A puzzle about Gödel's numbering

James Avery[1] Jean-Yves Moyen[1] Jakob Grue Simonsen[1]
Jean-Yves.Moyen@lipn.univ-paris13.fr

[1]Datalogisk Institut
University of Copenhagen

Supported by the VILLUM FONDEN network for Experimental Mathematics in Number Theory, Operator Algebras, and Topology; the Marie Curie action "Walgo" program H2020-MSCA-IF-2014 number 655222; and the Danish Council for Independent Research *Sapere Aude* grant "Complexity via Logic and Algebra" (COLA).

October 6-7 2016

Part 2: some answers

The puzzle

Can you choose:

- a programming language, `Pgms`;
- a Gödel's numbering, ε, for it;
- a binary operator, $\mathbb{F}$, on it;

such that the induced operator, F, on numbers is "as simple as possible"?

Sequential composition: $\mathbb{S}$ (on programs), S (on numbers).
Parallel composition: $\mathbb{P}, \mathrm{P}$.

Compositions

What is a "sequential composition" operator on programs?

Something that behaves as expected with respect to semantics!

$$\mathbb{S}(\mathtt{p}, \mathtt{q}) = \mathtt{r} \text{ with } [\![\mathtt{r}]\!] = [\![\mathtt{p}]\!] \circ [\![\mathtt{q}]\!]$$

Same goes with (non-deterministic, no communication) parallel composition:

$$[\![\mathbb{P}(\mathtt{p}, \mathtt{q})]\!] = [\![\mathtt{p}]\!] \mid\mid [\![\mathtt{q}]\!]$$

A deceptively simple answer

Commutativity

If S (on number) is commutative, then so must be $\mathbb{S}$ (on programs). (because ε is a morphism)

$$\varepsilon(\mathbb{S}(\mathtt{p},\mathtt{q})) = \mathrm{S}(\varepsilon(\mathtt{p}),\varepsilon(\mathtt{q})) = \mathrm{S}(\varepsilon(\mathtt{q}),\varepsilon(\mathtt{p})) = \varepsilon(\mathbb{S}(\mathtt{q},\mathtt{p}))$$

By injectivity: $\mathbb{S}(\mathtt{p},\mathtt{q})) = \mathbb{S}(\mathtt{q},\mathtt{p})$.

Addition is commutative. Sequential composition is not commutative (because $\circ$ is not). Therefore, there is no Gödel encoding and sequential composition such that S is addition.

Associativity

Sequential composition may be not associative: we're on the syntactical level, so `{{x++;y++};z++}` and `{x++;{y++;z++}}` are two different commands (strings).

But since $\circ$ is associative, associative sequential composition operator do exists.

Theorem (Bell, 1936): the only associative polynomials with 2 variables are the projections and
$P(X, Y) = a + b \cdot (X + Y) + c \cdot XY$.

Sequential composition cannot be a projection. The other solution is commutative.

There is no Gödel encoding and associative sequential composition such that S is a polynomial.

Going further

Other functions

Theorem (Aczèl, 1948): a function on the real numbers is continuous, strictly increasing and associative iff it has the shape

$$M(x, y) = f^{-1}(f(x) + f(y))$$

Especially, it is then commutative.

There is no Gödel encoding and sequential composition such that S can be extended as a continuous, strictly increasing and associative function.

One extension with the property is enough!

Thus, we need infinitely many discontinuities (or decreases) in **all** the possible extensions to the reals.

Concatenation

It is possible to design a language and an encoding such that concatenation (of the programs, or the binary encodings) is a sequential composition.

Idea: assembly like language, one designed input-output register (must reset all other to 0 before ending), only relative jumps, encoding with leading '1' everywhere.

Concatenation is $x, y \mapsto x \times 2^{\lfloor \log y \rfloor + 1} + y$, roughly equal to $(2x+1) \cdot y$. Simple, and polynomially bounded!

Parallel composition

Distributivity

Parallel composition can be commutative, so we cannot rule out addition so easily.

On functions, sequential composition is distributive over parallel composition:

$$f \circ (g \mid\mid h) = (f \circ g) \mid\mid (f \circ h)$$

Thus, there exist sequential composition operators which are distributive over a parallel composition operator.

There is no operation on the natural number that is distributive over multiplication.

Therefore, parallel composition cannot be multiplication (if there is a sequential composition distributing over it).

It's all about functions

$$
\begin{array}{ccc}
(\mathtt{Pgms}, \mathbb{F}) & \xrightarrow{\mathcal{E}} & (N, \mathrm{F}) \\
\Big\downarrow \llbracket \bullet \rrbracket & & \Big\downarrow [\bullet] \\
(\mathcal{C}, \widehat{\mathbb{F}}) & \xrightarrow{\widehat{\mathcal{E}}} & (C, \widehat{\mathrm{F}})
\end{array}
$$

Sequential composition: $\widehat{\mathbb{S}} = \circ$, parallel composition: $\widehat{\mathbb{P}} = ||$.
$\widehat{\mathbb{P}}$ is compatible with $\llbracket \bullet \rrbracket$:

$$\llbracket \mathtt{p} \rrbracket = \llbracket \mathtt{p}' \rrbracket \Rightarrow \left\llbracket \widehat{\mathbb{P}}(\mathtt{p}, \mathtt{q}) \right\rrbracket = \left\llbracket \widehat{\mathbb{P}}(\mathtt{p}', \mathtt{q}) \right\rrbracket$$

Computable functions

$$
\begin{array}{ccc}
(\texttt{Pgms}, \mathbb{P}) & \xrightarrow{\varepsilon} & (N, \mathrm{P}) \\
\Big\downarrow \llbracket \bullet \rrbracket & & \Big\downarrow [\bullet] \\
(\mathcal{C}, \widehat{\mathbb{P}}) & \xrightarrow{\widehat{\varepsilon}} & (C, \widehat{\mathrm{P}})
\end{array}
$$

$\llbracket \bullet \rrbracket$ is the extensional equivalence, it must have the same structure as $[\bullet]$, especially P must be compatible with $[\bullet]$.

Equivalences on the natural numbers compatible with addition have finitely many non-singleton classes. $\llbracket \bullet \rrbracket$ has infinitely many infinite classes.

Therefore, there is no Gödel encoding and parallel composition such that P is addition.