Communications to SIMAI Congress,
ISSN 1827-9015, Vol. 3 (2009) 313 (12pp)
DOI: 10.1685/CSC09313

Fractal Riemann surfaces: chaotic scenarios and applications

Walter Arrighetti[1,2]

[1] *"Sapienza" Università di Roma, Department of Electronic Engineering, via Eudossiana 18, 00184 Rome,* Italy
riemann.chaos@gmail.com

[2] Technicolor *Creative Services, Digital Services for film and post-production, via Tiburtina 1138, 00156 Rome,* Italy

Abstract

Fractal Riemann surfaces are generated as iterators of branched covers (complex multi-valued functions). They feature self-similar geometries, an interesting Iterated Monodromy Group (IMG) driving their topologies, and an easy way to get their symbolic dynamics browsed. On the contrary, convergence issues, numerical accuracy and the onset of chaotic dynamics are present in the direct, homotopy problem of computing paths on them. Theoretical results of analysis and synthesis will be given, with a final look to possible applications in Computer Science (signing and private-key cryptography) and Physics (scattering in fractal resonators).

Keywords: `Fractal Riemann surface, Riemann surface, branched cover, branch point, sheet, self-similarity, fractal dimension, surface genus, homotopy group, monodromy group, IMG, iterated monodromy group, symbolic dynamics, pre-fractal, IFS`

1. Algebraic Toplogy

Let $P \in \left(\mathbb{C}^d[z] \backslash \mathbb{C}^{d-1}[z]\right)/\mathbb{C}$ for some $d \in \mathbb{N}\backslash\{1\}$ (i.e. P be a complex-coefficients, monic, d^{th}-degree polynomial) with $1 \leq j \leq r$ distinct roots' vector $\mathbf{z} \equiv (z_1, z_2, ..., z_r) \in \mathbb{C}^r$ of multiplicities' vector $\mathbf{m} \equiv (m_1, m_2, ..., m_r)$ (and $m_1+m_2+...+m_r=d$). Consider Riemann surface $\mathcal{A}_1$ defined by the implicit equation [1]

$$w^p - P(z) = 0. \tag{1}$$

$\mathcal{A}_1$ is equivalent a covering space of $\tilde{\mathbb{C}}$ via map $f^{-1}: \mathcal{A}_1 \longrightarrow \tilde{\mathbb{C}}$, where

$$w = f(z) \equiv \sqrt[p]{P(z)}, \tag{2}$$

Received 15/02/2009, in final form 25/06/2009
Published 31/07/2009

is the explicit, multivalued equation defining the same Riemann surface. Polynomial P can be written in factorized form in a compact notation too, where $\mathbf{1}_n :\equiv (1,1,...,1)\in\mathbb{N}^n$ as:

$$P(z)=\prod_{j=1}^{r}(z-z_j)^{m_j} :\equiv (z\mathbf{1}_r-\mathbf{z})^{\mathbf{m}}. \tag{3}$$

In a similar fashion let the r-tuplets $\boldsymbol{\mu},\boldsymbol{\pi}\in\mathbb{N}^r$, $\frac{\boldsymbol{\mu}}{\boldsymbol{\pi}}:\equiv\left(\frac{\mu_1}{\pi_1},\frac{\mu_2}{\pi_2},...,\frac{\mu_r}{\pi_r}\right)\in\mathbb{Q}^r$ and $\pi_\infty\in\mathbb{N}$ such that $(1\leq j\leq r)$:

$$\left.\begin{aligned} m_j &= \mu_j \mathrm{GCD}(m_j,p)\\ p &= \pi_j \mathrm{GCD}(m_j,p)\\ d &= \pi_\infty \mathrm{GCD}(d,p)\end{aligned}\right\} \implies \begin{cases}\frac{\mathbf{m}}{p}=\frac{\boldsymbol{\mu}}{\boldsymbol{\pi}}\\ \mathrm{GCD}(\mu_j,\pi_j)=1\end{cases} \tag{4}$$

Then (3) may be compactly rewritten as:

$$w=f(z)=(z\mathbf{1}_r-\mathbf{z})^{\frac{\boldsymbol{\mu}}{\boldsymbol{\pi}}}. \tag{5}$$

Next paragraph is dedicated to the algebraic-geometric properties of multivalued function f, whereas next Chapter is devoted to studying the n^{th} iteration $f^n(z)=(f\circ f\circ ...\circ f)(z)$.

1.1. *First iteration*

Equation $w=f(z)$ globally defines a Remann surface with $\mathrm{LCM}\boldsymbol{\pi}$ sheets, where $\mathrm{LCM}\boldsymbol{\pi}\leq p$ and equality holding iff $m_1,m_2,...,m_r|p$, so we may assume that is the case (otherwise such an f could be simplified). All the roots of P such that $\pi_j>1$ are branch points of multiplicity π_j-1 (as well as ∞, of multiplicity $\pi_\infty-1$); let $B\subset\tilde{\mathbb{C}}$ be this set of branch points.

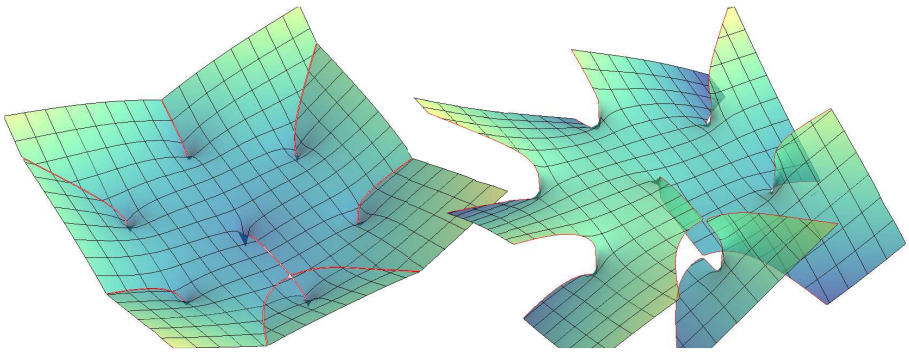

Fig. 1. Real and Imaginary parts of $\sqrt[5]{z\,(z^6-1)}$, with branch cuts in red.

DOI: 10.1685/CSC09313

Considering f^{-1} as a *branched* p-covering [2] of $\mathcal{A}_0{:=}\tilde{\mathbb{C}}\backslash B$ allows to compute the topology of $\mathcal{A}_0$: any closed path $\gamma{\subset}\mathcal{A}_0$ winding clockwise around the j^{th} branch point $k_j{\in}\mathbb{Z}$ times, jumps 'up' by $k_j m_j \mathrm{mod} p$ sheets, so there is a 1-cycles' homomorphism

$$\begin{array}{ccccc} \mathrm{Z}_1(\mathcal{A}_0) & \longrightarrow & \mathrm{Z}_1(\mathcal{A}_1) & \longrightarrow & \mathrm{H}_1(\mathcal{A}_1) \\ \updownarrow & & \updownarrow & & \updownarrow \\ \mathbb{Z}^r & \longrightarrow & \mathbb{Z}_p^r & \longrightarrow & \frac{\boldsymbol{\mu}}{\boldsymbol{\pi}}\mathbb{Z}_{\boldsymbol{\pi}} \end{array} := \textstyle\bigoplus_{j=1}^{r} \frac{\mu_j}{\pi_j}\mathbb{Z}_{\pi_j}, \tag{6}$$

a homology class of loops (1-cycles) in $\mathcal{A}_0$ being thus represented by a mod$p$ multi-index $[\mathbf{k}]{\in}\mathbb{Z}_p^r$, whereas its generalized genus is, cfr. (12):

$$\kappa_1 = |\boldsymbol{\pi}| + \pi_\infty - 2p - r + 1, \tag{7}$$

and if κ_1 is even, then $g_1{=}\frac{\kappa_1}{2}$ and $\mathcal{A}_1$ is homeomorphic to a g_1-handled torus $\mathbb{T}_{g_1}$. This is also consistent with the well-known *hyperellipticity* condition [2] (i.e. $p=2$ and P with simple roots only), in fact in that case

$$g_1 = \left\lceil \frac{d}{2} \right\rceil - 1. \tag{8}$$

1.2. *Monodromy groups*

Let $c{:}C{\longrightarrow}X$ be a finite covering of path-connected and locally path-connected topological space X and let γ_x be a loop based in $x{\in}X$; its lift $c \uparrow \gamma_x$ is a path on C ending in a different point from $c^{-1}(x)$. This fibres' permutation $\digamma_x$ is the (right) monodromy action [2] of $\pi_1(X,x)$ on $\mathrm{sym}\, c^{-1}(x)$; the *monodromy group* of x is the subgroup

$$\mathrm{MG}_x X \stackrel{\text{def}}{=} \digamma_x\left(\pi_1(X,x)\right) \cong \frac{\pi_1(X,x)}{c_*\pi_1(X,x)} \leq \mathrm{sym}\, c^{-1}(x). \tag{9}$$

Since on $\mathcal{A}_1$ all the branch points are present on every sheet its monodromy group does not depend of the chosen point, the surface's fundamental group $\mathbb{Z}_p^r$ acts as a permutation of the p sheets (with $\mathrm{sym}\mathbb{Z}_p = \mathbb{S}_p$) and the monodromy action $\digamma_s \in \mathrm{Hom}(\mathbb{S}_p, \mathbb{Z}_p^r)$ only depends on the sheet number $s \in \mathbb{Z}_p$ where the loop γ of winding vector $[\mathbf{k}]$ starts from:

$$\digamma_s[\gamma] = (s + [\mathbf{k}]\cdot\mathbf{m}) \,\mathrm{mod} p. \tag{10}$$

Let $f(z){=}(z-z_6)\sqrt[6]{(z-z_1)(z-z_2)^2(z-z_3)^3(z-z_4)^4(z-z_5)^5(z-z_7)^7}$ as an example. $p{=}6$, $r{=}7$, and $\mathbf{m}{=}(1,2,3,4,5,6,7)$; then $\boldsymbol{\mu}{=}(1,1,1,2,5,1,7)$ and $\boldsymbol{\pi}{=}(6,3,2,3,6,1,6)$ (with $\mathrm{LCM}\boldsymbol{\pi}{=}p{=}6$).

Consider a loop $[\mathbf{k}]$ with $\mathbf{k}{=}(-1,2,1,0,1,k_6,0)$ $\forall k_6{\in}\mathbb{Z}$ starting from 3^{rd} sheet. Whether its winding order around the branch points is

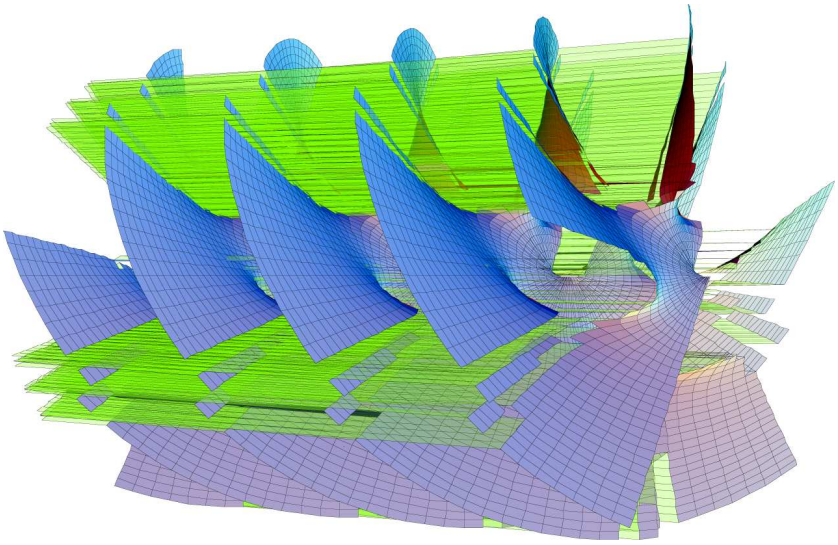

Fig. 2. Higher iteration of the imaginary part in Fig.1; branch-cuts are shown as transparent planes linking different-generation sheets.

$\curvearrowright z_1 \curvearrowleft z_2 \curvearrowleft z_2 \curvearrowleft z_3 \curvearrowleft z_5$ or $\curvearrowleft z_2 \curvearrowleft z_5 \curvearrowleft z_3 \curvearrowright z_1 \curvearrowleft z_2$, the visited sheets' sequence is $3 \rightsquigarrow 2 \rightsquigarrow 4 \rightsquigarrow 6 \rightsquigarrow 3 \rightsquigarrow 2$ or $3 \rightsquigarrow 5 \rightsquigarrow 4 \rightsquigarrow 1 \rightsquigarrow 6 \rightsquigarrow 2$, respectively, always ending on the 2^{nd} one, according to (10).

2. Higher iterations

Consider multivalued equation $w{=}f^n(z)$, defining the Riemann surface $\mathcal{A}_n$, $\forall n{\in}\mathbb{N}$; now formally letting $w_0{=}z$, $w_n{=}w$ and $w_k{=}f^k(z)$ for $1{\leq}k{<}n$ it is clear that $w_{k+1}{=}f(w_k)$, so f^{-1} is a branched p-covering $\mathcal{A}_{n+1}{\longrightarrow}\mathcal{A}_n$; this time branching happens with respect to variable w_{k+1} which depends from multivalued w_k: every sheet of $\mathcal{A}_n$ (which is called an n^{th}-*generation sheet*) ramifies to p sheets of $\mathcal{A}_{n+1}$ which, by induction on n, has p^{n+1} sheets. The n^{th}-*generation branch points* for the n^{th}-generation sheets are clearly for $f(w_k){\in}\{0,\infty\}$, with the same considerations of §2.1, but lower-generation branch points are present also, linking lower-generation sheets with each other. To find these branch points on the original Riemann surface one goes by induction: for example, consider the partial branched self-covering $\mathcal{A}_2 \xrightarrow{f^{-1}} \mathcal{A}_1 \xrightarrow{f^{-1}} \mathcal{A}_0$:

$$w_2 = f(f(z)) = f(w_1) = \sqrt[p]{\prod_{i=1}^{r} \left[\sqrt[p]{\prod_{j=1}^{r} (z - z_j)^{m_j} - z_i} \right]^{m_i}} \quad . \tag{11}$$

DOI: 10.1685/CSC09313

The 1st-generation branch points are $z \in B$, whereas 2nd-generation branch points are all the p determinations of w_1 being in B (i.e. the ramification points of $\mathcal{A}_1$ are the 2nd-generation branch points of $\mathcal{A}_2$). It may happen, though, that $f^n(z)=0$ has some solutions in common with $f^k(z)=0$ $(k<n)$ so there are n^{th}-generation branch points linking also lower-generation sheets with each other. This phenomenon, which will be called *cascading*, does not disrupt the self-similar branching of the surface, as it will happen between every sheets whose generations are multiple of n and k, respectively: a symmetry gets broken, but is restored later at higher orders. Also note that cascading trivially happens for every n if P is a homogeneous polynomial.

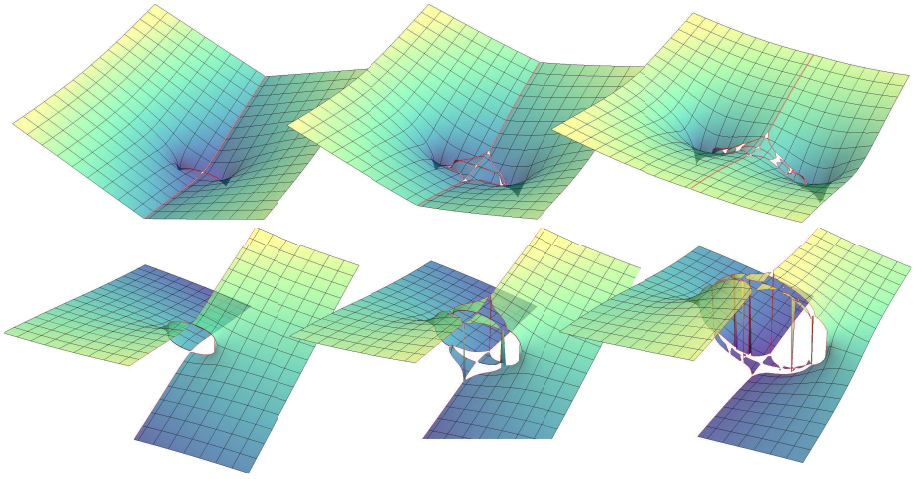

Fig. 3. Real (top) and Imaginary (bottom) parts of $f^n(z)$, for $f(z) = \sqrt[3]{z\left(z-\frac{1}{2}\right)}$ and (left to right) $n = 1, 2, 3$.

The topology of $\mathcal{A}_n$ is recovered by applying the Riemann-Hurwitz formula to the branched self-covering: the surface is homeomorphic to the connected sum of κ_n real projective planes and, if κ_n is even an $g_n = \frac{\kappa_n}{2}$, it is $\mathbb{T}_{g_n}$ — a sphere with g_n handles:

$$\kappa_n = \frac{p^n - 1}{p - 1}\left(|\boldsymbol{\pi}| + \pi_\infty - 2p - r + 1\right). \tag{12}$$

2.1. *The iterated monodromy group*

Let $(\mathcal{O}_n)_{n\in\mathbb{N}}$ be a self-cover of a topological space (or orbifold) $\mathcal{O}$, where $c{:}\mathcal{O}_1 \longrightarrow \mathcal{O}$ is the partial self-covering. Let $\curlywedge_x^n$ be the monodromy action of $c^n{:}\mathcal{O}_n \longrightarrow \mathcal{O}$ in $x \in \mathcal{O}$, then the *Iterated Monodromy Group* (or IMG) of $\mathcal{O}$ is

(cfr. [3] and [4]):

$$\text{IMG}\mathcal{O} \stackrel{\text{def}}{=} \frac{\pi_1(X)}{\bigcap_{n\in\mathbb{N}} \text{Ker}F_x^n}. \tag{13}$$

The IMG of a post-critically finte function like f^{-1} is the IMG of its *Julia set* $\mathcal{J}_f$, i.e. the accumulation points' set of the forward orbits of f. The $\text{IMG}\mathcal{J}_f$ is properly topologized and proven in [3] to be homeomorphic to $\mathcal{J}_f$, so it provides a algebraic (symbolic) explaination —via the *shift map*— to the symbolic dynamics of $\mathcal{J}_f$ under f (since every Julia set is invariant but not fixed by f itself).

Function f maps every point [sheet] $w_n{\in}\mathcal{A}_n$ to p points [sheets] in $w_{n+1}{\in}\mathcal{A}_{n+1}$ — exactly in the uncascaded case, so the p-ary rooted trees of f's images are all isomorphic with each other and the monodromy groups do not depend on starting point w_n. The monodromy groups act faithfully on the sheets by bringing forward the orbits of such points via automorphisms of the aforementioned tree. For $n{\to}\infty$, such actions become invariant on the orbispaces (orbifolds, since the underlying space of such discrete dynamics is a Riemann surface) of the monodromy groups. The IMG is generated as a portrait of the limit fractal Riemann surface itself and its elements act like a sort of 'global positioning system' (GPS) on it.

In fact, travels on such Riemann surfaces are represented by the symbolic dynamics of the visited sheets. In the absence of cascading, this means that every path on $\mathcal{A}_n$ is equivalent to a free product of winding vectors, such that every time the path stays on k^{th}-generation sheets, its symbolic dynamics is simplified to that of a path homeomorphic to one on $\mathcal{A}_k$, i.e. it is represented by the free-product group

$$\overbrace{\mathbb{Z}_p^r * \mathbb{Z}_p^r * \cdots * \mathbb{Z}_p^r}^{n \text{ times}} \tag{14}$$

Using (11) a loop $\gamma{\in}\,\text{C}^0([0,1],\mathcal{A}_0)$ travels on $\mathcal{A}_2$ by its lift $f^{-2}\restriction\gamma{=}f^2(\gamma)$ whose dynamics is coded by words of free double alphabet of $[\mathbf{k}_1]$ and $[\mathbf{k}_2]$:

$$f^2(\gamma(t)) = e^{2\pi i\mathbf{k}_1\cdot\frac{\boldsymbol{\mu}}{\boldsymbol{\pi}}} \sqrt[p]{\left|\prod_{i=1}^{r}\left(e^{2\pi i\mathbf{k}_2\cdot\frac{\boldsymbol{\mu}}{\boldsymbol{\pi}}}\sqrt[p]{\prod_{j=1}^{r}|z-z_j|^{m_j}}-z_i\right)^{m_i}\right|}. \tag{15}$$

Plots in Figs.2–5 show $\text{Arg}f^n(z)$ for several polynomial functions. Dots' brightness is proportional to the principal argument, with white-to-black discontinuities representing the branch cuts: most branch cuts tend toward infinity, whereas those between finite branch points often show *self-similar*

DOI: 10.1685/CSC09313

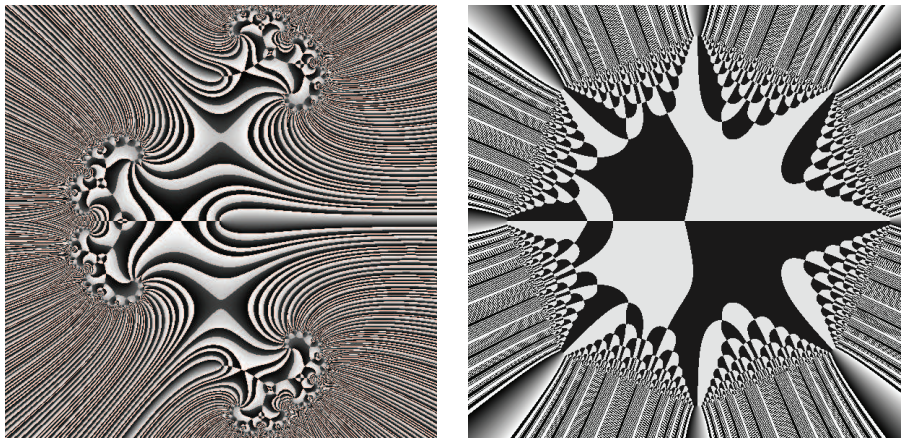

Fig. 4. Branch cuts shown as $\mathrm{Arg} f^n(z)$, for $f(z)=\sqrt{z\,(z^2+1)}$ ($n=13$, left) and $f(z)=\sqrt[7]{(z-1)(z^7+1)}$ ($n=11$, right).

discrete symmetries and/or bifurcations, as long as different-generation sheets are glued together.

Of course it is possible to use rational functions $\frac{N(z)}{D(z)}$ instead of simple polynomials $P(z)$: in this case, provided $\mathrm{GCD}(N,D)=1$, the branch points of f are of two types: *branch zero*es are N's roots, and *branch pole*s are D's roots (i.e. the polar singularities of the rational function), whereas ∞ can be either a branch point, a branch zero or a regular point. Other than cascading, a *pole-zero (*PZ*) cancellation* phenomenon may occur, where at some iteration the zero [pole] of a higher-generation rational function cancels a pole [zero] of some lower-generation functions out; cfr. Figs.5–6. Hereinafter, rational-type prefractal Riemann surfaces are indicated as $\mathcal{B}_n$. At every iteration the factors of N and D in f^n get mixed together, so the dynamics get more entangled and a few analytical examples can be found; the consecutive branching of prefractal surfaces is not only affected by occasional cascading, but also on PZ cancellations, removing branch points among different- and same-generation sheets and —in some pathological cases— dominate over the standard dynamics, leaving the sheets with poorer connections. In some cases this leads to prefractal surfaces with a number of sheets which is either fixed or grows with n slowly than the number of branch points (so the sheets' connection matrix is definitely sparse).

If $\deg N=\deg D$ the limit function $\lim_n f^n(z)$ is well-defined on the corresponding Julia set $\mathcal{J}_f$: this is guaranteed by the fact that branch poles are equipotent with regular branch points on $\mathbb{C}$ and that there always exist

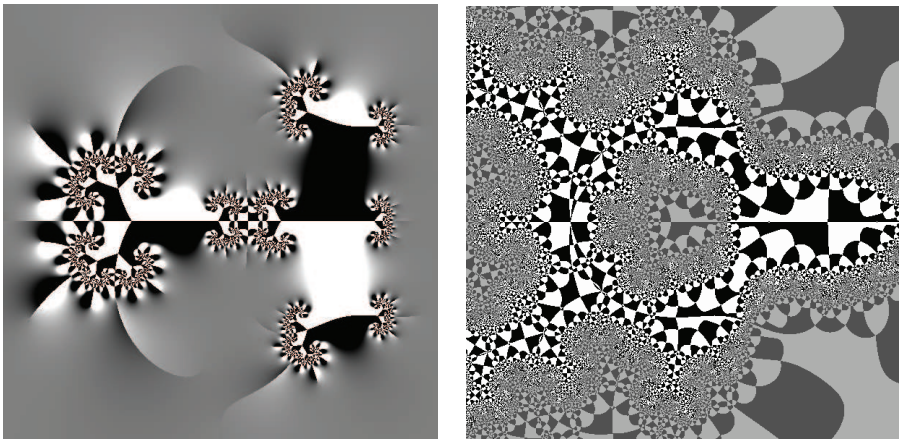

Fig. 5. Branch cuts shown as $\mathrm{Arg} f^n(z)$, for $f(z)=\sqrt[5]{\frac{z^5+1}{z(z^5-1)}}$ ($n=23$, left) and $f(z)=\sqrt[6]{\frac{z^6+1}{z(z^6-1)}}$ ($n=32$, right).

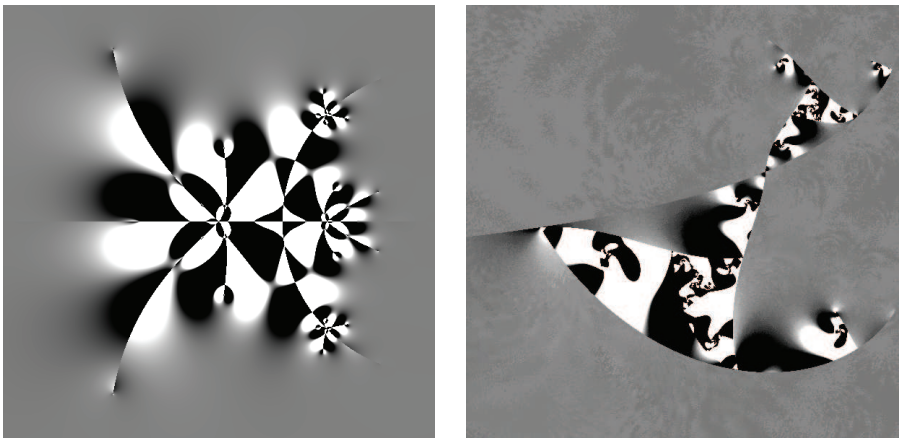

Fig. 6. Branch cuts shown as $\mathrm{Arg} f^n(z)$, for $f(z)=\sqrt{\frac{z^2+1}{z-1}}$ ($n=11$, left) and $f(z)=\sqrt{\frac{(z+\imath)^2}{z-1}}$ ($n=17$, right).

a connected open set which $|\mathrm{D}f^n|<1$ holds inside (it can be found by adjusting the monodromy path of a loop travelling on $\mathcal{A}_n$).

Plots of Figs.5–6 show the argument of such iterated functions as before, this time with equidistributed zeroes and poles along with the already observed self-similar symmetries.

DOI: 10.1685/CSC09313

3. Galois theory and the Iterated Monodromy Group

Consider the Galois group of $\mathbb{C}[w_n]/\mathbb{C}[w_m]$, for some $m<n$. Locally, every expression like $w_n = f^n(z)$ is represented by a Puiseux series in $\mathbb{C}[[w_m]]$; for example, near branch point z_j there exists one in $\mathbb{C}[[z-z_j]]$. In the simpler case $p=1$ (but with rational initiator), the explicit equation (1) can be written as $wD_n(z)-N_n(z)=0$; let Σ_n be the splitting field of (Weierstrass) polynomial $N_n - wD_n \in \mathbb{C}\{w\}[z]$, which is also a polynomial with respect to the unknown z and coefficients in the field of rational functions $\mathbb{C}\{w\}$ of variable w_{n+1}, since

$$w_{n+1} = \frac{N_n(z)}{D_n(z)} = \frac{N(w_n)}{D(w_n)}.$$

Thus $\Sigma_n = \mathbb{C}\{w_n\}(\ker(N_n - wD_n))$ is an *algebraic* extension field. The associated Galois field $\mathrm{Gal}\frac{\Sigma_n}{\mathbb{C}\{w\}}$ is well-known to be isomorphic to the monodromy group of the branches $f^n : \tilde{\mathbb{C}} \longrightarrow \tilde{\mathbb{C}}$, e.g. to the permutations' group of sets $f^{-n}(w_0)$ induced by the action of goup $\pi_1(\mathcal{B}_n, w_0)$, then:

$$\mathrm{Gal}\frac{\Sigma_n}{\mathbb{C}\{w\}} = \mathrm{MG} f^n. \tag{16}$$

Theorem 3.1. *If $f = N/D \in \mathbb{C}\{z\}$ is a post-critically finite rational function, then its profinite* IMG *is isomorphic to the corresponding Galois group,*

$$\overline{\mathrm{IMG}} f = \mathrm{Gal}\frac{\Sigma}{\mathbb{C}\{z\}},$$

where

$$\Sigma = \bigcup_{n=1}^{\infty} \Sigma_n = \lim_n \Sigma_n.$$

The splitting fields' sequence $(\Sigma_n)_{n\in\mathbb{N}_0}$, with $\Sigma_0 = \mathbb{C}\{w\}$, are inclusively mutual extension fields with $\Sigma_n \leq \Sigma_{n+1}$, whereas the Galois groups contain automorphic functions fixing $\mathbb{C}\{z\}$. That leads directly to a newly proven result:

Lemma 3.1. *The monodromy-group sequence of prefractal Riemann surfaces $(\mathcal{B}_n)_{n\in\mathbb{N}_0}$ is an inclusive sequence of mutually normal subgroups, i.e. [1]:*

$$\mathrm{MG}\mathcal{B}_n \lhd \mathrm{MG}\mathcal{B}_{n+1}$$

and

$$\mathrm{ord}_{\mathrm{MG}}\mathcal{B}_n = (\mathrm{ord}_{\mathrm{MG}}\mathcal{B}_1)^n$$

Theorem 3.2. *If f features no* PZ *cancellation phenomenon, then* $\mathrm{MG}\mathcal{B}_n$ *is solvable if and only if* $\mathrm{MG}\mathcal{B}_1$ *is solvable itself and,* $\forall m,n\in\mathbb{N}$ *s.t.* $m<n$*:*

$$\frac{\mathrm{MG}\mathcal{B}_{m+n}}{\mathrm{MG}\mathcal{B}_m}\cong\mathrm{MG}\mathcal{B}_n.$$

The profinite IMG *of the limit fractal surface* $\mathcal{B}_\infty$ *is the inverse limit of the (finite) monodromy groups' sequence, i.e.:*

$$\overline{\mathrm{IMG}}f\cong\varprojlim_n\mathrm{MG}\mathcal{B}_n.$$

Apart from being a sufficient condition for the solvability of the monodromy problem, this result shows that symbolic dynamics on a such a Riemann surface can be formally described by a starting sheet number and a sequence of winding vectors, each one accounting either consecutive windings on highest-generation branch points, or a single winding on another branch point, which means that the path crosses from one family of same-generation sheets to another (either the same generation or a different one).

4. Riemann chaos

The number of branch points (both poles and regular ones) exponentially increases and does so on every sheet —apart from pathological cases— due to dominant cascading or zero-pole cancellation. The branch points of lower generations are usually solved, locally near a higher-generation one, by cyclotomic-like equations, so the mean distance between them is locally decreasing as n increases. Any arbitrary choice of branch cuts produces a family of curves whose branch endpoints are definitely near with each other (locally, where f is contracting), so crossing any two of such near cuts may lead onto completely different sheets: this phenomenon is thus called *Riemann Chaos*. The main result regarding such phenomenon is related with the Wreath Recursion Theorem [3], where the self-similar action of $\mathrm{IMG}f$ on $\mathcal{B}_\infty$ is given by recursions $\mathrm{IMG}f=\mathbb{S}_p\wr\mathrm{IMG}f$. Then a discrete dynamical system $\left(\mathcal{J}_{\mathrm{IMG}f};f^{-1}\right)$ exists, behaving like a shift map on the boundary of $\mathcal{B}_\infty$, which is invariant (but *not* fixed) by f, cfr. [1].

Theorem 4.1. *The limit set of a post-critically finite, branched self-cover* $f:\mathcal{B}_0\longrightarrow\mathcal{B}_1$ *is homeomorphic to the multi-valued Julia set of* f*.*

The *complete* algebraic structure of a fractal Riemann surface is thus graphically represented by the Julia set of its iterator, which is the boundary between a surface where *regular motion* takes place —i.e. finite-length paths cross only a finite number of branch cuts— and one where *chaotic* motion

DOI: 10.1685/CSC09313

does — i.e. where finite-length paths cross a countably infinite number of cuts, thus leading to routes which are *irreversible* for any finite-precision arithmetics on the surface. There is also a natural boundary (the Julia set in fact) beyond which branch cuts are dense and no analytic continuation is viable: the associated multivalued functions are either ∞ or 0.

Many open problems arise from these considerations. Such entangled complex structures are described by iterating complex functions living in a simple parameter-space, like $(p, \mathbf{z}, \mathbf{m}) \in \mathbb{N} \times \mathbb{C}^r \times \mathbb{N}^r$: is there a way to further characterize their geometric, algebraic and analytical properties according by synthesis of such a space? Are there effectively computable Lyapunov exponents on them? Is it possible to find a (integrable) dynamical system whose phase space is given by a surface of this kind?

5. Applications

As far as applications are concerned, such functions are usable as cyphers: symbolic computation of direct paths is easy (provided sufficient numeric precision), whereas surfaces' synthesis in order to rebuild a symbolic dynamics from a path's lift is not. Two scenarios are available.

The first one is to let a digital message be codified in a base-p^n alphabet, then choose an aforementioned phase-point $(p, \mathbf{z}, \mathbf{m})$ as a *key* corresponding to some non-cascading, non-PZ function f. Such a $f^n(z)$ covers a p^n-sheeted Riemann surface $\mathcal{B}_n$ where, in some regions, almost-dense branch points are present. The encryption algorithm chooses a path $\gamma \in \mathrm{C}^0([0,1], \mathbb{C})$ which, staring from the sheet whose number corresponds to the first message symbol (encrypted in some other fashion and passed along with the key), travels on $\mathcal{B}_n$ winding around different-generation branch points (i.e. crossing branch cuts): the number-sequence of sheets visited by $f^{-n} \restriction \gamma$ corresponds to the symbols' sequence of the original message. Sampled coordinates of γ with a high-enough precision are then transferred through a untrusted channel, whereas the key must be through a trusted one (or broken into public and private parts by other cyphers, e.g. RSA). The decryption algorithm numerically computes back the path $f^n(\gamma(t))$ and extrapolates its visited sheets' number-sequence, i.e. the original message. The cypher's robustness is a smart-enough choice of paths winding near clustering branch points, such that missing them by little means definitely travelling on arbitrarily distant sheets (according $\mathcal{B}_n$'s metric), thus recovering a wrong message.

A harder way is to let γ be a path on the complex plane which representing the analogic message. Let such a Riemann surface be given by the phase-point above. For any large-enough iteration orders n the lifted path $f^{-n} \restriction \gamma = f^n(\gamma)$ is a new signal, this time traveling on a multi-sheeted Rie-

mann surface. By projecting this path back on $\mathbb{C}$ we have another simple *encrypted* signal, whose key is the phase-point. The robustness is in this case given by a smart choice of $(p, \mathbf{z}, \mathbf{m})$ which is critically near to a *topological phase transition*. This term refers to the distribution of the branch zeroes/poles on the polynomial (for $\mathcal{A}_n$-like surfaces) or rational (for $\mathcal{B}_n$-like ones) coefficients: such phase transitions occur when either such roots merge or split (thus changing the branching types) or move up to change the surface homotopy (and monodromy). If a phase is chosen near such a critical point, missing the key by little recovers a critically different message.

Restating that using symbolic dynamics, let the signal be given by either a sheet transition like $p_1 \rightsquigarrow p_2 \rightsquigarrow ... \rightsquigarrow p_s$ (former proposed kind of encryption scheme) or a specific homotopy class for a curve like $\curvearrowright z_1 \curvearrowleft z_2 \curvearrowright ... \curvearrowleft z_s$ (latter encryption scheme): whenever a wrong key is picked (thus leading to different Riemann surfaces along with their monodromy groups) the symbolic dynamics recovers a completely different curve (and thus message).

Before concluding the author would like to point out that such Riemann surfaces and the formalism introduced here are good starting points for the analysis of iterated complex functions (even of transcendental type). Another application which is currently being investigated is in the electromagnetic scattering from self-similar domains (or domains with multifractal inhomogeneities): in this case the classical direct and inverse scattering techniques can still be applied by induction on prefractal domains, where the scattering kernels are iterations of complex wave-vectors $\kappa \in \mathbb{C}^3$ functions.

REFERENCES

1. W. Arrighetti. *Mathematical models and methods for Electromagnetic fields in Fractal geometries*. PhD thesis, "Sapienza" Università di Roma, Rome (Italy), 2007.
2. B. A. Dubrovin, A. T. Fomenko, and S. P. Novikov, *Modern Geometry: methods and applications* (3 parts), Springer-Verlag, 1992,1985,1990.
3. V. Nekraševič. *Self-Similar Groups*, Mathematical surveys and monographs 117, AMS, 2005.
4. V. Nekraševič. *Iterated monodromy groups*, 2002, arXiv:math.DS/0312306.
5. W. Arrighetti, and G. Gerosa. *Can you hear the fractal dimension of a drum?*. In M. Primicerio, R. Spigler, V. Valente, editors, *Applied and Industrial Mathematics in Italy*, Series on Advances in Mathematics for Applied Sciences, Vol. 69, pp. 65–75. World Scientific, 2005. arXiv:math.SP/0503748.