

Program Verification in the presence of complex numbers, functions with branch cuts etc.

James Davenport (Bath)

Thanks to Russell Bradford, Acyr Locatelli, Gregory Sankaran and David Wilson (Bath) and Scott McCallum (Macquarie)

28 September 2012

Traditional Classification of Problems

blunder (of the coding variety) This is the sort of error traditionally addressed in “program verification”. Typically independent of the arithmetic.

blunder (of the coding variety) This is the sort of error traditionally addressed in “program verification”. Typically independent of the arithmetic.

parallelism Issues of deadlocks or races occurring due to the parallelism of an otherwise correct sequential program. Again, arithmetic-independent.

blunder (of the coding variety) This is the sort of error traditionally addressed in “program verification”. Typically independent of the arithmetic.

parallelism Issues of deadlocks or races occurring due to the parallelism of an otherwise correct sequential program. Again, arithmetic-independent.

numerical Do truncation and round-off errors, individually or combined, mean that the program computes approximations to the “true” answers which are out of tolerance.

Traditional Classification of Problems

How often are they considered?
Statistics from [CE05]

How often are they considered?

Statistics from [CE05]

blunder (of the coding variety) This is the sort of error

(83%) traditionally addressed in “program verification”.
Typically independent of the arithmetic.

parallelism Issues of deadlocks or races occurring due to the

(13%) parallelism of an otherwise correct sequential
program. Again, arithmetic-independent.

numerical Do truncation and round-off errors, individually or

(3%) combined, mean that the program computes
approximations to the “true” answers which are out
of tolerance.

Traditional Classification of Problems

How often are they considered?

Statistics from [CE05]

blunder (of the coding variety) This is the sort of error

(83%) traditionally addressed in “program verification”.
Typically independent of the arithmetic.

parallelism Issues of deadlocks or races occurring due to the

(13%) parallelism of an otherwise correct sequential
program. Again, arithmetic-independent.

numerical Do truncation and round-off errors, individually or

(3%) combined, mean that the program computes
approximations to the “true” answers which are out
of tolerance.

To this, I wish to add a fourth kind

“The bug that dares not speak its name”

manipulation A piece of algebra, which is “obviously correct”,
(0%!) turns out not to be correct when interpreted,

manipulation A piece of algebra, which is “obviously correct”,
(0%!) turns out not to be correct when interpreted, not as abstract algebra, but as the manipulation of functions $\mathbf{R} \rightarrow \mathbf{R}$ or $\mathbf{C} \rightarrow \mathbf{C}$.

A note on complex numbers

Most of our examples involve complex numbers, and people say
real programs don't use complex numbers

A note on complex numbers

Most of our examples involve complex numbers, and people say
real programs don't use complex numbers

However

Most of our examples involve complex numbers, and people say
real programs don't use complex numbers

However

- COMPLEX in Fortran II was the first computer data type not corresponding to a machine one

Most of our examples involve complex numbers, and people say
real programs don't use complex numbers

However

- COMPLEX in Fortran II was the first computer data type not corresponding to a machine one
- Even C99 introduced `_Complex`

Most of our examples involve complex numbers, and people say
real programs don't use complex numbers

However

- COMPLEX in Fortran II was the first computer data type not corresponding to a machine one
- Even C99 introduced `_Complex`
- Many examples, notably in fluid mechanics.

Flow in a slotted strip, transformed by

$$w = g(z) := 2 \operatorname{arccosh} \left(1 + \frac{2z}{3} \right) - \operatorname{arccosh} \left(\frac{5z + 12}{3(z + 4)} \right) \quad (1)$$

Kahan's example [Kah87]

Flow in a slotted strip, transformed by

$$w = g(z) := 2 \operatorname{arccosh} \left(1 + \frac{2z}{3} \right) - \operatorname{arccosh} \left(\frac{5z + 12}{3(z + 4)} \right) \quad (1)$$

Is this the same as

$$w \stackrel{?}{=} q(z) := 2 \operatorname{arccosh} \left(2(z + 3) \sqrt{\frac{z + 3}{27(z + 4)}} \right) ? \quad (2)$$

Kahan's example [Kah87]

Flow in a slotted strip, transformed by

$$w = g(z) := 2 \operatorname{arccosh} \left(1 + \frac{2z}{3} \right) - \operatorname{arccosh} \left(\frac{5z + 12}{3(z + 4)} \right) \quad (1)$$

Is this the same as

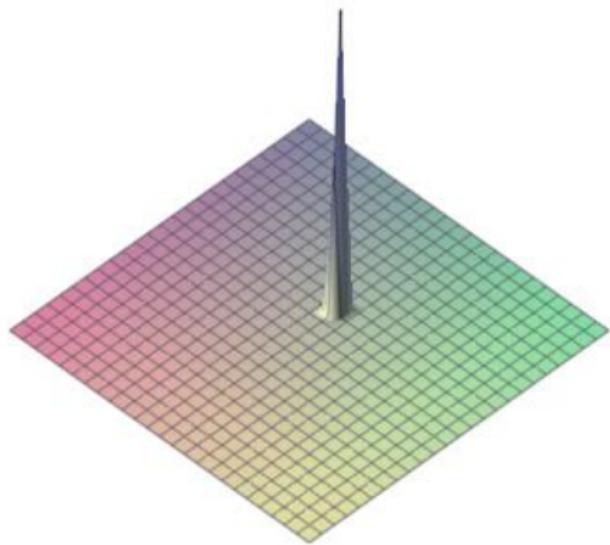
$$w \stackrel{?}{=} q(z) := 2 \operatorname{arccosh} \left(2(z + 3) \sqrt{\frac{z + 3}{27(z + 4)}} \right) ? \quad (2)$$

Or possibly

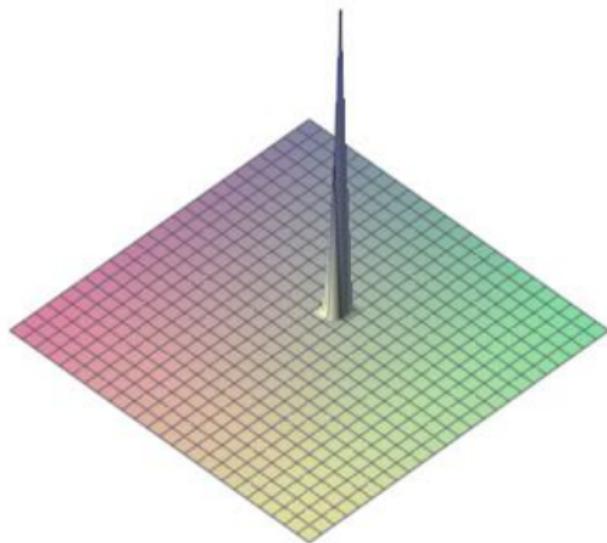
$$w = h(z) := 2 \ln \left(\frac{1}{3} \frac{\sqrt{3z + 12} (\sqrt{z + 3} + \sqrt{z})^2}{2\sqrt{z + 3} + \sqrt{z}} \right) ? \quad (3)$$

$g - q$ might look OK

$g - q$ might look OK

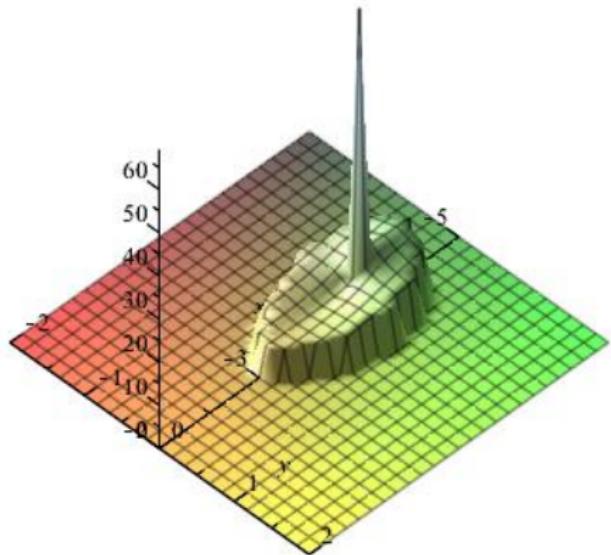


$g - q$ might look OK



“OK apart from a slight glitch.”

But if we look closer



Definitely not OK

But, in fact $g = h$

But, in fact $g = h$

Most computer algebra systems (these days!) will refuse to
“simplify” g to q

But, in fact $g = h$

Most computer algebra systems (these days!) will refuse to
“simplify” g to q

But will also refuse to simplify g to h .

But, in fact $g = h$

Most computer algebra systems (these days!) will refuse to “simplify” g to q

But will also refuse to simplify g to h .

Indeed Maple's `coulditbe(g<>h)` ; returns `true`, which *ought* to indicate that there is a counter-example.

But, in fact $g = h$

Most computer algebra systems (these days!) will refuse to “simplify” g to h

But will also refuse to simplify g to h .

Indeed Maple's `coulditbe(g<>h)` ; returns `true`, which *ought* to indicate that there is a counter-example.

$$\begin{aligned} \frac{d(g-h)}{dz} = & 2 \left(\sqrt{\frac{z}{z+4}} \sqrt{\frac{z+3}{z+4}} z^{3/2} - 2 z^{3/2} + 2 \sqrt{z+3} \sqrt{\frac{z}{z+4}} \right. \\ & \left. \sqrt{\frac{z+3}{z+4}} z - z \sqrt{z+3} + 4 \sqrt{\frac{z}{z+4}} \sqrt{\frac{z+3}{z+4}} \sqrt{z} + 8 \sqrt{z+3} \sqrt{\frac{z}{z+4}} \right. \\ & \left. \sqrt{\frac{z+3}{z+4}} - 6 \sqrt{z} \right) \frac{1}{\sqrt{z+3}} \frac{1}{\sqrt{z}} \frac{1}{\sqrt{\frac{z}{z+4}}} \frac{1}{\sqrt{\frac{z+3}{z+4}}} (z+4)^{-2} \left(2 \sqrt{z+3} + \sqrt{z} \right)^{-1} \end{aligned}$$

But, in fact $g = h$

Most computer algebra systems (these days!) will refuse to “simplify” g to h

But will also refuse to simplify g to h .

Indeed Maple's `coulditbe(g<>h)`; returns `true`, which *ought* to indicate that there is a counter-example.

$$\begin{aligned} \frac{d(g-h)}{dz} = & 2 \left(\sqrt{\frac{z}{z+4}} \sqrt{\frac{z+3}{z+4}} z^{3/2} - 2 z^{3/2} + 2 \sqrt{z+3} \sqrt{\frac{z}{z+4}} \right. \\ & \left. \sqrt{\frac{z+3}{z+4}} z - z \sqrt{z+3} + 4 \sqrt{\frac{z}{z+4}} \sqrt{\frac{z+3}{z+4}} \sqrt{z} + 8 \sqrt{z+3} \sqrt{\frac{z}{z+4}} \right. \\ & \left. \sqrt{\frac{z+3}{z+4}} - 6 \sqrt{z} \right) \frac{1}{\sqrt{z+3}} \frac{1}{\sqrt{z}} \frac{1}{\sqrt{\frac{z}{z+4}}} \frac{1}{\sqrt{\frac{z+3}{z+4}}} (z+4)^{-2} \left(2 \sqrt{z+3} + \sqrt{z} \right)^{-1} \end{aligned}$$

and it's a bold person who would say “ $= 0$ ”

Challenges

Challenge (1)

Demonstrate automatically that g and q are not equal, by producing a z at which they give different results.

Challenge (1)

Demonstrate automatically that g and q are not equal, by producing a z at which they give different results.

The technology described in [BBDP07] will isolate the curve

$y = \pm \sqrt{\frac{(x+3)^2(-2x-9)}{2x+5}}$ as a potential obstacle (it is the branch cut of q), but the geometry questions are too hard for a fully-automated solution at the moment.

Challenge (1)

Demonstrate automatically that g and q are not equal, by producing a z at which they give different results.

The technology described in [BBDP07] will isolate the curve

$y = \pm \sqrt{\frac{(x+3)^2(-2x-9)}{2x+5}}$ as a potential obstacle (it is the branch cut of q), but the geometry questions are too hard for a fully-automated solution at the moment.

Challenge (2)

Demonstrate automatically that g and h are equal.

Challenge (1)

Demonstrate automatically that g and q are not equal, by producing a z at which they give different results.

The technology described in [BBDP07] will isolate the curve

$y = \pm \sqrt{\frac{(x+3)^2(-2x-9)}{2x+5}}$ as a potential obstacle (it is the branch cut of q), but the geometry questions are too hard for a fully-automated solution at the moment.

Challenge (2)

Demonstrate automatically that g and h are equal.

Again, the technology in [BBDP07], implemented in a mixture of Maple and QEPCAD, could in principle do this

Joukowski (a)

Consider the Joukowski map [Hen74, pp. 294–298]:

$$f : z \mapsto \frac{1}{2} \left(z + \frac{1}{z} \right). \quad (4)$$

Lemma

f is injective as a function from $D := \{z : |z| > 1\}$.

Consider the Joukowski map [Hen74, pp. 294–298]:

$$f : z \mapsto \frac{1}{2} \left(z + \frac{1}{z} \right). \quad (4)$$

Lemma

f is injective as a function from $D := \{z : |z| > 1\}$.

This is also a function $\mathbf{R}^2 \rightarrow \mathbf{R}^2$:

$$f_R : (x, y) \mapsto \left(\frac{1}{2} x + \frac{1}{2} \frac{x}{x^2 + y^2}, \frac{1}{2} y - \frac{1}{2} \frac{y}{x^2 + y^2} \right) \quad (5)$$

Challenge (3)

Demonstrate automatically that f_R is injective, i.e.

$$\begin{aligned} \forall x_1 \forall x_2 \forall y_1 \forall y_2 \quad & \left(x_1^2 + y_1^2 > 1 \wedge x_2^2 + y_2^2 > 1 \wedge \right. \\ x_1 + \frac{x_1}{x_1^2 + y_1^2} &= x_2 + \frac{x_2}{x_2^2 + y_2^2} \quad \wedge \quad y_1 - \frac{y_1}{x_1^2 + y_1^2} = y_2 - \frac{y_2}{x_2^2 + y_2^2} \\ \Rightarrow & \left. (x_1 = x_2 \wedge y_1 = y_2) \right). \end{aligned} \tag{6}$$

Challenge (3)

Demonstrate automatically that f_R is injective, i.e.

$$\begin{aligned} \forall x_1 \forall x_2 \forall y_1 \forall y_2 \quad & \left(x_1^2 + y_1^2 > 1 \wedge x_2^2 + y_2^2 > 1 \wedge \right. \\ x_1 + \frac{x_1}{x_1^2 + y_1^2} &= x_2 + \frac{x_2}{x_2^2 + y_2^2} \quad \wedge \quad y_1 - \frac{y_1}{x_1^2 + y_1^2} = y_2 - \frac{y_2}{x_2^2 + y_2^2} \\ \Rightarrow & \left. (x_1 = x_2 \wedge y_1 = y_2) \right). \end{aligned} \tag{6}$$

We have failed to do this automatically, but Brown can reformulate manually then solve in QEPCAD (< 12 seconds)

Joukowski challenge (a1)

Challenge (3)

Demonstrate automatically that f_R is injective, i.e.

$$\begin{aligned} \forall x_1 \forall x_2 \forall y_1 \forall y_2 \quad & \left(x_1^2 + y_1^2 > 1 \wedge x_2^2 + y_2^2 > 1 \wedge \right. \\ x_1 + \frac{x_1}{x_1^2 + y_1^2} &= x_2 + \frac{x_2}{x_2^2 + y_2^2} \quad \wedge \quad y_1 - \frac{y_1}{x_1^2 + y_1^2} = y_2 - \frac{y_2}{x_2^2 + y_2^2} \\ \Rightarrow & \left. (x_1 = x_2 \wedge y_1 = y_2) \right). \end{aligned} \tag{6}$$

We have failed to do this automatically, but Brown can reformulate manually then solve in QEPCAD (< 12 seconds)

Challenge (4)

Automate these techniques and transforms.

So it's a bijection: what's the inverse?

Joukowski challenge (a2)

So it's a bijection: what's the inverse?

Figure: Maple's solve on inverting Joukowski

```
> [solve(zeta = 1/2*(z+1/z), z)];  
[ $\zeta + \sqrt{\zeta^2 - 1}, \zeta - \sqrt{\zeta^2 - 1}$ ]
```

The only challenge might be the choice implicit in the \pm symbol:
which do we choose?

Joukowski challenge (a2)

So it's a bijection: what's the inverse?

Figure: Maple's solve on inverting Joukowski

```
> [solve(zeta = 1/2*(z+1/z), z)];  
[ $\zeta + \sqrt{\zeta^2 - 1}, \zeta - \sqrt{\zeta^2 - 1}$ ]
```

The only challenge might be the choice implicit in the \pm symbol: which do we choose? Unfortunately, the answer is “neither”, or at least “neither, uniformly”.

Joukowski challenge (a2 continued)

$$f_1(\zeta) = \zeta \begin{cases} +\sqrt{\zeta^2 - 1} & \Im(\zeta) > 0 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) < 0 \\ +\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) > 1 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) < -1 \end{cases} \quad (7)$$

Joukowski challenge (a2 continued)

$$f_1(\zeta) = \zeta \begin{cases} +\sqrt{\zeta^2 - 1} & \Im(\zeta) > 0 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) < 0 \\ +\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) > 1 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) < -1 \end{cases} \quad (7)$$

In fact, a better (at least, free of case distinctions) definition is

$$f_2(\zeta) = \zeta + \sqrt{\zeta - 1} \sqrt{\zeta + 1}. \quad (8)$$

Joukowski challenge (a2 continued)

$$f_1(\zeta) = \zeta \begin{cases} +\sqrt{\zeta^2 - 1} & \Im(\zeta) > 0 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) < 0 \\ +\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) > 1 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) < -1 \end{cases} \quad (7)$$

In fact, a better (at least, free of case distinctions) definition is

$$f_2(\zeta) = \zeta + \sqrt{\zeta - 1} \sqrt{\zeta + 1}. \quad (8)$$

The techniques of [BBDP07] are able to **verify** (8), in the sense of showing that $f_2(f(z)) - z$ is the zero function on $\{z : |z| > 1\}$.

Joukowski challenge (a2 continued)

$$f_1(\zeta) = \zeta \begin{cases} +\sqrt{\zeta^2 - 1} & \Im(\zeta) > 0 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) < 0 \\ +\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) > 1 \\ -\sqrt{\zeta^2 - 1} & \Im(\zeta) = 0 \wedge \Re(\zeta) < -1 \end{cases} \quad (7)$$

In fact, a better (at least, free of case distinctions) definition is

$$f_2(\zeta) = \zeta + \sqrt{\zeta - 1} \sqrt{\zeta + 1}. \quad (8)$$

The techniques of [BBDP07] are able to **verify** (8), in the sense of showing that $f_2(f(z)) - z$ is the zero function on $\{z : |z| > 1\}$.

Challenge (5)

Derive automatically, and demonstrate the validity of, either (7) or (8). In terms of Maple, this would be ...

Joukowski challenge (a2 continued)

Figure: **Bad:** Maple's actual solve on inverting injective Joukowski

```
> [solve(zeta = 1/2*(z+1/z), z)] assuming abs(z) > 1
      
$$\left[ \zeta + \sqrt{\zeta^2 - 1}, \zeta - \sqrt{\zeta^2 - 1} \right]$$

```

Joukowski challenge (a2 continued)

Figure: **Bad:** Maple's actual solve on inverting injective Joukowski

```
> [solve(zeta = 1/2*(z+1/z), z)] assuming abs(z) > 1
      
$$\left[ \zeta + \sqrt{\zeta^2 - 1}, \zeta - \sqrt{\zeta^2 - 1} \right]$$

```

Figure: **Good:** Ideal Maple solve on inverting injective Joukowski

```
> solve(zeta = 1/2*(z+1/z), z) assuming abs(z) > 1
      
$$\zeta + \sqrt{\zeta - 1} \sqrt{\zeta + 1}$$

```

Joukowski challenge (a2 continued)

Figure: **Bad:** Maple's actual solve on inverting injective Joukowski

```
> [solve(zeta = 1/2*(z+1/z), z)] assuming abs(z) > 1
      
$$\left[ \zeta + \sqrt{\zeta^2 - 1}, \zeta - \sqrt{\zeta^2 - 1} \right]$$

```

Figure: **Good:** Ideal Maple solve on inverting injective Joukowski

```
> solve(zeta = 1/2*(z+1/z), z) assuming abs(z) > 1
      
$$\zeta + \sqrt{\zeta - 1} \sqrt{\zeta + 1}$$

```

As far as I can tell (supported by the documentation), Maple ignores the “assuming” as it’s on the codomain, not the domain.

Lemma

f is injective as a function from $H := \{z : \Im z > 0\}$.

Lemma

f is injective as a function from $H := \{z : \Im z > 0\}$.

Challenge (6)

Demonstrate automatically the truth of

$$\begin{aligned} & \forall x_1 \forall x_2 \forall y_1 \forall y_2 \quad \left(y_1 > 0 \wedge y_2 > 0 \wedge \right. \\ & x_1 + \frac{x_1}{x_1^2 + y_1^2} = x_2 + \frac{x_2}{x_2^2 + y_2^2} \quad \wedge \quad y_1 - \frac{y_1}{x_1^2 + y_1^2} = y_2 - \frac{y_2}{x_2^2 + y_2^2} \\ & \quad \Rightarrow \quad (x_1 = x_2 \wedge y_1 = y_2). \end{aligned} \tag{9}$$

Joukowski (b) challenge

Lemma

f is injective as a function from $H := \{z : \Im z > 0\}$.

Challenge (6)

Demonstrate automatically the truth of

$$\begin{aligned} \forall x_1 \forall x_2 \forall y_1 \forall y_2 \quad & \left(y_1 > 0 \wedge y_2 > 0 \wedge \right. \\ x_1 + \frac{x_1}{x_1^2 + y_1^2} = x_2 + \frac{x_2}{x_2^2 + y_2^2} \quad & \wedge \quad y_1 - \frac{y_1}{x_1^2 + y_1^2} = y_2 - \frac{y_2}{x_2^2 + y_2^2} \left. \right) \\ \Rightarrow \quad & (x_1 = x_2 \wedge y_1 = y_2). \end{aligned} \tag{9}$$

Brown's ideas probably apply here as well, but this is unproven

So it's a bijection: what's the inverse?

So it's a bijection: what's the inverse?

[Hen74, (5.1-13), p. 298] argues for

$$f_3(\zeta) = \zeta + \underbrace{\sqrt{\zeta - 1}}_{\arg \in (-\pi/2, \pi/2)} - \underbrace{\sqrt{\zeta + 1}}_{\arg \in (0, \pi]}. \quad (10)$$

Joukowski (b) challenge continued

So it's a bijection: what's the inverse?

[Hen74, (5.1-13), p. 298] argues for

$$f_3(\zeta) = \zeta + \underbrace{\sqrt{\zeta - 1}}_{\arg \in (-\pi/2, \pi/2)} - \underbrace{\sqrt{\zeta + 1}}_{\arg \in (0, \pi]}. \quad (10)$$

Challenge (7)

Find a way to represent functions such as $\underbrace{\sqrt{\zeta + 1}}_{\arg \in (0, \pi]}$

Alternative formulations

Fortunately this one is soluble in this case, we can write

Fortunately this one is soluble in this case, we can write

$$\underbrace{\sqrt{\zeta + 1}}_{\arg \in (0, \pi]} = i \quad \underbrace{\sqrt{-\zeta - 1}}_{\arg \in (-\pi/2, \pi/2)} ,$$

Fortunately this one is soluble in this case, we can write

$$\underbrace{\sqrt{\zeta + 1}}_{\arg \in (0, \pi]} = i \underbrace{\sqrt{-\zeta - 1}}_{\arg \in (-\pi/2, \pi/2)},$$

so we have an inverse function

$$f_4(\zeta) = \zeta + \sqrt{\zeta - 1}i\sqrt{-\zeta - 1}. \quad (11)$$

Alternative formulations

Fortunately this one is soluble in this case, we can write

$$\underbrace{\sqrt{\zeta + 1}}_{\arg \in (0, \pi]} = i \underbrace{\sqrt{-\zeta - 1}}_{\arg \in (-\pi/2, \pi/2)},$$

so we have an inverse function

$$f_4(\zeta) = \zeta + \sqrt{\zeta - 1}i\sqrt{-\zeta - 1}. \quad (11)$$

Challenge (8)

Demonstrate automatically that this is an inverse to f on $\{z : \Im z > 0\}$.

Why is this so hard? (1) — CAD

Why is this so hard? (1) — CAD

The first truly algorithmic approach is ten years old ([BCD⁺02], refined in [BBDP07]), and has various difficulties.

Why is this so hard? (1) — CAD

The first truly algorithmic approach is ten years old ([BCD⁺02], refined in [BBDP07]), and has various difficulties.

At its core is the use of Cylindrical Algebraic Decomposition of \mathbf{R}^N to find the connected components of $\mathbf{C}^{N/2} \setminus \{\text{branch cuts}\}$. The complexity of this is doubly exponential in N : upper bound of $d^{O(2^N)}$ and lower bounds of $2^{2^{(N-1)/3}}$.

Why is this so hard? (1) — CAD

The first truly algorithmic approach is ten years old ([BCD⁺02], refined in [BBDP07]), and has various difficulties.

At its core is the use of Cylindrical Algebraic Decomposition of \mathbf{R}^N to find the connected components of $\mathbf{C}^{N/2} \setminus \{\text{branch cuts}\}$. The complexity of this is doubly exponential in N : upper bound of $d^{O(2^N)}$ and lower bounds of $2^{2^{(N-1)/3}}$.

While better algorithms are in principle known ($d^{O(N\sqrt{N})}$), we do not know of any accessible implementations.

Why is this so hard? (1) — CAD

The first truly algorithmic approach is ten years old ([BCD⁺02], refined in [BBDP07]), and has various difficulties.

At its core is the use of Cylindrical Algebraic Decomposition of \mathbf{R}^N to find the connected components of $\mathbf{C}^{N/2} \setminus \{\text{branch cuts}\}$. The complexity of this is doubly exponential in N : upper bound of $d^{O(2^N)}$ and lower bounds of $2^{2^{(N-1)/3}}$.

While better algorithms are in principle known ($d^{O(N\sqrt{N})}$), we do not know of any accessible implementations.

Furthermore, we are clearly limited to small values of N , at which point looking at $O(\dots)$ complexity is of limited use. We note that the cross-over point between $2^{(N-1)/3}$ and $N\sqrt{N}$ is at $N = 21$.

Why is this so hard? (1) — CAD

The first truly algorithmic approach is ten years old ([BCD⁺02], refined in [BBDP07]), and has various difficulties.

At its core is the use of Cylindrical Algebraic Decomposition of \mathbf{R}^N to find the connected components of $\mathbf{C}^{N/2} \setminus \{\text{branch cuts}\}$. The complexity of this is doubly exponential in N : upper bound of $d^{O(2^N)}$ and lower bounds of $2^{2^{(N-1)/3}}$.

While better algorithms are in principle known ($d^{O(N\sqrt{N})}$), we do not know of any accessible implementations.

Furthermore, we are clearly limited to small values of N , at which point looking at $O(\dots)$ complexity is of limited use. We note that the cross-over point between $2^{(N-1)/3}$ and $N\sqrt{N}$ is at $N = 21$.

A more detailed comparison is given in [Hon91]. Hence there is a need for practical research on low- N Cylindrical Algebraic Decomposition.

Why is this so hard? (1) — CAD continued

While the fundamental branch cut of \log is simple enough, being $\{z = x + iy \mid y = 0 \wedge x < 0\}$, actual branch cuts are messier. Part of the branch cut of (2) is

$$2x^3 + 21x^2 + 72x + 2xy^2 + 5y^2 + 81 = 0 \wedge \text{other conditions, (12)}$$

whose solution accounts for the curious boundary of the bad region.

While the fundamental branch cut of \log is simple enough, being $\{z = x + iy \mid y = 0 \wedge x < 0\}$, actual branch cuts are messier. Part of the branch cut of (2) is

$$2x^3 + 21x^2 + 72x + 2xy^2 + 5y^2 + 81 = 0 \wedge \text{other conditions, (12)}$$

whose solution accounts for the curious boundary of the bad region. While there has been some progress in manipulating such images of half-lines (described in Phisanbut's Bath PhD), there is almost certainly more to be done.

Why is this so hard? (2) — Injectivity

Lemmas 1, 2 are statements about complex functions of one variable, so why do we need statements about four real variables to prove them? There are three reasons.

Why is this so hard? (2) — Injectivity

Lemmas 1, 2 are statements about complex functions of one variable, so why do we need statements about four real variables to prove them? There are three reasons.

- ① The statements require the $|\cdot|$ or \Im functions, neither of which are **C** analytic functions. Hence some recourse to **R** (twice as many variables) seems inevitable (proof?)

Why is this so hard? (2) — Injectivity

Lemmas 1, 2 are statements about complex functions of one variable, so why do we need statements about four real variables to prove them? There are three reasons.

- ① The statements require the $|\cdot|$ or \Im functions, neither of which are **C** analytic functions. Hence some recourse to **R** (twice as many variables) seems inevitable (proof?)
- ② Equations (6) and (9) are the direct translations of the basic definition of injectivity. In practice, certainly if we were looking at functions $\mathbf{R} \rightarrow \mathbf{R}$, we would want to use the fact that the function concerned was continuous.

Why is this so hard? (2) — Injectivity

Lemmas 1, 2 are statements about complex functions of one variable, so why do we need statements about four real variables to prove them? There are three reasons.

- ① The statements require the $|\cdot|$ or \Im functions, neither of which are **C** analytic functions. Hence some recourse to **R** (twice as many variables) seems inevitable (proof?)
- ② Equations (6) and (9) are the direct translations of the basic definition of injectivity. In practice, certainly if we were looking at functions $\mathbf{R} \rightarrow \mathbf{R}$, we would want to use the fact that the function concerned was continuous.

Challenge (9)

Find a better formulation of injectivity questions $\mathbf{R}^N \rightarrow \mathbf{R}^N$, making use of the properties of the functions concerned (certainly continuity, possibly rationality).

- 1 While these injectivity equations are statements from the existential theory of the reals, and so the theoretically more efficient algorithms quoted in [Hon91] are in principle applicable, the more modern developments described in [PJ09] do not seem to be directly applicable. However, we can transform them into a disjunction of statements to each of which the Weak Positivstellensatz [PJ09, Theorem 1] is applicable.

- 1 While these injectivity equations are statements from the existential theory of the reals, and so the theoretically more efficient algorithms quoted in [Hon91] are in principle applicable, the more modern developments described in [PJ09] do not seem to be directly applicable. However, we can transform them into a disjunction of statements to each of which the Weak Positivstellensatz [PJ09, Theorem 1] is applicable.

Challenge (10)

Solve these problems using the techniques of [PJ09],

Bibliography

-  J.C. Beaumont, RJB, JHD, and N. Phisanbut.
Testing Elementary Function Identities Using CAD.
AAECC, 18:513–543, 2007.
-  RJB, R.M. Corless, JHD, D.J. Jeffrey, and S.M. Watt.
Reasoning about the Elementary Functions of Complex Analysis.
Ann. Math. Artificial Intelligence, 36:303–318, 2002.
-  R. Cousot (Ed.).
Verification, Model Checking, and Abstract Interpretation.
Springer Lecture Notes in Computer Science 3385, 2005.
-  P. Henrici.
Applied and Computational Complex Analysis I. *Wiley*, 1974.
-  H. Hong. Comparison of several decision algorithms for the existential theory of the reals. *RISC Technical Report* 91-41, 1991.
-  W. Kahan. Branch Cuts for Complex Elementary Functions.
Proc. The State of Art in Numerical Analysis, pages 165–211, 1987.
-  G.O. Passmore and P.B. Jackson.
Combined Decision Techniques for the Existential Theory of the Reals. *Proc. Intelligent Computer Mathematics*, pages 122–137,