Congruential Functions in Category Theory & Logic

(extended abstract)

Peter M. Hines – University of York

Historical Background

In the 1930s Lothar Collatz described, but did not publish, a series of seemingly simple puzzles based on iterating elementary arithmetic functions. These rapidly became well-known, and have wasted a great deal of time from very many good mathematicians ever since.

The functions in question were simply piecewise-linear maps on the natural numbers, and a common reaction on first encountering them is that it should be simple, if not trivial, to decide – for example – whether a given number has a finite or infinite orbit. This is not the case; considering the most notorious of his problems (the $3x + 1$ conjecture) P. Erdös stated, 'mathematics is not yet ready for such problems'.

In 1972, J. Conway gave [6] a convincing explanation why such questions might be not only difficult, but impossible to resolve; not just 'beyond the reach of modern mathematics' [17], but beyond our reach forever. He demonstrated[1] that this toolkit of piece-wise linear arithmetic functions was sufficient to encode computational universality. Deciding whether a given natural number has a finite orbit is precisely as easy or difficult as deciding whether a computer program terminates on a given input. This may be possible or even easy for particular examples, but in general is undecidable.

1 Computational universality in elementary arithmetic

Collatz's problems, and J. Conway's demonstration of computational universality in elementary arithmetic, were based on *congruential functions*. These may be defined as follows[2]: The starting point is a dissection of the natural numbers into (disjoint) congruence classes $\{A_j\mathbb{N} + B_j\}_{j\in J}$, so $\mathbb{N} = \bigcup_{j\in J} A_j\mathbb{N} + B_j$ and $(A_i\mathbb{N} + B_i) \cap (A_j\mathbb{N} + B_j) = \emptyset$ for $i \neq j$. The congruential function is given by applying a distinct linear map, conditioned on the congruence class to which the argument number belongs. The overall effect is as the union of partial linear maps with disjoint domains, of the form $A_j\mathbb{N} + B_j \mapsto C_j\mathbb{N} + D_j$.

The demonstration of computational universality given in [6] was in terms of an encoding of Universal Register Machines. Conway also later gave a simple programming language that he called FRACTRAN [5], and demonstrated how this could compute $k.2^{2^n} \mapsto 2^{2^{f(n)}}$, for constant k and arbitrary computable function f. Other computationally universal systems include S. Burckel's encoding of Minsky Machines [3], and Sergei Maslov's representation of Post Production systems [19].

No direct explicit encoding of Turing Machines appears to have been given. This could of course be done via an encoding of TMs into any of the above computational models, but the resulting arithmetic system is unlikely to be particularly elegant! A similar route to encoding the pure untyped lambda calculus would likely be equally messy.

2 Categorical & logical interpretations of elementary arithmetic

The number theorists' loss is our gain: undecidability is simply a natural side-effect of the ability to express universal computation – which, ultimately, is much more interesting than questions of whether certain numbers eventually return to their starting point after repeated applications of some rather arbitrary-looking function.

In any such system capable of expressing computational universality, we expect to find structures and tools associated with fundamental features of logic, lambda calculus, and monoidal category theory, such as Cartesian or Compact Closure, reflexivity, and categorical coherence. This is the motivation behind this talk.

[1] In the Cold War era, many results were simultaneously and independently discovered on either side of the Iron curtain. Conway's result was no exception; Sergei Maslov's 1968 paper [19] would have been a very significant precursor.

[2] The following definition is the special case of S. Burckel [3]. This is enough to both express computational universality, and Collatz's original problems.

2.1 Logical systems based on iterated functions on the natural numbers

Our starting point is a model of linear logic that has long been known to have connections with iteration of functions on the natural numbers. It was independently discovered by many authors [11, 1, 10, 2] that J.-Y. Girard's Geometry of Interaction series of papers [7, 8, 9] interpret propositions as (partial, injective) functions on the natural numbers, and his famous resolution formula – describing the dynamics of cut-elimination – is precisely an encoding of Joyal, Street, & Verity's 'particle-style' categorical trace [16]. This operation has the natural interpretation as a form of conditional iteration [13] – a more 'refined' or 'controllable' version of the Kleene star – and this accounts for why it has since found uses outside models of linear logic, in fields such as two-way automata [12], Scott domains [13], combinatory algebras [2], space-bounded Turing machines [13], and quantum circuits [14].

2.2 Congruential functions & categorical conjunctions

The interpretation of Girard's resolution formula as iteration is well-established, and well-studied. This talk considers whether there is also a rôle for congruential functions in the Geometry of Interaction series, or related systems?

The key to this is the notion of *categorical coherence*, for both associativity and symmetry. The model of multiplicative conjunction used in [7, 8] is not only an injective monoid homomorphism of the form $(\_ \star \_) : \mathcal{M} \times \mathcal{M} \hookrightarrow \mathcal{M}$, but is a (semi-)monoidal tensor on this monoid. In [15], it is demonstrated – as a generalisation of J. Isbell's argument as quoted in [18] – that no such tensor can be strictly associative (i.e. satisfy $f \star (g \star h) = (f \star g) \star h$) unless the monoid in question is highly degenerate (abelian, with tensor and composition coinciding).

Although Girard's conjunction is not strictly associative, it is nevertheless associative *up to canonical isomorphism*; there exists some fixed bijection $\alpha : \mathbb{N} \to \mathbb{N}$ satisfying

Naturality $\alpha(f \star (g \star h)) = ((f \star g) \star h)\alpha$

MacLane's pentagon condition $\alpha^2 = (\alpha \star Id)\alpha(Id \star \alpha)$

The 'naturality' property allows us to perform arbitrary re-bracketings, and the 'pentagon', or 'coherence' condition ensures that any two ways of performing the same bracketing are identical.

The *associator* for Girard's conjunction is also a classic example of a congruential function in the sense of both [6, 3]. We thus encounter congruential functions not at the level of propositions, connectives, or operators, but as the structural morphisms that ensure properties such as 'associative up to isomorphism' are well-behaved.

As a preliminary step, we first demonstrate that Collatz-like problems for this congruential function are trivial, and give a characterisation of finite & infinite orbits of natural numbers. We then use the above naturality property, and the well-known connection between associativity laws and Thompson's group $\mathcal{F}$ to give a presentation of $\mathcal{F}$ as a group of congruential functions.

2.3 Generalised conjunctions, and congruential natural isomorphisms

Our next step is to generalise Girard's conjunction in a natural way to an indexed family of such homomorphisms. We treat these operadically, and compose them to give generalised conjunctions in 1:1 correspondence with the operad of rooted planar trees (and thus arbitrary facets of Stasheff's associahedra).

We exhibit a natural isomorphisms between generalised conjunctions; these have, as components, a much more general class of congruential functions. We give an explicit description of the simplest non-trivial case, which consists of the associator for Girard's conjunction, together with two distinct ways of expressing a problem posed by L. Collatz (the motivating example for J. Conway's result on computational universality in elementary arithmetic). As a simple corollary, we give a derivation of Thompson's $\mathcal{F}$ from a conjecture of Collatz.

The number-theoretic formulæ for the general case are also given, in terms of a formula commonly attributed to G. Cantor [4].

3 Congruential functions as canonical coherence isomorphisms

The 1:1 correspondence between (composites of) generalised conjunctions and rooted planar trees allows us to consider Stasheff's associahedra as having facets labelled by generalised conjunctions. The above family of congruential functions gives unique morphisms between any two facets, allowing us to treat arbitrary associahedra as commuting categorical diagrams. Thus, our interpretation takes place in a posetal category, closed under generalised conjunctions. This generalises MacLane's posetal monoidal category $\mathcal{W}$ in a natural way, and allows us to claim this family of congruential functions as canonical coherence isomorphisms.

References

[1] S. Abramsky. Retracing some paths in process algebra. In U. Montanari and V. Sassone, editors, *CONCUR '96: Concurrency Theory*, pages 1–17. Springer Berlin Heidelberg, 1996.

[2] S. Abramsky, E. Haghverdi, and P. Scott. Geometry of interaction and linear combinatory algebras. *Mathematical Structures in Computer Science*, 12 (5), 2002.

[3] Serge Burckel. Functional equations associated with congruential functions. *Theor. Comput. Sci.*, 123:397–406, 1994.

[4] Georg Cantor. Über einfache zahlensysteme. *Zeitschrift für Math. und Physik*, 14:121–128, 1869.

[5] J. H. Conway. *FRACTRAN: A Simple Universal Programming Language for Arithmetic*, pages 4–26. Springer New York, 1987.

[6] John Conway. Unpredictable iterations. *Proc. 1972 Number Theory*, pages 49–52, 1972.

[7] J.-Y. Girard. Geometry of interaction 1. In *Proceedings Logic Colloquium '88*, pages 221–260. North-Holland, 1988.

[8] J.-Y. Girard. Geometry of interaction 2: deadlock-free algorithms. In *Conference on Computer Logic*, volume 417 of *Lecture Notes in Computer Science*, pages 76–93. Springer, 1988.

[9] J.-Y. Girard. Geometry of interaction 3: Accommodating the additives. In *In: Advances in Linear Logic, LNS 222,CUP, 329–389*, pages 329–389. Cambridge University Press, 1995.

[10] E. Haghverdi. *A categorical approach to linear logic, geometry of proofs and full completeness.* PhD thesis, University of Ottawa, 2000.

[11] P. Hines. *The algebra of self-similarity and its applications.* PhD thesis, University of Wales, Bangor, 1997.

[12] P. Hines. A categorical framework for finite state machines. *Mathematical Strucures in Computer Science*, 13:451–480, 2003.

[13] P. Hines. Machine semantics. *Theoretical Computer Science*, 409:1–23, 2008.

[14] P. Hines. Quantum circuit oracles for abstract machine computations. *Theoretical Computer Science*, 411:1501–1520, 2010.

[15] P. Hines. Coherence and strictification for self-similarity. *Journal of Homotopy & Related Structures*, 2016.

[16] A. Joyal, R. Street, and D. Verity. Traced monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, 119(3):447–468, 1996.

[17] J. Lagarias. The $3x + 1$ problem and its generalisations. *Amer. Math. Monthly*, 92:3–23, 1985.

[18] S. MacLane. *Categories for the working mathematician.* Springer-Verlag, New York, second edition, 1998.

[19] Sergei Ju. Maslov. On e. l. post's "tag problem". In B. M. Budak, editor, *Eleven Problems on Logic, Algebra, Analysis, and Topology*, A.M.S. Translations. American Mathematical Society, 1971.