# Linear similarity of graphs

Peter Sin
University of Florida

New Directions in Combinatorics Workshop, National University Singapore, May 26th, 2016.

# Outline

Introduction

Paley and Peisert graphs

Matrix similarity over rings of algebraic integers

$\ell$-local similarity, for $\ell \neq p$

$p$-local similarity

Jacobi sums

# Matrix invariants

Γ simple graph, $A$ its $0-1$ adjacency matrix.

$A$ is symmetric so *similar* (by orthogonal matrices) to a diagonal matrix

$$D = PAP^{-1}$$

$A$ is integral, so is *equivalent* (by unimodular matrices) to its *Smith Normal Form*

$$E = UAV$$

# Matrix invariants

$\Gamma$ simple graph, $A$ its $0-1$ adjacency matrix.

$A$ is symmetric so *similar* (by orthogonal matrices) to a diagonal matrix

$$D = PAP^{-1}$$

$A$ is integral, so is *equivalent* (by unimodular matrices) to its *Smith Normal Form*

$$E = UAV$$

# Matrix invariants

$\Gamma$ simple graph, $A$ its $0-1$ adjacency matrix.

$A$ is symmetric so *similar* (by orthogonal matrices) to a diagonal matrix

$$D = PAP^{-1}$$

$A$ is integral, so is *equivalent* (by unimodular matrices) to its *Smith Normal Form*

$$E = UAV$$

If $\Gamma'$ is another graph, we can ask if $A$ and $A'$ are both similar (graphs cospectral) and equivalent.

Many examples exist, e.g. the saltire pair.

- But there may be some $c \in \mathbb{Z}$ such that $A + cI$ and $A' + cI$ are not equivalent.

If $\Gamma'$ is another graph, we can ask if $A$ and $A'$ are both similar (graphs cospectral) and equivalent.

Many examples exist, e.g. the saltire pair.

- But there may be some $c \in \mathbb{Z}$ such that $A + cI$ and $A' + cI$ are not equivalent.

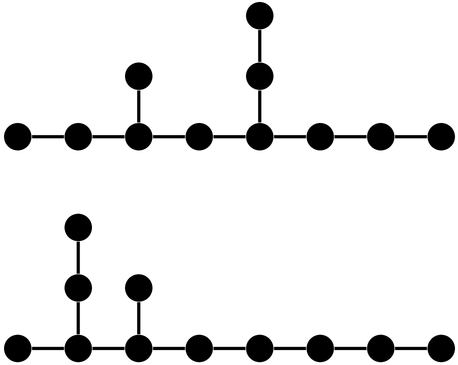
If $\Gamma'$ is another graph, we can ask if $A$ and $A'$ are both similar (graphs cospectral) and equivalent.

Many examples exist, e.g. the saltire pair.

- But there may be some $c \in \mathbb{Z}$ such that $A + cI$ and $A' + cI$ are not equivalent.

# Example from T. Hall on MathOverflow

http://mathoverflow.net/questions/52169/adjacency-matrices-of-graphs/



Hall showed that the adjacency matrices $A$ and $A'$ are similar by a unimodular integral matrix.

Hence for any integers $a$, $b$, $aA + bI$ and $aA' + bI$ are both equivalent and similar.

But $A + J$ is not equivalent to $A' + J$, where $J$ is the matrix whose entries are all equal to 1.

**Question**

Do there exist nonisomorphic graphs $\Gamma$ and $\Gamma'$ such that for all $a, b, c \in \mathbb{Z}$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are similar and equivalent?

These integral combinations are called *generalized adjacency matrices* and include the adjacency matrix of the complementary graph, the $(-1, 1, 0)$-adjacency matrix, and (for regular graphs) the Laplacian matrices.

Hall showed that the adjacency matrices $A$ and $A'$ are similar by a unimodular integral matrix.

Hence for any integers $a$, $b$, $aA + bI$ and $aA' + bI$ are both equivalent and similar.

But $A + J$ is not equivalent to $A' + J$, where $J$ is the matrix whose entries are all equal to 1.

**Question**

Do there exist nonisomorphic graphs $\Gamma$ and $\Gamma'$ such that for all $a, b, c \in \mathbb{Z}$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are similar and equivalent?

These integral combinations are called *generalized adjacency matrices* and include the adjacency matrix of the complementary graph, the $(-1, 1, 0)$-adjacency matrix, and (for regular graphs) the Laplacian matrices.

Hall showed that the adjacency matrices $A$ and $A'$ are similar by a unimodular integral matrix.

Hence for any integers $a$, $b$, $aA + bI$ and $aA' + bI$ are both equivalent and similar.

But $A + J$ is not equivalent to $A' + J$, where $J$ is the matrix whose entries are all equal to 1.

**Question**

Do there exist nonisomorphic graphs $\Gamma$ and $\Gamma'$ such that for all $a, b, c \in \mathbb{Z}$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are similar and equivalent?

These integral combinations are called *generalized adjacency matrices* and include the adjacency matrix of the complementary graph, the $(-1, 1, 0)$-adjacency matrix, and (for regular graphs) the Laplacian matrices.

Hall showed that the adjacency matrices $A$ and $A'$ are similar by a unimodular integral matrix.

Hence for any integers $a$, $b$, $aA + bI$ and $aA' + bI$ are both equivalent and similar.

But $A + J$ is not equivalent to $A' + J$, where $J$ is the matrix whose entries are all equal to 1.

## Question

Do there exist nonisomorphic graphs $\Gamma$ and $\Gamma'$ such that for all $a$, $b$, $c \in \mathbb{Z}$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are similar and equivalent?

These integral combinations are called *generalized adjacency matrices* and include the adjacency matrix of the complementary graph, the $(-1, 1, 0)$-adjacency matrix, and (for regular graphs) the Laplacian matrices.

Hall showed that the adjacency matrices $A$ and $A'$ are similar by a unimodular integral matrix.

Hence for any integers $a$, $b$, $aA + bI$ and $aA' + bI$ are both equivalent and similar.

But $A + J$ is not equivalent to $A' + J$, where $J$ is the matrix whose entries are all equal to 1.

## Question

Do there exist nonisomorphic graphs $\Gamma$ and $\Gamma'$ such that for all $a$, $b$, $c \in \mathbb{Z}$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are similar and equivalent?

These integral combinations are called *generalized adjacency matrices* and include the adjacency matrix of the complementary graph, the $(-1, 1, 0)$-adjacency matrix, and (for regular graphs) the Laplacian matrices.

Hall showed that the adjacency matrices $A$ and $A'$ are similar by a unimodular integral matrix.

Hence for any integers $a$, $b$, $aA + bI$ and $aA' + bI$ are both equivalent and similar.

But $A + J$ is not equivalent to $A' + J$, where $J$ is the matrix whose entries are all equal to 1.

## Question

Do there exist nonisomorphic graphs $\Gamma$ and $\Gamma'$ such that for all $a, b, c \in \mathbb{Z}$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are similar and equivalent?

These integral combinations are called *generalized adjacency matrices* and include the adjacency matrix of the complementary graph, the $(-1, 1, 0)$-adjacency matrix, and (for regular graphs) the Laplacian matrices.

# Strongly regular graphs

The adjacency matrix $A$ of a strongly regular graph $SRG(v, k, \lambda, \mu)$ satisfies

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J$$

Thus if $\Gamma$ and $\Gamma'$ are SRGs with the same parameters, and $\mu \neq 0$, any invertible matrix $C$ transforming $A$ to $A'$ must fix $J$ and conjugate $aA + bI + cJ$ to $aA' + bI + cJ$.

# Strongly regular graphs

The adjacency matrix $A$ of a strongly regular graph $SRG(v, k, \lambda, \mu)$ satisfies

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J$$

Thus if $\Gamma$ and $\Gamma'$ are SRGs with the same parameters, and $\mu \neq 0$, any invertible matrix $C$ transforming $A$ to $A'$ must fix $J$ and conjugate $aA + bI + cJ$ to $aA' + bI + cJ$.

# A family of examples

The rest of this talk is to give an infinite sequence of pairs of graphs such that for all integers $a$, $b$, $c$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are both similar and equivalent. The examples come from Paley graphs and Peisert graphs over fields of order $p^2$, $p \equiv 3 \pmod 4$. I stumbled across them in the process of computing critical groups (Smith Normal forms of Laplacians). Techniques I'll describe for proving equivalence grew out work a paper of Chandler-S-Xiang (2014) computing the critical groups of Paley graphs.

# A family of examples

The rest of this talk is to give an infinite sequence of pairs of graphs such that for all integers $a$, $b$, $c$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are both similar and equivalent. The examples come from Paley graphs and Peisert graphs over fields of order $p^2$, $p \equiv 3 \pmod 4$. I stumbled across them in the process of computing critical groups (Smith Normal forms of Laplacians). Techniques I'll describe for proving equivalence grew out work a paper of Chandler-S-Xiang (2014) computing the critical groups of Paley graphs.

# A family of examples

The rest of this talk is to give an infinite sequence of pairs of graphs such that for all integers $a$, $b$, $c$, the matrices $aA + bI + cJ$ and $aA' + bI + cJ$ are both similar and equivalent. The examples come from Paley graphs and Peisert graphs over fields of order $p^2$, $p \equiv 3 \pmod 4$. I stumbled across them in the process of computing critical groups (Smith Normal forms of Laplacians). Techniques I'll describe for proving equivalence grew out work a paper of Chandler-S-Xiang (2014) computing the critical groups of Paley graphs.

# Outline

# Paley graphs, Peisert graphs

Both graphs can be defined easily as Cayley graphs.

Let $q \equiv 1 \pmod 4$, $S = {\mathbb{F}_q^\times}^2$. The *Paley graph* $\Gamma(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S$.

Let $q = p^{2e}$, $p \equiv 3 \pmod 4$. and $\beta$ a generator of $\mathbb{F}_q^\times$. Set $S' = {\mathbb{F}_q^\times}^4 \cup \beta {\mathbb{F}_q^\times}^4$. The *Peisert graph* $\Gamma'(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S'$.

When both are defined $\Gamma(q)$ and $\Gamma'(q)$ are strongly regular graphs with the same parameters $(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{4})$. Hence they are cospectral.

Peisert (2001) showed that $\Gamma(q) \not\cong \Gamma'(q)$ if $q \neq 9$.

# Paley graphs, Peisert graphs

Both graphs can be defined easily as Cayley graphs.

Let $q \equiv 1 \pmod 4$, $S = {\mathbb{F}_q^\times}^2$. The *Paley graph* $\Gamma(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S$.

Let $q = p^{2e}$, $p \equiv 3 \pmod 4$. and $\beta$ a generator of $\mathbb{F}_q^\times$. Set $S' = {\mathbb{F}_q^\times}^4 \cup \beta {\mathbb{F}_q^\times}^4$. The *Peisert graph* $\Gamma'(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S'$.

When both are defined $\Gamma(q)$ and $\Gamma'(q)$ are strongly regular graphs with the same parameters $(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{4})$. Hence they are cospectral.

Peisert (2001) showed that $\Gamma(q) \not\cong \Gamma'(q)$ if $q \neq 9$.

# Paley graphs, Peisert graphs

Both graphs can be defined easily as Cayley graphs.

Let $q \equiv 1 \pmod 4$, $S = {\mathbb{F}_q^\times}^2$. The *Paley graph* $\Gamma(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S$.

Let $q = p^{2e}$, $p \equiv 3 \pmod 4$. and $\beta$ a generator of $\mathbb{F}_q^\times$. Set $S' = {\mathbb{F}_q^\times}^4 \cup \beta {\mathbb{F}_q^\times}^4$. The *Peisert graph* $\Gamma'(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S'$.

When both are defined $\Gamma(q)$ and $\Gamma'(q)$ are strongly regular graphs with the same parameters $(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{4})$. Hence they are cospectral.

Peisert (2001) showed that $\Gamma(q) \not\cong \Gamma'(q)$ if $q \neq 9$.

# Paley graphs, Peisert graphs

Both graphs can be defined easily as Cayley graphs.

Let $q \equiv 1 \pmod 4$, $S = {\mathbb{F}_q^\times}^2$. The *Paley graph* $\Gamma(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S$.

Let $q = p^{2e}$, $p \equiv 3 \pmod 4$. and $\beta$ a generator of $\mathbb{F}_q^\times$. Set $S' = {\mathbb{F}_q^\times}^4 \cup \beta {\mathbb{F}_q^\times}^4$. The *Peisert graph* $\Gamma'(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S'$.

When both are defined $\Gamma(q)$ and $\Gamma'(q)$ are strongly regular graphs with the same parameters $(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{4})$. Hence they are cospectral.

Peisert (2001) showed that $\Gamma(q) \not\cong \Gamma'(q)$ if $q \neq 9$.

# Paley graphs, Peisert graphs

Both graphs can be defined easily as Cayley graphs.

Let $q \equiv 1 \pmod 4$, $S = {\mathbb{F}_q^\times}^2$. The *Paley graph* $\Gamma(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S$.

Let $q = p^{2e}$, $p \equiv 3 \pmod 4$. and $\beta$ a generator of $\mathbb{F}_q^\times$. Set $S' = {\mathbb{F}_q^\times}^4 \cup \beta {\mathbb{F}_q^\times}^4$. The *Peisert graph* $\Gamma'(q)$ is the Cayley graph based on the group $(\mathbb{F}_q, +)$ with generating set $S'$.

When both are defined $\Gamma(q)$ and $\Gamma'(q)$ are strongly regular graphs with the same parameters $(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{4})$. Hence they are cospectral.

Peisert (2001) showed that $\Gamma(q) \not\cong \Gamma'(q)$ if $q \neq 9$.

# Outline

## Theorem

*(Guralnick (1980), Taussky(1979), Dade(1963), Reiner-Zassenhaus (1971)) Let $D$ be the ring of algebraic integers in a number field $K$. Suppose that $B$ and $B'$ are square matrices with entries in $D$ Then the following are equivalent.*

(i) *$B$ and $B'$ are similar over $D_P$ for every prime ideal $P$ of $D$.*

(ii) *$B$ and $B'$ are similar over some finite integral extension of $D$.*

(iii) *There is a finite extension $L$ of $K$, such that for each for each prime $P$ of $D$, there is a prime $Q$ of the ring $E$ of integers of $L$, with $Q \supseteq P$, such that $B$ and $B'$ are similar over the local ring $E_Q$.*

Note that the SNF is locally determined.

## Theorem

*(Guralnick (1980), Taussky(1979), Dade(1963), Reiner-Zassenhaus (1971)) Let $D$ be the ring of algebraic integers in a number field $K$. Suppose that $B$ and $B'$ are square matrices with entries in $D$ Then the following are equivalent.*

(i) *$B$ and $B'$ are similar over $D_P$ for every prime ideal $P$ of $D$.*

(ii) *$B$ and $B'$ are similar over some finite integral extension of $D$.*

(iii) *There is a finite extension $L$ of $K$, such that for each for each prime $P$ of $D$, there is a prime $Q$ of the ring $E$ of integers of $L$, with $Q \supseteq P$, such that $B$ and $B'$ are similar over the local ring $E_Q$.*

Note that the SNF is locally determined.

## Theorem

*(Guralnick (1980), Taussky(1979), Dade(1963), Reiner-Zassenhaus (1971)) Let $D$ be the ring of algebraic integers in a number field $K$. Suppose that $B$ and $B'$ are square matrices with entries in $D$ Then the following are equivalent.*

(i) *$B$ and $B'$ are similar over $D_P$ for every prime ideal $P$ of $D$.*

(ii) *$B$ and $B'$ are similar over some finite integral extension of $D$.*

(iii) *There is a finite extension $L$ of $K$, such that for each for each prime $P$ of $D$, there is a prime $Q$ of the ring $E$ of integers of $L$, with $Q \supseteq P$, such that $B$ and $B'$ are similar over the local ring $E_Q$.*

Note that the SNF is locally determined.

### Theorem

*(Guralnick (1980), Taussky(1979), Dade(1963), Reiner-Zassenhaus (1971)) Let $D$ be the ring of algebraic integers in a number field $K$. Suppose that $B$ and $B'$ are square matrices with entries in $D$ Then the following are equivalent.*

(i) *$B$ and $B'$ are similar over $D_P$ for every prime ideal $P$ of $D$.*

(ii) *$B$ and $B'$ are similar over some finite integral extension of $D$.*

(iii) *There is a finite extension $L$ of $K$, such that for each for each prime $P$ of $D$, there is a prime $Q$ of the ring $E$ of integers of $L$, with $Q \supseteq P$, such that $B$ and $B'$ are similar over the local ring $E_Q$.*

Note that the SNF is locally determined.

## Theorem

*(Guralnick (1980), Taussky(1979), Dade(1963), Reiner-Zassenhaus (1971)) Let $D$ be the ring of algebraic integers in a number field $K$. Suppose that $B$ and $B'$ are square matrices with entries in $D$ Then the following are equivalent.*

(i) *$B$ and $B'$ are similar over $D_P$ for every prime ideal $P$ of $D$.*

(ii) *$B$ and $B'$ are similar over some finite integral extension of $D$.*

(iii) *There is a finite extension $L$ of $K$, such that for each for each prime $P$ of $D$, there is a prime $Q$ of the ring $E$ of integers of $L$, with $Q \supseteq P$, such that $B$ and $B'$ are similar over the local ring $E_Q$.*

Note that the SNF is locally determined.

# Outline

# Discrete Fourier transform

$X$, complex character table of $(\mathbb{F}_q, +)$ with elements ordered in the same way as for the rows and columns of $A(q)$.

$X$ is invertible as a matrix in the ring $\mathbb{Z}[\zeta][\frac{1}{p}]$, $\zeta$ a complex primitive $p$-th root of unity.

(McWilliams-Mann (1968))

$$\begin{aligned} XA(q)X^{-1} &= \mathrm{diag}(\psi(S))_\psi \\ &= U\,\mathrm{diag}(\psi(S'))_\psi U^{-1} = UXA'(q)X^{-1}U^{-1}. \end{aligned} \quad (1)$$

where $\psi$ runs over the additive characters of $\mathbb{F}_q$ and $\psi(S) = \sum_{y \in S} \psi(y)$. Thus, the $\psi(S)$ are the eigenvalues of $A$.

Since $A'$ and $A$ are cospectral, we can extend the equation with some permutation matrix $U$.

# Discrete Fourier transform

$X$, complex character table of $(\mathbb{F}_q, +)$ with elements ordered in the same way as for the rows and columns of $A(q)$.

$X$ is invertible as a matrix in the ring $\mathbb{Z}[\zeta][\frac{1}{p}]$, $\zeta$ a complex primitive $p$-th root of unity.

(McWilliams-Mann (1968))

$$\begin{aligned} XA(q)X^{-1} &= \mathrm{diag}(\psi(S))_\psi \\ &= U\,\mathrm{diag}(\psi(S'))_\psi U^{-1} = UXA'(q)X^{-1}U^{-1}. \end{aligned} \quad (1)$$

where $\psi$ runs over the additive characters of $\mathbb{F}_q$ and $\psi(S) = \sum_{y \in S} \psi(y)$. Thus, the $\psi(S)$ are the eigenvalues of $A$.

Since $A'$ and $A$ are cospectral, we can extend the equation with some permutation matrix $U$.

# Discrete Fourier transform

$X$, complex character table of $(\mathbb{F}_q, +)$ with elements ordered in the same way as for the rows and columns of $A(q)$.

$X$ is invertible as a matrix in the ring $\mathbb{Z}[\zeta][\frac{1}{p}]$, $\zeta$ a complex primitive $p$-th root of unity.

(McWilliams-Mann (1968))

$$XA(q)X^{-1} = \mathrm{diag}(\psi(S))_\psi = U\,\mathrm{diag}(\psi(S'))_\psi U^{-1} = UXA'(q)X^{-1}U^{-1}. \quad (1)$$

where $\psi$ runs over the additive characters of $\mathbb{F}_q$ and $\psi(S) = \sum_{y \in S} \psi(y)$. Thus, the $\psi(S)$ are the eigenvalues of $A$.

Since $A'$ and $A$ are cospectral, we can extend the equation with some permutation matrix $U$.

# Discrete Fourier transform

$X$, complex character table of $(\mathbb{F}_q, +)$ with elements ordered in the same way as for the rows and columns of $A(q)$.

$X$ is invertible as a matrix in the ring $\mathbb{Z}[\zeta][\frac{1}{p}]$, $\zeta$ a complex primitive $p$-th root of unity.

(McWilliams-Mann (1968))

$$\begin{aligned} XA(q)X^{-1} &= \mathrm{diag}(\psi(S))_\psi \\ &= U\,\mathrm{diag}(\psi(S'))_\psi U^{-1} = UXA'(q)X^{-1}U^{-1}. \end{aligned} \tag{1}$$

where $\psi$ runs over the additive characters of $\mathbb{F}_q$ and $\psi(S) = \sum_{y \in S} \psi(y)$. Thus, the $\psi(S)$ are the eigenvalues of $A$.

Since $A'$ and $A$ are cospectral, we can extend the equation with some permutation matrix $U$.

# $\ell$-local similarity

For any prime $\ell \neq p$, choose a prime ideal $\Lambda$ of $\mathbb{Z}[\zeta]$ containing $\ell$.

Equation (1) can be viewed as similarity over $\mathbb{Z}[\zeta]_\Lambda$.

$$XA(q)X^{-1} = UXA'(q)X^{-1}U^{-1}.$$

**Proposition**

*Assume $q = p^{2e}$, $p \equiv 3 \pmod 4$. For each prime $\ell \neq p$, $A(q)$ is similar to $A'(q)$ over $\mathbb{Z}[\zeta]_\Lambda$, where $\Lambda$ is a prime ideal containing $\ell$.*

# $\ell$-local similarity

For any prime $\ell \neq p$, choose a prime ideal $\Lambda$ of $\mathbb{Z}[\zeta]$ containing $\ell$.

Equation (1) can be viewed as similarity over $\mathbb{Z}[\zeta]_\Lambda$.

$$XA(q)X^{-1} = UXA'(q)X^{-1}U^{-1}.$$

**Proposition**

*Assume $q = p^{2e}$, $p \equiv 3 \pmod 4$. For each prime $\ell \neq p$, $A(q)$ is similar to $A'(q)$ over $\mathbb{Z}[\zeta]_\Lambda$, where $\Lambda$ is a prime ideal containing $\ell$.*

# $\ell$-local similarity

For any prime $\ell \neq p$, choose a prime ideal $\Lambda$ of $\mathbb{Z}[\zeta]$ containing $\ell$.

Equation (1) can be viewed as similarity over $\mathbb{Z}[\zeta]_\Lambda$.

$$XA(q)X^{-1} = UXA'(q)X^{-1}U^{-1}.$$

**Proposition**

*Assume $q = p^{2e}$, $p \equiv 3 \pmod 4$. For each prime $\ell \neq p$, $A(q)$ is similar to $A'(q)$ over $\mathbb{Z}[\zeta]_\Lambda$, where $\Lambda$ is a prime ideal containing $\ell$.*

# Outline

Introduction

Paley and Peisert graphs

Matrix similarity over rings of algebraic integers

$\ell$-local similarity, for $\ell \neq p$

*p*-local similarity

Jacobi sums

From now on assume $q = p^2$, $p \equiv 3 \pmod 4$.

We wish to show that $A = A(p^2)$ is similar to $A' = A'(p^2)$ over the localization of some ring of algebraic integers at a prime containing $p$.

For convenience, replace $A$ and $A'$ by $K = 2A + I$ and $K' = 2A' + I$.

From now on assume $q = p^2$, $p \equiv 3 \pmod 4$.

We wish to show that $A = A(p^2)$ is similar to $A' = A'(p^2)$ over the localization of some ring of algebraic integers at a prime containing $p$.

For convenience, replace $A$ and $A'$ by $K = 2A + I$ and $K' = 2A' + I$.

From now on assume $q = p^2$, $p \equiv 3 \pmod 4$.

We wish to show that $A = A(p^2)$ is similar to $A' = A'(p^2)$ over the localization of some ring of algebraic integers at a prime containing $p$.

For convenience, replace $A$ and $A'$ by $K = 2A + I$ and $K' = 2A' + I$.

# The module $R^{\mathbb{F}_q}$

- $R_0 = Z[t]/\Phi_{q-1}(t) \cong \mathbb{Z}[\xi]$, $\xi$ a primitive $(q-1)$-st root of unity.
- $p$ is unramified in $R_0$, so if $P$ is a prime ideal of $R_0$ containing $p$, then $R = (R_0)_P$ is a DVR with maximal ideal $pR$ and $R/pR \cong \mathbb{F}_q$.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_K, \mu_{K'} : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication.

# The module $R^{\mathbb{F}_q}$

- $R_0 = Z[t]/\Phi_{q-1}(t) \cong \mathbb{Z}[\xi]$, $\xi$ a primitive $(q-1)$-st root of unity.
- $p$ is unramified in $R_0$, so if $P$ is a prime ideal of $R_0$ containing $p$, then $R = (R_0)_P$ is a DVR with maximal ideal $pR$ and $R/pR \cong \mathbb{F}_q$.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_K, \mu_{K'} : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication.

# The module $R^{\mathbb{F}_q}$

- $R_0 = Z[t]/\Phi_{q-1}(t) \cong \mathbb{Z}[\xi]$, $\xi$ a primitive $(q-1)$-st root of unity.
- $p$ is unramified in $R_0$, so if $P$ is a prime ideal of $R_0$ containing $p$, then $R = (R_0)_P$ is a DVR with maximal ideal $pR$ and $R/pR \cong \mathbb{F}_q$.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_K, \mu_{K'} : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication.

# The module $R^{\mathbb{F}_q}$

- $R_0 = Z[t]/\Phi_{q-1}(t) \cong \mathbb{Z}[\xi]$, $\xi$ a primitive $(q-1)$-st root of unity.
- $p$ is unramified in $R_0$, so if $P$ is a prime ideal of $R_0$ containing $p$, then $R = (R_0)_P$ is a DVR with maximal ideal $pR$ and $R/pR \cong \mathbb{F}_q$.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_K, \mu_{K'} : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication.

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters $T^i$, $i = 0, \ldots, q-2$.
- The component affording $T^i$ is spanned by

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{\mathbf{1}, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters $T^i$, $i = 0, \ldots, q-2$.
- The component affording $T^i$ is spanned by

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{\mathbf{1}, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters $T^i$, $i = 0,\ldots,q-2$.
- The component affording $T^i$ is spanned by

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{\mathbf{1}, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters $T^i$, $i = 0, \ldots, q-2$.
- The component affording $T^i$ is spanned by

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{\mathbf{1}, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters $T^i$, $i = 0, \ldots, q-2$.
- The component affording $T^i$ is spanned by

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{\mathbf{1}, [0]\}$,

# $\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$ of fourth powers.

$r := \frac{(q-1)}{4}$.

$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.

For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# ${\mathbb{F}_q^\times}^4$-decomposition

Next consider the action of the subgroup $H = {\mathbb{F}_q^\times}^4$ of fourth powers.

$r := \frac{(q-1)}{4}$.
$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.
For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# $\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$ of fourth powers.

$r := \frac{(q-1)}{4}$.
$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.
For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# $\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$ of fourth powers.

$r := \frac{(q-1)}{4}$.
$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.
For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# $\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$ of fourth powers.

$r := \frac{(q-1)}{4}$.

$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.

For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# $\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$ of fourth powers.

$r := \frac{(q-1)}{4}$.

$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.

For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# ${\mathbb{F}_q^\times}^4$-decomposition

Next consider the action of the subgroup $H = {\mathbb{F}_q^\times}^4$ of fourth powers.

$r := \frac{(q-1)}{4}$.
$T^i$,$T^{i+r}$,$T^{i+2r}$, and $T^{i+3r}$ are equal on $H$.
For $i \notin \{0, r, 2r, 3r\}$ the elements $e_i$, $e_{i+r}$, $e_{i+2r}$ and $e_{i+3r}$ span the $H$-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- $M_0$, the submodule of $H$-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, $e_r$, $e_{2r}$ and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- $\mu_K$ and $\mu_{K'}$ preserve $M_i$ as they are $RH$-module homomophisms.
- Can re-order new basis so that the matrices of $\mu_K$ and $\mu_{K'}$ are block-diagonal with $\frac{q-5}{4}$ $4 \times 4$ blocks and a single $5 \times 5$ block.

# Outline

# Jacobi Sums

**Definition**

Let $\theta$ and $\psi$ be multiplicative characters of $\mathbb{F}_q^\times$ taking values in $R^\times$. The *Jacobi sum* is

$$J(\theta, \psi) = \sum_{x \in \mathbb{F}_q} \theta(x)\psi(1 - x).$$

(At $x = 0$, nonprinc. chars take value 0, princ. char takes value 1.)

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x]$$

# Jacobi Sums

**Definition**

Let $\theta$ and $\psi$ be multiplicative characters of $\mathbb{F}_q^\times$ taking values in $R^\times$. The *Jacobi sum* is

$$J(\theta, \psi) = \sum_{x \in \mathbb{F}_q} \theta(x)\psi(1-x).$$

(At $x = 0$, nonprinc. chars take value 0, princ. char takes value 1.)

$$\mu_A(e_i) = \sum_{x \in \mathbb{F}_q^\times} \sum_{y \in S} T^i(x^{-1})[x+y]$$

# Jacobi Sums

## Definition

Let $\theta$ and $\psi$ be multiplicative characters of $\mathbb{F}_q^\times$ taking values in $R^\times$. The *Jacobi sum* is

$$J(\theta, \psi) = \sum_{x \in \mathbb{F}_q} \theta(x)\psi(1 - x).$$

(At $x = 0$, nonprinc. chars take value 0, princ. char takes value 1.)

$$\begin{aligned}
\mu_A(e_i) &= \sum_{x \in \mathbb{F}_q^\times} \sum_{y \in S} T^i(x^{-1})[x + y] \\
&= \sum_{x \in \mathbb{F}_q^\times} \sum_{y \in \mathbb{F}_q} \chi_S(y) T^i(x^{-1})[x + y]
\end{aligned}$$

# Jacobi Sums

## Definition

Let $\theta$ and $\psi$ be multiplicative characters of $\mathbb{F}_q^\times$ taking values in $R^\times$. The *Jacobi sum* is

$$J(\theta, \psi) = \sum_{x \in \mathbb{F}_q} \theta(x)\psi(1 - x).$$

(At $x = 0$, nonprinc. chars take value 0, princ. char takes value 1.)

$$\begin{aligned}
\mu_A(e_i) &= \sum_{x \in \mathbb{F}_q^\times} \sum_{y \in S} T^i(x^{-1})[x + y] \\
&= \sum_{x \in \mathbb{F}_q^\times} \sum_{y \in \mathbb{F}_q} \chi_S(y) T^i(x^{-1})[x + y] \\
&= \sum_{z \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q^\times} \chi_S(z - x) T^i(x^{-1})[z].
\end{aligned}$$

# Notation

- Recall $r = \frac{(p^2-1)}{4}$.
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- Write $J(T^{-i}, T^{-j})$ as $J(i,j)$ for short.

# Notation

- Recall $r = \frac{(p^2-1)}{4}$.
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- Write $J(T^{-i}, T^{-j})$ as $J(i, j)$ for short.

# Notation

- Recall $r = \frac{(p^2-1)}{4}$.
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- Write $J(T^{-i}, T^{-j})$ as $J(i, j)$ for short.

The matrix of $\mu_K$ on $M_i$ is

$$K_i = \begin{bmatrix} 0 & J(i{+}2r{,}2r) & 0 & 0 \\ J(i{,}2r) & 0 & 0 & 0 \\ 0 & 0 & 0 & J(i{+}3r{,}2r) \\ 0 & 0 & J(i{+}r{,}2r) & 0 \end{bmatrix}$$

The matrix of $\mu_{K'}$ on $M_i$ is

$$K_i' \begin{bmatrix} 0 & 0 & \alpha J(i{+}r{,}3r) & \overline{\alpha} J(i{+}3r{,}r) \\ 0 & 0 & \overline{\alpha} J(i{+}r{,}r) & \alpha J(i{+}3r{,}3r) \\ \overline{\alpha} J(i{,}r) & \alpha J(i{+}2r{,}3r) & 0 & 0 \\ \alpha J(i{,}3r) & \overline{\alpha} J(i{+}2r{,}r) & 0 & 0 \end{bmatrix}$$

The matrix of $\mu_K$ on $M_0$ is

$$K_0' \begin{bmatrix} q & 1 & -1 & 0 & 0 \\ 0 & 0 & q & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & J(3r, 2r) \\ 0 & 0 & 0 & J(r, 2r) & 0 \end{bmatrix}$$

The matrix $\mu_{K'}$ on $M_0$ is

$$K_0' \begin{bmatrix} q & 1 & -\alpha & 0 & -\overline{\alpha} \\ 0 & 0 & q\alpha & 0 & q\overline{\alpha} \\ 0 & \overline{\alpha} & 0 & \alpha J(2r, 3r) & 0 \\ 0 & 0 & \overline{\alpha} J(r, r) & 0 & \alpha J(3r, 3r) \\ 0 & \alpha & 0 & \overline{\alpha} J(2r, r) & 0 \end{bmatrix}$$

# Outline of proof of $R$-similarity of $K_i$ and $K_i'$

Proof of similarity of $K_i'$ with $K_i$ involves finding a new basis.

The definition of the new basis is not uniform for all i but depends on the $p$-adic valuations of the Jacobi sums appearing in these matrices.

By close examination of Jacobi sums, we can reduce to just three cases, corresponding to whether $K_i$ has $p$-rank 1, 2, or 3.

# Outline of proof of $R$-similarity of $K_i$ and $K_i'$

Proof of similarity of $K_i'$ with $K_i$ involves finding a new basis.

The definition of the new basis is not uniform for all i but depends on the $p$-adic valuations of the Jacobi sums appearing in these matrices.

By close examination of Jacobi sums, we can reduce to just three cases, corresponding to whether $K_i$ has $p$-rank 1, 2, or 3.

# Outline of proof of $R$-similarity of $K_i$ and $K_i'$

Proof of similarity of $K_i'$ with $K_i$ involves finding a new basis.

The definition of the new basis is not uniform for all i but depends on the $p$-adic valuations of the Jacobi sums appearing in these matrices.

By close examination of Jacobi sums, we can reduce to just three cases, corresponding to whether $K_i$ has $p$-rank 1, 2, or 3.

# $p$-adic valuation of Jacobi Sums

Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(p^2-1)}$.

$p$-digit expresssion: $j = a_0 + a_1 p$, $0 \le a_i \le p-1$.

Set $s(j) = a_0 + a_1$.

$r = \frac{p^2-1}{4} = \frac{3p-1}{4} + \frac{p-3}{4}p$.

$3r = \frac{p^2-1}{4} = \frac{p-3}{4} + \frac{3p-1}{4}p$.

$s(r) = s(3r) = p-1$.

# $p$-adic valuation of Jacobi Sums

Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(p^2-1)}$.

$p$-digit expresssion: $j = a_0 + a_1 p$, $0 \leq a_i \leq p-1$.

Set $s(j) = a_0 + a_1$.

$r = \frac{p^2-1}{4} = \frac{3p-1}{4} + \frac{p-3}{4} p$.

$3r = \frac{p^2-1}{4} = \frac{p-3}{4} + \frac{3p-1}{4} p$.

$s(r) = s(3r) = p - 1$.

# $p$-adic valuation of Jacobi Sums

Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(p^2-1)}$.

$p$-digit expresssion: $j = a_0 + a_1 p$, $0 \leq a_i \leq p-1$.

Set $s(j) = a_0 + a_1$.

$r = \frac{p^2-1}{4} = \frac{3p-1}{4} + \frac{p-3}{4}p$.

$3r = \frac{p^2-1}{4} = \frac{p-3}{4} + \frac{3p-1}{4}p$.

$s(r) = s(3r) = p-1$.

# $p$-adic valuation of Jacobi Sums

Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(p^2-1)}$.

$p$-digit expresssion: $j = a_0 + a_1 p$, $0 \leq a_i \leq p-1$.

Set $s(j) = a_0 + a_1$.

$r = \frac{p^2-1}{4} = \frac{3p-1}{4} + \frac{p-3}{4}p$.

$3r = \frac{p^2-1}{4} = \frac{p-3}{4} + \frac{3p-1}{4}p$.

$s(r) = s(3r) = p-1$.

# $p$-adic valuation of Jacobi Sums

Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(p^2-1)}$.

$p$-digit expresssion: $j = a_0 + a_1 p$, $0 \le a_i \le p-1$.

Set $s(j) = a_0 + a_1$.

$r = \frac{p^2-1}{4} = \frac{3p-1}{4} + \frac{p-3}{4}p$.

$3r = \frac{p^2-1}{4} = \frac{p-3}{4} + \frac{3p-1}{4}p$.

$s(r) = s(3r) = p-1$.

# $p$-adic valuation of Jacobi Sums

Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(p^2-1)}$.

$p$-digit expresssion: $j = a_0 + a_1 p$, $0 \leq a_i \leq p-1$.

Set $s(j) = a_0 + a_1$.

$r = \frac{p^2-1}{4} = \frac{3p-1}{4} + \frac{p-3}{4}p$.

$3r = \frac{p^2-1}{4} = \frac{p-3}{4} + \frac{3p-1}{4}p$.

$s(r) = s(3r) = p-1$.

# More on Jacobi sums

By Stickelberger's Theorem and relation between Gauss sums and Jacobi sums, we know that when $i$, $j$ and $i+j$ are not divisible by $p^2-1$ the $p$-adic valuation of $J(i,j)$ is equal to

$$c(i,j) := \frac{1}{p-1}(s(i)+s(j)-s(i+j)),$$

This valuation can be viewed as the number of carries, when adding the $p$-expansions of $i$ and $k$, modulo $p^2-1$.

Finally, we also need the exact values (Berndt-Evans (1979))

$$J(r,r) = J(r,2r) = J(3r,2r) = J(3r,3r) = p.$$

# More on Jacobi sums

By Stickelberger's Theorem and relation between Gauss sums and Jacobi sums, we know that when $i$, $j$ and $i+j$ are not divisible by $p^2-1$ the $p$-adic valuation of $J(i,j)$ is equal to

$$c(i,j) := \frac{1}{p-1}(s(i)+s(j)-s(i+j)),$$

This valuation can be viewed as the number of carries, when adding the $p$-expansions of $i$ and $k$, modulo $p^2-1$.

Finally, we also need the exact values (Berndt-Evans (1979))

$$J(r,r) = J(r,2r) = J(3r,2r) = J(3r,3r) = p.$$

# More on Jacobi sums

By Stickelberger's Theorem and relation between Gauss sums and Jacobi sums, we know that when $i$, $j$ and $i+j$ are not divisible by $p^2-1$ the $p$-adic valuation of $J(i,j)$ is equal to

$$c(i,j) := \frac{1}{p-1}(s(i)+s(j)-s(i+j)),$$

This valuation can be viewed as the number of carries, when adding the $p$-expansions of $i$ and $k$, modulo $p^2-1$.

Finally, we also need the exact values (Berndt-Evans (1979))

$$J(r,r) = J(r,2r) = J(3r,2r) = J(3r,3r) = p.$$

# Concluding remarks

For all primes $\ell$, $A(q)$ is similar to $A'(q)$ over $\mathbb{Z}_{(\ell)}$.

For all integers $a$,$b$,$c$ the generalized adjacency matrices $aA(q) + bI + cJ$ and $aA'(q) + bI + cJ$ are cospectral and equivalent.

For which values of $q$ are they are similar over $\mathbb{Z}$?

# Concluding remarks

For all primes $\ell$, $A(q)$ is similar to $A'(q)$ over $\mathbb{Z}_{(\ell)}$.

For all integers $a,b,c$ the generalized adjacency matrices $aA(q) + bI + cJ$ and $aA'(q) + bI + cJ$ are cospectral and equivalent.

For which values of $q$ are they are similar over $\mathbb{Z}$?

# Concluding remarks

For all primes $\ell$, $A(q)$ is similar to $A'(q)$ over $\mathbb{Z}_{(\ell)}$.

For all integers $a$,$b$,$c$ the generalized adjacency matrices $aA(q) + bI + cJ$ and $aA'(q) + bI + cJ$ are cospectral and equivalent.

For which values of $q$ are they are similar over $\mathbb{Z}$?

Thank you for your attention!