Computer Algebra and Automated Reasoning

Tom Kelsey - Theory Group - St Andrews

November 27, 2000

Overview

- Motivation
- Exact reals in computer algebra
- An interface between Maple and PVS
- Where next?

Computational mathematics

- Symbolic and numeric calculations
- Examples include Maple, MATLAB, Aldor, NAG libraries
- Used in the design and implementation of critical systems
- Can provide incorrect - or misleading - results
- Can check results up to a point
  - error tolerances for numerics
  - substitution and pattern matching for symbolics
- Have no **formal** reasoning capabilities

Computational logic

- Higher order packages are being developed and extended
- Examples include PVS, HOL and Isabelle
- Suited for use in the design and implementation of critical systems
- Can investigate properties of
  - interface specifications (code verification)
  - mathematical models (analytic validity)
- Have underdeveloped analytic capabilities

Exact reals in computer algebra

- computable real functions w.r.t type-2 theory of effectivity[a]
- computation over potentially infinite sequences of data, using procedures which obtain all data items necessary to guarantee a finite precision
- replace lazy functional arithmetic with symbolic procedures

[a] Grzegorczyk, Weihrauch

Real valued Maple expressions

The Maple type **realsym** consists of the expressions which can be converted into a floating point number

Examples include

$sin\frac{\pi}{2}$ $\quad e^{\sqrt[7]{cos(3)}}$ $\quad$ and $\quad \int_0^\infty x^3 - \arccos(x) + \sqrt[3]{17}\ dx$

These can be hard to express in an exact real representation implemented in a lazy functional language

Golden ratio exact reals

ϕ is the positive root of $x^2 - x - 1 = 0$

A real number, a, in $[0, \phi)$ is

- expressed as a potentially infinite list of binary digits
  $a = [1, 0, 0, 1, 1, 0, \cdots]$
- interpreted as a sum of negative powers of the golden ratio
  $a = \sum_{i \in \mathbb{N}} \frac{d_i}{\phi^i} \quad \text{for } d_i \in \{0, 1\}$

ϕ has useful properties, but could be replaced by any computable number in $(1, 2)$

Converting from symbols to exact reals

Consider $sin(\frac{\pi}{2})$ (which equals one)

To obtain the first digit, d_1, in our exact representation we

1. solve the algebraic inequality

$$\frac{d_1}{\phi} < sin(\frac{\pi}{2})$$

   for d_1, giving the range of values

$$[-\infty, \psi_1]$$

2. decide whether the right hand value is less than one
   (a) if it is, then $d_1 = 0$
   (b) if not, then $d_1 = 1$

Since, in this case, $\psi_1 = \phi \approx 1.618$, we have $d_1 = 1$

To obtain the second digit we

1. solve the algebraic inequality

$$\frac{d_1}{\phi} + \frac{d_2}{\phi^2} < sin(\frac{\pi}{2})$$

   for d_2, giving the range of values

$$(-\infty, \psi_2]$$

2. decide whether the right hand value is less than one
   (a) if it is, then $d_2 = 0$
   (b) if not, then $d_2 = 1$

We have $\psi_2 = 1$, so $d_2 = 1$

We can repeat this process for as many digits as required

The Maple conversion procedure

$rs2grlist := \mathbf{proc}(a{::}realcons,\ n)$

$\mathbf{local}\ \phi,\ partsum,\ binlist,\ i,\ range,\ value,\ digit;$

$\quad partsum := 0\,;\ binlist := [\,]\,;\ \phi := 1/2 + 1/2 \times \mathrm{sqrt}(5)\,;$

$\quad \mathbf{for}\ i\ \mathbf{to}\ n\ \mathbf{do}$

$\qquad range := \mathrm{solve}(partsum + d/\phi^i < a,\ d)\,;$

$\qquad value := \mathrm{op}(\mathrm{op}(2,\ range))\,;$

$\qquad \mathbf{if}\ \mathrm{type}(\mathrm{evalf}(value - 1),\ negative)\ \mathbf{then}\ digit := 0$

$\qquad \mathbf{else}\ digit := 1\,;\ partsum := partsum + digit/\phi^i$

$\qquad \mathbf{fi};$

$\qquad binlist := [\mathrm{op}(binlist),\ digit]$

$\quad \mathbf{od};$

$\quad binlist$

$\mathbf{end}$

An application

Consider[a] the naïve evaluation as a **float** of the derivative of $e^{\frac{1}{4}}$:

$$\frac{e^{\frac{1}{4}+10^{-i}} - e^{\frac{1}{4}}}{10^{-i}}$$

This will lose one digit of precision with every digit increment of i

If $i = 10$ and our precision is 10 digits, then the evaluation returns zero instead of 1.284025417

We retain precision by evaluation in golden ratio base, then converting to **float**

[a] Monagan and Geddes

Maple screenshot

sshot.mws - [Server 1]

```
> restart: libname := "grlib", libname;
```

$$libname := \text{"grlib"}, \text{"/usr/local/maple/update"}, \text{"/usr/local/maple/lib"}$$

```
> with(grlib);
```

$$[ps2float, rs2grlist, rs2phisum]$$

```
> expr := (exp(1/4 + 10^(-5)) - exp(1/4))/10^(-5);
```

$$expr := 100000\, e^{\left(\frac{25001}{100000}\right)} - 100000\, e^{\left(\frac{1}{4}\right)}$$

```
> evalf(expr,5);
```

$$0$$

```
> rs2grlist(expr,5);
```

$$[1, 1, 1, 0, 0]$$

```
> rs2phisum(expr,10);
```

$$\frac{1}{\frac{1}{2}+\frac{1}{2}\sqrt{5}} + \frac{1}{\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)^2} + \frac{1}{\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)^3} + \frac{1}{\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)^7} + \frac{1}{\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)^9}$$

```
> ps2float(%,5);
```

$$1.283665450$$

Conclusions

Uses:

- replacement of numeric procedures when error is too high
  - roundoff error e.g. Vancouver SE & Patriot missile
  - ill-conditioning - high and low singular values
  - long intervals of integration
- investigation of functional algorithms for new bases
  - What does $\frac{\pi}{4}$ look like in base $\frac{3}{2}$?
  - How much look-ahead is needed for division in base $\frac{\pi^2}{6}$?

Maple6 and PVS

- Maple6 permits calls to **C** and **f77** routines - e.g. the NAG library
- PVS augmented with real analysis and transcendental function libraries at St Andrews
- Aim: the analysis and discharge of side conditions in symbolic DE and integration calculations

Case study - continuity

We want to do *automatic* continuity checking in PVS

Definition 1. $f : T \subseteq \mathbb{R} \to \mathbb{R}$ is continuous at $x \in T$ *iff*
$\forall \epsilon \in \mathbb{R}_+ \exists \delta \in \mathbb{R}_+ \forall y \in T : |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$

Problem: given $f : T \subseteq \mathbb{R} \to \mathbb{R}$ and $x \in T$, is f continuous at x?

If we can answer this for $x \in T$, then we have also solved the problem: is f continuous on its domain?

In general this problem is undecidable

GRIND (naïve)

We can give `GRIND` the appropriate theories as parameters and get the following results:

Can prove:

```
test1 : LEMMA
  continuous(LAMBDA x : abs(x) + 3*x, y)
```

Can't prove:

```
test2 : LEMMA
  continuous(LAMBDA x : 1 / (abs(x) + 1), y)
```

GRIND with judgements

`GRIND` (naïve) fails - the typechecker cannot determine that functions are of the appropriate type to match the theorems

We use *judgements* to extend the typechecker

Example:

```
nzfun : TYPE = [T -> nzreal]
nzf, nzg : VAR nzfun

nzfun_times_nzfun_is_nzfun: JUDGEMENT *(nzf, nzg) HAS_TYPE nzfun
```

GRIND with judgements - results

Can prove:

```
test3 : LEMMA
  continuous(LAMBDA (x : negreal) :
         5 * (1/(abs(x) + 1) + 2/(x - abs(x))) - x * x,-4)
test4 : LEMMA
  continuous(LAMBDA x : exp(cos(x)+1), y)
test5 : LEMMA
  FORALL (z : I(2,3)) :
    continuous(LAMBDA (x : I(2,3)) : 1/x, z)
```

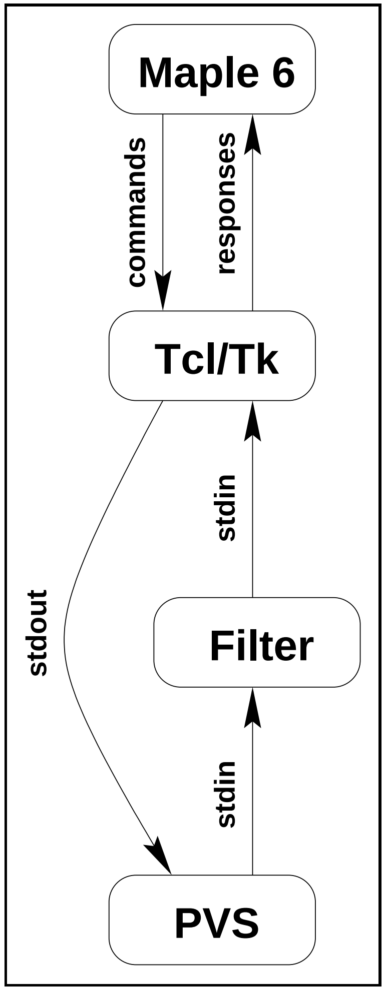
Can't yet prove:

```
test6 : LEMMA
    continuous(LAMBDA (x : real) : 1/(cos(x)+2), 4)
```

Architecture

Within a Maple session

- use **C** interface functions
  - start/end PVS subprocesses
  - send/receive information
- use Tcl/Tk windows
  - display options
  - monitor PVS progress
- PVS acts as a black box



Maple screenshot

screenshot.mws - [Server 2]

```
> restart: libname := "pvslib", libname: with(pvslib);
```

$$[contcheck, contpvs, forallpvs, hypopvs, intcheck, intpvs, qsolve, soltestpvs]$$

```
> ivp := {diff(y(x),x)+y(x)/x-x-2, y(1) = 2};
```

$$ivp := \left\{\left(\frac{\partial}{\partial x}\mathrm{y}(x)\right) + \frac{\mathrm{y}(x)}{x} - x - 2, \mathrm{y}(1) = 2\right\}$$

```
> soln := dsolve(ivp, {y}(x));
```

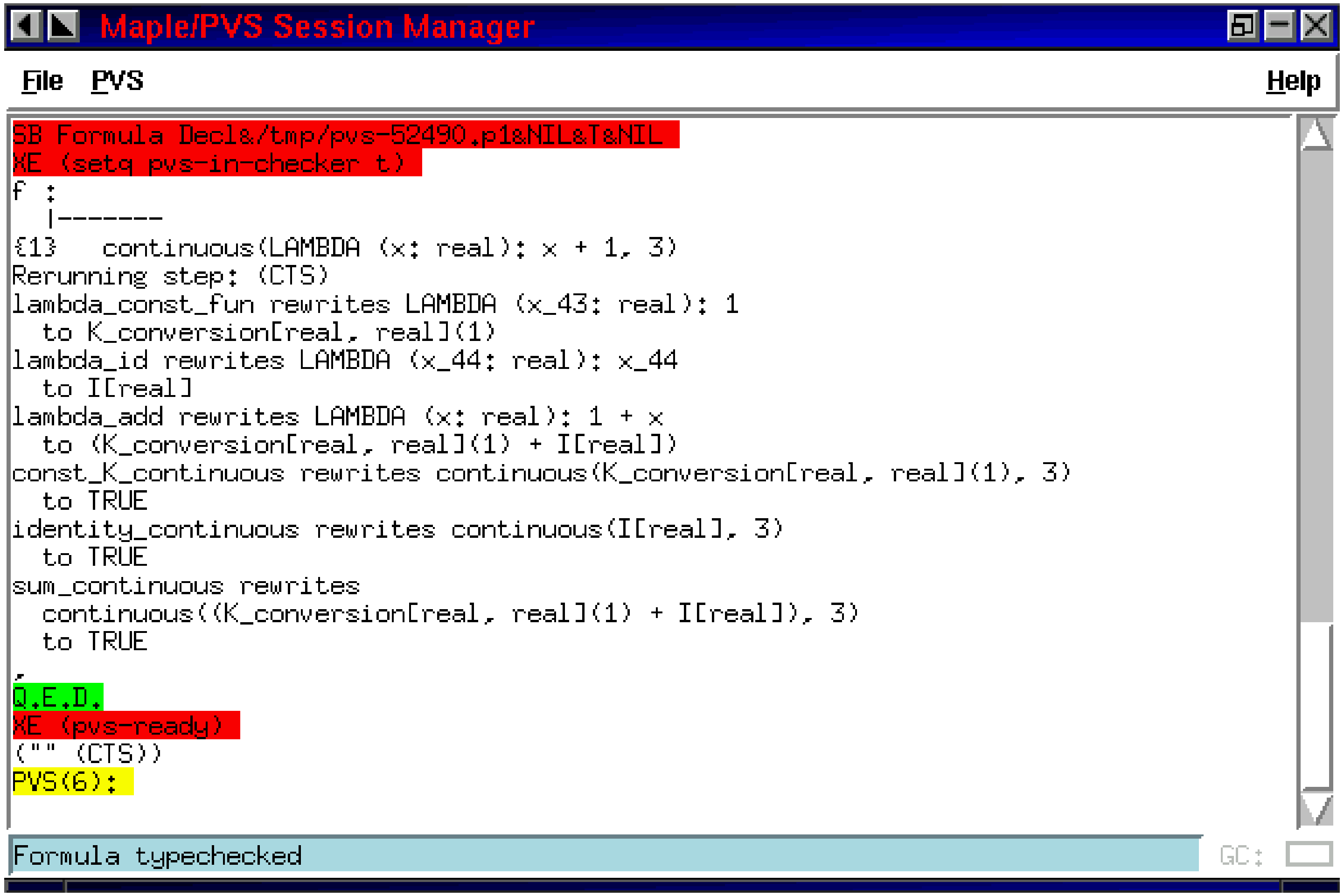
$$soln := \mathrm{y}(x) = \frac{1}{3}x^2 + x + \frac{2}{3}\frac{1}{x}$$

```
> qsolve("demo", x->1/x, x->x+2, 1, 2, 2, 3,{},{}," ");

% PVS call: prove {} implies 1/xi is continuous in [2,3]

continterval_"demo_1" : LEMMA
  FORALL (zi : I2(2,3)) :
       continuous(LAMBDA (xi : I2(2,3)) : 1/xi, zi)
```

Tcl/Tk screenshot



Where next?

- Dependable mathematics for critical systems
- Development of preceding projects and the formalisation of the AXIOM-Aldor type system
- ATP support for applications of continuous mathematics
- Formal methods support for mathematical modelling

Collaborators

- SRI International
- Maple inc
- NAG Ltd
- Mathworks inc
- Intel Corp
- DERA

Summary

Exact reals - Martin Dunstan[a], Martín Escardó[b], Tom Kelsey

Maple/PVS - Andrew Adams[c], Martin Dunstan, Hanne Gottliebsen, Tom Kelsey, Ursula Martin

Critical systems - Hanne Gottliebsen, Tom Kelsey, Ursula Martin

Details available at

`http://www.dcs.st-and.ac.uk/Rsch/output.html`

---

[a] NAG Ltd
[b] now at Birmingham
[c] now at Reading