Church, Turing and the Entscheidungsproblem

Dana S. Scott

University Professor Emeritus
Carnegie Mellon University
Visiting Scholar
University of California, Berkeley

Patrick Suppes' 90th Birthday Symposium
Stanford University, March 9-10-11, 2012

A Recent Letter to the AMS

This is a response to the article “A revolution in mathematics? What really happened a century ago and why it matters today”, by Frank Quinn, (Notices, Jan. 2012).

My mathematics colleagues almost never think about mathematical logic (see: “The ideal mathematician”, Philip J. Davis & Reuben Hersh, for what is simultaneously the funniest and most profound description of mathematicians!!). Mathematical logic is almost never taught in mathematics departments — it’s taught in computer science departments and philosophy departments — and, when it is, it is taught in a purely technical way with no concern for history or philosophy.

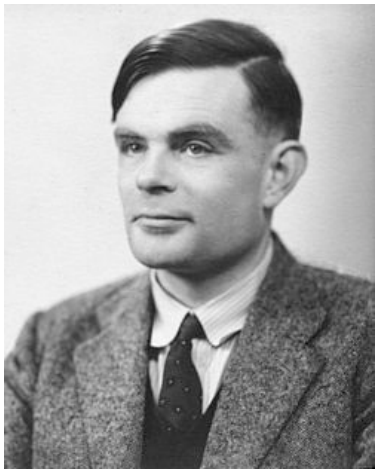
Mathematicians still live in Cantor’s paradise — or even Eilenberg’s paradise — in spite of Russell’s paradox; they simply learn not to make certain moves that lead to trouble (as long as the referee doesn’t complain, what, me worry?). The various formalizations for avoiding Russell’s paradox also prevent one from making certain moves which are usually safe and powerful. So mathematicians work informally and have always done so; there is almost no trace of mathematical logic in most of the history of modern mathematics!!

I’m not saying that mathematicians are aware of what I just said; most are totally unaware of these issues and are simply working in a successful research tradition.

— David A. Edwards (University of Georgia)

Church vs. Turing

Born: 14 June 1903 in Washington, D.C., USA.
Died: 11 Aug 1995 in Hudson, Ohio, USA.
Ph.D.: Princeton University, 1927, USA.



Born: 23 June 1912, Maida Vale, London, UK.
Died: 7 June 1954, Wilmslow, Cheshire, UK.
Ph.D.: Princeton University, 1938, USA.

Alonzo Church, "An Unsolvable Problem in Elementary Number Theory," Amer. J. of Math., vol. 5 (1936), pp. 345-363.

Alonzo Church, "A Note on the Entscheidungsproblem," J. of Symbolic Logic, vol. 1 (1936) pp. 40-41. Correction ibid, pp. 101-102.

Alan Turing,"On Computable Numbers with an Application to the Entscheidungsproblem," Proc. of the London Math. Soc., vol. 42 (1936), pp. 230-267. Correction: vol. 43 (1937), pp. 544-546.

Alan Turing,"Computability and λ-definability". Journal Symbolic Logic, vol. 2 (1937), pp. 153-163.

Church's Solution

Theorem. Only a finite number of axioms are needed to define a ***non-recursive*** set of integers.

R.M.Robinson's Arithmetic

(1) $\forall x \forall y [x = y \iff Sx = Sy]$

(2) $\forall x [x = 0 \iff \neg \exists y.\ x = Sy]$

(3) $\forall x \forall y [(x + 0) = x \ \& \ (x + Sy) = S(x + y)]$

(4) $\forall x \forall y [(x \times 0) = 0 \ \& \ (x \times Sy) = ((x \times y) + x)]$

Turing's Solution

Theorem. Only a finite number of axioms are needed to define the ***Universal Turing Machine***.

Minskyizing the UTS

Starting with Claude Shannon in 1956, many people — often in competition with Marvin Minsky — have proposed ***very small*** UTMs (but their operation usually requires extensive coding of patterns). But, axiomatically, they do not require as many axioms as Turing did.

Post-Markov's Solution

The basic idea of Post (1943) was that a logistic system is simply a set of rules specifying how to ***change*** one string of symbols (antecedent) into another string of symbols (consequent).

The Word Problem for Semigroups

(1) $\forall x \forall y [x\ 1 = x = 1\ x]$

(2) $\forall x\ \forall y\ \forall z [x\ (y\ z) = (x\ y)\ z]$

Problem: Determine the provability of

$A_0 = B_0 \ \& \ A_1 = B_1 \ \& \ \ldots \ \& \ A_{n-1} = B_{n-1} \Longrightarrow A_n = B_n$.

Schönfinkel-Curry's Solution

Schönfinkel in 1924 and then Curry in 1929, both at Göttingen, began the study of ***combinators***, which were quickly connected with Church's **λ-*calculus*** of 1932.

Another Undecidable Theory

(1) $\forall x \forall y [\mathbf{K}(x)(y) = x]$

(2) $\forall x \ \forall y \ \forall z [\mathbf{S}(x)(y)(z) = x(z)(y(z))]$

(3) $\neg \ \mathbf{K} = \mathbf{S}$

Problem: Determine the provability of T = **K**(**S**(**K**)(**K**)).

Introducing a New Notation

Instead of writing

F(X)

write

FX.

and also write

XF:

The idea is that — using Reverse Polish — FX. means calculate F first, and then apply it to X. But XF: means calculate X first, then do FX. .

Scott's Solution: Deterministic Combinators

⟨var⟩ ::= x | y | z | .....

⟨const⟩ ::= **K** | **S** | **Q**

⟨symb⟩ ::= ⟨var⟩ | ⟨const⟩ | **.** | **:**

⟨term⟩ ::= ⟨var⟩ | ⟨const⟩ | ⟨term⟩⟨term⟩**.** | ⟨term⟩⟨term⟩**:**

⟨end⟩ ::= ⟨var⟩ | ⟨const⟩ | ⟨const⟩⟨term⟩**.** | **S**⟨term⟩**.**⟨term⟩**.**

⟨chain⟩ ::= ⟨empty⟩ | ⟨term⟩**.**⟨chain⟩ | ⟨term⟩**:**⟨chain⟩

Theorem. All ***terms*** are uniquely of one of the four kinds, and all ***chains*** are uniquely of one of the three kinds.

Theorem. All terms are uniquely of the form ⟨end⟩⟨chain⟩ with ⟨end⟩ maximal, and strings of the form ⟨term⟩⟨chain⟩ are always terms.

Left-Right Reduction Rules

Because all terms are uniquely of the form ⟨end⟩⟨chain⟩ **with** ⟨end⟩ **maximal, and strings of the form** ⟨term⟩⟨chain⟩ **are always terms, we stipulate deterministic one-step reductions:**

(1) ⟨end⟩⟨term⟩**:**⟨chain⟩ ≽ ⟨term⟩⟨end⟩**.**⟨chain⟩

(2) **K**⟨term1⟩**.**⟨term2⟩**.**⟨chain⟩ ≽ ⟨term1⟩⟨chain⟩

(3) **S**⟨term1⟩**.**⟨term2⟩**.**⟨term3⟩**.**⟨chain⟩ ≽

⟨term1⟩⟨term3⟩**.**⟨term2⟩⟨term3⟩**..**⟨chain⟩

(4) **Q**⟨term1⟩**.**⟨term2⟩**.**⟨chain⟩ ≽ ⟨term1⟩⟨term2⟩**:**⟨chain⟩

Combinator Representations

Theorem. If [... x ... y ... z ...] is a term with free variables x, y, z, then there is a constant combinator term F such that

$Fx.y.z. \succcurlyeq^* [\ldots x \ldots y \ldots z \ldots]$

Theorem. Church's representation of numerals, $\underline{n}$, is such that for every general recursive function g(n), there is a constant combinator term G such that $G\underline{n}. \succcurlyeq^* \underline{g(n)}$.

Reduction can be Axiomatized!

$\forall x \forall y \forall z [\ 1x = x \ \& \ x1 = x \ \& \ x(yz) = (xy)z\ ]$

Const[**K**] & Const[**S**] & Const[**Q**]

$\forall t \forall s [$ Const[t] $\Longrightarrow$ Term[t]] & [Term[t] & Term[s] $\Longrightarrow$ Term[ts.] & Term[ts:]]]

$\forall t \forall s \forall k [$ Term[t] & Term[s] & Const[k] $\Longrightarrow$ End[k] & End[kt.] & End[**S**t.s.]]

$\forall t \forall c [$ Chain[1] & [Term[t] & Chain[c]] $\Longrightarrow$ Chain[t.c] & Chain[t:c]]

$\forall t \forall s [$ Term[t] $\Longrightarrow$ Red[t, t]] & [Red[t, s] & Red[s, r] $\Longrightarrow$ Red[t, r]]

$\forall e \forall t \forall s \forall r \forall c [$ End[e] & Term[t] & Term[s] & Term[r] & Chain[c] $\Longrightarrow$
Red[et:c, te.c] & Red[Kt.s.c, tc] & Red[St.s.r.c, tr.sr..c] & Red[Qt.s.c, ts:c]]

$\forall e \forall t [$ End[e] & Red[t, e] $\Longrightarrow$ Halt[t]]

Problem: Determine the provability of Halt[T].


THE END