A DECOMPOSITION THEOREM FOR CAYLEY GRAPHS OF PICARD GROUP QUOTIENTS

DOMINIC LANPHIER AND JASON ROSENHOUSE

ABSTRACT. The Picard group is defined as $\Gamma = SL(2, \mathbf{Z}[i])$; the ring of 2×2 matrices with Gaussian integer entries and determinant one. We consider certain graphs associated to quotients $\Gamma/\Gamma(p)$ where p is a prime congruent to three mod four and $\Gamma(p)$ is the congruence subgroup of level p. We prove a decomposition theorem on the vertices of these graphs, and use this decomposition to derive upper and lower bounds on their isoperimetric numbers.

1. INTRODUCTION

The Picard group $\Gamma = SL(2, \mathbb{Z}[i])$ is the group of two-by-two matrices with Gaussian integer entries and determinant one. This group acts on hyperbolic three-space $\mathbb{H}^3$ via fractional linear transformations. The center of this action is given by $\langle \pm 1 \rangle$, and we define $PSL(2, \mathbb{Z}[i]) = SL(2, \mathbb{Z}[i])/\langle \pm 1 \rangle$. In the following we will make no distinction between a matrix and the two-element coset it represents.

It is shown in [4] that $PSL(2, \mathbb{Z}[i])$ is generated by

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, d = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

This leads to the well-known presentation (as shown in [4])

$$PSL(2, \mathbb{Z}[i]) \cong \langle a, b, c, d \mid a^2 = d^2 = (ad)^2 = (bad)^2 = (cad)^2 = (cd)^3 = (ab)^3 = bcb^{-1}c^{-1} = 1 \rangle.$$

JCMCC **50** (2004), pp. 95-104

For a prime $p \equiv 3 \pmod 4$ we define the congruence subgroup of level p, denoted by $\Gamma(p)$ by

$$\Gamma(p) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma \;\middle|\; \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod p \right\}.$$

We note that if $p \equiv 1 \pmod 4$ then -1 is a square mod p. Consequently, the group $PSL(2, \mathbb{Z}_p[i])$ reduces to $PSL(2, \mathbb{Z}_p)$ in this case.

Let $\widetilde{\Gamma}$ be a finite group and let Ω be a symmetric generating set for $\widetilde{\Gamma}$. Then the Cayley graph of $\widetilde{\Gamma}$ with respect to Ω is the graph with vertex set $\widetilde{\Gamma}$, with group elements g_1 and g_2 connected by an edge if $g_1 = \omega g_2$ for some $\omega \in \Omega$. Cayley graphs of $PSL(2, \mathbb{Z}_p)$ have been the subject of much research. For example, in [1],[2] and [5] Cayley graphs of $PSL(2, \mathbb{Z}_p)$ are constructed whose isoperimetric numbers are related to the Cheeger constants of the fundamental domain of the action of $PSL(2, \mathbb{Z}_p)$ on the complex upper half plane. The work presented here can be viewed as an extension of that research. As in [1], the isoperimetric numbers computed here should be related to the Cheeger constants of the fundamental domain $\Gamma(p)\backslash\mathbb{H}^3$. Also observe that since $\Gamma(p)$ is the kernel of the reduction homomorphism from Γ to $PSL(2, Z_p[i])$ we have that $\Gamma(p)$ is a normal subgroup of Γ. It is easily shown that this homomorphism is onto, leading to the well-known formula (see [7] for a proof)

$$|\Gamma : \Gamma(p)| = |SL(2, \mathbb{Z}_p[i])| = \frac{p^6}{2}\left(1 - \frac{1}{p^4}\right)$$

where p is a prime congruent to 3 mod 4. For such primes, we have that -1 is not a square mod p and we define the group $\Gamma_p = PSL(2, \mathbb{Z}_p[i])$. The set $\Omega = \{a, b, b^{-1}, c, c^{-1}, d\}$ is easily seen to be a symmetric generating set for Γ_p. Let G_p denote the Cayley graph of Γ_p with respect to Ω.

Denote by N the following subgroup of Γ_p:

$$N = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Set $\Gamma'_p = N\backslash\Gamma_p$. Observe that if g is any matrix element in Γ_p, then left multiplication by elements of N does not change the bottom row of g. It follows that elements of Γ'_p can be indexed by ordered pairs representing the bottom rows of matrices. Specifically:

$$\Gamma'_p \cong \{(\alpha,\beta) \mid \alpha,\beta \in \mathbb{Z}_p[i],\ (\alpha,\beta) \not\equiv (0,0) \pmod p\}/\langle\pm 1\rangle.$$

Finally, we let G'_p denote the quotient graph $N\backslash G_p$ (i.e. The multigraph whose vertices are given by the cosets of Γ'_p, with distinct cosets $\gamma_1 N$ and $\gamma_2 N$ joined by as many edges as there are edges in G_p of the form (v_1, v_2), where $v_1 \in \gamma_1 N$ and $v_2 \in \gamma_2 N$). We note that Γ'_p is not a group. Therefore, the quotient graphs G'_p are not themselves Cayley graphs. They are, however, induced from the Cayley graphs G_p.

The goal of this paper is to prove a decomposition theorem on the vertices of the quotient graph G'_p. We will then use this decomposition to derive upper and lower bounds on the isoperimetric numbers of these graphs. As a corollary we will prove an upper bound on the isoperimetric number of the graphs G_p.

The isoperimetric number finds many applications in combinatorics, due to its close relationship to the eigenvalue spectrum of the graph. Also, as a measure of the connectedness of the graph, it aids in an analysis of the graph's expansion properties. More on these applications can be found in [3] and [6].

The authors thank the referees for a careful reading of the paper, and for clarifications and corrections which greatly improved the exposition.

2. The Decomposition Theorem

Lemma 1. *The vertices (α,β) and (γ,δ) in G'_p are adjacent if and only if*

$$\det\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \equiv \pm 1, \pm i \pmod p.$$

Proof. We have already noted that if $g \in \Gamma_p$ then left multiplication of g by elements of N preserves the bottom row of Γ_p. Therefore, $g' \in G'_p$ is adjacent to precisely those elements attainable from it by left action (multiplication) by $\xi \in \Omega$, with $\xi \notin N$. Observe that left multiplication by $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ multiplies the bottom row by -1 and then reverses the rows. Left multiplication by $d = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ reverses the rows and multiplies both by i. Specifically, if $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_p$ with $\alpha\delta - \beta\gamma \equiv 1 \pmod{p}$ and $\xi g = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$, then $(\gamma', \delta') = -(\alpha, \beta)$ or $(\gamma', \delta') = i(\alpha, \beta)$. It follows that we must have

$$\det \begin{pmatrix} \gamma & \delta \\ \gamma' & \delta' \end{pmatrix} \equiv \pm 1, \pm i \pmod{p}.$$

For the converse, note that if $\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \pm 1, \pm i \pmod{p}$ then we have $\begin{pmatrix} \epsilon\alpha & \epsilon\beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_p$ for some $\epsilon \in \{\pm 1, \pm i\}$. So multiplication by a or d takes (γ, δ) to (α, β) in Γ'_p, and so these are adjacent in G'_p. The proof is complete. □

We now observe that the graph G_p, with $p \neq 2$, is six-regular. Further, N is abelian and is easily seen to satisfy $|N| = p^2$. It follows that $|V(G'_p)| = \frac{p^4}{2}(1 - \frac{1}{p^4})$. Of the six edges incident with an arbitrary vertex $g \in G_p$, four of them arise from multiplication by elements of N, with the remaining two elements coming from elements of the cosets xN, yN, with $x, y \notin N$. Next, observe that any vertex in the quotient graph G'_p will correspond to p^2 vertices in G_p. It follows that G'_p is $2p^2$-regular and $|E(G'_p)| = \frac{p^6}{2}(1 - \frac{1}{p^4})$.

We make the following definition:

Definition 1. *Let $\alpha \in \mathbb{Z}_p[i] - \{0\}$. We define the set $V(\alpha) \subset V(G'_p)$ by*

$$V(\alpha) = \left\{(0, \alpha), (0, i\alpha), (\alpha^{-1}, \beta), (i\alpha^{-1}, \beta) \ : \ \beta \in \mathbb{Z}_p[i]\right\}.$$

Then we let $H(\alpha)$ denote the induced subgraph of G'_p on the vertices of $V(\alpha)$. We will refer to the vertices $\{(0,\alpha),(0,i\alpha)\}$ as the center of $H(\alpha)$ and the remaining vertices in $H(\alpha)$ as the crown of $H(\alpha)$.

It is easily seen that there are two vertices in the center of $H(\alpha)$ and $2p^2$ vertices in the crown. Our main theorem is a decomposition of G'_p. Specifically:

Theorem 2.2.1. *Let p be a prime satisfying $p \equiv 3 \pmod 4$. The vertices of G'_p can be partitioned into $\frac{p^2-1}{4}$ sets such that the subgraph of G'_p induced by each set is isomorphic to $H(\alpha)$, for some $\alpha \in \mathbb{Z}_p[i] - \{0\}$. If $\delta \notin \{\pm\alpha, \pm i\alpha\}$, then there are $16p^2$ edges connecting vertices in $H(\alpha)$ to vertices in $H(\delta)$. Alternatively, if G''_p denotes the multigraph obtained from G'_p by contracting each $H(\alpha)$ to a single vertex, then $G''_p \cong K^{16p^2}_{\frac{p^2-1}{4}}$, the complete multigraph on $\frac{p^2-1}{4}$ vertices, with $16p^2$ edges adjoining each pair of vertices.*

Proof. It is easily seen that $H(\alpha) \cap H(\delta) = \emptyset$ for $\delta \notin \{\alpha, -\alpha, i\alpha, -i\alpha\}$, and $H(\alpha) = H(\delta)$ otherwise. Any vertex $v \in G'_p$ lies in $V(\alpha)$ for some $\alpha \in \mathbb{Z}_p[i] - \{0\}$. So $V(G'_p)$ can be partitioned by the vertex sets of the $H(\alpha)$'s. That is,

$$V(G'_p) = \bigsqcup V(H(\alpha))$$

where the union is over the distinct $H(\alpha)$'s.

Next, recall that

$$|G'_p| = \frac{|G_p|}{p^2} = \frac{p^4-1}{2}.$$

Since $|H(\alpha)| = 2p^2+2$, we have

$$\frac{|G'_p|}{|H(\alpha)|} = \frac{p^2-1}{4}$$

many copies of $H(\alpha)$.

By Lemma 1, the vertices $(0, \alpha)$ and $(0, i\alpha)$ are adjacent to all vertices of the form (α^{-1}, β) or $(i\alpha^{-1}, \beta)$, where $\beta \in \mathbb{Z}_p[i]$. Since there are $2p^2$ such vertices and G'_p is $2p^2$ regular, we have accounted for all vertices adjacent to the center of $H(\alpha)$. It follows that vertices in the center of $H(\alpha)$ are adjacent only to vertices in the crown of $H(\alpha)$.

Now consider the vertices (α^{-1}, β) and $(i\alpha^{-1}, \beta)$. Each of these is adjacent to the vertices in the center of $H(\alpha)$, which accounts for two of their edges. Within the crown of a given $H(\alpha)$, we find that these vertices are also adjacent to each of the vertices

$$\left\{(i\alpha^{-1}, i\beta \pm \alpha), (i\alpha^{-1}, i\beta \pm i\alpha), (\alpha^{-1}, \beta \pm \alpha), (\alpha^{-1}, \beta \pm i\alpha)\right\}.$$

Therefore, each vertex in the crown of $H(\alpha)$ is adjacent to eight other vertices in the crown. It follows that

$$|E(H(\alpha))| = \frac{1}{2}(8)(2p^2) + 2(2p^2) = 12p^2.$$

By Lemma 1, we see that for $H(\alpha) \neq H(\gamma)$ the vertex (α^{-1}, β) in the crown of $H(\alpha)$ is adjacent to (γ^{-1}, x) in the crown of $H(\gamma)$ if and only if

$$\det \begin{pmatrix} \alpha^{-1} & \beta \\ \gamma^{-1} & x \end{pmatrix} \equiv \pm 1, \pm i \pmod{p}.$$

The number of solutions to this congruence is independent of the choice of γ. Similarly, (α^{-1}, β) will be adjacent to vertices of the form $(i\gamma^{-1}, x)$ provided

$$\det \begin{pmatrix} \alpha^{-1} & \beta \\ i\gamma^{-1} & x \end{pmatrix} \equiv \pm 1, \pm i \pmod{p},$$

and the number of solutions to this congruence is also independent of the choice of γ. It follows that the number of edges connecting vertices in $H(\alpha)$ to vertices in $H(\gamma)$ is independent of the choice of α and γ.

It only remains to determine the number of edges joining $H(\alpha)$ and $H(\gamma)$. Since for a given α we have that $H(\alpha)$ contains $12p^2$ edges, and since there

are $\frac{p^2-1}{4}$ isomorphic copies of $H(\alpha)$ in G'_p, we have $3p^2(p^2-1)$ edges joining pairs of vertices within the $\frac{p^2-1}{4}$ copies of $H(\alpha)$.

Also, since $|V(G'_p)| = \frac{p^4-1}{2}$ and since G'_p is $2p^2$-regular, we have $|E(G'_p)| = \frac{p^2(p^4-1)}{2}$. It follows that there are

$$\frac{p^2(p^4-1)}{2} - 3p^2(p^2-1) = \frac{1}{2}p^2(p^2-1)(p^2-5)$$

edges joining vertices in different $H(\alpha)$'s. Finally, since the number of edges joining $H(\alpha)$ to $H(\gamma)$ is independent of our choice of α and γ, and since there are $\binom{\frac{p^2-1}{4}}{2}$ choices for the ordered pair (α, γ) that give distinct $H(\alpha)$ and $H(\gamma)$, we conclude that the number of edges joining $H(\alpha)$ to $H(\gamma)$ is given by

$$\frac{\frac{1}{2}p^2(p^2-1)(p^2-5)}{\binom{\frac{p^2-1}{4}}{2}} = 16p^2$$

as was to be shown. □

3. The Isoperimetric Number of G_p

Let G be an arbitrary graph and let $S \subset V(G)$. Then the boundary of S, denoted by ∂S, is the set of all edges having precisely one endpoint in S. The isoperimetric number of G, denoted by $\mathrm{iso}(G)$, is then defined by

$$\mathrm{iso}(G) = \inf_S \frac{|\partial S|}{|S|},$$

where the infimum is taken over all subsets $S \subset V(G)$ satisfying $|S| \leq \frac{1}{2}|V(G)|$. A set S such that $\mathrm{iso}(G) = \frac{|\partial S|}{|S|}$ is called an isoperimetric set for G.

Our decomposition makes it possible to derive upper and lower bounds on $\mathrm{iso}(G'_p)$. Also, since each vertex in G'_p represents p^2 vertices in G_p, we have $p^2(\mathrm{iso}(G_p)) \leq \mathrm{iso}(G'_p)$. Thus, our decomposition permits us to derive an upper bound on the isoperimetric number of G_p.

First we need the following lemma (which we model after a similar result in [1]):

Lemma 2. *Given distinct vertices* $(\alpha, \beta), (\alpha', \beta') \in G'_p$ *with*

$$\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix} \neq 0,$$

there are exactly eight paths of length two joining (α, β) *to* (α', β').

Proof. ¿From Lemma 1, a path of length two joining (α, β) to (α', β') is given by a vector (γ, δ) such that

$$\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \pm 1, \pm i \pmod{p} \text{ and } \det \begin{pmatrix} \gamma & \delta \\ \alpha' & \beta' \end{pmatrix} \equiv \pm 1, \pm i \pmod{p}.$$

Since we are assuming $\alpha\beta' - \alpha'\beta = \omega \neq 0$, we have that (α, β) and (α', β'), are linearly independent in $\mathbb{C}^2$. It follows that we can find nonzero constants k_1, k_2 such that

$$(\gamma, \delta) = k_1(\alpha, \beta) + k_2(\alpha', \beta').$$

Calculating determinants we find

$$\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = k_2 \cdot \det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix} = k_2\omega,$$

and

$$\det \begin{pmatrix} \gamma & \delta \\ \alpha' & \beta' \end{pmatrix} = k_1 \cdot \det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix} = k_1\omega.$$

This leads to sixteen ordered pairs (k_1, k_2) for which the vector (γ, δ) has the required properties. Since vectors differing only by a factor of -1 are identical, these sixteen pairs represent eight distinct paths in G'_p. □

Theorem 3.3.1. *For the graphs* G'_p *we have*

$$\frac{(p^2-1)(p^2-3)}{2p^2-1} \leq \text{iso}(G'_p) \leq \frac{p^2(p^2-1)}{p^2+1}.$$

Proof. Let n be even and let K_n denote the complete graph on n vertices. Then any set S containing $\frac{n}{2}$ vertices will be an isoperimetric set for K_n. It is a simple calculation to show that $|\partial S| = \frac{n^2}{4}$ in this case.

Since $\frac{p^2-1}{4}$ is even we can apply this result in our case. As our set S we select any $\frac{p^2-1}{8}$ copies of $H(\alpha)$. Then we compute

$$|S| = (2p^2+2)\left(\frac{p^2-1}{8}\right) \text{ and } |\partial S| = 16p^2\left(\frac{\left(\frac{p^2-1}{4}\right)^2}{4}\right) = \frac{p^2(p^2-1)^2}{4}.$$

From this it follows that

$$\text{iso}(G'_p) \leq \frac{|\partial S|}{|S|} = \frac{\frac{p^2(p^2-1)^2}{4}}{(2p^2+2)\left(\frac{p^2-1}{8}\right)} = \frac{p^2(p^2-1)}{p^2+1}$$

as claimed.

For the lower bound we observe that if (α, β) is a vertex in G'_p and (α', β') is some other vertex that is not a multiple of (α, β), then Lemma 2 states that there are eight paths of length two joining them.

Partitioning the vertices of G'_p into sets S_1 and S_2 with $|S_1| \leq |S_2|$, it follows that at least one edge from each of these paths must be cut for every pair of vertices $v_1 \in S_1$ and $v_2 \in S_2$, where v_1 and v_2 are not multiples of each other. We also observe that for any vertex $v \in G'_p$ there are p^2-1 nonzero multiples of v in $\mathbb{Z}_p[i]$. Therefore the number of such pairs v_1, v_2 is at least $|S_1|(|S_2| - p^2 + 1)$. Finally, since G'_p is $2p^2$-regular, we note that each edge can lie in no more than $2(2p^2-1) = 4p^2-2$ different paths of length two. It follows that

$$|\partial S_1| \geq \frac{8|S_1|\left(|S_2| - p^2 + 1\right)}{4p^2-2},$$

and therefore, since $|S_2| \geq \frac{p^4-1}{4}$,

$$\frac{|\partial S_1|}{|S_1|} \geq \frac{8(|S_2| - p^2 + 1)}{4p^2-2} \geq \frac{(p^2-1)(p^2-3)}{2p^2-1}$$

as claimed. □

We then have the simple corollary

Corollary 1. *We have* $\mathrm{iso}(G_p) \leq \dfrac{p^2-1}{p^2+1}$.

Proof. This follows immediately from the previous theorem and the observation that $p^2(\mathrm{iso}(G_p)) \leq \mathrm{iso}(G'_p)$. □

References

[1] Brooks, R., Perry, P. and Petersen, P., "On Cheeger's inequality", *Comment. Math Helvetici*, Vol. 68 (1993), pp. 599-621.

[2] Brooks, R. and Zuk, A., "On the asymptotic isoperimetric constants for Riemann surfaces and graphs", J. Differential Geom., Vol. 62 (2002), pp. 49-78.

[3] Chung, F. R. K., *Spectral Graph Theory*, No. 92 in the Regional Conference Series in Mathematics, American Mathematical Society, Providence, RI, 1991.

[4] Fine, B., *Algebraic Theory of the Bianchi Groups*, Marcel Dekker, Inc., New York, 1989, pp. 115.

[5] Lanphier, D. and Rosenhouse, J., "Cheeger Constants of Platonic Graphs", to appear in *Discrete Math.*

[6] Mohar, B., "Isoperimetric numbers of graphs", *J. of Comb. Theory (B)*, Vol. 47 (1989), pp. 274-291.

[7] Newman, M., *Integral Matrices*, Pure and Applied Mathematics Vol. 45, Academic Press, New York-London, 1972.

Department of Mathematics, Kansas State University, 138 Cardwell Hall, Manhattan, KS 66506

E-mail address: lanphier@math.ksu.edu

Department of Mathematics and Statistics, James Madison University, 104 Burruss Hall, Harrisonburg, VA 22807

E-mail address: rosenhjd@jmu.edu