An Exploration of Integral Apollonian Circle Packings

Katherine Sanden
Summer 2007
Prof. Peter Sarnak

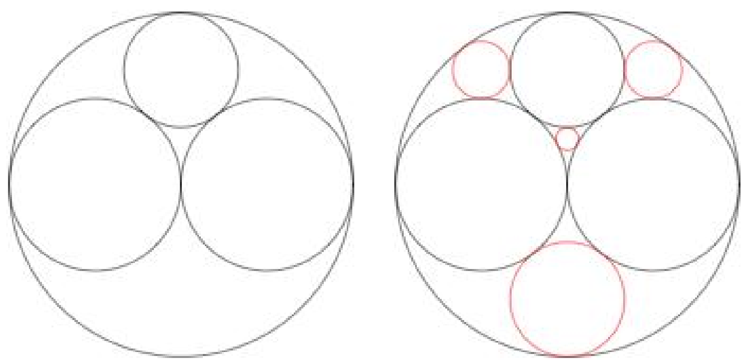
1 Background

1.1 What is an Apollonian circle packing?

Start with four mutually tangent circles in the plane. For each circle, define its *curvature* as the reciprocal of its radius. The four curvatures are then related by an equation formulated by René Descartes, a 17th century French mathematician. If four mutually tangent circles have curvatues a, b, c, and d, Descartes' equation states:

$$a^2 + b^2 + c^2 + d^2 = \frac{1}{2}(a + b + c + d)^2$$

If a set of four curvatures satisfies this equation, it is called a Descartes quadruple. After starting with such a quadruple, one can generate new Descartes quadruples. In each curvilinear triangle formed between circles, create a smaller circle tangent to the three circles surrounding it:



An *Apollonian circle packing* is formed by repeating this process recursively on the resulting curvilinear triangles (lunes).

1.2 Generating a packing

Define the *root quadruple* of a packing as the initial set of curvatures, i.e. the curvatures of the largest four circles. By convention, a root quadruple (a, b, c, d) is arranged so that $a \leq b \leq c \leq d$. Given a root quadruple (a_1, b, c, d), how does one produce the smaller circles that form the packing? Generating a new curvature (and thereby creating a new circle) corresponds to exchanging one root of Descartes' equation for another. For example, suppose our goal is to produce a new circle (besides the one with curvature a_1) that is tangent to the three circles with curvatures b, c, and d. We re-write Descartes' equation as a quadratic equation in a:

$$a^2 - 2(b + c + d)a + [b^2 + c^2 + d^2 - 2(bd + bc + cd)] = 0. \quad (1)$$

In a polynomial of the general form $x^2 + Bx + C$, we know that if r_1 and r_2 are its roots, then the polynomial can be factored into $(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1r_2$, meaning r_1 and r_2 must sum to $-B$. Therefore, in (1), if a_1 and a_2 are two roots of the quadratic equation, we must have

$$a_1 + a_2 = 2(b + c + d).$$

We use this information to produce a new circle, with curvature a_2. With this new curvature comes a new quadruple: (a_2, b, c, d). To obtain the new quadruple from the original root quadruple, a_1 gets replaced by $2(b + c + d) - a_1$. Viewing both quadruples as 4×1 column vectors, we can write this transformation as a 4×4 matrix, call it S_1:

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

At each generation of an Apollonian circle packing, a similar process is used to produce exactly one new circle inside each lune, so that the new circle is tangent to all three surrounding circles. Define the matrices S_1, S_2, S_3, and S_4 as:

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad S_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad S_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix}$$

Any quadruple of curvatures within a given packing can be obtained by applying a sequence of matrices to the root quadruple, where each matrix is one of S_1, S_2, S_3, and S_4. Observe that, if we apply any S_j $(1 \leq j \leq 4)$ to a vector whose entries are integers, the resulting vector will also have integer entries. Therefore, if we start with a root quadruple of integral curvatures, then each curvature throughout the packing will be integral. Such a packing is called an *integral Apollonian circle packing*, and will be the focus of this discussion.

Also note that each of S_1 through S_4 has determinant -1, and each is its own inverse:

$$S_j^2 = I \qquad (1 \leq j \leq 4)$$

Hence, the four matrices can be used, not only to generate larger curvatures from a root quadruple, but also to undo this process, i.e. to produce smaller curvatures from a given Descartes quadruple. In other words, one can use applications of S_1, S_2, S_3 and S_4 to "trace" a given quadruple back to its root quadruple. This can be done using Lagarias et al's **reduction algorithm**: given a Descartes quadruple q, where the j-th entry of q is the biggest entry, apply S_j. If the j-th entry of the resulting vector is smaller than the j-th entry of q, locate the biggest entry in the new vector and repeat this process. If applying S_j does not decrease the j-th entry, arrange the elements of q in increasing order to form q'. The root quadruple is q'.

From this reduction algorithm, we can see that a packing is completely determined by its root quadruple. For this reason, we identify packings by their root quadruples. Figure 1 displays the Apollonian packing generated by the root quadruple $(-1, 2, 2, 3)$. The largest circle, with radius 1, is pictured so that all tangent circles are on its interior. Its curvature receives a negative sign to denote that its "exterior" is taken to be its interior.

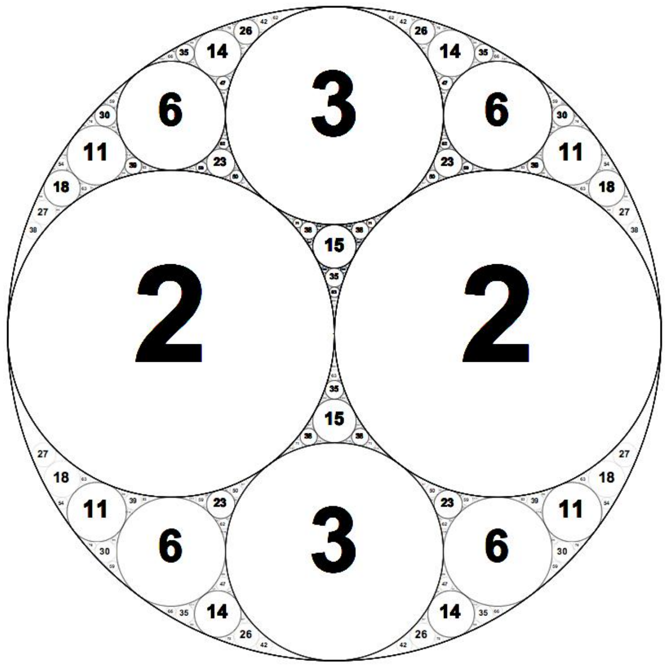


Figure 1: The integral Apollonian circle packing $(-1, 2, 2, 3)$, pictured up to five generations. Each circle is labeled with its curvature.

1.3 The Apollonian Group

One can rearrange Descartes' equation to write it as a quadratic form, called F:

$$F(a, b, c, d) = 2(a^2 + b^2 + c^2 + d^2) - (a + b + c + d)^2$$

A Descartes quadruple is therefore a set of four integers (x_1, x_2, x_3, x_4), such that $F(x_1, x_2, x_3, x_4) = 0$. Let $\mathcal{O}_F(\mathbb{Z})$ denote the orthogonal group of this quadratic form over the integers. Since $\mathcal{O}_F(\mathbb{Z})$ is the group of all matrices with integer entries that preserve the quadratic form F, $\mathcal{O}_F(\mathbb{Z})$ contains all matrices that take integral Descartes' quadruples to integral Descartes' quadruples. Let $\mathcal{A}$ denote the group generated by S_1, S_2, S_3, and S_4. $\mathcal{A}$ is a subgroup of $\mathcal{O}_F$; in fact it is the smallest subgroup of $\mathcal{O}$ containing these four matrices.

The main objective in studying integral Apollonian circle packings is to understand which integers, and in particular, which primes, will show up in a packing. This equates to understanding the group $\mathcal{A}$. Given a root quadruple, what can we say about the orbit of this quadruple under $\mathcal{A}$?

To approach this question, first we take a look at groups containing $\mathcal{A}$. Since each element of $\mathcal{O}_F$ has integer entries and determinant ± 1, $\mathcal{O}_F$ is a subgroup of $GL_4(\mathbb{Z})$, which is a subgroup of $GL_4(\mathbb{R})$. We already have a clear idea of how $GL_4(\mathbb{R})$ acts on a four-dimensional vector q. For example, the orbit of the vector $(1, 0, 0, 0)$ under $GL_4(\mathbb{R})$ is all vectors of the form (x_1, x_2, x_3, x_4), where x_1, x_2, x_3 and x_4 are real, besides the zero vector: $(0, 0, 0, 0)$. (No matrix can map the zero vector to a nonzero vector, so if a matrix M mapped a nonzero vector to zero, then M would not have an inverse. Thus we would have $\det(M) = 0$, so $M \notin GL_4(\mathbb{R})$.)

A similar statement can be said about the action of $GL_4(\mathbb{Z})$ on a vector:

Claim: The orbit of the column vector $v = (1, 0, 0, 0)^T$ under $GL_4(\mathbb{Z})$ is all vectors of the form $(x_1, x_2, x_3, x_4)^T$, where $gcd(x_1, x_2, x_3, x_4) = 1$.

Proof: First, observe that it is impossible to produce a vector $(x_1, x_2, x_3, x_4)^T$ with $gcd(x_1, x_2, x_3, x_4) > 1$, becuase: suppose we do produce such a vector. Suppose $gcd(x_1, x_2, x_3, x_4) = k$, with $k \neq 1$. We could then divide by k to obtain a vector $(y_1, y_2, y_3, y_4)^T$, with $gcd(y_1, y_2, y_3, y_4) = 1$. Then, for some matrix $M \in GL_4(\mathbb{Z})$,

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = k \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = M \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

This would imply that k divides each entry of the first column of M. Using expansion by minors down the first column of M, one sees k also divides $\det(M)$, contradicting the fact that $\det(M) = \pm 1$.

Now it remains to show that, given some vector $(x_1, x_2, x_3, x_4)^T$ with $gcd(x_1, x_2, x_3, x_4) = 1$, this vector can be obtained by applying some matrix $M \in GL_4(\mathbb{Z})$ to v. We need to find a matrix that, when applied to the vector $(1, 0, 0, 0)^T$, produces $(x_1, x_2, x_3, x_4)^T$. It is sufficient to find the inverse of this matrix, since if a matrix is in $GL_4(\mathbb{Z})$, its inverse is as well.

To find the desired matrix, we first consider a two dimensional situation: given a vector (x_1, x_2), with $gcd(x_1, x_2) = h$ ($h \in \mathbb{N}$), what matrix $A \in GL_2(\mathbb{Z})$ will map (x_1, x_2) to $(h, 0)$? In this case, we can find integers a and b such that $ax_1 + bx_2 = h$. Dividing both sides by h, we obtain

$$a\left(\frac{x_1}{h}\right) + b\left(\frac{x_2}{h}\right) = 1.$$

In choosing the entries of A, we need to satisfy $\det(A) = A_{11}A_{22} - A_{12}A_{21} = \pm 1$, so we can take $A_{11} = a$; $A_{12} = b$; $A_{21} = -\frac{x_2}{h}$; and $A_{22} = \frac{x_1}{h}$. (Note that A will still have integer entries, since h divides both x_1 and x_2.) Indeed,

$$\begin{bmatrix} a & b \\ -\frac{x_2}{h} & \frac{x_1}{h} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} h \\ 0 \end{bmatrix}.$$

This result can be used to find a 4×4 matrix that maps (x_1, x_2, x_3, x_4) (where $gcd(x_1, x_2, x_3, x_4) = 1$) to $(1, 0, 0, 0)$. Assume $gcd(x_1, x_2) = h$ and $gcd(x_3, x_4) = k$. Then we can find integers a, b, c, and d such that $ax_1 + bx_2 = h$ and $cx_3 + dx_4 = k$. We construct a block matrix $B \in GL_4(\mathbb{Z})$ of the form:

$$B = \begin{bmatrix} a & b & 0 & 0 \\ -\frac{x_2}{h} & \frac{x_1}{h} & 0 & 0 \\ 0 & 0 & c & d \\ 0 & 0 & -\frac{x_4}{k} & \frac{x_3}{k} \end{bmatrix}.$$

This matrix has determinant 1, since both 2×2 blocks on the diagonal have determinant 1. B will map (x_1, x_2, x_3, x_4) to $(h, 0, k, 0)$. We can a apply a permutation matrix S, of the form:

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

yielding the vector $(h,k,0,0)$. Since $gcd(x_1,x_2,x_3,x_4)=1$, we must have $gcd(h,k)=1$, so there exist integers m and n such that $mh+nk=1$. Thus, to obtain $(1,0,0,0)$ we multiply by one more matrix, M, where

$$M = \begin{bmatrix} m & n & 0 & 0 \\ -k & h & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

So, given any column vector w of four relatively prime integers, we know $(1,0,0,0)^T = MSBw$, where M, S, and B are in $GL_4(\mathbb{Z})$. Thus the orbit of $(1,0,0,0)$ is all quadruples of integers whose greatest common divisor is 1. □

We know far less about the Apollonian group than we do about either $GL_4(\mathbb{R})$ or $GL_4(\mathbb{Z})$, but would like to make analogous statements about the orbit of a quadruple q under the action of $\mathcal{A}$. Note that within the group $\mathcal{O}_F(\mathbb{Z})$, there is only one orbit: from any Descartes quadruple $\mathbf{x}$, we can use an element of $\mathcal{O}_F(\mathbb{Z})$ to obtain any other quadruple, $\mathbf{y}$. There are infinitely many orbits in $\mathcal{A}$, on the other hand: each root quadruple determines its own orbit, since each Apollonian packing is completely determined by its root quadruple.

1.4 Broad Objectives

The purpose of studying the group $\mathcal{A}$ is to try to answer fundamental questions about integral Apollonian circle packings, and correspondingly, about which solutions of the Diophantine equation $a^2+b^2+c^2+d^2 = \frac{1}{2}(a+b+c+d)^2$ will appear in a given orbit of $\mathcal{A}$. One such question addresses the different possible integers that appear in a packing. Given a root quadruple q, and some integer n, will n appear in the packing generated by q? If not, which integers will?

The first step in confronting this question is to look for *local obstructions* in a packing. We examine the curvatures in a packing modulo p, using various $p \in \mathbb{N}$. For some values of p, there are integers (mod p) that will never occur in certain packings. We say these integers are excluded from certain packings due to local obstructions. For instance, in the packing $(-1,2,2,3)$, there are no integers congruent to 1 (mod 3). However, not all p give rise to local obstructions; when $p=5$, for instance, there are no numbers (mod 5) that are excluded from the packing $(-1,2,2,3)$ (or any packing, for that matter).

On the other hand, some integers don't appear in certain packings, despite overcoming all local obstructions. We label these integers "bad" integers. Lagarias et al's **Strong Density Conjecture** asserts that, for any packing, there is a sufficiently large number β (depending on the packing), so that all integers greater than β, as long as they satisfy local congruences, will appear in the packing. In other words, there exists a β such that there are no "bad" integers greater than β.

The Strong Density Conjecture is crucial in understanding the different possible integers that appear in a packing. A related question is, what are the different possible primes that occur in a packing? In the next section, we develop some approaches to answering these questions.

2 A Graph of Descartes Quadruples

In connection to Lagarias et al's Strong Density Conjecture, we want to know whether or not a given integer will be excluded from a packing due to a local obstruction. We also want to understand which p will produce local obstructions (mod p) and which p won't.

To address these issues, look at the graph G formed by all Descartes quadruples. A quadruple v is a vertex of G iff v satisfies Descartes' equation. Two vertices v and w are adjacent iff $v = S_j w$ for some j

$(1 \leq j \leq 4)$. Conceptually, each edge in G corresponds to an application of S_1, S_2, S_3, or S_4. The graph is therefore 4-regular (each vertex has degree 4). Loops (cycles of length 1) occur when applying one of these matrices to v leaves v unchanged. Since $\mathcal{A}$ is an infinite group, G is an infinite graph with infinitely many connected components.

2.1 Connected Graphs

A more interesting situation occurs when we look at the graph of Descartes quadruples modulo p for some prime p. Call this graph G_p. This graph is finite, with at most p^4 vertices (a vertex in this graph corresponds to a quadruple of integers that satisfies Descartes' equation (mod p)). Is G_p connected? We know the vertices within a given packing form a connected component. But in G_p, if there is only one component overall, then from any quadruple v (mod p) we can get to any other quadruple w (mod p), regardless of which packing v and q belong to. Knowing if G_p is connected, therefore, tells us whether there can be local obstructions modulo p in a packing. What follows is a discussion of how to determine whether G_p is connected.

2.2 The Adjacency Matrix and its Eigenvalues

Let n be the number of vertices in G_p. Label the vertices $v_1, v_2, ..., v_n$. The *adjacency matrix*, A, is an $n \times n$ matrix whose ijth entry is equal to the number of edges between v_i and v_j. In the adjacency matrix for G_p, the sum of entries in each column and each row is 4, since G_p is 4-regular.

By the definition of matrix multiplication, if $(A)_{ij}$ is the number of paths of length 1 between v_i and v_j, then $(A^r)_{ij}$ is the number of paths of length r between v_i and v_j. To see this, consider A^2:

$$(A^2)_{ij} = \sum_{k=1}^{n} A_{ik}A_{kj}.$$

$(A^2)_{ij}$ gets incremented by 1 every time $A_{ik} = 1$ and $A_{kj} = 1$. In other words, $(A^2)_{ij}$ gets incremented every time v_i and v_j are both connected to v_k, which corresponds to a path of length 2 existing between v_i and v_j. Now, proceed by induction. Assume $(A^m)_{ij}$ is the number of paths of length m from v_i to v_j. Compute $(A^{m+1})_{ij}$:

$$(A^{m+1})_{ij} = (A^m A)_{ij} = \sum_{k=1}^{n} (A^m)_{ik}A_{kj}$$

$(A^{m+1})_{ij}$ gets incremented every time both $(A^m)_{ik}$ (the number of paths of length m from v_i to v_k) and A_{kj} (the number of paths of length 1 from v_k to v_j) are nonzero. In other words, A_{ij} gets incremented by the quantity $\alpha_k = (A^m)_{ik}A_{kj}$ every time there are α_k paths of length $m+1$ between v_i and v_j.

Since we know $(A^r)_{ij}$ is the number of paths of length r between v_i and v_j, we know that, when r is sufficiently large, the ijth entry of (A^r) will tell us whether v_i and v_j are in the same component. To see if *all* vertices are in the same component (i.e. G_p is connected), we turn to the eigenvalues of A.

Because the sum down each row and column of A is 4, we know there can't be any eigenvalues greater than 4. We also know that the eigenvalue $\lambda = 4$ is always attained, because we can divide each entry of A by 4 so that the sum down each row of the resulting matrix, A', is 1:

$$A'_{i1} + A'_{i2} + \ldots + A'_{in} = 1 \qquad (1 \leq i \leq n)$$

Therefore we can take the n-dimensional column vector $x = (1, 1, \ldots, 1)^T$ as an eigenvector, because $A'x = x$. Likewise, $Ax = 4x$, so the eigenvalue $\lambda = 4$ will always be attained. The multiplicity of this eigenvalue reveals whether the graph is connected, in the following relationship:

Claim: The eigenvalue $\lambda = 4$ has multiplicity 1 if and only if G_p is connected.

Proof: Let A' be the adjacency matrix A divided by 4. Let W be the n-dimensional vector space of all functions that map a vertex of G_p to a real number. In other words, W is the vector space of all $f : V(G_p) \longrightarrow \mathbb{R}$. A' applied to $f(v)$ is the average of f on all of v's neighbors:

$$A'f(v) = \frac{1}{4}\sum_{w\sim v} f(w) \qquad (\text{where} A' = \frac{1}{4}A)$$

Note that $f_1 = 1$ is an eigenvector with eigenvalue 1:

$$Af_1 = \frac{1}{4}(1+1+1+1) = 1 = f_1$$

We want to show that if G_p has 2 components, it is possible to find some $f_2 \in V$, linearly independent from f_1, so that

$$Af_2 = f_2$$

Label the components of G_p, A and B. Now define f_2 as:

$$f_2(v) = \begin{cases} 1 & \text{if } v \in A, \\ -1 & \text{if } v \in B. \end{cases}$$

Since f_2 is not a multiple of f_1, it is linearly independent. It also has eigenvalue 1, because:

$$\begin{aligned} Af_2(v) &= \begin{cases} \frac{1}{4}(1+1+1+1) & \text{if } v \in A \\ \frac{1}{4}(-1-1-1-1) & \text{if } v \in B \end{cases} \\ &= f_2(v) \end{aligned}$$

We've just shown the contrapositive of the "only if" direction, so we know that if $\lambda = 1$ has multiplicity 1, then the G_p is connected. Conversely, we'd like to show that if G_p is connected, then the only function f for which $A'f(v) = f(v)$ is the constant function (meaning $\lambda = 1$ must have multiplicity 1). To do this, take an f such that $A'f = f$. For all $v \in G_p$, we must have

$$\frac{1}{4}(f(w_1) + f(w_2) + f(w_3) + f(w_4)) = f(v)$$

where w_1, w_2, w_3, and w_4 are the neighbors of v. That is, we need $f(v)$ to be equal to the average of f on all neighbors of v. Suppose this average is equal to α. Now, to get a contradiction, suppose $f(w_1) > \alpha$ and $f(w_2) < \alpha$. The average of all four neighbors of w_1 must also be α; yet, $f(w_1) > \alpha$, contradicting our choice of f. Therefore, if $A'f = f$ (which is equivalent to saying $Af = 4f$) then f must be constant over all v. $\square$

If G_p is connected, we know that its biggest eigenvalue is 4, and its next biggest eigenvalue is strictly less than four. And since A is symmetric, there exists an orthonormal basis of eigenvectors of A. Therefore, we can raise A to powers in terms of its eigenvectors. Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of A, arranged in decreasing order ($\lambda_i \geq \lambda_j$ if $i \leq j$) and let $e_1, e_2, ..., e_n$ be an orthonormal eigenbasis for A. For f and g in the vector space W, define the inner product of f and g, written as $< f, g >$, to be the sum of $f(v)g(v)$ over all vertices v. (When f and g are thought of as $n \times 1$ vectors with real entries, this is just the standard dot product.) For any $f \in W$, we can write f as

$$f =< f, e_1 >, e_1 + < f, e_2 > e_2 + \ldots + < f, e_n > e_n.$$

Therefore,

$$\begin{aligned} A^m f &= \sum_{k=1}^{n} \lambda_k^m < f, e_k > e_k \\ &= \lambda_1^m < f, e_1 > + \sum_{k=2}^{n} \lambda_k^m e_k \end{aligned}$$

As long as λ_1 is strictly greater than all other eigenvalues (in absolute value), this eigenvalue dominates once m is big enough. In this case we can approximate $A^m f$ by $\lambda_1^m f$. The next biggest eigenvalue (in absolute value), call it θ, serves as an error term:

$$\theta = \max|\lambda_j|, \quad j \neq 1$$

After dividing the matrix A by 4, θ will be strictly less than 1. We know

$$\sum_{k=2}^{n} \lambda_k^m e_k \leq \theta^m \sum_{k=2}^{n} e_k.$$

As m increases, θ^m approaches 0, making $\lambda^m f$ a more accurate approximation of $A^m f$. The only issue to worry about is the possibilty that θ is equal to -1, meaning that $|\theta| = \lambda_1$. If this is case, θ^m no longer approaches 0, and λ_1 can no longer be used to accurately estimate powers of A. However, in the graph G_p (for any p), such a situation will never occur. What follows is an explanation of the conditions under which A will have an eigenvalue of -4, and why it will never occur in G_p.

Claim: A will have an eigenvalue of -4 if and only if G_p is bipartite

Proof: First, we show that if G_p is bipartite, then -4 will be attained as an eigenvalue. Consider the matrix A', equal to the adjacency matrix divided by 4 in each entry. Given a bipartite graph, we're searching for a function $f \in W$ (the vector space of all functions from $V(G)$ to $\mathbb{R}$), such that

$$A'f(v) = -\frac{1}{4} \sum_{w \sim v} f(w)$$

In other words, for each vertex v, we want $f(v)$ to be equal to the negative average of f on all neighbors of v. To do this, assign a 2-coloring to the graph. Split the vertices into 2 sets, A and B, where two vertices are in the same set if and only if they have the same color. Now, let

$$f(v) = \begin{cases} 1 & \text{if } v \in A, \\ -1 & \text{if } v \in B. \end{cases}$$

Any vertex v will only have neighbors in the opposite set. Therefore, the average of f on all neighbors of v will have the opposite sign of $f(v)$, meaning f is an eigenvector with eigenvalue -1.

For the other direction, we first show that, if there is an eigenvector f with eigenvalue -1, then $|f|$ must be constant over al vertices in the graph. Take an eigenvector f, such that $|A'f| = f$. For any vertex v, $f(v)$

is equal to the absolute value of the average of f on all neighbors of v. Suppose the absolute value of this average is equal to α. To get a contradiction, suppose $|f(w_1)| > \alpha$ and $|f(w_2)| < \alpha$. The absolute value of the average of all four neighbors of w_1 must also be α; yet, $|f(w_1)| > \alpha$, contradicting our choice of f.

Now we show that if G_p is not bipartite, there can be no function f with eigenvalue -1. Since the graph is not bipartite, G_p contains an odd cycle. Thus a function that takes some value α on some vertices and $-\alpha$ on others won't work, because along the odd cycle, there will be some vertex v_1 that is adjacent to another vertex v_2, such that $f(v_1)$ and $f(v_2)$ have the same sign. However, since $|f|$ must be constant over all vertices, there are no other possible constructions of f, meaning there can be no eigenvector with eigenvalue -1. □

Now one can observe that A will never have the eigenvalue -1, since as long as G_p is connected, it will never be bipartite. If G_p is connected, then there is a path from any Descartes quadruple to another, regardless of which packing the quadruples belong to. This means there will be paths to the root quadruple $(0, 0, 1, 1)$, and this quadruple is mapped to itself by S_3 and S_4. The mapping of a quadruple to itself corresponds to having a loop (a cycle of length 1) in the graph, meaning G_p is not bipartite. (Note that $(0, 0, 1, 1)$ is not the only root quadruple for which this is true. Other examples include $(-1, 2, 2, 3)$ and $(-3, 4, 12, 13)$, which are both mapped to themselves by S_4)

2.3 Computations

This observation about the eigenvalues of the adjacency matrix A, can be used to compute whether G_p is connected for various p. Here are some results for primes less than 15:

p	2	3	5	7	11	13	6	12
n	7	20	144	300	1220	2352	167	2687
multiplicity of biggest eigenvalue	7	2	1	1	1	1	23	383
next biggest eigenvalue in abs. value	n/a	3	3.618	3.6996	3.6569	3.6129	3	3

Although 6 and 12 are not prime, they are included since both have prime factorizations consisting only of powers of 2 and 3, and both are disconnected graphs.

3 A Prime Number Theorem

The well-known Prime Number Theorem states that the number of primes less than or equal x, denoted by $\pi(x)$, is asymptotic to $\frac{x}{\ln x}$. That is,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

We can ask a similar question in relation to Apollonian circle packings. Given some integer n, how many integers less than or equal to n will appear in a certain packing? Numerical investigations of Apollonian circle packings have pointed to some possible answers. Let C_q be the set of curvatures generated in a packing, by a certain root quadruple q. C_q is an infinite set, and each element has been obtained by applying a string of matrices in $\mathcal{A}$ to q. Define the *word length* of a curvature as the number of matrices in the string required to produce that curvature from the original. One can look at finite subsets of C_q by considering only those curvatures produced by strings of matrices with word length less than or equal to some number T.

Below are some results for the root quadruple $(-1, 2, 2, 3)$. Instead of looking at the number of prime curvatures less than an integer n, one can ask how many prime curvatures with word length less than or equal to T will appear in the packing. In the following table, $N(T)$ stands for the number of curvatures (counted with multiplicities) with word length less than or equal to T. $P(T)$ is the number of *prime* curvatures with word length less than or equal to T.

In the table, $P_w(T)$ is the weighted count of primes: while $P(T)$ is incremented by 1 each time a prime is produced, $P_w(T)$ is incremented by $\log p$ each time a prime p is produced. That is,

$$P_w(T) = \sum_{p \text{ prime}} \log p \qquad \text{summed over all } p \text{ with word length} \leq T$$

T	$N(T)$	$P(T)$	$P_w(T)$
0	4	3	2.484
1	8	4	3.583
2	20	8	14.650
3	56	20	59.443
4	164	38	141.432
5	488	92	441.873
6	1460	252	1460.351
7	4736	606	4042.478
8	13124	1516	11469.912
9	39368	4042	34311.203
10	118100	11132	105225.489

$P_w(T)$ is recorded as well as $P(T)$ because of the following fact:

Claim: The Prime Number Theorem is equivalent to the following statement:

$$\sum_{p \leq x} \log p \sim x \qquad \text{(where } p \text{ is prime)}$$

Proof: Define $\phi(x)$ as:

$$\phi(x) := \sum_{p \leq x} \log p.$$

Recall that $\pi(t) := \#\{\text{primes} \leq t\}$, and $\pi(t)$ tends to $\frac{t}{\log t}$, by the Prime Number Theorem. Using the $\pi(t)$ function, we can write $\phi(x)$ as an integral:

$$\begin{aligned} \phi(x) &= \int_1^x \log t \; d\pi(t) \\ &= \log t \; \pi(t)\Big|_1^x - \int_1^x \frac{\pi(t)}{t} \, dt \\ &= x - \int_1^x \frac{dt}{\log t} + \{\text{error term}\} \end{aligned}$$

Now we want to show that

$$\lim_{x \to \infty} \frac{\phi(x)}{x} = 1.$$

So far we know that

$$\lim_{x \to \infty} \frac{\phi(x)}{x} = 1 - \lim_{x \to \infty} \frac{1}{x} \int_1^x \frac{dt}{\log t}$$

We can use L'Hopital's theorem on the second term:

$$\lim_{x\to\infty} \frac{\int_1^x \frac{dt}{\log t}}{x} \quad = \quad \lim_{x\to\infty} \frac{1}{\log x} = 0.$$

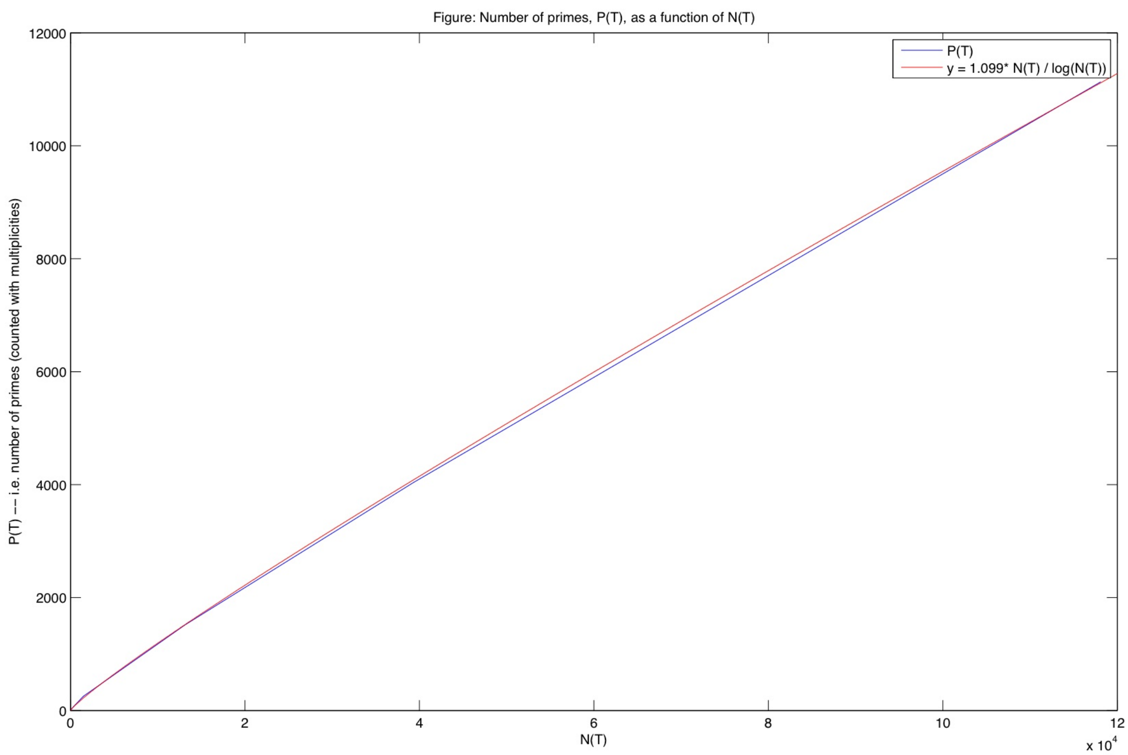
Thus,

$$\lim_{x\to\infty} \frac{\phi(x)}{x} = 1.$$

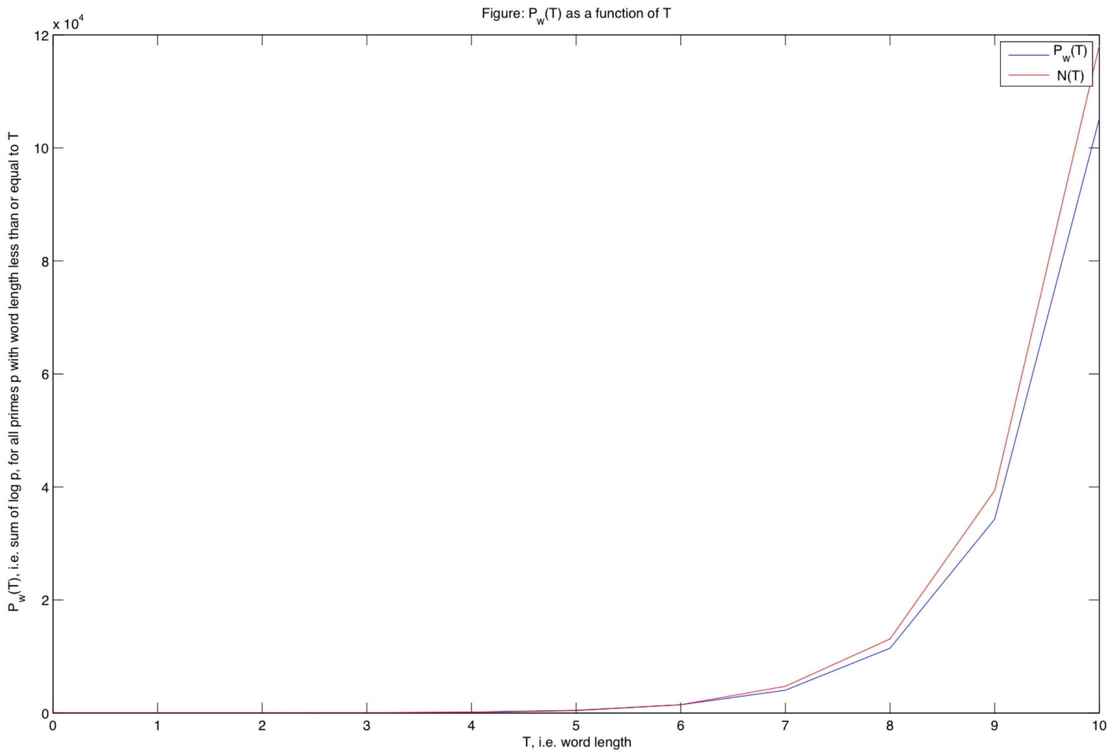
□

Below, we fit $P(T)$, the number of primes with word length less than T, to the model $k\frac{N(T)}{\log N(T)}$, where k is some constant. Here is a plot comparing the actual data to a fitted curve of the form

$$y = 1.099\,\frac{N(T)}{\log N(T)}.$$



Next is a plot of $P_w(T)$, as a function of T, compared with $N(T)$, up to 10 generations. Just as $P(T)$ appears to tend to $\frac{N(T)}{\log N(T)}$, we'd like to see if $P_w(T)$ tends to $N(T)$.



One future objective is to gain a deeper understanding of how prime numbers are distributed within a packing. It would be especially interesting to find theoretical explanations that are consistent with the above models.

References:

D. Austin, *When Kissing Involves Trigonometry*, American Mathematical Society: Feature Column (2006).

R.L. Graham, J.C. Lagarias, C.L. Mallows, A. Wilks, and C. Yan, *Apollonian circle packings: number theory*, Journal of Number Theory, 100 (2003), 1-45.

J.C. Lagarias, C.L. Mallows, and A. Wilks, *Beyond the Descartes Circle Theorem*, American Mathematical Monthly, 109 (2002), 338-361.

P. Sarnak, *Letter to J. Lagarias*, June 2007.