Jordan Curves with Polynomial Inverse Moduli of Continuity

Ker-I Ko
Fuxiang Yu
Stony Brook, NY

Computability and Continuity

$f:[0,1]{\to}\mathbb{R}$ is computable if $\exists$ oracle TM M:

$$(\forall \phi \in CF_x)\ |M^{\phi}(n) - f(x)| \le 2^{-n}.$$

[$\phi \in CF_x$ means $|\phi(n) - x| \le 2^{-n}$.]

- $f:[0,1]{\to}\mathbb{R}$ is computable on $[0,1]$
  $\Longleftrightarrow$ (a) It is continuous on $[0,1]$, and
  (b) It is computable at dyadic numbers:
  $$(\exists M)\ |M(d,n) - f(d)| \le 2^{-n}.$$
- $f:[0,1]{\to}\mathbb{R}$ is continuous on $[0,1]$
  $\Longrightarrow$ f is computable relative to some oracle set A.

Polynomial-Time Computability and Polynomial Modulus

$f : [0,1] \to \mathbb{R}$ is P-computable if $\exists$ oracle TM M:

M computes f in time $O(n^k)$.

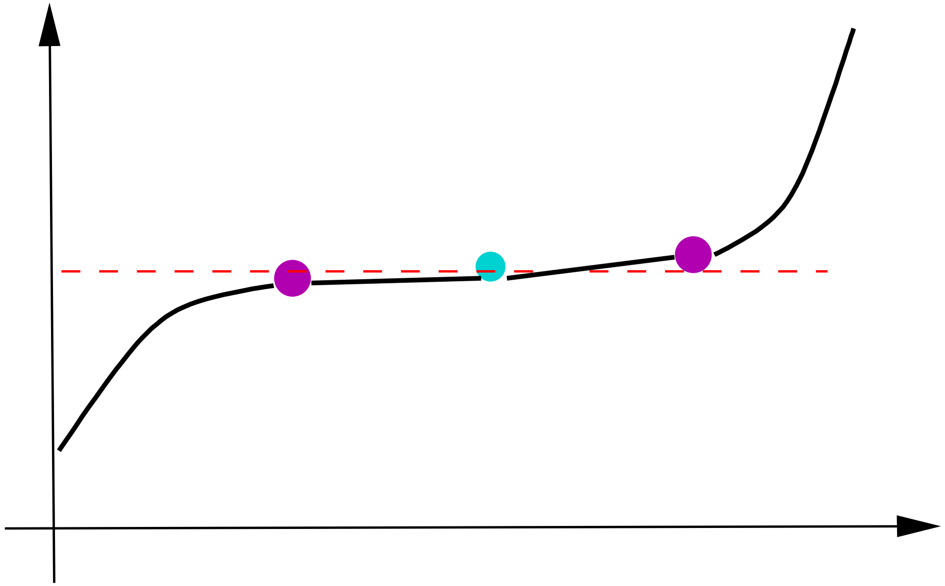
- $f : [0,1] \to \mathbb{R}$ is P-computable
  $\iff$ (a) f has a polynomial modulus of continuity on $[0,1]$:
  $$|x - y| \le 2^{-n^k} \;\Rightarrow\; |f(x) - f(y)| \le 2^{-n},$$
  (b) f is P-computable at dyadic points

- If $f : [0,1] \to \mathbb{R}$ has a polynomial modulus on $[0,1]$
  $\Longrightarrow$ f is P-computable relative to an oracle set A.

Computational Complexity of Inverse Function

Assume that $f : [0,1] \to [0,1]$ is one-to-one and P-comptable. How hard is it to compute f^{-1}?

- ($\forall$ recursive $t(n)$), $\exists f$: 1-1, P-computable, with modulus of f^{-1} satisfying $m(n) > t(n)$ (and so f^{-1} is not $t(n)$-time computable).



- If f^{-1} has a polynomial modulus, then f^{-1} is P-computable.

  Proof: By binary search.

$$f(x) \approx y \Rightarrow x \approx f^{-1}(y)$$

If f^{-1} has a polynomial modulus, we say f has a polynomial inverse modulus:

$$|x - y| > 2^{-n} \Longrightarrow |f(x) - f(y)| > 2^{-n^k}$$

Assume that $f : [0,1] \longrightarrow [0,1]^2$ is one-to-one and P-computable. How hard is it to compute f^{-1} (on $range(f)$)?

- If f has a polynomial inverse modulus, then f^{-1} is NP-computable.
  Proof: Guess $e = f^{-1}(d)$ and verify $f(e) \approx d$.

- Is f^{-1} P-computable?
  — probably not, as binary search no longer works in $[0,1]^2$.

- Can f encode an NP-complete problem so that f^{-1} is P-computable if and only if P $=$ NP?

Analogy in Discrete Complexity Theory

Assume that $g : \{0,1\}^* \rightarrow \{0,1\}^*$ is one-to-one and P-computable. How hard is it to compute g^{-1} (on $range(g)$)?

- For any recursive $t(n)$, it is possible that g^{-1} is not computable in time $t(n)$.
  Proof: $g(0^{t(n)+1}) = 0^n$.
- Assume that g is polynomially honest:
  $$|g(s)|^k \geq |s| \text{ for some constant } k.$$
  Then, the complexity of g^{-1} is related to one-way functions.

- If g is polynomially honest, one-to-one, and P-computable, then g^{-1} is UP-computable (so, $\mathrm{P} = \mathrm{UP} \;\Rightarrow\; g^{-1} \in \mathrm{P}$).

- If $\mathrm{P} \neq \mathrm{UP}$ then $\exists g$: 1-1, polynomially honest, P-computable, but g^{-1} is not P-computable.

  (Such a function g is called a weak one-way function.)

- UP (Unambiguous NP): Sets accepted by NP machines that have at most one accepting computation on any input.

- $\mathrm{P} \subseteq \mathrm{UP} \subseteq \mathrm{NP}$.

Theorem

(a) $\mathsf{P} = \mathsf{NP}$

$\Rightarrow$ (b) $f : [0,1] \rightarrow [0,1]^2$ is 1-1, P-computable, and has poly. inverse modulus $\Rightarrow$ f^{-1} is P-computable

$\Rightarrow$ (c) $\mathsf{P} = \mathsf{UP} \cap \mathsf{coUP}$

Why do we need (a) $\mathsf{P} = \mathsf{NP}$?

— $f^{-1}(d)$ *has many approximate values even if* f *is 1-1 and has polynomial inverse modulus.*

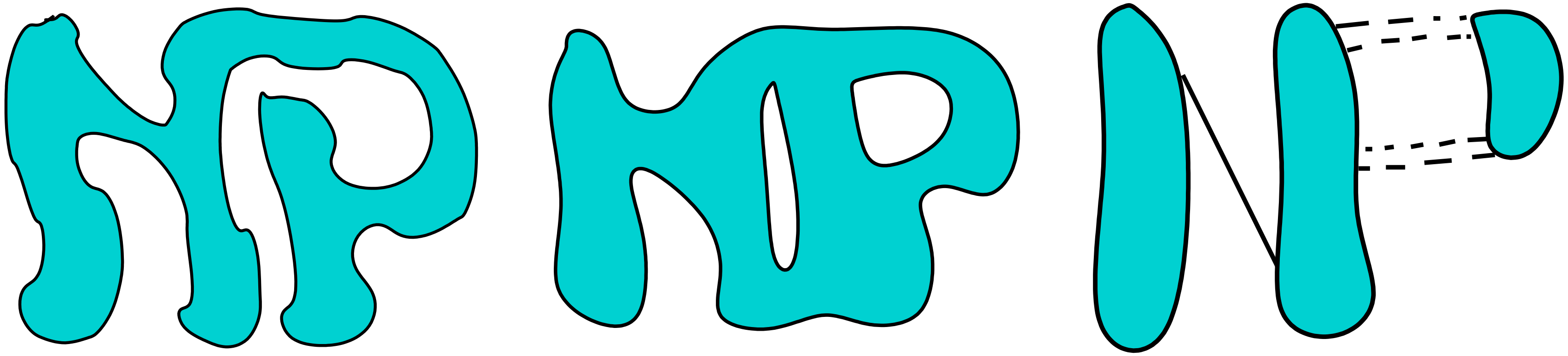
Why $\mathsf{UP} \cap \mathsf{coUP}$ instead of UP?

— *We need total one-way functions to prove* $\neg$(b).

A complexity theory for functions defined on $\mathbb{R}^2$

Basic Objects

Open or Closed Subsets of $\mathbb{R}^2$



What are the natural representations for these sets?

For a simply connected domain S, a natural representation is the

Boundary Curve ∂S

- A Jordan curve (a simple, closed curve) Γ is P-computable if $\exists$ P-computable $f : [0,1] \rightarrow \mathbb{R}^2$ whose image $f([0,1])$ is Γ (It follows that $|s-t| \leq 2^{-n^k} \implies |f(s)-f(t)| \leq 2^{-n}$.)

- A P-comutable Jordan curve may be a complex object from a different aspect.
  E.g., $\exists$ a P-computable Jordan curve Γ which has fractal dimension 2.

Goals

- Understand the properties of P-computable Jordan domains.
- Analyze the computational complexity of operations on P-computable Jordan domains.
- Generalize problems in Computational Geometry to more general subsets of $\mathbb{R}^2$.

Complexity of Numerical Operations on a Jordan Domain

Distance from ∂S	NP-complete
Circumscribed Rectangle	Σ_2^P-complete
Winding number	#P-complete
Membership	upper bound: #P lower bound: UP

Shortest Path	upper bound: PSPACE, if a path away from ∂S exists lower bound: $\#$P
Area	Noncomputable Computable but arbitrarily hard, if ∂S is not a fractal $\#$P-complete, if $leng(\partial S) < \infty$
Length of ∂S	Noncomputable, even if $leng(\partial S) < \infty$

Big gaps between upper bounds and lower bounds??

Proposal: Study these problems on a more restrictive class of Jordan domains S; i.e., those with a polynomial inverse modulus.

- A P-computable Jordan curve Γ has a polynomial inverse modulus if it is computed by a function f that is P-computable and has a polynomial inverse modulus:
  That is, $|s-t| > 2^{-n} \implies |f(s)-f(t)| > 2^{-n^k}$.
- A P-comutable Jordan curve with polynomial inverse modulus may still be complex; e.g., it may still be a fractal.
  In fact, all the Jordan domains constructed for the lower bound results have polynomial inverse moduli.

Membership Problem

For a Jordan domain $S \subseteq [0,1]^2$, determine whether or not a given point $\mathbf{z}$ is in S?

Need oracle TM M:

$$(\forall \phi \in CF_{\mathbf{z}})\ M^{\phi}(n) = \begin{cases} 1 & \text{if } \mathbf{z} \in S, \\ 0 & \text{if } \mathbf{z} \notin S. \end{cases}$$

However, by the basic relation between computability and continuity, such a machine cannot exist (unless S is trivial).

So, we can only solve Approximate Membership problem; i.e., we need to allow M to make errors.

A few different error controls

Let $S_M(n) = \{\mathbf{z} \mid (\exists \phi \in CF_{\mathbf{z}}) M^{\phi}(n) = 1\}$,
$E_M(n) = S \, \Delta \, S_M(n)$.

P-recognizable set

Errors can only occur near the boundary:
$\mathbf{z} \in E_M(n) \Rightarrow dist(\mathbf{z}, \partial S) \leq 2^{-n}$

P-approximable set

Total errors have small Lebesgue measure:
$\mu(E_M(n)) \leq 2^{-n}$

Strongly P-recognizable set

Errors can occur only near the boundary and outside S:
$\mathbf{z} \in E_M(n) \Rightarrow dist(\mathbf{z}, \partial S) \leq 2^{-n}$ and $\mathbf{z} \notin S$

Locally P-computable set

Errors can occur only outside the boundary, close but not very close to the boundary:

$\mathbf{z} \in E_M(n) \Rightarrow 2^{-n} \leq dist(\mathbf{z}, \partial S) \leq 2^{-(n-1)}$ and $\mathbf{z} \notin S$

Hausdorff approximable set

Errors are within 2^{-n} of Hausdorff distance from S:

$dist_H(S, S_M(n)) \leq 2^{-n}$

Some known relations between these formulations

- $\exists S$: S is P-recognizable but not even recursively approximable.
  (The boundary of S is a fractal.)

- FP $=$ #P
  $\Longrightarrow$ All P-approximable sets are P-recognizable
  $\Longrightarrow$ BPP $=$ P

- All locally P-computable sets are strongly P-recognizable.

- P $=$ NP $\Longleftrightarrow$ All strongly P-reconizable sets are locally P-computable.

Improving the Complexity Bounds by Polynomial Inverse Modulus

MEMBERSHIP (based on P-recognizability):
Assume ∂S is P-computable. Determine, for a given $\mathbf{z} \in \mathbb{R}^2$ with $dist(\mathbf{z}, \partial S) > 2^{-n}$, whether $\mathbf{z} \in S$.

- For a P-computable Jordan domain S:
  - $\text{MEMBERSHIP} \in \mathsf{P}^{\#\mathsf{P}}$
  - $\mathsf{P} \neq \mathsf{UP} \Longrightarrow \text{MEMBERSHIP} \notin \mathsf{P}$.
- If ∂S also has polynomial inverse modulus:
  - $\text{MEMBERSHIP} \in \mathsf{P}^{\mathsf{NP}} = \Delta_2^{\mathsf{P}}$
  - $\mathsf{P} \neq \mathsf{UP} \Longrightarrow \text{MEMBERSHIP} \notin \mathsf{P}$.

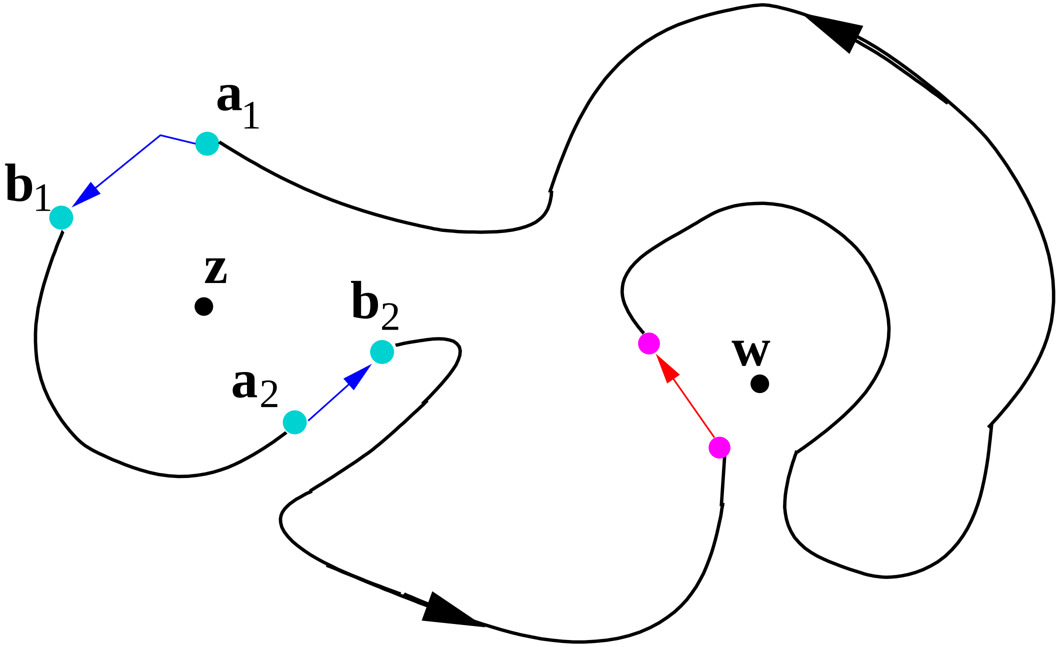
Proof Ideas

Why is there a gap between upper bound #P and lower bound UP?

— Upper bound #P comes from traversing the whole curve ∂S and calculating the winding number.

Idea: Just check the orientation of a short section of ∂S around the point $\mathbf{z}$.

But it does not work.

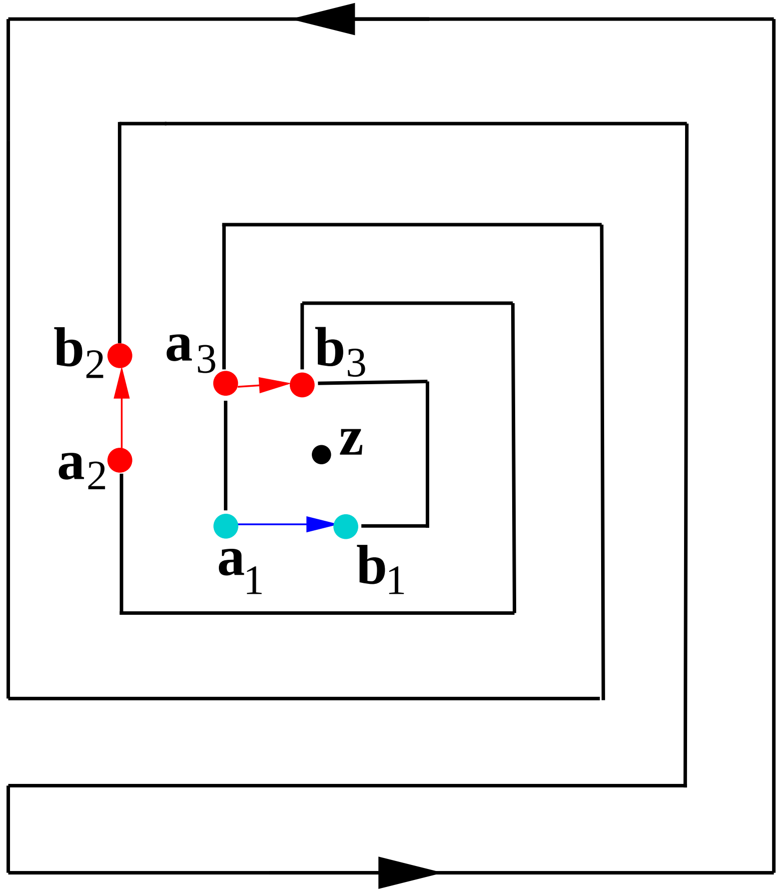


Two Problems:

1) Hard to find the closest section ($\mathbf{a}_2 \rightsquigarrow \mathbf{b}_2$?)
2) Might skip a big section ($\mathbf{a}_3 \rightsquigarrow \mathbf{b}_3$?)

New idea:

It might work if ∂S has a polynomial inverse modulus of continuity.



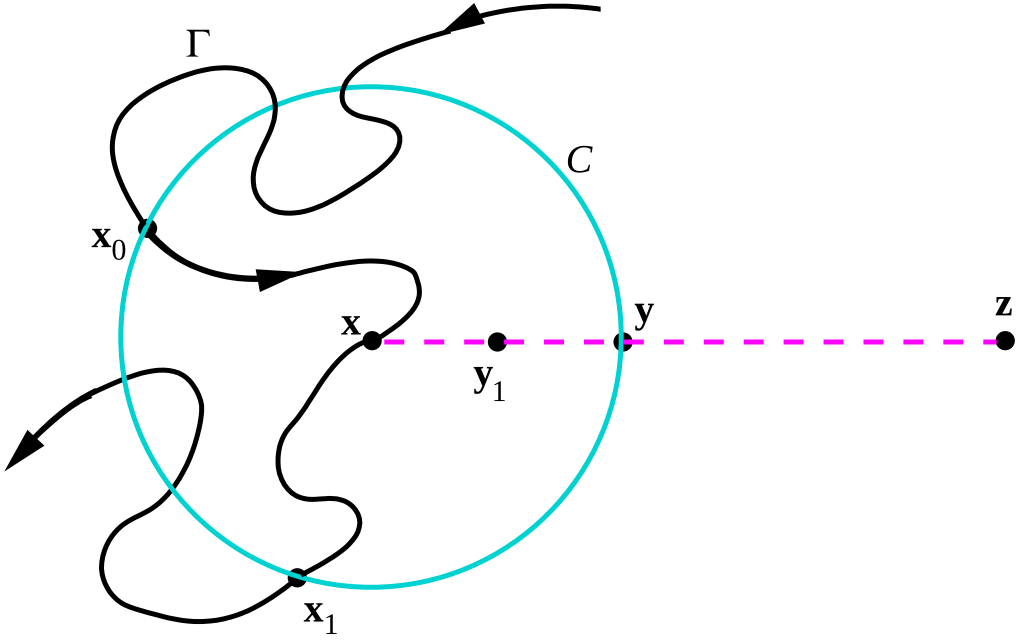
In particular, (2) cannot happen if $dist(\mathbf{z}, \partial S)$ is large enough.

$\mathbf{x} \in \partial S$:

$|\mathbf{x} - \mathbf{z}| \approx dist(\mathbf{z}, \partial S)$
$> 2^{-n}$.

C: Circle centered
at $\mathbf{x}$ with radius
$\ll 2^{-n}$

$\mathbf{x}_0, \mathbf{x}_1$: Starting and
ending points of
∂S inside C.



Lemma Assume ∂S goes around S in the counterclockwise direction. Then,

$\mathbf{z} \in S \Longleftrightarrow$ the orientation of $\mathbf{x}_1 \leadsto \mathbf{y} \leadsto \mathbf{x}_0$ around $\mathbf{x}$
is in the counterclockwise direction.

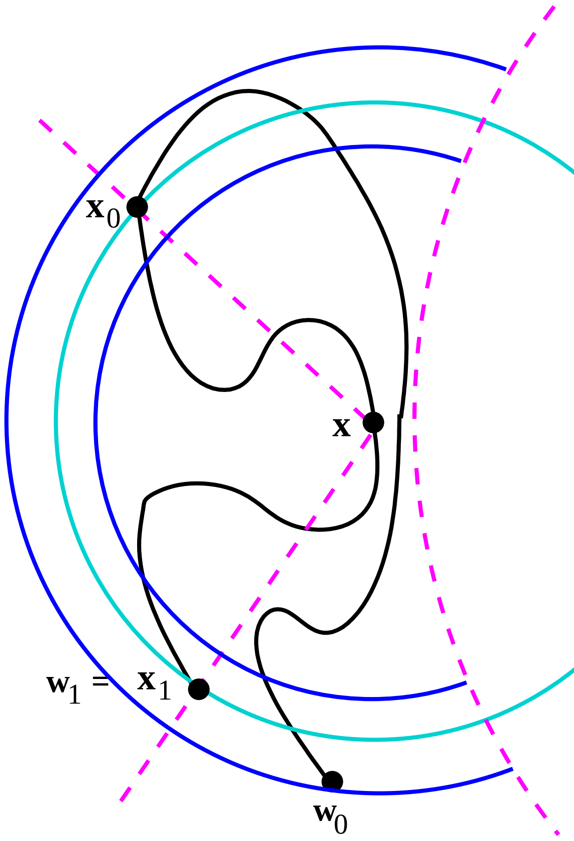
Algorithm (in time $\Delta_2^{\mathsf{P}} = \mathsf{P}^{\mathsf{NP}}$)

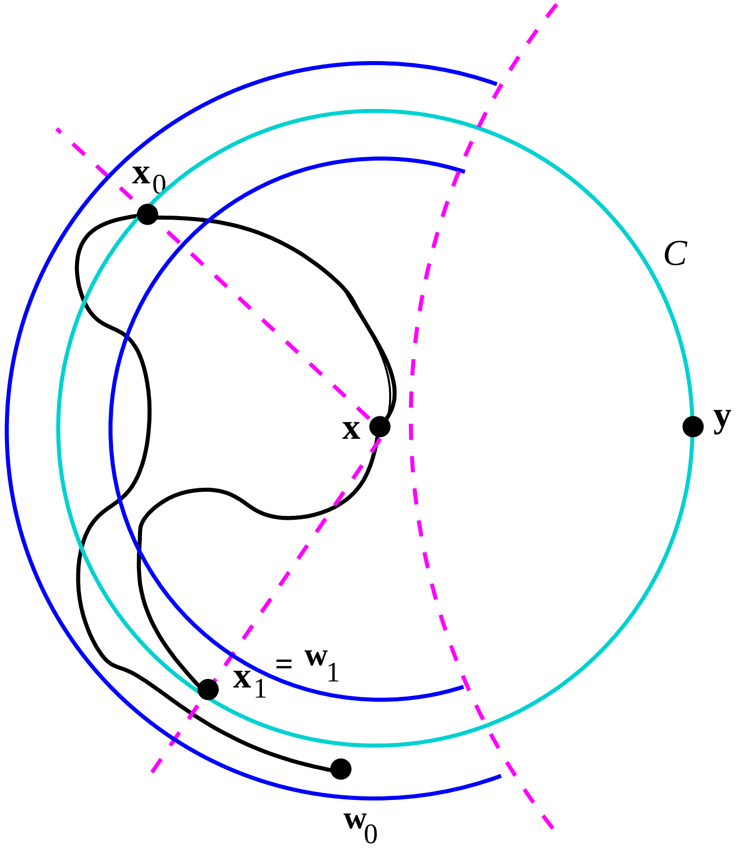
1) Assume that $dist(\mathbf{z}, \partial S) > 2^{-n}$. Let $m = p(n)$, where p bounds the modulus and inverse modulus of f.
2) Find $\mathbf{w} \in \partial S$ with $|\mathbf{z} - \mathbf{w}| \approx dist(\mathbf{z}, \partial S)$ (error $\ll 2^{-m}$).

   $\{\mathbf{w}$ is an approximation to $\mathbf{x}.\}$
3) Let C be the circle centered at $\mathbf{w}$ with radius 2^{-m}, and y the intersection point of $\overline{\mathbf{zw}}$ and C.
4) Let $\mathbf{w}_0$ and $\mathbf{w}_1$ be two points such that the section of ∂S from $\mathbf{w}_0$ to $\mathbf{w}_1$ are approximately in C.

   $\{\mathbf{w}_0$ and $\mathbf{w}_1$ are not necessarily approximations to $\mathbf{x}_0$ and $\mathbf{x}_1.\}$
5) Determine the orientation of $\mathbf{w}_1 \leadsto \mathbf{y} \leadsto \mathbf{w}_0$ around $\mathbf{w}$; answer $\mathbf{z} \in S$ if and only if it is counterclockwise.

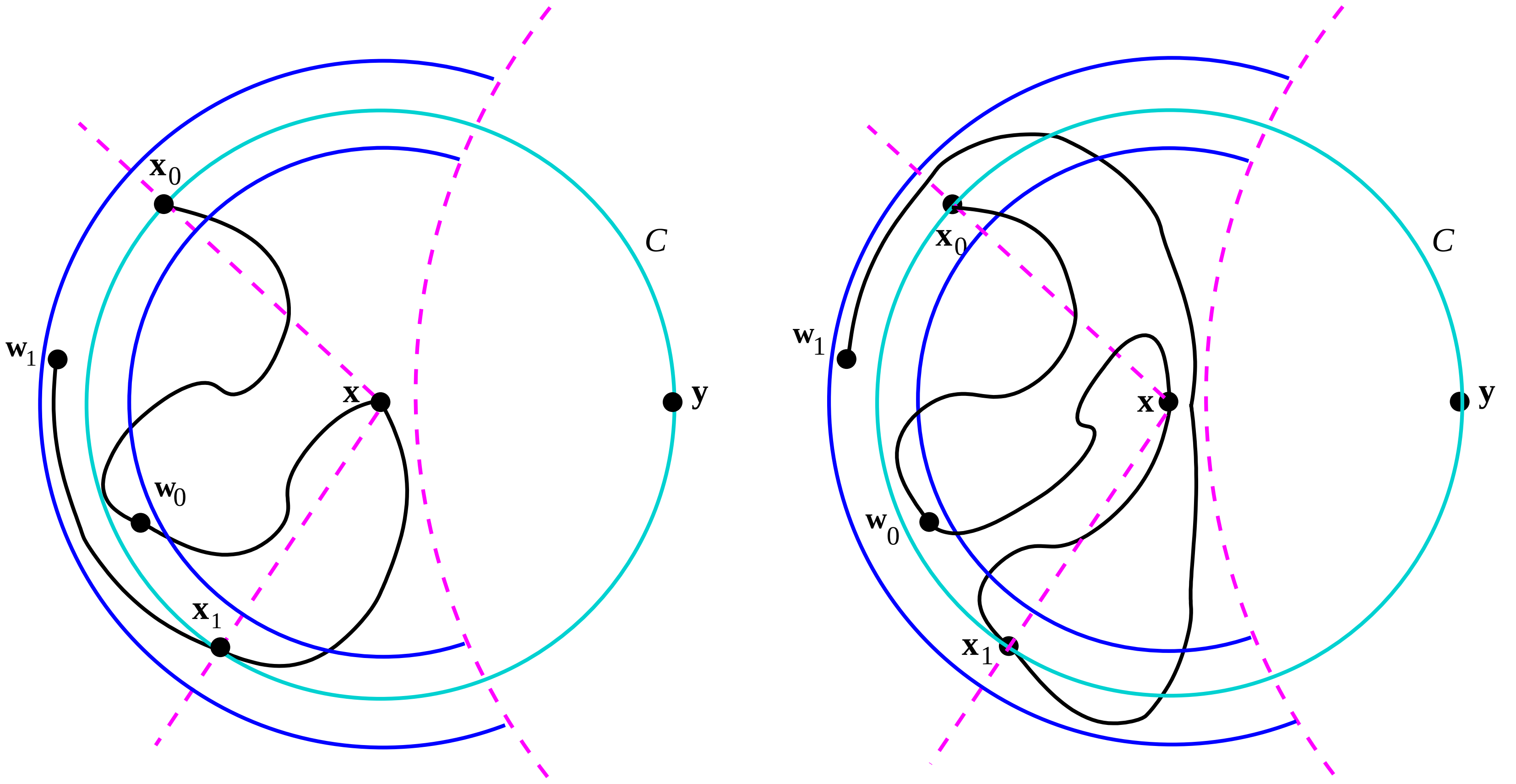
Correctness: We need to prove that the orientation of $\mathbf{w}_1 \rightsquigarrow \mathbf{y} \rightsquigarrow \mathbf{w}_0$ is the same as that of $\mathbf{x}_1 \rightsquigarrow \mathbf{y} \rightsquigarrow \mathbf{x}_0$:





Note: If ∂S has poly. inv. mod., and $\mathbf{a} \rightsquigarrow \mathbf{b}$ is long enough, then $\mathbf{a}$ and $\mathbf{b}$ cannot be too close.

Another possible case?



Shortest Path Problem

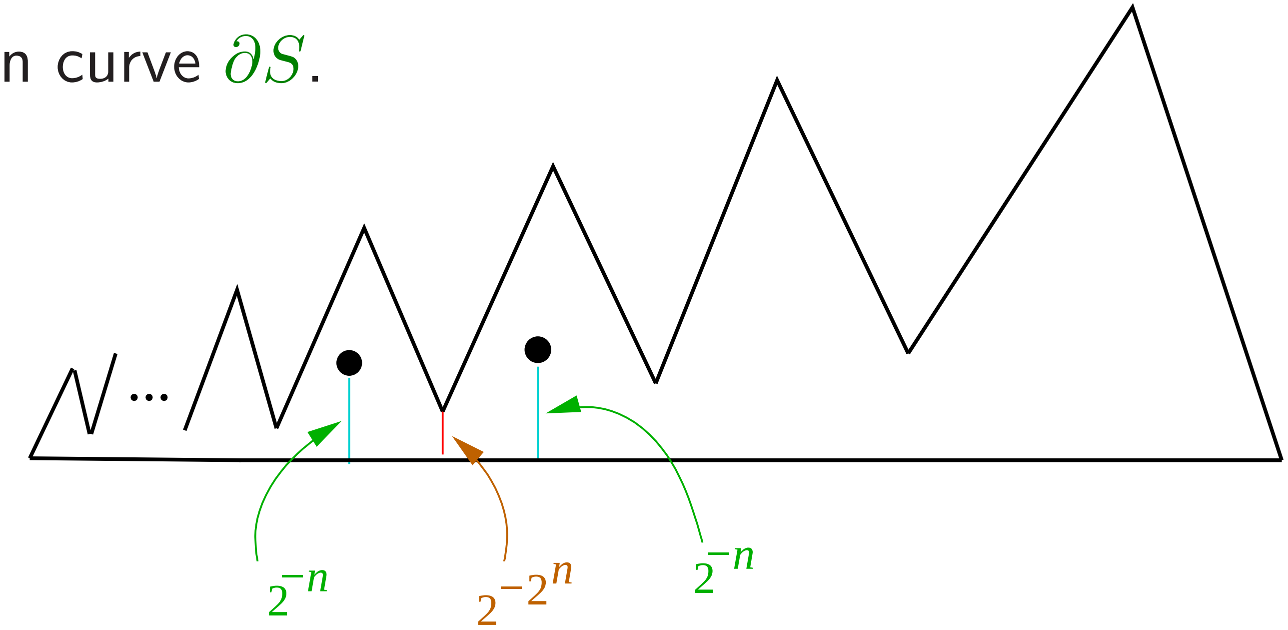
$\textsc{Shortest-Path}$: Assume ∂S is P-computable. Given $\mathbf{x}, \mathbf{y} \in S$, $n > 0$ and $L \in \mathbb{D}$, determine whether there is a path $\pi : \mathbf{x} \rightsquigarrow \mathbf{y}$ that lies within S with $dist(\pi, \partial S) > 2^{-n}$, and has length $\leq L$.

- For a P-computable Jordan domain S:
  $\textsc{Shortest-Path} \in$ PSPACE, if such a path exists
  P $\neq$ #P $\implies \textsc{Shortest-Path} \notin$ P
- If ∂S also has polynomial inverse modulus:
  $\textsc{Shortest-Path} \in$ PSPACE
  P $\neq$ #P $\implies \textsc{Shortest-Path} \notin$ P
- If S is not necessarily a Jordan domain, but is only required to be P-recognizable, then the lower bound #P can be improved to PSPACE.

Theorem If ∂S is P-computable and has polynomial inverse modulus, then

$$(\forall \mathbf{z}_0, \mathbf{z}_1 \in S,\ dist(\mathbf{z}_0, \partial S) > 2^{-n}, dist(\mathbf{z}_1, \partial S) > 2^{-n})$$
$$[\exists \pi : \mathbf{z}_0 \rightsquigarrow \mathbf{z}_1 \text{ with } dist(\pi, \partial S) > 2^{-n^k}]. \qquad (*)$$

The property $(*)$ does not hold for an an arbitrary Jordan curve ∂S.



Proof

Definitions

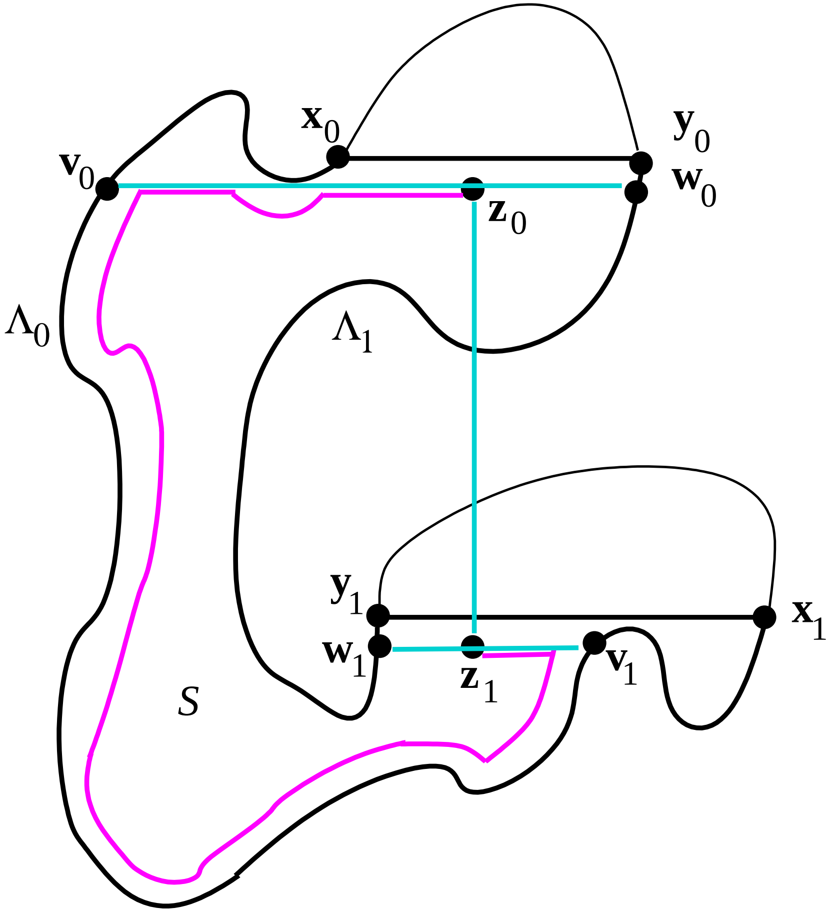
q: modulus and inv. mod.

$\overline{\mathbf{x}_0\mathbf{y}_0} \perp \overline{\mathbf{z}_0\mathbf{z}_1}$

$\overline{\mathbf{x}_1\mathbf{y}_1} \perp \overline{\mathbf{z}_0\mathbf{z}_1}$

Λ_0: ∂S from $\mathbf{x}_0$ to $\mathbf{x}_1$

Λ_1: ∂S from $\mathbf{y}_1$ to $\mathbf{y}_0$



Properties

- $dist(\Lambda_0, \Lambda_1) > 2^{-q(n)+2}$ (by the inv. mod. q)
- $\exists \mathbf{z}_0 \rightsquigarrow \mathbf{z}_1$ within distance $2^{-q(n)}$ of $\overline{\mathbf{x}_0\mathbf{y}_0}$, Λ_0,Λ_1, $\overline{\mathbf{x}_1\mathbf{y}_1}$.

Application to Analytic Continuation

ANALYTIC-CONT: Assume that ∂S is P-computable, and that g is analytic on S, with its power series expansion at $\mathbf{z}_0 \in S$ P-comutable. For a given $\mathbf{z} \in S$, find the power series expansion of g at $\mathbf{z}$.

- For a P-computable ∂S, is there a recursive upper bound for the complexity of ANALYTIC-CONT?

- If ∂S also has polynomial inverse modulus, ANALYTIC-CONT $\in$ EXPSPACE (solvable in space $2^{q(n)}$ for some polynomial q).

- For function $g = Log$, ANALYTIC-CONT has upper bound $=$ lower bound $=$ #P.

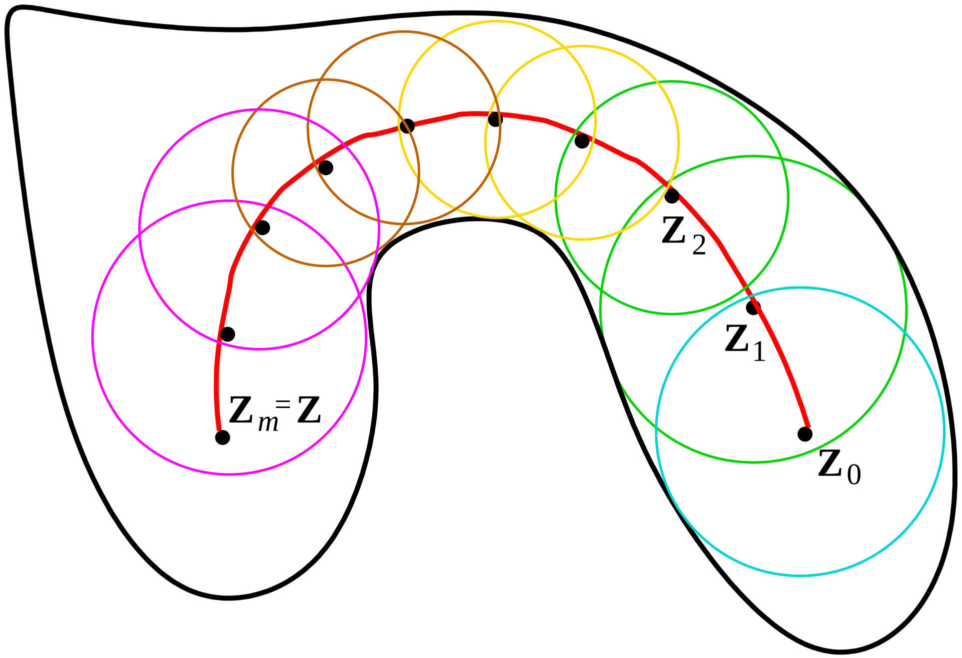
Analysis of Weierstrass's Algorithm

- Computing the power series along a path.

$$g(\mathbf{z}) = \sum_{n=0}^{\infty} a_n^{(k)} (\mathbf{z} - \mathbf{z}_k)^n$$

- The coefficients can be computed recursively:

$$a_n^{(k)} := \sum_{i=n}^{n2^c} \binom{i}{n} a_i^{(k-1)} h^{i-n}$$



- To compute $a_n^{(m)}$, we need the first $n2^{cm}$ terms of $g(\mathbf{z}_0)$.

- The number m of points depends on the width of the path.

- If ∂S has polynomial inverse modulus, then the width is $\geq 2^{-q(n)}$ and $m = 2^{O(q(n))}$.
- So, we need a double exponential number of terms of $g(\mathbf{z}_0)$ to compute $a_n^{(m)}$ correct within error 2^{-n}.
- These double exp. number of coefficients can be computed recursively in an exponential amount of space:
  The computation of $a_n^{(m)}$ is a tree of height m and width 2^{cm}.

Conclusion and Open Questions

- The notion of polynomial inverse modulus helps to reduce the upper bounds of several problems about two-dim. Jordan domains.
- P-computable Jordan domains with polynomial inverse moduli are a rich class of objects, which include fractals. Most Jordan curves constructed for the lower bound results have polynomial inverse moduli.
- Find mathematical and computational characterizations of P-computable Jordan domains with polynomial inverse moduli.
- Extend the study to multiply connected domains, and more general open or closed subsets of $\mathbb{R}^2$.