Decidability of integer multiplication and ordinal addition

Two applications of the Feferman-Vaught theory

Ting Zhang
Stanford University

STANFORD

February 2003

The motivation

- There are many similar ways of forming products of algebraic systems in modern algebra and set theory.
- Usually definitions of products involve an index set I and in some cases take into account the structure on I.
- How to discover the first order properties of a complex system by the properties of its components?

☞ The Feferman-Vaught theory answered the question in great generality. Namely, it provides a way of relating the first order properties of a product system to the properties of its factor systems and the properties of some subset algebras on the index set.

Direct Product

- Let $\langle \mathfrak{A}_i \mid i \in I \rangle$ be an indexed family of systems $\mathfrak{A}_i = \langle A_i, \ldots \rangle$ of the same signature μ and let the corresponding language be $\mathscr{L}_\mu$.
- The direct product $\mathfrak{A} = \prod_{i \in I} \mathfrak{A}_i$ is the $\mathscr{L}_\mu$-structure such that
  - The carrier A of $\mathfrak{A}$ is the Cartesian product of $\langle A_i \mid i \in I \rangle$.
  - If F is a n-ary function symbol and $\boldsymbol{a} = \langle a_0, \ldots, a_{n-1} \rangle$ is a n-tuple of A, then for each $i \in I$,

$$F^{\mathfrak{A}}(\boldsymbol{a})(i) = F^{\mathfrak{A}_i}(a_0(i), \ldots, a_{n-1}(i)).$$

  - If R is a n-ary relation symbol and $\boldsymbol{a} = \langle a_0, \ldots, a_{n-1} \rangle$ is a n-tuple of A, then

$$\boldsymbol{a} \in R^{\mathfrak{A}} \quad \textit{iff} \quad \langle a_0(i), \ldots, a_{n-1}(i) \rangle \in R^{\mathfrak{A}_i} \quad \textit{for each } i \in I.$$

Preliminary Notations

- Let $\mathscr{L}_\mu$ be the language of component systems $\langle \mathfrak{A}_i \mid i \in I \rangle$.
- Let $\mathscr{L}_\sigma$ be the language of the basic subset algebra

$$\mathfrak{S}_I = \langle S(I), \Lambda, \cup, \cap, ^-, \subseteq \rangle$$

- Let $\mathscr{L}_\pi$ be the language of generalized products $\mathscr{P}(\mathfrak{A}, \mathfrak{S})$.
- A sequence $\zeta = \langle \Phi, \theta_0, \ldots, \theta_m \rangle$ is called a **reduction sequence** if Φ is a formula of $\mathscr{L}_\sigma$ with at most the free variables $X_0, \ldots, X_m$, and $\theta_0, \ldots, \theta_m$ are formulas of $\mathscr{L}_\mu$.
- A variable v is **free** in ζ if v is free in at least one of $\theta_0, \ldots, \theta_m$.

Generalized products

- For each reduction sequence $\zeta = \langle \Phi, \theta_0, \ldots, \theta_m \rangle$ with p free variables, let P_ζ be

$$\left\{ \langle a_0, \ldots, a_{p-1} \rangle \mid \boldsymbol{a} \in A^\omega \textit{ and } \mathfrak{S} \models \Phi[\|\theta_0\|\boldsymbol{a}, \ldots, \|\theta_m\|\boldsymbol{a}] \right\}.$$

☞ By the **generalized product** $\mathscr{P}(\mathfrak{A}, \mathfrak{S})$ of the algebraic systems $\mathfrak{A} = \langle \mathfrak{A}_i \mid i \in I \rangle$ with respect to the algebra $\mathfrak{S}$ of subsets of I, we mean the system

$$\mathfrak{A} = \left\langle A, P_{\zeta_0}, \ldots, P_{\zeta_n}, \ldots \right\rangle.$$

☞ If all the system $\mathfrak{A}_i$ for $i \in I$ are identical to a system $\mathfrak{B}$, then $\mathscr{P}(\mathfrak{A}, \mathfrak{S})$ is called the **generalized power** of $\mathfrak{B}$ with respect to $\mathfrak{S}$.

The basic theorem for generalized products

☞ There is an effective procedure to compute, for each formula φ of $\mathscr{L}_\pi$, a partitioning sequence $\zeta = \langle \Phi, \theta_0, \ldots, \theta_m \rangle$ such that

given any non-empty indexed family $\mathfrak{A} = \langle \mathfrak{A}_i \mid i \in I \rangle$ and any algebra $\mathfrak{S} = \langle S(I), \ldots \rangle$ with product $\mathscr{P}(\mathfrak{A}, \mathfrak{S}) = \langle A, \ldots \rangle$ and any sequence $\boldsymbol{a} \in A^\omega$, we have:

$$\mathfrak{A} \models \varphi[\boldsymbol{a}] \quad \textit{iff} \quad \mathfrak{S} \models \Phi\big[\|\theta_0\|\boldsymbol{a}, \ldots, \|\theta_m\|\boldsymbol{a}\big].$$

☞ In particular, if φ is a sentence, so are $\theta_0, \ldots, \theta_m$, and

$$\mathfrak{A} \models \varphi \quad \textit{iff} \quad \mathfrak{S} \models \Phi\big[\|\theta_0\|, \ldots, \|\theta_m\|\big].$$

The construction

- Case $\varphi = \neg\varphi'$. Suppose that φ' and a reduction sequence $\zeta' = \langle \Phi', \theta'_0, \ldots, \theta'_m \rangle$ satisfy the induction hypothesis. Take

$$\zeta = \langle \neg\Phi', \theta_0, \ldots, \theta_m \rangle.$$

- Case $\varphi = \varphi_1 \vee \varphi_2$. Suppose that φ_i $(i = 0, 1)$ has a reduction sequence $\zeta_i = \langle \Phi_i, \theta_0^{(i)}, \ldots, \theta_{m_i}^{(i)} \rangle$. Take

$$\zeta = \langle \Phi_1 \vee \Phi_2, \theta_0^{(1)}, \ldots, \theta_{m_1}^{(1)}, \theta_0^{(2)}, \ldots, \theta_{m_2}^{(2)} \rangle.$$

The construction

☞ Case $\varphi = \exists v_k \varphi'$. Suppose that φ' and a reduction sequence $\zeta' = \langle \Phi', \theta'_0, \ldots, \theta'_m \rangle$ satisfy the induction hypothesis. Take

$$\zeta = \langle \Phi, \theta_0, \ldots, \theta_m \rangle, \tag{1}$$

where $\theta_i = \exists v_k \theta'_i \quad (i \leq m)$, and

$$\Phi = \exists U_0 \ldots U_m \big[Part_m(U_0, \ldots, U_m) \wedge \\ \bigwedge_{i \leq m} (U_i \subseteq V_i) \wedge \Phi'(U_0, \ldots, U_m) \big]. \tag{2}$$

Consequences of the basic theorem

- ☞ *The decision problem for the theory of the generalized product of systems $\langle \mathfrak{A}_i \mid i \in I \rangle$ with respect to $\mathfrak{S}$, in the case that I is finite can be reduced to the decision problem for the theories of the factors. I.e., if each factor has a decidable theory, then so has the (finite) generalized product.*
- ☞ *The decision problem for the theory of the generalized power $\mathfrak{B}^{\mathfrak{S}}$ reduces to the decision problems for the theories of $\mathfrak{B}$ and of $\mathfrak{S}$. I.e., if theory of $\mathfrak{B}$ and theory of $\mathfrak{S}$ are decidable, so is the theory of $\mathfrak{B}^{\mathfrak{S}}$.*

Examples of generalized products

- **Direct products**
- **Weak direct products**
- **Cardinal sums**
- Countably weak direct products
- Ordinal products
- Weak ordinal products
- Ordinal sums

Direct products

- The **direct product** of an indexed family $\mathfrak{A} = \langle \mathfrak{A}_i \mid i \in I \rangle$, where for each $i \in I$, $\mathfrak{A}_i = \langle A_i, R_i \rangle$, is the system

$$\langle A, R \rangle,$$

where $A = \mathscr{P}(A_i \mid i \in I)$, and for any $a, b \in A$,

$$\langle a, b \rangle \in R \ \textit{ iff } \ \{i \mid \langle a(i), b(i) \rangle \in R_i\} = I.$$

☞ A direct product can be viewed as a generalized product by letting

- $\mathfrak{S} = \langle S(I), \Lambda, \cup, \cap, {}^{-}, \subseteq \rangle$,
- $\theta = Rv_0v_1, \ \Phi \equiv V_0 = \overline{\Lambda}$ *and* $\zeta = \langle \Phi, \theta \rangle$.

Weak direct products

- A **weak direct product** of an family $\mathfrak{A} = \langle \mathfrak{A}_i \mid i \in I \rangle$, where for each $i \in I$, $\mathfrak{A}_i = \langle A_i, R_i \rangle$, is the system $\langle A^*, R^* \rangle$, where $A^* \subseteq A$,

$$a \in A^* \quad \textit{iff} \quad \{\, i \mid i \in I \textit{ and } \mathfrak{A}_i \models \neg\psi[a(i)] \,\} \textit{ is finite},$$

  and where R^* is the relation R restricted to A^*.

☞ A weak direct product can be viewed as a *relativized* generalized product by letting

- $\mathfrak{S} = \langle S(I), \Lambda, \cup, \cap, ^{-}, \subseteq, Fin \rangle$,
- $\theta^* = \neg\psi(v_0)$, $\theta = Rv_0v_1$, $\Phi \equiv V_0 = \overline{\Lambda}$, *and* $\zeta = \langle \Phi, \theta^*, \theta \rangle$.

Cardinal sums

- A **cardinal sum** of a non-empty indexed family $\mathfrak{A} = \langle \mathfrak{A}_i \mid i \in I \rangle$, where A_i and A_j are disjoint for any $i, j \in I$, is the system

$$\langle \bigcup_{i \in I} A_i, \bigcup_{i \in I} R_i \rangle.$$

- The cardinal sum can be reformulated as the relativized generalized product of the systems $\mathfrak{B} = \langle \mathfrak{B}_i \mid i \in I \rangle$, where

$$\mathfrak{B}_i = \langle A_i \cup \{c_i\}, R_i, \{c_i\} \rangle$$

and for each $i \in I$, $c_i \notin A_i$.

Cardinal sums

- More precisely, let $A = \mathscr{P}(B_i \mid i \in I)$ and let $A^* \subseteq A$ for which

$$a \in A^* \quad \textit{iff} \quad \{i \mid a(i) \neq c_i\} \textit{ is a singleton.}$$

- For $a, b \in A^*$, let

$$\langle a, b\rangle \in R^* \quad \textit{iff} \quad \{i \mid \langle a(i), b(i)\rangle \in R_i\} \neq \Lambda.$$

☞ A cardinal sum can be viewed as a relativized generalized product by putting

- $\mathfrak{S} = \langle S(I), \Lambda, \cup, \cap, {}^-, \subseteq\rangle$,
- $\theta^* \equiv v_0 \neq c$, $\theta = Rv_0v_1$, $\Phi \equiv X_0 \neq \Lambda$, *and* $\zeta = \langle \Phi, \theta^*, \theta\rangle$.

The basic subset algebras

- ☞ A sentence of $\mathscr{L}_\sigma$ of the basic subset algebras says "how many elements are in the domain."
- ☞ The theory of any one system $\mathfrak{S}_I$ is decidable.
- ☞ The theory of all systems $\mathfrak{S}_I$ is decidable.
- ☞ The theory of all systems $\mathfrak{S}_I$ is the same as the theory of all systems $\mathfrak{S}_I$ where I is finite.
- ☞ Two systems $\mathfrak{S}_I$ and $\mathfrak{S}_{I'}$ are elementarily equivalent if and only if I and I' both have the same finite cardinality or both are infinite.

Subset algebras with Fin

- Denote by $\mathfrak{S}'_I = \langle S(I), \Lambda, \cup, \cap, {}^-, \subseteq, Fin \rangle$ the subset algebras with Fin and let $\mathscr{L}'_\sigma$ be the corresponding language.
- Any formula $\varphi(\boldsymbol{y})$ of $\mathscr{L}'_\sigma$ reduces to a disjunctive normal form where each literal is in one of the following forms

$$
\begin{array}{lll}
E_i(C(\boldsymbol{y})) & \textit{or} & A_j(C(\boldsymbol{y})) \\
 & \textit{or} & A_k(C(\boldsymbol{y})) \wedge Fin(C(\boldsymbol{y})) \\
 & \textit{or} & \neg Fin(C(\boldsymbol{y})).
\end{array}
$$

☞ A sentence of $\mathscr{L}'_\sigma$ says "how many elements are in the domain" and/or "whether the domain is finite."

Integer multiplication

- Let $\mathfrak{A} = \langle \mathbb{P}, \cdot \rangle$ be the system where $\mathbb{P}$ is the set of positive integers and $\cdot$ is the ordinary multiplication.
- Let $\mathfrak{B} = \langle \omega, + \rangle$ be Presburger arithmetic.
- Let $\mathfrak{C} = \langle C, M \rangle$ be the relational system, where C is the set of sequences $a \in \omega^{(\omega)}$ for which

  $$\{i \mid i \in \omega \text{ and } a(i) \neq 0\} \text{ is finite},$$

  and for $a, b, c \in C$,

  $$\langle a, b, c \rangle \in M \quad \text{iff} \quad a(i) + b(i) = c(i) \text{ for all } i \in \omega.$$

Integer multiplication

- $\mathfrak{C}$ is a relativized generalized power of $\mathfrak{B}$ with respect to the subset algebra

$$\mathfrak{S}'_\omega = \langle S(\omega), \Lambda, \cup, \cap, ^-, \subseteq, Fin \rangle.$$

- $\mathfrak{C}$ is isomorphic to $\mathfrak{A}$ under the map $f : C \to \mathbb{P}$ for which

$$f(x) = f(x_0, \ldots, x_n, \ldots) = p_0^{x_0} p_1^{x_1} \cdots p_n^{x_n} \cdots$$

where $p_0, \ldots, p_n, \ldots$ is the increasing enumeration of primes.

☞ The theory of $\mathfrak{A}$ is decidable. It follows that the theory of integer multiplication is also decidable.

Decision procedure for integer multiplication

1. Given a sentence of structure $\mathfrak{C}$, find the reduction sequence

$$\langle \Phi, \theta_0, \ldots, \theta_{m-1} \rangle$$

   where Φ is a formula of $\mathfrak{S}'_\omega$, and θ_i $(i < m)$ are sentences of Presburger arithmetic $\mathfrak{B}$.

2. Call the decision procedure of $\mathfrak{B}$ to construct an assignment tuple

$$\langle V_0, \ldots, V_{m-1} \rangle$$

   where for each $i < m$, $V_i = I$, if θ_i is true, and $V_i = \Lambda$ otherwise.

3. Call the decision procedure of the basic subset algebra to decide the truth of the sentence

$$\Phi[V_0, \ldots, V_{m-1}]$$

Subset algebras with $\prec$

- Denote by $\mathfrak{S}_I^{\prec} = \langle S(I), \Lambda, \cup, \cap, ^{-}, \subseteq, \prec \rangle$ the subset algebras, where I is linearly ordered by a relation $<$ and $\prec$ is an induced order on singleton subsets of I, for which

$$X \prec Y \quad \textit{iff} \quad \textit{there exist } i, j \in I \textit{ s.t. } X = \{i\}, Y = \{j\} \textit{ and } i < j.$$

☞ $\mathfrak{S}_I^{\prec}$ is a version of monadic second order systems of linear orders.

☞ In particular, when $I = \omega$, $Th(\mathfrak{S}_\omega^{\prec})$ is $S1S$ and decidable.

Ordinal addition

- Let $\mathfrak{A} = \langle \omega, + \rangle$ be Presburger arithmetic.
- Let $\mathfrak{B} = \langle B, R \rangle$ be the relativized generalized power of $\mathfrak{A}$ with respect to the subset algebra $\mathfrak{S}_\rho^{\prec}$, where B is the weak power $\omega^{(\rho)}$, and where the relation R is defined such that for $a, b, c \in A$,

$\langle a, b, c \rangle \in R$ *if and only if*

either, *for all* $\xi < \rho$, $b(\xi) = 0$ *and* $a(\xi) = c(\xi)$;

or, *for some* $\xi < \rho$, $b(\xi) \neq 0$ *and* $a(\xi) + b(\xi) = c(\xi)$,

and, for all η *such that* $\xi < \eta < \rho$, $b(\eta) = 0$ *and* $a(\eta) = c(\eta)$,

and, for all $\eta < \xi$, $b(\eta) = c(\eta)$.

Ordinal addition

- Let $\mathfrak{C} = \langle \omega^\rho, S \rangle$ be the relational system of addition of ordinal numbers, where ω^ρ should be read as the ordinal exponentiation, and S is addition of ordinal numbers restricted to ω^ρ.

- $\mathfrak{C}$ and $\mathfrak{B}$ are isomorphic under the map $f : C \to B$ for which if the Cantor normal form of α ($\alpha < \omega^\rho$) is

$$\alpha = \omega^{\xi_0} \cdot k_0 + \omega^{\xi_1} \cdot k_1 + \ldots + \omega^{\xi_{p-1}} \cdot k_{p-1}$$

(where $\rho > \xi_0 > \xi_1 \ldots > \xi_{p-1}$ and $0 \neq k_i \in \omega$ for $i < p$), then

$$f(\xi_i) = k_i \;\; \textit{for each} \;\; i < p, \;\; \textit{and} \;\; f(\eta) = 0 \; \textit{otherwise.}$$

☞ The theory of $\mathfrak{B}$ is decidable, and so is the theory of $\mathfrak{C}$.

Cardinal addition

- Let $\mathfrak{A} = \langle \omega, + \rangle$ be Presburger arithmetic.
- Let $\mathfrak{B} = \langle \rho, S \rangle$ be the relational system, where ρ is an arbitrary ordinal number different from 0 and S be the relation such that for $\alpha, \beta, \gamma \in \rho$,

$$\langle \alpha, \beta, \gamma \rangle \in S \;\; \textit{iff} \;\; \alpha \leq \beta \textit{ and } \gamma = \beta \textbf{\textit{ or }} \beta \leq \alpha \textit{ and } \gamma = \alpha.$$

- Let $\mathfrak{C} = \langle C, + \rangle$ be the relational system of addition of cardinal numbers, where C is the set of all cardinal numbers $\leq \aleph_\rho$ and $+$ is addition of cardinal numbers restricted to C.

Cardinal addition

- Let $\mathfrak{D} = \langle D, R\rangle$ be the relativized generalized product of $\mathfrak{A}$ and $\mathfrak{B}$, where D is the disjoint union of ω and ρ, and where the relation R is defined such that for $\alpha, \beta, \gamma \in D$,

$$
\begin{array}{lll}
\langle \alpha, \beta, \gamma\rangle \in R & \textit{iff} & \alpha, \beta \in \omega \textit{ and } \alpha + \beta = \gamma \\
 & or & \alpha \in \omega \textit{ and } \beta \in \rho \textit{ and } \gamma = \beta \\
 & or & \alpha \in \rho \textit{ and } \beta \in \omega \textit{ and } \gamma = \alpha \\
 & or & \alpha \in \rho \textit{ and } \beta \in \rho \textit{ and } \langle \alpha, \beta, \gamma\rangle \in S.
\end{array}
$$

- $\mathfrak{D}$ and $\mathfrak{C}$ are isomorphic under the map $f : D \to C$ for which

$$f(\alpha) = \alpha \quad \textit{if } \alpha \in \omega, \quad \textit{and} \quad f(\alpha) = \aleph_\alpha \quad \textit{if } \alpha \in \rho.$$

☞ The theory of $\mathfrak{D}$ is decidable, and so is the theory of $\mathfrak{C}$.

References

[FV59] S. Feferman and R.L. Vaught. The first order properties of products of algebraic systems. *Fundamenta Mathematicae*, 47:57–103, 1959.

[Hod97] Wilfrid Hodges. *A Shorter Model Theory*. Cambridge University Press, Cambridge, 1997.