CALCULATING THE IHARA-ZETA FUNCTION FOR $PSL(2, \mathbb{Z}_{2^n})$

CASEY GREEN, ELIZABETH WICKS AND STRATOS PRASSIDIS

Abstract. We are interested in calculating the Ihara-Zeta Function (IZF) for $PSL(2, \mathbb{Z})$. Our first approach to this problem was to compute the IZF for $PSL(2, \mathbb{Z})/\Gamma_{2^n}$ for small n, find a formula to obtain the IZF for all n, and take the limit as $n \to \infty$. It is a fact that $PSL(2, \mathbb{Z})/\Gamma_{2^n} \cong PSL(2, \mathbb{Z}_{2^n})$, where $\Gamma_{2^n} = ker(PSL(2, \mathbb{Z}) \to PSL(2, \mathbb{Z}_{2^n}))$. Hence, we calculated the IZF for $PSL(2, \mathbb{Z}_{2^n})$ instead. As we went through this process, we were unable to come up with a concrete formula for the IZF for $PSL(2, \mathbb{Z})$. However, we developed an algorithm for calculating the IZF for $PSL(2, \mathbb{Z}_{2^n})$. Calculating the function in this manner necessitates a computer with high computational capabilities, but it can be done for any n. In this paper, we will describe our algorithm and prove that it works for all n.

1. Preliminaries

Let $p : V(G \times^{\phi} \hat{\Gamma}_{2^n}) \to V(G)$ be a regular covering, where $V(G)$ are the vertices of a graph G. Here, we will take our base graph G to be the Cayley graph of $PSL(2, \mathbb{Z}_2)$ and our covering graph $G \times^{\phi} \hat{\Gamma}_{2^n}$ to be the Cayley graph of $PSL(2, \mathbb{Z}_{2^n})$. Then $\hat{\Gamma}_{2^n} = \langle \phi(e) | e \in E(\vec{G}) \rangle$ is the group generated by the voltage assignments $\phi(e)$, where $E(\vec{G})$ are the directed edges of G and $\phi(e) \in Aut(G)$. The voltage assignment $\phi(e)$ satisfies the property that $\phi(e)^{-1} = \phi(e^{-1})$. Voltage assignments are defined for a particular lifting of $V(G)$ onto $V(G \times^{\phi} \hat{\Gamma}_{2^n})$. Here G has 6 vertices. To choose a lifting, pick 6 elements in $PSL(2, \mathbb{Z}_{2^n})$ that become the 6 elements of $PSL(2, \mathbb{Z}_2)$ under arithmetic modulo 2. Let u and v be the vertices that $p(u)$ and $p(v)$ were lifted to. Then for an edge $e = uv$ connecting $u, v \in V(G \times^{\phi} \hat{\Gamma}_{2^n})$, if $p(u) \sim p(v) \Rightarrow u \sim v$ then $\phi(uv) = I$, the identity automorphism. Now suppose $p(u) \sim p(v) \Rightarrow u \not\sim v$. Since a covering implies a bijective function from $N(u) \to N(p(u))$, there must exist $x \in N(u)$ such that $p(x) = p(v)$. By the regularity of the covering, $\exists \gamma \in Aut(G)$ such that $\gamma x = v$. This γ is our $\phi(uv)$. In our case, all $\phi(e)$ are 2×2 matrices that send elements from $PSL(2, \mathbb{Z}_{2^n})$ to the elements in $PSL(2, \mathbb{Z}_{2^n})$ that become the same matrix under arithmetic modulo 2.

2. Description of Our Algorithm

We will refer to the six elements of $PSL(2, \mathbb{Z}_2)$ as follows:

$$\left\{ \mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{2} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \mathbf{3} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \ \mathbf{4} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ \mathbf{5} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \ \mathbf{6} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

University of Rochester, Rochester, NY & University of Washington, Seattle, WA & Canisius College, Buffalo, NY
REU sponsored by the NSF.

We will use the following generating set for $PSL(2,\mathbb{Z})$:

$$S = \left\{ S_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, S_2 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, S_3 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \right\}.$$

First, we noticed that three of the elements in $PSL(2,\mathbb{Z}_2)$ always appear in the cover $PSL(2,\mathbb{Z}_{2^n})$ for all n, so those elements can be lifted to themselves. Those elements are **1**, **2**, and **4**. This is because $det(\mathbf{1}) = det(\mathbf{2}) = det(\mathbf{4}) = 1$, and $PSL(2,\mathbb{Z}_{2^n})$ contains all 2×2 matrices J with $det(J) \equiv 1 \bmod 2^n$.

Next, the other three elements of $PSL(2,\mathbb{Z}_2)$ can be mapped to our chosen generators of $PSL(2,\mathbb{Z}_{2^n})$ for all n. These liftings were obtained by multiplying $\mathbf{1}, \mathbf{2}$, and $\mathbf{4}$ by the special generator S_1. Thus, $\mathbf{3} \to S_3$, $\mathbf{5} \to S_2$, and $\mathbf{6} \to S_1$. This can be done for all n because $-1 \equiv (2^n - 1) \bmod 2^n$, so the generators can be written with the -1 entries replaced by $2^n - 1$. It is a fact that $(2^n - 1) \equiv 1 \bmod 2$, so the generators under arithmetic modulo 2 become **3**, **5**, and **6** as desired.

3. Generating $\hat{\Gamma}_{2^n}$ with this Lifting

We have modified the following theorem to use for our purposes. This theorem gives the adjacency matrix for a graph $G \times^{\phi} \hat{\Gamma}_{2^n}$ that covers a base graph G. The general theorem and proof is available on page 2 of [1].

Theorem 1. $A(G \times^{\phi} \hat{\Gamma}_{2^n}) = \sum_{\gamma \in \hat{\Gamma}_{2^n}} A(\vec{G}_{(\phi,\gamma)}) \otimes P(\gamma)$, *where* $P(\gamma)_{ij} = \begin{cases} 1, & if\ j = \gamma i \\ 0, & otherwise \end{cases}$.

For a particular $\gamma \in \hat{\Gamma}_{2^n}$, $\vec{G}_{(\phi,\gamma)}$ is the spanning subgraph of $\vec{G}$ consisting of all the vertices of G and the directed edges with voltage assignment γ. The tensor product $A \otimes B$ is defined as the matrix B with the element b_{ij} replaced by the matrix Ab_{ij}.

In order to find $\hat{\Gamma}_{2^n}$, it is necessary to draw a partial Cayley graph of $PSL(2,\mathbb{Z}_{2^n})$ to find the voltage assignments for the 6 vertices of the lifting.

Proposition 2. *Using our lifting, we will always obtain the same partial Cayley graph, which is shown in Figure 1.*

Proof. It is easy to show by matrix multiplication that the adjacencies in the graph hold for any n, because our method of lifting is independent of n. □

Proposition 3. *From this partial Cayley graph and the labeling of $Cay(PSL(2,\mathbb{Z}_2),S)$ in Figure 2,*

$$\hat{\Gamma}_{2^n} = \left\langle \phi(e_4^{-1}) = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix},\ \phi(e_4) = \begin{pmatrix} -3 & 2 \\ -2 & 1 \end{pmatrix},\ \phi(e_5^{-1}) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\right.$$

$$\left. \phi(e_5) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix},\ \phi(e_6^{-1}) = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix},\ \phi(e_6) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle,$$

and

$$\phi(e_m) = \phi(e_m^{-1}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \forall m \in \{1,2,3,7,8,9\}.$$

Proof. We will show two examples of finding $\phi(e)$, which is independent of n. The rest of the proof is left to the reader. In Figures 1 and 2, the colors represent which vertices correspond to each other under the lifting. Solid colors in Fig. 1 represent the actual lifting ($\mathbf{1} \to \mathbf{1}$, $\mathbf{2} \to \mathbf{2}$, $\mathbf{3} \to S_3$, $\mathbf{4} \to \mathbf{4}$, $\mathbf{5} \to S_2$, and $\mathbf{6} \to S_1$). Vertices with a border in Fig. 1 become the vertex in Fig. 2 of the same color under arithmetic modulo 2, but are not part of the lifting. This means that two vertices with the same color are equivalent modulo 2, since we are using the Cayley graph of $PSL(2,\mathbb{Z}_2)$ as our base graph.

In order to find $\phi(e_2)$, where e_2 is the edge from $\mathbf{3} \to \mathbf{5}$ in Fig. 2, one must examine the lifting of $\mathbf{3}$ and $\mathbf{5}$. We know that $\mathbf{3} \to S_3$ and $\mathbf{5} \to S_2$. Because $S_3 \sim S_2$ in Fig. 1, $\phi(e_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Going through this process for $\phi(e_m), \forall m \in \{1,2,3,7,8,9\}$ reveals that $\phi(e_m)$ is the identity matrix. By the property $\phi(e)^{-1} = \phi(e^{-1})$, it is true that $\phi(e_m^{-1}) = \phi(e_m)^{-1} = \phi(e_m)$.

Our next example is finding $\phi(e_4)$. We have e_4 going from $\mathbf{2} \to \mathbf{4}$. However, the lift of $\mathbf{2}$ is not adjacent to the lift of $\mathbf{4}$ in Fig. 1. Therefore, there must exist $x \in N(\mathbf{2}) \subset V(PSL(2,\mathbb{Z}_{2^n}))$ such that $p(x) = p(\mathbf{4}) = \mathbf{4} \in V(PSL(2,\mathbb{Z}_2))$. This $x = \begin{pmatrix} 1 & 7 \\ 2 & 7 \end{pmatrix}$, the orange-bordered vertex in Fig. 1, since modulo 2 it becomes $\mathbf{4}$. Therefore, $\gamma x = \mathbf{4}$, which implies that $\gamma = \begin{pmatrix} -3 & 2 \\ -2 & 1 \end{pmatrix}$, where $\gamma = \phi(e_4)$. By our preliminary statements, $\phi(e_4^{-1}) = \gamma^{-1} = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}$. ☐

4. Properties of $\hat{\Gamma}_{2^n}$

Proposition 4. *The elements of $S(\hat{\Gamma}_{2^n})$, the generating set for $\hat{\Gamma}_{2^n}$, have order 2^{n-1} for $n \geq 2$. Recall*

$$S(\hat{\Gamma}_{2^n}) = \left\{ \phi(e_4^{-1}) = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}, \phi(e_4) = \begin{pmatrix} -3 & 2 \\ -2 & 1 \end{pmatrix}, \phi(e_5^{-1}) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \right.$$

$$\left. \phi(e_5) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \phi(e_6^{-1}) = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \phi(e_6) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}.$$

Proof. We will prove this by induction. We will first show that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{2^{n-1}} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^n.$$

Base Case: $(n = 2)$ Consider the element $\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}$ of $\hat{\Gamma}_4$. We have:

$$\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix} = \begin{pmatrix} -3 & 4 \\ -4 & 5 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 4.$$

The remaining elements are easy to verify.

Inductive Step: Assume that for all $x \in S(\hat{\Gamma}_{2^n})$, $(x^{2^{n-1}}) \bmod 2^n$ is the identity matrix for all n. We want to show that for all $y \in S(\hat{\Gamma}_{2^{n+1}})$, $y^{2^n} \bmod 2^{n+1}$ is the identity matrix. Let $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in S(\hat{\Gamma}_{2^n})$. From the inductive hypothesis, we know

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}^{2^{n-1}} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^n = \begin{pmatrix} 1+2^n a & 2^n b \\ 2^n c & 1+2^n d \end{pmatrix},$$

where $a, b, c, d, p, q, r, s \in \mathbb{Z}$. Squaring both sides we see that

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}^{2^n} = \begin{pmatrix} (1+2^n a)^2 + 2^{2n}bc & 2^{n+1}b + 2^{2n}ab + 2^{2n}bd \\ 2^{n+1}c + 2^{2n}ac + 2^{2n}cd & (1+2^n d)^2 + 2^{2n}bc \end{pmatrix}.$$

Consider the following fact:

$$2n = n+1+n-1 \Rightarrow 2^{2n} = 2^{n+1+n-1} = 2^{n+1}2^{n-1}.$$

Now consider each entry individually:

$$\begin{aligned} (1+2^n a)^2 + 2^{2n}bc &= 1 + 2^{n+1}a + 2^{2n}a^2 + 2^{2n}bc \\ &= 1 + 2^{n+1}a + 2^{n+1}2^{n-1}a^2 + 2^{n+1}2^{n-1}bc \\ &= 1 + 2^{n+1}(a + 2^{n-1}a^2 + 2^{n-1}bc) \equiv 1 \bmod 2^{n+1}. \end{aligned}$$

$$\begin{aligned} 2^{n+1}b + 2^{2n}ab + 2^{2n}bd &= 2^{n+1}b + 2^{n+1}2^{n-1}ab + 2^{n+1}2^{n-1}bd \\ &= 2^{n+1}(b + 2^{n-1}ab + 2^{n-1}bd) \equiv 0 \bmod 2^{n+1}. \end{aligned}$$

$$\begin{aligned} 2^{n+1}c + 2^{2n}ac + 2^{2n}cd &= 2^{n+1}c + 2^{n+1}2^{n-1}ac + 2^{n+1}2^{n-1}cd \\ &= 2^{n+1}(c + 2^{n-1}ac + 2^{n-1}cd) \equiv 0 \bmod 2^{n+1}. \end{aligned}$$

$$\begin{aligned} (1+2^n d)^2 + 2^{2n}bc &= 1 + 2^{n+1}d + 2^{2n}d^2 + 2^{2n}bc \\ &= 1 + 2^{n+1}d + 2^{n+1}2^{n-1}d^2 + 2^{n+1}2^{n-1}bc \\ &= 1 + 2^{n+1}(d + 2^{n-1}d^2 + 2^{n-1}bc) \equiv 1 \bmod 2^{n+1}. \end{aligned}$$

$$\Rightarrow \begin{pmatrix} p & q \\ r & s \end{pmatrix}^{2^n} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^{n+1}.$$

In order to complete our proof, we must show that for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S(\hat{\Gamma}_{2^n})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^m \not\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^n, \text{ where } m < 2^{n-1}.$$

Base Case: $(n = 2)$ The proof is matrix multiplication.
Inductive Step: Assume that for all n,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^m \not\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^n,$$

where $m < 2^{n-1}$. Then it is obvious that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^m \not\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^{n+1},$$

for $m < 2^{n-1}$. We must show that this non-equivalency holds true for $2^{n-1} \leq m < 2^n$. To this end, we will prove that for non-negative integers $k < 2^{n-1}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{2^{n-1}+k} \not\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^{n+1}.$$

Lemma 5. *For all $n \in \mathbb{Z}^+$,*

$$\phi(e_4^{-1})^n = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^n = \begin{pmatrix} (-1)^{n+1}(2n-1) & (-1)^n(2n) \\ (-1)^{n+1}(2n) & (-1)^n(2n+1) \end{pmatrix},$$

$$\phi(e_4)^n = \begin{pmatrix} -3 & 2 \\ -2 & 1 \end{pmatrix}^n = \begin{pmatrix} (-1)^n(2n+1) & (-1)^{n+1}(2n) \\ (-1)^n(2n) & (-1)^{n+1}(2n-1) \end{pmatrix},$$

$$\phi(e_5^{-1})^n = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix},$$

$$\phi(e_5)^n = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & -2n \\ 0 & 1 \end{pmatrix},$$

$$\phi(e_6^{-1})^n = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ -2n & 1 \end{pmatrix}, \text{ and}$$

$$\phi(e_6)^n = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}.$$

Proof. We will prove this lemma for $\phi(e_4^{-1})$. The $n = 1$ case is trivial. The rest of the proof follows the same format as $\phi(e_4^{-1})$.

Assume for induction that $\phi(e_4^{-1})^n = \begin{pmatrix} (-1)^{n+1}(2n-1) & (-1)^n(2n) \\ (-1)^{n+1}(2n) & (-1)^n(2n+1) \end{pmatrix}$ for all n. We must show the following:

$$\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^{n+1} = \begin{pmatrix} (-1)^n(2n+1) & (-1)^{n+1}(2n+2) \\ (-1)^n(2n+2) & (-1)^{n+1}(2n+3) \end{pmatrix}.$$

Multiply both sides of our inductive hypothesis on the right by $\phi(e_4^{-1})$ as follows:

$$\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^{n} \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix} = \begin{pmatrix} (-1)^{n+1}(2n-1) & (-1)^n(2n) \\ (-1)^{n+1}(2n) & (-1)^n(2n+1) \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}$$

$$= \begin{pmatrix} (-1)^{n+1}(2n-1) + (-1)^n 4n & (-1)^{n+1}(2n-1)(-2) + (-1)^n(-6n) \\ (-1)^{n+1}(2n) + (-1)^n(2(2n+1)) & (-1)^{n+1}(4n) + (-1)^n(2n+1)(-3) \end{pmatrix}$$

$$= \begin{pmatrix} (-1)^n(2n+1) & (-1)^{n+1}(2n+2) \\ (-1)^n(2n+2) & (-1)^{n+1}(2n+3) \end{pmatrix}.$$

□

We know that each element of $\hat{\Gamma}_{2^n}$ is the identity matrix modulus 2^{n+1} after it is multiplied by itself 2^n times. We must show that each element of $\hat{\Gamma}_{2^n}$ does not equal the identity at some point prior. We will prove this for $\phi(e_4^{-1})$. The other elements are left to the reader. Thus, our goal is to show that for some $k < 2^{n-1}$,

$$\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^{2^{n-1}+k} \not\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^{n+1}.$$

By Lemma 5, we have

$$\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^{2^{n-1}+k} = \begin{pmatrix} (-1)^{2^{n-1}+k+1}(2(2^{n-1}+k)-1) & (-1)^{2^{n-1}+k}(2(2^{n-1}+k)) \\ (-1)^{2^{n-1}+k+1}(2(2^{n-1}+k)) & (-1)^{2^{n-1}+k}(2(2^{n-1}+k)+1) \end{pmatrix}.$$

Consider the second entry:

$$(-1)^{2^{n-1}+k}(2(2^{n-1}+k)) = (-1)^{2^{n-1}+k}(2^n+2k).$$

In order for this entry to be congruent to $0 \bmod 2^{n+1}$, it must be divisible by 2^{n+1}. However, upon closer inspection we see that

$$2k < 2^n \Rightarrow 2^n + 2k < 2^n + 2^n = 2^{n+1}.$$

Thus,

$$(-1)^{2^{n-1}+k}(2^n+2k) < (-1)^{2^{n-1}+k}(2^{n+1}) \Rightarrow (-1)^{2^{n-1}+k}(2^n+2k) \not\equiv 0 \bmod 2^{n+1}.$$

Hence,

$$\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^{2^{n-1}+k} \not\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^{n+1}.$$

□

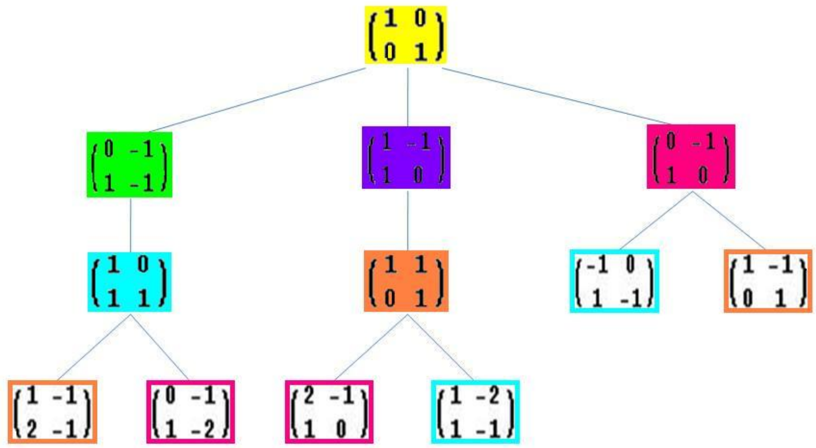

Figure 1. Partial Cayley Graph of $PSL(2,\mathbb{Z}_{2^n})$

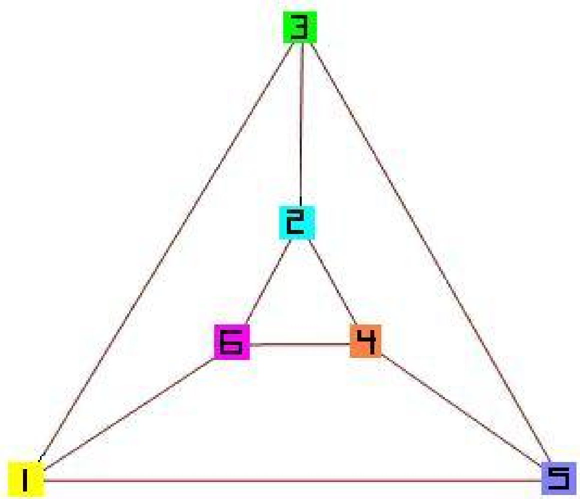

Figure 2. Cayley Graph of $PSL(2,\mathbb{Z}_2)$

5. References

1. Kwak, Jin Ho and Young Soo Kwon. "Characteristic polynomials of graph bundles having voltages in a dihedral group*." 2.