From High School Algebra to University Algebra

Thorsten Altenkirch

Functional Programming Laboratory
School of Computer Science
University of Nottingham

June 13, 2013
Primary School Algebra (PSA)

\[
A + B = B + A
\]
\[
A + (B + C) = (A + B) + C
\]
\[
1 \times A = A
\]
\[
B \times A = B \times A
\]
\[
A \times (B + C) = (A \times B) + (A \times C)
\]

- 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 +

\[ 1^A = 1 \]
\[ (A \times B)^C = A^C \times B^C \]
\[ A^1 = A \]
\[ A^{B \times C} = (A^B)^C \]
\[ A^{B+C} = A^B \times A^C \]

- Tarski conjecture: HSA is complete.
- Certainly wrong when we add 0, we cannot derive
  \[ 0^x = 0^{0^x} \]
  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

\[ A = 1 + x \quad B = 1 + x + x^2 \]
\[ C = 1 + x^3 \quad D = 1 + x^2 + x^4 \]

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?

\[ A = 1 + x \quad B = 1 + x + x^2 \]
\[ C = 1 + x^3 \quad D = 1 + x^2 + x^4 \]

Let \( E = 1 - x + x^2 \), we have

\[ A \times E = C \]
\[ B \times E = D \]

Hence:

\[
(A^x + B^x)^y \times (C^y + D^y)^x
\]
\[ = (A^x + B^x)^y \times ((A \times E)^y + (B \times E)^y)^x \]
\[ = (A^x + B^x)^y \times (E^y)^x \times (A^y + B^y)^x \]
\[ = (A^x + B^x)^y \times (E^x)^y \times (A^y + B^y)^x \]
\[ = ((E \times A)^x + (E \times B)^x)^y \times (A^y + B^y)^x \]
\[ = (C^x + D^x)^y \times (A^y + B^y)^x \]
\[ = (A^y + B^y)^x \times (C^x + D^x)^y \]
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 negative 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:
  \[ A + B \] disjoint union
  \[ A \times B \] cartesian product
  \[ A^B \] function types \( B \rightarrow A \)

- 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

  \[
  \phi : ((B + C) \rightarrow A) \rightarrow (B \rightarrow A) \times (C \rightarrow A) \\
  \phi = \lambda f.(f \circ \text{inl}, f \circ \text{inr}) \\
  \phi^{-1} : (B \rightarrow A) \times (C \rightarrow A) \rightarrow ((B + C) \rightarrow A) \\
  \phi^{-1} = \lambda (g, h).\lambda x.\text{case} x g h
  \]

- 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
  \[
  (Y \to (X \to A) + (X \to B)) \times (X \to (Y \to C) + (Y \to D)) \\
  \simeq (X \to (Y \to A) + (Y \to B)) \times (Y \to (X \to C) + (X \to D))
  \]
- What happens if we add dependent types?
We use a Type Theory with 1, 2, Π, Σ:

\[
\begin{align*}
\Phi_{2C} & : \quad \Sigma x : 2.\text{if } x A \Sigma y : 2.\text{if } y B C & \quad \Sigma x : 2.\text{if } x (\Sigma y : 2.\text{if } y A B) C \\
\Phi_{2A} & : \quad \Sigma a : A.\Sigma b : B a.C a b & \quad \Sigma (a, b) : (\Sigma a : A.B a).C a b \\
\Phi_{\Sigma A} & : \quad \Pi \rightarrow : A.1 & \quad 1 \\
\Phi_{\Pi 1} & : \quad \Pi x : 1.B x & \quad B () \\
\Phi_{1\Pi} & : \quad \Pi b : 2.B b & \quad (B \text{tt}) \times (B \text{ff}) \\
\Phi_{1\Sigma} & : \quad \Sigma x : 1.B x & \quad B () \\
\Phi_{\Sigma \Pi} & : \quad \Pi a : A.\Pi b : B a.C a b & \quad \Pi(a, b) : (\Sigma a : A.B a).C a b \\
\Phi_{\Pi \Sigma} & : \quad \Pi a : A.\Sigma b : B a.C a b & \quad \Sigma f : (\Pi a : A.B a).\Pi a : A.C a (f a)
\end{align*}
\]
Deriving the Wilkie-Isomorphism

- We define $A + B = \Sigma x : 2.\text{if } x \, A \, B$.
- We can define $A \times B$ either as $\Sigma x : A.B$ or as $\Pi x : 2.\text{if } x \, A \, B$.
- 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 $\Phi_{\Pi\Sigma}$:

\[
A \to B + C \\
= A \to \Sigma x : 2.\text{if } x \, B \, C \\
\simeq \Sigma f : A \to 2.\Pi x : A.\text{if } (f \, x) \, B \, C
\]

- 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 whether 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:

\[
\begin{align*}
NF &:: \Sigma x : NF\Pi . NF | NF\Pi \\
NF\Pi &:: \Pi x : NF.NF\Pi | NF_0 \\
NF_0 &:: X | n | T[NF]
\end{align*}
\]

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