COVERING SPACES AND SUBGROUPS OF THE FREE GROUP

SAMANTHA NIEVEEN AND ALLISON SMITH

Adviser: Dennis Garity
Oregon State University

Abstract. In this paper we will use the known link between covering spaces of a topological space and subgroups of its fundamental group to investigate the subgroup structures of the free groups on two and more generators. Some of our conclusions, such as Marshall Hall's formula for the number of subgroups of a free group of finite index, have been shown before. (Hopefully others, such as some calculations for the number of normal subgroups of finite index, have not been. That would be cool.)

1. Introduction

The correspondence between the covering spaces of a space X and subgroups of π_1(X, x_0), the fundamental group of X at a base point x_0 is well known from topology. In particular, for any subgroup H of π_1(X, x_0), there exists a unique (up to covering equivalence) covering p :E→X and a point e_0 in $p^{-1}(x_0)$ so that π_1(E, e_0) is homomorphic to H under a homomorphism induced by p and E is path connected. Also, each covering space E corresponds in this way to a conjugacy class of subgroups of π_1(X, x_0) as e_0 ranges through $p^{-1}(x_0)$. For more information see Munkres[4] Chapter 8. Throughout this paper we say that a subgroup corresponds to a particular covering and choice of base point or that a covering and choice of base point corresponds to a particular subgroup, referring to the correspondence described here.

We note that if for a given e_0, E corresponds to a normal subgroup of π_1(X, x_0), then E corresponds to this subgroup for any choice of e_0 in $p^{-1}(x_0)$, since a normal subgroup is alone in its conjugacy class.

We note also that if E is an n-covering of X (that is, for each x∈X, $|p^{-1}(x)|=n$), the subgroup H of π_1(X, x_0) to which E corresponds is of index n in π_1(X, x_0).

1.1. The Figure Eight Space.

Definition 1.1. *The* figure eight space *(Figure 1) is a graph consisting of one vertex and two labeled, directed loops beginning and ending at the vertex. More generally, a* wedge of circles *is a graph consisting of one vertex and a number of labeled, directed loops beginning and ending at the vertex. The figure eight space is the wedge of two circles.*

The fundamental group of a wedge of r circles is the free group on r generators, which we will write F(r). The fundamental group of the figure eight space, therefore, is F(2). We will

Date: July 12 2006.
This work was done during the Summer 2006 REU program in Mathematics at Oregon State University.

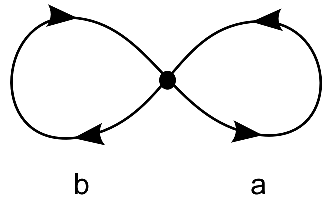

FIGURE 1. The figure eight space

write the generators of F(2) a and b, and these will correspond to the labels which we have given to the loops in the figure eight space.

Definition 1.2. *Let $p : E \to B$ be continuous and surjective. If every point b of B has a neighborhood U such that the inverse image $p^{-1}(U)$ can be written as the union of disjoint open sets V_α in E and for each α the restriction of p to V_α is a homeomorphism of V_α onto U, then p is called a* covering map*, and E is said to be a* covering space *of B.*

Definition 1.3. *Let $p : E \to B$ be a covering map; let B be connected. If $p^{-1}(b_0)$ has k elements for some $b_0 \in B$, then $p^{-1}(b)$ has k elements for every $b \in B$. In such a case, E is called a k-*covering *of B. k is called the* degree *of the covering.*

An n-covering of a wedge of r circles will consist of n vertices each the origin of r differently labeled directed edges and the terminus of r differently labeled directed edges. Some edges may be loops. We will be interested only in connected n- coverings.

Definition 1.4. *An element of F(r) may be represented as a string of symbols from the set $\{a_1, a_2, ..., a_r, a_1^{-1}, a_2^{-1}, ..., a_r^{-1}\}$ where $a_1, a_2, ..., a_r$ are the generators of F(r). This string is called a* word in $a_1, a_2, ..., a_r$*, or, if confusion is not likely, a* word*. More generally, an element may be represented as a word in any appropriate symbols, such as the generators of a subgroup to which the element represented belongs.*

Words appear in covering spaces as paths along the directed edges of the space, where a_k is represented by travel along an a_k edge in the direction of an arrow and a_k^{-1} is represented by travel in the direction opposite the arrow. Words in covering spaces are read from left to right, with $a_j a_k$ representing travel first along the edge a_j and then along the edge a_k. a_k^{-1} will sometimes be written $\overline{a}_k$.

Example 1.5. *There are three distinct 2-coverings of the figure eight space. (Figure 2.) Each consists of two vertices, each of which is the origin of an a-edge and a b-edge and the terminus of an a-edge and a b-edge.*

They correspond respectively to the following subgroups of F(2): $< b^2, ba\overline{b}, a| \quad >$, $< a^2, ab\overline{a}, b| \quad >$, and $< a^2, a\overline{b}, ab| \quad >$. These are the subgroups of F(2) of index 2.

2. HALL'S FORMULA FOR SUBGROUPS OF F(r) OF FINITE INDEX

In 1949, Marshall Hall, Jr. published an algebraic proof of a recursive formula to calculate the number of subgroups of F(r) of a given finite index [1]. He gave this formula as

$$N_{n,r} = n(n!)^{r-1} - \sum_{i=1}^{n-1} [(n-i)!]^{r-1} N_{i,r}$$

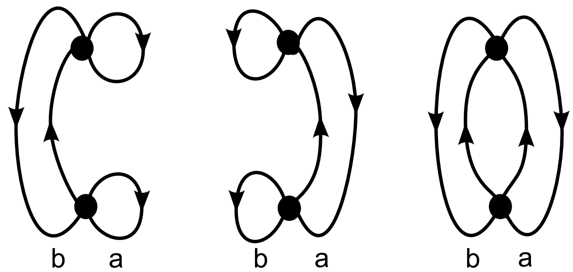

FIGURE 2. 2-coverings of the figure eight space

where $N_{n,r}$ is the number of subgroups of F(r) of index n and $N_{1,r} = 1$, since any group is its own single subgroup of index 1. This proof was modified slightly and related to coverings of the wedge of circles by Jin Ho Kwak and Jaeun Lee [3]. We give here an expanded and somewhat more concrete proof for F(2).

Theorem 2.1. *The number N_n of subgroups of index n of F(2) is given by*

$$N_n = n(n!) - \sum_{i=1}^{n-1} [(n-i)!] N_i.$$

Proof. $N_1 = 1(1) - 0 = 1$. Obviously, since there is one subgroup of F(2) of index 1, the formula works for $n = 1$. Then supposing that the formula holds for all natural numbers less than n, we will show that it holds for n. We first observe that we may consider any (connected or unconnected) n-covering of the figure eight space to be represented by an element of $S_n \times S_n$, and we may consider any element of $S_n \times S_n$ as representing some (connected or unconnected) n-covering of the figure eight space. We do this by naming the vertices of an n-covering $1, 2, ..., n$, with the base point e_0 labeled 1 for convenience and the other vertices labeled in any way. We can then follow the a-edges in cycles which together make an element α of S_n and the b-edges in cycles which make an element β of S_n. Then we associate the covering with the element (α, β) in $S_n \times S_n$. For example, the 3-covering s! hown in Figure 3 is represented by $((12)(3), (132)) \in S_3 \times S_3$.

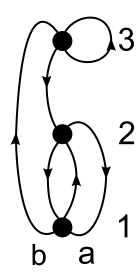

FIGURE 3

We can also easily reverse this process to find a covering represented by any element of $S_n \times S_n$. Since we know that each subgroup of F(2) of index n is associated with a connected n-covering, and each covering is represented by at least one element of $S_n \times S_n$, we start by considering all elements of $S_n \times S_n$ and proceed to remove elements until we are considering only elements which represent connected n-coverings which are either distinct from each other or have distinct base points: in other words, until we are considering only elements which are associated to distinct subgroups of index n. We are starting by considering the $(n!)^2$ elements of $S_n \times S_n$.

Some of these elements do not represent connected n- coverings; we will now count these elements and subtract them from the total number of elements in which we are interested. We will sum over i, the number of vertices in the connected component containing the base point in the covering represented by the element. i cannot be less than 1, since the base point must always be connected to itself, nor are we interested when $i \geq n$, since it does not make sense for $i > n$ and when $i = n$ we have a connected covering which we do not want to subtract from our count.

For each i we must choose from $n-1$ labeled vertices which are not the base point $i-1$ which are to be connected to the base point. We can do this in $\binom{n-1}{i-1} = \frac{(n-1)!}{(i-1)!(n-i)!}$ ways. Also, this connected component will be associated with a subgroup of $\mathrm{F}(n)$ of index i, and there are N_i distinct subgroups to choose from. Of the i vertices connected to the base point, the only one whose labeling is determined by the subgroup of $\mathrm{F}(2)$ with which the component is associated is the base point, which is labeled 1. The other $i-1$ vertices may be anywhere in the component, so there are $(i-1)!$ ways to arrange them. Furthermore, the $n-i$ vertices not connected to the base point must also be accounted for. These vertices may or may not be connected to each other: since they are labeled already because we are dealing with their representations in $S_n \times S_n$, there are $((n-i)!)^2$ ways to arrange both their a-edges and b-edges! in products of cycles, or permutations.

Now we have counted the elements of $S_n \times S_n$ that represent unconnected n- coverings and subtracted them, but we are still left with elements of $S_n \times S_n$ where we want subgroups of $\mathrm{F}(2)$. We solve this problem by noting that while elements of $S_n \times S_n$ account for the labeling of all n vertices in a covering, subgroups of $\mathrm{F}(2)$ are associated with coverings with only one vertex, the base point, labeled. So we have in each case $n-1$ too many points labeled, which means that we have $(n-1)!$ times more elements of $S_n \times S_n$ than subgroups. Thus we get the following formula.

$$N_n = \frac{(n!)^2 - \sum_{i=1}^{n-1} \binom{n-1}{i-1}[(i-1)!N_i]((n-i)!)^2}{(n-1)!} = n(n!) - \sum_{i=1}^{n-1}[(n-i)!]N_i$$

□

Corollary 2.2. *The number $N_{n,r}$ of subgroups of index n of $F(r)$ is given by*

$$N_{n,r} = n(n!)^{r-1} - \sum_{i=1}^{n-1}[(n-i)!]^{r-1}N_i.$$

Proof. We can see this in the argument above by replacing a and b edges with edges labeled by the set $\{a_1, a_2, ..., a_r\}$. We then are dealing throughout the proof with the $(n!)^r$ elements of $S_n \times S_n \times ... \times S_n$ (formed by r copies of S_n).

□

3. Normal Subgroups of F(2) of Finite Index

Covering spaces of the figure eight space give us a powerful and intuitive tool for finding and examining the normal subgroups of F(2). As we mentioned above, a covering of the figure eight space that corresponds to a normal subgroup of F(2) does so independent of the choice of base point within the covering. Therefore, such a covering is highly symmetric, with every point in some sense the same as every other point [2]. In particular, every word that is a loop at one point is a loop starting from every other point, since such a loop corresponds to a word in the subgroup to which the covering space corresponds.

Definition 3.1. *A covering E of a space X which corresponds to a normal subgroup of $\pi_1(X, x_0)$ is a* regular *covering.*

The task of finding and classifying the normal subgroups of F(2) of index n can thus be reduced to the task of finding and classifying the regular n- coverings of the figure eight space. This task, in turn, is made easier because the n-coverings of the figure eight space, particularly for small n, are easy to imagine or draw and to check for regularity.

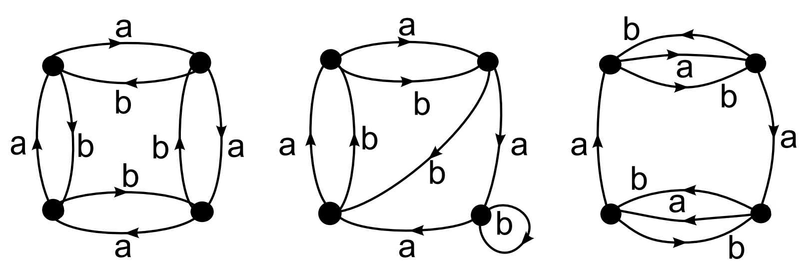

Figure 4. Three 4-coverings of the figure eight space

Example 3.2. *The covering to the left in Figure 4 is regular, while the coverings in the center and to the right are not. In the covering in the center, note that one of the b-edges forms a loop, or 1-cycle, while the others are arranged in a 3-cycle. Whenever the a or b edges are not divided into cycle all of the same length, we immediately know that the covering is not regular. It is not, however, true that whenever a covering is not regular either the a or b edges are not divided into cycles all of the same length, as the covering to the right shows. In this covering the word* ab *forms a loop at some vertices and not at others, so the vertices are not all the same.*

It is thus possible to find many normal subgroups of F(2) (or even F(r)) of very low index without an organized way of attacking the problem. Such a method would however become both tedious and unreliable as the index of the subgroups desired (and thus the size of the covering graphs needed) increased.

3.1. **An Algorithm for Generating Normal Subgroups of F(r) of Index n.** In order to more quickly and thoroughly investigate normal subgroups of F(2) of finite index, we developed an algorithm suitable for programming that would generate and count subgroups and normal subgroups of F(r) of a given finite index. Since we were interested primarily in normal subgroups of F(2), we then implemented it for F(2). generating normal subgroups.

These adjustments prevented the algorithm from generating many subgroups which were not normal, but as Hall's Formula already gives the number of such subgroups, and as that number quickly becomes too high for individual inspection of the subgroups to make sense, this was acceptable to us. (We need this if we include the modifications to the program. We would also need to explain those modifications, I think.)

Theorem 3.3. *An algorithm exists to generate uniquely the subgroups of F(r) of a given index n.*

Proof. We note first that given the one-to-one correspondence between subgroups of F(r) of index n and n- coverings (E, e_0) of the wedge of r circles, it is enough to find an algorithm to generate uniquely the n-coverings (E, e_0) of the wedge of r circles.

We will define algorithmically a map $f : C \to M(n, \mathbb{Z})$ where C is the set of connected n-coverings (E, e_0) of the wedge of r circles and $M(n, \mathbb{Z})$ is the set of $n \times n$ matrices with entries in $\mathbb{Z}$. We will show that f is a bijective function when the range is restricted to a set B of matrices which can be generated uniquely by an algorithm.

We define f((E,e_0)) as follows: let A=$\{a_1, a_2, ..., a_r\}$ be the generators of F(r), and let the set of edges with origin v for any $v \in$E contain one edge labeled with each element of A. Also let the set of edges with terminus v for any $v \in$E contain one edge labeled with each element of A. Then we label the vertices of E with {1, 2, ..., n} by the following procedure. Label e_0 as 1. Following in order the edges $\{a_1, a_2, ..., a_r\}$ with origin e_0=1, if the terminus of edge a_k is not yet labeled, label it with the next unused element of {1, 2, ..., n}. When this has been accomplished for $\{a_1, a_2, ..., a_r\}$ with origin 1, follow the same procedure with $\{a_1, a_2, ..., a_r\}$ with origin 2. Repeat for the set of edges with each origin in {1, 2, ..., n} until all vertices have been labeled and all labels have been used. (Since there are n vertices and n labels, these events will happen s! imultaneously.) Now construct a $n \times n$ matrix. In the ith row, jth column, place an entry 2^{k-1} if the edge a_k with origin i has terminus j, and an entry 0 if there is no edge with origin i and terminus j. If more than one edge has origin i and terminus j, add the entries together and place their sum in the appropriate place in the matrix. (For example, if edge a_1 and edge a_2 with origin i both have terminus j, place $2^0 + 2^1 = 3$ in the ith row, jth column of the matrix.) The matrix thus constructed is f((E,e_0)).

We claim that f is a bijective function onto a set B of matrices which we will now define. Let B be the set generated by the following algorithm:

(1) Make a stack of $n \times n$ matrices containing only the matrix with all entries zero. Make an empty set B of $n \times n$ matrices.
(2) Take the top matrix off the stack.
(3) Find the bottom-most row i so that the entries in row i sum to $2^0 + 2^1 + ... + 2^{r-1}$. If there is no such row, go to the next step. Read the sub-matrix consisting of rows 1 through i and columns 1 through i. If the entries of each row in the sub-matrix sum to $2^0 + 2^1 + ... + 2^{r-1}$, discard the matrix and return to step 2. Otherwise, continue.
(4) Find the topmost row j whose entries sum to less than $2^0 + 2^1 + ... + 2^{r-1}$. If there is no such row, go to step 7. In row j, find the least k so that 2^{k-1} is greater than the sum of the entries in the row. Such a k will exist because each of the terms in the sequence $2^0 + 2^1 + ... + 2^{r-1}$ is greater than the sum of the previous terms.

(5) Find all of the places in row j which are in columns not already containing an entry *whose binary decomposition includes a term* 2^{k-1} and which are in columns so that every column to their left other than the 1st column contains a non-zero entry.
(6) Make a new copy of the matrix for each place found in step 5, in each copy adding 2^{k-1} to the entry in the place found in step 5 to which the new matrix corresponds. Discard the old matrix. Put the new copies on the stack and return to step 2.
(7) Add the matrix to the set B.

We need to prove that $f : C \to B$ is well- defined, injective, and surjective, and that its range really is contained in B.

We begin by showing that f is well-defined. Consider a connected n-covering (E, e_0). Let D=f((E, e_0)) and let G=f((E, e_0)). Suppose $D \neq G$. Then there is some $i < n$ and some $j < n$ so that the entry d_{ij} in the ith row jth column of D is not equal to the entry g_{ij} in the ith row, jth column of G. Without loss of generality, suppose that the binary representation of d_{ij} includes a term not included in the binary representation of g_{ij}. This term is 2^k for some k. By the construction of f, it is 2^k for some k so that $k+1 \leq r$, and it represents and edge a_{k+1} with origin i and terminus j in (E, e_0). Then either there is an edge in (E, e_0) which is not in (E, e_0), a clear contradiction, or i and j refer to different points in D than they do in G. In other words, in constructing f((E, e_0)) twice, we must have labeled the points in (E, e_0) in two different ways. ! But since (E, e_0) is connected, this is impossible, since the algorithm for f specifies the exact order in which we must label the points connected to the base point, which is e_0 in both cases. Only if E were not connected would we ever be able to make a choice of which point to label next. Then it is a contradiction that $D \neq G$, so f is well defined on C, since the choice of (E, e_0) was arbitrary.

We show next that f is injective. Let (E, e_0)$\in C$, (D, d_0)$\in C$, and let f((E, e_0))=f((D, d_0)). Then for any vertices i and j in (E, e_0) connected by an edge a_k with origin i, by the construction of f there is a pair of vertices i and j in (D, d_0) connected by an edge a_k with origin i. Also, for any two vertices i' and j' in (D, d_0) connected by an edge a'_k with origin i', there is a pair of vertices i' and j' in (E, e_0) connected by an edge a'_k with origin i'. Then the vertices, edges, labels, and orientations in (E, e_0) are the same as those in (D, d_0), and (E, e_0)=(D, d_0). Then f is injective.

Now we show that the range of f is contained in B. We have shown that f is well-defined on all elements of C. Consider $D = f$((E, e_0)) for some (E, e_0)$\in C$. We assert that $D \in B$. We know by the construction of $D = f$((E, e_0)) that D is an $n \times n$ matrix, and that 2^{k-1} appears exactly once in each row for every $1 \leq k \leq r$, since each edge from $\{a_1, ..., a_r\}$ leaves each vertex exactly once, although numbers of the form 2^{k-1} may be summed together in an entry to represent multiple edges leaving the same vertex and entering the same vertex. Similarly, we know that each 2^{k-1} appears exactly once in each column, since each edge from $\{a_1, ..., a_r\}$ enters each vertex exactly once. These facts about D ensure that it will be generated through the algorithm that places elements in B, except that we must also show that the matrices along the way to generating D are never discarded in step 3 of t! he algorithm, and that no entry 2^{k-1} need be placed by the algorithm so that a column to its left (other than the 1st column) has all zero entries.

For the matrices which become D to be discarded at step 3 of the algorithm, it would be necessary for there to be some number of rows i, $1 \leq i < n$, so that all of the nonzero entries in the first i rows of D fall in the first i columns of D. This is clear from the description of step 3. In particular, it is important that this step deals only with rows whose entries will no longer be changed by the algorithm, and which therefore will come through to D unchanged. If there is some such number of rows i, then by the construction of D there are i vertices in (E, e_0) such that all entries leaving them (nonzero entries in rows 1 through i) return to these same i vertices (columns 1 through i). But then each of the vertices would have all r edges leaving it accounted for, and all r edges entering it accounted for, without these i vertices being connected to the other $n-i$ vertices in the covering, and (E, $e!_0$), not being connected, would not be an element of C. Then the matrices which will become D may never be discarded at step 3.

Assume that at some point in producing D the algorithm had to place an entry 2^{k-1} so that a column to its left (other than the 1st column) had all zero entries. Let first such entry be in row i, column j. Let some column to the left with all zero entries be column j'. Then consider the process by which $D = f((\text{E}, e_0))$ was originally defined. According to this process, the entry 2^{k-1} in row i, column j was placed there because there is an edge a_k in (E, e_0) going from the vertex labeled i to the vertex labeled j. Also, there is no edge going to vertex j' from any vertex i' with $i' < i$, and there is no edge a'_k going from vertex i to vertex j' with $k' < k$. Furthermore, we know that $j' < j$, since column j' is the further left of the two. But according to the construction process for $f((\text{E}, e_0))$, if $j' < j$, then there is an edge going to vertex j' from a vertex i' with $i' < i$, or there is an edge a'_k going from v! ertex i to vertex j' with $k' < k$. This contradicts the assumption, so D is produced by the algorithm and is an element of B. Then the range of f is contained in B.

Finally we show that $f : C \to B$ is surjective. Let $D \in B$. Draw a graph with n vertices and label them from {1, ..., n}. For each entry in D, decompose it into the form $2^{k_1-1} + 2^{k_2-1} + ...$ with each k_l represented at most once. There is only one way to do this. Then for $1 \le i \le n$ and $1 \le j \le n$, draw an edge a_k with origin i and terminus j for every k in the decomposition of the entry of matrix D in row i column j. This is a graph with n vertices, each of which has an edge a_k leaving for $1 \le k \le r$ and an edge a_k entering for $1 \le k \le r$ because each row and column in D has exactly one entry whose decomposition includes exactly one copy of 2^{k-1} for every such k. Furthermore, it is a connected graph because D was never discarded in step 3 and so there are no i points including the point labeled 1 which are only connected to each other so that $1 \le i < n$. Then ca! ll this graph E and the vertex labeled 1 e_0. (E, e_0) $\in C$.

We claim that $D = f((\text{E}, e_0))$. Consider the construction of $f((\text{E}, e_0))$. We label e_0 as 1 and proceed to label the other vertices and create an $n \times n$ matrix as described above. Suppose that this matrix were not D. Then in some ith row and jth column, the values of the entries in D and in $f((\text{E}, e_0))$ would not agree. Suppose without loss of generality that the entry in D had in its binary decomposition the number 2^{k_1-1} and the entry in $f((\text{E}, e_0))$ did not. Then by the construction of E from D, there is an edge a_{k_1} in E with origin i and terminus j, and by the construction of $f((\text{E}, e_0))$ there is no such edge in E. Then either there is a contradiction or the vertices of E were labeled differently in the construction of E than in the construction of $f((\text{E}, e_0))$. But the vertices cannot have been labeled differently: in the construction of E from D, a vertex after the 1st one gets labeled when a new column ! gets its first entry. This in turn happens strictly in order from left to right ($1 \le j \le n$) as entries are filled in starting with all of the entries in the first row in ascending order and then moving down the matrix. In the construction of E, this order means labeling in order each vertex with the next element of the set {1, ..., n} as the vertex first appears as the terminus of an edge, starting with all the edges with origin 1 in the order $\{a_1, ..., a_r\}$ and moving in order through the edges going from other vertices. But this is the very same labeling given to the vertices in the construction of $f((\mathrm{E}, e_0))$, so $D = f((\mathrm{E}, e_0))$, and f is surjective.

Then the elements of B are in one-to-one correspondence with the elements of C, which are in one-to-one correspondence with the subgroups of $\mathrm{F}(r)$ of index n, so the algorithm to generate the elements of B generates uniquely all subgroups of $\mathrm{F}(r)$ of index n. □

Theorem 3.4. *An algorithm exists to tell whether a given subgroup of F(r) of finite index is normal.*

Proof. Given the known correspondence between subgroups and covering spaces, as well as the results of the previous theorem, it is enough to find an algorithm to tell whether one of the matrices from set B of the previous theorem corresponds to a regular covering space and therefore a normal subgroup. Let $D \in B$, and let $D = f((\mathrm{E}, e_0))$ for some covering space (E, e_0) of the wedge of r circles. If E is regular, then any vertex of E is equivalent to any other vertex in E. In particular, the choice of e_0 does not affect the subgroup to which E corresponds. This in turn implies that the choice of e_0 does not affect the matrix in B to which E corresponds. The choice of e_0 in E corresponds, as we have seen, to the choice of vertex to associate with the first row and column of D. An algorithm that would check each vertex to see whether it could be substituted interchangeably with e_0 would determine whether E was regular. An algorithm to determine whether! D corresponds to a regular covering space E would therefore check to see whether the vertex associated with the each row and column of D could be substituted for the vertex associated with the first row and column without changing D.

To rename a vertex i in E j, we switch the ith and jth rows of D and the ith and jth columns of D. Then according to the correspondence between E and D, those edges that had been leaving or entering a vertex labeled i are now leaving or entering a vertex labeled j and vice versa. However, the matrix D' that results after we have performed this operation on D may no longer be an element of B. In particular, sometimes D' will have a column k whose first entry appears in an earlier row than the first entry in a column k' while $1 \neq k' < k$ or whose first entry is 2^{l-1} while the first entry in column k' is $2^{l'-1}$ in the same row, with $1 \neq k' < k$ and $l' > l$. In this case D' needs to be converted into an element of B in order to be meaningfully compared with other elements of B, including D itself, because the one-to-one correspondence that has been established is between elements of B and covering spaces rather than b! etween $n \times n$ matrices and covering spaces.

Example 3.5. *The following matrix is the image under f of the covering to the left in Figure 4:*

$$\begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 0 & 0 & 1 \\ 1 & 0 & 0 & 2 \\ 0 & 2 & 1 & 0 \end{pmatrix}$$

If we try to rename vertex 2 as 1, we switch the first and second rows and columns of the matrix to obtain :

$$\begin{pmatrix} 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 \end{pmatrix}$$

which is no longer an element of B.

When we convert D' into an element of B, we must take care to preserve the association between vertices in E and row-column pairs in D' so that we maintain the association between D' and E as we did in the first step of creating D'. To convert D' into an element of B while maintaining this association, we look for a column i whose first entry would have been placed by the algorithm of Theorem 3.3 before the first entry of some earlier column $j \neq 1$, and then switch these columns and then the rows i and j. This is equivalent to switching the labels of vertex i and vertex j in E. When there are no more such columns, D' will be an element of B, since the labels in E will have been rearranged so that they follow the rules in the definition of f in Theorem 3.3. If E is regular, at this point $D' = D$.

Example 3.6. *In order to convert the second matrix of Example 3.5 into an element of B, we first switch the second and fourth rows and columns and then the third and fourth rows and columns:*

$$\begin{pmatrix} 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 0 & 0 & 1 \\ 1 & 0 & 0 & 2 \\ 0 & 2 & 1 & 0 \end{pmatrix}$$

We end with the same matrix with which we began Example 3.5, as we would expect, since the covering to which this matrix corresponds is regular.

Then the algorithm for checking to see whether an $n \times n$ matrix $D \in B$ corresponds to a regular n-covering of the wedge of r circles is as follows:

For $1 < i \leq n$:

(1) Switch row i with row 1 and column i with column 1.
(2) For $1 \leq j < n$ switch column $j+1$ with the column k, $j < k \leq n$, having the entry placed first in the algorithm of Theorem 3.3 of all such columns k (that is, the entry in the topmost row of all such columns k or the entry in the topmost row with the lowest term 2^{l-1} in its binary decomposition of all such columns k.) Switch row $j+1$ with row k. Begin step 2 for next j.
(3) Compare this matrix to D. (This is $D' \in B$ formed by switching vertex i with vertex 1.) If this matrix is identical to D, begin the process for next i. If this matrix is not identical to D, then D does not correspond to a regular covering, so stop checking. If this matrix is identical to D for all i, then D corresponds to a regular covering.

□

We implemented this algorithm in C++ for subgroups of F(2) with index ≤ 14. The code is contained in the appendices; Table 1 contains the numbers produced by Hall's Formula and our algorithm. Notably, while the total number of subgroups increases steadily with the index of the subgroups, the number of normal subgroups fluctuates, although showing a general upward trend. This fluctuation is linked to the prime factorization of the index.

Index	Total Subgroups	Normal Subgroups
1	1	1
2	3	3
3	13	4
4	71	7
5	461	6
6	3447	15
7	29093	8
8	273343	19
9	2829325	13
10	31998903	21
11	392743957	12
12	5201061455	41
13	73943424413	14
14	1123596277863	27

TABLE 1. Subgroups and Normal Subgroups of F(2) of Index ≤ 14

4. Enumerating normal subgroups of $F(2)$

Definition 4.1. *The* order *of a generator, a, at a vertex is the smallest integer k such that a^k is a loop at that vertex.*

Since in a regular covering one must be able to choose any vertex as the base point and still obtain the same fundamental group, any word that forms a loop at one vertex of a regular covering must form a loop at every vertex of that covering. Therefore, if a generator a has order k at one vertex of a regular covering, then it has order k at every other vertex of the covering, and the order of a can be referred to without specifying a base point.

Definition 4.2. *A regular covering of the figure eight space is a $k \times j$* covering *if a has order k and b has order j.*

Lemma 4.3. *The order of a generator in a regular covering must divide the degree of the covering.*

Proof. Let a be the generator and let k be the order of a. Pick an initial vertex and label it 1. Since a has order k and each vertex has exactly one a edge leaving and one a edge arriving, there will be $k-1$ other vertices that can be reached from vertex 1 by a word in a and these form the set X_1. Each of the vertices lead to another vertex in the same set by the word a, and therefore each vertex can be reached by a word in a if and only if the starting vertex is in the same set. If there are any vertices left, pick a new vertex that has not been previously

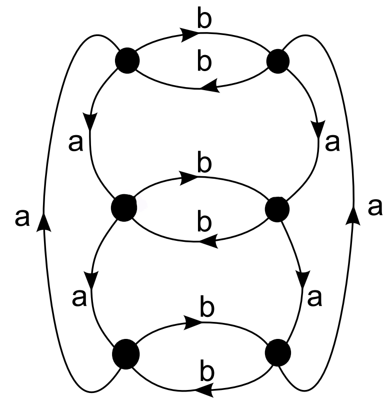

FIGURE 5. A 3×2 covering

reached and label it 2. There will again be $k-1$ other vertices that can be reached from vertex 2 and they will not be in any previous set. We can continue in this fashion. Since the degree of the covering is assumed to be finite and k more vertices are reached at each step, eventually all the vertices will have been reached. This means that the vertices can be divided into sets of size! k. Therefore k divides the degree of the covering. □

Lemma 4.4. *There are n regular n-coverings of the figure eight space such that a has order n.*

Proof. There is a unique way to arrange n undistinguished vertices such that a has order n. We can pick an arbitrary vertex and label it 0, and then label the rest of the vertices 1 through $n-1$ according to the order in which they are reached by repeatedly traveling along a edges starting at 0. The b edge that leaves vertex 0 may arrive at any of the n vertices. If the b edge that leaves vertex 0 arrives at vertex i, then the word $a^i b^{-1}$ is a loop beginning at vertex 0. In order to ensure regularity, $a^i b^{-1}$ must be a loop beginning at every vertex, and therefore the b edge that leaves vertex j must arrive at vertex $j+i \pmod{n}$. This implies that once a single b edge is placed, the rest of the covering space is completely determined. Since there are n ways to place the initial b edge, there are n possible regular coverings when a has order n. The way the initial b edge is placed also uniquely determines the number $!i \in \mathbb{Z}/n\mathbb{Z}$ such that $a^i b^{-1}$ is a loop, which means that the n possible regular coverings are distinct. Each of the coverings can also be rotated to make any point the base point and still be the exact same covering, which means that they are in fact regular. Therefore there are n regular coverings such that a has order n. □

4.1. **Covering spaces that “skip” and “twist”.** A convenient way to view a regular covering space of the figure eight space is as a stack of cycles. Consider the case when a has order p and b has order q and the degree of the covering is pq, where p and q are primes, not necessarily distinct. Since the vertices can be partitioned into sets of size p as in Lemma 4.3 according to which are connected by words in a, the vertices can be organized as a stack of q p-gons where the sides of the p-gons are a edges organized as a cycle oriented in a counter-clockwise direction.

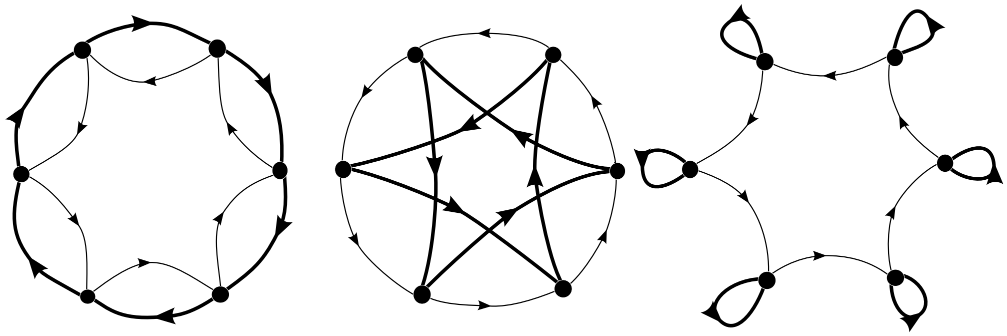

FIGURE 6. A 6×6 covering and a 6×3 and a 6×1 covering

If a b edge were to connect two vertices on the same a-cycle, then there would be a word of the form $a^m b^{-1}$ that would be a loop at one of the vertices. Since we are assuming the space is regular, this means that this word must be a loop at all vertices and therefore all b edges connect vertices on the same a-cycle. This is impossible since the space would then be unconnected. Therefore b edges must connect vertices that belong to different a- cycles.

Since b has order q, the b edges can also be organized as cycles of q edges which travel between the a-cycles. If a b-cycle visits the same a- cycle more than once during one trip through the b edges of that cycle, then there is a word of the form $b^s a^t$ where $0 < s < q$ that forms a loop at a vertex. In order for the space to be regular, this word must be a loop at all vertices, and therefore the b-cycle must visit all the a-cycles it visits more than once. For each repeat visit to an a-cycle there is another word of that form that is a loop, and therefore, if a space is to be regular, a b-cycle must visit all the a-cycles it visits an equal number of times. Since each b edge in the cycle corresponds to exactly one visit to an a-cycle, the number of times each a-cycle is visited must divide the order of b. We are assuming the order of b is prime, however, and since we have already established that a b-cycle cannot simply visit th! e same a-cycle q times, this implies that a b- cycle can only visit the same cycle once. Since there are q a-cycles and b has order q, each b- cycle must visit every a-cycle exactly once.

In any regular covering of this kind, one of the b- cycles may be chosen to be the "backbone" of the stack and and the a-cycles may be oriented so that this b-cycles visits each a-cycle in order from bottom to top and each visited vertex is directly above the others. Each a-cycle in the stack can then be numbered 0 through $q-1$ beginning with the bottom cycle, and within each cycle the vertices can be labeled 0 through $p-1$ beginning with the vertex that is visited by the backbone. Each vertex can then be named $v_{i,j}$ where i is the number of the cycle and j the number of the vertex within the cycle.

Once a backbone has been chosen, we may consider the possibilities for the b edge that begins at $v_{0,1}$.

Definition 4.5. *If the b edge that begins at $v_{0,1}$ ends on the a-cycle numbered k, the covering is considered to be* skipping *by k. If that edge ends on a vertex numbered l, the covering is considered to be* twisting *by l. A regular covering that is skipping by 1 is considered to be not skipping and a covering that is twisting by 1 is considered to be not twisting.*

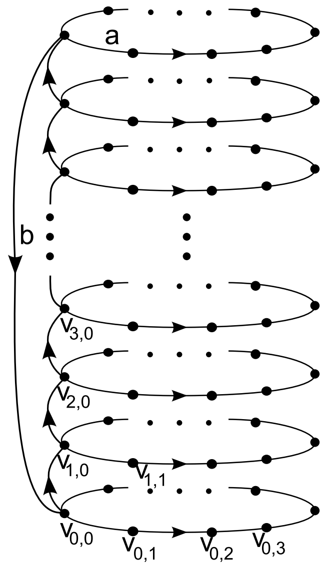

FIGURE 7. Stack with a backbone

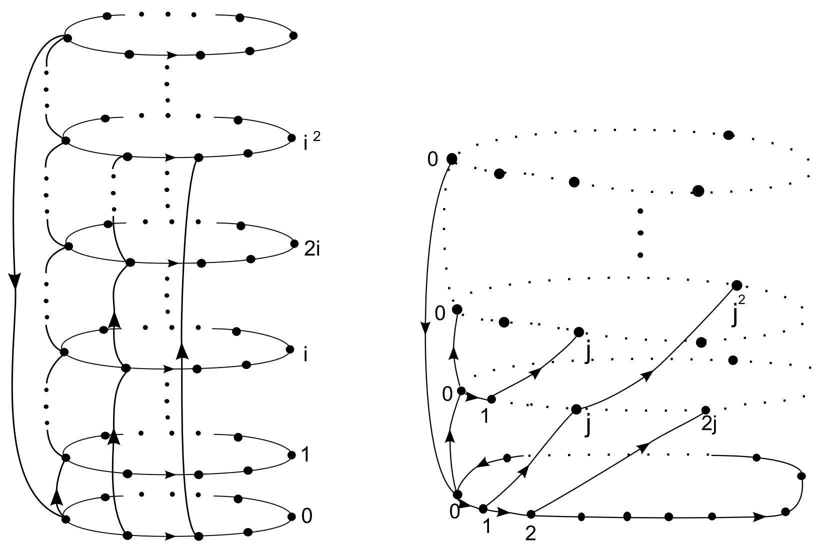

FIGURE 8. "Skipping" and "Twisting"

If that edge ends at $v_{i,j}$, then the word $aba^{-j}b^{-i}$ is a loop beginning at $v_{0,0}$. The covering is regular, therefore $aba^{-j}b^{-i}$ must be a loop beginning at every vertex. In order for it to be a loop at vertex $v_{n,0}$, the b edge beginning at a vertex $v_{n,1}$ must end at $v_{n+i \pmod q, j}$. Then in order for it to be a loop at vertex $v_{n,1}$, the b edge beginning at vertex $v_{n,2}$ must end at $v_{n+i^2 \pmod q, 2j \pmod p}$. Continuing around the cycles in this manner, we can see that the b edge beginning at vertex $v_{n,m}$ must end at $v_{n+i^m \pmod q, mj \pmod p}$.

This must be true even after a full circle around the cycles; i.e. $v_{0,0}$ must obey the above rule as if it were named $v_{0,p}$. However, since the b edge beginning at $v_{0,0}$ already has a predetermined end, this places restrictions on i. The b edge beginning at $v_{0,p}$ ($v_{0,0}$) already ends at $v_{1,0}$, therefore $v_{i^p \pmod q), pj \pmod p)}$ must be the same vertex as $v_{1,0}$. Thus, i must satisfy $i^p \equiv 1 \pmod q$.

The requirement that b have order q places a restriction on j. We must be able to follow the path of the word b^q beginning at vertex $v_{0,1}$ and return to the same vertex. According to the rules established above, the word follows the path: $v_{0,1} \to v_{i,j} \to v_{i+i^j \pmod q), j^2 \pmod p)} \to v_{i+i^j+i^{j^2} \pmod q), j^3 \pmod p)} \to \cdots \to v_{\sum_{n=0}^{q-1} i^{j^n} \pmod q), j^q \pmod p)} = v_{0,1}$. Thus, j must satisfy $j^q \equiv 1 \pmod p$.

These restrictions imply that the $ord_q(i) \mid p$ and $ord_p(j) \mid q$, but since p and q are prime either $i = 1$ or $ord_q(i) = p$ and either $j = 1$ or $ord_p(j) = q$. By Fermat's Little Theorem, $i^{q-1} \equiv 1 \pmod q$ and $j^{p-1} \equiv 1 \pmod p$; therefore $ord_q(i) \mid q-1$ and $ord_p(j) \mid p-1$. This means that i can take values other than 1 only if $p \mid q-1$ and j can take values other than 1 only if $q \mid p-1$. But $p \mid q-1$ implies $p < q$ and $q \mid p-1$ implies $q < p$; therefore only one of i or j can have a value other than 1 and then only if $p \mid q-1$ or $q \mid p-1$.

If $p \mid q-1$, then it is a known result in number theory that the congruence equation $x^p \equiv 1 \pmod q$ has exactly p solutions [5]. Since, as stated earlier, i completely determines a regular covering, this implies that there are p $p \times q$ coverings when $p \mid q-1$. Similarly, when $q \mid p-1$ there are q $p \times q$ coverings.

This discussion has proven the following lemma:

Lemma 4.6. *Let p and q be primes, not necessarily distinct and consider regular pq-coverings. If $p \mid q-1$, then there are p regular $p \times q$ coverings, 1 that does not skip or twist and $p-1$ that skip but do not twist. If $q \mid p-1$, then there are q regular $p \times q$ coverings, 1 that does not skip or twist and $q-1$ that twist but do not skip. If $p \nmid q-1$ and $q \nmid p-1$, then there is 1 regular $p \times q$ covering and it does not skip or twist.*

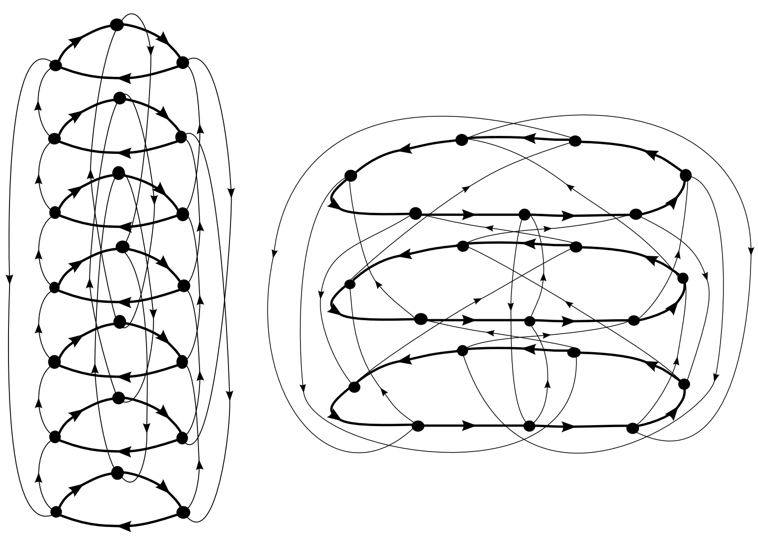

FIGURE 9. A 3×7 covering that skips and a 7×3 covering that twists

4.2. **Normal subgroups and quotient groups.** For normal subgroups of certain forms, it is helpful to consider the quotient group of F(2) over the subgroup. Results from group theory, such as the Sylow Theorems, can then be applied to determine whether such subgroups actually exist. In particular, we will use this approach to study the normal subgroups of index pq which correspond to $p \times p$ coverings, where p and q are distinct primes.

a and b haver order p, which means that p is the smallest integer r such that a^r is a loop and such that b^r is a loop. This means that the corresponding subgroup contains a^p and b^p but no smaller powers of a or b. When the quotient is taken, we have that p is the smallest integer r such that $a^r = 1$ and such that $b^r = 1$. Therefore the subgroup of the quotient group generated by a, $< a >$, and the subgroup generated by b, $< b >$, both have order p.

Consider an a-cycle. If a b edge were to connect two vertices on the same a-cycle, then there would be a word of the form $a^m b^{-1}$ that would be a loop at one of the vertices. Since we are assuming the space is regular, this means that this word must be a loop at all vertices and therefore all b edges connect vertices on the same a-cycle. This is impossible since the space would then be unconnected. Therefore b edges must connect vertices that belong to different a-cycles, which means that words of the form $a^m b^{-1}$ cannot be loops.

If $a^m b^{-1}$ is not a loop in the covering space, then $a^m b^{-1}$ is not a member of the subgroup to which that covering space corresponds and is therefore not trivial in the quotient group of F(2) over the subgroup. This implies that $a^m \neq b$ for all m and therefore $b \notin < a >$ and $< a > \neq < b >$. This means that any $p \times p$ covering must correspond to a quotient group that contains at least two distinct subgroups of order p.

Since the subgroups we are interested in have index pq in $F(2)$, when we take the quotient of $F(2)$ over one of these subgroups, we obtain a group of order pq. p and q are assumed to be distinct primes, therefore a subgroup of order p in the quotient group is a Sylow p-subgroup. The Third Sylow Theorem states that the number, n_p, of Sylow p-subgroups in a group of order pq satisfies the following conditions [6]:

- $n_p \mid q$
- $n_p \equiv 1 \pmod p$

Since q is prime, $n_p \mid q$ implies that n_p is 1 or q. We already know that the quotient groups we are considering have at least two Sylow p- subgroups, $< a >$ and $< b >$, so n_p cannot be 1. Therefore n_p must be q. But the second condition implies that $q \equiv 1 \pmod p$, which is true only when $p \mid q - 1$. This means that if $p \nmid q - 1$ then we have a contradiction and therefore no such quotient group and therefore no such subgroup of index pq can exist. This proves the following lemma:

Lemma 4.7. *Let p and q be primes, not necessarily distinct and consider regular pq-coverings. If $p \nmid q - 1$, then there are no regular $p \times p$ coverings.*

4.3. **Counting the normal subgroups of particular indices.**

Theorem 4.8. *$F(2)$ has $p + 1$ normal subgroups of index p, where p is prime.*

Proof. Each normal subgroup of index p is represented by a regular covering of degree p and the correspondence is 1 to 1; therefore it suffices to count the regular p-coverings of the figure eight space. Since the orders of the generators must divide the degree of the covering and p is prime, there are two possible orders for the generators, 1 and p. Therefore, we can divide the possible regular p- coverings into the following cases:

(1) 1×1 **coverings:** These could not possibly be connected, therefore there are no such regular coverings.
(2) $1 \times p$ **coverings:** There is a unique way to arrange p undistinguished vertices such that b has order p. There is also a unique way to arrange the a edges so that each is a loop. Since each of the vertices of this covering are indistinct from the others, it is regular. Therefore there is one $1 \times p$ covering.
(3) $p \times 1$ **and** $p \times p$ **coverings:** By Lemma 4.4, there are p regular coverings such that a has order p.

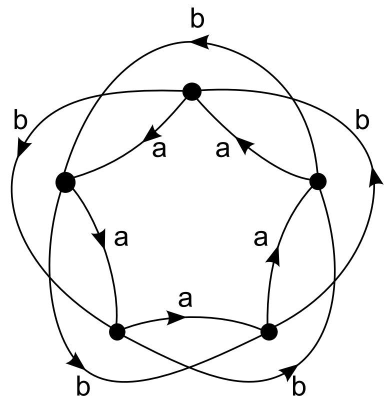

FIGURE 10. A 5×5 covering

Summing over all the possible forms of a regular p- covering, we find that there are $p+1$ regular p- coverings. Because of the direct correspondence between regular coverings and normal subgroups, this implies that there are $p+1$ normal subgroups of $F(2)$ of index p when p is prime. □

Theorem 4.9. *$F(2)$ has p^2+p+1 normal subgroups of index p^2, where p is prime.*

Proof. As in Theorem 4.8, it suffices to count the regular p^2-coverings and we can divide the possible regular p^2-coverings into the following cases:

(1) 1×1 **and** $1 \times p$ **and** $p \times 1$ **coverings:** These could not possibly be connected, therefore there are no such regular coverings.
(2) $p^2 \times 1$ **and** $p^2 \times p$ **and** $p^2 \times p^2$ **coverings:** By Lemma 4.4, there are p^2 regular coverings such that a has order p^2.
(3) $1 \times p^2$ **and** $p \times p^2$ **coverings:** Just as there are p^2 regular coverings such that a has order p^2, there are p^2 regular coverings such that b has order p^2. In some of those coverings, however, a also has order p^2 and these coverings should not be counted twice; therefore we must count them and subtract them from the total number of regular coverings such that b has order p^2. Using the numbering of the vertices established in Lemma 4.4, let vertex i be the terminal point of the a edge starting at vertex 0. Since the word a^j beginning at vertex 0 ends at vertex $ij \pmod{p^2}$, a^j is a loop if and only if $ij \equiv 0 \pmod{p^2}$. This implies that a has order p^2 if and only if p^2 is the smallest positive integer k such that $ik \equiv 0 \pmod{p^2}$, which is equivalent to saying that i and p^2 are relatively prime. There are $\phi(p^2) = p(p-1)$ such i in $\mathbb{Z}/p^2\mathbb{Z}$,

wher! e ϕ is the Euler phi function. Therefore in $p(p-1)$ of the p^2 regular coverings where b has order p^2, a also has order p^2. This means that there are p regular $1 \times p^2$ and $p \times p^2$ coverings.

(4) $p \times p$ **coverings:** Coverings of this type are discussed in the section on twisting and skipping. Since p cannot possibly divide $p-1$, by Lemma 4.6 there is 1 regular $p \times p$ covering.

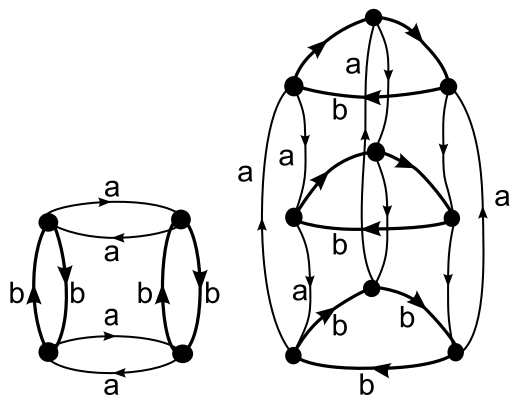

FIGURE 11. A 2×2 covering and a 3×3 covering

Summing over all the possible forms of a regular p^2- covering, we find that there are p^2+p+1 regular p^2-coverings. Because of the direct correspondence between regular coverings and normal subgroups, this implies that there are p^2+p+1 normal subgroups of $F(2)$ of index p^2 when p is prime. □

Theorem 4.10. *$F(2)$ has $pq+p+q+1$ normal subgroups of index pq, where p and q are distinct primes, $p < q$, and $p \nmid q-1$.*

Proof. As in Theorem 4.8, it suffices to count the regular pq-coverings and we can divide the possible regular pq-coverings into the following cases:

(1) 1×1**,** $1 \times p$**,** $1 \times q$**,** $p \times 1$ **and** $q \times 1$ **coverings:** These could not possibly be connected, therefore there are no such regular coverings.

(2) $pq \times 1$**,** $pq \times p$**,** $pq \times q$**, and** $pq \times pq$ **coverings:** By Lemma 4.4, there are pq regular coverings such that a has order pq.

(3) $1 \times pq$**,** $p \times pq$**, and** $q \times pq$ **coverings:** Just as there are pq regular coverings such that a has order pq, there are pq regular coverings such that b has order pq. As in Theorem 4.9, we must avoid counting those coverings where both a and b have order pq twice; therefore we must count them and subtract them from the total number of regular coverings such that b has order pq. Using the numbering of the vertices established in Lemma 4.4, let vertex i be the terminal point of the a edge starting at vertex 0. Since the word a^j beginning at vertex 0 ends at vertex $ij \pmod{pq}$, a^j is a loop if and only if $ij \equiv 0 \pmod{pq}$. This implies that a has order pq if and only if pq is the smallest positive integer k such that $ik \equiv 0 \pmod{pq}$, which is equivalent to saying that i and pq are relatively prime. There are $\phi(pq) = (p-1)(q-1)$ such i in $\mathbb{Z}/pq\mathbb{Z}$. ! Therefore in $(p-1)(q-1)$ of the pq regular coverings where b has order

pq, a also has order pq. This means that there are $p+q-1$ regular $1 \times pq$, $p \times pq$, and $q \times pq$ coverings.

(4) $p \times p$ **coverings:** $p \nmid q-1$, therefore by Lemma 4.7, there are no $p \times p$ coverings.

(5) $p \times q$ **coverings:** Coverings of this type are discussed in the section on twisting and skipping. Since $q > p$, q does not divide $p-1$, and we have assumed that p does not divide $q-1$; therefore, by Lemma 4.6 there is 1 regular $p \times q$ covering.

(6) $q \times p$ **coverings:** Since $q \nmid p-1$ and $p \nmid q-1$, by Lemma 4.6 there is 1 regular $q \times p$ covering.

(7) $q \times q$ **coverings:** Since $q > p$, $q \nmid p-1$; therefore, by Lemma 4.7, there are no $q \times q$ coverings.

Summing over all the possible forms of a regular pq- covering, we find that there are $pq+p+q+1$ regular pq-coverings. Because of the direct correspondence between regular coverings and normal subgroups, this implies that there are $pq+p+q+1$ normal subgroups of $F(2)$ of index pq when p and q are distinct primes, $p < q$, and $p \nmid q-1$. □

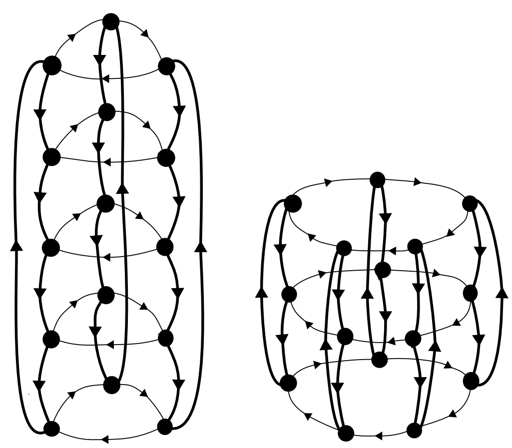

Figure 12. A 5×3 covering and a 3×5 covering

Theorem 4.11. *$F(2)$ has $3(p+2)$ normal subgroups of index $2p$, where p is an odd prime.*

Proof. As in Theorem 4.8, it suffices to count the regular $2p$-coverings and we can divide the possible regular $2p$-coverings into the following cases:

(1) 1×1**,** 1×2**,** $1 \times p$**,** 2×1 **and** $p \times 1$ **coverings:** These could not possibly be connected, therefore there are no such regular coverings.

(2) $2p \times 1$**,** $2p \times 2$**,** $2p \times p$**, and** $2p \times 2p$ **coverings:** By Lemma 4.4, there are $2p$ regular coverings such that a has order $2p$.

(3) $1 \times 2p$**,** $2 \times 2p$**, and** $p \times 2p$ **coverings:** Just as there are $2p$ regular coverings such that a has order $2p$, there are $2p$ regular coverings such that b has order $2p$. As in Theorem 4.9, we must avoid counting those coverings where both a and b have order $2p$ twice; therefore we must count them and subtract them from the total number of regular coverings such that b has order $2p$. Using the numbering of the vertices established in Lemma 4.4, let vertex i be the terminal point of the a edge starting at

vertex 0. Since the word a^j beginning at vertex 0 ends at vertex $ij \pmod{2p}$, a^j is a loop if and only if $ij \equiv 0 \pmod{2p}$. This implies that a has order $2p$ if and only if $2p$ is the smallest positive integer k such that $ik \equiv 0 \pmod{2p}$, which is equivalent to saying that i and $2p$ are relatively prime. There are $\phi(2p) = p - 1$ such i in $\mathbb{Z}/2p\mathbb{Z}$. Theref! ore in $p-1$ of the $2p$ regular coverings where b has order $2p$, a also has order $2p$. This means that there are $p+1$ regular $1 \times 2p$, $2 \times 2p$, and $p \times 2p$ coverings.

(4) 2×2 **coverings:** Consider the $2p$-covering formed by placing $2p$ vertices in a circle, numbering them v_0 to v_{2p-1} as we travel clockwise around the circle (with v_0 also referred to as v_2p when necessary), and placing p a edges such that they start at v_{2n} and end at v_{2n+1} and p a edges such that they start at v_{2n+1} and end at v_{2n} for $0 \leq n < p$ and then placing p b edges such that they start at v_{2n-1} and end at v_{2n} and p b edges such that they start at v_{2n} and end at v_{2n-1} for $1 < n \leq p$. Both a and b have order 2 in this covering, making it a 2×2 covering. Any even numbered point v_{2n} can be taken to the base point v_0 by the transformation $v_i \to v_{i-2n \pmod{2p}}$ and the above rules on placement of a and b edges will still hold. Any odd numbered point v_{2n-1} can be taken to the base point v_0 by the transformation $v_{2n-1-i \pmod{2p}}$ and the above rules on placement will also still hold. Therefore this is a regular 2×2 covering.

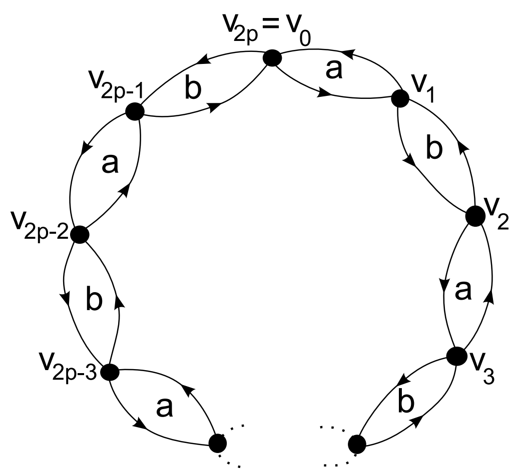

FIGURE 13. A 2×2 covering

Suppose there was another, distinct 2×2 covering. Pick an initial vertex and label it v_0. Travel along the a edge beginning at v_0 and label the terminal vertex v_1, then travel along the b edge beginning at v_1 and label the terminal vertex v_2. Continue in this manner, alternating between a and b edges until v_0 is reached again. Let n be the number of vertices that were reached during this process. Let v_i be one of these vertices and let i be even. According to our numbering process, the a edge arriving at v_i must have come from $v_{i+1 \pmod{n}}$ and the b edge leaving v_i must arrive at $v_{i-1 \pmod{n}}$. Since a and b are assumed to have order 2, the a edge leaving v_i must arrive at $v_{i+1 \pmod{n}}$ and the b edge arriving at v_i must have come from $v_{i-1 \pmod{n}}$. This accounts for all edges arriving at or leaving from v_i where i is even. Let v_j be one of these vertices and let j be! odd. According to our numbering process, the a edge arriving at v_j must have come from $v_{j-1 \pmod n}$ and the b edge leaving v_j must arrive at $v_{j+1 \pmod n}$. Since a and b are assumed to have order 2, the a edge leaving v_j must arrive at $v_{j-1 \pmod n}$ and the b edge arriving at v_j must have come from $v_{j+1 \pmod n}$. This accounts for all edges arriving at or leaving from v_j where j is odd. Therefore, no numbered vertex is connected to an unnumbered vertex. Since the covering must be connected, $n = 2p$. But this gives the same covering as the one given earlier and depicted in Figure 13. Therefore there is only one 2×2 covering.

(5) $2 \times p$ **coverings:** Coverings of this type are discussed in the section on twisting and skipping. Since p is odd, 2 divides $p-1$; therefore, by Lemma 4.6 there are 2 regular $2 \times p$ covering.
(6) $p \times 2$ **coverings:** Since $2 \mid p-1$, by Lemma 4.6 there are 2 regular $p \times 2$ covering.
(7) $p \times p$ **coverings:** Since $p > 2$, $p \nmid 2-1$; therefore, by Lemma 4.7, there are no $p \times p$ coverings.

Summing over all the possible forms of a regular $2p$- covering, we find that there are $3(p+2)$ regular $2p$- coverings. Because of the direct correspondence between regular coverings and normal subgroups, this implies that there are $3(p+2)$ normal subgroups of $F(2)$ of index $2p$ when p is an odd prime. ☐

Theorem 4.12. *$F(2)$ has $4(p+3)$ normal subgroups of index $3p$, where p is a prime such that $3 \mid p-1$.*

Proof. As in Theorem 4.8, it suffices to count the regular $3p$-coverings and we can divide the possible regular $3p$-coverings into the following cases:

(1) 1×1, 1×3, $1\times p$, 3×1 **and** $p\times 1$ **coverings:** These could not possibly be connected, therefore there are no such regular coverings.
(2) $3p \times 1$, $3p \times 2$, $3p \times p$, **and** $3p \times 3p$ **coverings:** By Lemma 4.4, there are $3p$ regular coverings such that a has order $3p$.
(3) $1 \times 3p$, $3 \times 3p$, **and** $p \times 3p$ **coverings:** Just as there are $2p$ regular coverings such that a has order $3p$, there are $3p$ regular coverings such that b has order $3p$. As in Theorem 4.9, we must avoid counting those coverings where both a and b have order $3p$ twice; therefore we must count them and subtract them from the total number of regular coverings such that b has order $3p$. Using the numbering of the vertices established in Lemma 4.4, let vertex i be the terminal point of the a edge starting at vertex 0. Since the word a^j beginning at vertex 0 ends at vertex $ij \pmod{3p}$, a^j is a loop if and only if $ij \equiv 0 \pmod{3p}$. This implies that a has order $3p$ if and only if $3p$ is the smallest positive integer k such that $ik \equiv 0 \pmod{3p}$, which is equivalent to saying that i and $3p$ are relatively prime. There are $\phi(3p) = 2(p-1)$ such i in $\mathbb{Z}/3p\mathbb{Z}$. The! refore in $2(p-1)$ of the $3p$ regular coverings where b has order $3p$, a also has order $3p$. This means that there are $p+2$ regular $1 \times 3p$, $3 \times 3p$, and $p \times 3p$ coverings.
(4) 3×3 **coverings:** This section will be completed later.
(5) $3 \times p$ **coverings:** Coverings of this type are discussed in the section on twisting and skipping. Since 3 divides $p-1$, by Lemma 4.6 there are 3 regular $3 \times p$ covering.
(6) $p \times 3$ **coverings:** Since $3 \mid p-1$, by Lemma 4.6 there are 3 regular $p \times 3$ covering.

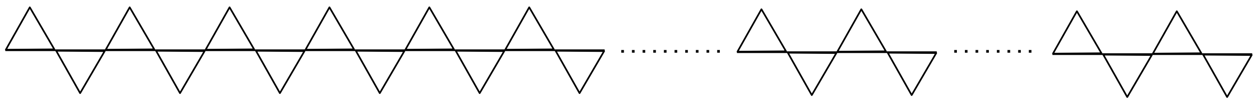

FIGURE 14. A 3×3 covering

(7) $p \times p$ **coverings:** Since $p > 3$, $p \nmid 3 - 1$; therefore, by Lemma 4.7, there are no $p \times p$ coverings.

Summing over all the possible forms of a regular $3p$- covering, we find that there are $4(p+3)$ regular $3p$- coverings. Because of the direct correspondence between regular coverings and normal subgroups, this implies that there are $4(p+3)$ normal subgroups of $F(2)$ of index $3p$ when p is an odd prime. □

5. Enumerating normal subgroups of F(r)

Our enumeration of normal subgroups of F(2) provides a basis for the enumeration of normal subgroups of F(r).

Definition 5.1. *A regular covering of the wedge of r circles is a* $k_1 \times k_2 \times ... \times k_r$ covering *if a_i has order k_i for all $1 \leq i \leq r$.*

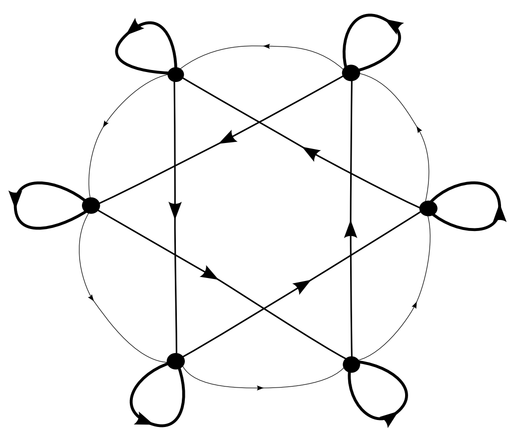

FIGURE 15. A $6 \times 3 \times 1$ covering of degree 6

Once we have $r > 2$, it remains useful to consider the generators pairwise.

Definition 5.2. *We consider an arrangement of a_i edges to be* regular relative to an arrangement of a_j edges *if the (not necessarily connected) covering of the figure eight space defined by these arrangements is regular. In a covering where this is true we say that a_i and a_j are* pairwise regular*. If the covering of the figure eight space defined by the arrangements of a_i and a_j edges is connected, we say that a_i and a_j are* pairwise connected*.*

It is easy to see that in a given covering of the wedge of r circles, if there are any two generators which are pairwise connected, the covering is connected, and if there are any two generators which are not pairwise regular, the covering is not regular.

Lemma 5.3. *When in an n-covering of the wedge of r circles some generator a_i has order n and is pairwise regular with every other generator, the covering space is regular.*

Proof. Let a_i have order n and be pairwise regular with a_j for all $j \neq i$, $1 \leq j \leq r$. Then for each j the covering of the figure eight space defined by the arrangement of the a_i and a_j edges is regular, so we can think of it as one of the coverings described in Lemma 4.4. In fact, we can allow the vertices in the covering of the wedge of r circles to be labeled by choosing one vertex and labeling it 0 and then labeling the rest of the vertices 1 through $n-1$ according to the order in which they are reached by traveling along a_i edges from 0. We then notice that, as in Lemma 4.4, the a_j edge leaving vertex 0 enters some vertex k_j and the constraints of regularity then impose that the a_j edge leaving vertex l must enter vertex $l + k_j \pmod{n}$. Then at any given vertex l, the a_1 edge leaving l enters vertex $l + k_1 \pmod{n}$, the a_2 edge leaving l enters vertex $l + k_2 \pmod{n}$, and so on up to the a_r edge ! which enters vertex $l + k_r \pmod{n}$. ($k_i = 1$.) Each vertex is then clearly symmetric to each other vertex, and so the covering is regular. □

5.1. Counting the normal subgroups of particular indices.

Theorem 5.4. *There are*

$$\sum_{k=0}^{r-1} p^k = \frac{p^r - 1}{p - 1}$$

normal subgroups of $F(r)$ of index p where p is prime.

Proof. It is enough to consider the regular p-coverings of the wedge of r circles, since there is a one-one correspondence between these and the normal subgroups of $\mathrm{F}(r)$ of index p.

By Lemma 4.3, in such a covering the order of each generator must divide p, and thus must be either 1 or p. If the order of every generator is 1, then the covering will obviously not be connected, so there must be at least one generator a_i with order p. By Lemma 5.3, it is enough to show that a_i is pairwise regular with every other generator in order to see that the covering as a whole is regular. By Lemma 4.4, there are p ways to construct a regular covering of the figure eight space with a_i of index p and one other generator of unknown index. Now we can begin to count the possible regular p- coverings of the wedge of r circles. In order to avoid double-counting, we will sum over the first generator from $\{a_1, ..., a_r\}$ to have index p. If we call this generator a_i, then there is only one possibility for the generators before and including a_i: those generators appearing in the list before a_i must have order ! 1 and there is only one way for this to happen, and a_i must have order p and there is also only one way for this to happen. The generators that appear after a_i may have any order so long as taken pairwise with a_i they are regular: then each such generator has p possible configurations in order to be pairwise regular with a_i and each of these choices yields a distinct regular covering of the wedge of r circles. So we have

$$\sum_{i=1}^{r} p^{r-i} = \sum_{k=0}^{r-1} p^k = \frac{p^r - 1}{p - 1}$$

distinct regular p-coverings of the wedge of r circles. □

Theorem 5.5. *There are*

$$\sum_{k=1}^{r} p^{2r-k-1} + \sum_{k=1}^{r-1}\sum_{j=k+1}^{r} p^{j-k-1}(2p-1)^{r-j} = \frac{-4p^r + 2p^{r-1} + 2p^{2r} - 2p^{2r-1} + 1 + (2p-1)^r}{2(p-1)^2}$$

normal subgroups of $F(r)$ of index p^2 where p is prime.

Proof. Again, it is enough to consider the regular p^2- coverings of the wedge of r circles.

By Lemma 4.3, a given generator may have order 1, p, or p^2. If all of the generators have order 1, then the covering is clearly not connected. We divide the possible coverings into two cases, that where the generator of highest order has order p^2 and that where the generator of highest order has order p.

If some generator a_k has order p^2, then by Lemma 5.3 in order for the covering to be regular it is enough for a_k to be pairwise regular with every other generator. Furthermore, the covering is connected by a_k alone. Then to avoid double- counting, we take a_k to be the first generator of $\{a_1, ..., a_r\}$ to have order p^2. There is one possible arrangement of a_k that has order p^2 when the vertices, prior to the imposition of that arrangement, are undistinguished. We note that the generators $\{a_1, ..., a_{k-1}\}$ may each have order either 1 or p and must each be pairwise regular with a_k. From Theorem 4.9 we see that there are p regular $1 \times p^2$ and $p \times p^2$ coverings of the figure eight space, and thus p choices for the configuration of each element of $\{a_1, ..., a_{k-1}\}$. Finally, the generators $\{a_{k+1}, ..., a_r\}$ are subject only to the condition that they be pairwise regular with a_k and need! not have any particular order, so there are p^2 possible configurations for each of these generators by Lemma 4.4. Then summing over the choice of a_k we find that there are

$$\sum_{k=1}^{r} p^{k-1}(p^2)^{r-k} = \sum_{k=1}^{r} p^{2r-k-1}$$

regular p^2-coverings of the wedge of r circles where at least one generator has order p^2.

If no generator has order p^2, then clearly at least two generators must have order p. Call these generators a_k and a_j. They must be pairwise regular. From the discussion preceding Lemma 4.6, we see that either each a_j-cycle has only one a_k-cycle which it visits, and a_k and a_j are not pairwise connected, since they do not connect the space any more than a_k alone did, or each a_j-cycle visits each a_k-cycle exactly once and a_k and a_j are pairwise connected. If a_k and a_j are not pairwise connected, there must be some other pair of generators that is, so without loss of generality we will suppose that a_k and a_j are pairwise connected. Then by Lemma 4.6, since $p \nmid p-1$, there is exactly one possible arrangement of the a_j edges that is regular with respect to a_k. The other generators each have either order 1 or order p. If a generator has order 1, it leaves the regularity of the covering un! changed. If a generator a_i other than a_k and a_j has order p, then we must consider how to arrange the a_i edges so that the covering remains regular.

We label the points as in Figure 7, where the a_k-cycles are in a stack connected by the a_j-cycles and some arbitrary vertex is $v_{0,0}$. If the a_i edge leaving $v_{0,0}$ enters some v_{0,l_i} then the a_i edge leaving $v_{0,m}$ must enter $v_{0,m+l_i}$ (mod p) in order to ensure pairwise regularity with a_k and the a_i edge leaving $v_{m,0}$ must enter v_{m,l_i} (mod p) in order to ensure pairwise regularity with a_j. In general, then, the a_i edge leaving $v_{m,n}$ enters $v_{m,n+l_i}$ (mod p) and the

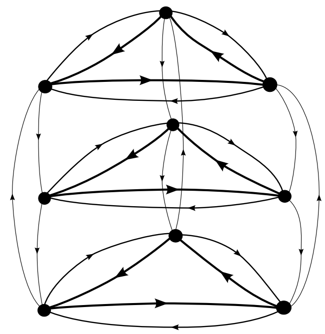

FIGURE 16. A $3 \times 3 \times 3$ covering of degree 9

covering is regular. If the a_i edge leaving $v_{0,0}$ enters some $v_{l_i,0}$ then by a similar argument the a_i edge leaving $v_{m,n}$ enters $v_{m+l_i,n}$ (mod p) and the covering is regular. If on the other hand the a_i edge leaving $v_{0,0}$ enters $v_{l_i,l_i'}$ with $l_i \neq 0$ and $l_i' \neq 0$ then by Lemma 4.6 a_i and a_k are not pairwise regular. Then we have exhausted the possibilitie! s for arranging the a_i edges in a manner that preserves regularity.

Now we count the possible regular coverings with no generator of order p^2. To avoid double-counting, we will let a_k be the first generator from $\{a_1, ..., a_r\}$ to have order p and a_j be the first generator from $\{a_1, ..., a_r\}$ to be pairwise connected with a_k. Obviously, $j > k$. a_k can be any generator from $\{a_1, ..., a_{r-1}\}$, allowing at least one choice for a_j. Once we have a_k, there is one choice for the configuration of the edges from the set $\{a_1, ..., a_k\}$, since all of the generators before a_k have order 1 and a_k simply arranges undistinguished points into p-cycles. Then we can choose a_j from $\{a_{k+1}, ..., a_r\}$, and we will have one choice for the arrangement of the a_j edges by Lemma 4.6. Any generator a_i from the set $\{a_{k+1}, ..., a_{j-1}\}$ can have order 1 or p, but since we know that it is not pairwise connected with a_k we know that the edge a_i leaving $v_{0,0}$ enters some !v_{0,l_i} (with l_i possibly equal to 0). Then there are p choices for the arrangement of the a_i edges. Any generator a_i from the set $\{a_{j+1}, ..., a_r\}$ can have order either 1 or p and has the full complement of possible arrangements from the preceding paragraph, or $2p-1$ possible arrangements. (The a_i edge leaving $v_{0,0}$ enters some v_{0,l_i} or some $v_{l_i,0}$, but we are careful not to count its entering $v_{0,0}$ twice.) Then the number of possible regular coverings with no generator of order p^2 is

$$\sum_{k=1}^{r-1} \sum_{j=k+1}^{r} p^{j-k-1}(2p-1)^{r-j}$$

and the total number of regular p^2-coverings of the wedge of r circles is

$$\sum_{k=1}^{r} p^{2r-k-1} + \sum_{k=1}^{r-1} \sum_{j=k+1}^{r} p^{j-k-1}(2p-1)^{r-j} = \frac{-4p^r + 2p^{r-1} + 2p^{2r} - 2p^{2r-1} + 1 + (2p-1)^r}{2(p-1)^2}$$

□

Theorem 5.6. *There are*

$$\sum_{k=1}^{r}(pq)^{r-k}(p+q-1)^{k-1}+\sum_{k=1}^{r-1}\sum_{j=k+1}^{r}p^{j-k-1}(p+q-1)^{r-j}+\sum_{k=1}^{r-1}\sum_{j=k+1}^{r}q^{j-k-1}(p+q-1)^{r-j}$$
$$=\frac{(pq)^r-p^r-q^r+1}{(p-1)(q-1)}$$

normal subgroups of $F(r)$ of index pq where p and q are prime, $p<q$ and $p\nmid q-1$.

Proof. We will consider the regular pq-coverings of the wedge of r circles, since these are in one-one correspondence with the normal subgroups of $\mathrm{F}(r)$ of index pq.

First we consider the case where some generator a_k has order pq. a_k alone connects the space, and in order for the covering to be regular it is enough for each generator to be pairwise regular with a_k by Lemma 5.3.

(This section will be completed later.) □

6. Conclusion

Appendix A. C++ code that generates normal subgroups of index n

A.1. Matrix.h.

```
// Matrix.h
// NormalSubgroup

// Created by Samantha Nieveen on 7/11/06.
// Oregon State University REU Program

#ifndef OSU_REU_2006_NORMAL_GUARD
#define OSU_REU_2006_NORMAL_GUARD

#include <iostream>
#include <fstream>

class Matrix { //A class for the matrix representations
of our n-coverings
  private:
    int **mtrx;          //a pointer to the matrix
    int dim;  //a variable that holds the dimension of
the matrix,
              //which is the index of the corresponding
subgroup
    int lastColumn;     //first non-distinguished
column
    int lastCompRow;    //last row that has both a 1
and a 2 in it
    int letter; //a variable that stores which
```

```
generator is
                //next to be added to the matrix. 1 =
a, 2 = b.
  public:
    //Constructors
    Matrix();
    Matrix(int n);  //Creates an n by n matrix with all
entries 0
    Matrix(const Matrix& param);        //Copy
Constructor

    //Destructor
    ~Matrix();  //leaves mtrx null

    //overloading operators
    Matrix operator= (const Matrix& param);
    bool operator== (const Matrix& param);
    bool operator!= (const Matrix& param);

    //useful functions
    int lastCol();  //returns the number of the first
all zero column
    int lastRow();  //returns the number of the last
completed row
    void increase(int row, int col); //places the
currently selected
                                       //letter in the
matrix at row, col
    void print() const;  //displays the matrix
    void flip(int x, int y); //switches row x with row
y, and col x with
                        //col y. This preserves the
subgroup that the
                        //matrix represents but does
not necessarily
                        //preserve our special format
    void reformat(int fixed, int row, int let); //takes
a matrix and puts it
                                                  //into
our special format
    bool colLacksLet(int col); //checks to make sure
that a column in the
                              //matrix does not
already contain the current letter
```

```
    bool allZeros(int m); //checks the block of the
matrix between rows 0
                          //and m-1 and cols m+1 and
dim and returns true
                          //if it contains only zeros
    bool isConnected(); //returns true iff the matrix
                        //corresponds to a connected
covering
    bool isNormal(); //returns true if and only if the
matrix
                     //corresponds to a normal subgroup
};

#endif
```

A.2. **Matrix.cpp.**

```
// Matrix.cpp
// NormalSubgroup
// Created by Samantha Nieveen on 7/11/06.

#include "Matrix.h"
#include <iostream>

Matrix::Matrix() {
  mtrx = NULL;
  dim = 0;
  lastColumn = 1;
  lastCompRow = -1;
  letter = 1;
}

Matrix::Matrix(int n) {
  mtrx = new int*[n];
  dim = n;
    lastColumn = 1;
  lastCompRow = -1;
  letter = 1;
  for(int i=0; i<n; i++) {
    mtrx[i] = new int[n];
    for(int j=0; j<n; j++) {
      mtrx[i][j] = 0; }}
}

Matrix::Matrix(const Matrix& param) {
```

```
  dim = param.dim;
  lastColumn = param.lastColumn;
  lastCompRow = param.lastCompRow;
  letter = param.letter;
  mtrx = new int*[dim];
  for(int i=0; i<dim; i++) {
    mtrx[i] = new int[dim];
    for(int j=0; j<dim; j++) {
      mtrx[i][j] = param.mtrx[i][j]; }}
}


Matrix::~Matrix() {
  if(mtrx != NULL) {
    for(int i=0; i<dim; i++) {
      if(mtrx[i] != NULL) {
        delete[] mtrx[i];
        mtrx[i] = NULL; }}
    delete[] mtrx;
    mtrx = NULL; }
  dim = 0;
  lastColumn = 0;
}



Matrix Matrix::operator= (const Matrix& param) {
  dim = param.dim;
  lastColumn = param.lastColumn;
  lastCompRow = param.lastCompRow;
  letter = param.letter;
  for(int p=0; p<dim; p++) {
    for(int q=0; q<dim; q++) {
      mtrx[p][q] = param.mtrx[p][q]; }}
  return *this;
}


bool Matrix::operator== (const Matrix& param) {
  if(dim = param.dim) {
    for(int i=0; i<dim; i++) {
      for(int j=0; j<dim; j++) {
        if(mtrx[i][j] != param.mtrx[i][j]) {
          return false; }}}
```

```
    return true;
  } else {
    return false; }
}

bool Matrix::operator!= (const Matrix& param) {
  return !(*this==param);
}

int Matrix::lastCol() {
  return std::min(lastColumn, dim-1);
}

int Matrix::lastRow() {
  return lastCompRow;
}

void Matrix::increase(int row, int col) {
  if((row<dim) && (col<dim)) {
    mtrx[row][col] += letter;
  } else {
    std::cout << "error"; }
  if(col >= lastColumn) {
    lastColumn = col+1; }
  if(letter == 1) {
    letter += 1;
  } else {
    letter -= 1;
    lastCompRow++; }
}

void Matrix::print() const {
  for(int i=0; i<dim; i++) {
    for(int j=0; j<dim; j++) {
      std::cout << mtrx[i][j] << "  "; }
    std::cout << std::endl; }
  std::cout << std::endl;
}


void Matrix::flip(int x, int y) {
  int* temp = mtrx[y];      //this flips the yth row
with the xth row
  mtrx[y] = mtrx[x];
```

```
  mtrx[x] = temp;
  int j=0;                       //this flips
the yth column with the xth column
  for(int i=0; i<dim; i++) {
    j=mtrx[i][y];
    mtrx[i][y] = mtrx[i][x];
    mtrx[i][x] = j; }
}

void Matrix::reformat(int fixed, int row, int let) {
  bool done = false;
  int i=fixed+1;
  while((!done) && (i != dim)) {
    if((mtrx[row][i] == let) || (mtrx[row][i] == 3)) {
      flip(fixed+1, i);
      fixed++;
      done = true; }
    i++; }
  let = (let % 2) +1;
  if(let == 1) {
    row++; }
  if(fixed != dim-1) {
    reformat(fixed, row, let); }
}

bool Matrix::colLacksLet(int col) {
  for(int i=0; i<=lastCompRow; i++) {
    if((mtrx[i][col]==letter) || (mtrx[i][col]==3)) {
      return false; }}
  return true;
}

bool Matrix::allZeros(int m) {
  for(int i=m+1; i<dim; i++) {
    for(int j=0; j<=m; j++) {
      if(mtrx[j][i]!=0) {
        return false; }}}
  return true;
}

bool Matrix::isConnected() {
  for(int i=0; i<dim-1; i++) {
    if(allZeros(i)) {
      return false; }}
```

```
  return true;
}

bool Matrix::isNormal() {
  Matrix temp (dim);
  for(int i=1; i<(dim/2)+1; i++) {
    temp = *this;
    temp.flip(0, i);
    int letter=1;
    if(temp.mtrx[0][0] == 1) {
      letter = 2; }
    temp.reformat(0, 0, letter);
    if(temp != *this) {
      return false; }}
  return true;
}
```

A.3. **main.cpp.**

```
#include <iostream>
#include <stack>
#include <fstream>
#include "Matrix.h"
using namespace std;

int main () {
  cout << "Choose an index: ";
  int n;
  cin >> n;
  cout << endl;

  int count = 0;
  cout<<"The normal subgroups of index "<< n <<" are
represented by:"<<endl;
  stack<Matrix> s;
  Matrix zeros (n);     //this is the initial,
empty matrix
  s.push(zeros);

  while(!s.empty()) {
    Matrix current = s.top();
    s.pop();
    if(current.lastRow()==n-1) {    //checks to see if
the matrix is complete
      if(current.isConnected() && current.isNormal()) {
```

```
//checks to make
        current.print();
                   //sure the matrix is
connected
        count++;                             //and
normal before counting it
      }
    } else { //if it is not complete, it creates it's
daughter matrices
             //and adds them to the stack
      for(int i=0; i<current.lastCol()+1; i++) {
        if(current.colLacksLet(i)) {
          Matrix next (n);
          next = current;
          next.increase(current.lastRow()+1, i);
          s.push(next);
  }}}}
  cout <<"There are "<< count <<" normal subgroups of
index" << n <<".";

  return 0;
}
```

References

[1] Marshall Hall Jr., *Subgroups of finite index in free groups*, Canadian J. Math. **1** (1949), 187–190.

[2] Ilya Kapovich and Alexei Myasnikov, *Stallings foldings and subgroups of free groups*, J. Algebra **248** (2002), no. 2, 608–668.

[3] Jin Ho Kwak and Jaeun Lee, *Enumeration of graph coverings and surface branched coverings*, Lecture Note Series, vol. 1, Com^{2}Mac-KOSEF, Korea, 2001. See Chapter 3.

[4] James R. Munkres, *Topology: a first course*, Prentice-Hall, Englewood Cliffs, New Jersey, 1975.

[5] Harold M. Stark, *An Introduction to Number Theory*, Markham Publishing Company, Chicago, 1970.

[6] David S. Dummit and Richard M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.

University of California- Los Angeles
E-mail address: snieveen@ucla.edu

Carleton College
E-mail address: smithal@carleton.edu