Evaluating winding numbers through Cauchy indices in Isabelle/HOL

Wenda Li

University of Cambridge

wl302@cam.ac.uk

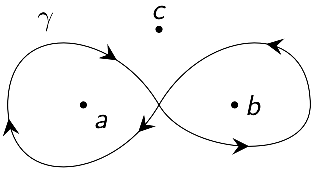
July 17, 2017

Contributions

- A novel tactic to evaluate a winding number through Cauchy indices.
- Novel verified procedures to count the number of complex roots of a polynomial in some domain (e.g. a rectangle, a half plane).

What is a winding number?

- The winding number $n(\gamma, z_0)$ is the number of times the path γ travels counterclockwise about the point z_0.



For example, $n(\gamma, a) = -1$, $n(\gamma, b) = 1$ and $n(\gamma, c) = 0$.

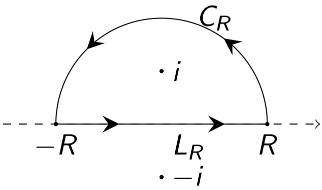
Formally, we can have

$$n(\gamma, z) = \frac{1}{2\pi i} \oint_\gamma \frac{dw}{w - z}.$$

A motivating example

To evaluate an improper integral:

$$\int_{-\infty}^{\infty} \frac{dx}{x^2+1}$$



Let

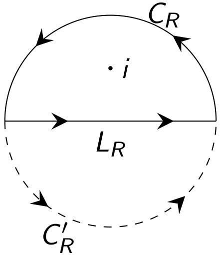
$$C_R(t) = Re^{it} \qquad \text{for} \quad t \in [0, \pi]$$
$$L_R(t) = (1-t)(-R) + tR \qquad \text{for} \quad t \in [0, 1]$$
$$\gamma = L_R + C_R,$$

$$\int_{-\infty}^{\infty} \frac{dx}{x^2+1} = \lim_{R\to\infty} \oint_{L_R+C_R} \frac{dx}{x^2+1}$$
$$= 2\pi i(\mathrm{Res}(\gamma, i)\boxed{n(\gamma, i)} + \mathrm{Res}(\gamma, -i)\boxed{n(\gamma, -i)}) = \pi$$

Previous proof for $n(L_R + C_R, i) = 1$

Let

$$C'_R(t) = Re^{it} \quad \text{for } t \in [\pi, 2\pi].$$



As $C_R + C'_R$ is a circular path, we have

$$n(C_R + C'_R, i) = 1$$

Moreover, we can show that $C_R + C'_R$ and $L_R + C_R$ are homotopic on $\mathbb{C} - \{i\}$, hence

$$n(L_R + C_R, i) = n(C_R + C'_R, i) = 1$$

which concludes the proof.

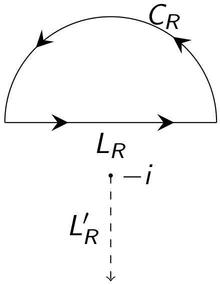
Previous proof for $n(L_R + C_R, -i) = 0$

Let L'_R be a ray such that

$$L'_R(t) = (-i) - ti \quad \text{for } t \in [0, \infty).$$

We can then show that L'_R does not intersect with $L_R + C_R$, hence

$$|\operatorname{Re}(n(L_R + C_R, -i))| < 1.$$



Since $n(L_R + C_R, -i) \in \mathbb{Z}$, we have $n(L_R + C_R, -i) = 0$ and conclude the proof.

My previous proofs for $n(L_R + C_R, i) = 1$ and $n(L_R + C_R, -i) = 0$ are ad hoc and involve manual construction of auxiliary paths/rays.

Is there a more systematic/uniform approach?

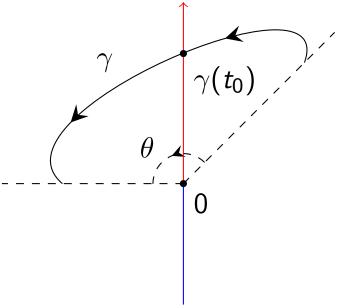
Approximate a winding number

Suppose we know that γ counterclockwise crosses the imaginary axis exactly once at $\gamma(t_0)$ such that $\text{Re}(\gamma(t_0)) > 0$. We then have

$$0 < \theta < 2\pi,$$

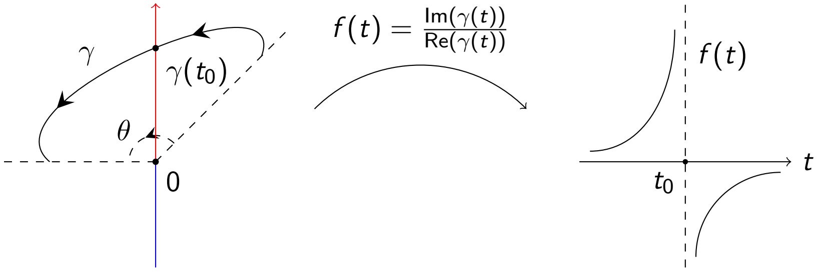
and hence

$$\text{Re}(n(\gamma, 0)) = \frac{\theta}{2\pi} \in (0, 1).$$



That is, we can approximate the real part of a winding number by the way it crosses the imaginary axis.

Approximate a winding number



$$\mathrm{jump}(f, x) = \begin{cases} -1 & \text{if } \lim_{u \to x^-} f(u) = \infty \text{ and } \lim_{u \to x^+} f(u) = -\infty \\ 1 & \text{if } \lim_{u \to x^-} f(u) = -\infty \text{ and } \lim_{u \to x^+} f(u) = \infty \\ 0 & \text{ otherwise} \end{cases}$$

Here, we have $\mathrm{jump}(f, t_0) = -1$.

The Cauchy index

By summing the jumps of f over some interval (a, b) we can define the Cauchy index $\mathsf{Ind}_a^b(f)$:

$$\mathsf{Ind}_a^b(f) = \sum_{x \in (a,b)} \mathrm{jump}(f, x),$$

which leads to a way to approximate $\mathsf{Re}(n(\gamma, z_0))$ for $\gamma : [a, b] \to \mathbb{C}$:

$$\left| \mathsf{Re}(n(\gamma, z_0)) + \frac{\mathsf{Ind}(\gamma, z_0)}{2} \right| < \frac{1}{2}.$$

where

$$f(t) = \frac{\mathsf{Im}(\gamma(t) - z_0)}{\mathsf{Re}(\gamma(t) - z_0)}$$

$$\mathsf{Ind}(\gamma, z_0) = \mathsf{Ind}_a^b(f)$$

.

Evaluating a winding number through the Cauchy indices

Given

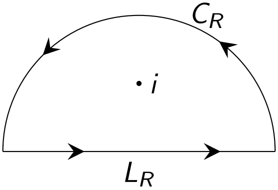
$$\left|\mathrm{Re}(n(\gamma, z_0)) + \frac{\mathrm{Ind}(\gamma, z_0)}{2}\right| < \frac{1}{2},$$

if we also know that γ is a loop, we have $n(\gamma, z_0) \in \mathbb{Z}$, hence

$$n(\gamma, z_0) = -\frac{\mathrm{Ind}(\gamma, z_0)}{2}$$

as $\mathrm{Ind}(\gamma, z_0) \in \mathbb{Z}$ by definition.

New proof for $n(L_R + C_R, i) = 1$



$$
\begin{aligned}
n(L_R + C_R, i) &= -\frac{\mathrm{Ind}(L_R + C_R, i)}{2} \\
&= -\frac{1}{2}(\mathrm{Ind}(L_R, i) + \mathrm{Ind}(C_R, i)) \\
&= -\frac{1}{2}((-1) + (-1)) \\
&= 1
\end{aligned}
$$

A tactic for $n(\gamma_1 + \gamma_2 + ... + \gamma_n, z_0) = k$

For the general cases, I have built a tactic to convert

$$n(\gamma_1 + \gamma_2 + ... + \gamma_n, z_0) = k$$

into

$$-\frac{1}{2}(\text{Ind}(\gamma_1, z_0) + \text{Ind}(\gamma_2, z_0) + ... + \text{Ind}(\gamma_n, z_0)) = k$$

where $\gamma_1 + \gamma_2 + ... + \gamma_n$ is a loop. When each γ_j is either a linear path

$$\gamma_j(t) = (1 - t)z_1 + tz_2 \quad \text{for } t \in [0, 1]$$

or part of a circular path

$$\gamma_j(t) = z + Re^{it} \quad \text{for } t \in [a, b],$$

deciding $\text{Ind}(\gamma_j, z_0)$ is usually straightforward.

Count the number of complex roots of a polynomial?

Thanks to the argument principle,

$$\frac{1}{2\pi i}\oint_{\gamma}\frac{p'(x)}{p(x)}dx = N$$

where γ is a loop, $p \in \mathbb{C}[x]$ and N is the number of complex roots of p counted with multiplicity inside the path γ.

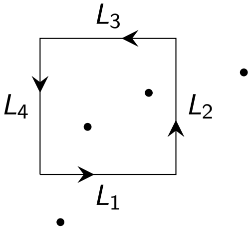
By the definition of winding numbers, we have

$$n(p \circ \gamma, 0) = \frac{1}{2\pi i}\oint_{\gamma}\frac{p'(x)}{p(x)}dx$$

hence

$$n(p \circ \gamma, 0) = N.$$

Deciding the number of complex roots in a rectangle



Let N be the number of complex roots of a polynomial p inside the rectangle path $L_1 + L_2 + L_3 + L_4$.

We have

$$N = n(p \circ (L_1 + L_2 + L_3 + L_4), 0)$$
$$= -\frac{1}{2}(\mathrm{Ind}(p \circ L_1, 0) + \mathrm{Ind}(p \circ L_2, 0) + \mathrm{Ind}(p \circ L_3, 0) + \mathrm{Ind}(p \circ L_4, 0))$$

Deciding the number of complex roots in a rectangle

Given $p \in \mathbb{C}[x]$ and a linear path $L : [0, 1] \to \mathbb{C}$, the path

$$p \circ L : [0, 1] \to \mathbb{C}$$

is neither a linear path nor part of a circular path. Can we still evaluate $\text{Ind}(p \circ L, 0)$?

Yes, thanks to the Sturm-Tarski theorem,

$$\text{Ind}(p \circ L, 0) = \mathrm{Var}(\mathrm{SRemS}(q_1, q_2; 0, 1))$$

where $q_1, q_2 \in \mathbb{R}[x]$ and

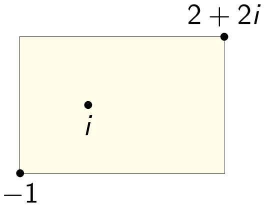
$$p \circ L(t) = q_1(t) + iq_2(t).$$

Deciding the number of complex roots in a rectangle

For example, to count the number of complex roots of the polynomial

$$p(x) = x^2 - 2ix - 1 = (x - i)^2$$

inside the rectangle defined by $(-1, 2 + 2i)$.

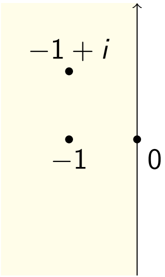


We can type the following command in Isabelle:

```
value "proots_rectangle [:-1,-2*ii,1:]
          (Complex (-1) 0) (Complex 2 2)"
```

which will return 2 as p has exactly two complex roots (i.e. i with multiplicity 2) within the rectangle box $(-1, 2 + 2i)$.

Deciding the number of complex roots in a half plane



Similarly, we can now use the following command

```
value "proots_half [:1-ii,2-ii,1:]
       0 (Complex 0 1)"
```

to decide that the polynomial

$$p(x) = x^2 + (2 - i)x + (1 - i) = (x + 1)(x + 1 - i)$$

has exactly two roots within the left-half plane of the imaginary axis.

- Routh-Hurwitz stability criterion

Remarks

- About 13000 LOC, 7 months.
- Subtleties (e.g. missing assumptions and corner cases) in almost every formulation of this problem.

Conclusion

In this talk, I have described:

- A tactic to evaluate a winding number through Cauchy indices;
- Verified procedures to count the number of complex roots.

Thanks for your attention.