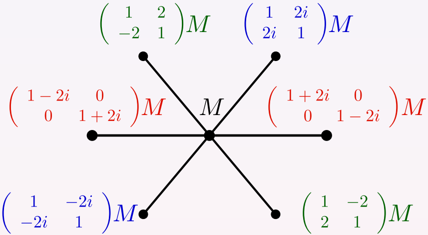
- Excellent growth rate ($6 \cdot 5^{\ell-1}$ circuits of length ℓ).
- Compiling: e.g. $M = \begin{pmatrix} -2373-4484i & -4716+922i \\ 2092+4326i & -5011+792i \end{pmatrix}$ satisfies $M^*M = 5^{11} \cdot I$ and $M \equiv I \pmod 5$, so $M \in \langle S_5 \rangle$.
- Decompose M as a circuit in S_5 by navigating the tree $Cay(\langle S_5 \rangle, S_5)$.
- Hard (Ross-Selinger, Sardari): approximate $M \in PU(2)$ by $M' \in \langle S_p \rangle$.

- How efficient are the LPS gates?

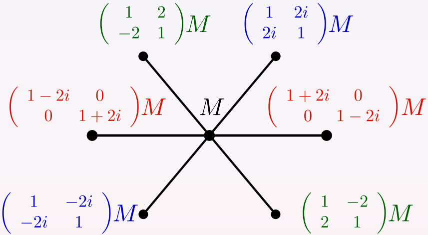
- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right), S_p\right)$

- How efficient are the LPS gates?
- Think of the (disconnected)
  Cayley graph $Cay\left(PU\left(2\right), S_p\right)$
  $x \sim sx$ for $x \in PU\left(2\right)$, $s \in S_p$.

- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right), S_p\right)$ $x \sim sx$ for $x \in PU\left(2\right)$, $s \in S_p$.



- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right), S_p\right)$ $x \sim sx$ for $x \in PU\left(2\right)$, $s \in S_p$.

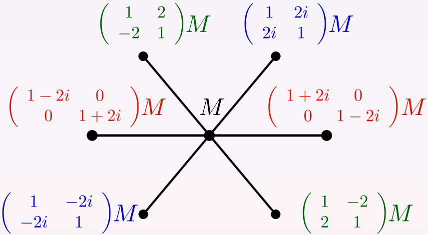


- Look at the adjacency operator on $L^2\left(PU\left(2\right)\right)$.

$$A : L^2\left(PU\left(2\right)\right) \to L^2\left(PU\left(2\right)\right), \qquad \left(Af\right)\left(x\right) = \sum_{s \in S_p} f\left(sx\right).$$

Topological expanders

- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right),S_p\right)$ $x\sim sx$ for $x\in PU\left(2\right)$, $s\in S_p$.

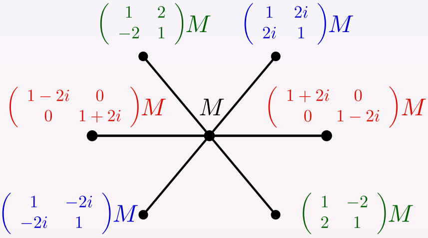


- Look at the adjacency operator on $L^2\left(PU\left(2\right)\right)$.

$$A:L^2\left(PU\left(2\right)\right)\to L^2\left(PU\left(2\right)\right),\qquad \left(Af\right)\left(x\right)=\sum_{s\in S_p}f\left(sx\right).$$

This is $k=(p+1)$-regular. In particular $A\mathbb{1}=k\cdot\mathbb{1}$.

- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right), S_p\right)$ $x \sim sx$ for $x \in PU\left(2\right)$, $s \in S_p$.



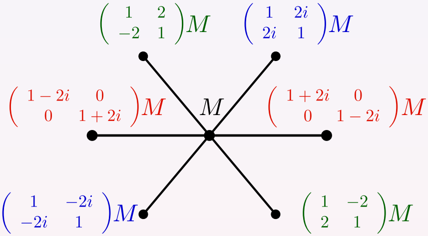
- Look at the adjacency operator on $L^2\left(PU\left(2\right)\right)$.

$$A : L^2\left(PU\left(2\right)\right) \to L^2\left(PU\left(2\right)\right), \qquad \left(Af\right)\left(x\right) = \sum_{s \in S_p} f\left(sx\right).$$

This is $k = (p+1)$-regular. In particular $A\mathbb{1} = k \cdot \mathbb{1}$.

- If S_p topologically generates $PU\left(2\right)$, then $Af = kf$, implies $f \equiv const$

- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right), S_p\right)$ $x \sim sx$ for $x \in PU\left(2\right)$, $s \in S_p$.



- Look at the adjacency operator on $L^2\left(PU\left(2\right)\right)$.

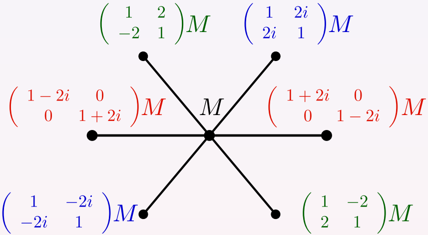
$$A : L^2\left(PU\left(2\right)\right) \to L^2\left(PU\left(2\right)\right), \qquad \left(Af\right)\left(x\right) = \sum_{s \in S_p} f\left(sx\right).$$

This is $k = (p+1)$-regular. In particular $A\mathbb{1} = k \cdot \mathbb{1}$.

- If S_p topologically generates $PU\left(2\right)$, then $Af = kf$, implies $f \equiv const$ (at least for continuous f).

Topological expanders

- How efficient are the LPS gates?
- Think of the (disconnected) Cayley graph $Cay\left(PU\left(2\right),S_p\right)$ $x\sim sx$ for $x\in PU\left(2\right)$, $s\in S_p$.



- Look at the adjacency operator on $L^2\left(PU\left(2\right)\right)$.

$$A:L^2\left(PU\left(2\right)\right)\to L^2\left(PU\left(2\right)\right),\qquad \left(Af\right)\left(x\right)=\sum_{s\in S_p}f\left(sx\right).$$

This is $k=(p+1)$-regular. In particular $A\mathbb{1}=k\cdot\mathbb{1}$.

- If S_p topologically generates $PU\left(2\right)$, then $Af=kf$, implies $f\equiv const$ (at least for continuous f).
- Suggests: Expander = small nontrivial spectrum.

Golden Gates

Hecke Operators and Distributing Points on the Sphere $\mathrm{I} + \mathrm{II}$ (LPS '86, '87)

Hecke Operators and Distributing Points on the Sphere $\mathrm{I}+\mathrm{II}$ (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2(PU(2)) \to L^2(PU(2)), \qquad (Af)(x) = \sum_{s \in S} f(sx)$$

Hecke Operators and Distributing Points on the Sphere $\mathrm{I}+\mathrm{II}$ (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2(PU(2)) \to L^2(PU(2)), \qquad (Af)(x) = \sum_{s\in S} f(sx)$$

1. If λ_S is small, S generates $PU(2)$ efficiently

Hecke Operators and Distributing Points on the Sphere $\mathrm{I} + \mathrm{II}$ (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2(PU(2)) \to L^2(PU(2)), \qquad (Af)(x) = \sum_{s \in S} f(sx)$$

1. If λ_S is small, S generates $PU(2)$ efficiently:
   for every ℓ, the circuits of length ℓ in S_p distribute pseudo-randomly over $PU(2)$.

Hecke Operators and Distributing Points on the Sphere $\mathrm{I} + \mathrm{II}$ (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2(PU(2)) \to L^2(PU(2)), \qquad (Af)(x) = \sum_{s \in S} f(sx)$$

1. If λ_S is small, S generates $PU(2)$ efficiently:
   for every ℓ, the circuits of length ℓ in S_p distribute pseudo-randomly over $PU(2)$.
2. If $S \subseteq PU(2)$, $S^{-1} = S$ and $|S| = k$

Hecke Operators and Distributing Points on the Sphere I + II (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2\left(PU\left(2\right)\right) \to L^2\left(PU\left(2\right)\right), \qquad \left(Af\right)\left(x\right) = \sum_{s \in S} f\left(sx\right)$$

1. If λ_S is small, S generates $PU\left(2\right)$ efficiently:
   for every ℓ, the circuits of length ℓ in S_p distribute pseudo-randomly over $PU\left(2\right)$.
2. If $S \subseteq PU\left(2\right)$, $S^{-1} = S$ and $|S| = k$, then $\lambda_S \geq 2\sqrt{k-1}$.

Hecke Operators and Distributing Points on the Sphere I + II (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2(PU(2)) \to L^2(PU(2)), \qquad (Af)(x) = \sum_{s \in S} f(sx)$$

1. If λ_S is small, S generates $PU(2)$ efficiently: for every ℓ, the circuits of length ℓ in S_p distribute pseudo-randomly over $PU(2)$.
2. If $S \subseteq PU(2)$, $S^{-1} = S$ and $|S| = k$, then $\lambda_S \geq 2\sqrt{k-1}$.
3. For $p \equiv 1 \pmod 4$, the LPS generators obtain $\lambda_{S_p} = 2\sqrt{k-1}$.

Hecke Operators and Distributing Points on the Sphere $\mathrm{I}+\mathrm{II}$ (LPS '86, '87)

- Define: $\lambda_S =$ second largest eigenvalue of

$$A : L^2(PU(2)) \to L^2(PU(2)), \qquad (Af)(x) = \sum_{s\in S} f(sx)$$

1. If λ_S is small, S generates $PU(2)$ efficiently:
   for every ℓ, the circuits of length ℓ in S_p distribute pseudo-randomly over $PU(2)$.
2. If $S \subseteq PU(2)$, $S^{-1} = S$ and $|S| = k$, then $\lambda_S \geq 2\sqrt{k-1}$.
3. For $p \equiv 1 \pmod 4$, the LPS generators obtain $\lambda_{S_p} = 2\sqrt{k-1}$.

- Proof uses even more number theory.

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.
- Advantage over LPS-gates: fault-tolerance (Shor-Kitaev).

Clifford+T

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.
- Advantage over LPS-gates: fault-tolerance (Shor-Kitaev).
- Disadvantage: suboptimal growth rate.

Clifford+T

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.
- Advantage over LPS-gates: fault-tolerance (Shor-Kitaev).
- Disadvantage: suboptimal growth rate.
- New gates (P-Sarnak): Efficient fault-tolerant gates.

Clifford+T

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.
- Advantage over LPS-gates: fault-tolerance (Shor-Kitaev).
- Disadvantage: suboptimal growth rate.
- New gates (P-Sarnak): Efficient fault-tolerant gates.
- LPS: $\langle S_p \rangle$ acts simply transitively on the vertices of a regular tree.

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.
- Advantage over LPS-gates: fault-tolerance (Shor-Kitaev).
- Disadvantage: suboptimal growth rate.
- New gates (P-Sarnak): Efficient fault-tolerant gates.
- LPS: $\langle S_p \rangle$ acts simply transitively on the vertices of a regular tree.
- We find $\Gamma \leq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$ which acts simply transitively on the *directed edges* of the tree.

- Clifford+T gates:

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq S_4, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$$

- Kliuchnikov-Maslov-Mosca '13: $\langle C, T \rangle = PGU_2\left(\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right]\right)$.
- Advantage over LPS-gates: fault-tolerance (Shor-Kitaev).
- Disadvantage: suboptimal growth rate.
- New gates (P-Sarnak): Efficient fault-tolerant gates.
- LPS: $\langle S_p \rangle$ acts simply transitively on the vertices of a regular tree.
- We find $\Gamma \leq PGU_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$ which acts simply transitively on the *directed edges* of the tree.
- Example:

$$\Gamma = \left\langle \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \begin{pmatrix} 1-\sqrt{2} & i \\ -i & \sqrt{2}-1 \end{pmatrix} \right\rangle$$

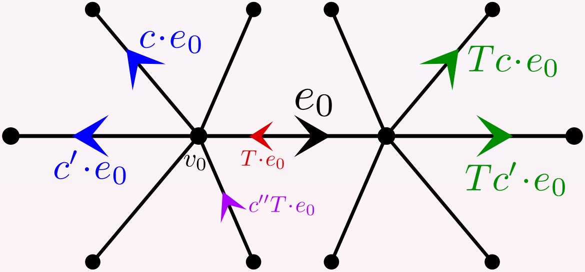
  has a finite index in $\langle C, T \rangle$, and acts simply transitively on the edges of a 3-regular tree.

- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that

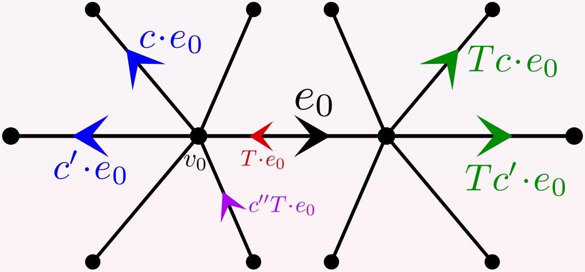
- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.

- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.
  - T is an involution which flips an edge e_0 touching the origin.

- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.
  - T is an involution which flips an edge e_0 touching the origin.

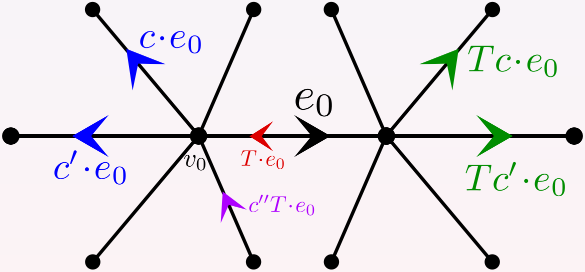


- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.
  - T is an involution which flips an edge e_0 touching the origin.



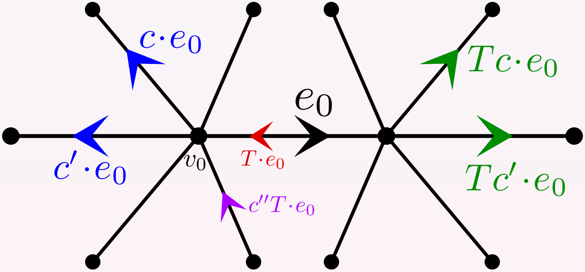
- Then, $\Gamma = \langle C, T \rangle$ acts simply-transitively on the edges of the tree.

- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.
  - T is an involution which flips an edge e_0 touching the origin.



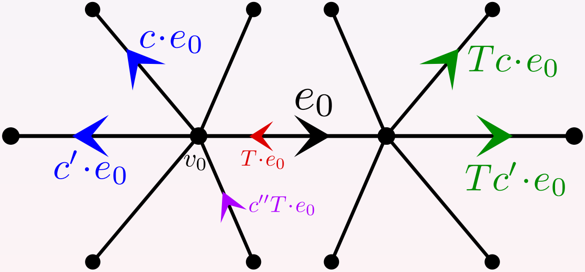
- Then, $\Gamma = \langle C, T \rangle$ acts simply-transitively on the edges of the tree.
- Fault-tolerance: T and all $c \in C$ are of finite order.

- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.
  - T is an involution which flips an edge e_0 touching the origin.

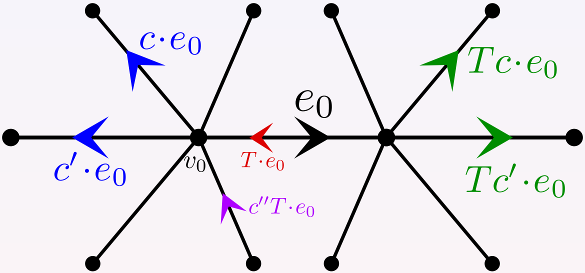


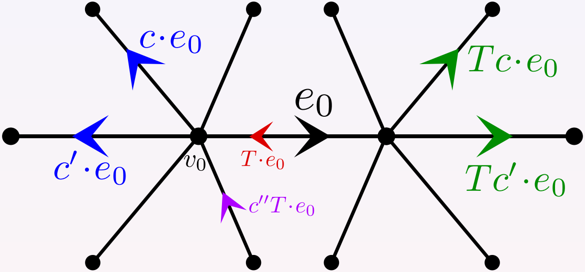
- Then, $\Gamma = \langle C, T \rangle$ acts simply-transitively on the edges of the tree.
- Fault-tolerance: T and all $c \in C$ are of finite order.
- Γ is a free product of C and $\langle T \rangle \cong \mathbb{Z}/2 \Rightarrow$ optimal growth rate (under assumptions).

- Want $C \leq PU(2)$, $T \in PU(2)$, acting on T_k, so that
  - C fixes $v_0 \in V(T_k)$ and acts simply-transitively on its neighbors.
  - T is an involution which flips an edge e_0 touching the origin.

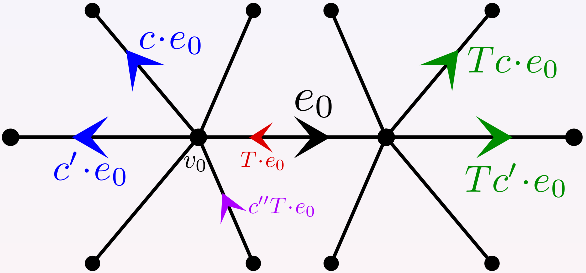


- Then, $\Gamma = \langle C, T \rangle$ acts simply-transitively on the edges of the tree.
- Fault-tolerance: T and all $c \in C$ are of finite order.
- Γ is a free product of C and $\langle T \rangle \cong \mathbb{Z}/2 \Rightarrow$ optimal growth rate (under assumptions).
- Navigation/compiling by the action on edges.

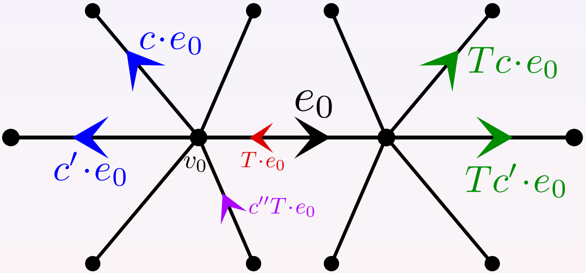

$c \cdot e_0$
$Tc \cdot e_0$
e_0
$c' \cdot e_0$
v_0
$T \cdot e_0$
$Tc' \cdot e_0$
$c''T \cdot e_0$



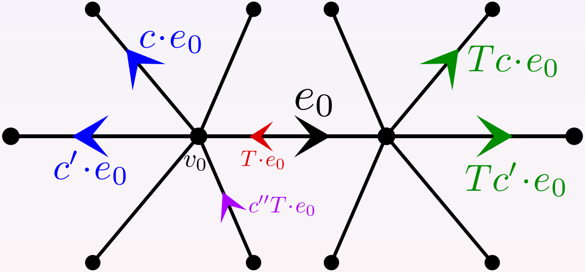
- Observe $S = \{ Tc \mid 1 \neq c \in C \}$ $\quad (|S| = k - 1)$.



- Observe $S = \{Tc \mid 1 \neq c \in C\}$ $(|S| = k - 1)$.
- $S \cdot \ldots \cdot S \cdot e_0$ - non-backtracking random walk starting from e_0.



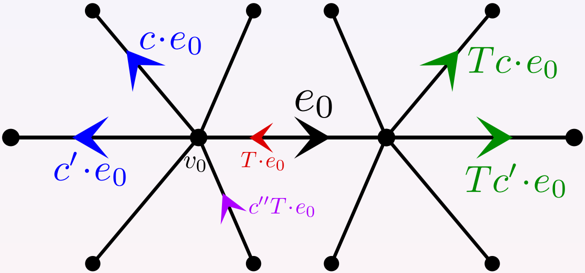
- Observe $S = \{ Tc \mid 1 \neq c \in C \}$ $(|S| = k - 1)$.
- $S \cdot \ldots \cdot S \cdot e_0$ - non-backtracking random walk starting from e_0.
- S generates a free semigroup $\Rightarrow$ optimal growth rate $(|S|^\ell)$.



- Observe $S = \{Tc \mid 1 \neq c \in C\}$ $(|S| = k-1)$.
- $S \cdot \ldots \cdot S \cdot e_0$ - non-backtracking random walk starting from e_0.
- S generates a free semigroup $\Rightarrow$ optimal growth rate $(|S|^{\ell})$.
- For our S, which come from arithmetics, we obtain

$$|\lambda_S| \leq \sqrt{k-1}$$

for the second eigenvalue of $(A_S f)(x) = \sum_{s\in S} f(sx)$ on $L^2(PU(2))$.



- Observe $S = \{Tc \mid 1 \neq c \in C\}$ $\quad (|S| = k - 1)$.
- $S \cdot \ldots \cdot S \cdot e_0$ - non-backtracking random walk starting from e_0.
- S generates a free semigroup $\Rightarrow$ optimal growth rate ($|S|^{\ell}$).
- For our S, which come from arithmetics, we obtain

$$|\lambda_S| \leq \sqrt{k-1}$$

  for the second eigenvalue of $(A_S f)(x) = \sum_{s \in S} f(sx)$ on $L^2(PU(2))$.
- $\sqrt{k-1}$: spectrum of NBRW on the k-regular tree.

Icosahedral gates

- Super-golden-gates?

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & \varphi - \varphi^{-1} i \\ \varphi + \varphi^{-1} i & -1 \end{pmatrix} \right\rangle \cong A_5, \qquad T = \begin{pmatrix} 2+\varphi & 1-i \\ 1+i & -2-\varphi \end{pmatrix}$$

where $\varphi = \frac{1+\sqrt{5}}{2}$.

- Super-golden-gates?

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & \varphi - \varphi^{-1} i \\ \varphi + \varphi^{-1} i & -1 \end{pmatrix} \right\rangle \cong A_5, \qquad T = \begin{pmatrix} 2+\varphi & 1-i \\ 1+i & -2-\varphi \end{pmatrix}$$

where $\varphi = \frac{1+\sqrt{5}}{2}$.

- C acts simply-transitively on the origin of a 60-regular tree, and T flips an edge.

Icosahedral gates

- Super-golden-gates?

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & \varphi - \varphi^{-1} i \\ \varphi + \varphi^{-1} i & -1 \end{pmatrix} \right\rangle \cong A_5, \qquad T = \begin{pmatrix} 2+\varphi & 1-i \\ 1+i & -2-\varphi \end{pmatrix}$$

  where $\varphi = \frac{1+\sqrt{5}}{2}$.
- C acts simply-transitively on the origin of a 60-regular tree, and T flips an edge.
- Γ is a finite extension of $PGU_2\left(\mathbb{Z}\left[\varphi, \frac{1}{7+5\varphi}\right]\right)$.

Icosahedral gates

- Super-golden-gates?

$$C = \left\langle \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & \varphi - \varphi^{-1} i \\ \varphi + \varphi^{-1} i & -1 \end{pmatrix} \right\rangle \cong A_5, \qquad T = \begin{pmatrix} 2+\varphi & 1-i \\ 1+i & -2-\varphi \end{pmatrix}$$

  where $\varphi = \frac{1+\sqrt{5}}{2}$.
- C acts simply-transitively on the origin of a 60-regular tree, and T flips an edge.
- Γ is a finite extension of $PGU_2\left(\mathbb{Z}\left[\varphi, \frac{1}{7+5\varphi}\right]\right)$.
- $\Gamma = \langle C, T \rangle$ is the full $\{7+5\varphi\}$-arithmetic group in the Icosian ring:

$$\mathbb{I} = \left\{ \frac{1}{2} \begin{pmatrix} (a+b\varphi) + (c+d\varphi)\, i \\ + (e+f\varphi)\, j + (g+h\varphi)\, k \end{pmatrix} \,\middle|\, \begin{matrix} a,b,c,d,e,f,g,h \in \mathbb{Z} \\ a+c+e+g \equiv b+d+f+h \equiv 0 \pmod 2 \\ (c,e,a) \equiv (b,d,f) \text{ or } \equiv (1,1,1)+(b,d,f) \pmod 2 \end{matrix} \right\} \subseteq \mathbb{H}.$$

- Back to the discrete world.

- Back to the discrete world.
- We identified the edges of the tree with an arithmetic group Γ.

Ramanujan digraphs

- Back to the discrete world.
- We identified the edges of the tree with an arithmetic group Γ.
- If we take $S = \{ Tc \,|\, 1 \neq c \in C \}$ as generators for Γ, we can identify the Cayley graph of Γ with the edge-digraph of the tree, and the adjacency operator becomes the NBRW.

Ramanujan digraphs

- Back to the discrete world.
- We identified the edges of the tree with an arithmetic group Γ.
- If we take $S = \{\, Tc \,|\, 1 \neq c \in C \,\}$ as generators for Γ, we can identify the Cayley graph of Γ with the edge-digraph of the tree, and the adjacency operator becomes the NBRW.
- The spectrum of NBRW on a Ramanujan graph is

$$\operatorname{Spec} A \subseteq \{\pm p\} \cup \{ z \in \mathbb{C} \,|\, |z| \leq \sqrt{p} \}.$$

- Back to the discrete world.
- We identified the edges of the tree with an arithmetic group Γ.
- If we take $S = \{Tc \mid 1 \neq c \in C\}$ as generators for Γ, we can identify the Cayley graph of Γ with the edge-digraph of the tree, and the adjacency operator becomes the NBRW.
- The spectrum of NBRW on a Ramanujan graph is

$$\operatorname{Spec} A \subseteq \{\pm p\} \cup \{z \in \mathbb{C} \mid |z| \leq \sqrt{p}\}.$$

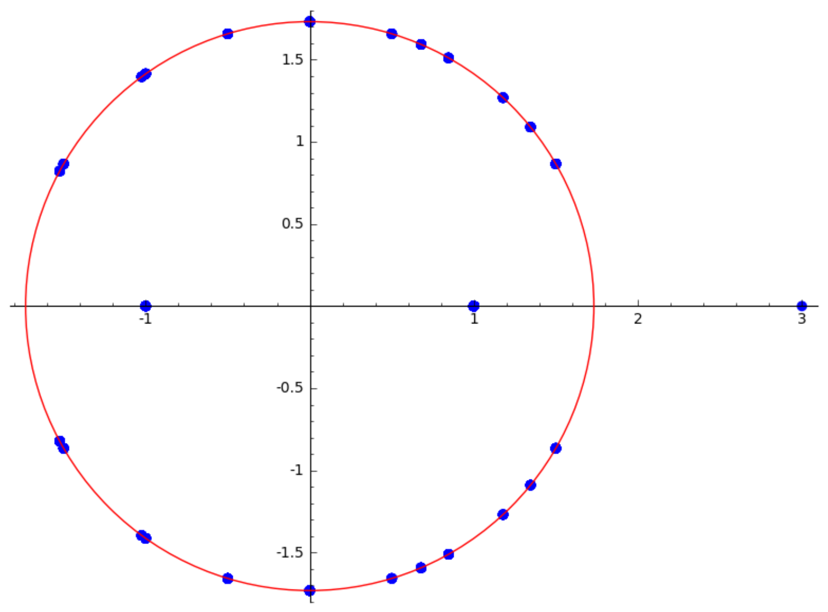
- We call this a Ramanujan digraph.

Ramanujan digraphs

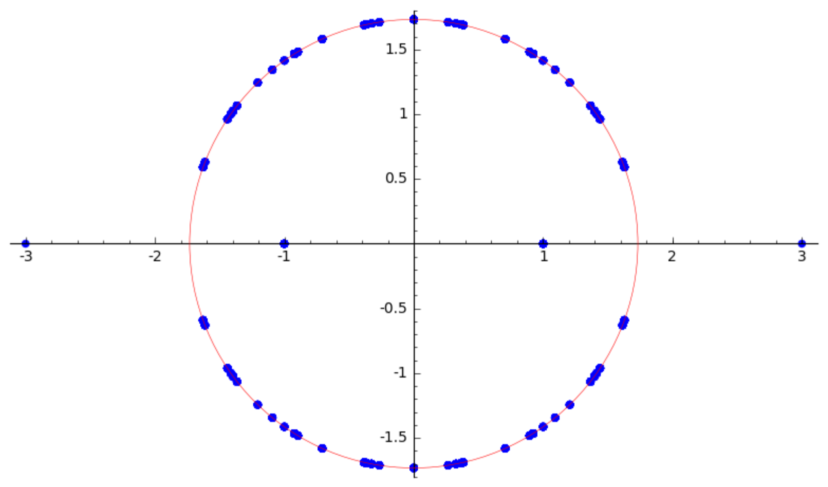
- Back to the discrete world.
- We identified the edges of the tree with an arithmetic group Γ.
- If we take $S = \{ Tc \mid 1 \neq c \in C \}$ as generators for Γ, we can identify the Cayley graph of Γ with the edge-digraph of the tree, and the adjacency operator becomes the NBRW.
- The spectrum of NBRW on a Ramanujan graph is

$$\operatorname{Spec} A \subseteq \{\pm p\} \cup \{z \in \mathbb{C} \mid |z| \leq \sqrt{p}\}.$$

- We call this a Ramanujan digraph.
- For arithmetic quotients $\Gamma_q \backslash \Gamma$, we obtain Cayley Ramanujan digraphs.



Adjacency spectrum of $PSL_2(\mathbb{F}_{13})$ with respect to $\begin{pmatrix} 12 & 9 \\ 7 & 12 \end{pmatrix}, \begin{pmatrix} 6 & 8 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 4 & 12 \\ 1 & 7 \end{pmatrix}$



Adjacency spectrum of $PGL_2(\mathbb{F}_{17})$ with respect to $\left(\begin{smallmatrix}16 & 14\\ 12 & 16\end{smallmatrix}\right), \left(\begin{smallmatrix}5 & 13\\ 13 & 14\end{smallmatrix}\right), \left(\begin{smallmatrix}3 & 16\\ 1 & 12\end{smallmatrix}\right)$

- Ramanujan graphs $\Rightarrow$ Ramanujan complexes

Higher dimensions

- Ramanujan graphs $\Rightarrow$ Ramanujan complexes
- k-regular tree $\Rightarrow$ Bruhat-Tits building - infinite contractible simplicial complex

Higher dimensions

- Ramanujan graphs $\Rightarrow$ Ramanujan complexes
- k-regular tree $\Rightarrow$ Bruhat-Tits building - infinite contractible simplicial complex
- $PU(2) \Rightarrow PU(n)$

- Ramanujan graphs $\Rightarrow$ Ramanujan complexes
- k-regular tree $\Rightarrow$ Bruhat-Tits building - infinite contractible simplicial complex
- $PU(2) \Rightarrow PU(n)$
- No arithmetic free groups for $n \geq 5$ (Kazhdan '67).

Higher dimensions

- Ramanujan graphs $\Rightarrow$ Ramanujan complexes
- k-regular tree $\Rightarrow$ Bruhat-Tits building - infinite contractible simplicial complex
- $PU(2) \Rightarrow PU(n)$
- No arithmetic free groups for $n \geq 5$ (Kazhdan '67).
- No simply-transitive actions for $n \geq 8$ (Mohammadi-Salehi Golsefidy '12).

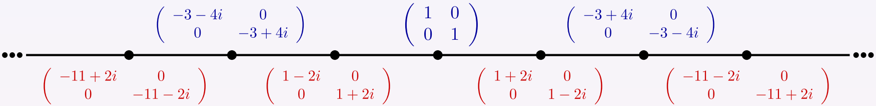
- Ramanujan graphs $\Rightarrow$ Ramanujan complexes
- k-regular tree $\Rightarrow$ Bruhat-Tits building - infinite contractible simplicial complex
- $PU(2) \Rightarrow PU(n)$
- No arithmetic free groups for $n \geq 5$ (Kazhdan '67).
- No simply-transitive actions for $n \geq 8$ (Mohammadi-Salehi Golsefidy '12).
- Compiling is done by navigating the building.

Higher dimensions

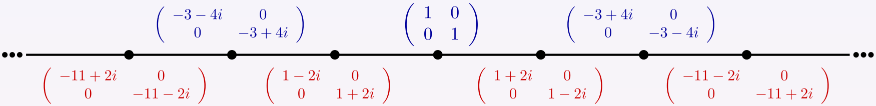
- Ramanujan graphs $\Rightarrow$ Ramanujan complexes
- k-regular tree $\Rightarrow$ Bruhat-Tits building - infinite contractible simplicial complex
- $PU(2) \Rightarrow PU(n)$
- No arithmetic free groups for $n \geq 5$ (Kazhdan '67).
- No simply-transitive actions for $n \geq 8$ (Mohammadi-Salehi Golsefidy '12).
- Compiling is done by navigating the building.
- Approximation is much harder.

PU(3)

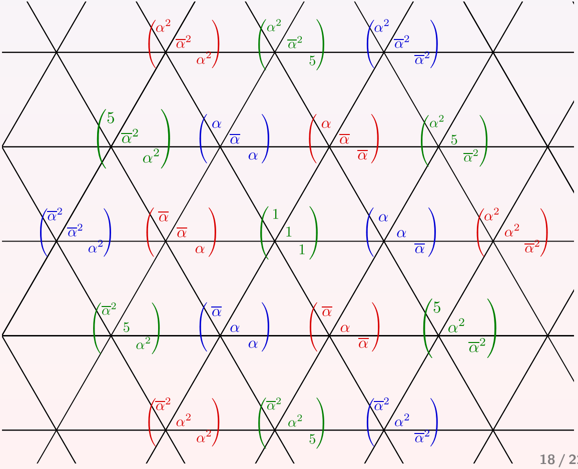
PU(3)



$\begin{pmatrix} -3-4i & 0 \\ 0 & -3+4i \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} -3+4i & 0 \\ 0 & -3-4i \end{pmatrix}$
$\begin{pmatrix} -11+2i & 0 \\ 0 & -11-2i \end{pmatrix}$
$\begin{pmatrix} 1-2i & 0 \\ 0 & 1+2i \end{pmatrix}$
$\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix}$
$\begin{pmatrix} -11-2i & 0 \\ 0 & -11+2i \end{pmatrix}$

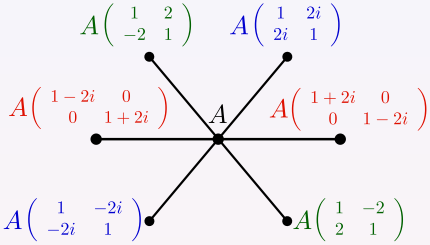


Is replaced in PGU_3
by a Euclidean plane:
$(\alpha = 1 + 2i)$

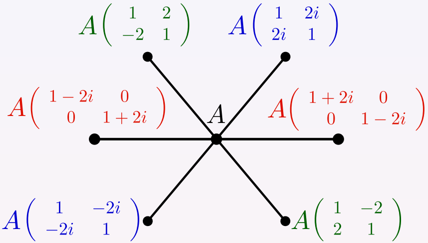


The vista of a vertex in $\Gamma \leq PU(2)$:

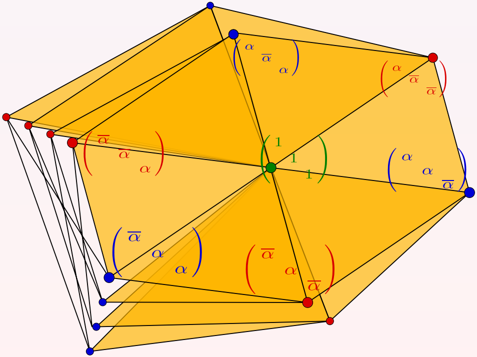
The vista of a vertex in $\Gamma \leq PU(2)$:



The vista of a vertex in $\Gamma \leq PU(2)$:



Vista of a vertex in $\Gamma \leq PU(3)$:



- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2+|\beta|^2+|\gamma|^2=p, \qquad \alpha,\beta,\gamma\in\mathbb{Z}[i].$$

- Can these be completed to $\left(\begin{smallmatrix}\alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ?\end{smallmatrix}\right) \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

Explicit constructions

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Can these be completed to $\left(\begin{smallmatrix} \alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ? \end{smallmatrix}\right) \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

$$\left(\begin{smallmatrix} 1 & i-1 & -i-1 \\ -i+1 & 1 & -i+1 \\ -i-1 & i-1 & 1 \end{smallmatrix}\right)$$

Explicit constructions

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Can these be completed to $\begin{pmatrix} \alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ? \end{pmatrix} \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

$$\begin{pmatrix} 1 & i-1 & -i-1 \\ -i+1 & 1 & -i+1 \\ -i-1 & i-1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & i+1 & 3i-1 \\ i+1 & -3 & i+1 \\ 3i-1 & i+1 & 1 \end{pmatrix}$$

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Can these be completed to $\begin{pmatrix} \alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ? \end{pmatrix} \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

$$\begin{pmatrix} 1 & i-1 & -i-1 \\ -i+1 & 1 & -i+1 \\ -i-1 & i-1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & i+1 & 3i-1 \\ i+1 & -3 & i+1 \\ 3i-1 & i+1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2i+2 & 2i+2 \\ 2i+2 & 2i-1 & 2 \\ -2i+2 & -2 & 2i-1 \end{pmatrix}$$

Explicit constructions

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Can these be completed to $\left(\begin{smallmatrix} \alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ? \end{smallmatrix}\right) \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

$$\begin{pmatrix} 1 & i-1 & -i-1 \\ -i+1 & 1 & -i+1 \\ -i-1 & i-1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & i+1 & 3i-1 \\ i+1 & -3 & i+1 \\ 3i-1 & i+1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2i+2 & 2i+2 \\ 2i+2 & 2i-1 & 2 \\ -2i+2 & -2 & 2i-1 \end{pmatrix}, \begin{pmatrix} -12i+1 & -2i-2 & -2i \\ 2i-2 & -10i+3 & -6i-2 \\ -2i & -2i+6 & 8i-7 \end{pmatrix}$$

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Can these be completed to $\begin{pmatrix} \alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ? \end{pmatrix} \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

$$\begin{pmatrix} 1 & i-1 & -i-1 \\ -i+1 & 1 & -i+1 \\ -i-1 & i-1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & i+1 & 3i-1 \\ i+1 & -3 & i+1 \\ 3i-1 & i+1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2i+2 & 2i+2 \\ 2i+2 & 2i-1 & 2 \\ -2i+2 & -2 & 2i-1 \end{pmatrix}, \begin{pmatrix} -12i+1 & -2i-2 & -2i \\ 2i-2 & -10i+3 & -6i-2 \\ -2i & -2i+6 & 8i-7 \end{pmatrix}$$

- Siegel's Mass formula allows us to count the solutions

- Jacobi's six-square theorem: for $p \equiv 1 \pmod 4$, there are $12\left(p^2+1\right)$ solutions to

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = p, \qquad \alpha, \beta, \gamma \in \mathbb{Z}[i].$$

- Can these be completed to $\begin{pmatrix} \alpha & \beta & \gamma \\ ? & ? & ? \\ ? & ? & ? \end{pmatrix} \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$?

$$\begin{pmatrix} 1 & i-1 & -i-1 \\ -i+1 & 1 & -i+1 \\ -i-1 & i-1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & i+1 & 3i-1 \\ i+1 & -3 & i+1 \\ 3i-1 & i+1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2i+2 & 2i+2 \\ 2i+2 & 2i-1 & 2 \\ -2i+2 & -2 & 2i-1 \end{pmatrix}, \begin{pmatrix} -12i+1 & -2i-2 & -2i \\ 2i-2 & -10i+3 & -6i-2 \\ -2i & -2i+6 & 8i-7 \end{pmatrix}$$

- Siegel's Mass formula allows us to count the solutions: count solutions in $PGU_2(\mathbb{Q}_p)$ for all p, including $\mathbb{Q}_\infty = \mathbb{R}$.

- Theorem (P):

- Theorem (P): for $p \equiv 1 \pmod 4$,

$$\Gamma = \left\{ A \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv \left(\begin{smallmatrix} 1 & * & * \\ * & 1 & * \\ * & * & 1 \end{smallmatrix}\right) \pmod{2+2i} \right\}$$

acts simply-transitively on the vertices of the building of $PU(3)$.

- Theorem (P): for $p \equiv 1 \pmod 4$,

$$\Gamma = \left\{ A \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \,\middle|\, A \equiv \begin{pmatrix} 1 & * & * \\ * & 1 & * \\ * & * & 1 \end{pmatrix} \pmod{2+2i} \right\}$$

acts simply-transitively on the vertices of the building of $PU(3)$.

- Golden qutrits?

- Theorem (P): for $p \equiv 1 \pmod 4$,

$$\Gamma = \left\{ A \in PGU_3\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \middle| A \equiv \left(\begin{smallmatrix} 1 & * & * \\ * & 1 & * \\ * & * & 1 \end{smallmatrix}\right) \pmod{2+2i} \right\}$$

acts simply-transitively on the vertices of the building of $PU(3)$.

- Golden qutrits?
- Similar results on $PU(4)$ - not as nice. Work in progress!

Thank You!