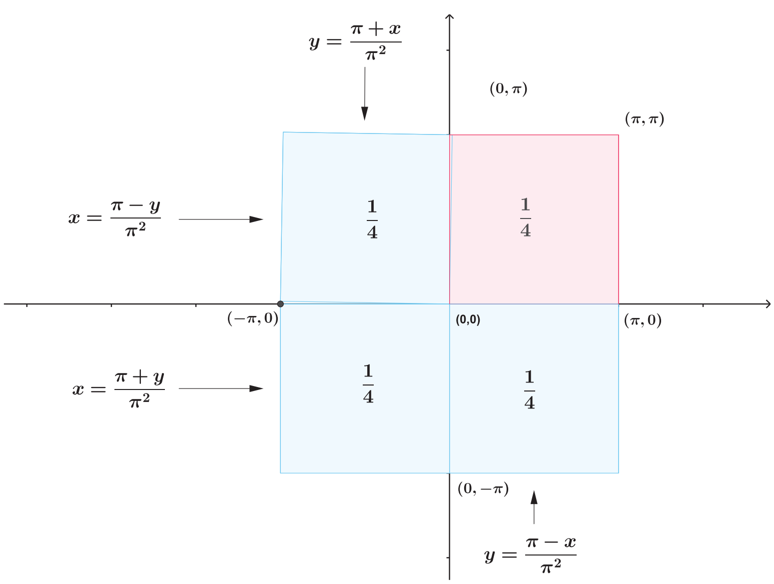
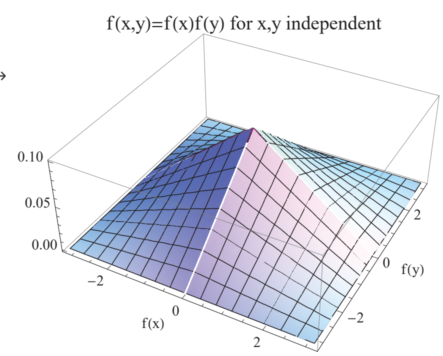
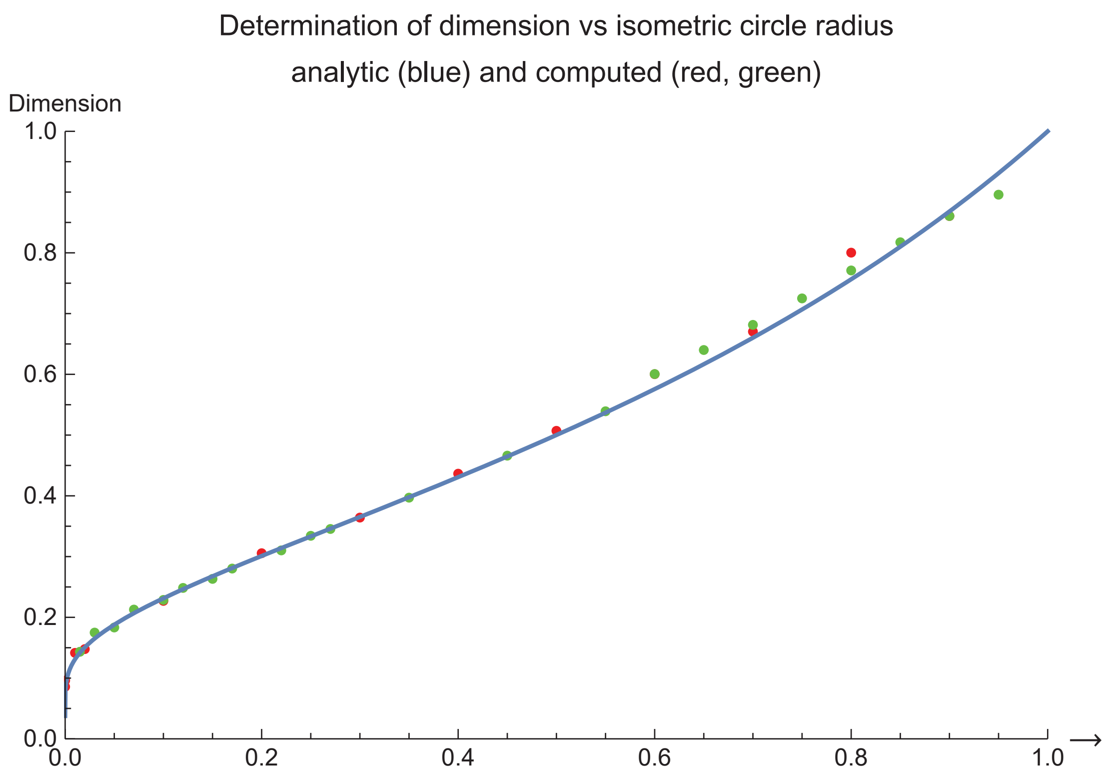
Random discrete groups of Möbius transformations: Probabilities and limit set dimensions.

A Thesis presented in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in
Mathematics
at Massey University, Albany, New Zealand





November 2017
This thesis represents original work of the author unless otherwise attributed.



Graeme K O'Brien

Institute for Advanced Study, Massey University, Auckland New Zealand

Acknowledgements

Distinguished Professor Gaven Martin

It was my good fortune to have a great mathematician for my supervisor, but he made me work for the privilege. With his professional scepticism he made me fight for every claim, standard challenges were "I don't believe it", or maybe "It's either well known or it's wrong, I don't know which". Thanks Gaven.

Associate Professor Shaun Cooper

Thanks Shaun for your encouragement and tenacious insistence that the proof of a particular theorem be unassailable.

Lynette O'Brien, BBS (Hons), MSc (Mathematics)

Well, who could have a more loving, patient and supportive mathematical wife?

ABSTRACT

This thesis addresses two areas related to the quantification of discrete groups. We study "random" groups of Möbius transformations and in particular random two-generator groups; that is, groups where the generators are selected randomly. Our intention is to estimate the likelihood that such groups are discrete and to calculate the expectation of their associated geometric and topological parameters. Computational results of the author [55] that indicate a low probability of a random group being discrete are extended and we also assess the expected Hausdorff dimension of the limit set of a discrete group. In both areas of research analytic determinations are correlated with computational results. Our results depend on the precise notion of randomness and we introduce geometrically natural probability measures on the groups of all Möbius transformations of the circle and the Riemann sphere.

Contents

Chapter 1

Introduction

1.1 Möbius transformations and hyperbolic geometry

We are interested in discrete groups of Möbius transformations because this gives us a way to understand some of the geometric aspects of hyperbolic spaces. Decomposition of 2-manifolds into a few structures (spheres, tori and projective planes) has been possible for some time. Thurston's geometrisation conjecture (see for example [69]), since proven by Perelman ([57] for the first of a series of papers), allows the decomposition of any closed 3-manifold into sub manifolds with precisely eight possible geometric structures which are quotient groups of the manifold by discrete subgroups of a Lie group on the manifold.

Lie groups are mathematical groups in the usual sense but with the additional property of topological isomorphism to some smooth (differentiable) manifold. That is, the identification of groups of Möbius transformations with groups of hyperbolic isometries has important connections to 3-manifold theory. The group of Möbius transformations under composition is homomorphic to a subgroup of 2×2 complex matrices under multiplication, unique up to sign, allowing Möbius transformations to be studied by considering subgroups of the matrix groups $GL(2, \mathbb{C})$ and $SL(2, \mathbb{C})$ for instance via theorems by Jørgensen [36], Gehring and Martin [21] and Klein (see [25]). The classic works of Ford [20] and Beardon [5] present much of the mathematical foundation for analysis of discrete groups.

Beardon shows that for any subdomain of $\hat{\mathbb{C}}$ invariant under a group G of Möbius transformations, provided the group action is discontinuous then the quotient of the subdomain by G is a Riemann surface

1.2 Random groups

In this thesis we introduce the notion of a random Fuchsian group. Our ultimate aim is to study random Kleinian groups, but the Fuchsian case is quite distinct in many ways, for instance the set of precompact cyclic subgroups (generated by elliptic elements) has nonempty interior in the Fuchsian case, and therefore will have positive measure in any reasonable imposed measure. For Kleinian groups this is not the case. However, the motivation for the probability measure we chose is similar in both cases. We seek something "geometrically natural" and with which we can perform both computational and mathematical analysis. We should expect that almost surely (that is with probability one) a finitely generated subgroup of the Möbius group is free.

1.3 Discrete groups

We shall see that a random two generator group is discrete with probability greater than $\frac{1}{20}$, a value we conjecture to being close to optimal, and we know with certainty that this value is less than $\frac{1}{4}$. If we condition by choosing only hyperbolic elements, this probability becomes $\frac{1}{5}$ and if we condition by choosing only parabolic elements the probability of discreteness is $\frac{1}{6}$. We also consider such things as whether or not axes of hyperbolic generators cross in order to get some understanding of the likelihood of different topologies arising. To examine discreteness we set up a topological isomorphism between n pairs of random arcs on the circle and n-generator Fuchsian groups. We determine the statistics of a random cyclic group completely, however, the statistics of commutators is an important challenge with topological consequences which we only partially resolve. For instance if we choose two random hyperbolic elements with pairwise disjoint isometric circles, the quotient space is either the two-sphere with three holes, or a torus with one hole, the latter occurring with probability $\frac{1}{3}$.

The mathematics of discrete groups of Möbius transformations is the basis of our study of hyperbolic geometry. We now view Euclid's parallel postulate as allowing the contrary existence of other geometries and the successful application of hyperbolic geometry is ample justification. Hyperbolic geometry is the realm of spaces with constant negative curvature as opposed to zero curvature for Euclidean spaces and constant positive curvature for spherical spaces.

With the aid of discrete groups and some deep theorems we can perform topological decomposition of convoluted surfaces in hyperbolic spaces into much simpler component parts for which the geometry is locally Euclidean at every point, these surfaces we call *manifolds* (or *orbifolds* if the group contains elements of finite order). A 2-manifold is a two dimensional surface that we can usually envisage embedded in three-dimensional space while a 3-manifold is a three dimensional "surface" that we find extremely difficult to envisage at all. There are well known examples of manifolds that will not even embed in such Euclidean spaces. The Möbius strip, Klein bottle and projective plane are examples of manifolds which are non orientable surfaces.

The *extended complex plane* $\hat{\mathbb{C}} = \mathbb{C} + \{\infty\}$ is a two dimensional non planar connected space, topologically a sphere, and we call it the Riemann sphere. We can define two and three-dimensional hyperbolic space embedded in $\mathbb{R}^2$ and $\mathbb{R}^3$ respectively as:

$$\mathbb{H}^2 = \{\mathbf{z} = (x, y) : y > 0\}$$

together with the metric $ds = \frac{|d\mathbf{z}|}{|x|}$ of constant negative curvature -1, and

$$\mathbb{H}^3 = \{\mathbf{z} = (x, y, t) : t > 0\}$$

together with the metric $ds = \frac{|d\mathbf{z}|}{t}$.

We also use the Poincaré unit disc model where two dimensional hyperbolic space is emdedded in the interior $\mathbb{D}^2$ of the unit circle and the metric is:

$$ds = \frac{|\mathbf{dz}|}{1 - |\mathbf{z}|^2}, \qquad |\mathbf{z}| < 1.$$

Information about these spaces together with some formulae we will use from time to time can be found in Beardon [5].

Möbius transformations are linear fractional functions of the form $f(\mathbf{z}) = \dfrac{\mathbf{az} + \mathbf{b}}{\mathbf{cz} + \mathbf{d}}$ where $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}$ are complex numbers and the functions map the point $\mathbf{z} = x + iy$ to the point $f(\mathbf{z})$ in the extended complex plane $\hat{\mathbb{C}}$. Such functions are differentiable provided $\mathbf{c}$ and $\mathbf{d}$ are not both zero, a condition satisfied by a requirement that the products $\mathbf{ad}$ and $\mathbf{bc}$ are never equal, and the functions form a group under composition. It turns out that the Möbius transformation group is isomorphic to the group of orientation-preserving isometries of not only $\hat{\mathbb{C}}$, but of hyperbolic 3-space, they can be shown to act as conformal (that is, with preservation of angles) transformations in $\hat{\mathbb{C}}$, see [5].

If we consider matrix representation of Möbius transformations then for inverses to exist we must require 2×2 complex matrices of the form $\begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix}$ to be non singular, with $\mathbf{ad} - \mathbf{bc} \neq 0$. We find that such matrices form a group under multiplication, which group generates under composition all isometries of $\hat{\mathbb{C}}$.

So all conformal automorphisms on the sphere are Möbius transformations and the Möbius group is homomorphic to groups of matrices in $SL(2, \mathbb{C})$, a group which has representation mathematically as a differentiable manifold. Möbius transformations can be represented by matrices in $GL(2, \mathbb{C})$ up to determinant, in $SL(2, \mathbb{C})$ up to $\pm I$ (where I is the identity matrix for $GL(2, \mathbb{C})$ and all subgroups), and uniquely in $PSL(2, \mathbb{C}) = SL(2, \mathbb{C})/\{\pm I\}$. Conversely, matrices in these groups induce Möbius transformations.

Following Gehring and Martin [21] we define the *parameters* of a two generator group $\langle f, g \rangle$ as β and γ where:

$$\beta(f) = \mathrm{trace}^2(\mathrm{f}) - 4, \ \beta(\mathrm{g}) = \mathrm{trace}^2(\mathrm{g}) - 4$$

and where the commutator of f and g is $[f, g] = fgf^{-1}g^{-1}$:

$$\gamma([f, g]) = \mathrm{trace}([\mathrm{f}, \mathrm{g}]) - 2. \tag{1.1}$$

A discrete subgroup G of Möbius transformations contains no sequence of elements of G that tends to the identity transformation, this is equivalent to the group inheriting the discrete topology from $SL(2, \mathbb{C})$ and the discreteness property can be established by demonstrating that the identity is isolated (see for example Beardon [5]). Jørgensen [36] proves a necessary condition for non elementary two-generator groups $\langle f, g\rangle$ to be discrete, in terms of the parameters:

$$|\beta(f)| + |\gamma([(f, g)])| \geq 1. \tag{1.2}$$

Jørgensen also establishes that a non elementary group G of Möbius transformations is discrete if and only if for all $f, g \in G$, the two generator group $\langle f, g\rangle$ is discrete, this important result allows us to restrict analysis to two generator groups. Klein, see for example [25], proves that if the discs enclosed by the 4 isometric circles of matrices A, B, A^{-1}, B^{-1} representing two Möbius transformations and their inverses are mutually disjoint then the two-generator group $\langle A, B\rangle$ is discrete.

Möbius transformations being linear fractional functions, representative transformations in $GL(2, \mathbb{C})$ can always be reduced to transformations in $SL(2, \mathbb{C})$ and we define *Kleinian groups* to be that subgroup of $SL(2, \mathbb{C})$ consisting of all discrete Möbius transformations. If under a Möbius transformation group there is an invariant disc in $\hat{\mathbb{C}}$ in which the group action is discontinuous then the group is *Fuchsian* and discrete, such are conjugate to subgroups of $SL(2, \mathbb{R})$ hence have real trace and act as groups of isometries in the Poincaré disc model of hyperbolic space.

In order to extend the computational results of [55] (which applied quite generally to Möbius transformations close to the identity) we develop both analytical and computational methodologies, quantifying the nature of the sets of discrete groups embedded in Fuchsian or Kleinian groups via probability distributions that are geometrically natural. Among the objectives of this thesis are discovery of lower bounds to the probability that particular two generator groups are discrete and understanding of the likelihood that Jørgensen's inequality is violated.

1.4 Limit sets

The concept of an accumulation point of a set is well known, that any neighbourhood of the point no matter how small contains another point of the set. The limit set $\Lambda(G)$ of a group G of transformations is defined by Ford [20] to be the set of all accumulation points of the isometric circle centres of $f \in G$. The fixed points of the generators X_i of $G = \langle X_i, |_{i=1}^{m}\rangle$ being invariant under the action of the respective X_i are necessarily contained in $\Lambda(G)$.

Non commutative finitely generated groups can be specified completely by an infinite set of sequences of the individual group generators and their inverses. For a two-generator group $\langle f, g\rangle$ the possible operations are $\{f, f^{-1}, g, g^{-1}\}$, these are the letters of sentences representing such sequences. We note however that it would be non productive to allow sentences having any letter and its inverse adjacent, accordingly we will always use *reduced sentences* which omit all adjacent combinations of elements of the units of the set of group generators. It is easy to see that such exclusions also obviate the possibility of any compound words (sub-sentences) being adjacent to their inverses, that is, a reduced sentence is *completely* *reduced*, containing no adjacent elements of units of the group.

The group action of a finitely generated group G on a metric space H can then generate the limit set $\Lambda(G)$ via the operation of the set W of all infinite sentences of elements of G on all points $p \in H$. $\Lambda(G)$ is invariant under the action of G. Further, for all $p \in H$ there exist fixed points τ and infinite sequences of elements $\gamma_n \in G$ such that $\gamma_n(p) \to \tau$ as $n \to \infty$, hence $\Lambda(G)(p_1){=}\Lambda(G)(p_2)\ \ \forall p_1, p_2 \in H$ and given G, H the limit set of the action of G on H, $\Lambda(G)$ is unique and can be generated as the closure of the set W acting on any point $p \in H$.

Since the limit set $\Lambda(G)$ is a group invariant we can generate the set via group operations on the fixed points of the generators. This is the approach we follow for our computational determinations.

We will restrict our attention to 2-generator groups $G = \langle f, g\rangle$ represented by matrices in $SL(2, \mathbb{C})$ and the group action on the extended complex plane $\hat{\mathbb{C}}$. Surface groups are discrete and their limit sets are circles. We study the case where G is discrete and the limit set is totally disconnected and confined to the interiors of the four isometric circles of the matrix representations of the generators and their inverses. In any sequence γ_n, as $n \to \infty$ the radii of the corresponding pairs of isometric circles tend to zero very rapidly and consequently for any point $p \in \hat{\mathbb{C}}$, a transformed point $p' = \gamma_n\ p$ rapidly becomes indistinguishable from a limit set point. That is, the limit sets can be defined by rapidly convergent sequences.

We can classify group elements by the order of the reduced sentences and will refer to the resultant classes as *generations*. For the two generator group $\langle f, g\rangle$ we take generation 0 to be the identity, generation 1 then consists of $\{f, f^{-1}, g, g^{-1}\}$. We also classify group actions and parameters in the same fashion, and in each case the resulting structure is an iterated function system. The concept was introduced by Barnsley and Demko [4]. Formally, an **iterated function system** (IFS) is a finite set of contraction mappings on a complete metric space and the dynamical system consists of repeated application of these maps.

1.5 Dimension

We adopt the following definition of dimension based on work of Barenblatt [3], Sagan [61] and Riemann [59]:

Definition 1.1. *The dimension function (the dimension) supported on a metric or topological space is the function that determines the constant factor by which the numerical value of an entity changes upon passage from one generation to another within a given IFS class.*

We define in the normal manner a Lebesgue outer measure via all countable covers $\cup_i U_i$ of non-empty subsets $U_i \subset \mathbb{R}^n$ of bounded diameter as $\mathscr{H}^s_\delta(E) = \inf \sum_{i=1}^\infty |U_i|^s$ where the diameter and dimension bounds are respectively $0 < \sup |U_i| \le \delta$ and $0 < s \le \infty$. As we take the limit $\lim_{\delta\to 0} \mathscr{H}^s_\delta(E)$ (which always exists) then we have the Hausdorff s-dimensional outer measure $\mathscr{H}^s(E) = \sup_{\delta>0} \mathscr{H}^s_\delta(E)$ for $s \in \mathbb{R}^+$. There is a unique non-zero non-infinite value which is the **Hausdorff dimension** of the set. Anderson and Rocha [1] show that in the context of Kleinian groups the Hausdorff dimension is an analytic function.

The resemblance of Hausdorff dimension to the Minkowski (box counting) dimension is apparent if we choose for covering sets only subsets of dimension δ. Mainieri [40] establishes that the Hausdorff and box counting dimensions agree for fractal sets generated by rapidly convergent functions. Kleinian groups are by definition discrete and totally disconnected and their limit sets are necessarily fractal and bounded by the disjoint isometric circles in $\hat{\mathbb{C}}$ of the generators. The limit sets can be defined by rapidly convergent sequences, accordingly we assess Hausdorff dimension via a modification of the box counting process. Since the limit sets are group invariants then if a measurable dimension exists for such sets then the measure is also a group invariant, hence our interest.

Noting that the limit sets of ortho-central groups are contained within the unit circle $\mathbb{S}$ we represent each limit point by a single real number in the interval $[0, 2\pi)$ and consider only covering balls on $\mathbb{S}$, these are essentially one dimensional boxes on the circular domain. Thus for computational determination of the Hausdorff dimension we create a minimal coverings for limit sets E on $\mathbb{S}$ with balls of radius ϵ which map to intervals $[2\epsilon(j-1), 2\epsilon j) \subset \mathbb{R}$ indexed by $j \in [1, \frac{\pi}{\epsilon})$. Should $E = \mathbb{S}$ then the set E is 1-dimensional and the number of covering intervals is $N(\epsilon) = \frac{\pi}{\epsilon}$. We consider $\mathbb{S} - E \neq \varnothing$ and let C_i be constants, clearly whenever E contains an arc of $\mathbb{S}$ we can cover the set with fewer small intervals but the set remains 1-dimensional and $N(\epsilon) = C_0 \times \frac{\pi}{\epsilon}$ say. We recognise that if $E \neq \varnothing$ is totally disconnected then the dimension will be some number $D = dim(E) \mid 0 \leq D \leq 1$, and define the *box dimension* (Minkowski dimension) of E to be $D = dim(E) \mid N(\epsilon) = C_1 \frac{\pi}{\epsilon^D}$. Taking logs and rearranging, we have $D = dim(E) = \frac{log(N(\epsilon))}{-log(\epsilon)} - \frac{C_2}{log(\epsilon)}$. The expression $d = \frac{log(N(\epsilon))}{-log(\epsilon)}$ will yield a number d for any minimum covering of a set E by $N(\epsilon)$ intervals of width ϵ and we note that $d \to dim(E)$ as $\epsilon \to 0$ and that $dim(E)$ is the Hausdorff dimension for limit sets E of ortho-central groups.

Falconer [18] lists requirements that any dimensional measure $dim(E)$ of a set E must satisfy, in our case it is clear that if $\lim_{\epsilon \to 0} d = dim(E)$, then $d = \frac{log(N(\epsilon))}{-log(\epsilon)}$ which is the sum of the dimension $dim(E)$ and a function $\frac{C_2}{log(\epsilon)}$ of ϵ alone, must also satisfy Falconer's requirements, and specifically if $E \subset F$ then $dim(E) \leq dim(F) \Rightarrow d(E) \leq d(F)$.

We design and implement several algorithms, improving progressively on techniques similar to those indicated in the literature.

1.6 Computation

Computer programs to aid analytical calculations and perform computational analysis were central to this project. Some of these programs were available via commercial or academic license or on-line by courtesy of various acknowledged authors, others were designed and written by the author of this thesis for the various phases of this project. Microsoft Visual Basic 6, the last version ever produced of this superb structured scientific processing language, was used for implementation of the various algorithms developed and data presentation was via import into either Mathematica or Corel Draw, in the latter case using the Visual Basic 6 scripting language feature. Wolfram Mathematica especially has been a useful tool for preliminary analytical calculations. Occasional use has been made of GeoGebra and Adobe Illustrator to produce and convert diagrams into postscript files for incorporation into LaTeXdocument files.

Random number generation for matrix entry components is discussed in [55], in essence the fast methods have inherent aliasing problems while those producing results of high integrity are prohibitively slow for real-time calculation. For the current project a very large database of high integrity double precision fixed point random numbers in the range $[0, 1]$ was created once only using the CryptoSys API [13], this database then being accessed via purpose written virtual memory API's to allow fast random matrix generation. These random numbers have a higher specification than required by ANSI X9.31, the relevant publications are [54] and [19]. An additional advantage of the predefined database approach is that any computational experiment can be duplicated precisely for verification purposes.

1.7 Chapter order

The following is an explanation of the order of subsequent chapters.

- Chapter 2 covers some background theory for the decomposition of hyperbolic surfaces by Möbius transformations and also introduces concepts essential to the mathematical and computational analysis of random variables.
- The main results on Fuchsian groups can be found in Chapter 3.
- Chapter 4 develops random variable theory necessary for analysis of isometric circle intersection topology.
- Chapter 5 covers algorithmic considerations for computation and presents some computational results.
- Chapter 6 is a preliminary investigation into limit sets of some Möbius transformations and presents both computational and analytic results.

Chapter 2

Foundations

2.1 Möbius transformations

We will use the symbol $\mathfrak{M}$ to refer to the Möbius group with representation in $SL(2,\mathbb{C})$. We will normally be considering transformations of the extended complex plane, and it is important to note that Möbius transformations map circles to circles (where a straight line is a circle of infinite radius), see Beardon [5]. With matrix representation of $f \in \mathfrak{M}$ the trace function defined as the sum of leading diagonal entries is well defined for f as a linear fractional function, this allows us to refer to trace(f).

Möbius transformations do not generally commute; for g followed by f we would normally write $f(g) = f \circ g$ but we will use a product notation fg since by matrix representation of f by A and g by B the composition $f \circ g$ is represented by the matrix product AB.

In this thesis complex variables, sometimes treated as vectors, are represented in bold. For instance, $\mathbf{z} = x + iy$ expresses a complex variable in terms of real and imaginary parts and the conjugate of $\mathbf{z}$ is $\overline{\mathbf{z}} = x - iy$. We write for a vector in polar form $\mathbf{z} = |\mathbf{z}|\ e^{i\ Arg(\mathbf{z})}$ and for the modulus $z = |\mathbf{z}|$. We will treat the entries $\mathbf{a}, \mathbf{b}, \mathbf{c}$ and $\mathbf{d}$ of the matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix}$ as vectors through the origin $(0,0)$ in the extended complex plane.

2.1.1 The cross ratio

We follow Beardon [5] and define the *cross ratio* of four points $\mathbf{z_1}, \mathbf{z_2}, \mathbf{z_3}, \mathbf{z_4} \in \mathbb{C}$ to be

$$[\mathbf{z_1}, \mathbf{z_2}, \mathbf{z_3}, \mathbf{z_4}] = \frac{(\mathbf{z_1} - \mathbf{z_3})(\mathbf{z_2} - \mathbf{z_4})}{(\mathbf{z_1} - \mathbf{z_2})(\mathbf{z_3} - \mathbf{z_4})}. \tag{2.1}$$

Beardon shows that the cross ratio of any four points in $\hat{\mathbb{C}}$ is invariant under the action of Möbius transformations. We note that since any three points in $\hat{\mathbb{C}}$ determine a circle uniquely and Möbius transformations map circles to circles we can always find specific transformations $f = \frac{(\mathbf{z}-\mathbf{z_1})(\mathbf{z_2}-\mathbf{z_3})}{(\mathbf{z}-\mathbf{z_2})(\mathbf{z_1}-\mathbf{z_3})}$ to perform such mappings. Specifically, any three points can be mapped to the points $\{0, 1, \infty\}$ in $\hat{\mathbb{C}}$.

2.1.2 Conjugation

Möbius transformations f and g are conjugate whenever the products fg and gf are identical transformations. Then we can say that the conjugate of f by g is gfg^{-1} and f and g are congugate if and only if $f = gfg^{-1}$, see for example Beardon [5]. Some parameters are invariant under conjugation, notably the trace and the cross ratio of four points on a circle.

2.1.3 Classification and fixed points

Möbius transformations can usefully be classified according to the square of the trace or equivalently according to the parameter β (see e.g. Beardon [5]). Let f be a transformation in $\mathfrak{M}$ that maps points in $\hat{\mathbb{C}}$ to points in $\hat{\mathbb{C}}$. Then:

(1) For the identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\text{trace}(\pm \text{I}) = \pm 2$ and $\text{trace}^2(\pm \text{I}) = 4$, $\beta(\pm I) = 0$.

(2) If the trace is real and $\text{trace}^2(\text{f}) = 4$, $\beta(I) = 0$ and f is said to be *parabolic*. Such transformations have a single fixed point $\mathbf{z_1}$ (where $\mathbf{z_1} = f(\mathbf{z_1})$ in $\hat{\mathbb{C}}$), the transformation translates all but the fixed point in $\hat{\mathbb{C}}$ and is represented by a matrix conjugate to I.

(3) If the trace is real and $\text{trace}^2(\text{f}) < 4$, $\beta(I) \leq 0$ and f is said to be *elliptic*. Such transformations have infinitely many fixed points (where $\mathbf{z_i} = f(\mathbf{z_i})$, $(i \in \mathbb{N}^+)$ in $\hat{\mathbb{C}}$), the transformation rotates points in $\hat{\mathbb{C}}$ by an angle α when f is represented by a matrix conjugate to $\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$.

(4) If the trace is complex then f is said to be *loxodromic*. Such transformations have two fixed points (where $\mathbf{z_1}, \mathbf{z_2} = f(\mathbf{z_1}, \mathbf{z_2})$ in $\hat{\mathbb{C}}$), the transformation scales (dilates) points in $\hat{\mathbb{C}}$ by a factor $\mathbf{k} \in \mathbb{C}$ when f is represented by a matrix conjugate to $\begin{pmatrix} \mathbf{k} & 0 \\ 0 & 1 \end{pmatrix}$.

(5) If the trace is real and $\text{trace}^2(\text{f}) > 4$, $\beta(I) > 0$, then f is said to be *hyperbolic*. Such transformations have two fixed points (where $\mathbf{z_1}, \mathbf{z_2} = f(\mathbf{z_1}, \mathbf{z_2})$ in $\hat{\mathbb{C}}$), the transformation scales (dilates) points in $\hat{\mathbb{C}}$ by a factor $k \in \mathbb{R}$ when f is represented by a matrix conjugate to $\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$.

Beardon uses the term *strictly loxodromic* to denote loxodromic transformations f with non real $\beta(f) = \text{trace}^2(\text{f}) - 4$, that is, hyperbolic transformations are loxodromic but not strictly loxodromic. We will include the term hyperbolic where such explicitness avoids the possibility of confusion as in Theorem 2.4.

Theorem 2.1. *Let the Möbius transformation* $g(\mathbf{z}) = \frac{\mathbf{a\,z+b}}{\mathbf{c\,z+d}}$ *be represented by the matrix* $\begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix}$. *Then for* $\mathbf{c} \neq 0$ *the fixed points of the Möbius transformation* g *are given by:*

$$\mathbf{z} = \frac{\mathbf{a} - \mathbf{d} \pm \sqrt{\beta(g)}}{2\mathbf{c}}$$

where $\beta(g)$ *is the complex parameter,* $\text{trace}^2(\text{g}) - 4$.

Proof. The fixed points of a Möbius transformation g are the solutions in $\hat{\mathbb{C}}$ to $\mathbf{z} = \frac{\mathbf{a\,z+b}}{\mathbf{c\,z+d}}$; that is for $f \in SL(2,\mathbb{C})$,

$$\begin{aligned} & \mathbf{z}(\mathbf{cz}+\mathbf{d}) = \mathbf{az}+\mathbf{b} \\ \text{therefore} \quad & \\ & \mathbf{cz}^2 + (\mathbf{d}-\mathbf{a})\mathbf{z} - \mathbf{b} = 0 \end{aligned} \tag{2.2}$$

and the since the same equation is obtained for the inverse transformation, for $\mathbf{c} \neq 0$, $\mathbf{z} = \frac{\mathbf{d\,z-b}}{\mathbf{-c\,z+a}}$ and there are two fixed points given by:

$$\begin{aligned} \mathbf{z} &= \frac{\mathbf{a-d} \pm \sqrt{(\mathbf{a-d})^2 + 4\mathbf{bc}}}{2\mathbf{c}} \\ &= \frac{\mathbf{a-d} \pm \sqrt{\beta(f)}}{2\mathbf{c}}. \end{aligned} \tag{2.3}$$

□

Whenever $\mathbf{c} = 0$, (2.2) is linear and the only fixed point in $\hat{\mathbb{C}}$ is ∞ unless $\frac{\mathbf{b}}{\mathbf{d}} = 0$, in which case 0 is also a fixed point.

2.1.4 Isometric circles

The concepts of isometric circles as developed by Ford [20] have a close relationship to the operation of Möbius transformations in the complex plane.

Definition 2.2. *An isometric circle is the locus of points in whose neighbourhood distances are preserved under Möbius transformation.*

That such a locus is always a circle for Möbius transformations is easily established since the transformation group is a Lie group and hence differentiable. Then an isometric circle defines two disjoint discs in $\hat{\mathbb{C}}$ one consisting of the interior $\mathcal{D}_f$ and the other the exterior $\mathcal{D}'_f$ of the bounding circle. Our initial interest is due to Klein's determination of the relationship between discreteness of Möbius groups and the disjointedness of the isometric circles of the matrices representing the group generators.

Theorem 2.3. *For the Möbius transformation* $f(\mathbf{z}) = \frac{\mathbf{az+b}}{\mathbf{cz+d}}$ *represented by the matrix*

$$A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix} \in SL(2,\mathbb{C}) \tag{2.4}$$

acting on the extended complex plane $\hat{\mathbb{C}}$*:*

(1) *the isometric circles of the matrices induced by Möbius transformations* f *and* f^{-1} *are of radius* $\frac{1}{|\mathbf{c}|}$ *and are centered respectively on the points* $\frac{-\mathbf{d}}{\mathbf{c}}$ *and* $\frac{\mathbf{a}}{\mathbf{c}}$*,*

(2) *the transformation* f *sends the centre of the induced isometric circle to infinity and the point at infinity to the centre of the isometric circle induced by the inverse transformation* f^{-1}*,*

(3) *the transformation f maps the isometric circle induced by f to that of f^{-1} and maps the discs of the isometric circles according to:*

$$\begin{aligned} \mathcal{D}_f &\mapsto \mathcal{D'}_{f^{-1}} \\ \mathcal{D'}_f &\mapsto \mathcal{D}_{f^{-1}}. \end{aligned} \tag{2.5}$$

Proof.

(1) We differentiate $f(z) = \frac{\mathbf{az+b}}{\mathbf{cz+d}}$:

$$\frac{df}{d\mathbf{z}} = \frac{\mathbf{ad} - \mathbf{bc}}{(\mathbf{cz} + \mathbf{d})^2}$$

but since the Möbius transformations are represented by matrices in $SL(2, \mathbb{C})$, we may assume $\mathbf{ad} - \mathbf{bc} = 1$ and thus:

$$df = \frac{d\mathbf{z}}{(\mathbf{cz} + \mathbf{d})^2}$$

We note that

$$|df| = |d\mathbf{z}| \Leftrightarrow |\mathbf{cz} + \mathbf{d}| = 1 \tag{2.6}$$

which is the equation of a circle of radius $\frac{1}{|\mathbf{c}|}$ centered on $\frac{-\mathbf{d}}{\mathbf{c}}$. Similarly the inverse function $f(z) = \frac{\mathbf{dz-b}}{\mathbf{-cz+a}}$ yields the equation of a circle of radius $\frac{1}{|\mathbf{c}|}$ centered on $\frac{\mathbf{a}}{\mathbf{c}}$:

$$|df| = |d\mathbf{z}| \Leftrightarrow |-\mathbf{cz} + \mathbf{a}| = 1 \tag{2.7}$$

so the action of every Möbius transformation on the extended complex plane $\hat{\mathbb{C}}$ defines two (possibly co-incident) isometric circles of equal radii.

(2) Since $A \in SL(2, \mathbb{C})$ implies $\mathbf{ad} - \mathbf{bc} = 1$,

$$f\left(\frac{-\mathbf{d}}{\mathbf{c}}\right) = \frac{\mathbf{a}\frac{-\mathbf{d}}{\mathbf{c}} + \mathbf{b}}{\mathbf{c}\frac{-\mathbf{d}}{\mathbf{c}} + \mathbf{d}} = \frac{-\mathbf{ad} + \mathbf{bc}}{-\mathbf{cd} + \mathbf{cd}} = \infty \in \hat{\mathbb{C}}$$

and if we write the transformation function as $\mathbf{z}$ in the form $\frac{\mathbf{a}+\frac{\mathbf{b}}{\mathbf{z}}}{\mathbf{c}+\frac{\mathbf{d}}{\mathbf{z}}}$, then:

$$f(\infty) = \frac{\mathbf{a} + 0}{\mathbf{c} + 0} = \frac{\mathbf{a}}{\mathbf{c}}$$

(3) The centre of the isometric circle of f is $\frac{-\mathbf{d}}{\mathbf{c}}$. Consider a point a vector distance $\frac{\mathbf{k}}{\mathbf{c}}$ away from this centre, then:

$$
\begin{aligned}
f(\tfrac{-\mathbf{d}}{\mathbf{c}} + \tfrac{\mathbf{k}}{\mathbf{c}}\quad) = f(\tfrac{\mathbf{k}-\mathbf{d}}{\mathbf{c}}) \\
= \frac{\mathbf{a}\left(\frac{\mathbf{k}-\mathbf{d}}{\mathbf{c}}\right)+\mathbf{b}}{\mathbf{c}\left(\frac{\mathbf{k}-\mathbf{d}}{\mathbf{c}}\right)+\mathbf{d}} \\
= \frac{\mathbf{ak}-\mathbf{ad}+\mathbf{bc}}{\mathbf{ck}-\mathbf{cd}+\mathbf{cd}} \\
= \frac{\mathbf{a}}{\mathbf{c}} - \frac{1}{\mathbf{ck}}.
\end{aligned} \tag{2.8}
$$

If $|\mathbf{k}| = 1$ then $\left(\frac{-\mathbf{d}}{\mathbf{c}} + \frac{\hat{\mathbf{k}}}{\mathbf{c}}\right)$ are points on the isometric circle representing f (since the isometric circle radius is $r = \frac{1}{|\mathbf{c}|}$) and according to (2.8) are mapped to points $\left(\frac{\mathbf{a}}{\mathbf{c}} - \frac{\hat{\mathbf{k}}}{\mathbf{c}}\right)$ on the isometric circle representing f^{-1}. When $|\mathbf{k}| = n > 1$ then $\left(\frac{-\mathbf{d}}{\mathbf{c}} + \frac{n\hat{\mathbf{k}}}{\mathbf{c}}\right)$ are points outside the isometric circle of f and map to points $\left(\frac{\mathbf{a}}{\mathbf{c}} - \frac{\hat{\mathbf{k}}}{n\mathbf{c}}\right)$ inside the isometric circle representing f^{-1} and when $|\mathbf{k}| = n < 1$ then $\left(\frac{-\mathbf{d}}{\mathbf{c}} + \frac{n\hat{\mathbf{k}}}{\mathbf{c}}\right)$ are points inside the isometric circle of f and map to points $\left(\frac{\mathbf{a}}{\mathbf{c}} - \frac{\hat{\mathbf{k}}}{n\mathbf{c}}\right)$ outside the isometric circle representing f^{-1}.

□

If we refer to the single isometric circle of a matrix A we mean that circle represented by the equation $|\mathbf{cz} + \mathbf{d}| = 1$, if we refer to plural isometric circles of a matrix A we mean both the isometric circle of A and the isometric circle of A^{-1}, that is, the circle $|-\mathbf{cz} + \mathbf{a}| = 1$. If we on occasion refer to the isometric circles of, for instance f, we mean those of the matrix induced by f.

Theorem 2.4. *The isometric circles of a matrix representing a Möbius transformation g are disjoint or tangential if and only if g is hyperbolic or loxodromic.*

Proof. By definition (see e.g. Beardon [5]) a Möbius transformation g is hyperbolic or loxodromic if and only if $|\text{trace(g)}| > 2$. But the Euclidean distance between isometric circle centres of a matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix} \in SL(2, \mathbb{C})$ representing g (as depicted in Figure 2.1) is given by:

$$
\Delta = \frac{|\mathbf{a} + \mathbf{d}|}{|\mathbf{c}|} = r\ \ |\text{trace(A)}| \tag{2.9}
$$

while the actual separation distance between the isometric circles of A and A^{-1} is:

$$
\delta = r(|\text{trace(A)}| - 2). \tag{2.10}
$$

The isometric circles of $A \in SL(2, \mathbb{C})$ are then disjoint if and only if $|\text{trace(A)}| \geq 2$. □

We take the term *disjoint* to mean *disjoint or tangential.*

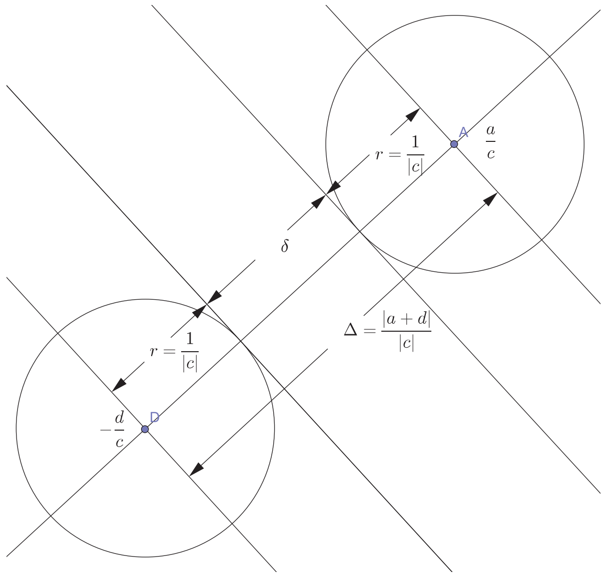


Figure 2.1: Euclidean distance between the isometric circles of a matrix in $SL(2,\mathbb{C})$.

2.1.5 The axis of a transformation

We define the *axis* of an isometric circle pair of a matrix to be the unique hyperbolic geodesic between the centres of the isometric circles in hyperbolic space. We then say that if the axes of two isometric circle pairs in $\mathbb{H}^2$ cross then the pair of transformations represented is *axis-crossing*. The axis-crossing condition then divides a matrix group into two equivalence classes.

2.1.6 Discrete groups

The following *Klein combination theorem* is at times known as the "ping pong" lemma, a more recent statement is in [69]:

Theorem 2.5. *If the discs enclosed by the four isometric circles of matrices A, B representing Möbius transformations f, g respectively are mutually disjoint then the group $\langle f, g\rangle$ generated by f and g is discrete and isomorphic in the free product $\langle f\rangle \times \langle g\rangle$.*

In view of Theorem 2.4 this allows us to calculate or compute explicit lower bounds for the probability that groups are discrete.

2.2 Random variables and probability distributions

We use concepts and terminology of probability theory as espoused by Papoulis and Pillai [56], Kolmogorov [39] and Springer [66] and attempt to reconcile differences between experimental and analytical approaches. Our "experiments" are actually deterministic mathematics based on algorithmic manipulation of subsets of a large predetermined set of high integrity uniformly distributed random numbers.

2.2.1 Random variables

An algebraic variable is an entity whose value is unknown, changeable, replaceable by any value in a specified domain of support. A *random variable* is defined by its probability density which is of necessity a function everywhere non negative and of unity integrated value over its domain of support. We use the symbols $\mathcal{P}$ for the *cumulative distribution function* (c.d.f.), defined as the probability that a random variable is less than a particular value, and $\mathbb{P}$ for the *probability density function* (p.d.f.), the derivative of the c.d.f. The term *distribution* may refer to a portion of the total p.d.f.

We distinguish between analytically and computationally determined distributions; the analytical p.d.f. that describes the distribution is defined via a (possible piecewise) equation, while a computationally (or experimentally) determined distribution is a set of data points with implied interpolation to a smooth curve. If we state that any set of computational or experimental data is (for instance) uniformly distributed, then such is to be taken as a statistical statement.

2.2.2 Kolmogorov's σ-fields

Kolmogorov [39] (in translation) defines the concepts of probability based on an algebraic field $\mathfrak{F}$ of random events, defined as a set of subsets of a finite set E of elementary events, and assigns (by way of measure) to each subset $A \in \mathfrak{F}$ a non negative real number $\mathbb{P}_A$ (called the *probability*) such that $\mathbb{P}_E = 1$.

Kolmogorov calls his algebraic field a *field of probability*, and together with complements this is a set-theoretical σ-field. The product space of two σ-fields is also a σ-field and we can construct σ-fields from finite sets E of elementary events ξ_i with associated probabilities p_i where $\sum p_i = 1$ and for any element $A \in \mathfrak{F}$ (a specific set of elements indexed by i), $\mathbb{P}_A = \sum p_{Ai}$, and $\mathbb{P}_A \in [0, 1]$.

We note that $\{\varnothing\} \in \mathfrak{F}$ and $E \subset \mathfrak{F}$. Since $\mathfrak{F}$ is a field, binary operations apply to elements of the field and since we can define the structure of the field without reference to specific (algebraic) binary operations the σ-field is also called in the literature a σ-algebra. In view of Theorem 2.5, we are mainly concerned with probabilities of isometric circle disjoint intersection events only and we will use the term σ-field more loosely to refer to specific restricted σ-fields $\mathfrak{F}$ omitting both the null element and all probability complements. We will be using Kolmogorov's concepts initially for assessment of probabilities associated with isometric circle intersections. His general σ-field concept can be specialised via Definition 2.6 in order to impose an algebra suitable for isometric circle intersection probabilities and we denote such by $\mathfrak{F}_n$:

Definition 2.6. *$\mathfrak{F}_n$ is a σ-field of events whose binary operator is set union and whose elementary events are the pairwise intersections of $n \in \{2, 4, 6 \cdots\}$ isometric circles representing $\frac{n}{2} \in \mathbb{N}$ matrices.*

Theorem 2.7. *For the σ-field $\mathfrak{F}_n$ of isometric circle intersection events for $\frac{n}{2} \in \mathbb{N}$ matrices,*

(1) *There are* $\frac{n(n-1)}{2}$ *elementary events.*

(2) *The only independent events are elementary and* $\frac{n}{2}$ *of the elementary events are independent while* $\frac{n(n-2)}{2}$ *are dependent.*

(3) *If the order of the set of elementary events is* m *then the order of the power set* $\mathfrak{F}_m$ *is* 2^m.

(4) *For* $\mathfrak{F}_n$ *containing* $m = \frac{n(n-1)}{2}$ *elementary events, the* m *equivalence classes of* $\mathfrak{F}_n$ *under union of* $k \in [1, m]$ *pairwise intersection events are of order* $\binom{m}{k}$, $k \in [1, m]$.

Proof.

(1) For $\frac{n}{2} \in \mathbb{N}$ matrices there are n isometric circles. We choose one of n circles and consider the intersection with one of the remaining $n - 1$ circles. Since the order is immaterial there are $\frac{n(n-1)}{2}$ ways in which the intersection can occur.

(2) Independent intersection events can only be joint pairwise intersection events, hence elementary. For independent intersections there is only one way to choose the second circle of a pair, hence $\frac{n}{2}$ of the elementary events are independent and $\frac{n(n-1)}{2} - \frac{n}{2} = \frac{n(n-2)}{2}$ are dependent.

(3) The set of non elementary events in $\mathfrak{F}_n$ is composed of all possible unions of the elementary events. If we place the elementary events in any specific order and apply a binary weighting to each then all possible unions (including the elementary events) correspond to all combinations of these weights. Since the order of the set of elementary events is $m = \frac{n(n-1)}{2}$, the set $\mathfrak{F}_n$ of events can then be indexed by an m-bit binary number and accordingly is of order 2^m.

(4) The number of equivalence classes is clearly equal to the order of the set of elementary events and the result follows since the number of subsets of k elementary events in a set of m such events is $\binom{m}{k}$.

□

2.2.3 Experimental definition

Assuming the need for computational analysis, we define an experiment by an algorithm implemented via a computer program which encapsulates an iteration of a random number generating algorithm that supplies arguments for specific defined functions. Of the set S of all possible outcomes of an experiment, actual events T are recorded from specific program runs. The set S is the domain of a random variable function X indexed by an outcome reference ξ, a particular instance of which from the event $T \subset S$ is $X(\xi)$.

Example 2.8.

Concept	***symbol***	***example***
Experimental outcomes	S	random matrices
Event	T	a set of $10,000,000$ specific matrix pairs A, B
Outcome	ξ	an index $\mathrm{i} \in [0, 9999999]$ into the event set
Random variable	$X(\xi)$	argument of an entry of a matrix $\mathrm{A_i}$.

We see that events, outcomes and random variables are quite distinct concepts.

2.2.4 Random events

Algorithms determine the way in which arguments involving random numbers determine experimental events but to make use of Kolmogorov's σ-fields we generalise the random variable definition. As indicated in Section 2.2.3 above, an event is a single outcome of a set of experiments, depending on the particular parameters under investigation for a given experiment an event may involve one or more random variables. For our purposes a *random event* is a mathematical structure or function of one or more random variables. To every random variable we can assign a probability density function, hence a probability that the variable is in any particular domain. Similarly for every random event, the probability is an expression of the likelihood of some stated circumstance occurring. In our context random events will usually be joint isometric circle intersections where we indicate by $\mathcal{A}$ the isometric circle of a matrix A and by $(\mathcal{A} \cap \mathcal{B})$ the intersection of the isometric circles of matrices A and B. That is, $\mathbb{P}_{(\mathcal{A} \cap \mathcal{B})}$ is the probability that the two isometric circles of matrices A and B intersect.

Example 2.9. *The isometric circle intersection event* $(\mathcal{A} \cap \mathcal{A}^{-1})$ *is independent of the event* $(\mathcal{B} \cap \mathcal{B}^{-1})$ *but* $(\mathcal{A} \cap \mathcal{B}^{-1})$ *is not independent of* $(\mathcal{A} \cap \mathcal{A}^{-1})$ *since certainly* $(\mathcal{A} \cap \mathcal{A}) \neq \varnothing$.

The following is based on Kolmogorov [39]:

Definition 2.10.

(1) *For independent random events* X, Y*, the joint probability is:*

$$\mathbb{P}_{X \cap Y} = \mathbb{P}_X \, \mathbb{P}_Y. \tag{2.11}$$

(2) *For mutually exclusive random events* X, Y*:*

$$\mathbb{P}_{X \cup Y} = \mathbb{P}_X + \mathbb{P}_Y. \tag{2.12}$$

(3) *For random events* X, Y*:*

$$\mathbb{P}_{X \cup Y} = \mathbb{P}_X + \mathbb{P}_Y - \mathbb{P}_{X \cap Y}. \tag{2.13}$$

In order to introduce the geometrical results as early as possible we leave the detailed development of the necessary probability and random variable concepts in our context to Chapter 4, Chapter 3 which follows here is based on this work. This approach entails a small amount of repetition.

Chapter 3

Random Möbius groups and the Fuchsian space

A Möbius transformation f with matrix representation $A \in GL(2,\mathbb{C})$ is a function of eight real variables. Normalisation to $\tilde{A} \in SL(2,\mathbb{C})$ leaves the linear fractional function invariant ($f = \tilde{f}$) but in six real variables. For a set of random Möbius transformations we want to view each random matrix in $SL(2,\mathbb{C})$ as a random event, which leaves us with the problem of deciding what is a reasonable way of determining the individual matrix entry distributions. A number of problems with definition of random matrices are discussed in [55]. It appears impractical to assign homogeneous uniform distributions to $SL(2,\mathbb{C})$ matrix entries as there is a determinant condition which sets up a highly non linear mutual constraint between the matrix entries and any attempt to impose uniform distributions on $GL(2,\mathbb{C})$ prior to normalisation is completely non productive. But an even greater problem is that we cannot specify uniform variables over infinite domains. If large finite domains are used for the variables defining A then the normalised variables constituting $\tilde{A}$ approximate uniform distributions only when the matrix is close to the identity, [55]. To progress further requires a different approach to defining a random transformation.

What we are looking for is a geometrically natural way of imposing distributions, preferably uniform, on random Möbius transformations. Indeed it turns out that an important class of Möbius transformations does have such natural random matrix representations and their structure facilitates both calculation and computation of various parameters and specifically provides rotationally invariant measures. We consider the set $\mathcal{F}$ of Möbius transformations:

$$f = \frac{\mathbf{az} + \overline{\mathbf{c}}}{\mathbf{cz} + \overline{\mathbf{a}}} : \hat{\mathbb{C}} \mapsto \hat{\mathbb{C}} \tag{3.1}$$

with matrix representation.

Theorem 3.1. *For a set $\mathcal{F}$ of matrices of the form $\begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix} \in PSL(2,\mathbb{C})$, denote by r the isometric circle radius of a specific matrix A representing $f \in \mathcal{F}$. Then:*

(1) *$\mathcal{F}$ forms a group under matrix multiplication.*

(2) *The trace of $f \in \mathcal{F}$ is real so $\mathcal{F}$ contains no strictly loxodromic elements.*

(3) *The isometric circles of A and A^{-1} of radii r intersect the unit circle $\mathbb{S}$ orthogonally and are centred on the circle of radius R concentric with $\mathbb{S}$ where $R^2 = r^2 + 1$ and the determinant condition becomes $|\mathbf{a}|^2 = |\mathbf{c}|^2 + 1$.*

(4) *The arc length intersection of the isometric circles with $\mathbb{S}$ is 2α where $\tan(\alpha) = r$ and $\sec(\alpha) = R$.*

(5) *$\mathcal{F}$ preserves the unit disc $\mathcal{D}$ (the interior of the unit circle $\mathbb{S}$) and its exterior $\mathcal{D}'$, hence $\mathcal{F}$ is a Fuchsian group.*

Proof. Let elements of G be represented by the matrices:

$$A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}, \quad B = \begin{pmatrix} \mathbf{e} & \overline{\mathbf{g}} \\ \mathbf{g} & \overline{\mathbf{e}} \end{pmatrix}.$$

(1) Since matrix multiplication is the group operation, $AB = \begin{pmatrix} \mathbf{a}\,\mathbf{e} + \overline{\mathbf{c}}\,\mathbf{g} & \mathbf{a}\,\overline{\mathbf{g}} + \overline{\mathbf{c}}\,\overline{\mathbf{e}} \\ \mathbf{c}\,\overline{\mathbf{e}} + \overline{\mathbf{a}}\,\mathbf{g} & \mathbf{c}\,\overline{\mathbf{g}} + \overline{\mathbf{a}}\,\overline{\mathbf{e}} \end{pmatrix}$. But $\overline{\mathbf{a}}\ \mathbf{e} + \overline{\mathbf{c}}\ \mathbf{g} = \mathbf{c}\ \overline{\mathbf{g}} + \overline{\mathbf{a}}\ \overline{\mathbf{e}}$ and $\overline{\mathbf{c}}\ \overline{\mathbf{e}} + \overline{\mathbf{a}}\ \mathbf{g} = \mathbf{a}\ \overline{\mathbf{g}} + \overline{\mathbf{c}}\ \mathbf{e}$, so $AB \in \mathcal{F}$. Also, since for $A \in SL(2,\mathbb{C})$, $\mathbf{a}\ \overline{\mathbf{a}} - \overline{\mathbf{c}}\ \mathbf{c} = 1$ and the inverse of A is $A^{-1} = \begin{pmatrix} \overline{\mathbf{a}} & -\overline{\mathbf{c}} \\ -\mathbf{c} & \mathbf{a} \end{pmatrix}$, we have $AA^{-1} = \begin{pmatrix} \mathbf{a}\,\overline{\mathbf{a}} - \overline{\mathbf{c}}\,\mathbf{c} & -\mathbf{a}\,\overline{\mathbf{c}} + \overline{\mathbf{c}}\,\mathbf{a} \\ -\mathbf{c}\,\overline{\mathbf{a}} - \overline{\mathbf{a}}\,\mathbf{c} & -\overline{\mathbf{c}}\,\mathbf{c} + \overline{\mathbf{a}}\,\mathbf{a} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hence the set G contains all products, all inverses of all elements, together with the identity since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is of the form $\begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$.

(2) trace(A) $= \mathbf{a} + \overline{\mathbf{a}} = 2\,\Re\mathrm{e}(\mathbf{a}) \in \mathbb{R}$.

(3) Inspection of the appropriate triangle in Figure 3.1 shows that the condition for orthogonal intersection of an isometric circle with $\mathbb{S}$ is that $R^2 = 1 + r^2$ where R is the radius of the circle on which the isometric circles are centred and $r = \frac{1}{|\mathbf{c}|}$ is the isometric circle radius, then $R \geq r \geq 1$ and orthogonal intersections can occur only for the centre of the intersecting isometric circle on or outside $\mathbb{S}$. Since the centres of the isometric circles of a matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix}$ in $SL(2,\mathbb{C})$ are $-\frac{\mathbf{d}}{\mathbf{c}}$ and $\frac{\mathbf{a}}{\mathbf{c}}$,

$$\left|\frac{\mathbf{a}}{\mathbf{c}}\right| = \left|-\frac{\mathbf{d}}{\mathbf{c}}\right| \Leftrightarrow \mathbf{a}\,\overline{\mathbf{a}} = \mathbf{d}\,\overline{\mathbf{d}}$$

and since $\left|\frac{\mathbf{a}}{\mathbf{c}}\right| = \left|-\frac{\mathbf{d}}{\mathbf{c}}\right|$ is the radius R, the orthogonal intersection condition above implies:

$$\begin{aligned} &\left|\tfrac{\mathbf{a}}{\mathbf{c}}\right|^2 = \left|-\tfrac{\mathbf{d}}{\mathbf{c}}\right|^2 = 1 + \tfrac{1}{\mathbf{c}\,\overline{\mathbf{c}}} \\ &\Leftrightarrow |\mathbf{a}|^2 = |\mathbf{d}|^2 = |\mathbf{c}|^2 + 1. \end{aligned} \tag{3.2}$$

If we rewrite this equation as $\mathbf{a}\ \overline{\mathbf{a}} - \mathbf{c}\ \overline{\mathbf{c}} = 1$ we see that the orthogonal intersection condition is satisfied by the determinant condition for an element of $\mathcal{F}$ to be in $SL(2,\mathbb{C})$.

(4) From the geometric construction in Figure 3.1, the arc length intersection of the disc of the isometric circle of an element of $\mathcal{F}$ is 2α where $\sec(\alpha) = R$ and $\tan(\alpha) = r$.

(5) Since G contains no strictly loxodromic elements, the transformation of any point in $\hat{\mathbb{C}}$ consists of an inversion in the isometric circle of the matrix A representing f followed by a reflection in the perpendicular bisector L of the line joining the centres of this isometric circle and that of the inverse A^{-1} (see for example Ford [20]). For elements of $\mathcal{F}$ both isometric circles are centred on a circle C concentric with $\mathbb{S}$, hence this inversion leaves a point $\mathbf{z}$ the same radial distance from the centre of $\mathbb{S}$; that is, if and only if $\mathbf{z}$ is inside $\mathbb{S}$ does it remain inside $\mathbb{S}$ after the inversion. Again since the isometric circle of A^{-1} is centred on C, after the reflection in L $f(\mathbf{z})$ remains inside $\mathbb{S}$ if and only if $\mathbf{z}$ was inside $\mathbb{S}$, so G preserves the unit disc D (the interior of the unit circle $\mathbb{S}$) and its also its exterior D'.

□

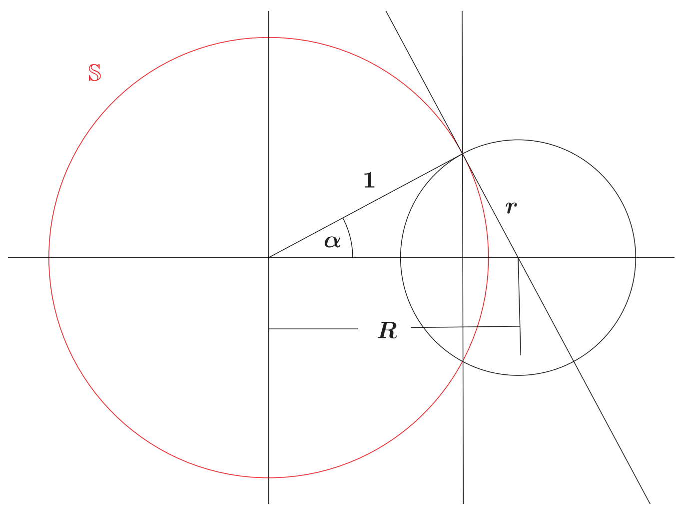


Figure 3.1: Orthogonal intersection of an isometric circle of a transformation with $\mathbb{S}$: defining the isometric circle radius r, the radius R of the circle on which the isometric circles are centered and the angle α which is half the intersection arc of the disc of the isometric circle with $\mathbb{S}$.

Since it is always possible to find a Möbius transformation that maps a circle to any other circle there are transformations that map any Fuchsian group to $\mathcal{F}$, and we refer to $\mathcal{F}$ as Fuchsian space. We can always find a Möbius transformation that maps $\mathbb{S}$ to the real axis, and since every $f \in \mathcal{F}$ has isometric circles orthogonal to $\mathbb{S}$, under suitably chosen transformation the isometric circles cross $\mathbb{R}$ orthogonally and have their centres on $\mathbb{R}$. Hence we can construct an algebraic isomorphism, $[1, i, -1, -i] \mapsto [1, \infty, -1, 0] : \mathcal{F} \equiv PSL(2, \mathbb{R})$, the isometry group of two-dimensional hyperbolic space.

$\mathcal{F}$ contains both the usual rotation subgroup $\mathbf{K}$ of the disc, $z \mapsto \zeta^2 z$, $|\zeta| = 1$, and the nilpotent subgroup (conjugate to the translations); these have the respective matrix representations:

$$\begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}, \quad |\zeta| = 1, \qquad \begin{pmatrix} 1+it & t \\ t & 1-it \end{pmatrix}, \quad t \in \mathbb{R}. \tag{3.3}$$

3.1 Distributions on the space of matrices $\mathcal{F}$

We use a notation with brackets to indicate a domain interval in the usual fashion and subscripts where necessary to distinguish between types of domain. A distribution of a random variable over a domain is indicated by the symbol $\in$, a subscript to $\in$ indicates a specific distribution (for example u for uniform) and a subscript also may indicate a domain type (for example $\circ$ for circular).

Example 3.2.

(1) *$D = [a, b]_{\mathbb{R}}$ is a closed interval domain for a random variable, $D \subset \mathbb{R}$.*

(2) *$x \in_u D$ describes a random variable x distributed uniformly over the (unspecified) domain D.*

We impose distributions on the entries of the matrices

$$(i) \quad \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix} \qquad (ii) \quad \begin{pmatrix} 1+it & t \\ t & 1-it \end{pmatrix} \in \mathcal{F}, \tag{3.4}$$

selecting:

- (i) Unit vectors $\hat{\mathbf{a}} = \dfrac{\mathbf{a}}{|\mathbf{a}|}$ and $\hat{\mathbf{c}} = \dfrac{\mathbf{c}}{|\mathbf{c}|}$ with uniformly distributed angular measure in the circle $\mathbb{S}$, and
- (ii) $t = |\mathbf{c}| \geq 0$ so that the half arc length intersection of the isometric circle with $\mathbb{S}$, $\alpha = \arctan\left(\frac{1}{t}\right)$ and also the total arc length intersection 2α are uniformly distributed $[0, \frac{\pi}{2}]$ and $[0, \pi]$ respectively.

Notice that where the matrix entries are $\mathbf{a} = a\, e^{i\theta_a}$ etc., the product $\hat{\mathbf{a}}\,\hat{\mathbf{c}} = e^{i\theta_a}\, e^{i\theta_c} = e^{i(\theta_a+\theta_c)}$ is uniformly distributed on the circle as a simple consequence of the rotational invariance of arclength measure. Further, this measure is equivalent to the uniform probability measure $\arg(\mathbf{a}) \in [0, 2\pi)$. It is thus clear that this selection process is invariant under the rotation subgroup $\mathbf{K}$ of the circle.

We have $|\mathbf{a}|^2 = t^2+1$, so if α is uniformly distributed in $[0, \frac{\pi}{2}]$, then since $t = \cot(\alpha)$ is strictly decreasing with increasing α on that domain the probability distribution of $|\mathbf{a}| = \operatorname{cosec}(\alpha)$ can be calculated via the change of variables formula with result as in the following lemma:

Lemma 3.3. *The random variable $|\mathbf{a}| \in (1, \infty)$ has p.d.f. given by:*

$$\mathfrak{D}_{|a|}(x) = \frac{2}{\pi} \frac{1}{x\sqrt{x^2-1}} \qquad x \in (1, \infty).$$

Another equivalent formulation is the following. We require that the matrix entries **a** and **c** have arguments $\theta_a = \arg(\mathbf{a})$ and $\theta_c = \arg(\mathbf{c})$ uniformly distributed on $\mathbb{R} \pmod{2\pi}$. We write this as $\arg(\mathbf{a}) \in_u [0, 2\pi)_\circ$ and $\arg(\mathbf{c}) \in_u [0, 2\pi)_\circ$ and illustrate with a lemma which follows from Theorem 3.23.

Lemma 3.4. *If* $\arg(\mathbf{a}), \arg(\mathbf{b}) \in_u [0, 2\pi)_\circ$, *then* $\arg(\mathbf{ab}), \arg(\mathbf{a}/\mathbf{b}) \in_u [0, 2\pi)_\circ$.

Definition 3.5. *The elements of a set of random variables distributed uniformly over an interval* $I \subset \mathbb{S}$ *are* ***circular uniform****.*

If θ, η are selected from a uniformly distributed probability measure on $[0, 2\pi)$, then the p.d.f. for $\theta + \eta \in [0, 4\pi]$ is as shown in Figure 3.2:

$$g(\zeta) = \begin{cases} \dfrac{\zeta}{4\pi^2} & 0 \le \zeta < 2\pi \\ \dfrac{4\pi - \zeta}{4\pi^2} & 2\pi \le \zeta \le 4\pi. \end{cases}$$

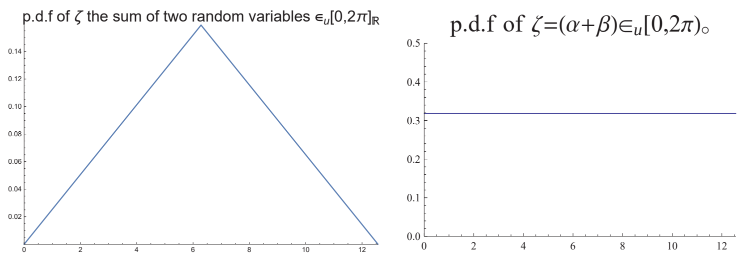


Figure 3.2: p.d.f. of the sum of two random variables $\in_u [0, 2\pi)$.

We reduce mod 2π and observe

$$\frac{\zeta}{4\pi^2} + \frac{4\pi - \zeta - 2\pi}{4\pi^2} = \frac{1}{2\pi}$$

and this gives us once again the uniform probability density on $[0, 2\pi)$. The result also follows for $\theta - \eta$ as clearly $-\eta \in_u [0, 2\pi]_\mathbb{R}$ and $\theta - \eta = \theta + (-\eta)$, and also for $k\,\theta \in_u [0, 2\pi)_\mathbb{R}$, $\quad k \in \mathbb{R}$ as we will later show that this is an additive group. In what follows we will also need to consider variables supported in $[0, \pi]$ or smaller sub intervals and as above we will use nomenclature such as the $\alpha \in_u [0, \pi]_\circ$ for circular uniform random variables α over any subdomain of a circle.

We will shortly calculate some distributions naturally associated with Möbius transformations such as traces and translation lengths, but first note that every Möbius transformation of the unit disc $\mathcal{D}$ can be written in the form:

$$z \mapsto \zeta^2 \frac{z - w}{1 - \bar{w}z}, \quad |\zeta| = 1, w \in \mathcal{D} \tag{3.5}$$

For matrices in the form 3.4 we can see this by setting $\zeta^2 = \mathbf{a}/\bar{\mathbf{a}}$ and $w = -\bar{\mathbf{c}}/\bar{\mathbf{a}}$. It follows that $|\zeta| = 1$, and since $|\mathbf{c}|^2 = |\mathbf{a}|^2 - 1$ implies $|\mathbf{c}| \le |\mathbf{a}|$ it is clear that w is a vector inside $\mathcal{D}$. Furthermore, if we write the arguments of the entry vectors as θ_a etc., then $\zeta^2 = \mathbf{a}/\bar{\mathbf{a}} = e^{2i\theta_a}$ therefore $\zeta = \mathrm{e}^{\mathrm{i}\theta_\mathrm{a}}$ and $w = -\bar{\mathbf{c}}/\bar{\mathbf{a}} = \frac{|\mathbf{c}|}{|\mathbf{a}|}e^{-i(\theta_a + \theta_c)}$ and it follows that both ζ and w are circular uniform. The matrix representation of (3.5) in the form (3.4 (i)) is:

$$\zeta^2 \frac{z-w}{1-\bar{w}z} \leftrightarrow \begin{pmatrix} \frac{\zeta}{\sqrt{1-|w|^2}} & -\frac{\zeta w}{\sqrt{1-|w|^2}} \\ -\frac{\zeta \bar{w}}{\sqrt{1-|w|^2}} & \frac{\zeta}{\sqrt{1-|w|^2}} \end{pmatrix}.$$

Then since $\mathbf{a} = \zeta\frac{1}{\sqrt{1-|w|^2}}$, $|\mathbf{a}| = \frac{1}{\sqrt{1-|w|^2}}$ and $2\ \alpha = 2\sin^{-1}\left(\sqrt{1-|w|^2}\right) \in [0,\pi]$, where the half intersection arc is $\alpha \in [0, \frac{\pi}{2}]$,

$$|w| = \frac{|\mathbf{c}|}{|\mathbf{a}|} = |\cos(\alpha)|\,.$$

From the table in Figure 4.3 we have the p.d.f. of $\cos(\theta)$ for $\theta \in_u [0,\pi]$ as $\frac{1}{\pi\sqrt{1-y^2}}$, $y \in [-1,1]$ and the p.d.f. of $|\cos(\theta)|$ is $\frac{2}{\pi\sqrt{1-y^2}}$, $\theta \in [0, \frac{\pi}{2}]$ $y \in [0,1]$ (which is the same as the p.d.f. of $\cos(\theta)$ for $\theta \in [0, \frac{\pi}{2}]$). Then

$$\alpha = \arccos(|w|) = \arcsin(\sqrt{1-|w|^2}) \in [0, \pi/2]$$

is uniformly distributed and we find $|w|$ has the p.d.f. as in Figure 3.3.

$$g(|w|) = \frac{2}{\pi\sqrt{1-|w|^2}}\,,\ \ |w| \in [0,1]$$

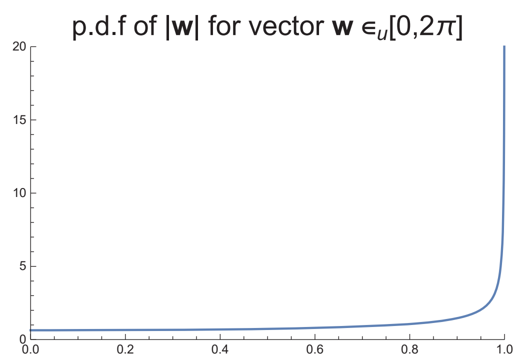


Figure 3.3: p.d.f. of $|\mathbf{w}|$ for the random vector $\mathbf{w} \in \mathcal{D} = -\frac{\bar{\mathbf{c}}}{\bar{\mathbf{a}}} \in_u [0, 2\pi)$.

But noting that for a transformation f represented by a matrix in the form (3.4 (i)), $\frac{\mathbf{c}}{\mathbf{a}} = f(0)$, we have the Corollary 3.6:

Corollary 3.6. *Let $f \in \mathcal{F}$ be a random Möbius transformation in the Fuchsian space, then the p.d.f. for $y = |f(0)|$ is $\frac{2}{\pi\sqrt{1-y^2}}$. The expected value of $|f(0)|$ is:*

$$E[[\ |f(0)|\ ]] = \frac{2}{\pi}\int_0^1 y\frac{1}{\sqrt{1-y^2}}\,dy = \frac{2}{\pi} \approx 0.63662.$$

3.2 Isometric circles

The isometric circles of the Möbius transformation f defined by (3.1) are the two circles:

$$C_+ = \left\{ \left| \mathbf{z} + \frac{\overline{\mathbf{a}}}{\overline{\mathbf{c}}} \right| = \frac{1}{|\mathbf{c}|} \right\}, \quad C_- = \left\{ \mathbf{z} : \left| \mathbf{z} - \frac{\mathbf{a}}{\overline{\mathbf{c}}} \right| = \frac{1}{|\mathbf{c}|} \right\}.$$

Then $f^{\pm 1}(C_\pm) = C_\mp$. Since $|\mathbf{a}|^2 = 1 + |\mathbf{c}|^2 \geq 1$, both these circles meet the unit circle in an arc of magnitude $\theta \in [0, \pi]$. Some elementary trigonometry reveals that

$$\sin\left(\frac{\theta}{2}\right) = \frac{1}{|\mathbf{a}|}. \tag{3.6}$$

Figures 3.4 and 3.5 show respectively the intersections with $\mathbb{S} \in \hat{\mathbb{C}}$ of the two isometric circles of a hyperbolic and an elliptic transformation $f \in \mathcal{F}$ using nomenclature as in Theorem 2.1; the figures should be read subject to a rotation by θ_c. From Theorem 2.1, in hyperbolic space the fixed points of hyperbolic transformations in $\mathcal{F}$ lie on the unit circle and also lie on the common geodesic between isometric circle centres, this line is the axis of the transformation. In $\hat{\mathbb{C}}$ the transformation axis is then parallel to the entry vector $e^{-i\theta_c}$.

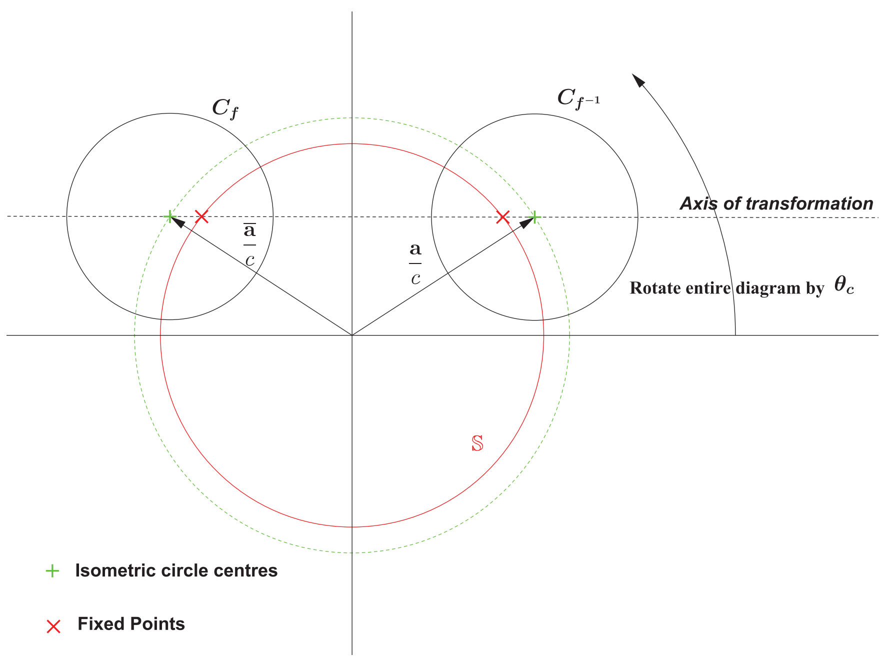


Figure 3.4: Orthogonal intersection of the two isometric circles C_f and $C_{f^{-1}}$ of a hyperbolic transformation $f \in \mathcal{F}$ with the unit circle $\mathbb{S}$ in $\hat{\mathbb{C}}$ showing fixed points and isometric circle centres along with the axis of the transformation. For f parabolic the circles are tangential at their intersection with $\mathbb{S}$ which is the single fixed point.

By our choice of distribution for $|\mathbf{a}|$ we obtain the following result:

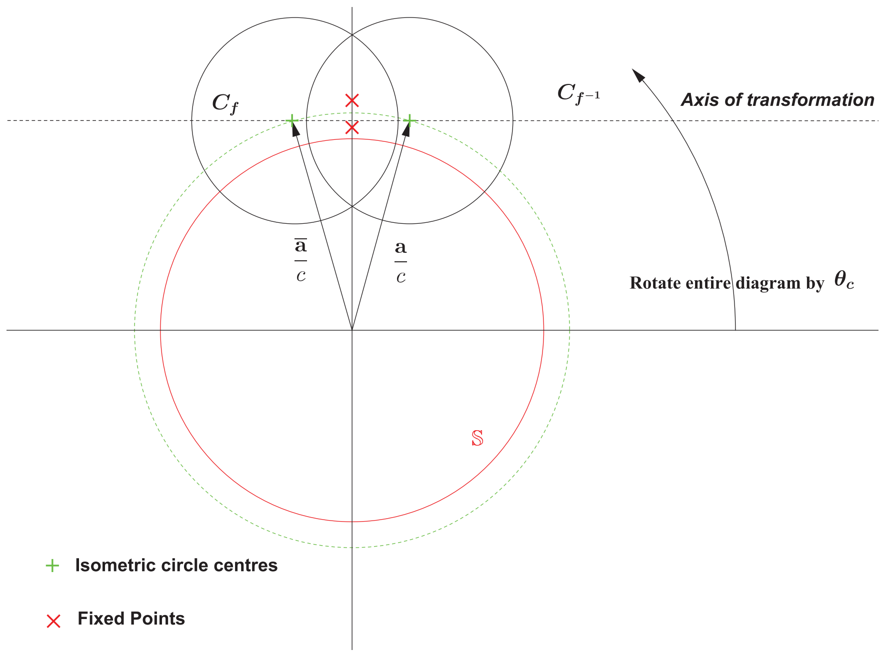


Figure 3.5: Orthogonal intersection of the two isometric circles C_f and $C_{f^{-1}}$ of an elliptic transformation $f \in \mathcal{F}$ with the unit circle $\mathbb{S}$ in $\hat{\mathbb{C}}$ showing fixed points in the exterior of $\mathbb{S}$.

Lemma 3.7. *The arcs determined by the intersections of the finite discs bounded by the the isometric circles of f chosen according to the distribution (i) and (ii), are centered on uniformly distributed points of $\mathbb{S}$ and have arc lengths uniformly distributed in $[0, \pi]$.*

It is this lemma which supports our claim that the p.d.f. on $\mathcal{F}$ is natural and suggests the way forward for an analysis of random Kleinian groups.

3.3 Distributions on $\mathbb{S}$ and the group $\mathfrak{C}$

We now consider random variables with uniform distributions over domains within a circle.

3.3.1 Circular uniform distribution

The following two theorems are trivial where points and arcs are algebraic variables rather than random variables but proofs are included as the consequential development is far from trivial.

Theorem 3.8. *Points on a Euclidean circle have a natural uniform distribution of position on $[0, 2\pi)_\circ$ unless subject to an imposed distribution.*

Proof. Since the Euclidean line $\mathbb{R}$ is an additive group of real numbers, points selected without favour are uniformly distributed over any finite interval $I \in \mathbb{R}$, hence specifically so for the interval $[0, 2\pi) \in \mathbb{R}$. Since Euclidean circles of radius r map bijectively and locally isometrically onto intervals $[0, 2\pi r) \in \mathbb{R}$, the points on a circle are distributed uniformly. $\square$

While we may regard a point on a circle as an arc of zero magnitude, in general to specify an arc we require both magnitude and position. From Theorem 3.8 a natural arc has uniformly distributed position, it is immaterial whether this is defined by start or end points or a mid-point. However, having chosen a point that specifies the position of an arc α uniformly in $\mathbb{S}$ we cannot say that any other point in α is uniformly distributed even if the arc length of α is uniformly distributed.

Theorem 3.9. *Arcs on a Euclidean circle have a natural uniform distribution of magnitude in* $[0, 2\pi)_\circ$ *unless subject to an imposed distribution.*

Proof. The result follows from Theorem 3.8 since arcs of Euclidean circles of radius r map bijectively and locally isometrically onto intervals $[0, 2\pi r) \in \mathbb{R}$. We note that both random points on a circle and random arc magnitudes modulo 2π are random numbers in $[0, 2\pi)$. □

Corollary 3.10. *A point distributed naturally on a circle lies within an arc of magnitude* θ *with probability* $\mathbb{P} = \frac{\theta}{2\pi}$.

Then the elements of $\mathfrak{C}$ are circular uniform. We denote by $\alpha_\circ$ an arc of length α in the unit circle $\mathbb{S}$, noting that any statement about distributions of arcs or points made with respect to $\mathbb{S}$ also applies to arcs or points on any circle.

3.3.2 The group $\mathfrak{C}$

Theorem 3.11. *The set* $\mathfrak{C}_p$ *of all circular uniform random points on* $\mathbb{S}$ *is a group under addition modulo* 2π.

Proof. Let $x = a \pm b$ where a and b are real random variables distributed uniformly over a domain $(-k, k)_\mathbb{R}$. Then via the characteristic function method we determine that the random variable x has distribution $\mathfrak{D}_{(a\pm b)_\mathbb{R}}$ supported on the domain $(-2k, 2k)_\mathbb{R}$ as follows:

$$\mathfrak{D}_{(a\pm b)_\mathbb{R}}(x) = \frac{2k - |x|}{4k^2} \quad -2k \leq x \leq 2k. \tag{3.7}$$

Suppose now that $k = \pi$ and that $(-2\pi, 2\pi)_\circ$ is a circular domain, then since $\mathfrak{D}_{(a\pm b)_\mathbb{R}}(x)$ is an even symmetrical distribution we superpose the piecewise p.d.f.'s over the two sub domains $(-2\pi, 0)$ and $[0, 2\pi)$ (see Figure 3.2) and conclude that:

$$a, b \in_u [0, 2\pi)_\circ \text{ therefore a} \pm \text{b} \in_\text{u} [0, 2\pi)_\circ.$$

Hence the set $\mathfrak{C}_p$ is closed under addition modulo 2π, and contains the inverses of all elements together with an additive identity, hence $\mathfrak{C}_p$ is a group. □

Corollary 3.12.

(1) *The group* $\mathfrak{C}_p$ *has for identity the element* 2π.

(2) *The inverse of* θ *in* $\mathfrak{C}_p$ *is* $2\pi - \theta$.

Proof. Suppose $\theta, \eta \in \mathbb{S}$, then:

(1) The only solution in $\mathfrak{C}_p$ to $\theta + \eta = \theta$ is $\eta = 2\pi|_{mod(2\pi)}$.

(2) The only solution in $\mathfrak{C}_p$ to $\theta + \eta = 0$ is $\eta = 2\pi - \theta$.

□

Theorem 3.13. *The set $\mathfrak{C}_a$ of all circular uniform random arcs on $\mathbb{S}$ is a group under union modulo 2π.*

Proof. Let α, β be arcs in $\mathbb{S}$. Then for a point $x \in \mathbb{S}$, $(x \in \alpha) \cup (x \in \beta)$ if and only if $x \in \alpha \cup \beta$, the result follows from Theorem 3.11. □

Corollary 3.14.

(1) *The group $\mathfrak{C}_a$ has for identity the element $\mathbb{S}$.*

(2) *The inverse of θ in $\mathfrak{C}_a$ is $\overline{\theta} = \mathbb{S} \backslash \theta$.*

Proof. Since the group $\mathfrak{C}_a$ is closed, $\mathbb{S}$ is itself an arc (of magnitude 2π) in $\mathfrak{C}_a$. Suppose $\theta, \eta \in \mathfrak{C}_a$, then:

(1) The only solution in $\mathfrak{C}_a$ to $\theta + \eta = \theta$ is $\eta = 2\pi|_{mod(2\pi)} = \mathbb{S}$.

(2) The only solution in $\mathfrak{C}_a$ to $\theta + \eta = 0$ is $\eta = 2\pi - \theta = \mathbb{S} \backslash \theta$.

□

We note that while the inverse of an element θ of $\mathfrak{C}_p$ is $(2\pi - \theta)|_{mod(2\pi)}$ and the identity is 2π, the inverse of an element of $\mathfrak{C}_a$ is its complement in $\mathbb{S}$ and the identity is $\mathbb{S}$ itself.

Lemma 3.15. *The groups $\mathfrak{C}_p$ and $\mathfrak{C}_a$ are homeomorphic.*

Accordingly, we will where the context is unambiguous refer to either group of circular uniform random variables as $\mathfrak{C}$ and signify a general group operator by $\bigoplus$.

Corollary 3.16. *If α_i are elements of $\mathfrak{C}$ with $\bigoplus \alpha_i \bigoplus \beta \in \mathfrak{C}$ then either $\beta \in \mathfrak{C}$ or β is constant.*

In the context of Corollary 3.16 we consider a constant point to be fixed in $\mathbb{S}$ and a constant arc be an arc of fixed length (but not necessarily fixed position).

3.3.3 Arcs and points

Theorem 3.17. *A random point $\mathbf{z}$ on a circle lies outside all of n circular uniform random arcs with probability $\mathbb{P} = \frac{1}{n+1}$. That is,*

$$\mathbb{P}_{(\mathbf{z} \notin \cup_{i=1}^{n} \alpha_i)} = \frac{1}{n+1} \qquad \alpha_i \in \mathfrak{C}. \tag{3.8}$$

Proof. Since the position of a random arc α_i on $\mathbb{S}$ does not affect the probability that a random point is in α_i we can consider the condition where n random arcs happen to be contiguous on $\mathbb{S}$, leaving an $n+1^{th}$ non constant arc α_{n+1}. (In practice no such condition need be imposed; since $\mathfrak{C}_a$ is a group the union of arcs in $\mathbb{S}\backslash \cup \alpha_i$ modulo 2π will do just as well). Then:

$$\cup_1^{n+1}\alpha_i = \mathbb{S}.$$

Since the n original arcs and $\mathbb{S}$ (the group identity) are all in $\mathfrak{C}_a$ we conclude that the $n+1^{th}$ arc must be constant or in $\mathfrak{C}_a$, and since α_{n+1} is non constant it must be circular uniform. Then a random point $\mathbf{z}$ is in any one of the $n+1$ arcs with equal probability $\mathbb{P} = \frac{1}{n+1}$. Now a point $\mathbf{z}$ that is in none of the n original arcs must be in the $n+1^{th}$ arc, hence $\mathbf{z}$ lies outside all the n arcs with probability $\mathbb{P} = \frac{1}{n+1}$. □

3.3.4 Matrix entry vectors

Definition 3.18. *The **entry vectors** of a matrix in $A \in GL(2,\mathbb{C})$ are the complex matrix entries A_{mn} expressed as vectors where if $A_{mn} = \mathbf{z} = x + iy$ then the vector (x, y) is written $\mathbf{z} = |\mathbf{z}|\ e^{\arg(\mathbf{z})}$.*

We will be interchanging between complex number and vector representations at will, and using the term *entry vector* to refer to a matrix entry written in either form. The matrix entries are not of equal significance, $\mathbf{c}$ alone determines the isometric circle radius while $\mathbf{a}$ and $\mathbf{d}$ alone occur in the trace of the matrix, and accordingly we will often pair these two entries together. The entry $\mathbf{b}$ having neither distinction will be treated as the dependent entry for matrices in $SL(2,\mathbb{C})$.

Definition 3.19. *If the arguments of the entry vectors $\mathbf{a}, \mathbf{b}, \mathbf{c}$ and $\mathbf{d}$ of a matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix} \in GL(2,\mathbb{C})$ are circular uniform then we say that the matrix A is circular uniform.*

The proof of the following theorem shows how the vector representation of complex matrix entries gives us a new perspective on the meaning of $SL(2,\mathbb{C})$ as a subgroup of $GL(2,\mathbb{C})$.

Theorem 3.20. *If the arguments of the entry vectors $\mathbf{a}, \mathbf{d}$ and $\mathbf{c}$ of a matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix} \in SL(2,\mathbb{C})$ are circular uniform then the matrix A is circular uniform.*

Proof. Suppose $A = \begin{pmatrix} ae^{i\theta_a} & be^{i\theta_b} \\ ce^{i\theta_c} & de^{i\theta_d} \end{pmatrix} \in SL(2,\mathbb{C})$, then the determinant condition is:

$$a\ e^{i\theta_a} d\ e^{i\theta_d} - b\ e^{i\theta_b} c\ e^{i\theta_c} = 1.$$

We can write this as a vector equation:

$$ad\ e^{i(\theta_a+\theta_d)} = bc\ e^{i(\theta_b+\theta_c)} + 1\ e^{i0}. \tag{3.9}$$

Figure 3.6 shows a representation of the vector summation in (3.9).

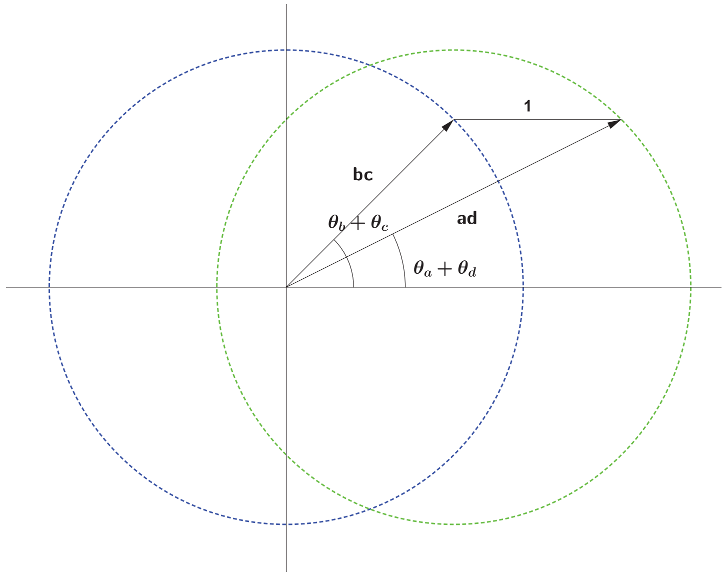


Figure 3.6: What it means for a matrix to be in $SL(2,\mathbb{C})$: vectors $bc\ e^{i(\theta_b+\theta_c)}$ and $ad\ e^{i(\theta_a+\theta_d)}$ are mutually constrained.

If in (3.9) we regard the scalar products ad and bc as parameters then in Figure 3.6 for every given parameter set $\{ad, bc\}$, the blue circle is the locus of points $bc\ e^{i(\theta_b+\theta_c)}$ as $(\theta_b + \theta_c)$ varies. To arrive at the locus of points as $(\theta_a + \theta_d)$ varies (the green circle) we must displace every point on the blue circle by 1 to the right; the locii are then two identical but displaced circles. That is, the determinant condition for a matrix in $SL(2,\mathbb{C})$ constrains the vectors $bc\ e^{i(\theta_b+\theta_c)}$ and $ad\ e^{i(\theta_a+\theta_d)}$ to a point-by-point bijective relationship for each constant set of real numbers ad and bc. We have that the vector arguments θ_a, θ_d and θ_c are in $\mathfrak{C}$ the set of all circular uniform random variables so this bijective relationship between the locii of the product vectors means:

$$(\theta_a + \theta_d) \in \mathfrak{C} \Leftrightarrow (\theta_b + \theta_c) \in \mathfrak{C}. \tag{3.10}$$

But $\mathfrak{C}$ is an additive group, so:

$$\theta_a, \theta_d \in \mathfrak{C} \Rightarrow (\theta_a + \theta_d) \in \mathfrak{C}$$

therefore, from (3.10),

$$(\theta_b + \theta_c) \in \mathfrak{C}.$$

But since $\theta_c \in \mathfrak{C}$ and $\mathfrak{C}$ is an additive group, unless θ_b is constant:

$$\theta_b \in \mathfrak{C}.$$

The conclusion applies to all sets of real parameters $\{ad, bc\}$ hence to all matrices in $SL(2,\mathbb{C})$.
□

Corollary 3.21. *If any three of the entry vectors of a matrix in $SL(2,\mathbb{C})$ are circular uniform then so is the fourth.*

Definition 3.22. *If a vector has argument with circular uniform distribution then we say that the vector is circular uniform.*

Theorem 3.23. *The set of all circular uniform vectors is a group under addition.*

Proof. If we replace the vector $1\ e^{i0}$ in (3.9) by any constant vector $\mathbf{k}$ then the reasoning of Theorem 3.20 can still be applied. That is, if we generalise (3.9) to:

$$k_v v\ e^{i\alpha_v} = k_u u\ e^{i\alpha_u} + \mathbf{k} \tag{3.11}$$

then with reference to Figure 3.7 the vector $\mathbf{k}$ applies a constant translation to the vector $k_u\mathbf{u}$. Since translations in $\mathbb{R}^2$ are conformal transformations the locii of the points defined by vectors $\mathbf{u}$ and $\mathbf{v}$ are related bijectively, and:

$$\alpha_u \in \mathfrak{C} \Leftrightarrow \alpha_v \in \mathfrak{C}.$$

By extension, whenever a constant vector $\mathbf{k}$ imposes a constraint on a linear combination of vectors as in (3.12) below:

$$\sum_{j=0}^{n-1} k_j v_j\ e^{i\alpha_j} = \mathbf{k} \tag{3.12}$$

for scalar multipliers k_j and vectors $\mathbf{v_j} = v_j\ e^{i\alpha_j}$, then a vector argument α_i must be circular uniform (or constant) if the remaining $n-1$ vector arguments are circular uniform. As we are free to take $\mathbf{k} = \mathbf{0}$ the set of all vectors $\mathbf{v_j}$ with arguments in $\mathfrak{C}$ must form an additive group. □

More generally, we can always treat such a constant vector $\mathbf{k}$ as the kernel of a homomorphism which maps the set of vectors $\{\mathbf{v_j}\}$ onto a space $\{\mathbf{u_j}\}$ such that for each j,

$$k_j \mapsto \frac{k_j}{|\mathbf{k}|}; \quad \arg(\mathbf{k}) \mapsto 0$$

and such a homomorphism (consisting of a dilation and a rotation) will reduce any non zero constant vector to $1 = 1e^{i0}$ as in Theorem 3.20. Since these transformations are conformal they do not affect whether any particular vectors are circular uniform or not, and we state the following as corollary:

Corollary 3.24. *Neither multiplication of vectors by complex constants nor addition of complex constants affects the condition of circular uniform distribution of components of a random variable expression.*

Theorem 3.11 establishes that $\{\alpha_j \in_u [0, 2\pi)_\circ\}$ is an additive group, this is a non trivial result although $\{a_j \in \mathbb{R}\}$ is an additive group. Theorem 3.23 establishes that the set of all circular uniform vectors is an additive group, again this is not a trivial result despite a similar result for algebraic vectors in $\mathbb{R}^2$. Algebraic results cannot be taken over to random variable algebra without justification.

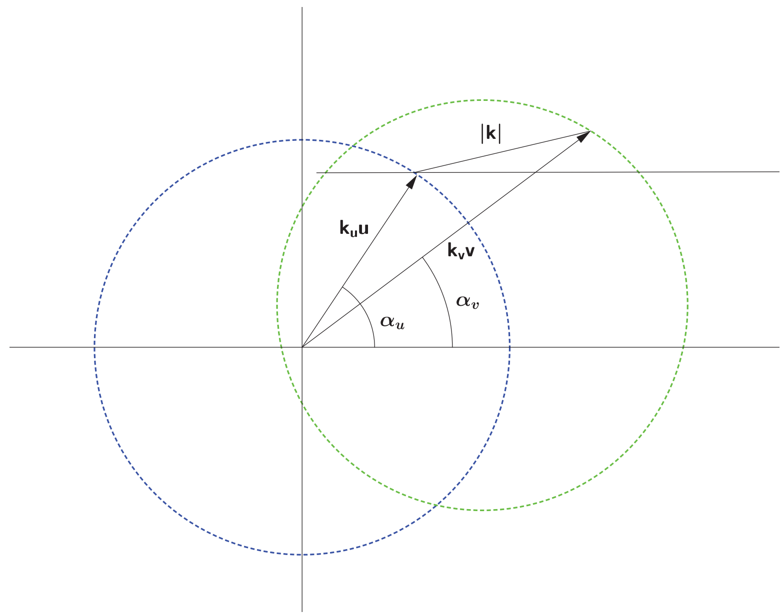


Figure 3.7: Linear combination of two constrained vectors.

Corollary 3.25. *If a set of circular uniform vectors* $\{\mathbf{v}_j\}$ *remains circular uniform with the inclusion of a vector* $\mathbf{u}$ *then* $\mathbf{u}$ *is either circular uniform or constant.*

Theorem 3.26. *The set of all circular uniform matrices in* $GL(2,\mathbb{C})$ *is a group.*

Proof. It is sufficient to show that a general matrix product AB for A, B circular uniform is a circular uniform matrix. Suppose $A = \begin{pmatrix} a\ e^{i\theta_a} & b\ e^{i\theta_b} \\ c\ e^{i\theta_c} & d\ e^{i\theta_d} \end{pmatrix}$ and $B = \begin{pmatrix} e\ e^{i\theta_e} & f\ e^{i\theta_f} \\ g\ e^{i\theta_g} & e\ h^{i\theta_h} \end{pmatrix}$ are circular uniform matrices in $GL(2,\mathbb{C})$. We form the product:

$$AB = \begin{pmatrix} ae\ e^{i(\theta_a+\theta_e)} + bg\ e^{i(\theta_b+\theta_g)} & af\ e^{-i(\theta_a+\theta_f)} + bh\ e^{(\theta_b+\theta_h)} \\ \\ ce\ e^{i(\theta_c+\theta_e)} + dg\ e^{i(\cos(\theta_d+\theta_g)} & cf\ e^{-i(\theta_c+\theta_f)} + dh\ e^{i(\theta_d+\theta_h)} \end{pmatrix}. \tag{3.13}$$

The result follows from Theorem 3.23 since all entries of AB in (3.13) are linear combinations of circular uniform vectors. □

Theorem 3.27. *If a Möbius transformation is represented by a circular uniform matrix in* $GL(2,\mathbb{C})$ *then the arguments of the vectors through the isometric circle centres in* $\hat{\mathbb{C}}$ *are circular uniform.*

Proof. Suppose $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix} = \begin{pmatrix} ae^{i\theta_a} & be^{i\theta_b} \\ ce^{i\theta_c} & de^{i\theta_d} \end{pmatrix}$, then the vectors through the isometric circle centres are:

$$\begin{aligned} -\tfrac{\mathbf{d}}{\mathbf{c}} &= -\tfrac{d\ e^{i\theta_d}}{c\ e^{i\theta_c}} &= -\tfrac{d}{c}e^{i(\theta_d-\theta_c)} \\ \tfrac{\mathbf{a}}{\mathbf{c}} &= \tfrac{a\ e^{i\theta_a}}{c\ e^{i\theta_c}} &= \tfrac{a}{c}e^{i(\theta_a-\theta_c)} \end{aligned} \tag{3.14}$$

and the arguments of the vectors to the isometric circle centres are then respectively:

$$\begin{aligned} \eta &= \theta_c - \theta_d \\ \eta' &= \theta_a - \theta_c. \end{aligned} \tag{3.15}$$

Hence from Theorem 3.23, since $\mathfrak{C}$ is an additive group η and η' are circular uniform. ☐

Theorem 3.28.

(1) *If* $a, b \in_u [0, 2\pi)_\circ$ *then* $|a - b| \in_u [0, 2\pi)_\circ$.

(2) $|x| \in [-k, k]$ *has the same distribution as* $2\,x \in [0, k]$ *whenever* x *is symmetrical.*

Proof. Using the definition of modulus of a random variable in 4.10, both results follow from Theorem 3.11 since $\mathfrak{D}_{(x_2-x_1)_\mathbb{R}}(x)$ is an even symmetrical distribution over an interval of $\mathbb{R}$ about 0 and $\mathfrak{D}_{(x_2-x_1)_\circ}(x)$ is uniform over the circle. ☐

Theorem 3.29. *Let the arguments of vectors to the isometric circle centres of a circular uniform matrix be* η *and* η', *then the angular separation* d *between the centres of the two isometric circles* $|\eta - \eta'|$ *is distributed uniformly over* $[0, \pi)_\circ$.

Proof. From Theorem 3.27 the angular separation between the centres of the two isometric circles is:

$$\begin{aligned} \mathsf{d} &= |\eta - \eta'| = |\theta_c - \theta_d - \theta_a + \theta_c| \\ &= |2\theta_c - \theta_a - \theta_d|\,. \end{aligned} \tag{3.16}$$

From Theorem 3.28 and since $\mathfrak{C}$ is an additive group, d is circular uniform. The greatest angular separation of two points on the complex plane is π. ☐

We now have a converse to Theorem 3.27.

Theorem 3.30. *For a matrix in* $A \in SL(2, \mathbb{C})$ *representing a Möbius transformation, let the vectors defining the isometric circle centres* η, η' *(with nomenclature as in Theorem 3.27) be circular uniform. Then matrix* A *is circular uniform.*

Proof. Since η, η' are circular uniform, from (3.15) in Theorem 3.27 $\theta_c - \theta_d$ and $\theta_a - \theta_c$ are circular uniform. Then from Corollary 3.25, (i) either both θ_c and θ_d are circular uniform or η is a constant vector; and (ii) either both θ_a and θ_c are circular uniform or η' is a constant vector. But since η and η' are circular uniform they cannot be constant vectors and:

$$\eta, \eta' \in_u [0, 2\pi)_\circ \text{ therefore } \theta_\mathrm{c}, \theta_\mathrm{a}, \theta_\mathrm{d} \in_\mathrm{u} [0, 2\pi)_\circ.$$

The result follows from Theorem 3.20. ☐

Corollary 3.31. *A matrix in* $SL(2, \mathbb{C})$ *representing a Möbius transformation is circular uniform if and only if the the vectors defining the isometric circle centres are circular uniform.*

3.4 Traces, disjointedness and discreteness

It can be readily verified that the trace function is invariant under conjugation. The isometric circles of f can be seen to be disjoint if $\left|\frac{\mathbf{a}}{\mathbf{c}} + \frac{\bar{\mathbf{a}}}{\mathbf{c}}\right| \geq \frac{2}{|\mathbf{c}|}$. This occurs when

$$|\mathrm{trace(f)}| = |\mathbf{a} + \bar{\mathbf{a}}| = 2|\Re\mathrm{e}(\mathbf{a})| \geq 2.$$

Thus we wish to find the p.d.f. for the random variable $t = |\mathrm{trace(f)}|$. As $|\Re e(\mathbf{a})| = |\mathbf{a}|\,|\cos(\theta_a)|$, for $\theta_a \in_u [0, 2\pi)$:

$$\mathbb{P}_{t\geq 2} = \mathbb{P}_{\Re e(\mathbf{a})\geq 1} = \mathbb{P}_{|\mathbf{a}||\cos(\theta_a)|\geq 1} = \mathbb{P}_{|\mathbf{a}|\geq 1/|\cos(\theta_a)|}$$

But:

$$\mathbb{P}_{|\mathbf{a}|\geq 1/\cos(\theta_a)} = 1 - \frac{2}{\pi}\int_1^{1/\cos(\theta_a)} \frac{dx}{x\sqrt{x^2-1}} = 1 - \frac{2}{\pi}\theta_a. \tag{3.17}$$

As $\mathbf{a}/|\mathbf{a}|$ is circular uniform, we have θ_a uniformly distributed in $[0, 2\pi)$. Therefore using the obvious symmetries we may calculate that

$$\mathbb{P}_{|\mathbf{a}+\bar{\mathbf{a}}|\geq 2} = \frac{2}{\pi}\int_0^{\pi/2} \left(1 - \frac{2}{\pi}\theta\right) d\theta = \frac{1}{2}.$$

This proves the following theorem.

Theorem 3.32. *Let $f \in \mathcal{F}$ be chosen randomly from the distribution described in (i) and (ii). Then the isometric circles of the matrix A representing f are disjoint with probability equal to $\frac{1}{2}$.*

We have the following simple consequence concerning random cyclic groups:

Corollary 3.33. *Let $f \in \mathcal{F}$ be chosen randomly from the distribution described in (i) and (ii). Then the probability that the cyclic group $\langle f\rangle$ is discrete is equal to $\frac{1}{2}$.*

Proof. The matrix A represents a hyperbolic Möbius transformation if and only if $|\mathrm{trace(A)}| > 2$. This occurs with probability $\frac{1}{2}$. The set of values of $\mathrm{trace(A)} \in [-2, 2]$ representing elliptic transformation of finite order or representing parabolic transformations is countable and therefore has measure zero. The result follows. □

We now note the following trivial consequence:

Corollary 3.34. *Let $f, g \in \mathcal{F}$ be chosen randomly from the distribution described in (i) and (ii). Then the probability that the group $\langle f, g\rangle$ is discrete is no more than $\frac{1}{4}$.*

Actually we can modify (3.17) to determine the p.d.f. for $|\mathrm{trace(f)}|$. We will do this two ways. For parameter $s \geq 2$ let $f(s) = \int_1^{s/2\cos\theta} \frac{dx}{x\sqrt{x^2-1}}\, d\theta = \cos^{-1}\left(\frac{2\cos(\theta)}{s}\right)$, this is the p.d.f. of $\sec(\theta)$, $x \in [1, \infty)$:

$$
\begin{aligned}
\mathbb{P}_{|\mathrm{trace(f)}|\geq \mathrm{s}} &= \mathbb{P}_{2|\mathbf{a}|\cos\theta_a \geq s} = \mathbb{P}_{|\mathbf{a}|\geq s/(2\cos\theta_a)} \\
&= 1-\tfrac{2}{\pi}\int_0^{\pi/2} \tfrac{2}{\pi}\int_1^{s/2\cos\theta} \tfrac{dx}{x\sqrt{x^2-1}}\, d\theta \qquad (3.18)\\
&= 1-\tfrac{4}{\pi^2}\int_0^{\pi/2} \cos^{-1}\left(\tfrac{2\cos\theta}{s}\right) d\theta.
\end{aligned}
$$

We are going to use Liebnitz' rule, since if we differentiate a cumulative probability function we get a probability distribution:

$$
\begin{aligned}
\frac{df(s)}{ds} &= \frac{2\cos(\theta)}{s\sqrt{s^2-(2\cos(\theta))^2}} \\
\int \frac{df(s)}{ds}\, d\theta &= \frac{1}{s}\tanh^{-1}\left(\frac{2\sin(\theta)}{\sqrt{s^2-2\cos(2\theta)-2}}\right) \qquad (3.19)\\
\int_0^{\pi/2} \frac{df(s)}{ds}\, d\theta &= \frac{1}{s}\tan^{-1}\left(\frac{2}{s}\right).
\end{aligned}
$$

Now

$$
\tanh^{-1}(x) = \frac{1}{2}\log\frac{1+x}{1-x}, \quad \text{so } \tanh^{-1}\left(\frac{2}{\mathrm{s}}\right) = \frac{1}{2}\log\frac{\mathrm{s}+2}{\mathrm{s}-2}
$$

while

$$
\cosh^{-1}(x) = \log(x+\sqrt{x^2-1})
$$

therefore

$$
\begin{aligned}
\cosh^{-1}\left(\frac{s}{\sqrt{s^2-4}}\right) &= \log\left(\frac{s}{\sqrt{s^2-4}} + \sqrt{\frac{s^2}{\sqrt{s^2-4}}-1}\right) \qquad (3.20)\\
&= \frac{1}{2}\log\frac{s+2}{s-2}.
\end{aligned}
$$

Hence from (3.18), if $F[s]$ is the distribution corresponding to the probability $\mathbb{P}_{|\mathrm{trace(f)}|\geq 2}$, then

$$
F[s] = \frac{4}{\pi^2\, s}\cosh^{-1}\left(\frac{s}{\sqrt{s^2-4}}\right), \quad s \geq 2 \qquad (3.21)
$$

and the total integrated probability over $[2,\infty)$ is $\frac{1}{2}$ as before. There is another way to see these results which is more useful as it more clearly relates to the geometry. We work from a determination of the distribution of the parameter β for transformations in $\mathcal{F}$. We will require the following lemma:

Lemma 3.35. *The distribution of* $w = \frac{\cos^2(\theta)}{\sin^2(\alpha)}$ *for* $\theta \in_u [0, 2\pi)$ *and* $\alpha \in_u [0, \frac{\pi}{2}]$ *is given by:*

$$h(w) = \frac{1}{\pi^2 w} \begin{cases} \log \frac{\sqrt{w}+1}{\sqrt{w}-1} & w > 1 \\ \\ \log \frac{1+\sqrt{w}}{1-\sqrt{w}} & 0 < w < 1. \end{cases} \tag{3.22}$$

Proof. We have the p.d.f.'s of $x = \cos^2(\theta)$ and $y = \sin^2(\alpha)$ as in Figure 4.3, and these random variables are identically distributed when both θ and α are identically distributed, and monotonic for $x, y \in [0, \frac{1}{2})$ and also for $x, y \in (\frac{1}{2}, 1]$ and the distributions are anti-symmetric about $\frac{1}{2}$, hence Theorem 4.16 can be invoked.

$$\begin{aligned} f(x) &= \frac{1}{\pi\sqrt{x(1-x)}} && \text{for } \cos^2(\theta) \\ \text{and} \\ f(y) &= \frac{1}{\pi\sqrt{y(1-y)}} && \text{for } \sin^2(\alpha). \end{aligned} \tag{3.23}$$

Let $x = \cos^2(\theta)$, $y = \sin^2(\alpha)$ and $w = \frac{\cos^2(\theta)}{\sin^2(\alpha)}$; then $w = \frac{x}{y}$, so $wy = x$ and:

$$y = x \times \frac{1}{w}. \tag{3.24}$$

We use the Mellin convolution for quotients as in (4.12), noting that since the distributions $f(x)$ and $f(y)$ in (3.23) are identical, $f_2 = f_1$. For $x, y \in (0, 1)$ the upper integration limits for the convolution integrals according to (3.24) will be $y < 1 \times \frac{1}{w}$ whenever $w > 1$ and $y < 1$ otherwise. Accordingly the Mellin convolution for the quotient of the p.d.f.'s over $[0, \infty)\backslash 0$ (since we want to ensure differentiability) is a piecewise integral:

$$h(w) = \begin{cases} \int_0^1 y\, f(x) f(y) dy & w < 1 \\ \\ \int_0^{\frac{1}{w}} y\, f(x) f(y) dy & w > 1 \end{cases} \tag{3.25}$$

and the indefinite integral embedded in both components of (3.25) is:

$$\begin{aligned} \int y\, f(yw) f(y) dy &= \int y\, \frac{1}{\pi\sqrt{yw(1-yw))}} \frac{1}{\pi\sqrt{y(1-y)}} dy \\ &= \frac{1}{\pi^2\sqrt{w}} \int \frac{1}{\sqrt{(1-y)(1-yw)}} dy \\ &= \frac{1}{\pi^2\sqrt{w}} \frac{2\log\left(w\sqrt{(y-1)}+\sqrt{w(yw-1)}\right)}{\sqrt{w}} \\ &= \frac{1}{\pi^2 w} \log\left(w^2(y-1) + w(yw-1) + 2w^{\frac{3}{2}}\sqrt{(y-1)(yw-1)}\right). \end{aligned} \tag{3.26}$$

Evaluation of the log term in (3.26) yields:

$$\log\left(w\left(w(2y-1) - 1 + 2\sqrt{w(y-1)(yw-1)}\right)\right) =$$

$$\begin{cases} e_0 & = \log(-w(w+1-2\sqrt{w})) \qquad at\ y=0 \\ e_1 & = \log(w(w-1)) \qquad at\ y=1 \\ e_{1/w} & = \log(-w(w-1)) \qquad at\ y=\frac{1}{w}. \end{cases} \tag{3.27}$$

and accordingly the definite integrals in (3.25) evaluate to:

$$\begin{aligned} \int_0^1 y\ f(yw)f(y)dy &= \tfrac{1}{\pi^2 w}(e_1 - e_0) \\ \int_0^{\frac{1}{w}} y\ f(yw)f(y)dy &= \tfrac{1}{\pi^2 w}(e_{1/w} - e_0). \end{aligned} \tag{3.28}$$

But if we let $v = \sqrt{w}$ then:

$$\begin{aligned} e_1 - e_0 &= \log(w(w-1)) - \log(-w(w+1-2\sqrt{w})) = \log\left(\tfrac{w(w-1)}{-w(w+1-2\sqrt{w})}\right) \\ &= \log\left(\tfrac{(v^2-1)}{-(v^2+1-2v)}\right) = \log\left(\tfrac{(v-1)(v+1)}{-(v-1)^2}\right) = \log\left(\tfrac{(v+1)}{-(v-1)}\right) \\ &= \log\left(\tfrac{1+\sqrt{w}}{1-\sqrt{w}}\right) \end{aligned} \tag{3.29}$$

and

$$\begin{aligned} e_{1/w} - e_0 &= \log(-w(w-1)) - \log(-w(w+1-2\sqrt{w})) = \log\left(\tfrac{\log(-w(w-1))}{-w(w+1-2\sqrt{w})}\right) \\ &= \log\left(\tfrac{-(v^2-1)}{-(v^2+1-2v)}\right) = \log\left(\tfrac{-(v-1)(v+1)}{-(v-1)^2}\right) = \log\left(\tfrac{-(v+1)}{-(v-1)}\right) \\ &= \log\left(\tfrac{\sqrt{w}+1}{\sqrt{w}-1}\right). \end{aligned} \tag{3.30}$$

The distribution result follows. □

3.4.1 The parameter $\beta(f)$

Theorem 3.36. *For transformation $f \in \mathcal{F}$,*

$$\beta(f) = 4\left(\frac{\cos^2(\theta)}{\sin^2(\alpha)} - 1\right) \qquad \theta \in_u [0, 2\pi),\ \alpha \in_u \left[0, \frac{\pi}{2}\right]$$

where 2α is the arc length intersection with $\mathbb{S}$ of the isometric circles of A representing f and θ is the argument of the leading entry of matrix A.

Proof. For $f \in \mathcal{F}$ represented by a matrix $A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$ we have that $\beta(A) \in \mathbb{R}$ and for isometric circles of radii r, the arc length intersection $2\alpha \in [0, \pi]$ with $\mathbb{S}$ can be determined via:

$$\tan(\alpha) = r = \frac{1}{|\mathbf{c}|} \geq 0, \quad \alpha \in \left[0, \frac{\pi}{2}\right]$$

Hence from Theorem 3.1 since $\alpha \in \left[0, \frac{\pi}{2}\right]$ implies $\operatorname{cosec}(\alpha) \geq 0$:

$$|\mathbf{c}| = \cot(\alpha) \Rightarrow |\mathbf{a}|^2 = \cot^2(\alpha) + 1 \Rightarrow |\mathbf{a}| = \operatorname{cosec}(\alpha).$$

If the argument of the entry vector $\mathbf{a}$ is $\theta \in [0, 2\pi)$ then:

$$\Re e(\mathbf{a}) = \operatorname{cosec}(\alpha)\cos(\theta) = \frac{\cos(\theta)}{\sin(\alpha)}.$$

Hence:

$$\text{trace(A)} = 2\ \Re\text{e}(\mathbf{a}) = 2\ \frac{\cos(\theta)}{\sin(\alpha)}$$

and:

$$\begin{aligned}
\beta(A) &= \text{trace}^2(\text{A}) - 4 \\
&= \left(2\ \tfrac{\cos(\theta)}{\sin(\alpha)}\right)^2 - 4 \qquad (3.31)\\
&= 4\ \left(\tfrac{\cos^2(\theta)}{\sin^2(\alpha)} - 1\right), \qquad \text{for } \theta \in_{\text{u}} [0, 2\pi),\ \alpha \in_{\text{u}} [0, \tfrac{\pi}{2}].
\end{aligned}$$

□

We come now to the important result for the parameter $\beta(f)$ for a random transformation $f \in \mathcal{F}$.

Theorem 3.37. *For an element $f \in \mathcal{F}$ the distribution of the parameter $w = \beta(f)$ is given by:*

$$h(w) = \frac{1}{\pi^2(w+4)} \begin{cases} \log \frac{\sqrt{w+4}+2}{\sqrt{w+4}-2} & w > 0 \\ \log \frac{2+\sqrt{w+4}}{2-\sqrt{w+4}} & -4 < w < 0. \end{cases} \qquad (3.32)$$

Proof. For the argument of the leading entry of the matrix $\theta \in_u [0, 2\pi)$, if $\alpha \in_u [0, \frac{\pi}{2}]$ such that 2α is the arc length intersection of the isometric circles of A with $\mathbb{S}$ then from Theorem 3.36 the parameter $\beta(A)$ is $4(\frac{\cos^2(\theta)}{\sin^2(\alpha)} - 1)$. Also, from Lemma 3.35 the distribution for $w = \frac{\cos^2(\theta)}{\sin^2(\alpha)}$ is:

$$h(w) = \frac{1}{\pi^2 w} \begin{cases} \log \frac{\sqrt{w}+1}{\sqrt{w}-1} & w > 1 \\ \log \frac{\sqrt{w}+1}{1-\sqrt{w}} & 0 < w < 1. \end{cases} \qquad (3.33)$$

We then obtain the distribution of $v = w + 1 = \frac{\cos^2(\theta)}{\sin^2(\alpha)} + 1$ as:

$$h(v) = \frac{1}{\pi^2(w+1)} \begin{cases} \log \frac{\sqrt{w+1}+1}{\sqrt{w+1}-1} & w > 0 \\ \log \frac{\sqrt{w+1}+1}{1-\sqrt{w+1}} & -1 < w < 0. \end{cases} \qquad (3.34)$$

The justification is Theorem 4.5, and we call on the theorem again to obtain from (3.34) the distribution of $w = 4\left(\frac{\cos^2(\theta)}{\sin^2(\alpha)} + 1\right)$ as:

$$h(w)=\frac{1}{4\pi^2\left(\frac{w}{4}+1\right)}\begin{cases}\log\frac{\sqrt{\frac{w}{4}+1}+1}{\sqrt{\frac{w}{4}+1}-1} & w>0\\ \\ \log\frac{\sqrt{\frac{w}{4}+1}+1}{1-\sqrt{\frac{w}{4}+1}} & -4<w<0\end{cases} \tag{3.35}$$

and after simplification we have the result.

□

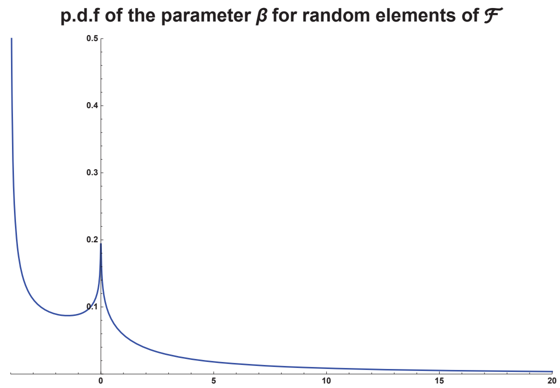


Figure 3.8: Distribution of parameter β for random elements of $\mathcal{F}$.

We shortly use (3.32) to find the distribution of the translation length of hyperbolic elements, but here note that the integral of $h(w)$ over the interval $(-4,0)$ and also over the interval $(0,\infty)$ both take the value $\frac{1}{2}$, which establishes the following theorem:

Theorem 3.38. *A randomly selected element $f\in\mathcal{F}$ is hyperbolic or elliptic with* probability $\frac{1}{2}$.

3.4.2 The parameter $\gamma([f,g])$

With our usual matrix representation we put $\gamma=\gamma([A,B])=\text{trace}([\text{A},\text{B}])-2$.

Theorem 3.39. *For pairs of elements f,g represented by matrices $A,B\in\mathcal{F}$, the γ parameter is a combination of several non independent components:*

$$\begin{aligned}\gamma([A,B])=\ &\cot^2(\alpha_B)\text{cosec}^2(\alpha_\text{A})\sin^2(\theta_\text{a})+\cot^2(\alpha_\text{A})\text{cosec}^2(\alpha_\text{B})\sin^2(\theta_\text{e})\\ &+\sin^2(\sigma)\cot^2(\alpha_A)\cot^2(\alpha_B)-\cos(\sigma)\frac{\cot(\alpha_A)}{\sin(\alpha_A)}\frac{\cot(\alpha_B)}{\sin(\alpha_B)}\sin(\theta_a)\sin(\theta_e).\end{aligned} \tag{3.36}$$

Proof. Matrices $A,B\in\mathcal{F}$ can be expressed in terms of the half intersection arc length α and matrix entry arguments θ as:

$$A=\begin{pmatrix}\frac{\cos(\theta_a)+i\sin(\theta_a)}{|\sin(\alpha_A)|} & \frac{\cos(\theta_c)-i\sin(\theta_c)}{|\tan(\alpha_A)|}\\ \\ \frac{\cos(\theta_c)+i\sin(\theta_c)}{|\tan(\alpha_A)|} & \frac{\cos(\theta_a)-i\sin(\theta_a)}{|\sin(\alpha_A)|}\end{pmatrix},B=\begin{pmatrix}\frac{\cos(\theta_e)+i\sin(\theta_e)}{|\sin(\alpha_B)|} & \frac{\cos(\theta_g)-i\sin(\theta_g)}{|\tan(\alpha_B)|}\\ \\ \frac{\cos(\theta_g)+i\sin(\theta_g)}{|\tan(\alpha_B)|} & \frac{\cos(\theta_e)-i\sin(\theta_e)}{|\sin(\alpha_B)|}\end{pmatrix}. \tag{3.37}$$

By forming the product $ABA^{-1}B^{-1}$ and simplifying we obtain the trace of the commutator of A and B as:

$$\begin{aligned}\text{trace}([\text{A},\text{B}]) = \; & 2\cos(2(\theta_c-\theta_g))\cot^2(\alpha_A)\cot^2(\alpha_B) - 2\cos(2\theta_a)\cot^2(\alpha_B)\text{cosec}^2(\alpha_\text{A}) \\ & -2\cos(2\theta_e)\cot^2(\alpha_A)\text{cosec}^2(\alpha_\text{B}) + 2\text{cosec}^2(\alpha_\text{A})\text{cosec}^2(\alpha_\text{B}) \\ & -8\,\xi\cos(\theta_c-\theta_g)\cot(\alpha_A)\cot(\alpha_B)\text{cosec}(\alpha_\text{A})\text{cosec}(\alpha_\text{B})\sin(\theta_\text{a})\sin(\theta_\text{e})\end{aligned} \tag{3.38}$$

where $\xi = \text{sign}(\sin(\alpha_\text{A})\sin(\alpha_\text{B})\tan(\alpha_\text{A})\tan(\alpha_\text{B}) = +1$ since $\alpha_A, \alpha_B \in [0, \frac{\pi}{2}]$. We note that the trace of the commutator depends on the difference $\sigma = \theta_c - \theta_g$ rather than the individual vector arguments, and we accordingly calculate γ as:

$$\begin{aligned}\gamma([A,B]) \; & = \frac{\cos^2(\alpha_B)\sin^2(\theta_a)}{\sin^2(\alpha_A)\sin^2(\alpha_B)} + \frac{\cos^2(\alpha_A)\sin^2(\theta_e)}{\sin^2(\alpha_A)\sin^2(\alpha_B)} + \frac{(\cos^2(\sigma)-1)\cos^2(\alpha_A)\cos^2(\alpha_B)}{\sin^2(\alpha_A)\sin^2(\alpha_B)} \\ & -\frac{2\cos(\sigma)\cos(\alpha_A)\cos(\alpha_B)\sin(\theta_a)\sin(\theta_e)}{\sin^2(\alpha_A)\sin^2(\alpha_B)}.\end{aligned} \tag{3.39}$$

which leads to the result. □

Since the components of the terms of $\gamma([A,B])$ in (3.36) exhibit dependence, analytical calculation of the distribution function is not feasible at present, Figure 3.10 shows computationally determined distributions of $\gamma([A,B])$, first for random elements of $\mathcal{F}$, and then for hyperbolic elements only. We have the following computational results from this experiment for $1,000,000$ outcomes:

Probability ↓ **in domain**	**random** $f,g \in \mathcal{F}$	**random** f,g **elliptic**	**random** f,g **hyperbolic**
$\mathbb{P}_{\gamma([A,B])<-4}$	0.0664	0	0.2676816
$\mathbb{P}_{\gamma([A,B])\in[-4,0)}$	0.040252	0	0.16172425
$\mathbb{P}_{\gamma([A,B])\in[0,4)}$	0.363511	0.650488	0.1513727888
$\mathbb{P}_{\gamma([A,B])>4}$	0.529837	0.349512	0.41922135423231964

Figure 3.9: Computational experiment, $\gamma([f,g])$ for $f,g \in \mathcal{F}$.

Note that in Figure 3.9, for random elements of $\mathcal{F}$, $\mathbb{P}_{\gamma([f,g])<0} = 0.106652$ while if the element pairs are conditioned to be hyperbolic then $\mathbb{P}_{\gamma([f,g])<0} = 0.429406$.

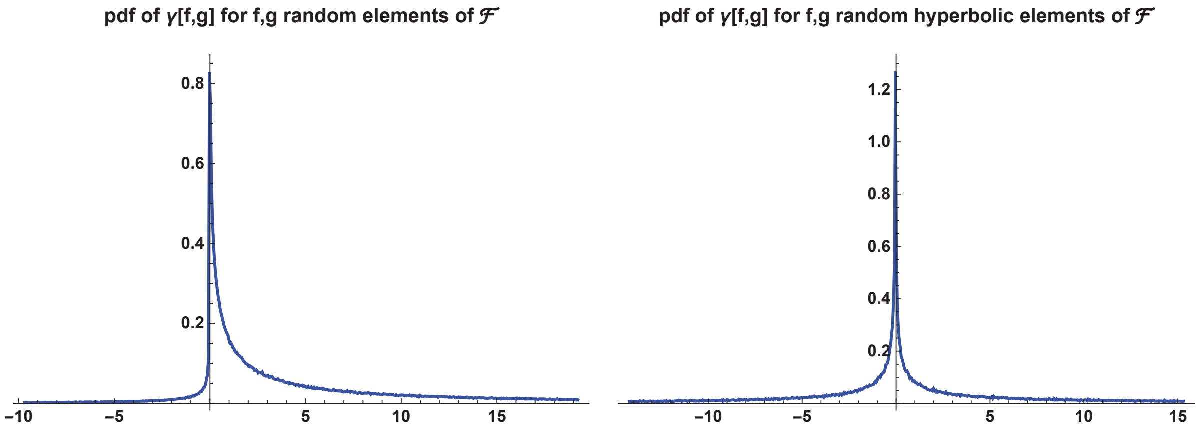


Figure 3.10: The γ parameter. Left: random elements of $\mathcal{F}$. Right: random hyperbolic elements of $\mathcal{F}$.

3.4.3 Jørgensen's inequality

Given that we do not at present have an analytical determination for the distribution of $\gamma([f,g])$, we can still look at the results of a computational analysis of $|\beta(A)| + |\gamma([A,B])|$. Figure 3.11 shows for $10,000,000$ pairs of random matrices in $\mathcal{F}$ the calculated probabilities that $\langle f, g\rangle$ will be possibly not discrete; the distribution is illustrated in Figure 3.12.

Probability $\downarrow$ **in domain**	**random** $f, g \in \mathcal{F}$	**random** f, g **elliptic**	**random** f, g **hyperbolic**
$\mathbb{P}_{\|\gamma([f,g])\|+\|\beta(f)\|<1}$	$0.071697 \approx \frac{1}{14}$	$0.09524 \approx \frac{2}{21}$	$0.275322 \approx \frac{3}{11}$

Figure 3.11: Computational experiment, $1,000,000$ pairs of elements of $\mathcal{F}$ that fail Jørgensen's inequality, that is $|\gamma([f,g])| + |\beta(f)| < 1$.

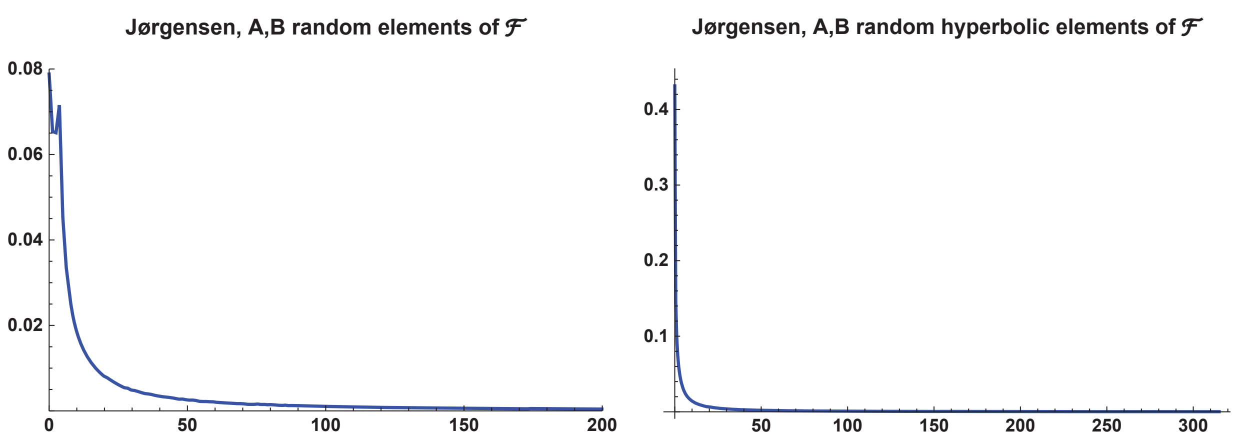


Figure 3.12: Jørgensen's inequality. Left: random elements of $\mathcal{F}$. Right: random hyperbolic elements of $\mathcal{F}$.

Overall about $\frac{1}{14}$ of pairs of random matrices in $\mathcal{F}$ failed Jørgensen's criterion for discreteness while about $\frac{3}{11}$ of such hyperbolic pairs failed the criterion for discreteness, [36].

3.4.4 Fixed points

The fixed points of a random $f \in \mathcal{F}$ are solutions to $\mathbf{z} = \dfrac{\mathbf{az} + \overline{\mathbf{c}}}{\mathbf{cz} + \overline{\mathbf{a}}}$, that is, with the representation of f by the matrix $A = \begin{pmatrix} ae^{i\theta_a} & be^{i\theta_b} \\ ce^{i\theta_c} & de^{i\theta_d} \end{pmatrix}$:

$$\begin{aligned} \mathbf{z} &= \tfrac{1}{\mathbf{c}} \left[\pm \sqrt{\Re e(\mathbf{a})^2 - 1} + i\, \Im m(\mathbf{a}) \right] \\ &= \tfrac{a}{c} \left[\pm \sqrt{\cos^2(\theta_a) - \tfrac{1}{a^2}} + i\, \sin(\theta_a) \right] e^{-i\theta_c}. \end{aligned} \tag{3.40}$$

We have chosen $\arg(\mathbf{c})$ to be uniformly distributed. There are three cases to consider:

Case 1. f hyperbolic. Then $\Re e(a) > 1$ and $|\mathbf{z}_\pm| = 1$ as illustrated in Figure 3.4.
Case 2. f elliptic. Then $|\Re e(a)| \leq 1$ and so

$$\mathbf{z} = i\, \frac{a}{c} \left[\sin(\theta_a) \pm \sqrt{\cos^2(\theta_a) - \frac{1}{a^2}} \right] e^{-i\theta_c}$$

as illustrated in Figure 3.5.
Case 3. f parabolic. Then

$$\begin{aligned} & 2\Re e(\mathbf{a}) = \pm 2 \Rightarrow \Re e(\mathbf{a}) = \pm 1 \\ \text{therefore} \quad & \\ & z = \frac{a}{c} i \sin(\theta_a) e^{-i\theta_c} = \frac{1}{\mathbf{c}}\, i\, \Im m(\mathbf{a}) \end{aligned} \tag{3.41}$$

which is a single fixed point with argument uniformly distributed in $[0, 2\pi)$.

Note that the non elliptic fixed points of Fuchsian transformations lie on the unit circle $\mathbb{S}$. We will shortly establish that $\mathbb{P}_{|\Re e(a)| \leq 1\} = \frac{1}{2}}$.

Lemma 3.40. *The Euclidean distance between the fixed points of $f \in \mathcal{F}$ where the isometric circles of the representative matrices make intersections of arc length 2α with $\mathbb{S}$ is:*

$$d = \frac{\beta(f)}{\cos(\alpha)}.$$

Proof. Suppose the fixed points of $f \in \mathcal{F}$ are given as in (3.40) by $\mathbf{z} = \frac{|\mathbf{a}|}{|\mathbf{c}|} [\pm\, x + i\, y]\, e^{-i\,\theta_c}$, then with the nomenclature of Theorem 3.1 we have $\sin(\alpha) = \frac{r}{R}$ therefore $\sin^2(\alpha) = \frac{\mathrm{r}^2}{\mathrm{r}^2 + 1}$ (see Figure 3.1) and:

$$
\begin{aligned}
|y_2 - y_1|^2 &= 0 \\
|x_2 - x_1|^2 &= 4\left(\Re e(\mathbf{a})^2 - 1\right) \\
&= 4\left(|\mathbf{a}|^2 \cos^2(\theta_a) - 1\right) \\
&= 4\left((|\mathbf{c}|^2 + 1)\cos^2(\theta_a) - 1\right) \\
&= 4\left(\left(\tfrac{r^2+1}{r^2}\right)\cos^2(\theta_a) - 1\right) \\
&= 4\left(\tfrac{\cos^2(\theta_a)}{\sin^2(\alpha)} - 1\right) = \beta(f),
\end{aligned}
\tag{3.42}
$$

the last by Theorem 3.36. The result follows since the separation distance is invariant under rotation by θ_c and as illustrated in Figure 3.1 $\frac{|\mathbf{a}|}{|\mathbf{c}|} = R = \sqrt{r^2+1} = \frac{1}{\cos(\alpha)}$. □

This distribution is calculable, but the following approach provides a much more straightforward calculation for hyperbolic elements of $\mathcal{F}$.

Lemma 3.41. *The arc length separation 2ϕ between the fixed points of $f \in \mathcal{F}$ where the isometric circles of the representative matrices make intersections of arc length 2α with $\mathbb{S}$ is given by:*

$$\sin(\phi) = \frac{\sin(\theta_a)}{\cos(\alpha)}.$$

Proof. From (3.40) via Pythagoras,

$$\sin(\phi) \;= \frac{\Im m(\mathbf{a})}{(\Re e(\mathbf{a})^2 - 1) + (\Im m(\mathbf{a})^2)} = \frac{|\mathbf{a}|}{|\mathbf{c}|}\sin(\theta_a) = \frac{\sin(\theta_a)}{\cos(\alpha)}. \tag{3.43}$$

□

Theorem 3.42. *The distribution of $w = \frac{\sin(\theta)}{\cos(\alpha)}$ for $\theta \in_u [0, 2\pi)$ and $\alpha \in_u [0, \frac{\pi}{2}]$ is given by:*

$$h(w) = \frac{2}{\pi^2 w}\log\left(\frac{1+w}{1-w}\right) \qquad -1 < w < 1 \tag{3.44}$$

Proof. We have the p.d.f.'s of $x = \sin(\theta)$ and $y = \cos(\alpha)$ (reported in Figure 4.3) and these are identically distributed when both θ and α are identically distributed, and monotonic for $x, y \in [0, 1)$ and also for $x, y \in (-1, 0]$ and the distributions are anti-symmetric about 0, hence Theorem 4.16 can be invoked. We prove the distribution for the first quadrant only, $x, y \in [0, 1)$, by symmetry the total p.d.f. is four times the contribution calculated.

$$
\begin{aligned}
f(x) &= \frac{1}{\pi\sqrt{1-x^2}} \qquad \text{for } \sin(\theta) \\
\text{and} \quad & \\
f(y) &= \frac{1}{\pi\sqrt{1-y^2}} \qquad \text{for } \cos(\alpha).
\end{aligned}
\tag{3.45}
$$

Let $x = \sin(\theta)$, $y = \cos(\alpha)$ and $w = \frac{\sin(\theta)}{\cos(\alpha)}$; then $w = \frac{x}{y}$, therefore $wy = x$ and:

$$y = x \times \frac{1}{w} \tag{3.46}$$

We use the Mellin convolution for quotients as in (4.12), noting that since the distributions $f(x)$ and $f(y)$ in (3.45) are identical, $f_2 = f_1$. For $x, y \in (0,1)$ the upper integration limits for the convolution integrals according to (3.46) will be $y < 1 \times \frac{1}{w}$ whenever $w > 1$ and $y < 1$ otherwise, accordingly the Mellin convolution for the quotient of the p.d.f.'s over $[0,\infty)\backslash 0$ (since we want to ensure differentiability) is a piecewise integral:

$$h(w) = \begin{cases} \int_0^1 y\, f(x) f(y) dy & w < 1 \\ \\ \int_0^{\frac{1}{w}} y\, f(x) f(y) dy & w > 1 \end{cases} \tag{3.47}$$

and the indefinite integral embedded in both components of (3.25) is:

$$\begin{aligned} \int y\, f(yw) f(y) dy &= \int y \frac{1}{\pi\sqrt{1-(yw)^2}} \frac{1}{\pi\sqrt{1-y^2}} dy \\ &= \frac{1}{\pi^2} \int \frac{y}{\sqrt{(1-y^2)(1-y^2w^2)}} dy \\ &= -\frac{1}{\pi^2 w} \log\left(w^2\sqrt{(1-y^2} + w\sqrt{1-y^2w^2}\right). \end{aligned} \tag{3.48}$$

Evaluation of the log term in (3.48) yields:

$$\log\left(w^2\sqrt{(1-y^2} + w\sqrt{1-y^2w^2}\right) = \\ \begin{cases} e_0 & = \log\left(w(w+1)\right) & \text{at y} = 0 \\ e_1 & = \log\left(w\sqrt{1-w^2}\right) & \text{at y} = 1 \\ e_{1/w} & = \log\left(w\sqrt{w^2-1}\right) & \text{at y} = \frac{1}{\text{w}}. \end{cases} \tag{3.49}$$

and accordingly the definite integrals in (3.25) evaluate to:

$$\begin{aligned} \int_0^1 y\, f(yw) f(y) dy &= -\frac{1}{\pi^2 w}(e_1 - e_0) \\ &= \frac{1}{\pi^2 w} \log\left(\frac{\sqrt{1+w}}{\sqrt{1-w}}\right) \\ \int_0^{\frac{1}{w}} y\, f(yw) f(y) dy &= -\frac{1}{\pi^2 w}(e_{1/w} - e_0) \\ &= \frac{1}{\pi^2 w} \log\left(\frac{\sqrt{w+1}}{\sqrt{w-1}}\right). \end{aligned} \tag{3.50}$$

The distribution of $w = \frac{\sin(\theta)}{\cos(\alpha)}$ in all four quadrants is then given by:

$$h(w) = \frac{4}{\pi^2 w} \begin{cases} \log\left(\frac{\sqrt{1+w}}{\sqrt{1-w}}\right) & w < 1 \\ \\ \log\left(\frac{\sqrt{w+1}}{\sqrt{w-1}}\right) & w > 1. \end{cases} \tag{3.51}$$

□

Noting that $\frac{|\mathbf{a}|}{\sqrt{|\mathbf{a}|^2-1}} \geq 0$, we restrict to positive values of $x = \sin(\phi)$. The p.d.f. of the arc length separation of the fixed points on $\mathbb{S}$ of hyperbolic elements of $\mathcal{F}$ then reduces to:

$$h(x) = \frac{4}{\pi^2 x} \log\left(\frac{1+x}{1-x}\right), \quad 0 \leq x < 1.$$

3.4.5 Translation lengths

Every element $f \in \mathcal{F}$ which is not elliptic (conjugate to a rotation, equivalently $\beta \in [-4, 0)$) or parabolic (conjugate to a translation, equivalently $\beta = 0$) fixes two points on the circle and the hyperbolic line with those points as endpoints. The transformation acts as a translation by constant hyperbolic distance along this line. This distance is called the translation length τ and this number is related to the parameter $\beta(f)$, hence to the trace, via the formula [46]:

$$\beta = 4\sinh^2 \frac{\tau}{2}, \quad \tau = \cosh^{-1}\left(1 + \frac{\beta}{2}\right). \tag{3.52}$$

We use the distribution of β as in (3.32)to obtain the distribution for τ via the change of variables formula.

Theorem 3.43. *The p.d.f. of the translation length τ for randomly selected hyperbolic $f \in \mathcal{F}$ is given by:*

$$\begin{aligned} H[\tau] &= -\tfrac{4}{\pi^2} \tanh\left(\tfrac{\tau}{2}\right) \log\left(\tanh\left(\tfrac{\tau}{4}\right)\right) \\ \textit{or} \\ H[\tau] &= \tfrac{4}{\pi^2} \tanh\left(\tfrac{\tau}{2}\right) \log\left(\tfrac{\cosh(\frac{\tau}{2})-1}{\cosh(\frac{\tau}{2})+1}\right). \end{aligned} \tag{3.53}$$

Proof. For f hyperbolic $\beta(f) \geq 0$ implies $\tau \geq 0$ and the resultant p.d.f. for $w = \beta(f)$, f hyperbolic is from Theorem 3.37:

$$g(w) = \frac{2}{\pi^2(w+4)} \log \frac{\sqrt{w+4}+2}{\sqrt{w+4}-2} \tag{3.54}$$

then:

$$\beta = 4\sinh^2\left(\frac{\tau}{2}\right), \text{ therefore } \beta + 4 = 4(\sinh^2\left(\frac{\tau}{2}\right) + 1) = 4\cosh^2\frac{\tau}{2} \tag{3.55}$$

and also:

$$\sqrt{\beta+4} = \pm 2\cosh\frac{\tau}{2}. \tag{3.56}$$

But $\frac{d\beta}{d\tau} = \frac{d(\beta+4)}{d\tau} = 4\cosh\left(\frac{\tau}{2}\right)\sinh\left(\frac{\tau}{2}\right) = 2\sinh(\tau)$ and since $\tau \geq 0$ implies $\sinh(\tau) \geq 0$, from (3.54) for hyperbolic $f \in \mathcal{F}$ and $w = \beta(f)$,

$$\begin{aligned} h(w) &= \tfrac{2}{\pi^2(\beta+4)} \log\left(\tfrac{\sqrt{\beta+4}+2}{\sqrt{\beta+4}-2}\right) \\ \text{therefore} \\ H(\tau) &= \tfrac{2}{4\pi^2\cosh^2\frac{\tau}{2}} \log\left(\tfrac{\pm 2\cosh(\frac{\tau}{2})+2}{\pm 2\cosh(\frac{\tau}{2})-2}\right) 2\sinh(\tau) \qquad \tau \geq 0. \end{aligned} \tag{3.57}$$

We note that $\cosh(x)+1 = 2\cosh^2(\frac{x}{2})$ while $\cosh(x)-1 = 2\sinh^2(\frac{x}{2})$ and because application of the $\pm$ signs has no nett effect on evaluation of the fraction:

$$\begin{aligned} H(\tau) &= \frac{\sinh(\tau)}{\pi^2\cosh^2\frac{\tau}{2}}\log\left(\coth^2\frac{\tau}{4}\right) = \frac{2\sinh(\tau)}{\pi^2\cosh^2\frac{\tau}{2}}\log\left(\coth\frac{\tau}{4}\right) = \frac{4\sinh\frac{\tau}{2}\cosh\frac{\tau}{2}}{\pi^2\cosh^2\frac{\tau}{2}}\log\left(\coth\frac{\tau}{4}\right) \\ &= \frac{4}{\pi^2}\tanh\frac{\tau}{2}\log\left(\coth\frac{\tau}{4}\right) = -\frac{4}{\pi^2}\tanh\frac{\tau}{2}\log\left(\tanh\frac{\tau}{4}\right) \qquad \tau \geq 0 \end{aligned} \tag{3.58}$$

hence the result. □

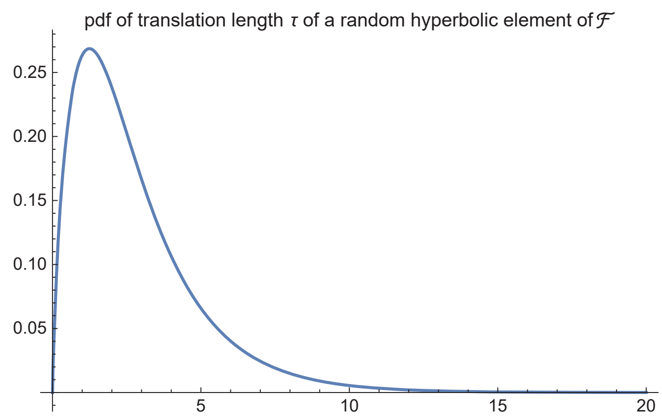


Figure 3.13: Distribution of the translation length for randomly selected hyperbolic $f \in \mathcal{F}$.

Unlike our earlier distributions, the p.d.f. for τ has all moments. In particular by writing $\tanh(\tau/2)$ as $\frac{1-e^{-\tau}}{1+e^{-\tau}}$ and $\tanh(\tau/4)$ as $\frac{1-e^{-\tau/2}}{1+e^{-\tau/2}}$ we observe

$$\int_0^\infty \tau \tanh\frac{\tau}{2}\log\left[\tanh\frac{\tau}{4}\right]d\tau = -\pi^2\log 2$$

and the expected value of the translation length is

$$E[[\tau]] = 4\log 2 \approx 2.77259\ldots \tag{3.59}$$

3.5 Random arcs on a circle

Let α be an arc on the circle $\mathbb{S}$. We denote its midpoint by $\mathbf{m}_\alpha \in \mathbb{S}$ and its arclength by $\ell_\alpha \in [0, 2\pi)$. Conversely, given $\mathbf{m}_\alpha \in \mathbb{S}$ and $\ell_\alpha \in [0, 2\pi)$ we determine a unique arc $\alpha = \alpha(\mathbf{m}_\alpha, \ell_\alpha)$ with this data.

A random arc α is the arc uniquely determined when we choose $\mathbf{m}_\alpha \in \mathbb{S}$ uniformly (equivalently $\arg(\mathbf{m}_\alpha) \in_u [0, 2\pi)$) and $\ell_\alpha \in_u [0, 2\pi)$. We will abuse notation and also refer to random arcs when we restrict to $\ell_\alpha \in_u [0, \pi]$ as for the case of isometric disc intersections. We will make the distinction clear in context.

A simple consequence of our earlier result is the following corollary.

Corollary 3.44. *If* $\mathbf{m}_\alpha, \mathbf{m}_\beta \in_u \mathbb{S}$ *and* $\ell_\alpha, \ell_\beta \in_u [0,\pi]$ *then*

$$\mathbb{P}_{\alpha\cap\beta=\varnothing} = \frac{1}{2}.$$

We need to observe the following lemma.

Lemma 3.45. *If* $\mathbf{m}_\alpha, \mathbf{m}_\beta \in_u \mathbb{S}$ *and* $\ell_\alpha, \ell_\beta \in_u [0,2\pi)$*, then*

$$\mathbb{P}_{\alpha\cap\beta=\varnothing} = \frac{1}{6}.$$

We present two proofs:

Proof.

(1) We need to calculate the probability that the argument of $\zeta = \mathbf{m}_\alpha\overline{\mathbf{m}_\alpha}$ is greater than $(\ell_\alpha + \ell_\beta)/2$. Now $\theta = \arg(\zeta)$ is uniformly distributed in $[0,\pi]$. The joint distribution is uniform, and so we calculate

$$\begin{aligned} \mathbb{P}_{\theta\geq\ell_\alpha+\ell_\beta} &= \tfrac{1}{\pi^3}\int\int\int_{\{\theta\geq\alpha+\beta\}} 1\ d\theta\ d\alpha\ d\beta \\ &= \tfrac{1}{\pi^3}\int_0^\pi\int_0^\theta\int_0^{\theta-\alpha} 1\ d\theta\ d\alpha\ d\beta = \tfrac{1}{6} \end{aligned} \tag{3.60}$$

and the result follows.

(2) By Theorem 3.27 the arguments $\mathbf{m}_\alpha, \mathbf{m}_\beta$ of the vectors to the centres of the arcs ℓ_α, ℓ_β respectively have circular uniform distribution in $[0,2\pi)$ and similarly $\ell_\alpha, \ell_\beta \in [0,2\pi)$. Then by Theorem 3.29 the angular distance $d = |\mathbf{m}_\alpha - \mathbf{m}_\beta| \in [0,2\pi)$ between the centres of the arcs is also circular uniform. The separation distance between the circles is $\delta = |d| - \frac{\ell_\alpha+\ell_\beta}{2}$ and the distance between the arcs can be calculated:

$$\text{then}\quad \begin{aligned} &|d| \in_u [0,2\pi)_\circ = \tfrac{1}{2}d \in_u [0,2\pi]_\mathbb{R} = d \in_u [0,\pi]_\mathbb{R} \\ &\delta = d \in_u [0,\pi]_\mathbb{R} - \tfrac{\ell_\alpha}{2} \in_u [0,\pi]_\mathbb{R} - \tfrac{\ell_\beta}{2} \in_u [0,\pi]_\mathbb{R}. \end{aligned} \tag{3.61}$$

The result is a random variable of the form of $x_1 - x_2 - x_3$ for $x_1, x_2, x_3 \in_u [0,\pi]$ and since $x_1 = d = |\mathbf{m}_\alpha - \mathbf{m}_\beta|$, $x_2 = \frac{\ell_\alpha}{2}$ and $x_2 = \frac{\ell_\beta}{2}$ are independent the distribution $\mathfrak{D}_{(x_1-x_2-x_3)}$ in (4.37) applies and δ is non negative with probability $\frac{1}{6}$.

□

3.6 Random arcs to Möbius groups

Given data $\mathbf{m}_{\alpha_1}, \mathbf{m}_{\alpha_2} \in \mathbb{S}$ with arc length $\ell_\alpha \in [0,\pi]$ we determine that the arcs centered on the $\mathbf{m}_{\alpha_i}$ and of length ℓ_α determine a matrix which can be calculated by examination of the isometric circles. We have

$$A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}, \quad \mathbf{c} = i\sqrt{\mathbf{m}_{\alpha_1}\mathbf{m}_{\alpha_2}} \cot\frac{\ell_\alpha}{2}, \quad \mathbf{a} = i\sqrt{\overline{\mathbf{m}_{\alpha_1}}\mathbf{m}_{\alpha_2}}\mathrm{cosec}\frac{\ell_\alpha}{2} \tag{3.62}$$

where we make a consistent choice of sign by ensuring that:

$$\frac{\mathbf{c}}{\mathbf{a}} = \mathbf{m}_{\alpha_1} \cos\frac{\ell_\alpha}{2}.$$

Of course interchanging $\mathbf{m}_{\alpha_1}$ and $\mathbf{m}_{\alpha_2}$ sends $\mathbf{a}$ to $-\overline{\mathbf{a}}$, so the data uniquely determines the cyclic group $\langle f \rangle$ generated by the associated Möbius transformation:

$$f(\mathbf{z}) = -\mathbf{m}_{\alpha_2} \frac{\mathbf{z} + \mathbf{m}_{\alpha_1}\cos\frac{\ell_\alpha}{2}}{\mathbf{z}\cos\frac{\ell_\alpha}{2} + \mathbf{m}_{\alpha_1}}$$

and not necessarily f itself. As a consequence we have the following theorem:

Theorem 3.46. *There is a one-to-one correspondence between collections of n pairs of random arcs and n-generator Fuchsian groups. A randomly chosen $f \in \mathcal{F}$ corresponds uniquely to $\mathbf{m}_{\alpha_1}, \mathbf{m}_{\alpha_2} \in_u \mathbb{S}$ and $\ell_\alpha \in_u [0, \pi]$.*

Notice also that if we recognise the association of cyclic groups with the data and say two cyclic groups are close if they have close generators, then this association is continuous.

If f is a parabolic element of $\mathcal{F}$, then the isometric circles are adjacent and meet at the fixed point. Conversely, if two random arcs both of arclength ℓ_α are adjacent we have $\arg(\mathbf{m}_{\alpha_1}\overline{\mathbf{m}}_{\alpha_2}) = \ell_\alpha$, and from (3.62):

$$\mathbf{a} = i\left(\cos\frac{\ell_\alpha}{2} + i\ \sin\frac{\ell_\alpha}{2}\right)\ \mathrm{cosec}\frac{\ell_\alpha}{2} = -1 + \mathrm{i}\ \cot\frac{\ell_\alpha}{2}$$

and $\mathrm{trace}^2(\mathrm{A}) - 4 = 0$ so the matrix A represents a parabolic transformation. Similarly if the arcs overlap, then $\mathrm{trace}^2(\mathrm{A}) = 2$ and A represents an elliptic transformation, then from Lemma 3.45:

$$\mathbb{P}_{\langle f,g\rangle \text{is discrete given f,g} \in \mathcal{F} \text{ are parabolic}} = \frac{1}{6}.$$

Notice that f is parabolic or the identity if and only if $\Re e(a) \in \{\pm 1\}$.

Theorem 3.47. *Let f, g be randomly chosen parabolic elements in $\mathcal{F}$. Then the probability that $\langle f, g \rangle$ is discrete is at least $\frac{1}{6}$.*

Proof. As f and g are parabolic, their isometric discs are tangential and the point of intersection lies in a random arc of arclength uniformly distributed in $[0, 2\pi)$. Discreteness follows from the Klein combination theorem and Lemma 3.45. □

3.7 The topology of the quotient space

Two transformations $f, g \in \mathcal{F}$ acting on $\hat{\mathbb{C}}$ exhibit two pairs of isometric circles orthogonal to $\mathbb{S}$. Should all the isometric circles be disjoint (which implies the group $\langle f, g\rangle$ is discrete) then we can construct hyperbolic quotient spaces by identifying the intersection arcs of each pair of circles in the interior of $\mathbb{S}$. It is clear from consideration of the Ford fundamental domain [20] that we have two distinct topologies, that is, there are two surfaces whose fundamental group is isomorphic to F_2, the free group on two generators.

(1) Isometric circles of each pair adjacent: Pairing the arcs leaves a hole between each pair and a single hole between adjacent pairs, that is, taking into account the opposite direction of group elements along the arc pairs the resultant topology is $\mathbb{S}^2_3$, a 2-sphere with a total of three holes.

(2) Isometric circles of each pair non adjacent: Pairing the arcs results in T^2_1, a torus with a single hole.

Thus we can expect that a group $\Gamma = \langle f, g\rangle$ generated by two random hyperbolic elements of $\mathcal{F}$ if discrete, has quotient:

$$\mathbb{D}^2/\Gamma \in \{\mathbb{S}^2_3, T^2_1\}.$$

We would like to understand the likelihood of one of these topologies over the other, this is the same thing as asking whether the hyperbolic lines between the fixed points of f and the fixed points of g cross or not, and this in turn is determined by a suitable cross ratio of the four fixed points. In fact, the geometry of the commutator $\gamma([f,g]) = \mathrm{trace([f,g])} - 2$ determines not only the topology of the quotient, but also the hyperbolic length of the shortest geodesic; this is represented by f, g or $[f,g] = fgf^{-1}g^{-1}$ or by their Nielsen equivalents $f^{-1}, g^{-1}, [f,g]^{-1}$.

3.7.1 Commutators and cross ratios

We now consider the relation of the parameters of a two-generator group as expressed in Jørgensen's inequality (1.2) to the cross ratio of points on $\mathbb{S}$. In the previous section we analysed the distribution of the trace of a transformation, in order to address the distribution of the trace of the commutator $[A,B] = ABA^{-1}B{-}1$ we consider the γ parameter:

$$\gamma([A,B]) = \mathrm{trace([A,B])} - 2. \tag{3.63}$$

We need to understand the cross ratio distribution first. This is because of the following result from [5], sections §7.23 and §7.24, together with a little manipulation. Beardon's results in relation to the hyperbolic distance ρ between hyperbolic lines $\ell_1 = [\mathbf{z_1}, \mathbf{z_2}]$ and $\ell_2 = [\mathbf{w_1}, \mathbf{w_2}]$ and their angle of intersection θ are respectively:

$$\begin{aligned} &[\mathbf{z_1}, \mathbf{w_1}, \mathbf{z_2}, \mathbf{w_2}] \tanh^2\left(\tfrac{1}{2}\rho(\ell_1, \ell_2)\right) &= 1 \\ \text{and} \quad & \\ &[\mathbf{z_1}, \mathbf{w_1}, \mathbf{z_2}, \mathbf{w_2}] \sin^2\left(\tfrac{\theta}{2}\right) &= 1. \end{aligned} \tag{3.64}$$

Theorem 3.48. *Let ℓ_1, with endpoints $\mathbf{z_1}, \mathbf{z_2}$, and ℓ_2, with endpoints $\mathbf{w_1}, \mathbf{w_2}$, be hyperbolic lines in the unit disc model of hyperbolic space. So $\mathbf{z_1}, \mathbf{z_2}, \mathbf{w_1}, \mathbf{w_2} \in \mathbb{S}$, the circle at infinity. Let δ be the hyperbolic distance between ℓ_1 and ℓ_2, and should they cross, let $\theta \in [0, \pi/2]$ be the angle at the intersection. Then*

$$\sinh^2\left[\frac{1}{2}(\delta + i\theta)\right] \times [\mathbf{z_1}, \mathbf{w_1}, \mathbf{z_2}, \mathbf{w_2}] = -1. \tag{3.65}$$

The number $\delta + i\theta$ is called the *complex distance* between the lines ℓ_1 and ℓ_2, where we put $\theta = 0$ if the lines do not meet. The proof of this theorem is simply to use Möbius invariance of the cross ratio. If the two lines do not intersect, we choose the Möbius transformation which sends $\{\mathbf{z_1}, \mathbf{z_2}\}$ to $\{-1, +1\}$ and $\{\mathbf{w_1}, \mathbf{w_2}\}$ to $\{-s, s\}$ for some real $s > 1$. Then $\delta = \log s$ and

$$[-1, -s, 1, s] = \frac{-4s}{(1-s)^2} = \frac{-4}{(e^{\delta/2} - e^{-\delta/2})^2} = -\frac{1}{\sinh^2(\delta/2)}$$

while if the axes meet at a finite point, we choose a Möbius transformation so the line endpoints are ± 1 and $e^{\pm i\theta}$ and the result follows similarly.

We next recall the result in Equation (6.4) of [46] which allows us to relate the parameters of a pair of Möbius transformations to cross ratios.

Theorem 3.49. *Let f and g be Möbius transformations and let $\delta + i\theta$ be the complex distance between their axes. Then*

$$4\gamma(f, g) = \beta(f)\,\beta(g)\,\sinh^2(\delta + i\theta). \tag{3.66}$$

For a pair of hyperbolics f and g we have by definition $\beta(f), \beta(g) > 0$, and the axes meet if and only if the complex distance between the axes is zero. Thus the axes cross if and only if $\delta = 0$, under which condition $\sinh^2(\delta + i\theta) = \sinh^2(i\theta) = -\sin^2(\theta)$ and the axis crossing condition becomes $\gamma(f, g) \leq 0$. From (3.65) we have then the equivalent condition:

$$[\mathbf{z_1}, \mathbf{w_1}, \mathbf{z_2}, \mathbf{w_2}] \geq 1. \tag{3.67}$$

To see this we choose the Möbius transformation which sends $\mathbf{z_1} \mapsto 1, \mathbf{z_2} \mapsto i, \mathbf{w_1} \mapsto -1$ and $\mathbf{w_2} \mapsto z \in \mathbb{S}$ say, then:

$$[\mathbf{z_1}, \mathbf{w_1}, \mathbf{z_2}, \mathbf{w_2}] = \frac{(1 - -1)(i - \mathbf{z})}{(1 - i)(-1 - \mathbf{z})} = 1 - \frac{\Im m(\mathbf{z})}{1 + \Re e(\mathbf{z})} + 0\,i. \tag{3.68}$$

Then the image of the axes (and therefore the axes themselves) cross when:

$$\text{that is, if and only if} \quad \begin{array}{l} 1 - \frac{\Im m(\mathbf{z})}{1+\Re e(\mathbf{z})} \geq 1 \\ \\ \Im m(\mathbf{z}) \leq 0. \end{array} \tag{3.69}$$

The result becomes clear as a simple geometric condition if in the disc model of hyperbolic space we visualise the two hyperbolic lines with endpoints mapped as above on the circle at ∞. We note that not only is the cross ratio invariant under Möbius transformation, but since we can always find a Möbius transformation to take a circle to any other a cross ratio can always be found to take any 3 points to any 3 points. Hence the result in (3.68) that the cross ratio of four points on a circle is always real.

3.7.2 Cross ratio of fixed points

Supposing that f and g are randomly chosen hyperbolic elements represented respectively by matrices A and B in $\mathcal{F}$:

$$\begin{aligned} A &= \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix} = \begin{pmatrix} a\, e^{i\theta_a} & c\, e^{-i\theta_c} \\ c\, e^{i\theta_c} & a\, e^{-i\theta_a} \end{pmatrix} \\ \text{and} \\ B &= \begin{pmatrix} \mathbf{e} & \overline{\mathbf{g}} \\ \mathbf{g} & \overline{\mathbf{e}} \end{pmatrix} = \begin{pmatrix} e\, e^{i\theta_e} & g\, e^{-i\theta_g} \\ g\, e^{i\theta_g} & e\, e^{-i\theta_e} \end{pmatrix}. \end{aligned} \tag{3.70}$$

We now want to discuss the probability of the axes of transformations f and g crossing. Let the fixed points of f and g be respectively $\mathbf{z}_1, \mathbf{z}_2$ and $\mathbf{w}_1, \mathbf{w}_2$. Since the fixed points of hyperbolic transformations in $\mathcal{F}$ lie in $\mathbb{S}$, with reference to (3.40) we may express the fixed points in terms of some arguments $\alpha, \beta \in [0, 2\pi)$:

$$\begin{aligned} &\mathbf{z_1} = e^{-i\theta_c} e^{i\alpha} = e^{i(\alpha-\theta_c)} && \mathbf{z_2} = e^{-i\theta_c} e^{i(\pi-\alpha)} = -e^{i(-\alpha-\theta_c)} \\ &\mathbf{w_1} = e^{-i\theta_g} e^{i\beta} = e^{i(\beta-\theta_g)} && \mathbf{w_2} = e^{-i\theta_g} e^{i(\pi-\beta)} = -e^{i(-\beta-\theta_g)} \\ \text{hence} \\ &\mathbf{z_1} - \mathbf{z_2} = 2\cos(\alpha)\, e^{-i\theta_c} && \mathbf{w_1} - \mathbf{w_2} = 2\cos(\beta)\, e^{-i\theta_g} \\ \text{and} \\ &\mathbf{z_1} - \mathbf{w_1} = e^{i(\alpha-\theta_c)} - e^{i(\beta-\theta_g)} && \mathbf{z_2} - \mathbf{w_2} = -e^{i(-\alpha-\theta_c)} + e^{i(-\beta-\theta_g)}. \end{aligned} \tag{3.71}$$

We form the numerator and denominator of the cross ratio:

$$\begin{aligned} (\mathbf{z_1} - \mathbf{z_2})(\mathbf{w_1} - \mathbf{w_2}) &= 4\cos(\alpha)\cos(\beta) e^{-i(\theta_c+\theta_g)} \\ (\mathbf{z_1} - \mathbf{w_1})(\mathbf{z_2} - \mathbf{w_2}) &= \left(e^{i(\alpha-\theta_c)} - e^{i(\beta-\theta_g)}\right)\left(e^{i(-\beta-\theta_g)} - e^{i(-\alpha-\theta_c)}\right) \\ &= e^{i(\alpha-\beta-\theta_c-\theta_g)} - e^{-2i\theta_c} - e^{-2i\theta_g} + e^{i(-\alpha+\beta-\theta_c-\theta_g)} \\ &= e^{-i(\theta_c+\theta_g)}\left(e^{i(\alpha-\beta)} + e^{i(-\alpha+\beta)}\right) - e^{-2i\theta_c} - e^{-2i\theta_g} \\ &= 2\cos(\alpha-\beta) e^{-i(\theta_c+\theta_g)} - e^{-2i\theta_c} - e^{-2i\theta_g}. \end{aligned} \tag{3.72}$$

The inverse cross ratio is then:

$$\begin{aligned} [\mathbf{z_1}, \mathbf{z_2}, \mathbf{w_1}, \mathbf{w_2}] &= \frac{2\cos(\alpha-\beta) e^{-i(\theta_c+\theta_g)}}{4\cos(\alpha)\cos(\beta) e^{-i(\theta_c+\theta_g)}} - \frac{e^{-2i\theta_c}}{4\cos(\alpha\cos(\beta) e^{-i(\theta_c+\theta_g)}} - \frac{e^{-2i\theta_g}}{4\cos(\alpha)\cos(\beta) e^{-i(\theta_c+\theta_g)}} \\ &= \frac{\cos(\alpha)\cos(\beta)+\sin(\alpha)\sin(\beta)}{2\cos(\alpha)\cos(\beta)} - \frac{e^{i(\theta_g+\theta_c)}}{4\cos(\alpha)\cos(\beta)} - \frac{e^{i(\theta_c+\theta_g)}}{4\cos(\alpha)\cos(\beta)} \\ &= \frac{1}{2}\left[1 + \tan(\alpha)\tan(\beta) - \frac{\cos(\psi)}{\cos(\alpha)\cos(\beta)}\right] \end{aligned} \tag{3.73}$$

where $\psi = \theta_c + \theta_g$ is circular uniform. We want to understand the statistics of the cross ratio, and in particular to determine when $[\mathbf{z_1}, \mathbf{w_1}, \mathbf{z_2}, \mathbf{w_2}] > 1$, that is when $[\mathbf{z_1}, \mathbf{z_2}, \mathbf{w_1}, \mathbf{w_2}] < 1$. We note that in (3.73) there are two terms in both α and β so the expression is a sum of non independent variables and so not amenable to analytic determination of the distribution function. We can however substitute from (3.40) for the general variables used:

$$
\begin{aligned}
\alpha &= \tan^{-1} \frac{|\mathbf{a}| \sin(\theta_a)}{\pm\sqrt{|\mathbf{a}|^2 \cos^2(\theta_a) - 1}} \\
\beta &= \tan^{-1} \frac{|\mathbf{e}| \sin(\theta_e)}{\pm\sqrt{|\mathbf{e}|^2 \cos^2(\theta_e) - 1}}
\end{aligned}
\tag{3.74}
$$

and noting that for hyperbolic elements the respective discriminants are non negative we compute the distribution as in Figure 3.14 for $4,000,000$ outcomes:

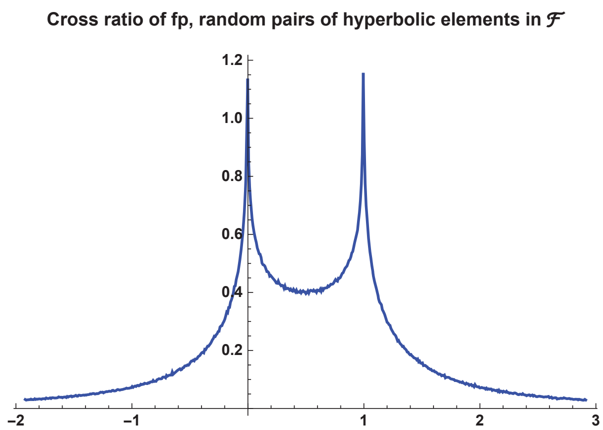


Figure 3.14: Computed distribution of the inverse cross ratio of fixed points of pairs of random hyperbolic transformations in $\mathcal{F}$.

Since this is the inverse cross ratio, the axis-crossing condition becomes $[z_1, z_2, w_1, w_2] \leq 1$, and we have from the computational experiment:

$\downarrow$ **Probability in domain**	**hyperbolic** $f, g \in \mathcal{F}$	**conjectured**
$\mathbb{P}_{[z_1,z_2,w_1,w_2]<0}$	0.1996453	$\frac{1}{5}$
$\mathbb{P}_{[z_1,z_2,w_1,w_2]\in[0,1]}$	0.60052001	$\frac{3}{5}$
$\mathbb{P}_{[z_1,z_2,w_1,w_2]>1}$	0.199834721	$\frac{1}{5}$

Figure 3.15: Computational experiment, cross ratio probabilities for pairs of transformations in $\mathcal{F}$.

Note that the fractional probabilities are here conjectured from the computational experiment, however Corollary 3.60 will confirm the axis-crossing probability of $\mathbb{P} = \frac{1}{5}$, as in the third row of Figure 3.15 above.

In contrast we have the following theorem.

Theorem 3.50. *For a matrix group in $\mathcal{F}$ two random elements are axis-crossing with probability $\mathbb{P} = \frac{1}{3}$.*

Proof. Suppose $f, g \in \mathcal{F}$ and $\Gamma = \langle f, g \rangle$. If we choose any three of the isometric circles representing f, g, f^{-1} and g^{-1} then they intersect $\mathbb{S}$ as illustrated in Figure 3.16 (Left).

Figure 3.16: Axis crossing geometry for transformations $f \in \mathcal{F}$.

Project the ray from the centre of $\mathbb{S}$ through the centre of the fourth isometric circle and designate its intersection with $\mathbb{S}$ as $\mathbf{z}$, an example is illustrated in Figure 3.16 (Right). There are now precisely three circle segments on which $\mathbf{z}$ could lie, but only one of these choices corresponds to the axis-crossing condition.

Since the axes of the transformations pass through the isometric circle centres and the isometric circle centres have circular uniform distribution about the centre of $\mathbb{S}$ there are twice as many non axis-crossing pairs of isometric circles as axis-crossing. That is:

$$\begin{aligned} \mathbb{P}_{\gamma \in \Gamma \ axis-crossing} &= \tfrac{1}{3} \\ \mathbb{P}_{\gamma \in \Gamma \ non\ axis-crossing} &= \tfrac{2}{3}. \end{aligned} \tag{3.75}$$

□

The argument of this theorem can be reduced to an invocation of Theorem 3.17, with three isometric centres on $\mathbb{S}$ and three arcs between them we wish to know with what probability a fourth random isometric circle centre is centered on any one of the these arcs. According to the theorem the answer is $\mathbb{P} = \frac{1}{3}$, and the conclusion follows since only choice of that arc between the two isometric circle centres of the same transformation results in crossing of the transformation axes.

Together Theorem 3.50 and Corollary 3.60 quantify the degree to which the fixed points are correlated on the circle. However what we would like to understand is with what probability $\gamma([f, g]) < 0$ for a discrete group $\langle f, g \rangle$ with hyperbolic generators, so we turn to a discussion of positive results for discreteness.

3.8 Discreteness

Notice that $\gamma([A, B]) \in [-4, 0]$ implies $(\text{trace}([\text{A}, \text{B}]) - 4)^2 \in [-4, 0]$ and $[A, B]$ is elliptic and of finite order on a countable subset of $[-4, 0]$, hence the following theorem:

Theorem 3.51. *If $f, g \in \mathcal{F}$ are randomly chosen and if $\gamma([f, g]) \in [-4, 0]$, then $\langle f, g\rangle$ is almost surely not discrete.*

From the results of the computational experiment reported in Figure (3.9), we have $\mathbb{P}_{\gamma\in[-4,0]} \approx 0.161724$ and this is our estimate that the probability that pairs of hyperbolic elements of $\mathcal{F}$ are not discrete and free.

Since independent events X and Y always have no greater probability of occurrence than if X and Y exhibited any degree of dependence, we can use Theorem 2.5 to give us an obvious bound: if $f, g \in \mathcal{F}$ are randomly chosen, then the probability that $\langle f, g\rangle$ is discrete is at least $\frac{1}{64}$. We can generalise this conclusion as follows:

Theorem 3.52. *For n independent random elements of $f_n \in \mathcal{F}$, with matrix representation any distinct $m \leq n(2n-1)$ of the elementary isometric circle intersection events correspond to mutually disjoint intersections with probability $\mathbb{P} = \frac{1}{(n!)^m}$.*

Proof. By Theorem 2.7 the set of independent pairs of intersections in $\mathfrak{F}_{2n}$ is of order $n(2n-1)$. Theorems 3.54 and 3.55 generalise via Theorem 4.24 so that each elementary event corresponds to a disjoint intersection with probability $\frac{1}{n!}$. Since these probabilities are independent any m intersection pairs correspond to disjoint intersections with probability $\mathbb{P} = \frac{1}{(n!)^m}$. □

For n generator groups this number is at least $2^{-(2n-1)!}$.

We will improve the lower bound for the probability that $\langle f, g\rangle$ is discrete for $f, g \in \mathcal{F}$ to $\mathbb{P} = \frac{1}{20}$, but this will require some prepatory work.

3.8.1 The Klein combination theorem and isometric circles

The Klein combination theorem has been presented as Theorem 2.5, this provides an easy method for determining a lower bound for the probability that a group generated by two random elements of $\mathcal{F}$ is discrete. The methodology follows since Theorem 2.4 identifies hyperbolic transformations with disjoint isometric circles. Note again that the isometric circles of $\mathcal{F}$ are orthogonal to the unit circle $\mathbb{S}$, and hence have their closest disjoint approach on $\mathbb{S}$. We have already seen that the isometric discs of a randomly chosen $f \in \mathcal{F}$ are disjoint with probability $\frac{1}{2}$ and we generalise this slightly in the next section.

3.8.2 Intersections of two isometric circles of elements of $\mathcal{F}$

Lemma 3.53. *Let α and β be arcs on $\mathbb{S}$ with uniformly randomly chosen midpoints ζ_α and ζ_β and subtending angles θ_α and θ_β uniformly chosen from $[0, \pi]$. Then α and β meet with probability $\frac{1}{2}$.*

Proof. The smaller arc subtended between ζ_α and ζ_β has length $\Theta = \arg(\zeta_\alpha\overline{\zeta_\beta})$ and is uniformly distributed in $[0, \pi]$. Then α and β are disjoint if $\Theta - \theta_\alpha/2 - \theta_\beta/2 \geq 0$. Since Corollary 3.24 tells us that $2\Theta - \theta_\alpha - \theta_\beta$ is uniformly distributed in $[-2\pi, 2\pi)$, this number is positive is with probability $\frac{1}{2}$. □

Some of the following theorems rely on linear combination results obtained via the method of characteristic functions, relevant distributions for random variables $x_j \in_u [0,\pi]$ are listed in Figure 4.5.

Theorem 3.54. *An element of $\mathcal{F}$ represented by a matrix A has isometric circles disjoint with probability $\mathbb{P} = \frac{1}{2}$; that is, for the isometric circles of A:*

$$\mathbb{P}_{\mathcal{A}\cap\mathcal{A}^{-1}} = \frac{1}{2}.$$

Proof. By Theorem 3.27 the arguments η, η' of the vectors to the centres of the isometric circles of A, A^{-1} respectively have circular uniform distribution. Then by Theorem 3.29 the angular distance $d = |\eta - \eta'| \in [0, 2\pi)$ between these centres is also circular uniform. Since the circles are of identical radius they are centered on the same circle about $\mathbb{S}$ and since they intersect $\mathbb{S}$ orthogonally their closest approach is on $\mathbb{S}$. Then the isometric circles subtend arcs of equal length $\phi = 2\alpha \in_u [0,\pi]_{\mathbb{R}}$ with circular uniform distribution. The arc length separation between the circles is $\delta = |d| - 2\alpha = |d| - \phi$ and the arc distance between the isometric circle intersections with $\mathbb{S}$ is then:

$$\begin{aligned} & |d| \in_u [0,2\pi)_{\circ} = \tfrac{1}{2}d \in_u [0,2\pi)_{\mathbb{R}} = d \in_u [0,\pi]_{\mathbb{R}} \\ \text{and} \quad & \\ & \delta = d \in_u [0,\pi]_{\mathbb{R}} - \phi \in_u [0,\pi]_{\mathbb{R}}. \end{aligned} \tag{3.76}$$

The result is a random variable of the form of $x_1 - x_2$ for $x_1, x_2 \in_u [0,\pi]$ and since $x_1 = d$ and $x_2 = \phi$ are independent the distribution in (4.32) applies and δ is non negative with probability $\frac{1}{2}$. □

Theorem 3.55. *For two elements of $f, g \in \mathcal{F}$, with matrix representation an isometric circle of f is disjoint from an isometric circle of g with probability $\mathbb{P} = \frac{1}{2}$; that is, for the isometric circles of matrices A and B:*

$$\mathbb{P}_{\mathcal{A}\cap\mathcal{B}} = \mathbb{P}_{\mathcal{A}\cap\mathcal{B}^{-1}} = \mathbb{P}_{\mathcal{A}^{-1}\cap\mathcal{B}} = \mathbb{P}_{\mathcal{A}^{-1}\cap\mathcal{B}^{-1}} = \frac{1}{2}.$$

Proof. Suppose the intersection arcs of the circles with $\mathbb{S}$ are of lengths $2\alpha_A$ and $2\alpha_B \in_u [0,\pi]_{\mathbb{R}}$ respectively. By Theorem 3.27 the angular distance between centres of the isometric circles of each matrix is separately uniformly distributed, accordingly the distribution of the distance between the centres of dissimilar circle pairs on $\mathbb{S}$ can be calculated as:

$$\begin{aligned} \delta &= d \in_u [0,2\pi]_{\mathbb{R}} - \alpha_A \in_u [0,\pi]_{\mathbb{R}} - \alpha_B \in_u [0,\pi]_{\mathbb{R}} \\ &= 2d \in_u [0,\pi]_{\mathbb{R}} - \alpha_A \in_u [0,\pi]_{\mathbb{R}} - \alpha_B \in_u [0,\pi]_{\mathbb{R}}. \end{aligned} \tag{3.77}$$

This is a random variable of the form of $2x_1 - x_2 - x_3$ for $x_1, x_2, x_3 \in_u [0,\pi]$ and since $x_1 = d$ and $x_2, x_3 = \alpha_A, \alpha_B$ respectively are all independent the distribution in (4.36) applies and δ is non negative with probability $\frac{1}{2}$. □

The two distributions in Theorems 3.54 and 3.55 are quite different but both symmetrical about 0, hence the non negative probabilities are identical.

We next consider the more complicated problem of disjoint pairs of arcs not necessarily of equal magnitude, terming a set of arcs which have no intersections *mutually disjoint*.

3.8.3 Intersections of the four isometric circles of two elements of $\mathcal{F}$

We consider the intersection events of the four isometric circles of two independent random transformations in $\mathcal{F}$.

Theorem 3.56. *If two elements of $\mathcal{F}$ are represented by matrices A and B then the isometric circle pairs of A are disjoint while the isometric circles of B are disjoint with probability $\mathbb{P} = \frac{1}{4}$; that is, for the isometric circles of matrices A and B and event e_3 in class $\mathcal{E}_2$ of $\mathfrak{F}_4$:*

$$\mathbb{P}_{(\mathcal{A}\cap\mathcal{A}^{-1})\cup(\mathcal{B}\cap\mathcal{B}^{-1})} = \frac{1}{4}.$$

We provide two proofs.

Proof.

(1) Via Kolmogorov's theorem:
The only independent pair of intersection events in the $\sigma-$field $\mathfrak{F}_4$ is:

$$\{(\mathcal{A}\cap\mathcal{A}^{-1}),\ (\mathcal{B}\cap\mathcal{B}^{-1})\}$$

and by Theorem 3.54 each elementary event corresponds to disjoint intersection with probability $\frac{1}{2}$. Then the two independent intersection events $\{(\mathcal{A}\cap\mathcal{A}^{-1})$ and $(\mathcal{B}\cap\mathcal{B}^{-1})\}$ are disjoint with probability $\frac{1}{2}\times\frac{1}{2}=\frac{1}{4}$.

(2) A geometric proof:
Each of the events $(\mathcal{A}\cap\mathcal{A}^{-1})$ and $(\mathcal{B}\cap\mathcal{B}^{-1})\}$ has p.d.f. according to:

$$f(x) = \frac{1}{\pi^2}\begin{cases} \pi + x & -\pi \le x < 0 \\ \pi - x & 0 \le x \le \pi \\ 0 & elsewhere. \end{cases} \tag{3.78}$$

Figure 3.17 represents the probability surface for the joint distribution $f(x, y) = f(x)f(y)$ of two independent random variables each distributed according to (3.78), but we are interested in only non negative joint probability represented by the red rectangle in the first quadrant:

$$\begin{aligned} \int\int f(x,y)\,dx\,dy &= \int\int \left(\tfrac{\pi-y}{\pi^2}\right)\left(\tfrac{\pi-x}{\pi^2}\right)\,dx\,dy \\ &= \tfrac{xy}{4\pi^4}(4\pi^2+1-2\pi(x+y)) \end{aligned} \tag{3.79}$$

and we obtain the total probability of non negativity by evaluating the indefinite integral in (3.79) over the square representing non negative occurrences:

$$\int_{y=0}^{\pi}\int_{x=0}^{\pi} f(x,y)\,dx\,dy = \frac{1}{4}.$$

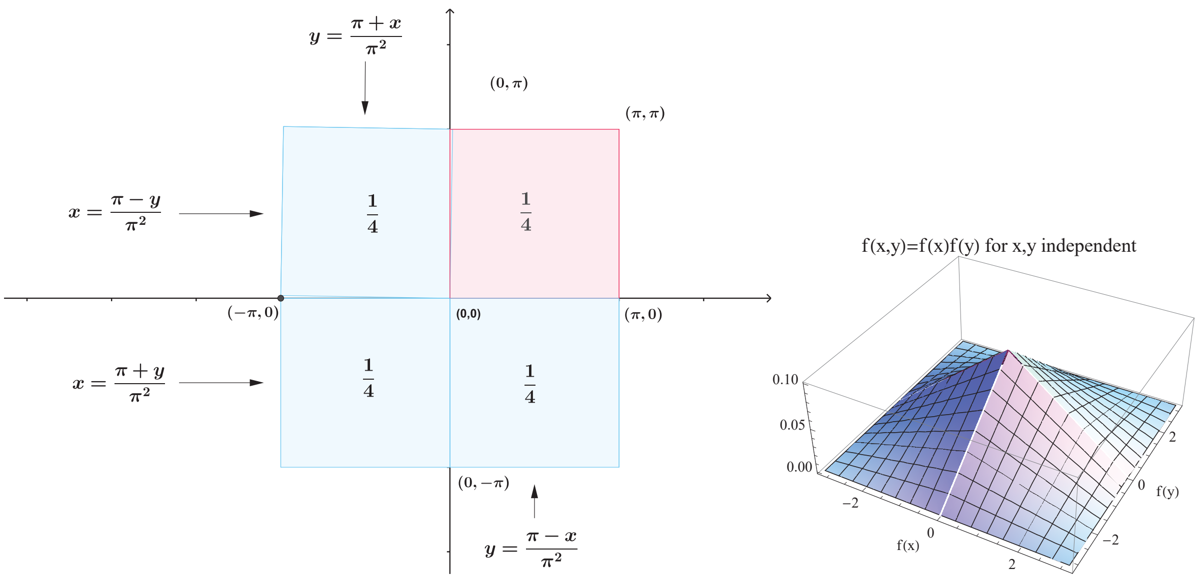


Figure 3.17: Probability surface for $\mathfrak{D}_{x=(x_1-x_2)} \times \mathfrak{D}_{y=(x_3-x_4)}$, $x_i \in_u [0, \pi]$ corresponding to the independent pair of intersection events in the $\sigma-$field $\mathfrak{F}_4$, Left: showing the total probability that random variables x and y are in each sub domain of the supporting domain of $f(x, y)$, Right: showing the 3-D surface of $f(x, y)$ supported on $[-\pi, \pi] \times [-\pi, \pi]$.

$\square$

We cannot make the claim of Theorem 3.52 for events that include any of the dependent elementary events, another approach is required. There is actually an order relationship that must be considered and this is the basis of Theorem 3.57. Essentially if the intersection arcs are in order such that all four events $(\mathcal{A}\cap\mathcal{B}), (\mathcal{A}\cap\mathcal{B}^{-1}), (\mathcal{A}^{-1}\cap\mathcal{B})$ and $(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$ are disjoint then the events $(\mathcal{A} \cap \mathcal{A}^{-1})$ and $(\mathcal{B} \cap \mathcal{B}^{-1})$ must be always disjoint by reason of the order of the arcs (for instance as illustrated in Figure 3.18), so such ordering of the random variables involved constrains the nett probability. The classic work on ordered random variables is Herbert and Nagaraja, [28].

Theorem 3.57. *In the σ-field $\mathfrak{F}_4$ the elementary events $(\mathcal{A} \cap \mathcal{B}), (\mathcal{A} \cap \mathcal{B}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B})$ and $(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$ for matrices A and B representing random elements of $\mathcal{F}$ correspond to mutually disjoint intersections with probability $\mathbb{P} = \frac{1}{5}$. That is, for the isometric circles of matrices A and B:*

$$\mathbb{P}_{(\mathcal{A}\cap\mathcal{B})\cup(\mathcal{A}\cap\mathcal{B}^{-1})\cup(\mathcal{A}^{-1}\cap\mathcal{B})\cup(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})} = \frac{1}{5}. \tag{3.80}$$

Proof. Let $\mathcal{E}$ be the ordered set of random isometric circle intersection arcs $\{\mathcal{A},\ \mathcal{B}, \mathcal{A}^{-1}\mathcal{B}^{-1}\}$ while allowing any cyclic permutation and order in either direction. Then from Theorem 3.17 the probability that a random point on $\mathbb{S}$ is excluded from $\cup\{\mathcal{E}\}$ is $\mathbb{P} = \frac{1}{5}$. We note that with this ordering, if $\cap\{\mathcal{E}\} = \varnothing$ then necessarily $\{(\mathcal{A} \cap \mathcal{A}^{-1})\} = \varnothing$ and $\{(\mathcal{B} \cap \mathcal{B}^{-1})\} = \varnothing$ and the topology ensures that (3.80) correctly assigns the probability of mutual disjoint occurrence of the events in $\mathcal{E}$. That is, $\mathbb{P}_{\cap\{\mathcal{E}\}=\varnothing} = \frac{1}{5}$. □

The importance of Theorem 3.57 is that it supplies corollaries relating to the independence of independent events and mutual intersection events (3.59), a lower bound for the probability that a group with two hyperbolic generators in $\mathcal{F}$ is discrete (3.58), and eventually to a lower bound on the discreteness of two-generator subgroups of $\mathcal{F}$ (3.61). Notice that the possible distinct topologies of ordered sets $\mathcal{E}$ correspond to the two transformations being axis-crossing or not. The arcs of $\mathcal{A}$ and $\mathcal{A}^{-1}$ being adjacent (which necessitates the adjacency of the arcs of $\mathcal{B}$ and $\mathcal{B}^{-1}$) corresponds to the two transformations being non axis-crossing.

Although at first sight events containing the same random variable would seem to be dependent, Theorem 3.57 indicates that there are circumstances in which this is not so. We have the following Corollary to Theorem 3.57:

Corollary 3.58. *Two randomly chosen hyperbolic transformations $f, g \in \mathcal{F}$ generate a discrete group $\langle f, g\rangle$ with probability at least $\frac{1}{5}$.*

Corollary 3.59. *The event $(\mathcal{A} \cap \mathcal{A}^{-1}) \cup (\mathcal{B} \cap \mathcal{B}^{-1})$ is independent of the event $(\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap \mathcal{B}^{-1}) \cup (\mathcal{A}^{-1} \cap \mathcal{B}) \cup (\mathcal{A}^{-1} \cap \mathcal{B}^{-1})$.*

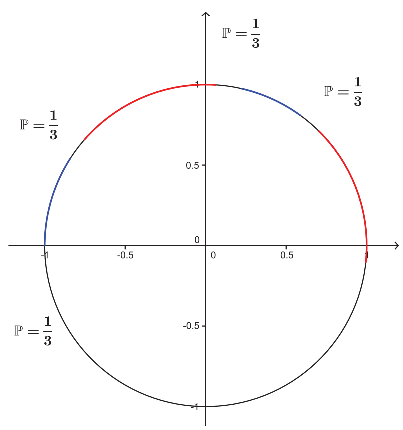


Figure 3.18: An ordered set of random isometric circle intersection arcs $\{\mathcal{A},\ \mathcal{B}, \mathcal{A}^{-1}\mathcal{B}^{-1}\}$: the order precludes the intersections $\mathcal{A} \cap \mathcal{A}^{-1}$ or $\mathcal{B} \cap \mathcal{B}^{-1}$ as long as $\mathcal{A} \cap \mathcal{B} = \varnothing$ etc.

The following corollary supplies a proof of the computationally derived axis-crossing probability reported in Figure 3.15 for hyperbolic transformations in $\mathcal{F}$.

Corollary 3.60. *Let f, g be randomly chosen hyperbolic elements of $\mathcal{F}$. Then the axes of f and g cross with probability $\frac{1}{5}$.*

3.8.4 $\mathcal{F}$ is discrete with $\mathbb{P} \geq \frac{1}{20}$

One of the main results of this thesis follows.

Theorem 3.61. *Randomly chosen Möbius transformations $f, g \in \mathcal{F}$ generate a discrete group $\langle f, g \rangle$ with probability at least $\frac{1}{20}$.*

Proof. With matrix representation of random transformations in $\mathcal{F}$, two pairs of isometric circles are independently disjoint with probability $\mathbb{P} = \frac{1}{4}$ by Theorem 3.56 and mutually disjoint with probability $\mathbb{P} = \frac{1}{5}$ by Theorem 3.57. Since these two events are independent by Corollary 3.59 we conclude that the isometric circles of the matrices induced by f and g are disjoint with probability $\mathbb{P} = \frac{1}{4} \times \frac{1}{5} = \frac{1}{20}$. The result follows from the Klein combination theorem, 2.5. □

Chapter 4

Probability and random variables

In this supporting chapter we develop theory specifically for mathematical and computational analysis of isometric circle intersection probabilities on circular domains.

4.1 Isometric circle intersections

Definition 2.10 is usually taken to define of random event independence but we must be very careful. A single complex matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix}$ representing a Möbius transformation determines two isometric circles, $\mathcal{A}$ and $\mathcal{A}^{-1}$. We will assume that the Möbius transformation represented by A is in $\mathcal{F}$ but the following argument is easily generalised.

The radii r of the two isometric circles of A are identical and the isometric circle centres are both related to the matrix entry $\mathbf{c}$ (and located on a circle of radius $\sqrt{1+r^2}$) so random events $\mathcal{A}$ and $\mathcal{A}^{-1}$ clearly exhibit dependence. However, given any fixed isometric circle radius the angular position of the isometric circle intersection arcs on $\mathbb{S}$ are independent random variables. We will be working with σ-fields where the elementary events are intersections of isometric circles with $\mathbb{S}$, and the angular positions of the intersection arcs on $\mathbb{S}$ of $\mathcal{A}$, $\mathcal{A}^{-1}$ $\mathcal{B}$ and $\mathcal{B}^{-1}$ are mutually independent random variables and all the elementary events are pairwise unions of these independent random variables. When we consider the non elementary intersection events in the σ-field, only the single event $\mathcal{A} \cap \mathcal{A}^{-1} \cup \mathcal{B} \cap \mathcal{B}^{-1}$ is the union of independent events as for instance $\mathcal{A} \cap \mathcal{A}^{-1}$ and $\mathcal{A} \cap \mathcal{B}$ have a random variable in common, the intersection arc of $\mathcal{A}$ with $\mathbb{S}$.

Example 4.1.

(1) *For a single random matrix A the set of isometric circles is:*

$$S_2 = \{\mathcal{A}, \mathcal{A}^{-1}\}$$

and the set of elementary events is:

$$E_2 = \{(\mathcal{A} \cap \mathcal{A}^{-1})\}.$$

In this case the σ-field is strictly $\{(\mathcal{A}\cap\mathcal{A}^{-1}), \overline{(\mathcal{A}\cap\mathcal{A}^{-1})}, \varnothing\}$*, but as indicated in Section 2.2.4 we will use a relaxed form (both here and from now on) since we have little interest in the event complements or null events:*

$$\mathfrak{F}_2 = \{(\mathcal{A}\cap\mathcal{A}^{-1})\}.$$

(2) *For two random matrices* A, B *the set of isometric circles is:*

$$S_4 = \{\mathcal{A}, \mathcal{A}^{-1}, \mathcal{B}, \mathcal{B}^{-1}\}.$$

The set of elementary events is:

$$E_4 = \{(\mathcal{A}\cap\mathcal{A}^{-1}), (\mathcal{B}\cap\mathcal{B}^{-1}), (\mathcal{A}\cap\mathcal{B}), (\mathcal{A}\cap\mathcal{B}^{-1}), (\mathcal{A}^{-1}\cap\mathcal{B}), (\mathcal{A}^{-1}\cap\mathcal{B}^{-1})\}$$

and the σ-field is $\mathfrak{F}_4$ *which is the power set of all subsets of* E_4 *and is of order* 2^6*, and can be partitioned into six subsets of orders* $|\mathfrak{F}_{4,k}| \in \{6, 15, 20, 15, 6, 1\}$ *each corresponding to* k *isometric circle intersection pairs. Computationally determined probabilities for the entire* $\mathfrak{F}_4$ *σ-field for a specific experiment can be found in Section 5.2.*

(3) *The set of independent events in* $\mathfrak{F}_4$ *is* $\{(\mathcal{A}\cap\mathcal{A}^{-1}), (\mathcal{B}\cap\mathcal{B}^{-1})\}$.

Definition 4.2. *The sets of events under union of* $k \in [1, m]$ *pairwise intersection events in a σ-field of* $\mathfrak{F}_n$ *are the* m ***equivalence classes*** $\mathcal{E}_k$ *of* $\mathfrak{F}_n$.

4.2 Domains of support for random variables

A function supported on any one-dimensional domain can always be "straightened" so that all points are mapped without distortion of distances onto a domain in $\mathbb{R}$, such a statement is not true for dimensions greater than one. Such a domain is a set E of possibly disconnected intervals $I_i \subset \mathbb{R}$ for which a bijective and locally isometric mapping $\Psi : D \mapsto E = \cup_i I_i$ maps a one-dimensional domain D in some Euclidean space onto $E \subset \mathbb{R}$ with $|E| = |D|$ for all sub intervals I_i. Theorem 4.3 follows from the fact that $\mathbb{R}$ is an additive group.

Theorem 4.3. *All linear combinations* $F = \pm x_1, \pm x_2, \ldots, \pm x_N$ *of* N *non negative random variables identically distributed over a domain which maps to* $I \in \mathbb{R}^+$ *result in distributions of identical form over a domain of magnitude* $NI \in \mathbb{R}^+$.

Corollary 4.4. *With the nomenclature of Theorem 4.3, if* n *of the random variables in the expression* F *have negative signs and* p *have positive signs then the domain of the resultant random variable is the union of* n *negative sub domains and* p *positive sub domains, where* $n + p = N$.

Theorem 4.5. *For a random variable distributed over a domain that maps to a union of sub domains in* $\mathbb{R}$*:*

(1) *Scalar multiplication by* $k \in \mathbb{R}$ *results in exactly the same mathematical form of distribution as the original random variable but with the resultant function supported on* $\frac{1}{k}$ *times the original interval. That is, for* x *uniformly distributed over* $[0, \pi]$*:*

$$\mathbb{P}_{kx\in[0,\pi]_\mathbb{R}} = \frac{1}{k}\,\mathbb{P}_{x\in[0,k\pi]_\mathbb{R}}. \tag{4.1}$$

(2) *Addition of a signed scalar to a random variable results in a corresponding adjustment to the domain.*

Proof.

(1) Since $\mathbb{R}$ is a ring, for any interval $I \subset \mathbb{R}$ and constant $k \in \mathbb{R}$, $x \in I \Rightarrow kx \in kI$, and since the p.d.f. integrates to 1 over the domain the resultant must be scaled by $\frac{1}{k}$.

(2) If $g(x)$ is supported on $[a, b]$ then $g(x) - k$ is supported on $[a - k, b - k]$.

□

A direct result of Theorem 4.5 is that we can always replace scaled random variables with random variables and as a result of Theorem 4.3 linear combinations can be analysed as sums of random variables. To obtain the p.d.f. of the sum of n signed random variables distributed over equal sized domains, we merely count the number m of negative signs and allow the absolute p.d.f. to be positioned on a domain m sub domain magnitudes to the left of 0. It is trivial to extend this to allow adjustment of all random variables in an expression so that they are supported on identical domains, or alternatively to replace scalar multiples of random variables with unmodified random variables over scaled domains.

Definition 4.6. *A random variable is symmetrical if its p.d.f. is even.*

Then for symmetrical random variables (or those which can be made symmetrical via Corollary 4.4), taking the modulus of the p.d.f. results in a distribution over the positive half domain only with function values doubled at all points in the range. That is, if a random variable x is symmetrical with p.d.f. $f(x)$ supported on a domain $[-k, k]$ then:

$$|f(x)| \in [-k, k] = 2\, f(x) \in [0, k]. \tag{4.2}$$

4.2.1 Modular domains

Definition 4.7. *A* ***modular domain*** *is a closed interval $M = [m_1, m_2] \subset \mathbb{R}$ of magnitude $\zeta = |m_2 - m_1|$ for which the equivalence relation:*

$$\forall x \in M,\ x + \zeta = x \tag{4.3}$$

is satisfied.

Definition 4.8. *A* ***circular domain*** *is a modular domain for which the equivalence relation:*

$$\forall x \in [0, 2\pi),\ x + 2\pi = x \tag{4.4}$$

is satisfied.

We note here that the uniform distribution can be seen to be "natural" for a random variable defined on a modular domain in that the p.d.f. would indicate equal probability of occurrence of the random variable over the entire domain.

Example 4.9. *Figure 3.2 shows how for a random variable the experimental outcomes in the two equivalence classes* $[-2\pi, 0]_{\mathbb{R}}$ *and* $[0, 2\pi]_{\mathbb{R}}$ *sum to give a net uniform distribution for the difference between two uniform distributions over* $[0, 2\pi)_o$ *on a circular (modular) domain.*

The important difference between modular domains and intervals of $\mathbb{R}$ is brought out by the following two definitions.

Definition 4.10. *The modulus of a random variable* X *with experimental outcomes* ξ_i *distributed over a sub interval of* $\mathbb{R}$ *is the random variable* $|X|_{\mathbb{R}}$ *with experimental outcomes* $|\xi_i|$.

Definition 4.11. *The modulus of a random variable* X *distributed over a modular domain* M *is the random variable* $|X|_M$ *which is constituted by the mapping of outcomes from all equivalence classes onto* M.

4.3 Functional transformations of random variables

Our objective here is to present for reference or develop methods of calculating p.d.f.'s for functional combination and composition of random variables of known distribution, we quote without proof some standard results.

4.3.1 Multi-variable transformations

Theorem 4.12. *For transformations* $y_1 = h(x_1, x_2)$ *and* $y_2 = g(x_1, x_2)$ *of a joint p.d.f.* $f(x_1, x_2)$ *(where the* x_i *are the pre-images of the* y_i*) with first partial derivatives and having unique inverses, the resultant joint p.d.f. is given by:*

$$g(y_1, y_2) = f(h^{-1}(y_1, y_2), g^{-1}(y_1, y_2))\ J \tag{4.5}$$

where J *is the Jacobian:*

$$J = \left| \det \begin{pmatrix} \frac{\partial h^{-1}(y_1,y_2)}{\partial y_1)} & \frac{\partial h^{-1}(y_1,y_2)}{\partial y_2)} \\ \frac{\partial g^{-1}(y_1,y_2)}{\partial y_1)} & \frac{\partial g^{-1}(y_1,y_2)}{\partial y_2)} \end{pmatrix} \right| . \tag{4.6}$$

Hence the bivariate change of variables formula is:

$$g(y) = f(x_1)\ f(x_2)\quad \left| \frac{df(x_1)}{dy_1} \frac{df(x_2)}{dy_2} \right| . \tag{4.7}$$

In Theorem 4.12, for independent random variables with p.d.f.'s f_1 and f_2, the Jacobian evaluates to 1 and we arrive at the same result. Donahue points out that the result can be used for products and quotients, as in Corollary 4.13 for quotients:

Corollary 4.13. *Subject to the monotonicity and differentiability conditions of Theorem 4.14,*

(1) *The distribution of the quotient of two random variables* X_1 *and* X_2 *is given by:*

$$g(y_1) = \int_\beta f_{X_1,X_2}(y_1 \times y_2, y_2)\,|y_2|\;dy_2$$

where $f_{X_1,X_2}(x_1, x_2)$ *is the joint p.d.f. of* X_1 *and* X_2*.*

(2) *The distribution of the quotient of two independent random variables* X_1 *and* X_2 *is given by:*

$$g(y) = \int_\beta f_1(y_1 \times y_2) f_2(y_2)\,|y_2|\;dy_2.$$

(3) *The distribution of the quotient of two independent identically distributed random variables* X_1 *and* X_2 *is given by:*

$$g(y) = \int_\beta f(y_1 \times y_2) f(y_2)\,|y_2|\;dy_2.$$

4.3.2 Change of variables

The results of the previous section lead directly to the familiar change of variables formula:

Theorem 4.14. *For strictly increasing or strictly decreasing differentiable transformation* φ *of a p.d.f.* $f(x)$*, the resultant p.d.f. is given by:*

$$g(y) = f(\varphi^{-1}(y))\,\left|\tfrac{d(\varphi^{-1}(y))}{dy}\right|. \tag{4.8}$$

Theorem 4.14 allows us to derive a new p.d.f. $g(y)$ from an initial p.d.f. $f(x)$ provided only that a strict monotonic condition (which is essential to ensure that inverses are well defined) applies to the transformation φ and that the inverse transformation function $\varphi^{-1}(y)$ is differentiable everywhere on β. In terms of $f(x) = \varphi^{-1}(y)$, provided $f(x)$ (which is y in (4.9)) is monotonic and its derivative exists over the domain of support then:

$$g(y) = f(x)\left|\frac{dx}{dy}\right|. \tag{4.9}$$

4.3.3 Mellin convolutions

We recognise in the equations of Corollary 4.13 the Mellin convolutions for quotients of random variables (immediately generalisable to products as well) and conclude that the monotonicity and differentiability conditions for the component functions must apply. It is not valid to presume that arbitrary functions supplied to a Mellin convolution will result in appropriate results unless the component functions are first inspected for monotonicity and differentiability.

4.3.4 Unary functions

We can successfully use the change-of-variables formula (4.9) to calculate functional transformations of some p.d.f.'s but we are left with the problem of unary functions which do not meet the monotonicity or differentiability criteria, this does not seem to have had much attention in the published literature apart from consideration by Donahue [15] whose approach is consistent with that of Theorem 4.15 whose proof is trivial:

Theorem 4.15. *If functions that are not strictly increasing or strictly decreasing are piecewise monotonic on n partitions of the total domain D then for each partition $D_j \subset D$:*

$$g_j(y) = f_j(x) \left| \frac{dx}{dy} \right|_{D_j} \qquad x \in \ D_j. \tag{4.10}$$

Thus each $f_j(x)$ makes a contribution $g_j(y)$ to the resultant p.d.f. $g(y)$ which must be assessed by summation of infinitesimal probabilities at each point of the total domain D. That is, the functions $f_j(x)$ derived by piecewise transformation of random variables are themselves independent random variables which must be combined by an appropriate linear combination technique such as the characteristic function method. This can be a daunting procedure unless we are able to invoke symmetry considerations as in Theorem 4.16:

Theorem 4.16. *The monotonicity requirement for change-of-variable transformations and Mellin convolution components can be relaxed to allow functions with precise repetitions over the same size sub domain whether the sub domain is taken as being in either a positive direction or a negative direction.*

Proof. For any function the shape of the curve represents variation of functional value over the domain and hence uniquely determines the density of occurrence of values over infinitesimal sub domains. If n copies of such functional portions of identical density are supported on n sub domains the density is the same as for a single portion. □

4.4 Elements of a random variable algebra

With the provisos of differentiability and monotonicity, the use of Mellin convolutions is very effective for calculating products and quotients of random variables especially when we include functions covered by Theorem 4.16. The Fourier convolution methods developed in [55] for calculation of linear combinations rapidly become unmanageable however for larger numbers of random variables, but Springer [66] (especially Theorem 3.2.2 and Equations 2.8.5) provides the basis of a more practical method for determining in principle the distributions of linear combinations of independent random variables.

4.4.1 Products and quotients of independent random variables

The Mellin convolution for products and quotients of functions is derived in [55] from the Fourier convolution as applied to sums and products and also from Donahue's [15] bivariate distribution theorem (see above: Theorems 4.12 and also Corollary 4.13); the derived expressions are (apart from nomenclature) the same as Springer's [66].

(1) Let w be the product of two differentiable and monotonic distribution functions $f_1(x)$ and $f_2(y)$ of non negative independent random variables x and y, then the distribution $g(w) = g(xy)$ is given by:

$$g(w) = \int_0^\infty \frac{1}{y} f_1\left(\frac{w}{y}\right) f_2(y)\, dy. \tag{4.11}$$

(2) Let w be the quotient of two differentiable and monotonic distribution functions $f_1(x)$ and $f_2(y)$ of non negative independent random variables x and y, then the distribution $h(w) = h\left(\frac{x}{y}\right)$ is given by:

$$h(w) = \int_0^\infty y f_1(wy) f_2(y)\, dy. \tag{4.12}$$

Both expressions (4.11) and (4.12) are subject to the constraints that the random variables be independent and non negative and that the functions f_1 and f_2 (either of which with interchange of arguments can be regarded as the transformation between domains) must be monotonic and have first derivatives over the domains of xy or $\frac{x}{y}$ as appropriate. We recall that Theorem 4.16 contains a conditional relaxation of the monotonicity requirement.

4.4.2 Linear combinations of independent random variables

The *characteristic function* $\phi(t)$ as defined in (4.13) encapsulates both distribution function $f(x)$ and the domain of support D in a single complex function, and is the Fourier integral of a (possibly bounded) p.d.f. $f(x)$ which yields an unbounded complex function which uniquely determines the p.d.f.:

$$\phi(f(x)) = \phi(t) = \int_D e^{itx}\, f(x)\, dx \qquad t, x \in \mathbb{R} \tag{4.13}$$

and the appropriate inverse Fourier integral restores the p.d.f.:

$$f(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{-itx}\, \phi(t)\, dt \qquad t, x \in \mathbb{R}. \tag{4.14}$$

Springer [66] (especially Theorem 3.2.2 and Equations 2.8.5) establishes the basis, and his Theorem 3.2.5 allows the generalisation:

$$\phi(f_1(k_1x_1) + f_2(k_2x_2) + \cdots) = (k_1k_2\cdots)\phi_1\phi_2\cdots \tag{4.15}$$

where the k_i are any real numbers and the $\phi_i = \phi(f_i(x_i))$ are characteristic functions corresponding to p.d.f.'s f_i of independent random variables x_i. Application of (4.13), (4.14) and (4.15) allows us to determine in principle the distributions of linear combinations of independent random variables. Such distributions will in general be polynomials defined piecewise over subdomains.

Definition 4.17. *The* ***absolute p.d.f.*** *of a linear combination of random variables is the polynomial representing the distribution of the sum of the same random variables.*

4.5 Linear combinations via characteristic functions

We will require the following definitions and theorem:

Definition 4.18. *The **components of a p.d.f.** $g(x)$ are the terms in powers of x that sum to the piecewise polynomial over each subdomain of $g(x)$.*

Definition 4.19. *The **pieces of a p.d.f.** $g(x)$ are the piecewise portions of $g(x)$ over the subdomains that sum to the domain of support for $g(x)$.*

Definition 4.20. *The sign function is:*

$$\mathrm{sign}(\omega) = \begin{cases} 1 & \omega > 0 \\ 0 & \omega = 0 \\ -1 & \omega < 0 \end{cases} \tag{4.16}$$

4.5.1 A closed form for the p.d.f. of a sum of independent random variables

We will require the Fourier transform of $\frac{1}{t^n}$.

Theorem 4.21. *The integral $I_n = \int_{-\infty}^{\infty} \frac{1}{t^n} e^{i\omega t} dt$ has a closed form expression for all n:*

$$I_n = \frac{i^n \omega^{n-1}}{(n-1)!} \pi \ \mathrm{sign}(\omega). \tag{4.17}$$

It is important to note that by writing $\frac{1}{t^n}$, we do not literally mean the function that is the reciprocal of the n^{th} power of t. Instead, what is meant is that "$\frac{1}{t^n}$ *is the homogeneous distribution defined by the distributional derivative* $\frac{(-1)^n}{(n-1)!} \frac{d^n}{dx^n} \log|x|$" —see Erdelyi [16], (Entry 310).

Proof. We refer to a table of Fourier transforms, e.g. [16], (Entry 310). □

Theorem 4.22. *The absolute distribution of a linear combination of n independent random variables $\sum_{j=1}^{n} a_j$ uniformly distributed over $[0, k]$ is a polynomial of degree $n-1$, is defined piecewise on n sub domains of $[0, nk]$, and is given by:*

$$g(x) = \frac{n(-1)^n}{2k^n} \sum_{j=0}^{n} \frac{(-1)^j}{j!(n-j)!} (jk - x)^{n-1} \ \mathrm{sign}(jk - x).$$

Proof. We consider the n non zero independent random variables $a_j \in_u [0, k],\ k \in \mathbb{R}$. For all integers $j \in [1, n]$ the distributions $f(a_j)$ identically uniform over $[0, k]$ are $f(a_j) = \frac{1}{k}$ and 0 elsewhere and the appropriate characteristic functions according to (4.13) are identical and of the form:

$$\phi(f(y)) = \phi_y(t) = \int_0^k \frac{1}{k} e^{ity} \, dy = \frac{1}{itk}(e^{itk} - 1) \tag{4.18}$$

and for the sum of n random variables with identical uniform distributions ϕ:

$$\prod_{j=1}^{n}\phi_j = \frac{1}{i^n t^n k^n}(e^{itk}-1)^n. \tag{4.19}$$

With binomial expansion this becomes:

$$\prod_{j=1}^{n}\phi_j = \frac{1}{i^n t^n k^n}\sum_{j=0}^{n}(-1)^{n-j}\frac{n!}{j!(n-j)!}e^{ijtk}. \tag{4.20}$$

This being the characteristic function of the sum of the n random variables $\in_u [0,k]$, we apply the inverse transformation according (4.14) to obtain the resultant distribution on the piecewise sub intervals of $[0,nk]$, that is, for:

$$x\in[0,k],\ x\in[k,2k]\ \cdots\ x\in[(r-1)k,rk]\ \cdots\ x\in[(n-1)k,nk]:$$

$$\begin{aligned} g(x) &= \tfrac{1}{2\pi}\int_{-\infty}^{\infty} e^{-itx}\ \prod_{j=1}^{n}\phi_j\ dt \\ &= \tfrac{1}{2i^nk^n\pi}\int_{-\infty}^{\infty}\tfrac{1}{t^n}e^{-itx}\ \sum_{j=0}^{n}(-1)^{n-j}\tfrac{n!}{j!(n-j)!}e^{ijtk}\ dt \\ &= \tfrac{(-1)^n n!}{2i^nk^n\pi}\ \sum_{j=0}^{n}\tfrac{(-1)^j}{j!(n-j)!}\int_{-\infty}^{\infty}\tfrac{1}{t^n}e^{i(jk-x)t}\ dt. \end{aligned} \tag{4.21}$$

Let $\omega = jk-x$ for $j\in\{0,1,\cdots,n\}$, then the equation becomes:

$$g(\omega) = \frac{n!(-1)^n}{2i^nk^n\pi}\ \sum_{j=0}^{n}\frac{(-1)^j}{j!(n-j)!}\int_{-\infty}^{\infty}\frac{1}{t^n}e^{i\omega t}\ dt \tag{4.22}$$

then:

$$g(\omega) = \frac{n!(-1)^n}{2i^nk^n\pi}\ \sum_{j=0}^{n}\frac{(-1)^j}{j!(n-j)!}I_n. \tag{4.23}$$

With $\omega = jk-x$, I_n is a function of x:

$$\begin{aligned} I_n &= \tfrac{i^n\omega^{n-1}}{(n-1)!}\pi\ \mathrm{sign}(\omega) \\ &= \tfrac{i^n\pi}{(n-1)!}\,(jk-x)^{n-1}\ \ \mathrm{sign}(jk-x) \end{aligned} \tag{4.24}$$

supported piecewise on the n subdomains of the absolute p.d.f. $g(x)$, these are the intervals:

$$[0,k),\cdots,[(m-1)k,mk),\cdots,[(n-1)k,nk)$$

where interval m is $[(m-1)k,mk)$. Then $\mathrm{sign}(jk-x)$ takes values as follows for $x\in m$:

Figure 4.1: Values of $\text{sign}(jk - x)$.

↓ **Interval**	$\mathbf{j=0}$	$\mathbf{j=1}$	$\mathbf{j=2}$	$\mathbf{j=3}$	$\mathbf{j=4}$
$m = 1: \quad x \in (0, k)$	-1	1	1	1	1
$m = 2: \quad x \in (k, 2k)$	-1	-1	1	1	1
$m = 3: \quad x \in (2k, 3k)$	-1	-1	-1	1	1
$m = 4: \quad x \in (3k, 4k)$	-1	-1	-1	-1	1
$m = 5: \quad x \in (4k, 5k)$	-1	-1	-1	-1	-1

$$\begin{array}{ll} \text{sign}(jk - x) = -1 & j < m \\ \text{sign}(jk - x) = +1 & j \geq m \end{array} \tag{4.25}$$

and we show in Figure 4.1 some early evaluations of $\text{sign}(jk - x)$. When the expression for I_n from (4.17) is substituted into (4.23), j becomes an index into the $n + 1$ integrals in the expression for $g(x)$, hence the expression $(jk - x)^{n-1}\,\text{sign}(jk - x)$ must be evaluated in terms of j and applied to each jth term for each sub domain m. From (4.23):

$$\begin{aligned} g(x) &= \tfrac{n!(-1)^n}{2i^n k^n \pi} \sum_{j=0}^{n} \tfrac{(-1)^j}{j!(n-j)!} I_n \\ &= \tfrac{n!(-1)^n}{2i^n k^n \pi} \sum_{j=0}^{n} \tfrac{(-1)^j}{j!(n-j)!} \tfrac{i^n \pi}{(n-1)!} (jk - x)^{n-1} \;\; \text{sign}(jk - x) \\ &= \tfrac{n(-1)^n}{2k^n} \sum_{j=0}^{n} \tfrac{(-1)^j}{j!(n-j)!} (jk - x)^{n-1} \;\; \text{sign}(jk - x). \end{aligned} \tag{4.26}$$

□

Example 4.23.

(1) *For* $n = 1$ *we arrive back at a uniform distribution over* $[0, k]$*, in the evaluated form of* (4.26) *there is only one subdomain:*

$$g(x) = -\frac{1}{2k}\left((-x)^0(-1) + (-1)(k - x)^0(1)\right) = -\frac{1}{2k}(-1 - 1) = \frac{1}{k}.$$

(2) *For* $n = 2$ *from* (4.26) *we have to consider both* $x \in [0, k)$ $(m = 1)$ *and* $x \in [k, 2k)$ $(m = 2)$ *where* $\text{sign}(jk - x)$ *is determined via* (4.25) *(or see Table 4.1):*

$$\begin{aligned} g(x)_{m=1} &= \tfrac{2}{2k^2}\left(\tfrac{1}{2}(-x)^1(-1) + (-1)(k - x)^1(1) + \tfrac{1}{2}(2k - x)^1(1)\right) \\ &= \tfrac{1}{k^2}\left(\tfrac{x}{2} - (k - x) + \tfrac{2k-x}{2}\right) \\ &= \tfrac{x}{k^2}, \end{aligned} \tag{4.27}$$

$$
\begin{aligned}
g(x)_{m=2} &= \tfrac{2}{2k^2}\left(\tfrac{1}{2}(-x)^1(-1)+(-1)(k-x)^1(-1)+\tfrac{1}{2}(2k-x)^1(1)\right)\\
&= \tfrac{1}{k^2}\left(\tfrac{x}{2}-+k-x)+\tfrac{2k-x}{2}\right) \qquad (4.28)\\
&= \tfrac{2k-x}{k^2}.
\end{aligned}
$$

Hence:

$$
g(x)=\begin{cases}\frac{x}{k^2} & x\in[0,k)\\[2ex] \frac{2k-x}{k^2} & x\in[k,2k]\end{cases} \qquad (4.29)
$$

which is the distribution $\mathfrak{D}_{x_1+x_2}$ where $x_1, x_2 \in_u [0,k]$ as derived via characteristic functions.

4.5.2 Probabilities for linear combinations

Theorem 4.24. *For a linear combination $g(x)$ of independent uniformly distributed random variables, the probability that a random variable x is in the subdomain m of $g(x)$ (that is, that x is in the interval $[(m-1)k, mk]$) is independent of the subdomain size and is given by:*

$$
\mathbb{P}_{x\in m}=\frac{(-1)^n}{2}\sum_{j=0}^{n}\frac{(-1)^j}{j!(n-j)!}\left[(j+1-m)^n\operatorname{sign}(j+1-m)-(j-m)^n\operatorname{sign}(j-m)\right].
$$

Proof. Integration of the expression (4.26) for the p.d.f. over $[(m-1)k, mk]$ gives the probability that x is in that particular subdomain:

$$
\int_{(m-1)k}^{mk} g(x)\,dx = -\tfrac{(-1)^n}{2k^n}\sum_{j=0}^{n}\tfrac{(-1)^j}{j!(n-j)!}\left[(jk-x)^n\ \operatorname{sign}(jk-x)\right]_{x=(m-1)k}^{mk}
$$

therefore

$$
\begin{aligned}
\mathbb{P}_{x\in m} &= -\tfrac{(-1)^n}{2k^n}\sum_{j=0}^{n}\tfrac{(-1)^j}{j!(n-j)!}k^n\left[(j-m)^n\ \operatorname{sign}(k(j-m))\right.\\
&\qquad\left. -\,k^n\left(j-(m-1)\right)^n\ \operatorname{sign}(k(j-(m-1)))\right]\\
&= \tfrac{(-1)^n}{2}\sum_{j=0}^{n}\tfrac{(-1)^j}{j!(n-j)!}\left[(j+1-m)^n\operatorname{sign}(j+1-m)-(j-m)^n\operatorname{sign}(j-m)\right].
\end{aligned} \qquad (4.30)
$$

□

4.6 Some distributions of trigonometric functions via the change of variables formula

We determine the distributions of some trigonometric functions via the change of variables formula. We are free to chose monotonic regions where the shape of the curve on its sub domain is representative of all such sub domains, again up to sign, and elsewhere in this thesis the term *monotonic* is taken to mean including the considerations of Theorem 4.16. In the case of trigonometric functions reference to Figure 4.2 shows that considerable simplification results by recognising the symmetries and phase shifts. Then the p.d.f.'s of the pairs $\{\sin(x), \cos(x)\}$, $\{\text{cosec(x)}, \text{sec(x)}\}$, $\{\tan(x), \cot(x)\}$, $\{\sin^2(x), \cos^2(x)\}$, $\{\text{cosec}^2\text{(x)}, \text{sec}^2\text{(x)}\}$ and $\{\tan^2(x), \cot^2(x)\}$ are by elementary calculation identical, see Figure 4.4.

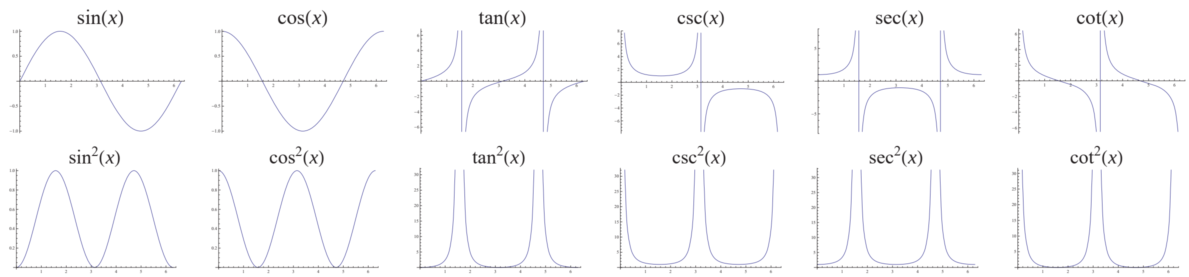


Figure 4.2: Polarity and phase of trigonometric functions.

Function set	**Distribution name, Representative: f(x)=y**	**Monotonic domain rep.**	**p.d.f.**	**range of y**
$\{\sin(x), \cos(x)\}$	$\mathfrak{D}_{\cos(x)}$	$[0, \pi)$	$\frac{1}{\pi\sqrt{1-y^2}}$	$(-1, 1)$
$\{\text{cosec(x)}, \text{sec(x)}\}$	$\mathfrak{D}_{\text{cosec(x)}}$	$(0, \frac{\pi}{2}], [\frac{\pi}{2}, \pi)$	$\frac{2}{\pi y\sqrt{y^2-1}}$	$(1, \infty)$
$\{\cot(x), \tan(x)\}$	$\mathfrak{D}_{\cot(x)}$	$(0, \pi]$	$\frac{1}{\pi(1+y^2)}$	$(-\infty, \infty)$
$\{\sin^2(x), \cos^2(x)\}$	$\mathfrak{D}_{\cos^2(x)}$	$(0, \pi), (\pi, 2\pi)$	$\frac{1}{\pi\sqrt{y(1-y)}}$	$(0, 1)$
$\{\text{cosec}^2\text{(x)}, \text{sec}^2\text{(x)}\}$	$\mathfrak{D}_{\text{cosec}^2\text{(x)}}$	$(0, \frac{\pi}{2}), (\frac{\pi}{2}, \pi)$	$\frac{1}{\pi y\sqrt{y-1}}$	$(1, \infty)$
$\{\cot^2(x), \tan^2(x)\}$	$\mathfrak{D}_{\cot^2(x)}$	$[0, \frac{\pi}{2}), (\frac{\pi}{2}, \pi]$	$\frac{1}{\pi(1+y)\sqrt{y}}$	$(0, \infty)$

Figure 4.3: Distributions of some trigonometric functions.

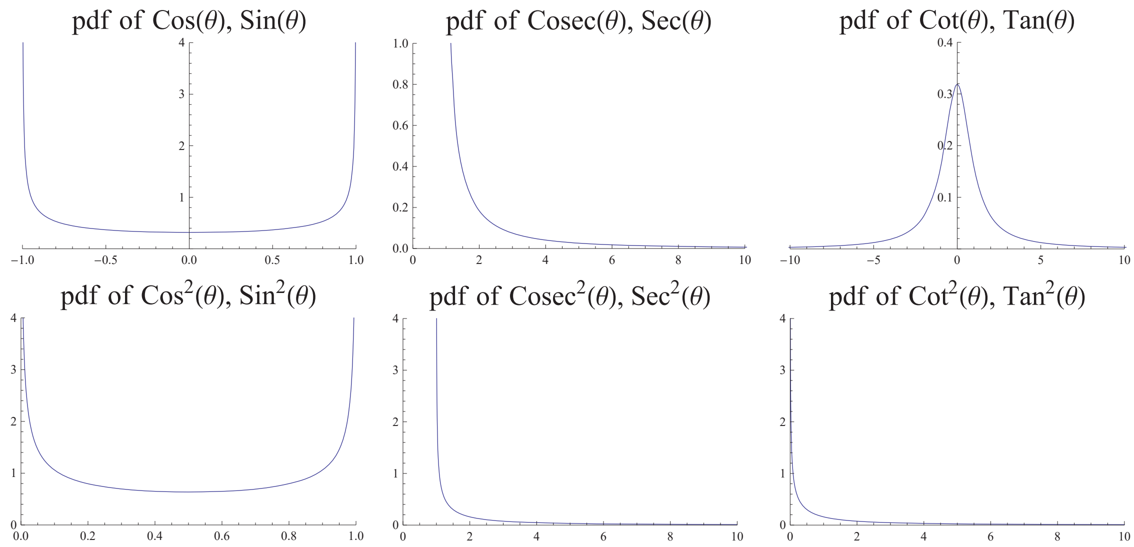


Figure 4.4

4.7 Some distributions via characteristic functions

We record some relevant results of calculation via the characteristic function method for some distributions $g(x) = \sum_{i=1}^{n} k_i x_i$ where $k_i \in \mathbb{N}$ for individual random variables $x_i \in_u [0, \pi]$, see Figures 4.5 and 4.6.

(1) $\mathfrak{D}_{(x_1+x_2)}, \quad \mathbb{P}_{g(x)>0} = 1$:

$$g(x) = \frac{1}{\pi^2} \begin{cases} x & 0 \leq x < \pi \\ \\ 2\pi - x & \pi \leq x \leq 2\pi. \end{cases} \tag{4.31}$$

(2) $\mathfrak{D}_{(x_1-x_2)}, \quad \mathbb{P}_{g(x)>0} = \frac{1}{2}$:

$$g(x) = \frac{1}{\pi^2} \begin{cases} \pi + x & -\pi \leq x < 0 \\ \\ \pi - x & 0 \leq x \leq \pi \end{cases} \tag{4.32}$$

(3) $\mathfrak{D}_{|x_1-x_2|}, \quad \mathbb{P}_{g(x)>0} = 1$:

$$g(x) = \frac{2(\pi - x)}{\pi^2}. \tag{4.33}$$

(4) $\mathfrak{D}_{(x_1-2\,x_2)}, \quad \mathbb{P}_{g(x)>0} = \frac{1}{4}$:

$$g(x) = \frac{1}{2\pi^2} \begin{cases} 2\pi + x & x \in [-2\pi, -\pi) \\ \\ \pi & x \in [-\pi, 0) \\ \\ \pi - x & x \in [0, \pi]. \end{cases} \tag{4.34}$$

(5) $\mathfrak{D}_{(2\,x_1-x_2)}, \quad \mathbb{P}_{g(x)>0} = \frac{3}{4}$:

$$g(x) = \frac{1}{2\pi^2} \begin{cases} \pi + x & x \in [-\pi, 0) \\ \\ \pi & x \in [0, \pi) \\ \\ 2\pi - x & x \in [\pi, 2\pi]. \end{cases} \tag{4.35}$$

Figure 4.5: Some distributions $\mathfrak{D}_x$ of linear combinations of independent random variables calculated via characteristic functions, $x_i \in_u [0, \pi]$ and the distribution function is $g(x) = \sum_{i=1}^{n} k_i x_i$ where $k_i \in \mathbb{N}$.

(6) $\mathfrak{D}_{(2\,x_1 - x_2 - x_3)}$, $\mathbb{P}_{g(x)>0} = \frac{1}{2}$:

$$g(x) = \frac{1}{4\pi^3} \begin{cases} x^2 + 4\pi x + 4\pi^2 & -2\pi \le x < -\pi \\ -x^2 + 2\pi^2 & -\pi \le x < \pi \\ x^2 - 4\pi x + 4\pi^2 & \pi \le x \le 2\pi. \end{cases} \tag{4.36}$$

(7) $\mathfrak{D}_{(x_1 - x_2 - x_3)}$, $\mathbb{P}_{g(x)>0} = \frac{1}{6}$:

$$g(x) = \frac{1}{2\pi^3} \begin{cases} x^2 + 4\pi x + 4\pi^2 & -2\pi \le x < -\pi \\ -2x^2 - 2\pi x + \pi^2 & -\pi \le x < 0 \\ x^2 - 2\pi x + \pi^2 & 0 \le x \le \pi. \end{cases} \tag{4.37}$$

Figure 4.6: Some further distributions of linear combinations of independent random variables calculated via characteristic functions, $x_i \in_u [0, \pi]$ and the distribution function is $g(x) = \sum_{i=1}^{n} k_i x_i$ where $k_i \in \mathbb{N}$.

Chapter 5

Computational determinations

Computation has been used to provide both prediction and confirmation of analytic determinations and also to give a clear view of results where the mathematics is too long and complicated or no clear mathematical methodology is yet apparent.

5.1 Algorithmic considerations

To generate matrices $A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$ representing random elements of $\mathcal{F}$ we take three random numbers from the virtual memory uniform random number database (see the main thesis introduction) and scale according to the desired domain. These random numbers become the arguments θ_a and θ_c in $[0, 2\pi)$ where $\mathbf{a} = |\mathbf{a}|\, e^{i\theta_a}$ and $\mathbf{c} = |\mathbf{c}|\, e^{i\theta_c}$, and the arc length 2α of the intersection of the isometric circles of A with $\mathbb{S}$ in $[0, \pi]$ where $\cos(\alpha) = r$ (the isometric circle radius as in Figure 3.1). Generation of the full complex matrix from these three real random numbers is accomplished via Theorem 3.1.

Our primary objective is to determine via Jørgensen's and Klein's Theorems some computational bounds for the probability that two-generator groups $\langle f, g\rangle$ of random elements of $f, g \in \mathcal{F}$ are discrete, accordingly we generate pairs of suitable matrices A, B and assess probabilities that the corresponding isometric circles are disjoint. Once we have a set of such matrices then calculation and the application of constraints allows the assessment of distributions for any matrix or matrix pair parameter. To obtain probabilities we simply count occurrences that meet specified constraints.

Noting that analytical results seem to yield isometric circle intersection probabilities expressable as simple vulgar fractions, it would be useful to be able to express computational results in terms of fractions rather than decimal numbers. Accordingly we have designed an algorithm to identify computational results with such fractions following an approach reminiscent of that of Sylvester [68] in converting vulgar fractions of the form $\frac{m}{n} \leq 1$ to sums of Egyptian fractions (indexed by i) of the form $\sum \frac{1}{a_i}$. Inspection of the results allows determination of the probable validity or otherwise of vulgar and Egyptian fraction identification in each case.

Figure 5.1: σ-field bit encoding for $\mathfrak{F}_4$.

5	4	3	2	1	0
$(\mathcal{A}^{-1} \cap \mathcal{B}^{-1})$	$(\mathcal{A}^{-1} \cap \mathcal{B})$	$(\mathcal{A} \cap \mathcal{B}^{-1})$	$(\mathcal{A} \cap \mathcal{B})$	$(\mathcal{B} \cap \mathcal{B}^{-1})$	$(\mathcal{A} \cap \mathcal{A}^{-1})$

For any matrix $A = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix} \in SL(2, \mathbb{C})$, according to (2.9) the Euclidean separation δ between the two isometric circles can be calculated from $|\text{trace(A)}| = |\mathbf{a} + \mathbf{d}|$ and the isometric circle radius $r_A = \frac{1}{|\mathbf{c}|}$:

$$\mathfrak{d} = \frac{|\mathbf{a} + \mathbf{d}| - 2}{|\mathbf{c}|} = r_A(|\text{trace(A)}| - 2). \tag{5.1}$$

For elements of $\mathcal{F}$ represented by matrices we can also compute from Theorem 3.1 the arc length separation between the isometric circles as:

$$\delta = |\eta - \eta'|_\circ - 2\, r_A. \tag{5.2}$$

Similar calculations allow all combinations of arc length separations between the isometric circles of two (or more) pairs of matrices A and B to be determined and incorporated into the disjointedness assessment algorithms for the isometric circles of elements of $\langle A, B \rangle$.

5.2 $\mathfrak{F}_4$ σ-field probabilities

For the four isometric circles of the matrices A, B, A^{-1}, B^{-1}, we consider the set S of all possible pairwise intersections of an isometric circle with another. Clearly:

$$S = \{(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{B} \cap \mathcal{B}^{-1}), (\mathcal{A} \cap \mathcal{B}), (\mathcal{A} \cap \mathcal{B}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B}), (\mathcal{A}^{-1} \cap \mathcal{B}^{-1})\}$$

and we can define a σ-field $\mathfrak{F}_4$ on S whose elements include all possible combinations of intersections of these elementary elements. We proceed to compute the disjointedness probabilities for all 64 elements of the field with a sample space of say $10,000,000$ pairs of matrices representing transformations in $\mathcal{F}$. The index into the σ-field is in accordance with the encoding in the 6$-$bit word (least significant bit last) incremented by 1 as indicated in Figure 5.1. The computed probabilities for elements of the σ-field for $1,000,000$ matrices representing transformations in $\mathcal{F}$ as expressed in terms of Egyptian fractions are shown in Figures 5.2 to 5.7.

5.2.1 Detailed analysis

We analyse the $\mathfrak{F}_4$ σ-field disjoint probabilities as presented in Figures 5.2 to 5.7. The computationally determined events are tabulated as follows: *Index* is a decimal representation of the 6-bit number incremented by 1 defined to index the elements of $\mathfrak{F}_4$, *Count* is the number of random events that meet specified intersection criteria for the particular experiment, *Fraction* is the unadjusted Egyptian fraction corresponding most closely to $\frac{Count}{1000000}$, *Adjust* is the

Figure 5.2: class $\mathcal{E}_1$ of $\mathcal{F}_4$: 1000000 pairs of matrices, 1 circle pair of 6 disjoint.

Index	Count	Pairs	Fraction	Adjust	Intersections
1	4999470	1	1/ 2	-1/ 18868	$(\mathcal{A} \cap \mathcal{A}^{-1})$
2	5002400	1	1/ 2	+1/ 4167	$(\mathcal{B} \cap \mathcal{B}^{-1})$
4	4997550	1	1/ 2	-1/ 4082	$(\mathcal{A} \cap \mathcal{B})$
8	5000169	1	1/ 2	+1/ 59172	$(\mathcal{A} \cap \mathcal{B}^{-1})$
16	4998850	1	1/ 2	-1/ 8696	$(\mathcal{A}^{-1} \cap \mathcal{B})$
32	4999870	1	1/ 2	-1/ 76923	$(\mathcal{A}^{-1} \cap \mathcal{B}^{-1)}$

Figure 5.3: class $\mathcal{E}_2$ of $\mathcal{F}_4$: 1000000 pairs of matrices, 2 circle pairs of 6 disjoint.

Index	Count	Pairs	Fraction	Adjust	Intersections
3	2502297	2	1/ 4	+1/ 4354	$(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{B} \cap \mathcal{B}^{-1})$
5	2914945	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{A} \cap \mathcal{B})$
6	2917363	2	1/ 3	-1/ 24	$(\mathcal{B} \cap \mathcal{B}^{-1}), (\mathcal{A} \cap \mathcal{B})$
9	2916726	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{A} \cap \mathcal{B}^{-1})$
10	2918071	2	1/ 3	-1/ 24	$(\mathcal{B} \cap \mathcal{B}^{-1}), (\mathcal{A} \cap \mathcal{B}^{-1})$
12	2915031	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{B}), (\mathcal{A} \cap \mathcal{B}^{-1})$
17	2915999	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B})$
18	2916956	2	1/ 3	-1/ 24	$(\mathcal{B} \cap \mathcal{B}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B})$
20	2915712	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{B}), (\mathcal{A}^{-1} \cap \mathcal{B})$
24	2917970	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{B}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B})$
33	2916920	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B}^{-1)}$
34	2919107	2	1/ 3	-1/ 24	$(\mathcal{B} \cap \mathcal{B}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B}^{-1)}$
36	2916979	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{B}), (\mathcal{A}^{-1} \cap \mathcal{B}^{-1)}$
40	2917891	2	1/ 3	-1/ 24	$(\mathcal{A} \cap \mathcal{B}^{-1}), (\mathcal{A}^{-1} \cap \mathcal{B}^{-1)}$
48	2915478	2	1/ 3	-1/ 24	$(\mathcal{A}^{-1} \cap \mathcal{B}), (\mathcal{A}^{-1} \cap \mathcal{B}^{-1)}$

Figure 5.4: class $\mathcal{E}_3$ of $\mathcal{F}_4$: 1000000 pairs of matrices, 3 circle pairs of 6 disjoint.

Index	Count	Pairs	Fraction	Adjust	Intersections
7	1667486	3	1/ 6	+1/ 12205	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B})$
11	1667972	3	1/ 6	+1/ 7661	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1})$
13	1872805	3	1/ 5	-1/ 79	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1})$
14	1563197	3	1/ 6	-1/ 97	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1})$
19	1667470	3	1/ 6	+1/ 12448	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
21	1561401	3	1/ 6	-1/ 95	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B})$
22	1874869	3	1/ 5	-1/ 80	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B})$
25	1876194	3	1/ 5	-1/ 81	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
26	1875468	3	1/ 5	-1/ 80	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
28	1874863	3	1/ 5	-1/ 80	$(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
35	1668740	3	1/ 6	+1/ 4823	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
37	1875005	3	1/ 5	-1/ 80	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
38	1876133	3	1/ 5	-1/ 81	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
41	1563412	3	1/ 6	-1/ 97	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
42	1876479	3	1/ 5	-1/ 81	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
44	1875237	3	1/ 5	-1/ 80	$(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
49	1873468	3	1/ 5	-1/ 79	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
50	1563073	3	1/ 6	-1/ 97	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
52	1874603	3	1/ 5	-1/ 80	$(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$
56	1876166	3	1/ 5	-1/ 81	$(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1})$

Figure 5.5: class $\mathcal{E}_4$ of $\mathcal{F}_4$: 1000000 pairs of matrices, 4 circle pairs of 6 disjoint.

Index	Count	Pairs	Fraction	Adjust	Intersections
15	1020886	4	1/ 10	+1/ 479	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1})$
23	1020733	4	1/ 10	+1/ 482	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B})$
27	1250825	4	1/ 8	+1/ 12121	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
29	1129524	4	1/ 9	+1/ 543	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
30	1130264	4	1/ 9	+1/ 522	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
39	1250968	4	1/ 8	+1/ 10331	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
43	1022281	4	1/ 10	+1/ 449	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
45	1129843	4	1/ 9	+1/ 534	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
46	1131016	4	1/ 9	+1/ 502	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
51	1021289	4	1/ 10	+1/ 470	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
53	1129217	4	1/ 9	+1/ 552	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
54	1130384	4	1/ 9	+1/ 519	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
57	1130691	4	1/ 9	+1/ 511	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
58	1130956	4	1/ 9	+1/ 504	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
60	1416854	4	1/ 7	-1/ 853	$(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$

Figure 5.6: class $\mathcal{E}_5$ of $\mathcal{F}_4$: 1000000 pairs of matrices, 5 circle pairs of 6 disjoint.

Index	Count	Pairs	Fraction	Adjust	Intersections
31	721950	5	1/ 14	+1/ 1305	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B})$
47	722634	5	1/ 14	+1/ 1198	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
55	722257	5	1/ 14	+1/ 1255	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
59	722884	5	1/ 14	+1/ 1163	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
61	812054	5	1/ 12	-1/ 470	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$
62	812755	5	1/ 12	-1/ 486	$(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$

Figure 5.7: class $\mathcal{E}_6$ of $\mathcal{F}_4$: 1000000 pairs of matrices, 6 circle pairs of 6 disjoint.

Index	Count	Pairs	Fraction	Adjust	Intersections
63	500000	6	1/ 20	$+1/\infty$	$(\mathcal{A}\cap\mathcal{A}^{-1}),(\mathcal{B}\cap\mathcal{B}^{-1}),(\mathcal{A}\cap\mathcal{B}),(\mathcal{A}\cap\mathcal{B}^{-1}),(\mathcal{A}^{-1}\cap\mathcal{B}),(\mathcal{A}^{-1}\cap\mathcal{B}^{-1)}$

signed adjustment fraction that is possibly used to convert results to vulgar fractions, *Intersections* specifies the actual disjoint event in terms of specific elementary events. To analyse the results sensibly, we check against the computed σ-field $\mathfrak{F}_6$ for the isometric circle intersections of three matrices representing transformations in $\mathcal{F}$, average the close-to-constant adjustment fraction denominators to a multiple of the first and then take first (probability) and second (adjustment) fractions to a common denominator to achieve a conjectured vulgar fractional result. The rationale for the reduction to vulgar fractions being the observed correlation with specific analytical results, we expect the wider experimental results to bear a close relationship to such fractions. There is of course some degree of subjectivity with the above process especially where denominators are close but not identical, but inspection of the tables in Figures 5.2 to 5.7 seems sufficient justification of the process. The tables also bring out the equivalence of elements of $\mathfrak{F}_4$ under topological intersection, this observation suggests Definition 5.1:

Definition 5.1. *The equivalence classes of a σ-field $\mathfrak{F}_n$ are the sets of elements of the field with identical isometric circle intersection topology.*

We apply this definition to specific cases, Figure 5.8 illustrates this diagramatically and includes conjectured probabilities for the equivalence classes of $\mathfrak{F}_4$. It is a nice statistical fluke that as reported in Figure 5.7 for this particular experiment, precisely $500,000$ of $1,000,000$ pairs of matrices of all six isometric circles are disjoint.

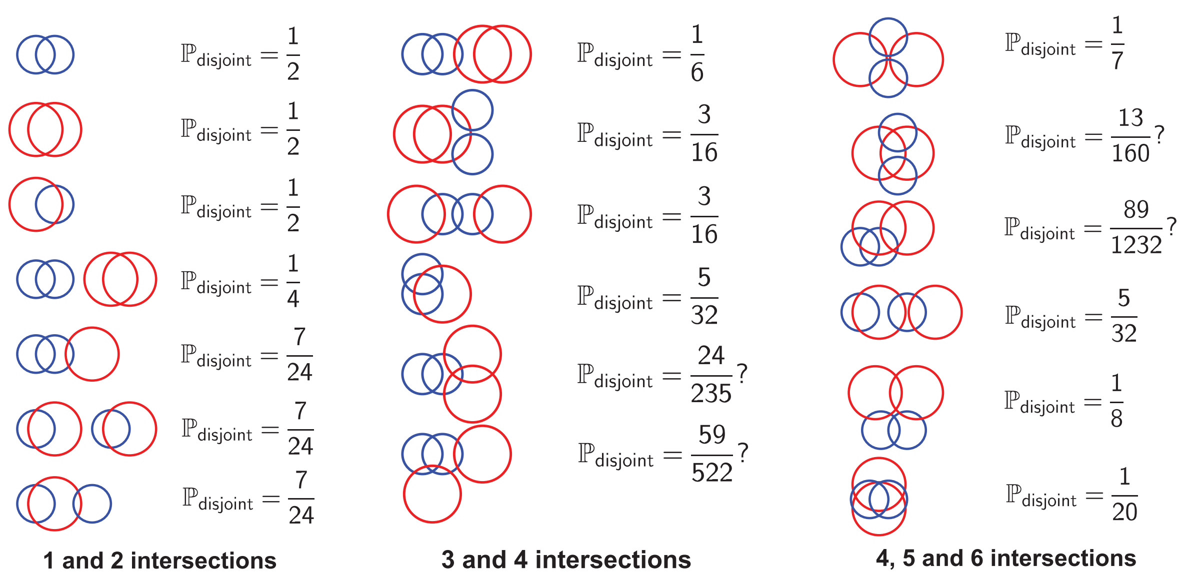


Figure 5.8: Diagrammatic representation showing computational results for all possible intersection topologies (represented by a blue pair for the isometric circles of A and a red pair for the isometric circles of B) for the σ-field $\mathfrak{F}_4$, the geometric topologies are disjoint with probability $\mathbb{P}_{disjoint}$ as indicated. The modifier "?" denotes a conjectured vulgar fraction close to the actual computed probability, uncertain because of greater magnitude adjustments.

Figure 5.8 tabulates intersection probabilities for the four isometric circles of two matrices; analytically determined values of $\mathfrak{F}_4$ elements provide the following correlations:

(1) Intersections involving pairs of isometric circles ($(\mathcal{A} \cap \mathcal{A}^{-1})$ etc) indices $1, 2, 4, 8, 16$ and 32: $\mathbb{P}_{disjoint} = \frac{1}{2}$.

(2) The sole independent double intersection ($(\mathcal{A} \cap \mathcal{A}^{-1}), (\mathcal{B} \cap \mathcal{B}^{-1})$, index 3), $\mathbb{P}_{disjoint} = \frac{1}{4}$.

(3) The mutual intersection probability $\mathbb{P}_{\mathcal{A},\mathcal{B}_{disjoint}} = \frac{1}{20}$.

Chapter 6

Limit sets of Möbius transformations

We begin a limited examination via iterated function systems of the statistics of the dimension of the limit set, a near proxy at least for the Hausdorff dimension.

6.1 Random Fuchsian groups

The fixed points of a random $f \in \mathcal{F}$ represented by a matrix $A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$ are solutions to the same quadratic equation (3.40) and one should therefore expect some correlation. We have chosen the isometric circle intersection arc $2\alpha = \arg(\mathbf{c})$ to be uniformly distributed and so the argument of either fixed point, say $\mathbf{z}_+$, is uniformly distributed. The arc length 2η between these points according to Theorem 3.53 is distributed according to:

$$Y(\eta) = \frac{4}{\pi^2}\ \tanh(\eta)\ \log\frac{\cosh(\eta)+1}{\cosh(\eta)-1}. \tag{6.1}$$

Since $\mathbb{P}_{|\Re e(a)|\leq 1} = \frac{1}{2}$, elliptic and hyperbolic elements occur with equal probability and we calculate the derivative in the case of hyperbolic elements $f \in \mathcal{F}$:

$$\begin{aligned} f(\mathbf{z}) &= \frac{\mathbf{az}+\overline{\mathbf{c}}}{\mathbf{cz}+\overline{\mathbf{a}}} \\ \text{therefore} \\ f'(\mathbf{z}) &= \mathbf{a}(\mathbf{cz}+\overline{\mathbf{a}})^{-1} - (\mathbf{az}+\overline{\mathbf{c}})(\mathbf{cz}+\overline{\mathbf{a}})^{-2}\mathbf{c} = \frac{1}{(\mathbf{cz}+\overline{\mathbf{a}})^2}. \end{aligned} \tag{6.2}$$

Substituting from(3.40):

$$\begin{aligned} |f'(\mathbf{z}_\pm)| &= \frac{1}{|\overline{\mathbf{c}\mathbf{z}}_\pm + \overline{\mathbf{a}}|^2} = \frac{1}{\left|i\Im m(\mathbf{a}) \pm \sqrt{\Re e(\mathbf{a})^2-1}+\overline{\mathbf{a}}\right|^2} \\ &= \frac{1}{\left|\Re e(\mathbf{a}) \pm \sqrt{\Re e(\mathbf{a})^2-1}\right|^2}. \end{aligned} \tag{6.3}$$

Hence $|f'(\mathbf{z}_+)| < 1$ and $\mathbf{z}_+$ is an *attracting* fixed point, with $\mathbf{z}_-$ being *repelling*. Note that $|f'(\mathbf{z}_+)|\,|f'(\mathbf{z}_-)| = 1$. The number $m_f = |f'(\mathbf{z}_+)| \in (0,1)$ is called the *multiplier* of f.

Lemma 6.1. *The multiplier of a hyperbolic Möbius transformation is a conjugacy invariant.*

Proof. By this we mean that if h is a Möbius transformation and f hyperbolic, then $g = h \circ f \circ h^{-1}$ is hyperbolic and has $m_g = m_f$. To see this note that g has fixed points $h(\mathbf{z}_\pm)$ and further that $g^n = h \circ f^n \circ h^{-1}$, so that $h(\mathbf{z}_+)$ is the attracting fixed point. Then:

$$\begin{aligned} m_g = |g'(h(\mathbf{z}_+)| &= \left|h'(f(h^{-1}(h(\mathbf{z}_+)))\right| \left|f'(h^{-1}(h(\mathbf{z}_+)))\right| \left|(h^{-1})'(h(\mathbf{z}_+))\right| \\ &= |h'(\mathbf{z}_+)| \, |f'(\mathbf{z}_+)| \left|(h^{-1})'(h(\mathbf{z}_+))\right| = m_f. \end{aligned}$$

□

The fixed points of $f \in \mathcal{F}$ are on $\mathbb{S}$, so to compute the multiplier we can arrange by conjugacy that the fixed points are ± 1 and that the axis of f (the hyperbolic line joining the fixed points) is the interval $(-1, 1) \subset \mathbb{R}$. This becomes apparent when we consider the situation in Figure 3.4 where vectors $\mathbf{a}$ and $\mathbf{c}$ rotate away from each other to become parallel, then both isometric circles come down to the real axis and $t = \frac{|\mathbf{c}|}{|\mathbf{a}|} = \sqrt{1 - \frac{1}{|\mathbf{a}|^2}}$. Then f represented by the matrix $A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$ has the form $f(\mathbf{z}) = \dfrac{\mathbf{z} + t}{1 + t\mathbf{z}}$ for $t \in [0, 1)$. We have:

$$f'(\mathbf{z}) = \frac{1}{1 + t\mathbf{z}} - \frac{\mathbf{z} + t}{(1 + t\mathbf{z})^2} t = \frac{1 + t\mathbf{z} - t(\mathbf{z} + t)}{(1 + t\mathbf{z})^2} = \frac{1 - t^2}{(1 + t\mathbf{z})^2}$$

hence the multiplier:

$$m_f = |f'(1)| = \frac{1 - t}{1 + t}.$$

We recall that the translation length of a transformation is by definition:

$$\tau(f) = \min_{z \in \mathbb{D}} \rho_{\mathbb{D}}(z, f(z))$$

and $\rho_{\mathbb{D}}$ is the hyperbolic metric of the disc. Noting that $f(0) = t$ the transformation f takes the point $(0, 0)$ to $(0, t)$ and that in the unit disc model of hyperbolic space the distance between these points is $\rho_{\mathbb{D}} = \log\left(\frac{1+t}{1-t}\right)$ we have the following theorem:

Theorem 6.2. *Let $f \in \mathcal{F}$ be a hyperbolic transformation. Then $m_f = e^{-\tau}$, where $\tau = \tau(f)$ is the translation length of f.*

Lemma 6.3. *Let $f \in \mathcal{F}$ be a hyperbolic Möbius transformation. Then the multiplier of the transformation is:*

$$m_f = 1 \Big/ \left[1 + 2(\Re e(\mathbf{a})^2 - 1)\left(1 + \sqrt{1 + \tfrac{1}{\Re e(\mathbf{a})^2 - 1}}\right)\right] \qquad \text{for f} \in \mathcal{F}. \tag{6.4}$$

Proof. Since $\cosh^{-1}(x) = \log(x + \sqrt{x^2 - 1})$ and from (3.52) we have $\tau = \cosh^{-1}(1 + \frac{\beta}{2})$, then for $f \in \mathcal{F}$:

$$\begin{aligned} 1 + \tfrac{\beta}{2} + \sqrt{(1 + \tfrac{\beta}{2})^2 - 1} &= 1 + \tfrac{\beta}{2} + \sqrt{1 + \tfrac{\beta^2}{4} + \beta - 1} = 1 + \tfrac{\beta}{2}\left(1 + \sqrt{1 + \tfrac{4}{\beta}}\right) \\ &= 1 + 2(\Re e(\mathbf{a})^2 - 1)\left(1 + \sqrt{1 + \tfrac{1}{\Re e(\mathbf{a})^2 - 1}}\right) \end{aligned} \tag{6.5}$$

hence:

$$\tau \quad = \log\left(1 + 2(\Re e(\mathbf{a})^2 - 1)\left(1 + \sqrt{1 + \tfrac{1}{\Re e(\mathbf{a})^2 - 1}}\right)\right) \qquad \text{for f} \in \mathcal{F} \tag{6.6}$$

and the result follows.

□

We have the p.d.f of the translation length for randomly selected hyperbolic $f \in \mathcal{F}$ from equation 3.53, the change of variables formula now allows us to calculate the distribution of the multiplier.

Theorem 6.4. *For randomly selected hyperbolic $f \in \mathcal{F}$ the p.d.f. for the multiplier M_f is:*

$$M_f(m) = \frac{4}{\pi^2 m}\,\frac{1-m}{1+m}\,\log\left(\frac{1+\sqrt{m}}{1-\sqrt{m}}\right), \quad m \in [0,1]. \tag{6.7}$$

Proof. Re-writing 3.53 in exponential form, we have:

$$\begin{aligned} H[\tau] &= -\frac{4}{\pi^2}\frac{e^{\tau}-1}{e^{\tau}+1}\log\frac{e^{\tau/2}-1}{e^{\tau/2}+1} \\ &= -\frac{4}{\pi^2}\frac{1-e^{-\tau}}{1+e^{-\tau}}\log\frac{1-\sqrt{e^{-\tau}}}{1+\sqrt{e^{-\tau}}} \\ &= \frac{4}{\pi^2}\frac{1-m}{1+m}\log\left(\frac{1+\sqrt{m}}{1-\sqrt{m}}\right) \end{aligned} \tag{6.8}$$

and the result follows since $m = e^{-\tau}$ implies $\log(m) = -\tau$ so $\left|\frac{d\tau}{dm}\right| = \frac{1}{m}$. □

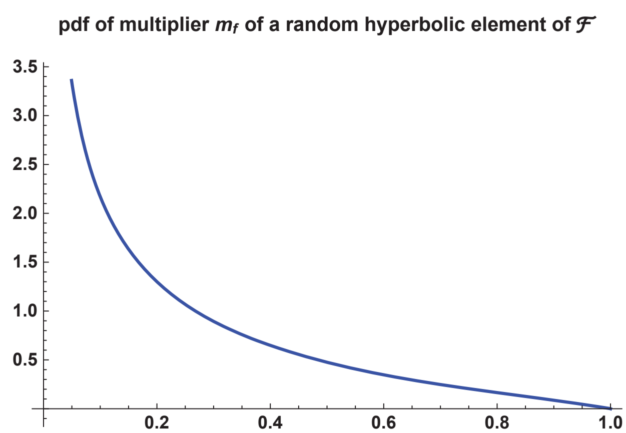


Figure 6.1: The p.d.f. for the multiplier m_f of a random hyperbolic element of $\mathcal{F}$.

We calculate that the expected value of the multiplier is $1 - \frac{8}{\pi^2} \approx 0.1894$.

Lemma 6.5. *We can relate the multiplier m and translation length τ to the geometry of the isometric circle by noting that $\frac{1}{t} = \frac{1}{\sqrt{1-1/|\mathbf{a}|^2}} = \sqrt{1+r^2}$ which is the radius R of the circle on which the isometric circles are centred. Then:*

(1) $\frac{1}{t} = R = \sqrt{r^2+1}$.

(2) $m = \frac{R-1}{R+1} = \frac{\sqrt{r^2+1}-1}{\sqrt{r^2+1}+1} = \frac{(\sqrt{r^2+1}-1)^2}{r^2}$.

(3) $\sqrt{m} = \frac{\sqrt{r^2+1}-1}{r}, \quad \frac{1}{\sqrt{m}} = \frac{r}{\sqrt{r^2+1}-1}$.

(4) $\tau = \log\frac{R+1}{R-1} = \log\left(\frac{\sqrt{r^2+1}+1}{\sqrt{r^2+1}-1}\right)$.

(5) $\frac{1-m}{1+m} = \frac{1}{R} = \frac{1}{\sqrt{r^2+1}} = t$.

(6) $\frac{1+\sqrt{m}}{1-\sqrt{m}} = r + R = r + \sqrt{r^2+1}$.

(7) $M(m) = \frac{4(R+1)}{\pi^2 R(R-1)}\log(R+r)$.

Corollary 6.6. *The multiplier of $r \in \mathcal{F}$ represented by the matrix $A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$ is:*

$$m_f = \frac{|\mathbf{a}| - |\mathbf{c}|}{|\mathbf{a}| + |\mathbf{c}|}$$

and again clearly $m_f < 1$ for isometric circle radii greater than zero and the fixed point $\mathbf{z}_+$ of f is attracting.

6.2 Iterated function systems

Hutchinson [32] showed that every IFS has a unique nonempty compact (closed and bounded) invariant set Λ. In our setting we will consider the group $\Gamma = \langle f, g\rangle$ generated by two random hyperbolic elements f and g and the IFS generated by $\{f, g, f^{-1}, g^{-1}\}$ on a subset $\Omega \subset \mathbb{S}$. For the Fuchsian group Γ this invariant set Λ is called the limit set, denoted $\Lambda(\Gamma)$ and a little theory quickly reveals that the limit set is the closure of the fixed point sets of the hyperbolic elements of Γ, unless Γ has an abelian subgroup of finite index. This latter case occurs with probability 0 if f and g are randomly chosen.

As we have noted, a key invariant of a Fuchsian group is the Hausdorff dimension of its limit set. If Γ is generated by randomly chosen hyperbolic elements of $\mathcal{F}$ and we wish to discuss the statistics of the Hausdorff dimension, we have a number of issues to consider, some of them quite intractable. These are:

(1) Γ is a group acting on $\mathbb{S}$ and so cannot be uniformly contracting.

(2) We want to consider only those Γ which are discrete (otherwise $\Lambda(\Gamma) = \mathbb{S}$).

(3) As far as we are aware the Hausdorff dimension of the limit set of any particular Fuchsian group is unknown, unless that dimension happens to be 1. Thus we must find a *computable* proxy for the Hausdorff dimension.

With respect to the first two questions we will restrict our attention to the case where f and g have disjoint isometric circles which we now discuss.

6.2.1 Isometric circles

The *isometric circles* of a hyperbolic Möbius transformation in $\mathcal{F}$ represented by the matrix $A = \begin{pmatrix} \mathbf{a} & \overline{\mathbf{c}} \\ \mathbf{c} & \overline{\mathbf{a}} \end{pmatrix}$ with $|\mathbf{a}|^2 - |\mathbf{c}|^2 = 1$ are:

$$C_{\pm} = \{\mathbf{z} : |\mathbf{cz} \pm \mathbf{a}| = 1\} = \{\mathbf{z} : |f'(\mathbf{z})| = 1\}.$$

The isometric discs are the finite regions bounded by the isometric circles. We recall lemma 3.7 which supports our claim that the p.d.f. on $\mathcal{F}$ is natural. Let us denote the arcs formed by the intersection of the isometric discs with the circle by $\alpha_{\pm}(f)$. Notice that:

$$f(\mathbb{S} \setminus \alpha_-) = \overline{\alpha_+}, \quad \text{and} \quad f^{-1}(\mathbb{S} \setminus \alpha_+) = \overline{\alpha_-}.$$

Thus if f and g are hyperbolic Möbius transformations then $\alpha_+(f) \cap \alpha_-(f) = \varnothing$ and if further $\alpha_{\pm}(f) \cap \alpha_{\pm}(g) = \varnothing$, then an elementary argument using the Klein combination theorem shows that $\langle f, g \rangle$ is discrete. Thus:

$$\Omega = \amalg_{h \in \{f,g\}} \alpha_{\pm}(h).$$

Then Ω consists of four intervals on $\mathbb{S}$ and each element of the function system $\{f, g, f^{-1}, g^{-1}\}$ will map three of these intervals inside another as a contraction:

$$\begin{aligned} f &: \Omega \setminus \alpha_-(f) \hookrightarrow \alpha_+(f), & f^{-1} &: \Omega \setminus \alpha_+(f) \hookrightarrow \alpha_-(f), \\ g &: \Omega \setminus \alpha_-(g) \hookrightarrow \alpha_+(g), & g^{-1} &: \Omega \setminus \alpha_+(g) \hookrightarrow \alpha_-(g). \end{aligned} \tag{6.9}$$

Thus the set $\overline{\Omega}$ and the functions $\{f, g, f^{-1}, g^{-1}\}$ are "similar" to an iterated function system.

6.2.2 Similarity dimension

If $f \backslash \Omega$ and $g \backslash \Omega$ were similarities we could have defined the similarity dimension of the invariant limit set following Moran [52] who shows that the similarity dimension would equal the Hausdorff dimension given the "open set condition". Our restriction to the case of Fuchsian groups with disjoint isometric circles will give us this open set condition. We would therefore like to explore the notion of similarity dimension.

For an IFS with contraction ratios λ_i for the i^{th} element of the generating set, the similarity dimension is defined to be the unique number d such that

$$\lambda_1^d + \lambda_2^d + \cdots \lambda_N^d = 1 \tag{6.10}$$

The number 1 on the right-hand side reflects the fact the dimension calculation is in Euclidean space.

A Fuchsian group Γ acts almost transitively on its limit set $\Lambda(\Gamma)$ in the following sense. If $f \in \Gamma$, then the set of fixed points of elements of Γ with the same multiplier m_f as that of f is dense in $\Lambda(\Gamma)$. To see this note that if $\mathbf{z}_+$ is the attracting fixed point of f, then

$\overline{\{h(\mathbf{z}_+) : h \in \Gamma\}}$ is closed and invariant under Γ. Since $\mathbf{z}_+ \in \Lambda(\Gamma)$, elementary considerations show that $\overline{\{h(\mathbf{z}_+) : h \in \Gamma\}} = \Lambda(\Gamma)$ as the limit set is the smallest closed invariant set. Then note that $h(\mathbf{z}_+)$ is the fixed point of $h \circ f \circ h^{-1}$ and $m_{h\circ f \circ h^{-1}} = m_f$. Thus the local scaling properties of the limit set are influenced by the elements with the largest multiplier. Next, we know that if the isometric discs are disjoint but $\mathbb{S}$ is contained in $\overline{\Omega}$ then $\Lambda(\Gamma) = \mathbb{S}$ and the dimension is therefore equal to 1. This suggests we adjust the right-hand side of (6.10) to accommodate this fact, together with the fact that the derivative of no element of the generating set is constant on *any* interval.

6.3 A calibration group

At this point we focus on an example. Choose isometric circle radius $r > 0$ and generators f_r, g_r with the respective matrix representations:

$$A = \begin{pmatrix} \sqrt{1+\frac{1}{r^2}} & \frac{1}{r} \\ \frac{1}{r} & \sqrt{1+\frac{1}{r^2}} \end{pmatrix}, \quad B = \begin{pmatrix} \sqrt{1+\frac{1}{r^2}} & \frac{i}{r} \\ \frac{-i}{r} & \sqrt{1+\frac{1}{r^2}} \end{pmatrix} \tag{6.11}$$

then:

$$\alpha_\pm(f_r) = \mathbb{D}(\pm\sqrt{1+r^2}, r), \qquad \alpha_\pm(g_r) = \mathbb{D}(\pm i\sqrt{1+r^2}, r).$$
$$\text{fix}(f) = \pm 1, \qquad \text{fix}(g) = \pm i.$$

We then have disjoint isometric circles if $r \leq 1$ and $\overline{\alpha_\pm(f) \cup \alpha_\pm(g)} = \mathbb{S}$ if and only if $r = 1$. We set $\Gamma_r = \langle f_r, g_r \rangle$ and $\Lambda_r = \Lambda(\Gamma_r)$. For the group Γ_r the isometric circles vary as illustrated in Figure 6.2.

We observe that the Hausdorff dimension $H_{\text{dim}}(\Lambda_r) = 1$ if $r = 1$ and $H_{\text{dim}}(\Lambda_r) \to 0$ as $r \to 0$. We calculate the multipliers to be

$$m_{f_r} = m_{g_r} = \frac{(\sqrt{r^2+1} - 1)^2}{r^2}.$$

This gives:

$$\frac{1}{r} = \frac{1}{2}\Big[\frac{1}{\sqrt{m}} - \sqrt{m}\Big] = \sinh(\tau/2) \tag{6.12}$$

Thus the condition $r = 1$ implies $\sinh(\tau_f/2) = \sinh(\tau_g/2) = 1$. In the calculation of dimension we have the two multipliers having the same value in (6.10) which suggests that we look at the dimension of Γ_r as having the form $\lambda^d = \gamma$ for some constant γ. We replace the multiplier λ by γ/r^2, as an average derivative. We find then that:

$$\Big[\frac{\gamma}{r^2}\Big]^d = \gamma.$$

We have $d = 1$ when $r = 1$. Experiment reveals that $\gamma = 2^{\#\text{generators}}$ to capture the rate of growth of the group. We then define the number d so that :

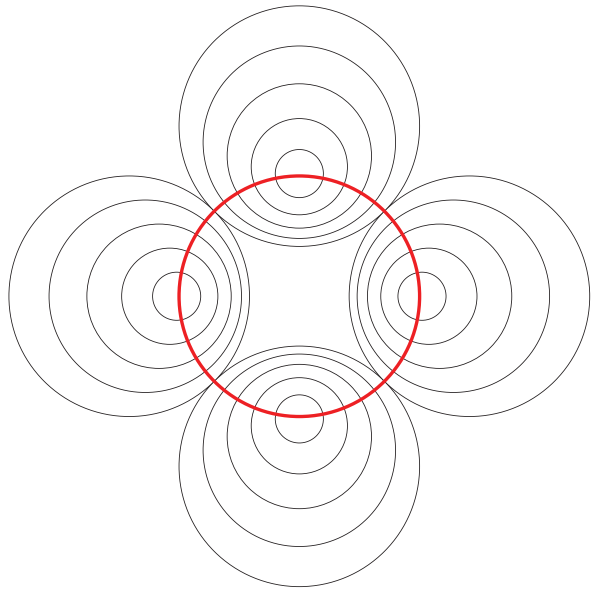


Figure 6.2: Calibration group Γ_r.

$$\Big[4\sinh(\tau_f/2)\sinh(\tau_g/2)\Big]^d = 4. \tag{6.13}$$

Equivalently:

$$\left[\frac{4}{r^2}\right]^d = 4, \quad \text{or} \quad \left[\frac{16\sqrt{m_f m_g}}{(1-m_f)(1-m_g)}\right]^d = 4.$$

We are going to call the number d defined in (6.13) a "dimension" but as it stands this dimension depends on the choice of generators f and g and will be different for another choice, say f and fg. This dimension is a function of a single parameter for the group Γ_r, for instance the translation length of the transformation or the isometric circle radius r. However, the generating pairs are all Nielson equivalent as our group is isomorphic to the free group on two generators. Our set up implies that the generators we have chosen have largest multipliers. This dimension is a conjugacy invariant, it depends on the two generators of smallest translation length, however we will show that this is a reasonable proxy for Hausdorff dimension.

For the group Γ_r we can calculate the distribution of the dimension d. In terms of the matrix A above we have $A_{1,1} = \sqrt{1+\frac{1}{r^2}}$ and for a random group we have $|A_{1,1}| = \frac{1}{\sin(\alpha)}$ with α uniformly distributed in $[0,\pi/2]$. Although $r = \tan(\alpha)$ (since $\sqrt{1+\frac{1}{r^2}} = \frac{1}{\sin(\alpha)}$), we require $r \leq 1$ so $\alpha \in_u [0,\pi/4]$ and we have:

$$\left[\frac{4}{\tan^2(\alpha)}\right]^d = 4, \quad d = \frac{\log 4}{\log 4/\tan^2(\alpha)} = \frac{\log 2}{\log(2\cot(\alpha))}$$

The p.d.f. for $\tan(\alpha)$ is $\frac{1}{\pi(1+y^2)}$. We use the change of variables formula via the function $t \mapsto \frac{\log 2}{\log 2/t}$ whose inverse is $s \mapsto 2^{1-\frac{1}{s}}$. Thus the p.d.f. of the "dimension" is:

$$D(d) = \frac{2^{\frac{1}{d}+3}\log(2)}{\pi\left(4^{1/d}+4\right)d^2} \tag{6.14}$$

which is plotted in Figure 6.3.

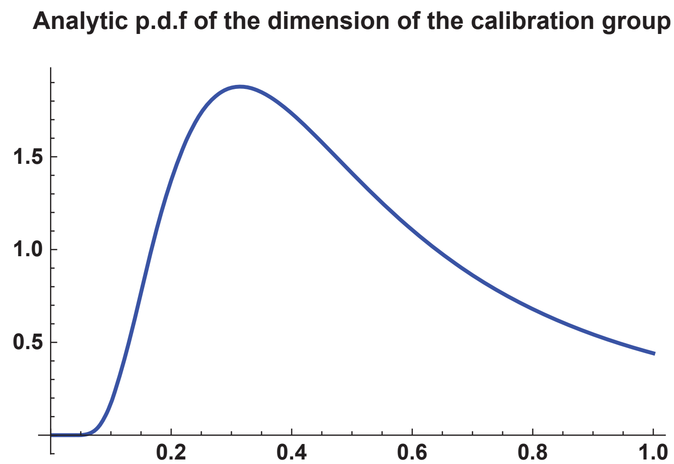


Figure 6.3: Analytically determined p.d.f of dimension for Γ_r from (6.14).

6.4 Covering set computational determinations

Our motivation is to be able to assess the validity of the dimensional analyses of the previous section by more traditional computational methods. Mainieri [40] establishes that the Hausdorff and box counting dimensions agree for fractal sets generated by rapidly convergent functions. Kleinian and Fuchsian groups are by definition discrete and totally disconnected and their limit sets are necessarily fractal and bounded by the disjoint isometric circles of the generators. Accordingly we assess Hausdorff dimension via a box counting process for two groups, the calibration group Γ_r and the single generator subgroup $\mathcal{F}_1 \subset \mathcal{F}$.

6.4.1 Algorithms

The constraints for computation are bit length of numbers, accessable storage capacity and processing speed, and these three factors have influenced the original algorithm design created by the author for this project. The two-pass algorithm using a modified "breadth first" technique (as defined in [53]) allows generation of the IFS data points sufficient to enable dimensional calculations for two-generator groups in $SL(2,\mathbb{C})$ up to 16 generations with resolution up to 10^{-15}. Generation 1 consists of the four fixed points in $\hat{\mathbb{C}}$ under action of the matrices induced by the group generators f and g, generation 2 is the set of points determined by $\{(g, g^{-1}\circ fix^+(f), fix^-(f)), (f, f^{-1}\circ fix^+(g), fix^-(g))\}$ of order 8 while subsequent generations j are determined by operations in each case on the three reduced sentences based on points in generation $j-1$.

6.4.2 Some results

The requirement for rapid convergence being verified computationally, we have calculated estimates for the Hausdorff dimension of the limit sets of the groups Γ_r and $\mathcal{F}_1$ for $0 < r \leq 1$ using the algorithm discussed above. The results are plotted in Figure 6.4 against isometric circle radius r for a sequence of choices of r together with a plot of our "dimension" defined using (6.13). Data points for the simpler calibration group Γ_r required less computation time to build than those for $\mathcal{F}_1$; despite this the (Γ_r) data point $(0.95, 0.895694)$ (green) took three weeks to build while the $\mathcal{F}_1$ data point $(0.015, 0.14332)$ (red) took only a few seconds. For very low values of r erratic results occur as the compiler runs into accuracy problems.

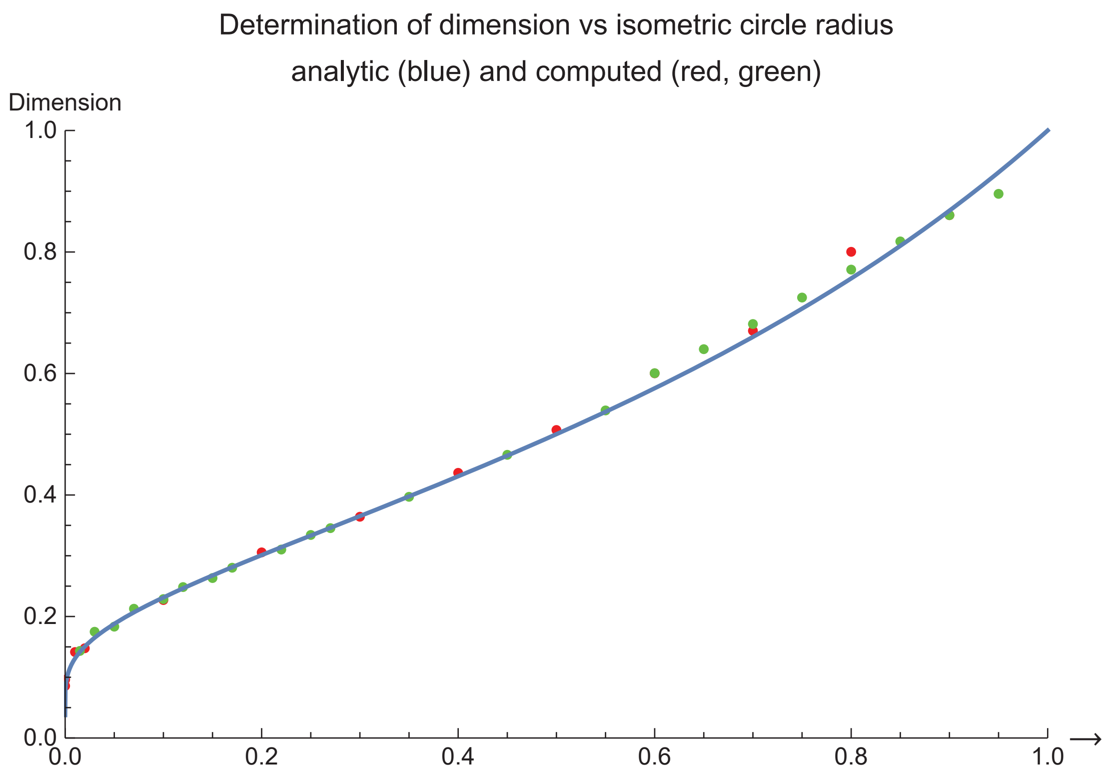


Figure 6.4: Dimension of the limit sets of Γ_r (red points) and of $\mathcal{F}_1$ (green points) together with a curve (blue) for d from (6.13).

Inspection of Figure 6.4 shows that for both the calibration group Γ_r and the Fuchsian group $\mathcal{F}_1$ we seem to have reasonable alignment of computation results with the analytical "dimension" $d = \frac{\log(4)}{\log(4/r^2)}$ derived from (6.13).

Bibliography

[1] J. W. Anderson and A. C. Rocha, *Analyticity of Hausdorff dimension of limit sets of Kleinian groups*, Annales Academiæ Scientiarum Fennicæ Mathematica, **22**, 349-364, 1997.

[2] G. E. Andrews, R. Askey and R. Roy, *Special functions*, Cambridge University Press, Cambridge, 2000.

[3] G. I. Barenblatt, *Scaling, self-similarity, and intermediate asymptotics*, Cambridge University Press, Cambridge, 1996.

[4] M. F. Barnsley and S. Demko, *Iterated function systems and the global construction of fractals*, Proc. R. Soc. Lond. **A399**, 243–275, 1985.

[5] A. F. Beardon, *The Geometry of discrete groups*, Springer-Verlag, Berlin and New York 1983.

[6] A F. Beardon, *A primer on Riemann Surfaces*, Cambridge University Press, Cambridge, 1984.

[7] A F. Beardon, *Continued Fractions, Discrete Groups and Complex Dynamics*, Computational Methods and Function Theory, **1 No. 2**, 535–594, 2001.

[8] D. M. Bradley and R. C. Gupta, *On the distribution of the sum of n non-identically distributed uniform random variables*, Annals of the Institute of Statistical Mathematics, **54 no. 3**, pp. 689–700, 2002.

[9] P. W. Bridgman, *Dimensional analysis*, Yale University Press, New Haven, CT 1931.

[10] J. A. Cookson, *P.L. Chebyshev and Chebyshev polynomials*, Montana State University, Department of Mathematical Sciences, Statistical writing project, 2007.

[11] P. de la Harpe, *Topics in geometric group theory*, The University of Chicago Press, Chicago, 2000.

[12] C. P. Dettman and O. Georgiou, *Product of n independent uniform random variables*, Statistics and Probability Letters **79, 24**, 2009.

[13] DI Management Services, Sydney, Australia, *Cryptosys API* `http://www.cryptosys.net/`, di-mgt.com.au.

[14] R. Diestel, *Graph theory*, Springer-Verlag Berlin, 2015.

[15] J. D. Donahue, *Products and quotients of random variables and their applications*, Office of Aerospace Research, United States Air Force, Denver, Colarado, 1964.

[16] A. Erdelyi, *Tables of integral transforms 1*, McGraw–Hill, New York, 1954.

[17] K. Falconer, *The geometry of fractal sets*, Cambridge University Press, Cambridge, 1985.

[18] K. Falconer, *Fractal geometry, mathematical foundations and applications*, John Wiley and Sons Ltd, Hoboken, NJ, 2014.

[19] FIPS PUB, *Security requirements for cryptographic modules*, Federal Information Processing Standards Publication **140–2**, 2001.

[20] L. R. Ford, *Automorphic Functions*, McGraw-Hill, 1929; (2nd ed., Chelsea, 1951).

[21] F. W. Gehring and G. J. Martin, *Inequalities for Möbius transformations and discrete groups*, J. Reine Angew. Math. **418**, 31–76, 1991.

[22] F. W. Gehring and G. J. Martin, *Chebyshev polynomials and discrete groups*, Proceedings of the Conference on Complex Analysis (Taijin, 1992), 114–125, Conf. Proc. Lecture Notes Anal., Int. Press, Cambridge, MA, 1994.

[23] F. W. Gehring and G. J. Martin, *Commutators, collars and the geometry of Möbius groups*, Jounal D'Analyse Mathematique, **63**, 1994.

[24] J. Gilman, *Recent developments in Nielson theory and discrete groups*, Contemporary Mathematics Series, 152, AMS 159–176, 1993.

[25] J. Gilman, *A discreteness condition for subgroups of PSL(2,*$\mathbb{C}$), Proceedings of the Bers Colloquium, Contemporary Math Series, **211**, AMS 261–267, 1997.

[26] W. M. Goldman, *Projective structures with Fuchsian holonomy*, Journal of differential geometry, **25**, 297–326, 1987.

[27] P. Herber, *JSD (Jackson structured design) stencil, template and add-on*, `http://www.paulherber.co.uk/visio-jsd/`, August 2016.

[28] A. D. Herbert and H. N. Nagaraja, *Order statistics*, John Wiley and Sons Ltd, Hoboken, NJ, 2003.

[29] M. Hohenwarter, *Geogebra: The graphing calculator for functions, geometry, algebra, calculus ...*, MSc thesis, University of Salzburg, 2002, followed by a PhD thesis and subsequent development, `http://www.geogebra.org`.

[30] R. D. Horowitz, *Characters of free groups represented in the two-dimensional special linear group*, Communications on Pure and Applied Mathematics, **25**, 635–649, 1972.

[31] J. C. R. Hunt, *Lewis Fry Richardson and his contributions to mathematics, meteorology, and models of conflict*, Annu. Rev. Fluid Mech. **30**, 13–36, 1968.

[32] J. E. Hutchinson, *Fractals and self similarity*, Indiana Univ. Math. J., **30**, 713–747, 1981.

[33] J. E. Hutchinson and L. Ruschendorf, *Selfsimilar fractals and selfsimilar random fractals*, Australian National University, 1991.

[34] M. A. Jackson, *Principles of program design*, Academic Press, Orlando 1975.

[35] S. Jaroszewicz and M. Korzen, *Arithmetic operations on independent random variables: a numerical approach*, SIAM J. Sci. Comput., **34, no. 3**, A1241–A1265, 2012.

[36] T. Jørgensen, *On discrete groups of Mobius transformations*, American Journal of Mathematics, **98 No. 3**, 739–749, 1973.

[37] T. Jørgensen and P. Klein, *Algebraic convergence of finitely generated Kleinian groups*, Quart. J. Math. Oxford (2), **33**, 325–332, 1982.

[38] S. Katok, *Fuchsian groups*, University of Chicago Press, 1992.

[39] A. N. Kolmogorov, *Foundations of the theory of probability*, (Translated, 2ed), Chelsea Publishing Co, 1956.

[40] R. Mainieri, *On the equality of Hausdorff and box counting dimensions*, American Institute of Physics, Chaos **Apr,3(2)**, 119–125, 1993.

[41] B. B. Mandelbrot, *How long is the coastline of Britain? Statistical self-similarity and fractional dimension*, Science, **156**, 636–638, 1967.

[42] B. B. Mandelbrot, *The fractal geometry of nature*, W. H. Freeman and Company, 1983.

[43] B. B. Mandelbrot, *The Mandelbrot set and beyond*, Springer, New York, 2004.

[44] B. B. Mandelbrot and M. Frame, *Some reasons for the effectiveness of fractals in Mathematics Education*, Mathematical Association of America, 2002.

[45] B. Maskit, *Kleinian groups*, Springer-Verlag, New York, 1988.

[46] G. J. Martin, *The geometry and arithmetic of Kleinian groups*, arXiv:1311.2636v1, **163**, (2013).

[47] G. Martin and G. O'Brien, *Random Kleinian Groups,* **I** *: Random Fuchsian Groups*, arXiv:1712.03602v1, (2017).

[48] G. Martin, G. O'Brien and Y. Yamashita, *Random Kleinian Groups,* **II** *: Two parabolic generators*, arXiv:1801.01167v1, (2018).

[49] J. C. Mason and D. C. Handscomb, *Chebyshev polynomials*, Chapman and Hall, London, 2003.

[50] W. S. Massey, *A basic course in algebraic topology*, Springer-Verlag, New York, 1991.

[51] D. Milios, *Probability distributions as program variables*, MSc thesis University of Edinburgh, 2009.

[52] M. Moran, *Hausdorff measure of infinitely generated self-similar sets*, Monatshefte für Mathematik, **122**, 387–399, 1996.

[53] D. Mumford, C. Series and D. Wright, *Indra's pearls, the vision of Felix Klein*, Cambridge University Press, Cambridge, 2002.

[54] NIST, *Recommendation for random number generation using deterministic random bit generators*, National Institute of Standards and Technology, SP 800–90, 2010.

[55] G. K. O'Brien, *Random discrete groups in the space of Möbius transformations*, MSc thesis, Massey University, 2012.

[56] A. Papoulis and S. U. Pillai, *Probability, random variables and stochastic processes*, McGraw Hill, 4ed 2002.

[57] G. Perelman, *The entropy formula for the Ricci flow and its geometric applications*, Cornell University Library, `arXiv:math/0211159v1[math.DG]`, 2002.

[58] T. Pignataro and D. Sullivan, *Ground state and lowest eigenvalue of the Laplacian for non-compact hyperbolic surfaces*, Communications in mathematical physics, Springer-Verlag, New York, 1986.

[59] B. Riemann, *On the hypotheses which lie at the basis of geometry*, (Translation of Riemann's 1854 Göttingen inaugural lecture by William Kingdon Clifford), Nature,**8. Nos. 183, 184**, 14–17, 36–37, 1854.

[60] T. J. Riven, *The Chebyshev polynomials from approximation theory to algebra and number theory*, John Wiley and Sons, Hoboken, NJ, 1974.

[61] H. Sagen, *Space-filling curves*, Springer-Verlag, New York, 1994.

[62] M. Schlichenmaier, *An introduction to Riemann surfaces, algebraic curves and moduli spaces*, Springer-Verlag, New York, 2007.

[63] M. A. Snyder, *Chebyshev methods in numerical approximation*, Prentice Hall, Upper Saddle River, NJ, 1966.

[64] M. R. Spiegel, *Laplace transforms* (Schaum's Outline Series), McGraw-Hill, New York, 1965.

[65] G. Springer, *Introduction to Riemann surfaces*, Chelsea Publishing Company, New York, 1957.

[66] M. D. Springer, *The algebra of random variables*, John Wiley and Sons, Hoboken, NJ, 1979.

[67] M. D. Springer and W. E. Thompson, *The distribution of products of independent random variables*, J. SIAM Appl. Math. **14 No. 3**, May 1966.

[68] J. J. Sylvester, *Mathematical papers III*, **47,** (1880), Chelsea Publishing Co, New York, 1973.

[69] W. P. Thurston, *The geometry and topology of three-manifolds*, Princeton University, Lecture notes, 1980.

[70] W. P. Thurston, *Three-dimensional geometry and topology*, Princeton University, Lecture notes, 1997.

[71] C. R. Traina, *Trace polynomial for two generator subgroups of $SL(2, C)$*, Proceedings of the American Mathematical Society, **79.3**, 369-372, 1980.

[72] E. W. Weisstein, *Hypersphere*, From MathWorld—A Wolfram Web Resource `http://mathworld.wolfram.com/Self-similarity.html`, 2017.

[73] E. W. Weisstein, *Self-Similarity*, From MathWorld—A Wolfram Web Resource `http://mathworld.wolfram.com/Self-Similarity.html`, 2016.

[74] R. C. Williamson, *Probabilistic arithmetic*, PhD Thesis, University of Queensland, 1989.

[75] R. C. Williamson and T. Downs, *The inverse and determinant of a 2×2 uniformly distributed random matrix,* Statistics and Probability Letters, **7**, 167–170, 1989.

[76] Wikimedia Foundation, The, *Fractal*, `https://en.wikipedia.org/wiki/Fractal`, Inc, 2016.

[77] Wikimedia Foundation, The, *Fractal Dimension*, `https://en.wikipedia.org/wiki/Fractal_dimension`, Inc, 2016.