Cauchy integral theorem in a TC^0 arithmetic

Emil Jeřábek

Institute of Mathematics
Czech Academy of Sciences
jerabek@math.cas.cz
https://users.math.cas.cz/~jerabek/

Logical foundations of complexity theory

Isaac Newton Institute for Mathematical Sciences
Cambridge, October 2026

Outline

1. **$\mathbf{TC}^0$ arithmetic with infinite sets**
2. **Working in VTC^0_∞**
3. **Cauchy integral theorem**

TC^0 arithmetic with infinite sets

1. **TC^0 arithmetic with infinite sets**
2. **Working in VTC^0_∞**
3. **Cauchy integral theorem**

Feasible analytic reasoning

Formalization of mathematical results in bounded arithmetic:

- feasible reasoning, "bounded reverse mathematics"
- uniform propositional proofs
- consistency of computational complexity conjectures

Typically: finite combinatorics, elementary number theory

Some arguments use tools from complex analysis:

- generating functions in enumerative combinatorics
- analytic number theory
- eigenvalues and eigenvectors

Can we do such things in bounded arithmetic?

$\mathbf{TC}^0$ and VTC^0

Minimal complexity class: $\mathbf{TC}^0$

- $+$, $-$, $\cdot$, $/$, $\sum_{i<n} X_i$, $\prod_{i<n} X_i$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(i)$ [HAB'02]
- approximation of functions given by nice power series: exp, log, sin, arctan, $\sqrt[k]{x}$, ...

Corresponding theory: VTC^0 [NC'06,CN'10]

- formalize basic arithmetic operations incl. $\prod_{i<n} X_i$ [J'22]
- model-theoretic construction of "reals":
  $\mathfrak{M} \vDash \mathrm{VTC}^0 \rightsquigarrow \mathbf{Q}^{\mathfrak{M}} \rightsquigarrow$ topological completion $\mathbf{R}^{\mathfrak{M}}, \mathbf{C}^{\mathfrak{M}}$
  - $\mathbf{R}^{\mathfrak{M}}$ real-closed field, $\mathbf{C}^{\mathfrak{M}}$ alg. closed [J'15]
  - construction of elementary analytic functions on $\mathbf{C}^{\mathfrak{M}}$: exp, log, trigonometric, hyperbolic, their inverses [J'23]
  - no general theory of analytic functions

Can't quantify over reals, sequences, functions, ...

$\Longrightarrow$ need a more robust setup

VTC^0 with infinite sets

VTC^0: Zambella-style two-sorted bounded arithmetic

- unary (index/auxiliary) integers: $0, 1, +, \cdot, \leq$
- finite sets $\approx$ binary integers $\approx$ binary strings: $\in$, $|X|$

VTC^0_∞: two-sorted arithmetic with infinite sets

- unary (index/auxiliary) integers: $0, 1, +, \cdot, \leq$
- sets of unary integers: $\in$ (no $=$)
- base theory ($\approx \mathrm{Q}$), induction:
  $0 \in X \wedge \forall n\,(n \in X \to n+1 \in X) \to \forall n\, n \in X$
- comprehension: $\exists X\, \forall n\,(n \in X \leftrightarrow \varphi)$, $\varphi \in \Sigma^B_0 = \Delta^0_0$
- counting: $\forall X\, \exists C\colon\ C^{(0)} = 0 \wedge \forall n\, C^{(n+1)} = C^{(n)} + [n \in X]$
- finite sets encoded as a set X & a bound n

Related work

Buss '85: variants of V^i_1, U^i_1 with infinite sets

F. Ferreira, G. Ferreira, A. Fernandes: theories for analysis

- BTFA $\approx \mathsf{S}^1_2 + \mathrm{B}\Sigma^b_\infty +$ recursive comprehension
- binary strings (numbers), sets of binary strings
- cons. over $\mathsf{S}^1_2 + \mathrm{B}\Sigma^b_\infty$, Π^0_2-cons. over $\mathsf{S}^1_2 \approx \mathsf{V}^1 \supseteq \mathrm{VTC}^0$
- BTFA $+ \Sigma^b_\infty$-WKL Π^1_1-cons. over BTFA
- for Riemann integration:
- TCA^2: BTFA-like extension of TCA = theory for **CH**
- TCA $\approx$ (quasipoly) VTC^0, but unary numbers reinterpreted as binary $\implies$ exponentially stronger

VTC^0_∞ vs. VTC^0

$\mathfrak{M} = \langle M_1, M_2, \dots \rangle \models \mathrm{VTC}^0_\infty$, $M_2 \subseteq \mathcal{P}(M_1)$
$\rightsquigarrow \mathfrak{M}^{<\infty} = \langle M_1, M_2^{<\infty}, \dots \rangle \models \mathrm{VTC}^0$:

$$M_2^{<\infty} = \{X \in M_2 : \exists n \in M_1\ X \subseteq [0, n)\}$$
$$= \{X \cap [0, n) : X \in M_2, n \in M_1\}$$

$\mathfrak{M} = \langle M_1, M_2, \dots \rangle \models \mathrm{VTC}^0$, $M_2 \subseteq \mathcal{P}(M_1)$
$\rightsquigarrow$ expands to many models of VTC^0_∞

- minimal: $\mathfrak{M}^\perp = \langle M_1, M_2^\perp, \dots \rangle$, $M_2^\perp =$ subsets of M_1 definable by $\mathbf{TC}^0$-formulas with parameters from M_2
- maximal: $\mathfrak{M}^\top = \langle M_1, M_2^\top, \dots \rangle$,

$$M_2^\top = \{X \subseteq M_1 : \forall n \in M_1\ X \cap [0, n) \in M_2\}$$

VTC^0_∞ is a conservative extension of VTC^0

Universal conservative extensions

In the spirit of Cook & Nguyen's $\widehat{\mathrm{VTC}}^0$ and $\overline{\mathrm{VTC}}^0$, we have

$\widehat{\mathrm{VTC}}^0_\infty$: new function symbols $\{u : \varphi(u, \vec{n}, \vec{X})\}$ for $\varphi \in \Sigma^B_0$, $\max(X \cap [0, n])$, $C(X)$: counting function for X

$\overline{\mathrm{VTC}}^0_\infty$: also $\{u : \varphi(u, \vec{n}, \vec{X})\}$ for $\varphi \in \Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty})$

- universally axiomatized, conservative over VTC^0_∞
- $\overline{\mathrm{VTC}}^0_\infty \vdash \Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty})$-comprehension, induction
- all $\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty}$-functions Δ^B_1-bit-definable in VTC^0_∞
  infinitary $\mathbf{TC}^0$ functions
- witnessing theorem: $\overline{\mathrm{VTC}}^0_\infty \vdash \forall \vec{n}, \vec{X}\, \exists \vec{m}, \vec{Y}\, \varphi(\vec{n}, \vec{X}, \vec{m}, \vec{Y})$, $\varphi \in \exists\Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty}) \implies$ there are $\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty}$-terms $\vec{t}$, $\vec{T}$ s.t.

$$\overline{\mathrm{VTC}}^0_\infty \vdash \forall \vec{n}, \vec{X}\, \varphi\big(\vec{n}, \vec{X}, \vec{t}(\vec{n}, \vec{X}), \vec{T}(\vec{n}, \vec{X})\big)$$

Working in VTC^0_∞

1. TC^0 arithmetic with infinite sets
2. **Working in** VTC^0_∞
3. Cauchy integral theorem

Objects encodable in VTC^0_∞

- Finite sets: a set X & a bound $n \rightsquigarrow X \cap [0, n)$
- Sequences of binary objects: $\{X_n\}_{n \in \mathbb{L}}$, $X_n \subseteq [0, n^c)$
  ($\mathbb{L}$ = unary/logarithmic integers, $c \in \mathbb{N}$ standard constant)
  encoded as $X_n = \{j < n^c : \langle n, j \rangle \in X\}$
- Real numbers: sequence of integers $a = \{A[n]\}_{n \in \mathbb{L}}$ s.t. $|A[n] - 2^{-m} A[n+m]| \leq 1$
  - represents $a = \lim_n 2^{-n} A[n]$
  - comparison: $a \leq b \iff \forall n \in \mathbb{L}\, A[n] \leq B[n] + 2$
  - complex numbers $z = x + iy$
- Double sequences $\{X_{n,m}\}_{n,m \in \mathbb{L}}$
  $\Longrightarrow$ real/complex sequences $\{a_n\}_{n \in \mathbb{L}}$
  $\Longrightarrow$ power series $f(z) = \sum_n a_n (z - w)^n$
- Analytic functions: sequence of power series (see later)

Polynomially Cauchy sequences

Real sequence $\{a_n\}_{n\in\mathbb{L}}$ encoded as double seq. $\{A_n[m]\}_{n,m\in\mathbb{L}}$

Polynomial modulus of Cauchyness:
$\forall n, m \geq p(k), r > k : \ |A_n[r] - A_m[r]| \leq 2^{r-k}$ for some poly p

$\Longrightarrow$ limit a in VTC^0_∞: $A[n] = \left\lfloor \frac{1}{16} A_{p(n+3)}[n+4] \right\rceil$

Applications:

- arithmetical operations $+, \cdot \ \Longrightarrow\ \mathbb{R}$ is an ordered field
  - more generally: $\{a_n\}_{n\in\mathbb{L}} \mapsto \left\{\sum_{n<N} a_n\right\}_{N\in\mathbb{L}}, \left\{\prod_{n<N} a_n\right\}_{N\in\mathbb{L}}$
  - adapting [J'15] to VTC^0_∞: $\mathbb{R}$ is a RCF, $\mathbb{C}$ ACF (wrt polynomials of standard degree)
- adapting [J'23]: VTC^0_∞ has well-behaved definitions of elementary analytic functions (exp, log, sin, arctan, ...)

Power series

Power series $f(z) = \sum_n a_n z^n$ represented by the seq. $\{a_n\}_{n\in\mathbb{L}}$

Convergence properties:

- $\sum_n a_n z^n$ converges for $|z| <^* r$ if $a_n = O(r^{-n})$
  $\{a_n z^n\}_{n\in\mathbb{L}}$ unbounded for $|z| \geq r$ if $a_n \neq O(r^{-n})$
- def.: $\sum_n a_n z^n$ has radius of convergence $\geq \varrho$
  if $a_n = O(r^{-n})$ for all $r <^* \varrho$
- $r <^* \varrho \implies$ converges polynomially uniformly on $B(0, r)$

Notation: $x <^* y \iff x \leq y(1 - m^{-1})$ for some $m \in \mathbb{L}$
$B^*(w, r) = \{z : |z - w| <^* r\}$

Operations on power series

Derivatives and primitive functions $f^{(n)}(z)$, $n \in \mathbb{Z}_{\mathbb{L}}$:

- explicit formula; same radius of convergence

$\sum_{n<N} f_n$: term-wise

$\prod_{n<N} f_n$, $f(g(z))$: $(g(0) = 0)$

- polynomials: evaluate at $\{e^{2\pi ij/m}\}_{j<m}$, interpolate (DFT)
- power series: apply to partial sums

Transfer: $f(z) = \sum_n a_n(z-u)^n \mapsto f_v(z) = \sum_n b_n(z-v)^n$

- f radius $\geq \varrho$, $v \in B^*(u, \varrho) \implies f_v$ radius $\geq \varrho - |v-u|$
- $|w-v| + |v-u| <^* \varrho \implies f(w) = f_v(w)$
  more generally: $f_w = (f_v)_w$

Analytic functions

$f : \Omega \to \mathbb{C}$ represented by $\{w_n, \varrho_n, b_n, a_{n,j}\}_{n,j \in \mathbb{L}}$ where

- $w_n, a_{n,j} \in \mathbb{C}$, $\rho_n, b_n \in \mathbb{Q}_{>0}$
- $|a_{n,j}| \leq b_n (3\rho_n)^{-j} \implies$
  $f_n(z) := \sum_j a_{n,j}(z - w_n)^j$ radius of convergence $\geq 3\varrho_n$
- domain $\Omega = \bigcup_n B^*(w_n, \varrho_n)$
- $w_m \in B^*(w_n, \varrho_n) \implies f_m = (f_n)_{w_m}$ (f_n transferred to w_m)

$z \in \Omega \implies f(z) := f_n(z)$ for any n s.t. $z \in B^*(w_n, \varrho_n)$

- independent of the choice of n
- more generally: $f_z := (f_n)_z$ also independent

Contour integration

Analytic function $f = \bigcup_n f_n$ as above,
$f_n(z) = \sum_j a_{n,j}(z - w_n)^j$ radius $\geq 3\varrho_n$

γ piecewise linear curve (contour) with endpoints $\{\gamma_j : j \leq \ell\}$

Define $\displaystyle\int_\gamma f(z)\,dz := \sum_{j<\tilde{\ell}} \big(F_{n_j}(\tilde{\gamma}_{j+1}) - F_{n_j}(\tilde{\gamma}_j)\big)$ if

- $\tilde{\gamma} \equiv \{\tilde{\gamma}_j : j \leq \tilde{\ell}\}$ subdivision of γ
- $\tilde{\gamma}_j, \tilde{\gamma}_{j+1} \in B^*(w_{n_j}, \varrho_{n_j})$ for each $j < \tilde{\ell}$
- $F_n =$ the primitive function of f_n

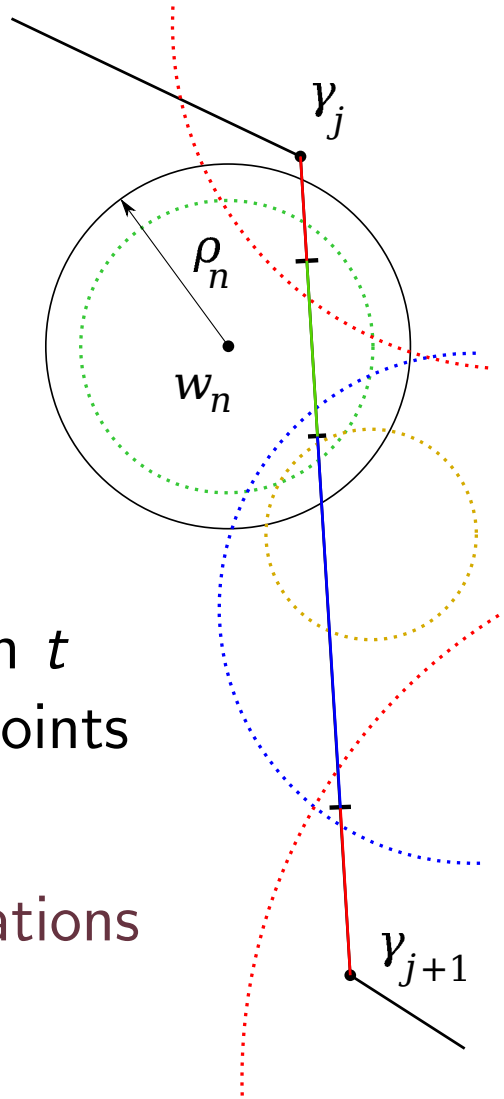
VTC^0_∞ proves

- uniqueness
- existence if γ covered by $\bigcup_{n<N} B^*(w_n, \varrho_n)$

Existence of integral

Goal: Assuming $\overline{\gamma_j\gamma_{j+1}} \subseteq \bigcup_{n<N} B^*(w_n, \varrho_n)$, subdivide it to segments each of which is covered by a specific $B^*(w_n, \varrho_n)$

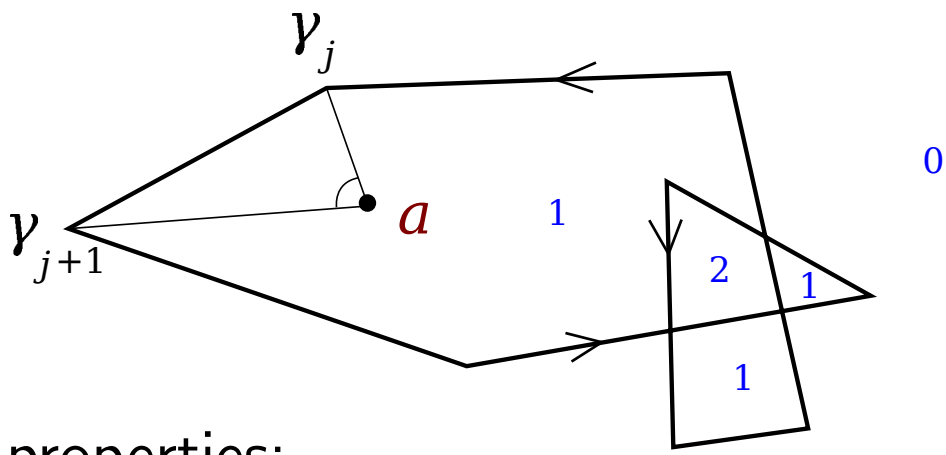
- idea: assign $z(t) = (1-t)\gamma_j + t\gamma_{j+1}$ to n with the best "fitness ratio" $\dfrac{|z(t) - w_n|}{\varrho_n}$
- $\dfrac{|z(t)-w_n|^2}{\varrho_n^2} \leq \dfrac{|z(t)-w_m|^2}{\varrho_m^2}$ quadratic inequality in t
  $\Longrightarrow$ holds on segments with explicit endpoints
- compute and sort the endpoints
- complication: need to work with approximations



Index (winding number)

$\gamma \equiv \{\gamma_j : j \leq \ell\}$ closed curve, $a \notin \mathrm{im}(\gamma) \implies$ index

$$\mathrm{Ind}_\gamma(a) = \frac{1}{2\pi} \sum_{j<\ell} \mathrm{Arg} \frac{\gamma_{j+1} - a}{\gamma_j - a} = \frac{1}{2\pi i} \int_\gamma \frac{dz}{z - a}$$



VTC^0_∞ proves expected properties:

- $\mathrm{Ind}_\gamma(a) \in \mathbb{Z}_{\mathbb{L}}$, constant on paths disjoint from γ
- 0 far away from γ, changes by 1 when crossing γ
- invariant under "small" perturbations of γ

Cauchy integral theorem

1. TC^0 arithmetic with infinite sets
2. Working in VTC^0_∞
3. **Cauchy integral theorem**

Cauchy integral theorem

Theorem (CIT) $f : \Omega \to \mathbb{C}$ analytic, $\mathrm{im}(\gamma) \subseteq \Omega$ closed curve:

$$\forall a \notin \Omega \ \mathrm{Ind}_\gamma(a) = 0 \implies \int_\gamma f(z)\, dz = 0$$

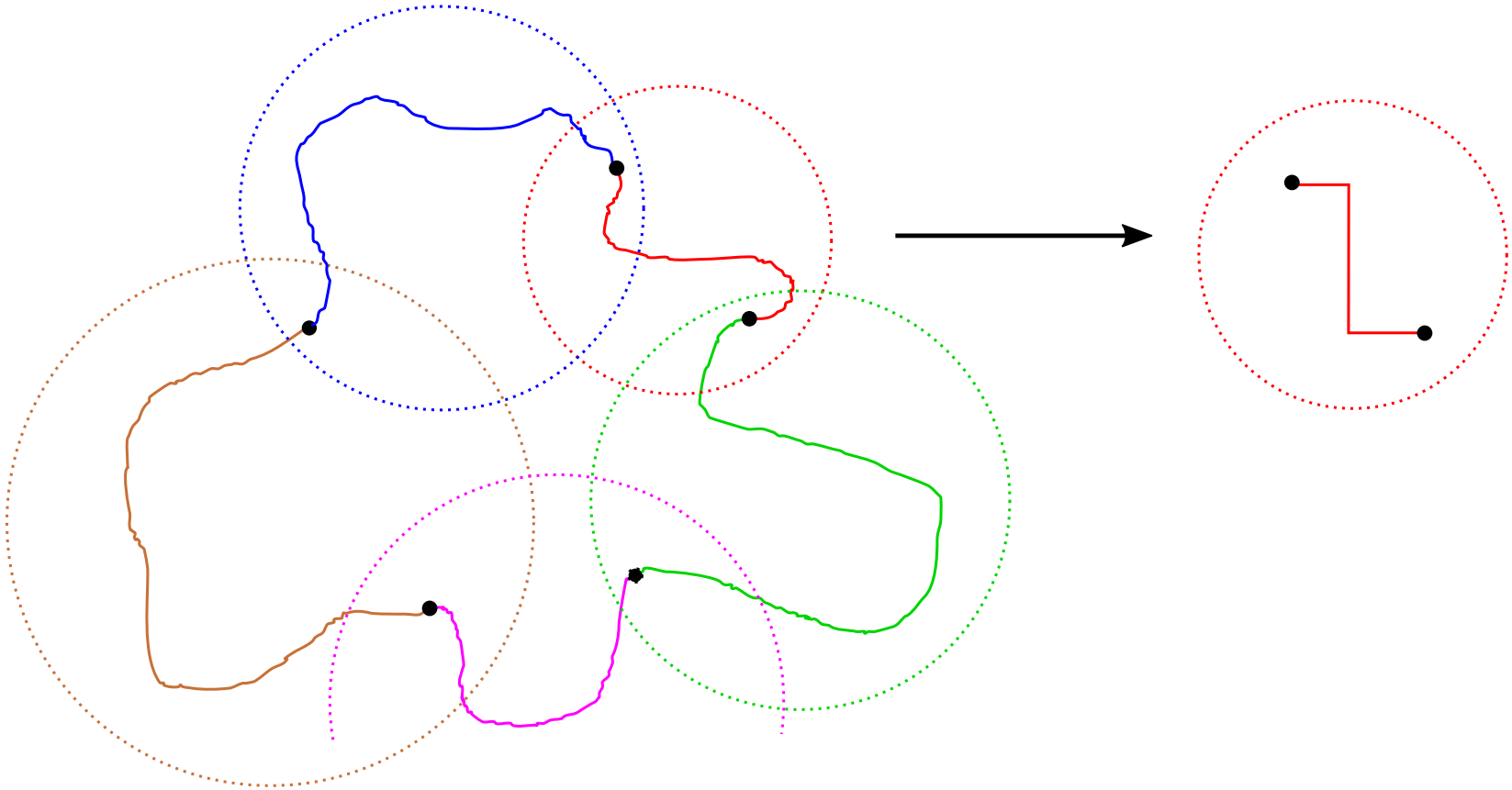
(γ doesn't go around any holes in Ω)

Main result: VTC^0_∞ proves CIT,
assuming Ω is covered by $\bigcup_{n<N} B^*(w_n, \varrho_n)$

- reduce to curves with axis-aligned segments
- reduce to a sum of rectangles
- cover rectangles using approximations of weighted Voronoi diagrams

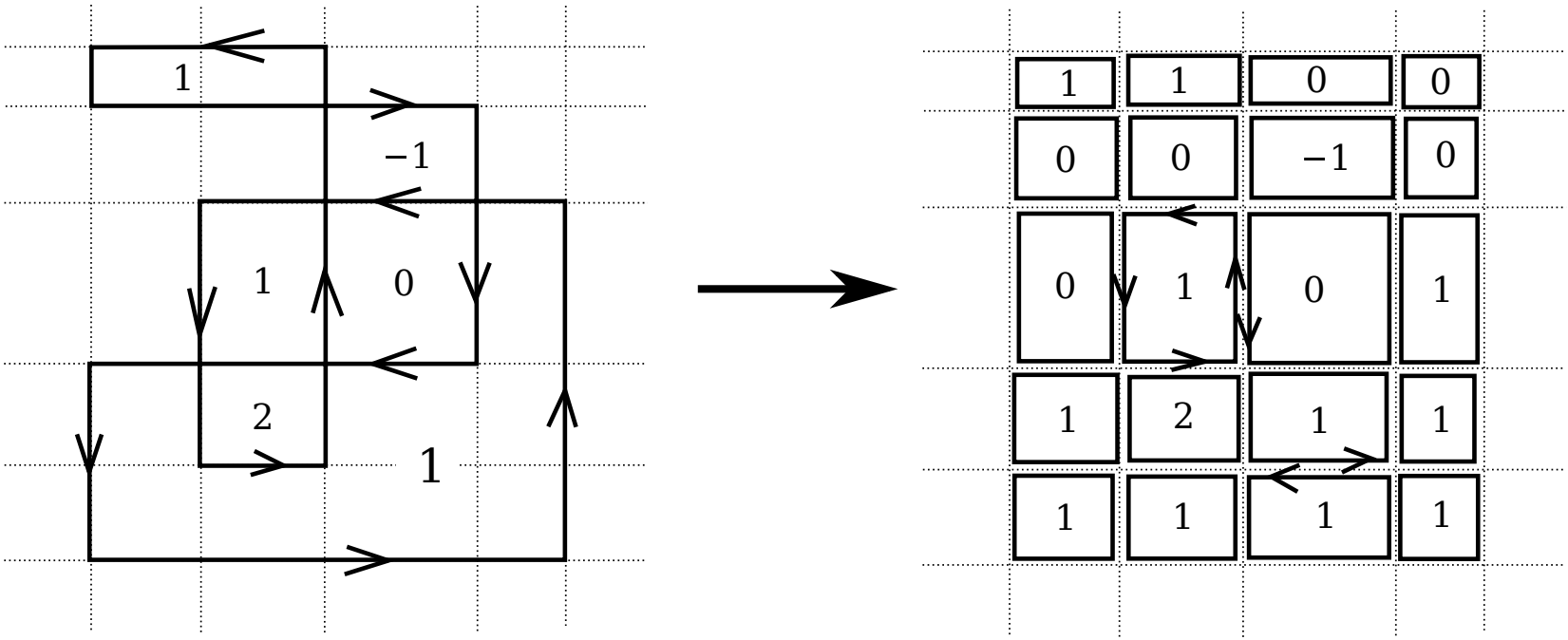
Axis-align the segments

- Subdivide γ to $\{\gamma_j : j \leq \ell\}$, $\gamma_j\gamma_{j+1} \subseteq B^*(w_{n_j}, \varrho_{n_j})$
- Replace $\gamma_j\gamma_{j+1}$ with 3 axis-aligned segments in $B^*(w_{n_j}, \varrho_{n_j})$
- Could even handle somewhat more complicated curves



Sum of rectangles

- Extend segments to lines $\Longrightarrow$ rectangular grid
- $\gamma \Longrightarrow$ sum of rectangles weighted by Ind_γ



CIT for rectangles

Goal: $\square \subseteq \bigcup_{n<N} B^*(w_n, \varrho_n) \implies$ split $\square$ into "simple" regions each of which is covered by a specific $B^*(w_n, \varrho_n)$

- 2D version of the "subdivide a segment" problem above
- Assigning each z to n with the best "fitness ratio"

$$\frac{|z - w_n|}{\varrho_n} \implies \text{weighted Voronoi diagram}$$

Voronoi diagrams

Points $\{w_n\}_{n<N} \rightsquigarrow$ partition plane into regions $\{V_n\}_{n<N}$:

$$V_n = \{z : |z - w_n| \,{}_{(\leq)}\, |z - w_m| \text{ for all } m\}$$

- convex polygons

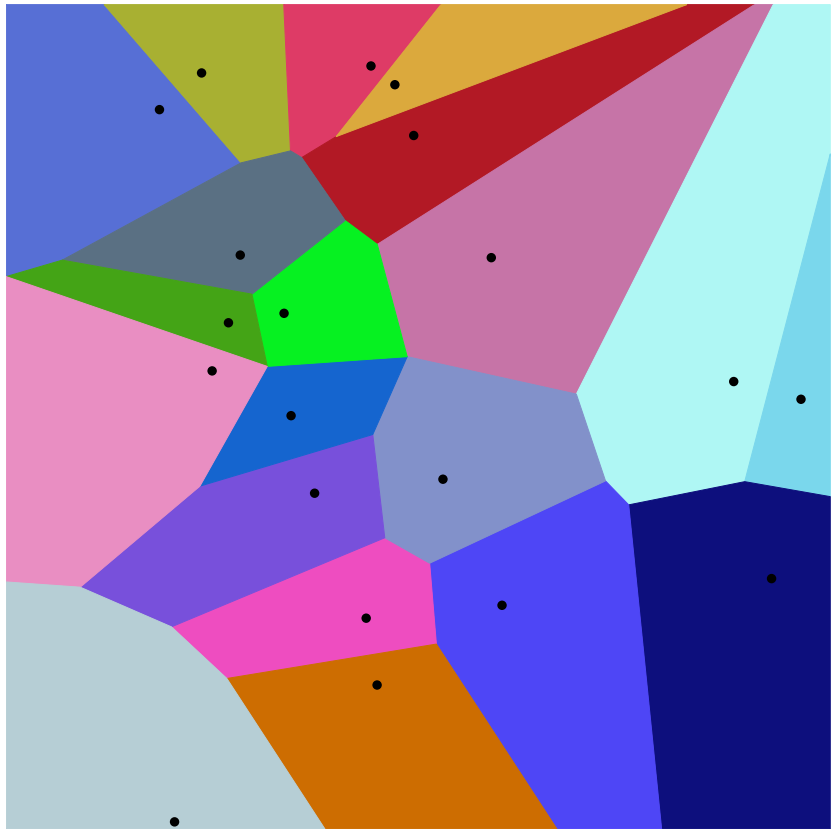


Image by Balu Ertl

https://commons.wikimedia.org/wiki/File:Euclidean_Voronoi_diagram.svg

Multiplicatively weighted Voronoi diagrams

Points $\{w_n\}_{n<N}$, weights $\{\varrho_n\}_{n<N} \rightsquigarrow$ regions $\{V_n\}_{n<N}$:

$$V_n = \left\{ z : \frac{|z - w_n|}{\varrho_n} \mathop{(\leq)} \frac{|z - w_m|}{\varrho_m} \text{ for all } m \right\}$$

- shapes bounded by circular arcs
$$\frac{|z - w_n|}{\varrho_n} = \frac{|z - w_m|}{\varrho_m}$$
- more complicated topology: non-convex, disconnected, may have holes

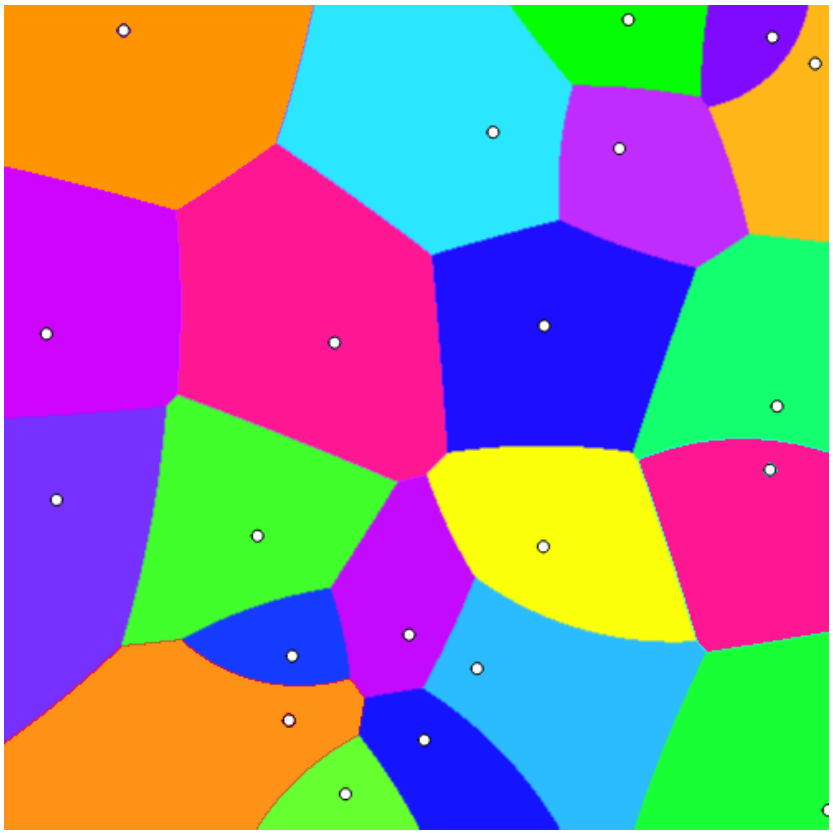


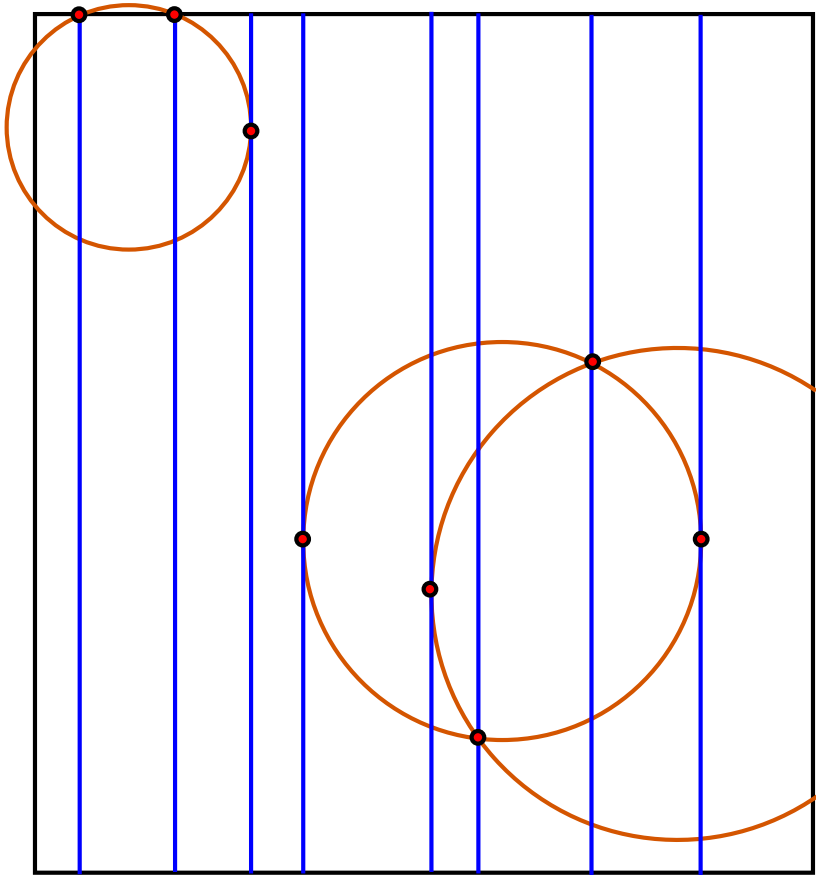
Image by SmallJarsWithGreenLabels
https://commons.wikimedia.org/wiki/File:Voronoi_AAAAA14.png

Split to strips

Given a $\square$ covered by $\bigcup_{n<N} B^*(w_n, \varrho_n)$:

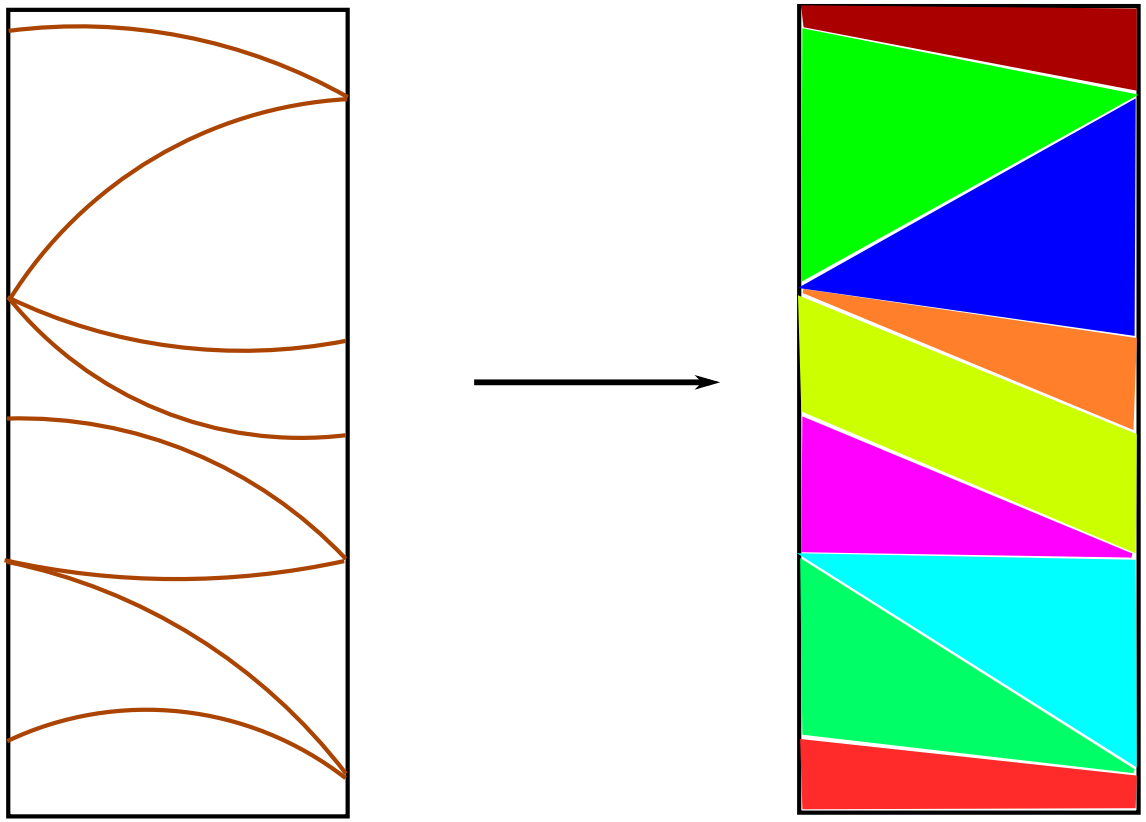
- Draw the Voronoi circles
  $$\frac{|z-w_n|}{\varrho_n} = \frac{|z-w_m|}{\varrho_m}$$
- Drop vertical lines from "interesting" points:
  - intersections of circles
  - intersections with boundary segments
  - vertical tangents

  $\Longrightarrow$ split $\square$ into vertical strips



On the strips

Voronoi arcs go from left to right, cannot intersect, can be straightened $\Longrightarrow$ ordered sum of triangles and trapezia each included in a single $B^*(w_n, \varrho_n)$



What's next?

Some goals to pursue:

- Meromorphic functions, calculus of residues, Cauchy's residue theorem
- Analytic continuation, Riemann surfaces
- Applications in combinatorics, number theory

References

- S. R. Buss: Bounded arithmetic, Bibliopolis, Naples, 1986
- S. Cook, P. Nguyen: Logical foundations of proof complexity, Cambridge Univ. Press, 2010
- A. M. Fernandes, F. Ferreira, G. Ferreira: Analysis in weak systems, in Logic and computation: Essays in honour of Amílcar Sernadas, College Publication, 2017, 231–262
- F. Ferreira: A feasible theory for analysis, J. Symb. Logic 59 (1994), 1001–1011
- F. Ferreira, G. Ferreira: The Riemann integral in weak systems of analysis, J. Univ. Computer Sci. 14 (2008), 908–937
- W. Hesse, E. Allender, D. M. Barrington: Uniform constant-depth threshold circuits for division and iterated multiplication, J. Comp. System Sci. 65 (2002), 695–716
- E. Jeřábek: Open induction in a bounded arithmetic for $\mathbf{TC}^0$, Arch. Math. Logic 54 (2015), 359–394
- E. Jeřábek: Iterated multiplication in VTC^0, Arch. Math. Logic 61 (2022), 705–767
- E. Jeřábek: Elementary analytic functions in VTC^0, Ann. Pure Appl. Logic 174 (2023), 103269
- P. Nguyen, S. Cook: Theories for TC^0 and other small complexity classes, Log. Methods Comput. Sci. 2 (2006), art. 3