Equational Reasoning - Presentation 2

Gabriel Silva

https://github.com/gabriel951/my_work

UnB

Professor: Daniele Nantes

December 17, 2020

Overview

Goal

Using Structured Proofs

$\mathcal{S}_{AGH}$ Is Isomorphic To $\mathbb{Z}[X]$

Proposition 6.6

Proposition 6.10

Goal

Present the proofs of:

- $\mathcal{S}_{AGH}$ is isomorphic to $\mathbb{Z}[X]$
- Proposition 6.6
- Proposition 6.10

of Nutt's paper: "Unification in Monoidal Theories is Solving Linear Equations Over Semirings" ([1]).

I decided to use **structured proofs** as described by Leslie Lamport in [2], [3].

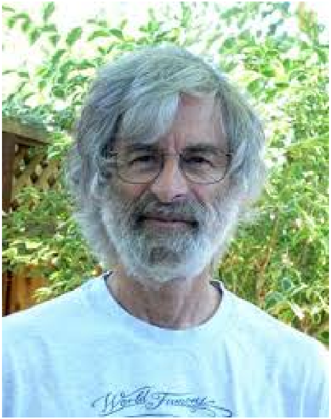

Figure 1: Leslie Lamport.

Why Use a Structured Proof?

A structured proof allows us to present a proof in details without compromising readability, due to its **hierarchical organization**.

Lemma

$\mathcal{S}_{AGH}$ is isomorphic to $\mathbb{Z}[X]$.

Proof:

$\langle 1 \rangle 1.$ **Let:** $\alpha \in \mathcal{S}_{AGH}$. Then α is a Σ-homomorphism
$\alpha : \mathcal{F}_{AGH}(u) \to \mathcal{F}_{AGH}(u)$.

By the definition of $\mathcal{S}_{\mathcal{E}}$ with $\mathcal{E} = AGH$.

$\langle 1 \rangle 2.$ **Let:** $u\alpha =_{AGH} ua_0 + h(u)a_1 + \ldots + h^k(u)a_k$, with $a_0, \ldots, a_k \in \mathbb{Z}$.
Associate to α, the polynomial $p_\alpha \in \mathbb{Z}[X]$, given by
$p_\alpha = a_0 + a_1 X + \ldots + a_k X^k$.

$\langle 1 \rangle 3.$ **Define:**

$$\begin{aligned} \psi : \mathcal{S}_{AGH} &\to \mathbb{Z}[X] \\ \alpha &\mapsto p_\alpha \end{aligned}$$

$\langle 1 \rangle 4.$ ψ is a semiring isomorphism between $\mathcal{S}_{AGH}$ and $\mathbb{Z}[X]$.

$\langle 2 \rangle 1.$ $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$ for all α, β in $\mathcal{S}_{AGH}$.

$\langle 3 \rangle 1.$ $u(\alpha + \beta) = u\alpha + u\beta$.

By the definition of $\alpha + \beta$.

$\langle 3 \rangle 2.$ $p_{\alpha+\beta} = p_\alpha + p_\beta$.

By Step $\langle 3 \rangle 1$ and the definition of p.

$\langle 3 \rangle 3.$ $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$.

By Step $\langle 3 \rangle 2$ and the definition of ψ.

Proof (cont.)

$\langle 2 \rangle 2.$ $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$.

$\langle 3 \rangle 1.$ $u(\alpha\beta) = (u\alpha)\beta$.

By the definition of $\alpha\beta$.

$\langle 3 \rangle 2.$ $p_{\alpha\beta} = p_\alpha p_\beta$.

By Step $\langle 3 \rangle 1$ and the definition of p.

$\langle 3 \rangle 3.$ $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$.

By Step $\langle 3 \rangle 2$ and the definition of ψ.

Proof (cont.)

$\langle 2\rangle 3.$ $\psi(id) = 1.$

$\langle 3\rangle 1.$ $uid = u.$

By the definition of id.

$\langle 3\rangle 2.$ $p_{id} = 1.$

By Step $\langle 3\rangle 1$ and the definition of p.

$\langle 3\rangle 3.$ $\psi(id) = 1.$

By Step $\langle 3\rangle 2$ and the definition of ψ.

Proof (cont.)

$\langle 2\rangle 4$. ψ is an semiring homomorphism.

By the definition of semiring homomorphism and Steps $\langle 2\rangle 1$, $\langle 2\rangle 2$ and $\langle 2\rangle 3$.

$\langle 2\rangle 5.$ ψ is injective.

$\langle 3\rangle 1.$ **Suffices:** to prove that $\psi(\alpha) = \psi(\beta)$ implies $\alpha = \beta$ for arbitraries α and β in $\mathcal{S}_{AGH}$.

By the definition of injective.

$\langle 3\rangle 2.$ $\psi(\alpha) = \psi(\beta)$.

By hypothesis.

$\langle 3\rangle 3.$ $p_\alpha = p_\beta$.

By Step $\langle 3\rangle 2$ and the definition of ψ.

$\langle 3\rangle 4.$ $u\alpha = u\beta$.

By Step $\langle 3\rangle 3$ and the definition of p.

$\langle 3\rangle 5.$ $\alpha = \beta$.

Since both α and β are endomorphisms over $\mathcal{F}_{AGH}(u)$ and $\mathcal{F}_{AGH}(u)$ is free over $\{u\}$, they are uniquely determined by $u\alpha$ and $u\beta$ respectively.

$\langle 2 \rangle 6.$ ψ is surjective.

$\langle 3 \rangle 1.$ **Suffices:** to consider an arbitrary polynomial $p \in \mathbb{Z}[x]$ and **Pick** an element $\alpha \in \mathcal{S}_{AGH}$ such that $\psi(\alpha) = p$.

By the definition of surjective.

$\langle 3 \rangle 2.$ **Let:** $p = a_0 + a_1 X + \ldots + a_k X^k$ be an arbitrary polynomial in $\mathbb{Z}[X]$.

$\langle 3 \rangle 3.$ **Pick** $\alpha \in \mathcal{S}_{AGH}$ given by:
$u\alpha = ua_0 + h(u)a_1 + \ldots + h^k(u)a_k$.

$\langle 3 \rangle 4.$ $\psi(\alpha) = p$.

By the definition of ψ.

$\langle 2 \rangle 7.$ ψ is a semiring isomorphism between $\mathcal{S}_{AGH}$ and $\mathbb{Z}[X]$.

By Step $\langle 2 \rangle 4$, ψ is a semiring homomorphism. By Steps $\langle 2 \rangle 5$ and $\langle 2 \rangle 6$, ψ is bijective.

$\langle 1 \rangle 5.$ $\mathcal{S}_{AGH}$ is isomorphic to $\mathbb{Z}[X]$.

Since we found a ring isomorphism ψ in Step $\langle 1 \rangle 4$.

Proposition 6.6 - Enunciate

Lemma (Proposition 6.6 of Nutt's paper)

$\mathcal{S}_{\mathcal{E}}$ is commutative if, and only if, $\mathcal{E}$ is a theory with commuting homomorphisms.

A Quick Note on Notation

Nutt, page 18, before Example 6.4:

> *"Observe that for the multiplication in $\mathcal{S}_{\mathcal{E}}$ we have $\alpha_s \alpha_t = \alpha_{s[u/t]}$."*

Proof:

$\langle 1 \rangle 1.$ If $\mathcal{S}_{\mathcal{E}}$ is commutative, then $\mathcal{E}$ is a theory with commuting homomorphisms.

$\langle 2 \rangle 1.$ **Let:** h, h' be arbitraries unary symbols from Σ.

$\langle 2 \rangle 2.$ $h(h'(u)) = u\alpha_{h(u)}\alpha_{h'(u)}$.

By the definition of $\alpha_{h(u)}$ and $\alpha_{h'(u)}$.

$\langle 2 \rangle 3.$ $u\alpha_{h(u)}\alpha_{h'(u)} =_{\mathcal{E}} u\alpha_{h'(u)}\alpha_{h(u)}$.

Since by hypothesis, $\mathcal{S}_{\mathcal{E}}$ is commutative.

Proof (cont.)

$\langle 2 \rangle 4.$ $u\alpha_{h'(u)}\alpha_{h(u)} = h'(h(u))$.
By the definition of $\alpha_{h'(u)}$ and $\alpha_{h(u)}$.

$\langle 2 \rangle 5.$ $\mathcal{E}$ is a theory with commuting homomorphisms.
By Steps $\langle 2 \rangle 2$, $\langle 2 \rangle 3$ and $\langle 2 \rangle 4$ we have $h(h'(u)) = h'(h(u))$. Since h and h' are arbitraries, by definition we conclude that $\mathcal{E}$ is a theory with commuting homomorphisms.

$\langle 1 \rangle 2.$ If $\mathcal{E}$ is a theory with commuting homomorphisms then $\mathcal{S}_{\mathcal{E}}$ is commutative.

$\langle 2 \rangle 1.$ $\mathcal{S}_{\mathcal{E}}$ is generated by elements that are of the form $\alpha_{h(u)}$ for some unary function symbol $h \in \Sigma$.

$\langle 3 \rangle 1.$ **Let:** α be an arbitrary element of $\mathcal{S}_{\mathcal{E}}$.

$\langle 3 \rangle 2.$ **Suffices:** to prove that there exists a composition α' of the terms $\alpha_{h(u)}$ such that $u\alpha = u\alpha' = t$.

Because every endomorphism α on $\mathcal{F}_{\mathcal{E}}(u)$ is uniquely determined by $u\alpha$, we just need to prove that α and α' give the same result on u.

Proof (cont.)

$\langle 3 \rangle 3$. Since $\mathcal{E}$ is a monoidal theory, every term t is obtained composing the constant 0, the symbol $+$ and the unary function symbols h. Therefore, we can prove Step $\langle 3 \rangle 2$ by induction on t.

Proof (cont.)

$\langle 2\rangle 2.$ $\mathcal{S}_{\mathcal{E}}$ has a set of commuting generators.

$\langle 3\rangle 1.$ **Let:** $h, h' \in \Sigma$ be arbitrary unary symbols.

$\langle 3\rangle 2.$ $\alpha_{h(u)}\alpha_{h'(u)} = \alpha_{h(h'(u))}$.
By definition.

$\langle 3\rangle 3.$ $\alpha_{h(h'(u))} = \alpha_{h'(h(u))}$.
Since, by hypothesis, $\mathcal{E}$ is a theory with commuting homomorphisms.

$\langle 3\rangle 4.$ $\alpha_{h'(h(u))} = \alpha_{h'(u)}\alpha_{h(u)}$.
By definition.

Proof (cont.)

$\langle 2 \rangle 3$. By Step $\langle 2 \rangle 2$, we conclude that $\mathcal{S}_{\mathcal{E}}$ is commutative.

Proposition 6.10

Lemma (Proposition 6.10 of Nutt's paper)

Let X, Y, Z *be finite and* $\sigma : \mathcal{S}_{\mathcal{E}}^{X} \to \mathcal{S}_{\mathcal{E}}^{Y}$ *and* $\tau : \mathcal{S}_{\mathcal{E}}^{Y} \to \mathcal{S}_{\mathcal{E}}^{Z}$ *be left linear. Then:*

1. $(id_{\mathcal{S}_{\mathcal{E}}^{X}})^{hom} = id_{X}$.
2. $(\sigma\tau)^{hom} = \sigma^{hom}\tau^{hom}$.

Proof

Proof:

$\langle 1 \rangle 1.$ $(id_{\mathcal{S}^X_\mathcal{E}})^{hom} = id_X$.

$\langle 2 \rangle 1.$ $(id_{\mathcal{S}^X_\mathcal{E}})^{hom} = \sum_{x,x' \in X} \pi_x \delta_{xx'} \iota_{x'}$.

The matrix of $id_{\mathcal{S}^X_\mathcal{E}}$ is the identity matrix $(\delta_{xx'})_{x,x' \in X}$. Then, by Definition of $\cdot^{hom}$ we obtain $(id_{\mathcal{S}^X_\mathcal{E}})^{hom} = \sum_{x,x' \in X} \pi_x \delta_{xx'} \iota_{x'}$.

Proof (cont.)

$\langle 2 \rangle 2.$ $\sum_{x,x' \in X} \pi_x \delta_{xx'} \iota_{x'} = \sum_{x \in X} \pi_x \iota_x$.

Since $\delta_{xx'}$ is 1 when $x = x'$ and is 0 otherwise.

Proof (cont.)

$\langle 2 \rangle 3.$ $\sum_{x \in X} \pi_x \iota_x = id_X.$

By item 1 of Lemma 6.8.

$\langle 1 \rangle 2.$ $(\sigma\tau)^{hom} = \sigma^{hom}\tau^{hom}$.

$\langle 2 \rangle 1.$ **Let:** $(\sigma_{xy})_{x \in X, y \in Y}$ be the matrix of σ and $(\tau_{yz})_{y \in Y, z \in Z}$ be the matrix of τ.

Proof (cont.)

$\langle 2 \rangle 2.$ $(\sigma\tau)^{hom} = \sum_{x,z} \pi_x (\sum_y \sigma_{xy}\tau_{yz})\iota_z.$

The matrix of $\sigma\tau$ has in the x-th row and z-th column the entry $\sum_y \sigma_{xy}\tau_{yz}$. Then, by the definition of $\cdot^{hom}$, we have:

$(\sigma\tau)^{hom} = \sum_{x,z} \pi_x (\sum_y \sigma_{xy}\tau_{yz})\iota_z.$

$\langle 2\rangle 3.$ $\sigma^{hom}\tau^{hom} = \sum_{x,z} \pi_x (\sum_y \sigma_{xy}\tau_{yz})\iota_z.$

$\langle 3\rangle 1.$ $\sigma^{hom}\tau^{hom} = (\sum_{x,y} \pi_x \sigma_{xy} \iota_y)(\sum_{y',z} \pi_{y'} \tau_{y'z} \iota_z).$

By the definition of $\cdot^{hom}$.

$\langle 3\rangle 2.$ $(\sum_{x,y} \pi_x \sigma_{xy} \iota_y)(\sum_{y',z} \pi_{y'} \tau_{y'z} \iota_z) = \sum_{x,y,y',z} \pi_x \sigma_{xy} \iota_y \pi_{y'} \tau_{y'z} \iota_z.$

By the distributivity of composition over pointwise addition (Proposition 6.2).

⟨3⟩3. $\sum_{x,y,y',z} \pi_x \sigma_{xy} \iota_y \pi_{y'} \tau_{y'z} \iota_z = \sum_{x,y,y',z} \pi_x \sigma_{xy} \delta_{yy'} \tau_{y'z} \iota_z$.

By item 2 of Lemma 6.8.

⟨3⟩4. $\sum_{x,y,y',z} \pi_x \sigma_{xy} \delta_{yy'} \tau_{y'z} \iota_z = \sum_{x,y,z} \pi_x \sigma_{xy} \tau_{yz} \iota_z$.

Since $\delta_{yy'} = 1$ if $y = y'$ and is 0 otherwise.

⟨3⟩5. $\sum_{x,y,z} \pi_x \sigma_{xy} \tau_{yz} \iota_z = \sum_{x,z} \pi_x (\sum_{y} \sigma_{xy} \tau_{yz}) \iota_z$.

By the distributivity of composition over pointwise addition (Proposition 6.2).

Thank You

Thank you! Any doubts? [1]

[1] I now have a webpage, where I make my texts and my slides available: https://github.com/gabriel951/my_work

Bibliography

[1] W. Nutt, "Unification in monoidal theories," in *International Conference on Automated Deduction*, Springer, 1990, pp. 618–632.

[2] L. Lamport, "How to write a 21st century proof," *J. of Fixed Point Theory and Applications*, vol. 11, no. 1, pp. 43–63, 2012.

[3] L. Lamport, "How to write a proof," *The American math. monthly*, vol. 102, no. 7, pp. 600–608, 1995.