DSLM: Presenting Mathematical Analysis Using Functional Programming

Cezar Ionescu
cezar@chalmers.se

Patrik Jansson
patrikj@chalmers.se

Paper + talk: `https://github.com/DSLsofMath/tfpie2015`

Style example

$$\forall\ \epsilon\ \in\ \mathbb{R}.\ \ (\epsilon > 0)\ \Rightarrow\ \exists\ a\ \in\ A.\ \ (|a - sup\ A| < \epsilon)$$

Background

Domain-Specific Languages of Mathematics [Ionescu and Jansson, 2015]: is a course currently developed at Chalmers in response to difficulties faced by third-year students in learning and applying classical mathematics (mainly real and complex analysis)

Main idea: encourage students to approach mathematical domains from a functional programming perspective (similar to Wells [1995]).

> "... ideally, the course would improve the mathematical education of computer scientists and the computer science education of mathematicians."

Introduction

- make functions and types explicit
- use types as carriers of semantic information, not just variable names
- introduce functions and types for implicit operations such as the power series interpretation of a sequence
- use a calculational style for proofs
- organize the types and functions in DSLs

Not working code, rather working understanding of concepts

Complex numbers

We begin by defining the symbol i, called **the imaginary unit**, to have the property

$$i^2 = -1$$

Thus, we could also call i the square root of -1 and denote it $\sqrt{-1}$. Of course, i is not a real number; no real number has a negative square.

(Adams and Essex [2010], Appendix I)

Complex numbers

We begin by defining the symbol i, called **the imaginary unit**, to have the property

$$i^2 = -1$$

Thus, we could also call i the square root of -1 and denote it $\sqrt{-1}$. Of course, i is not a real number; no real number has a negative square.

(Adams and Essex [2010], Appendix I)

data $I = i$

Complex numbers

Definition: A **complex number** is an expression of the form

$$a + bi \qquad \text{or} \qquad a + ib,$$

where a and b are real numbers, and i is the imaginary unit.

Complex numbers

Definition: A **complex number** is an expression of the form

$$a + bi \qquad \text{or} \qquad a + ib,$$

where a and b are real numbers, and i is the imaginary unit.

$$\begin{aligned} \textbf{data}\ \mathit{Complex} &= \mathit{Plus}_1\ \mathbb{R}\ \mathbb{R}\ I \\ &\mid\ \mathit{Plus}_2\ \mathbb{R}\ I\ \mathbb{R} \end{aligned}$$

$$\begin{aligned} \mathit{show} : \mathit{Complex} &\rightarrow \mathit{String} \\ \mathit{show}\ (\mathit{Plus}_1\ x\ y\ i) &= \mathit{show}\ x \mathbin{+\!\!+} \texttt{" + "} \mathbin{+\!\!+} \mathit{show}\ y \mathbin{+\!\!+} \texttt{"i"} \\ \mathit{show}\ (\mathit{Plus}_2\ x\ i\ y) &= \mathit{show}\ x \mathbin{+\!\!+} \texttt{" + "} \mathbin{+\!\!+} \texttt{"i"} \mathbin{+\!\!+} \mathit{show}\ y \end{aligned}$$

Complex numbers examples

Definition: A **complex number** is an expression of the form

$$a + bi \qquad \text{or} \qquad a + ib,$$

where a and b are real numbers, and i is the imaginary unit.

For example, $3 + 2\,i$, $\frac{7}{2} - \frac{2}{3}\,i$, $i\,\pi \;=\; 0 + i\,\pi$, and $-3 \;=\; -3 + 0\,i$ are all complex numbers. The last of these examples shows that every real number can be regarded as a complex number.

Complex numbers examples

For example, $3 + 2\ i$, $\frac{7}{2} - \frac{2}{3}\ i$, $i\ \pi\ =\ 0 + i\ \pi$, and $-3\ =\ -3 + 0\ i$ are all complex numbers. The last of these examples shows that every real number can be regarded as a complex number.

$$
\begin{aligned}
\textbf{data}\ \mathit{Complex}\ &=\ \mathit{Plus}_1\ \mathbb{R}\ \mathbb{R}\ I \\
&\mid\ \ \mathit{Plus}_2\ \mathbb{R}\ I\ \mathbb{R}
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{toComplex}\ :\ \mathbb{R}\ \rightarrow\ \mathit{Complex} \\
&\mathit{toComplex}\ x\ =\ \mathit{Plus}_1\ x\ 0\ i
\end{aligned}
$$

- what about i by itself?
- what about, say, $2\ i$?

Complex numbers version 2.0

(We will normally use $a + bi$ unless b is a complicated expression, in which case we will write $a + ib$ instead. Either form is acceptable.)

$$\textbf{data}\ \mathit{Complex}\ =\ \mathit{Plus}\ \mathbb{R}\ \mathbb{R}\ \mathit{I}$$

$$\textbf{data}\ \mathit{Complex}\ =\ \mathit{PlusI}\ \mathbb{R}\ \mathbb{R}$$

Name and reuse

It is often convenient to represent a complex number by a single letter; w and z are frequently used for this purpose. If a, b, x, and y are real numbers, and $w = a + bi$ and $z = x + yi$, then we can refer to the complex numbers w and z. Note that $w = z$ if and only if $a = x$ and $b = y$.

$$\textbf{newtype}\ \mathit{Complex} = C\ (\mathbb{R}, \mathbb{R})$$

Equality and pattern-matching

Definition: If $z = x + yi$ is a complex number (where x and y are real), we call x the **real part** of z and denote it $Re\ (z)$. We call y the **imaginary part** of z and denote it $Im\ (z)$:

$$\begin{aligned} Re\ (z) &= Re\ (x + yi) = x \\ Im\ (z) &= Im\ (x + yi) = y \end{aligned}$$

$$\begin{aligned} &Re : Complex && \rightarrow \mathbb{R} \\ &Re\ z@(C\ (x,\ y)) && = x \end{aligned}$$

$$\begin{aligned} &Im : Complex && \rightarrow \mathbb{R} \\ &Im\ z@(C\ (x,\ y)) && = y \end{aligned}$$

Shallow vs. deep embeddings

The sum and difference of complex numbers

If $w = a + bi$ and $z = x + yi$, where a, b, x, and y are real numbers, then

$$\begin{aligned} w + z &= (a + x) + (b + y)\, i \\ w - z &= (a - x) + (b - y)\, i \end{aligned}$$

Shallow embedding:

$$(+) : \mathit{Complex} \to \mathit{Complex} \to \mathit{Complex}$$
$$(C\ (a,\ b)) + (C\ (x,\ y)) = C\ ((a + x),\ (b + y))$$
$$\textbf{newtype}\ \mathit{Complex} = C\ (\mathbb{R},\ \mathbb{R})$$

Shallow vs. deep embeddings

The sum and difference of complex numbers

If $w = a + bi$ and $z = x + yi$, where a, b, x, and y are real numbers, then

$$\begin{aligned} w + z &= (a + x) + (b + y)\, i \\ w - z &= (a - x) + (b - y)\, i \end{aligned}$$

Deep embedding (buggy):

$$\begin{aligned} (+) &: \mathit{Complex} \to \mathit{Complex} \to \mathit{Complex} \\ (+) &= \mathit{Plus} \end{aligned}$$

$$\begin{aligned} \textbf{data}\ \mathit{ComplexDeep} \ = \ & i \\ \mid \ & \mathit{ToComplex}\ \mathbb{R} \\ \mid \ & \mathit{Plus}\ \ \ \mathit{Complex}\ \mathit{Complex} \\ \mid \ & \mathit{Times}\ \mathit{Complex}\ \mathit{Complex} \\ \mid \ & \ldots \end{aligned}$$

The sum and difference of complex numbers
If $w = a + bi$ and $z = x + yi$, where a, b, x, and y are real numbers, then

$$\begin{aligned} w + z &= (a + x) + (b + y)\,i \\ w - z &= (a - x) + (b - y)\,i \end{aligned}$$

Deep embedding:

$$\begin{aligned} (+) &: \mathit{Complex} \to \mathit{Complex} \to \mathit{Complex} \\ (+) &= \mathit{Plus} \end{aligned}$$

$$\begin{aligned} \textbf{data}\ \mathit{Complex} &= i \\ &\mid\ \mathit{ToComplex}\ \mathbb{R} \\ &\mid\ \mathit{Plus}\ \ \mathit{Complex}\ \mathit{Complex} \\ &\mid\ \mathit{Times}\ \mathit{Complex}\ \mathit{Complex} \\ &\mid\ \ldots \end{aligned}$$

Completeness property of $\mathbb{R}$

Next: start from a more "mathematical" quote from the book:

> The *completeness* property of the real number system is more subtle and difficult to understand. One way to state it is as follows: if A is any set of real numbers having at least one number in it, and if there exists a real number y with the property that $x \leqslant y$ for every $x \in A$ (such a number y is called an **upper bound** for A), then there exists a smallest such number, called the **least upper bound** or **supremum** of A, and denoted *sup* (A). Roughly speaking, this says that there can be no holes or gaps on the real line—every point corresponds to a real number.

(Adams and Essex [2010], page 4)

Min ("smallest such number")

Specification (not implementation)

$$
\begin{aligned}
min &: \mathcal{P}^{+}\,\mathbb{R} \to \mathbb{R} \\
min\ A = x &\iff x \in A \wedge (\forall\, a \in A.\ x \leqslant a)
\end{aligned}
$$

Example consequence (which will be used later):

If $y < min\ A$, *then* $y \notin A$.

Upper bounds

$$
\begin{aligned}
ubs &: \mathcal{P}\,\mathbb{R} \to \mathcal{P}\,\mathbb{R} \\
ubs\ A &= \{x \mid x \in \mathbb{R},\ x \text{ upper bound of } A\} \\
&= \{x \mid x \in \mathbb{R},\ \forall\, a \in A.\ \ a \leqslant x\}
\end{aligned}
$$

The completeness axiom can be stated as

Assume an $A : \mathcal{P}^{+}\,\mathbb{R}$ with an upper bound $u \in ubs\ A$.
Then $s = sup\ A = min\ (ubs\ A)$ exists.

where

$$
\begin{aligned}
sup &: \mathcal{P}^{+}\,\mathbb{R} \to \mathbb{R} \\
sup &= min \circ ubs
\end{aligned}
$$

Completeness and "gaps"

Assume an $A : \mathcal{P}^{+}\,\mathbb{R}$ *with an upper bound* $u \in ubs\ A$.
Then $s = sup\ A = min\ (ubs\ A)$ *exists.*

But s need not be in A — could there be a "gap"?

Completeness and "gaps"

Assume an $A : \mathcal{P}^+ \, \mathbb{R}$ *with an upper bound* $u \in ubs \, A$.
Then $s = sup \, A = min \, (ubs \, A)$ *exists.*

But s need not be in A — could there be a "gap"?
With "gap" = "an ϵ-neighbourhood between A and s" we can can show there is no "gap".

A proof: Completeness implications step-by-step

$$\begin{array}{ll} & \epsilon > 0 \\ \Rightarrow & \{ \text{arithmetic} \} \\ & s - \epsilon < s \end{array}$$

A proof: Completeness implications step-by-step

$$
\begin{array}{ll}
 & \epsilon > 0 \\
\Rightarrow & \quad \{ \text{ arithmetic } \} \\
 & s - \epsilon < s \\
\Rightarrow & \quad \{ \, s \; = \; \mathit{min} \; (\mathit{ubs} \; A), \text{ property of } \mathit{min} \, \} \\
 & s - \epsilon \; \notin \; \mathit{ubs} \; A
\end{array}
$$

A proof: Completeness implications step-by-step

$$\epsilon > 0$$

$\Rightarrow$ { arithmetic }

$$s - \epsilon < s$$

$\Rightarrow$ { $s = \mathit{min}\ (\mathit{ubs}\ A)$, property of min }

$$s - \epsilon \notin \mathit{ubs}\ A$$

$\Rightarrow$ { set membership }

$$\neg \forall a \in A.\ a \leqslant s - \epsilon$$

A proof: Completeness implications step-by-step

$$
\begin{array}{ll}
& \epsilon > 0 \\
\Rightarrow & \{ \text{arithmetic} \} \\
& s - \epsilon < s \\
\Rightarrow & \{ s = \mathit{min}\ (\mathit{ubs}\ A), \text{property of } \mathit{min} \} \\
& s - \epsilon \notin \mathit{ubs}\ A \\
\Rightarrow & \{ \text{set membership} \} \\
& \neg \forall a \in A.\ a \leqslant s - \epsilon \\
\Rightarrow & \{ \text{quantifier negation} \} \\
& \exists a \in A.\ s - \epsilon < a
\end{array}
$$

A proof: Completeness implications step-by-step

$$
\begin{array}{ll}
& \epsilon > 0 \\
\Rightarrow & \{ \text{arithmetic} \} \\
& s - \epsilon < s \\
\Rightarrow & \{ s = \mathit{min}\ (\mathit{ubs}\ A), \text{ property of } \mathit{min} \} \\
& s - \epsilon \notin \mathit{ubs}\ A \\
\Rightarrow & \{ \text{set membership} \} \\
& \neg \forall\, a \in A.\ a \leqslant s - \epsilon \\
\Rightarrow & \{ \text{quantifier negation} \} \\
& \exists\, a \in A.\ s - \epsilon < a \\
\Rightarrow & \{ \text{definition of upper bound} \} \\
& \exists\, a \in A.\ s - \epsilon < a \leqslant s
\end{array}
$$

A proof: Completeness implications step-by-step

$$
\begin{array}{ll}
 & \epsilon > 0 \\
\Rightarrow & \quad \{ \text{arithmetic} \} \\
 & s - \epsilon < s \\
\Rightarrow & \quad \{ s \; = \; \mathit{min}\ (\mathit{ubs}\ A), \text{ property of } \mathit{min} \} \\
 & s - \epsilon \notin \mathit{ubs}\ A \\
\Rightarrow & \quad \{ \text{set membership} \} \\
 & \neg \forall\ a \in A.\ \ a \leqslant s - \epsilon \\
\Rightarrow & \quad \{ \text{quantifier negation} \} \\
 & \exists\ a \in A.\ \ s - \epsilon < a \\
\Rightarrow & \quad \{ \text{definition of upper bound} \} \\
 & \exists\ a \in A.\ \ s - \epsilon < a \leqslant s \\
\Rightarrow & \quad \{ \text{absolute value} \} \\
 & \exists\ a \in A.\ \ (|a - s| < \epsilon)
\end{array}
$$

Completeness: proof interpretation (“no gaps”)

To sum up the proof says that the completeness axiom implies:

$$\mathit{proof} \;:\; \forall\, \epsilon \,\in\, \mathbb{R}.\;\; (\epsilon > \mathit{0}) \;\Rightarrow\; \exists\, a \,\in\, A.\;\; (|a - \mathit{sup}\ A| < \epsilon)$$

Completeness: proof interpretation ("no gaps")

To sum up the proof says that the completeness axiom implies:

$$\mathit{proof} : \forall\, \epsilon \in \mathbb{R}.\ (\epsilon > 0) \Rightarrow \exists\, a \in A.\ (|a - \mathit{sup}\ A| < \epsilon)$$

More detail:

Assume a non-empty $A : \mathcal{P}\,\mathbb{R}$ with an upper bound $u \in \mathit{ubs}\ A$.
Then $s = \mathit{sup}\ A = \mathit{min}\,(\mathit{ubs}\ A)$ exists.
We know that s need not be in A — could there be a "gap"?

Completeness: proof interpretation ("no gaps")

To sum up the proof says that the completeness axiom implies:

$$\mathit{proof} \;:\; \forall\, \epsilon \,\in\, \mathbb{R}.\;\; (\epsilon > 0) \;\Rightarrow\; \exists\, a \,\in\, A.\;\; (|a - \mathit{sup}\; A| < \epsilon)$$

More detail:

Assume a non-empty $A \;:\; \mathcal{P}\,\mathbb{R}$ with an upper bound $u \,\in\, \mathit{ubs}\; A$.
Then $s \;=\; \mathit{sup}\; A \;=\; \mathit{min}\,(\mathit{ubs}\; A)$ exists.
We know that s need not be in A — could there be a "gap"?
No, *proof* will give us an $a \,\in\, A$ arbitrarily close to the supremum.
So, there is no "gap".

Conclusions

- make functions and types explicit: $Re : Complex \to \mathbb{R}$, $min : \mathcal{P}^{+} \mathbb{R} \to \mathbb{R}$
- use types as carriers of semantic information, not just variable names
- introduce functions and types for implicit operations such as $toComplex : \mathbb{R} \to Complex$
- use a calculational style for proofs
- organize the types and functions in DSLs (for *Complex*, limits, power series, etc.)

Future work

Partial implementation in Agda:

- errors caught by formalization (but no "royal road")
  - *ComplexDeep*
  - *choice* function
- subsets and coercions
  - $\epsilon : \mathbb{R}_{>0}$, different type from $\mathbb{R}_{\geq 0}$ and $\mathbb{R}$ and $\mathbb{C}$
  - what is the type of $|\cdot|$? ($\mathbb{C} \to \mathbb{R}_{\geq 0}$?)
  - other subsets of $\mathbb{R}$ or $\mathbb{C}$ are common, but closure properties unclear

Bibliography

R. A. Adams and C. Essex. *Calculus: a complete course*. Pearson Canada, 7th edition, 2010.

C. Ionescu and P. Jansson. Domain-specific languages of mathematics, 2015. URL https://www.student.chalmers.se/sp/course?course_id=24179. Course plan for DAT325, Chalmers University of Technology.

C. Wells. Communicating mathematics: Useful ideas from computer science. *American Mathematical Monthly*, pages 397–408, 1995.