Why a “pointfree” (PF) transform

J.N. Oliveira

Dept. Informática,
Universidade do Minho
Braga, Portugal

DI/UM, 2007

Formal methods

Adopting a **formal** notation instead of some programming notation (language) doesn't mean by itself that one is following a formal approach:

- formal models involve **conditions** which lead to
- **proof obligations** that need to be discharged

As in other branches of engineering

$$e = m + c$$

that is,

engineering = *model first, then calculate* ...

Calculate? Verify?

We know how to **calculate** since the school desk...

Formal methods

Adopting a **formal** notation instead of some programming notation (language) doesn't mean by itself that one is following a formal approach:

- formal models involve **conditions** which lead to
- **proof obligations** that need to be discharged

As in other branches of engineering

$$e = m + c$$

that is,

engineering = *model first, then calculate* ...

Calculate? Verify?

We know how to **calculate** since the school desk...

Formal methods

Adopting a **formal** notation instead of some programming notation (language) doesn't mean by itself that one is following a formal approach:

- formal models involve **conditions** which lead to
- **proof obligations** that need to be discharged

As in other branches of engineering

$$e = m + c$$

that is,

$$\textit{engineering} = \underline{\textit{model}} \textit{ first, then } \underline{\textit{calculate}} \ldots$$

Calculate? Verify?

We know how to **calculate** since the school desk...

Problem-solving strategy

Recall the *universal problem solving* strategy which one is taught at school:

- **understand** your problem
- build a mathematical **model** of it
- **reason** in such a model
- upgrade your model, if necessary
- **calculate** a final solution and implement it.

School maths example

The problem

My three children were born at a 3 year interval rate. Altogether, they are as old as me. I am 48. How old are they?

The model

$$x + (x+3) + (x+6) = 48$$

The calculation

$$
\begin{aligned}
& 3x + 9 = 48 \\
\equiv & \quad \{ \text{ "al-djabr" rule } \} \\
& 3x = 48 - 9 \\
\equiv & \quad \{ \text{ "al-hatt" rule } \} \\
& x = 16 - 3
\end{aligned}
$$

School maths example

The problem

My three children were born at a 3 year interval rate. Altogether, they are as old as me. I am 48. How old are they?

The model

$$x + (x + 3) + (x + 6) = 48$$

The calculation

$$
\begin{array}{cl}
 & 3x + 9 = 48 \\
\equiv & \{ \text{“al-djabr” rule} \} \\
 & 3x = 48 - 9 \\
\equiv & \{ \text{“al-hatt” rule} \} \\
 & x = 16 - 3
\end{array}
$$

School maths example

The problem

My three children were born at a 3 year interval rate. Altogether, they are as old as me. I am 48. How old are they?

The model

$$x + (x+3) + (x+6) = 48$$

The calculation

$$\begin{array}{cl} & 3x + 9 = 48 \\ \equiv & \{ \text{ ``al-djabr'' rule } \} \\ & 3x = 48 - 9 \\ \equiv & \{ \text{ ``al-hatt'' rule } \} \\ & x = 16 - 3 \end{array}$$

School maths example

The solution

$$\begin{aligned} x &= 13 \\ x+3 &= 16 \\ x+6 &= 19 \end{aligned}$$

Questions....

- "al-djabr" rule ?
- "al-hatt" rule ?

Have a look at Pedro Nunes (1502-1578) *Libro de Algebra en Arithmetica y Geometria* (dated 1567) ...

School maths example

The solution

$$\begin{aligned} x &= 13 \\ x+3 &= 16 \\ x+6 &= 19 \end{aligned}$$

Questions....

- "al-djabr" rule ?
- "al-hatt" rule ?

Have a look at Pedro Nunes (1502-1578) *Libro de Algebra en Arithmetica y Geometria* (dated 1567) ...

School maths example

The solution

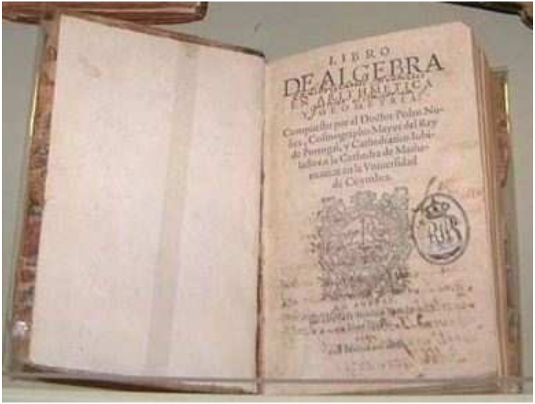
$$\begin{aligned} x &= 13 \\ x + 3 &= 16 \\ x + 6 &= 19 \end{aligned}$$

Questions....

- "al-djabr" rule ?
- "al-hatt" rule ?

Have a look at Pedro Nunes (1502-1578) *Libro de Algebra en Arithmetica y Geometria* (dated 1567) ...

Libro de Algebra en Arithmetica y Geometria (1567)



(...) the inventor of this art was a Moorish mathematician, whose name was Gebre, & in some libraries there is a small arabic treaty which contains chapters that we use
(fol. a ij r)

Reference to *On the calculus of al-gabr and al-muqâbala* by Abû Al-Huwârizmî, a famous 9c Persian mathematician.

Calculus of al-gabr, al-hatt and al-muqâbala

al-djabr

$$x - z \leq y \quad \equiv \quad x \leq y + z$$

al-hatt

$$x * z \leq y \quad \equiv \quad x \leq y * z^{-1} \qquad\qquad (z > 0)$$

al-muqâbala

Ex: $$4x^2 - 2x^2 = 2x + 6 - 3 \quad \equiv \quad 2x^2 = 2x + 3$$

Back to geometry and trigonometry . . .

Hot topic in the 16c: revisit old geometrical problems, inc. Euclid's Elements.

Problem 12 in Johan Müller's (1436-1476) *"De Triangulis"*, vol.II

Given

$$\begin{aligned} bc &= 20 \\ ad &= 5 \\ \frac{ab}{ac} &= \sqrt{5} \end{aligned}$$

find ab, ac and bd.

This is Question 46 in Nunes book (fol. 270r), given as example of problem which Müller could not solve on pure geometric grounds. . .

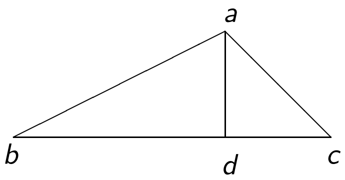
Back to geometry and trigonometry ...

Hot topic in the 16c: revisit old geometrical problems, inc. Euclid's Elements.

Problem 12 in Johan Müller's (1436-1476) *"De Triangulis"*, vol.II

Given

$$\begin{aligned} bc &= 20 \\ ad &= 5 \\ \frac{ab}{ac} &= \sqrt{5} \end{aligned}$$



find ab, ac and bd.

This is Question 46 in Nunes book (fol. 270r), given as example of problem which Müller could not solve on pure geometric grounds...

... solved "by algebra"

Nunes model is based on the *inuento Pithagorico* [1]:

Model

(...) Queriendo pos conoscer los lados (...) pornemos .d.c. parte menor ser .1.co. [read: $x = dc$, where *co* is "cousa" = "the thing" (we are looking for)] *(...) Y porque .bd. es .20.m̃.1.co (...) sera el su quadrado 400.p̃.1.ce.m̃.40.co* [read: $20^2 + x^2 - 40x$] *(...)*

Thus he reaches model

$$\frac{ab^2}{ac^2} = \frac{425 - 40x + x^2}{x^2 + 25} = 5$$

[1] "Pythagoras invention", ie. Prop. 47 of Euclid's Elements — see eg. `http://aleph0.clarku.edu/ djoyce/java/elements/bookI/propI47.html`

...solved "by algebra"

Nunes algebraic calculation

$$\frac{425 - 40x + x^2}{x^2 + 25} = 5$$

$$\equiv \qquad \{ \text{ rule } \tfrac{a}{b} = \tfrac{c}{d} \equiv ad = bc \text{ etc } \}$$

$$425 - 40x + x^2 = 5x^2 + 125$$

$$\equiv \qquad \{ \text{ "calculus of al-gabr and al-muqâbala" (...) } \}$$

$$75 = x^2 + 10x$$

This leads to the expected

Solution

(...) sera luego *.a.b. R.250.* e *.a.c. R.50* *[read: $ab = \sqrt{250}$ and $ac = \sqrt{50}$]*

"Algebra (...) is thing causing admiration"

> (...) Principalmente que vemos algumas vezes, no poder vn gran Mathematico resoluer vna question por medios Geometricos, y resolverla por Algebra, siendo la misma Algebra sacada de la Geometria, q̃ es cosa de admiraciõ.

ie.

> *(...) Mainly because we see often a great Mathematician unable to resolve a question by Geometrical means, and solve it by Algebra, being that same Algebra taken from Geometry, which is thing causing admiration.*

[*in* Nunes' *Libro de Algebra*, fols. 270–270v.]

Letting “the symbols do the work” in the 16c

Deduction first

> *Y tambien porque quien obra por Algebra va entendiendo la razon de la obra que haze, hasta la yqualacion ser acabada. (...) De suerte que, quien obra por Algebra, va haziendo discursos demonstrativos.*

ie.

> *And also because one performing by Algebra is understanding the reason of the work one does, until the equality is finished. (...) So much so that, who works by Algebra is doing a demonstrative discourse.*

[fol. 269r-269v]

Verdict

(...) De manera, que
quien sabe por Algebra,
sabe <u>scientificamente</u>.

(...) in this way, who knows by Algebra
knows <u>scientifically</u>)

Tradition on "al-djabr" equational reasoning

- **"Al-djabr"** rules are not a privilege of arithmetics.
- For instance, in predicate logic:

$$(x \wedge \neg z) \Rightarrow y \quad \equiv \quad x \Rightarrow (z \vee y) \tag{1}$$

$$(x \wedge z) \Rightarrow y \quad \equiv \quad x \Rightarrow (z \Rightarrow y) \tag{2}$$

hold, for all x, y and z.

- "Al-djabr" rules are nowadays known as **Galois connections**.

Question

Can we discharge **proof obligations** in program verification along the same tradition?

Tradition on "al-djabr" equational reasoning

- **"Al-djabr"** rules are not a privilege of arithmetics.
- For instance, in predicate logic:

$$(x \wedge \neg z) \Rightarrow y \quad \equiv \quad x \Rightarrow (z \vee y) \tag{1}$$

$$(x \wedge z) \Rightarrow y \quad \equiv \quad x \Rightarrow (z \Rightarrow y) \tag{2}$$

hold, for all x, y and z.

- "Al-djabr" rules are nowadays known as **Galois connections**.

Question

Can we discharge **proof obligations** in program verification along the same tradition?

Exercises (warming up)

Exercise 1: Show that equivalences (1) and (2) hold.

□

Exercise 2: Consider the following variant of the *al-hatt* rule (in $\mathbb{N}_0$)

$$x * z \leq y \quad \equiv \quad x \leq y/z \tag{3}$$

where y/z denotes the *integral division* of y by z, eg. such that $3/2 = 1$, etc. Resort directly to (3) in showing that $y/0$ is the largest of all natural numbers.

□

Trend for notation economy

Well-known throughout the history of maths — a kind of "natural language **implosion**" — particularly visible in the syncopated phase (16c), eg.

.40.p̃.2.ce. son yguales a .20.co

(P. Nunes, Coimbra, 1567) for nowadays $40 + 2x^2 = 20x$, or

B 3 in A quad - D plano in A + A cubo æquatur Z solido

(F. Viète, Paris, 1591) for nowadays $3BA^2 - DA + A^3 = Z$

Final touch

René Decartes (1596–1650), who studied algebra by the books of Clavius (1538–1612), a student of Nunes at Coimbra.

Trend for notation economy

Well-known throughout the history of maths — a kind of "natural language **implosion**" — particularly visible in the syncopated phase (16c), eg.

.40.p̃.2.ce. son yguales a .20.co

(P. Nunes, Coimbra, 1567) for nowadays $40 + 2x^2 = 20x$, or

B 3 in A quad - D plano in A + A cubo æquatur Z solido

(F. Viète, Paris, 1591) for nowadays $3BA^2 - DA + A^3 = Z$

Final touch

René Decartes (1596–1650), who studied algebra by the books of Clavius (1538–1612), a student of Nunes at Coimbra.

Later on (18c, 19c, ...)

More demanding problems to be modelled/solved, eg. electrical circuits:

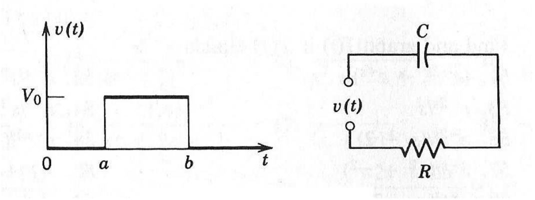
From a simple law ...

$V = R \times I$ by Georg Ohm (1789-1854) ...

...to linear RC-circuits

$$v(t) = Ri(t) + \frac{1}{C}\int_0^t i(\tau)d\tau$$

$$v(t) = V_0(u(t-a) - u(t-b)) \qquad (b > a)$$



Later on (18c, 19c, ...)

More demanding problems to be modelled/solved, eg. electrical circuits:

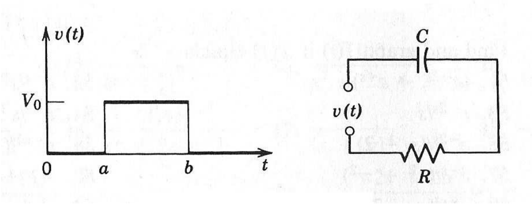
From a simple law ...

$V \quad = \quad R \times I$ by Georg Ohm (1789-1854) ...

...to linear RC-circuits

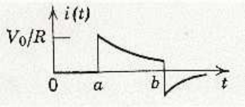
$$v(t) = Ri(t) + \frac{1}{C}\int_0^t i(\tau)d\tau$$

$$v(t) = V_0(u(t-a) - u(t-b)) \qquad (b > a)$$



Calculate $i(t)$

The following $i(t)$ can be observed on an oscilloscope:



Can you explain it?

Is 16c maths still enough for the required calculations?

No. Need for the the differential/integral calculus.

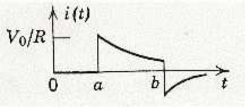
But there is more:

For the underlying maths to scale up

Need for an *integral transform*, eg. the Laplace transform.

Calculate $i(t)$

The following $i(t)$ can be observed on an oscilloscope:



Can you explain it?

Is 16c maths still enough for the required calculations?

No. Need for the the differential/integral calculus.

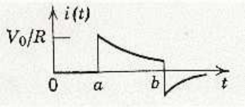
But there is more:

For the underlying maths to scale up

Need for an *integral transform*, eg. the Laplace transform.

Calculate $i(t)$

The following $i(t)$ can be observed on an oscilloscope:



Can you explain it?

Is 16c maths still enough for the required calculations?

No. Need for the the differential/integral calculus.

But there is more:

For the underlying maths to scale up

Need for an *integral transform*, eg. the Laplace transform.

Laplace transform

t-space

s-space

Given problem

$$y'' + 4y' + 3y = 0$$
$$y(0) = 3$$
$$y'(0) = 1$$

Subsidiary equation

$$s^2 Y + 4sY + 3Y = 3s + 13$$

Solution of subs. equation

$$Y = \frac{-2}{s+3} + \frac{5}{s+1}$$

Solution of given problem

$$y(t) = -2e^{-3t} + 5e^{-t}$$

An integral transform

$(\mathcal{L}\ f)s = \int_0^\infty e^{-st} f(t) dt$, eg.

$f(t)$	$\mathcal{L}(f)$
1	$\frac{1}{s}$
t	$\frac{1}{s^2}$
t^n	$\frac{n!}{s^{n+1}}$
e^{at}	$\frac{1}{s-a}$
etc	

Pierre Laplace (1749-1827)

Laplace-transformed RC-circuit model

$\mathcal{L}$(t-space RC model) is

$$RI(s) + \frac{I(s)}{sC} \quad = \quad \frac{V_0}{s}(e^{-as} - e^{-bs})$$

whose *algebraic* solution for $I(s)$ is

$$I(s) \quad = \quad \frac{\frac{V_0}{R}}{s + \frac{1}{RC}}(e^{-as} - e^{-bs})$$

Now, the converse transformation:

$$\mathcal{L}^{-1}\left(\frac{\frac{V_0}{R}}{s + \frac{1}{RC}}\right) \quad = \quad \frac{V_0}{R}e^{-\frac{t}{RC}}$$

Analytical solution

After some algebraic manipulation we will obtain an analytical answer ...

$$i(t) = \begin{cases} 0 \quad \text{if} \quad t < a \\ \left(\frac{V_0 e^{-\frac{a}{RC}}}{R}\right) e^{-\frac{t}{RC}} \quad \text{if} \quad a < t < b \\ \left(\frac{V_0 e^{-\frac{a}{RC}}}{R} - \frac{V_0 e^{-\frac{b}{RC}}}{R}\right) e^{-\frac{t}{RC}} \quad \text{if} \quad t > b \end{cases}$$

...with some help by Oliver Heaviside (1850-1925)

What's new?

While the underlying mathematics has changed,

- from systems of **polynomial** equations, to
- **differential/integral** equations

the overall approach is the same:

$$e = m + c$$

ie.

engineering = *model first, then calculate . . .*

Moreover, via the Laplace transform we get back to **polynomial** equations again.

$e = m + c$ challenges

A "notation problem":

Mathematical modelling

requires *descriptive* notations, therefore:

- intuitive
- domain-specific

Calculation

requires *elegant* notations, therefore:

- simple and compact
- generic
- cryptic, otherwise uneasy to manipulate

Recall Dijkstra's definition : *elegant* $\equiv$ *simple and remarkably effective*

$e = m + c$ challenges

A "notation problem":

Mathematical modelling

requires *descriptive* notations, therefore:

- intuitive
- domain-specific

Calculation

requires *elegant* notations, therefore:

- simple and compact
- generic
- cryptic, otherwise uneasy to manipulate

Recall Dijkstra's definition : *elegant* $\equiv$ *simple and remarkably effective*

$e = m + c$ challenges

A "notation problem":

Mathematical modelling

requires *descriptive* notations, therefore:

- intuitive
- domain-specific

Calculation

requires *elegant* notations, therefore:

- simple and compact
- generic
- cryptic, otherwise uneasy to manipulate

Recall Dijkstra's definition : *elegant* $\equiv$ *simple and remarkably effective*

Quoting Kreyszig's book, p.242

"(...) The Laplace transformation is a method for solving differential equations (...) [which] consists of three main steps:

1st step. *The given "hard" problem is transformed into a "simple" equation (subsidiary equation).*

2nd step. *The subsidiary equation is solved by* **purely algebraic** *manipulations.*

3rd step. *The solution of the subsidiary equation is transformed back to obtain the solution of the given problem.*

In this way the Laplace transformation reduces the problem of solving a differential equation to an **algebraic problem***".*

Question

All we have said applies to physics, mechanical eng., civil eng., electrical and electronic eng.

What about us? (software engineers)

Question

All we have said applies to physics, mechanical eng., civil eng., electrical and electronic eng.

What about us? (software engineers)

Need for a transform

Integration? Quantification?

$$(\mathcal{L}\ f)s = \int_0^\infty e^{-st} f(t) dt$$

$f(t)$	$\mathcal{L}(f)$
1	$\frac{1}{s}$
t	$\frac{1}{s^2}$
t^n	$\frac{n!}{s^{n+1}}$
e^{at}	$\frac{1}{s-a}$
etc	

A parallel:

$$\langle \int x \ : \ 0 \leq x \leq 10 : \ x^2 - x \rangle$$

$$\langle \forall\ x \ : \ 0 \leq x \leq 10 : \ x^2 \geq x \rangle$$

An "s-space analog" for logical quantification

The pointfree (PF) transform

ϕ	$PF\ \phi$
$\langle \exists\ a\ ::\ b\ R\ a \wedge a\ S\ c \rangle$	$b(R \cdot S)c$
$\langle \forall\ a, b\ ::\ b\ R\ a \Rightarrow b\ S\ a \rangle$	$R \subseteq S$
$\langle \forall\ a\ ::\ a\ R\ a \rangle$	$id \subseteq R$
$\langle \forall\ x\ ::\ x\ R\ b \Rightarrow x\ S\ a \rangle$	$b(R \setminus S)a$
$\langle \forall\ c\ ::\ b\ R\ c \Rightarrow a\ S\ c \rangle$	$a(S\ /\ R)b$
$b\ R\ a \wedge c\ S\ a$	$(b, c)\langle R, S \rangle a$
$b\ R\ a \wedge d\ S\ c$	$(b, d)(R \times S)(a, c)$
$b\ R\ a \wedge b\ S\ a$	$b\ (R \cap S)\ a$
$b\ R\ a \vee b\ S\ a$	$b\ (R \cup S)\ a$
$(f\ \ b)\ R\ (g\ \ a)$	$b(f^{\circ} \cdot R \cdot g)a$
TRUE	$b\ \top\ a$
FALSE	$b\ \bot\ a$

What are R, S, id ?

See next set of slides