From High School Algebra to University Algebra

Thorsten Altenkirch

Functional Programming Laboratory
School of Computer Science
University of Nottingham

June 21, 2013

Primary School Algebra (PSA)

$$
\begin{aligned}
A + B &= B + A \\
A + (B + C) &= (A + B) + C \\
1 \times A &= A \\
A \times B &= B \times A \\
A \times (B + C) &= (A \times B) + (A \times C)
\end{aligned}
$$

- An equation in PSA is provable, iff it is true for all (positive) natural numbers.
- I.e. PSA is complete for this interpretation.

High School Algebra (HSA)

PSA $+$

$$
\begin{aligned}
1^A &= 1 \\
(A \times B)^C &= A^C \times B^C \\
A^1 &= A \\
A^{B \times C} &= (A^B)^C \\
A^{B+C} &= A^B \times A^C
\end{aligned}
$$

- Tarski conjecture: HSA is complete.
- Certainly wrong when we add 0, we cannot derive

  $$0^x = 0^{0^{0^x}}$$

  from $A^0 = 1$ but it is true for the natural numbers.
- Note that

  $$0^x = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{otherwise} \end{cases}$$

- There is no equation to simplify $(A + B)^C$.

Wilkie's counterexample

$$\begin{array}{rclcrcl} A & = & 1+x & \qquad & B & = & 1+x+x^2 \\ C & = & 1+x^3 & & D & = & 1+x^2+x^4 \end{array}$$

Note that:

$$A \times D = B \times C = 1 + x + x^2 + x^3 + x^4 + x^5$$

Consider:

$$(A^x + B^x)^y \times (C^y + D^y)^x = (A^y + B^y)^x \times (C^x + D^x)^y$$

This equality is true for all positive natural numbers **but** it is not provable from the laws of HSA.

Why is it true?

$$\begin{array}{rclcrcl} A & = & 1 + x & \quad & B & = & 1 + x + x^2 \\ C & = & 1 + x^3 & \quad & D & = & 1 + x^2 + x^4 \end{array}$$

Let $E = 1 - x + x^2$, we have

$$\begin{array}{rcl} A \times E & = & C \\ B \times E & = & D \end{array}$$

Hence:

$$\begin{array}{rl} & (A^x + B^x)^y \times (C^y + D^y)^x \\ = & (A^x + B^x)^y \times ((A \times E)^y + (B \times E)^y)^x \\ = & (A^x + B^x)^y \times (E^y)^x \times (A^y + B^y)^x \\ = & (A^x + B^x)^y \times (E^x)^y \times (A^y + B^y)^x \\ = & ((E \times A)^x + (E \times B)^x)^y \times (A^y + B^y)^x \\ = & (C^x + D^x)^y \times (A^y + B^y)^x \\ = & (A^y + B^y)^x \times (C^x + D^x)^y \end{array}$$

Why can't we derive it?

- We cannot use $E = 1 - x + x^2$ because of the negative coefficient.
- Wilkie showed formally that this equality is not derivable in any other way using HSA.
- He also showed that if we add all equalities which are consequences of using negtive numbers we get completeness.
- Gurevich showed that there is no finite equational formalisation of HSA.
- Gurevich also showed that HSA is decidable.

The Numbers-as-types equivalence

- We can interpret the operations of HSA as operations on types:

$$\begin{array}{rl} A+B & \text{disjoint union} \\ A\times B & \text{cartesian product} \\ A^B & \text{function types } B\to A \end{array}$$

- The equalities of HSA become isomorphisms which hold in any Cartesian Closed Category with coproducts.
- E.g $A^{B+C} = A^B \times A^C$ is witnessed by

$$\begin{array}{rcl} \phi & : & ((B+C)\to A)\to (B\to A)\times(C\to A) \\ \phi & = & \lambda f.(f\circ \mathrm{inl}, f\circ \mathrm{inr}) \\ \phi^{-1} & : & (B\to A)\times(C\to A)\to((B+C)\to A) \\ \phi^{-1} & = & \lambda(g,h).\lambda x.\mathrm{case}\, x\, g\, h \end{array}$$

- The isomorphism corresponding to $A^{B\times C} = (A^B)^C$ is well known in functional programming.

Di Cosmo's question

- Does the incompleteness also apply if we want to derive isomorphisms?
- In particular does the Wilkie counterexample correspond to an isomorphism?
- This was answered positively by Fiore, Di Cosmo and Balat.
- Exercise: Implement the Wilkie counterexample in Haskell, that is assuming that $A \times D \simeq B \times C$ derive

$$\begin{aligned} &(Y \to (X \to A) + (X \to B)) \times (X \to (Y \to C) + (Y \to D)) \\ \simeq &(X \to (Y \to A) + (Y \to B)) \times (Y \to (X \to C) + (X \to D)) \end{aligned}$$

- What happens if we add dependent types?

University Algebra (UA)

We use a Type Theory with $1, 2, \Pi, \Sigma$:

$$
\begin{array}{lrcl}
\Phi_{2C} & : \quad 2 & \simeq & 2 \\
\Phi_{2A} & : \quad \Sigma x : 2.\mathrm{if}\; x\; A\; \Sigma y : 2.\mathrm{if}\; y\; B\; C & \simeq & \Sigma x : 2.\mathrm{if}\; x\; (\Sigma y : 2.\mathrm{if}\; y\; A\; B)\; C \\
\Phi_{\Sigma A} & : \quad \Sigma a : A.\Sigma b : B\, a.C\, a\, b & \simeq & \Sigma (a, b) : (\Sigma a : A.B\, a).C\, a\, b \\
\Phi_{\Pi 1} & : \quad \Pi - : A.1 & \simeq & 1 \\
\Phi_{1\Pi} & : \quad \Pi x : 1.B\, x & \simeq & B\, () \\
\Phi_{2\Pi} & : \quad \Pi b : 2.B\, b & \simeq & (B\, \mathrm{tt}) \times (B\, \mathrm{ff}) \\
\Phi_{1\Sigma} & : \quad \Sigma x : 1.B\, x & \simeq & B\, () \\
\Phi_{\Sigma\Pi} & : \quad \Pi a : A.\Pi b : B\, a.C\, a\, b & \simeq & \Pi (a, b) : (\Sigma a : A.B\, a).C\, a\, b \\
\Phi_{\Pi\Sigma} & : \quad \Pi a : A.\Sigma b : B\, a.C\, a\, b & \simeq & \Sigma f : (\Pi a : A.B\, a).\Pi a : A.C\, a\, (f\, a
\end{array}
$$

Deriving the Wilkie-Isomorphism

- We define $A + B = \Sigma x : 2.\mathrm{if}\, x\, A\, B$.
- We can define $A \times B$ either as $\Sigma x : A.B$ or as $\Pi x : 2.\mathrm{if}\, x\, A\, B$.
- Using $A \to B = \Pi x : A.B$ we can derive all isomorphisms of HSA.
- Unlike in HSA we can reduce $A \to B + C$ using $\Phi_{\Pi\Sigma}$:

$$\begin{aligned} & A \to B + C \\ = \quad & A \to \Sigma x : 2.\mathrm{if}\, x\, B\, C) \\ \simeq \quad & \Sigma f : A \to 2.\Pi x : A.\mathrm{if}\, (f\, x)\, B\, C \end{aligned}$$

- Using this idea we can derive the Wilkie-Isomorphism in UA see paper.

Questions

- In UA the counterexample to completeness is actually derivable.
- This raises the question wether UA is complete for (natural) isomorphisms in the category of non-empty finite sets.
- The key idea seems to be that UA unlike HSA has a normal form for types:

$$\begin{array}{rcl} \mathrm{NF} & :: & \Sigma x : \mathrm{NF}_\Pi . \mathrm{NF} \mid \mathrm{NF}_\Pi \\ \mathrm{NF}_\Pi & :: & \Pi x : \mathrm{NF} . \mathrm{NF}_\Pi \mid \mathrm{NF}_0 \\ \mathrm{NF}_0 & :: & X | n | \mathrm{T}[\mathrm{NF}] \end{array}$$

- I also conjecture that the extensional Type Theory with $1, 2, \Pi, \Sigma$ is decidable (again this fails if we add 0).