Propositions as Types

Philip Wadler
University of Edinburgh

Types and Semantics for Programming Languages

Part I

Computability

Euclid (325–265 BCE) / Al Khwarizmi (780–850)

Effective Computability

- Alonzo Church: Lambda calculus

  An unsolvable problem of elementary number theory

  Bulletin the American Mathematical Society, May 1935

- Kurt Gödel: Recursive functions

  Stephen Kleene, General recursive functions of natural numbers

  Bulletin the American Mathematical Society, July 1935

- Alan M. Turing: Turing machines

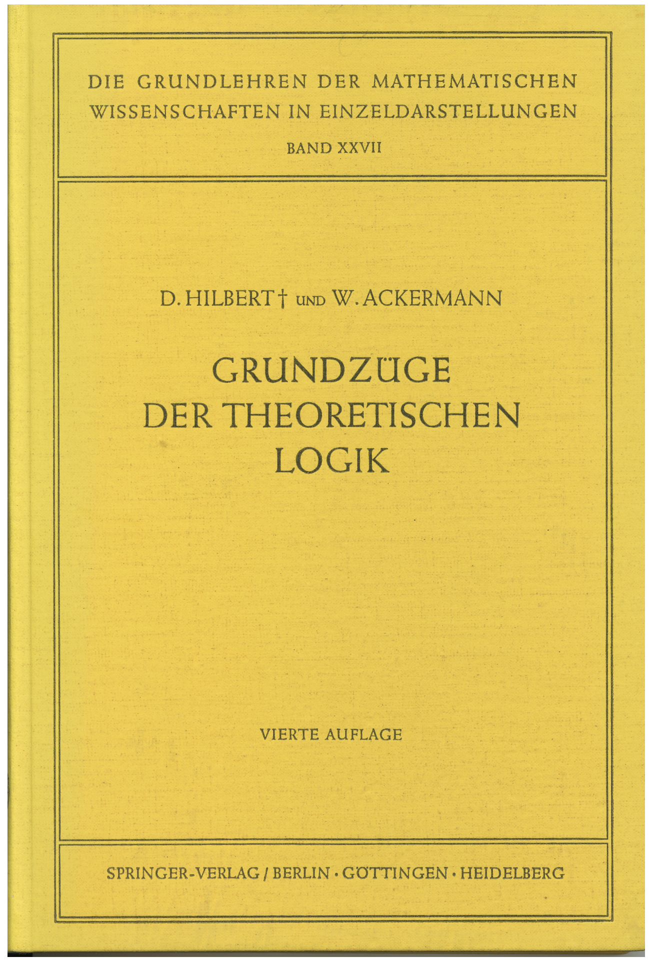
  On computable numbers, with an application to the *Entscheidungsproblem*

  Proceedings of the London Mathematical Society, received 25 May 1936


HARRODS GREATEST SALE
Oxford Circus

David Hilbert (1862–1943)

David Hilbert (1928) — Entscheidungsproblem



Kurt Gödel (1906–1978)

Kurt Gödel (1930) — Incompleteness

ON FORMALLY UNDECIDABLE PROPOSITIONS OF *PRINCIPIA MATHEMATICA* AND RELATED SYSTEMS I[1]

(*1931*)

42. $Ax(x) \equiv Z\text{-}Ax(x) \vee A\text{-}Ax(x) \vee L_1\text{-}Ax(x) \vee L_2\text{-}Ax(x) \vee R\text{-}Ax(x) \vee M\text{-}Ax(x)$,
x is an AXIOM.

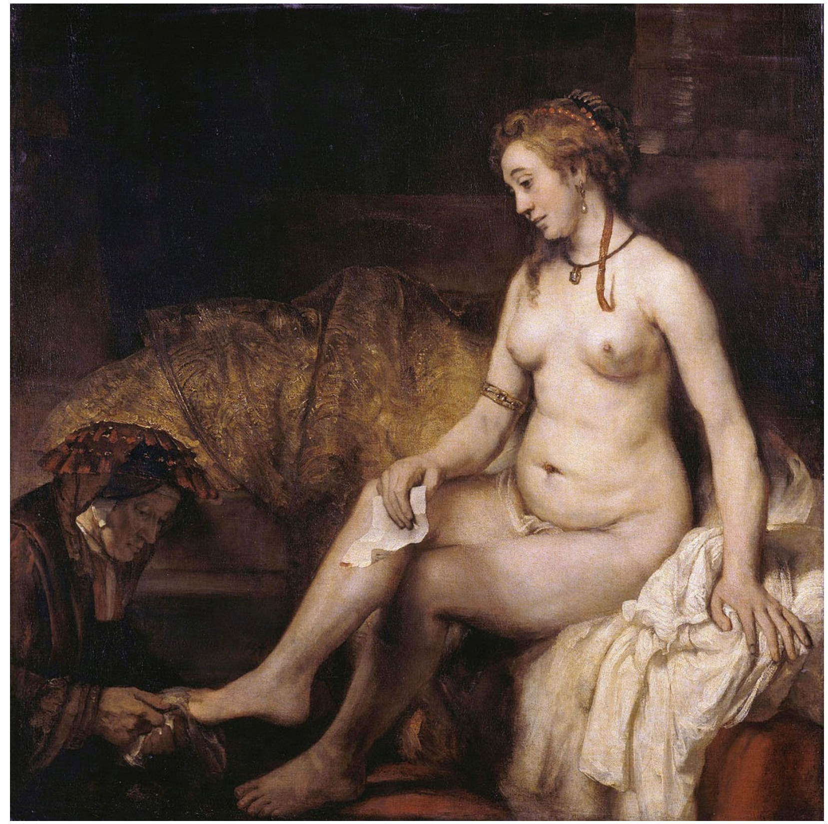
43. $Fl(x, y, z) \equiv y = z \text{ Imp } x \vee (Ev)[v \leqq x \,\&\, \mathrm{Var}(v) \,\&\, x = v \text{ Gen } y]$,
x is an IMMEDIATE CONSEQUENCE of y and z.

44. $Bw(x) \equiv (n)\{0 < n \leqq l(x) \rightarrow Ax(n\ Gl\ x) \vee (Ep, q)[0 < p, q < n \,\&\, Fl(n\ Gl\ x, p\ Gl\ x, q\ Gl\ x)]\} \,\&\, l(x) > 0$,
x is a PROOF ARRAY (a finite sequence of FORMULAS, each of which is either an AXIOM or an IMMEDIATE CONSEQUENCE of two of the preceding FORMULAS.

45. $x\ B\ y \equiv Bw(x) \,\&\, [l(x)]\ Gl\ x = y$,
x is a PROOF of the FORMULA y.

46. $\mathrm{Bew}(x) \equiv (Ey)y\ B\ x$,
x is a PROVABLE FORMULA. ($\mathrm{Bew}(x)$ is the only one of the notions 1–46 of which we cannot assert that it is recursive.)

“This statement is not provable”



Alonzo Church (1903–1995)

Alonzo Church (1936) — Lambda Calculus

AN UNSOLVABLE PROBLEM OF ELEMENTARY NUMBER THEORY.[1]

By Alonzo Church.

The purpose of the present paper is to propose a definition of effective calculability[3] which is thought to correspond satisfactorily to the somewhat vague intuitive notion in terms of which problems of this class are often stated, and to show, by means of an example, that not every problem of this class is solvable.

. . .

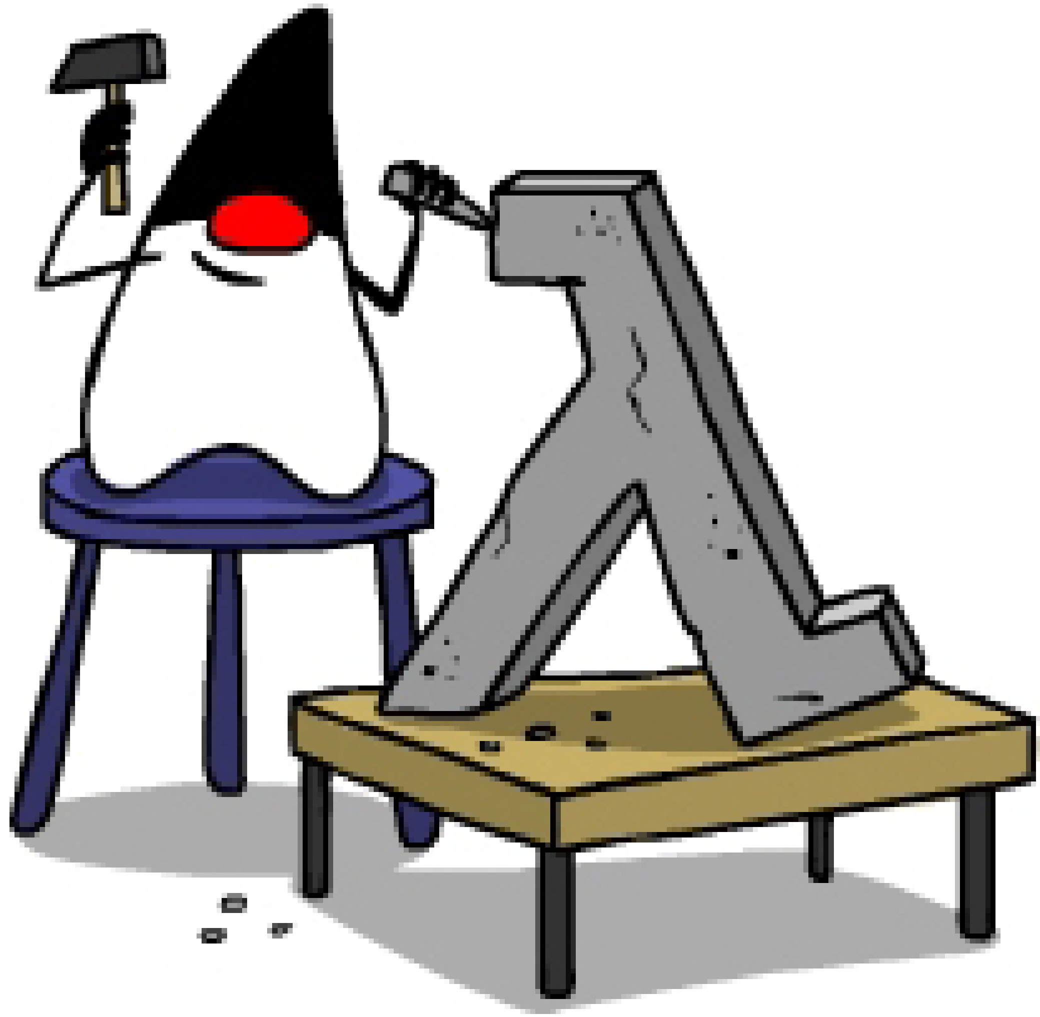
We introduce at once the following infinite list of abbreviations,

$$1 \rightarrow \lambda ab \cdot a(b),$$
$$2 \rightarrow \lambda ab \cdot a(a(b)),$$
$$3 \rightarrow \lambda ab \cdot a(a(a(b))),$$

and so on, each positive integer in Arabic notation standing for a formula of the form $\lambda ab \cdot a(a(\cdots a(b) \cdots))$.

Alonzo Church (1932) — λ-calculus

$$
\begin{array}{rcl}
L, M, N & ::= & x \\
& | & (\lambda x.\, N) \\
& | & (L\ M)
\end{array}
$$



Kurt Gödel (1906–1978)

Kurt Gödel (1936) — Recursive Functions

General recursive functions of natural numbers[1]).

Von

S. C. Kleene in Madison (Wis., U.S.A.).

The substitution

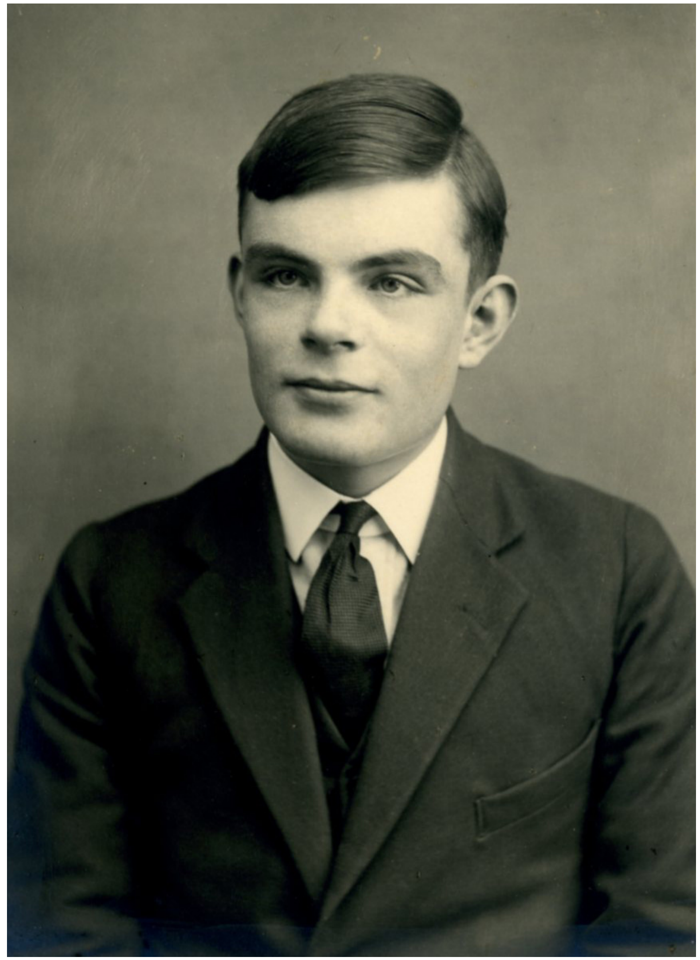
$$\varphi(x_1, \ldots, x_n) = \theta(\chi_1(x_1, \ldots, x_n), \ldots, \chi_m(x_1, \ldots, x_n)), \tag{1}$$

and the ordinary recursion with respect to one variable

$$\begin{aligned} \varphi(0, x_2, \ldots, x_n) &= \psi(x_2, \ldots, x_n) \\ \varphi(y+1, x_2, \ldots, x_n) &= \chi(y, \varphi(y, x_2, \ldots, x_n), x_2, \ldots, x_n), \end{aligned} \tag{2}$$

where $\theta, \chi_1, \ldots, \chi_m, \psi, \chi$ are given functions of natural numbers, are examples of the definition of a function φ by equations which provide a step by step process for computing the value $\varphi(k_1, \ldots, k_n)$ for any given set $k_1, \ldots, k_n$ of natural numbers. It is known that there are other definitions of this sort, e. g. certain recursions with respect to two or more variables simultaneously, which cannot be reduced to a succession of substitutions and ordinary recursions[2]). Hence, a characterization of the notion of recursive definition in general, which would include all these cases, is desirable. A definition of general recursive function of natural numbers was suggested by Herbrand to Gödel, and was used by Gödel with an important modification in a series of lectures at Princeton in 1934. In this paper we offer several observations on general recursive functions, using essentially Gödel's form of the definition.

Alan Turing (1912–1954)



Alan Turing (1936) — Turing Machine

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

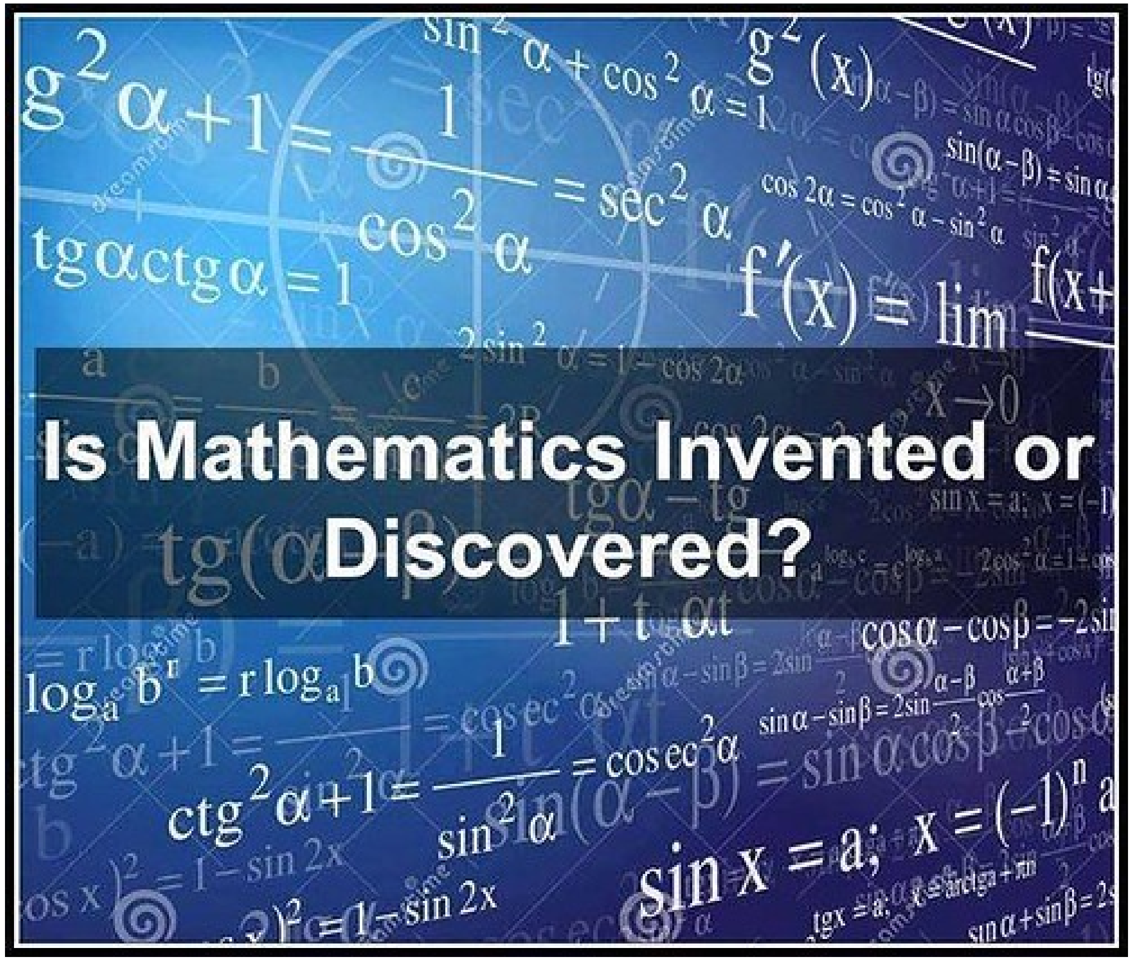
By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means.

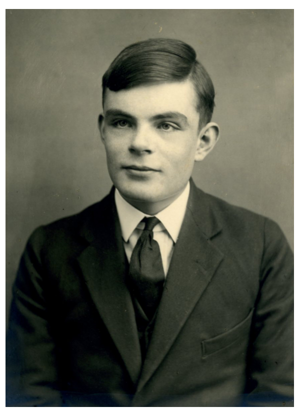
. . .

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.


Is Mathematics Invented or Discovered?

Kurt Gödel, 28

David Hilbert, 68



Alan Turing, 23

Alonzo Church, 33

Kurt Gödel, 30

Part II

Propositions as Types

Gerhard Gentzen (1909–1945)

Gerhard Gentzen (1935) — Natural Deduction

&–*I*	&–*E*	∨–*I*	∨–*E*
$\dfrac{\mathfrak{A} \quad \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}}$	$\dfrac{\mathfrak{A} \,\&\, \mathfrak{B}}{\mathfrak{A}} \qquad \dfrac{\mathfrak{A} \,\&\, \mathfrak{B}}{\mathfrak{B}}$	$\dfrac{\mathfrak{A}}{\mathfrak{A} \lor \mathfrak{B}} \qquad \dfrac{\mathfrak{B}}{\mathfrak{A} \lor \mathfrak{B}}$	$\dfrac{\mathfrak{A} \lor \mathfrak{B} \quad \begin{matrix}[\mathfrak{A}] \\ \mathfrak{C}\end{matrix} \quad \begin{matrix}[\mathfrak{B}] \\ \mathfrak{C}\end{matrix}}{\mathfrak{C}}$

∀–*I*	∀–*E*	∃–*I*	∃–*E*
$\dfrac{\mathfrak{F}\mathfrak{a}}{\forall \mathfrak{x}\, \mathfrak{F}\mathfrak{x}}$	$\dfrac{\forall \mathfrak{x}\, \mathfrak{F}\mathfrak{x}}{\mathfrak{F}\mathfrak{a}}$	$\dfrac{\mathfrak{F}\mathfrak{a}}{\exists \mathfrak{x}\, \mathfrak{F}\mathfrak{x}}$	$\dfrac{\exists \mathfrak{x}\, \mathfrak{F}\mathfrak{x} \quad \begin{matrix}[\mathfrak{F}\mathfrak{a}] \\ \mathfrak{C}\end{matrix}}{\mathfrak{C}}$

⊃–*I*	⊃–*E*	¬–*I*	¬–*E*
$\dfrac{\begin{matrix}[\mathfrak{A}] \\ \mathfrak{B}\end{matrix}}{\mathfrak{A} \supset \mathfrak{B}}$	$\dfrac{\mathfrak{A} \quad \mathfrak{A} \supset \mathfrak{B}}{\mathfrak{B}}$	$\dfrac{\begin{matrix}[\mathfrak{A}] \\ \curlywedge\end{matrix}}{\neg \mathfrak{A}}$	$\dfrac{\mathfrak{A} \quad \neg \mathfrak{A}}{\curlywedge} \qquad \dfrac{\curlywedge}{\mathfrak{D}}\ .$

Gerhard Gentzen (1935) — Natural Deduction

$$\dfrac{\begin{matrix}[A]^x \\ \vdots \\ B\end{matrix}}{A \supset B}\ \supset\text{-I}^x \qquad \dfrac{A \supset B \qquad A}{B}\ \supset\text{-E}$$

$$\dfrac{A \qquad B}{A \,\&\, B}\ \&\text{-I} \qquad \dfrac{A \,\&\, B}{A}\ \&\text{-E}_0 \qquad \dfrac{A \,\&\, B}{B}\ \&\text{-E}_1$$

A proof

$$\dfrac{\dfrac{[B \mathbin{\&} A]^z}{A}\,\&\text{-E}_1 \qquad \dfrac{[B \mathbin{\&} A]^z}{B}\,\&\text{-E}_0}{\dfrac{A \mathbin{\&} B}{(B \mathbin{\&} A) \supset (A \mathbin{\&} B)}\,\supset\text{-I}^z}\,\&\text{-I}$$

Simplifying proofs

$$\dfrac{\dfrac{\begin{matrix}[A]^x \\ \vdots \\ B\end{matrix}}{A \supset B}\,\supset\text{-I}^x \qquad \begin{matrix}\vdots \\ A\end{matrix}}{B}\,\supset\text{-E} \quad\Rightarrow\quad \begin{matrix}\vdots \\ A \\ \vdots \\ B\end{matrix}$$

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ A\end{matrix} \qquad \begin{matrix}\vdots \\ B\end{matrix}}{A \,\&\, B}\,\&\text{-I}}{A}\,\&\text{-E}_0 \quad\Rightarrow\quad \begin{matrix}\vdots \\ A\end{matrix}$$

Simplifying a proof

$$
\cfrac{\cfrac{\cfrac{[B \mathbin{\&} A]^z}{A}\ \&\text{-E}_1 \qquad \cfrac{[B \mathbin{\&} A]^z}{B}\ \&\text{-E}_0}{A \mathbin{\&} B}\ \&\text{-I}}{(B \mathbin{\&} A) \supset (A \mathbin{\&} B)}\ \supset\text{-I}^z \qquad \cfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\ \&\text{-I}}{A \mathbin{\&} B}\ \supset\text{-E}
$$

Simplifying a proof

$$
\dfrac{\dfrac{\dfrac{\dfrac{[B \mathbin{\&} A]^z}{A}\;\&\text{-E}_1 \qquad \dfrac{[B \mathbin{\&} A]^z}{B}\;\&\text{-E}_0}{A \mathbin{\&} B}\;\&\text{-I}}{(B \mathbin{\&} A) \supset (A \mathbin{\&} B)}\;\supset\text{-I}^z \qquad \dfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\;\&\text{-I}}{A \mathbin{\&} B}\;\supset\text{-E}
$$

$$
\Downarrow
$$

$$
\dfrac{\dfrac{\dfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\;\&\text{-I}}{A}\;\&\text{-E}_1 \qquad \dfrac{\dfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\;\&\text{-I}}{B}\;\&\text{-E}_0}{A \mathbin{\&} B}\;\&\text{-I}
$$

Simplifying a proof

$$\dfrac{\dfrac{\dfrac{\dfrac{[B \mathbin{\&} A]^z}{A}\;\&\text{-E}_1 \qquad \dfrac{[B \mathbin{\&} A]^z}{B}\;\&\text{-E}_0}{A \mathbin{\&} B}\;\&\text{-I}}{(B \mathbin{\&} A) \supset (A \mathbin{\&} B)}\;\supset\text{-I}^z \qquad \dfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\;\&\text{-I}}{A \mathbin{\&} B}\;\supset\text{-E}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\;\&\text{-I}}{A}\;\&\text{-E}_1 \qquad \dfrac{\dfrac{[B]^y \quad [A]^x}{B \mathbin{\&} A}\;\&\text{-I}}{B}\;\&\text{-E}_0}{A \mathbin{\&} B}\;\&\text{-I}$$

$$\Downarrow$$

$$\dfrac{[A]^x \quad [B]^y}{A \mathbin{\&} B}\;\&\text{-I}$$

Alonzo Church (1903–1995)

Alonzo Church (1940) — Typed λ-calculus

$$\dfrac{\begin{matrix}[x : A]^x \\ \vdots \\ N : B\end{matrix}}{\lambda x.\, N : A \supset B}\ \supset\text{-I}^x \qquad \dfrac{L : A \supset B \qquad M : A}{L\, M : B}\ \supset\text{-E}$$

$$\dfrac{M : A \qquad N : B}{(M,\, N) : A \,\&\, B}\ \&\text{-I} \qquad \dfrac{L : A \,\&\, B}{\mathsf{fst}\; L : A}\ \&\text{-E}_0 \qquad \dfrac{L : A \,\&\, B}{\mathsf{snd}\; L : B}\ \&\text{-E}_1$$

A program

$$
\dfrac{
  \dfrac{[z : B \,\&\, A]^z}{\mathsf{snd}\; z : A}\;\&\text{-E}_1
  \qquad
  \dfrac{[z : B \,\&\, A]^z}{\mathsf{fst}\; z : B}\;\&\text{-E}_0
}{
  \dfrac{(\mathsf{snd}\; z,\ \mathsf{fst}\; z) : A \,\&\, B}{\lambda z.\, (\mathsf{snd}\; z,\ \mathsf{fst}\; z) : (B \,\&\, A) \supset (A \,\&\, B)}\;\supset\text{-I}^z
}\;\&\text{-I}
$$

Evaluating programs

$$\cfrac{\cfrac{\begin{array}{c}[x : A]^{x}\\ \vdots\\ N : B\end{array}}{\lambda x.\,N : A \supset B}\,{\supset}\text{-I}^{x} \qquad \begin{array}{c}\vdots\\ M : A\end{array}}{(\lambda x.\,N)\,M : B}\,{\supset}\text{-E} \quad\Rightarrow\quad \begin{array}{c}\vdots\\ M : A\\ \vdots\\ N\{M/x\} : B\end{array}$$

$$\cfrac{\cfrac{\begin{array}{c}\vdots\\ M : A\end{array} \qquad \begin{array}{c}\vdots\\ N : B\end{array}}{(M,\, N) : A \,\&\, B}\,\&\text{-I}}{\mathsf{fst}\,(M,\, N) : A}\,\&\text{-E}_0 \quad\Rightarrow\quad \begin{array}{c}\vdots\\ M : A\end{array}$$

Alan Turing (1942)

AN EARLY PROOF OF NORMALIZATION
BY A.M. TURING

R.O. Gandy

*Mathematical Institute, 24-29 St. Giles,
Oxford OX1 3LB, UK*

Dedicated to H.B. Curry on the occasion of his 80th birthday

In the extract printed below, Turing shows that every formula of Church's simple type theory has a normal form. The extract is the first page of an unpublished (and incomplete) typescript entitled 'Some theorems about Church's system'. (Turing left his manuscripts to me; they are deposited in the library of King's College, Cambridge). An account of this system was published by Church in 'A formulation of the simple theory of types' (J. Symbolic Logic 5 (1940), pp. 56-68).

Evaluating a program

$$\dfrac{\dfrac{\dfrac{\dfrac{[z : B \,\&\, A]^z}{\mathsf{snd}\; z : A}\,\&\text{-E}_1 \qquad \dfrac{[z : B \,\&\, A]^z}{\mathsf{fst}\; z : B}\,\&\text{-E}_0}{(\mathsf{snd}\; z,\ \mathsf{fst}\; z) : A \,\&\, B}\,\&\text{-I}}{\lambda z.\,(\mathsf{snd}\; z,\ \mathsf{fst}\; z) : (B \,\&\, A) \supset (A \,\&\, B)}\,\supset\text{-I}^z \qquad \dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \,\&\, A}\,\&\text{-I}}{(\lambda z.\,(\mathsf{snd}\; z,\ \mathsf{fst}\; z))\,(y,\ x) : A \,\&\, B}\,\supset\text{-E}$$

Evaluating a program

$$\dfrac{\dfrac{\dfrac{\dfrac{[z : B \mathbin{\&} A]^z}{\mathsf{snd}\ z : A}\,\&\text{-E}_1 \qquad \dfrac{[z : B \mathbin{\&} A]^z}{\mathsf{fst}\ z : B}\,\&\text{-E}_0}{(\mathsf{snd}\ z,\ \mathsf{fst}\ z) : A \mathbin{\&} B}\,\&\text{-I}}{\lambda z.\,(\mathsf{snd}\ z,\ \mathsf{fst}\ z) : (B \mathbin{\&} A) \supset (A \mathbin{\&} B)}\,\supset\text{-I}^z \qquad \dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \mathbin{\&} A}\,\&\text{-I}}{(\lambda z.\,(\mathsf{snd}\ z,\ \mathsf{fst}\ z))\,(y,\ x) : A \mathbin{\&} B}\,\supset\text{-E}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \mathbin{\&} A}\,\&\text{-I}}{\mathsf{snd}\ (y,\ x) : A}\,\&\text{-E}_1 \qquad \dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \mathbin{\&} A}\,\&\text{-I}}{\mathsf{fst}\ (y,\ x) : B}\,\&\text{-E}_0}{(\mathsf{snd}\ (y,\ x),\ \mathsf{fst}\ (y,\ x)) : A \mathbin{\&} B}\,\&\text{-I}$$

Evaluating a program

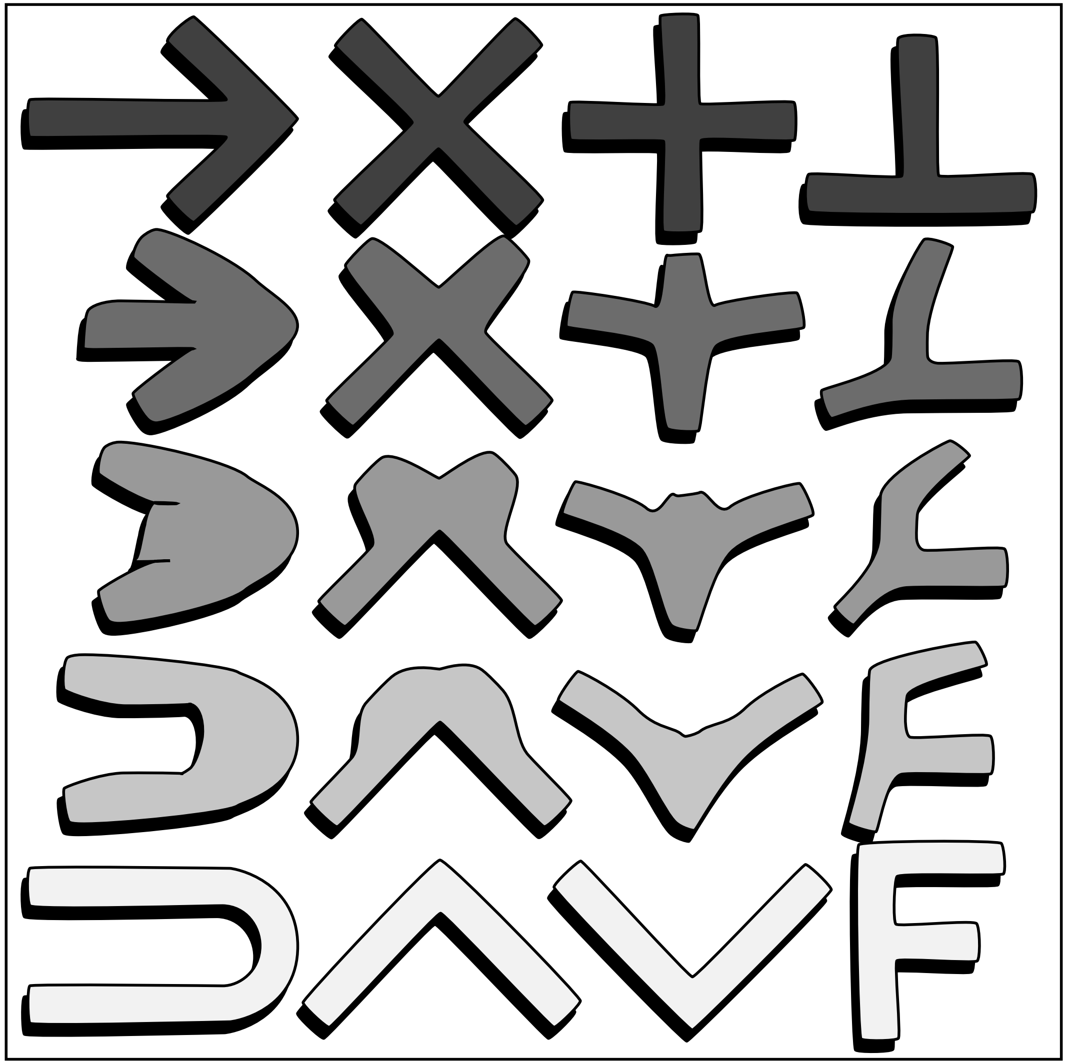
$$
\dfrac{\dfrac{\dfrac{[z : B \,\&\, A]^z}{\mathsf{snd}\, z : A}\,\&\text{-E}_1 \qquad \dfrac{[z : B \,\&\, A]^z}{\mathsf{fst}\, z : B}\,\&\text{-E}_0}{(\mathsf{snd}\, z,\ \mathsf{fst}\, z) : A \,\&\, B}\,\&\text{-I}}{\lambda z.\,(\mathsf{snd}\, z,\ \mathsf{fst}\, z) : (B \,\&\, A) \supset (A \,\&\, B)}\,{\supset}\text{-I}^z \qquad \dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \,\&\, A}\,\&\text{-I}}{(\lambda z.\,(\mathsf{snd}\, z,\ \mathsf{fst}\, z))\,(y,\ x) : A \,\&\, B}\,{\supset}\text{-E}
$$

$$\Downarrow$$

$$
\dfrac{\dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \,\&\, A}\,\&\text{-I}}{\mathsf{snd}\,(y,\ x) : A}\,\&\text{-E}_1 \qquad \dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y,\ x) : B \,\&\, A}\,\&\text{-I}}{\mathsf{fst}\,(y,\ x) : B}\,\&\text{-E}_0}{(\mathsf{snd}\,(y,\ x),\ \mathsf{fst}\,(y,\ x)) : A \,\&\, B}\,\&\text{-I}
$$

$$\Downarrow$$

$$
\dfrac{[x : A]^x \quad [y : B]^y}{(x,\ y) : A \,\&\, B}\,\&\text{-I}
$$



LC'90

The Curry-Howard homeomorphism

Haskell Curry (1900–1982) / William Howard (1926–)

Howard 1980

THE FORMULAE-AS-TYPES NOTION OF CONSTRUCTION

W. A. Howard

Department of Mathematics, University of Illinois at Chicago Circle, Chicago, Illinois 60680, U.S.A.

Dedicated to H. B. Curry on the occasion of his 80th birthday.

The following consists of notes which were privately circulated in 1969. Since they have been referred to a few times in the literature, it seems worth while to publish them. They have been rearranged for easier reading, and some inessential corrections have been made.

Curry-Howard correspondence

propositions	*as*	types
proofs	*as*	programs
normalisation of proofs	*as*	evaluation of programs

Curry-Howard correspondence

Natural Deduction	$\leftrightarrow$	Typed Lambda Calculus
Gentzen (1935)		Church (1940)
Type Schemes	$\leftrightarrow$	ML Type System
Hindley (1969)		Milner (1975)
System F	$\leftrightarrow$	Polymorphic Lambda Calculus
Girard (1972)		Reynolds (1974)
Modal Logic	$\leftrightarrow$	Monads (state, exceptions)
Lewis (1910)		Kleisli (1965), Moggi (1987)
Classical-Intuitionistic Embedding	$\leftrightarrow$	Continuation Passing Style
Gödel (1933)		Reynolds (1972)

Functional Languages

- Lisp (McCarthy, 1960)
- Iswim (Landin, 1966)
- Scheme (Steele and Sussman, 1975)
- ML (Milner, Gordon, Wadsworth, 1979)
- Haskell (Hudak, Peyton Jones, and Wadler, 1987)
- O'Caml (Leroy, 1996)
- Erlang (Armstrong, Virding, Williams, 1996)
- Scala (Odersky, 2004)
- $F^{\#}$ (Syme, 2006)

Proof assistants

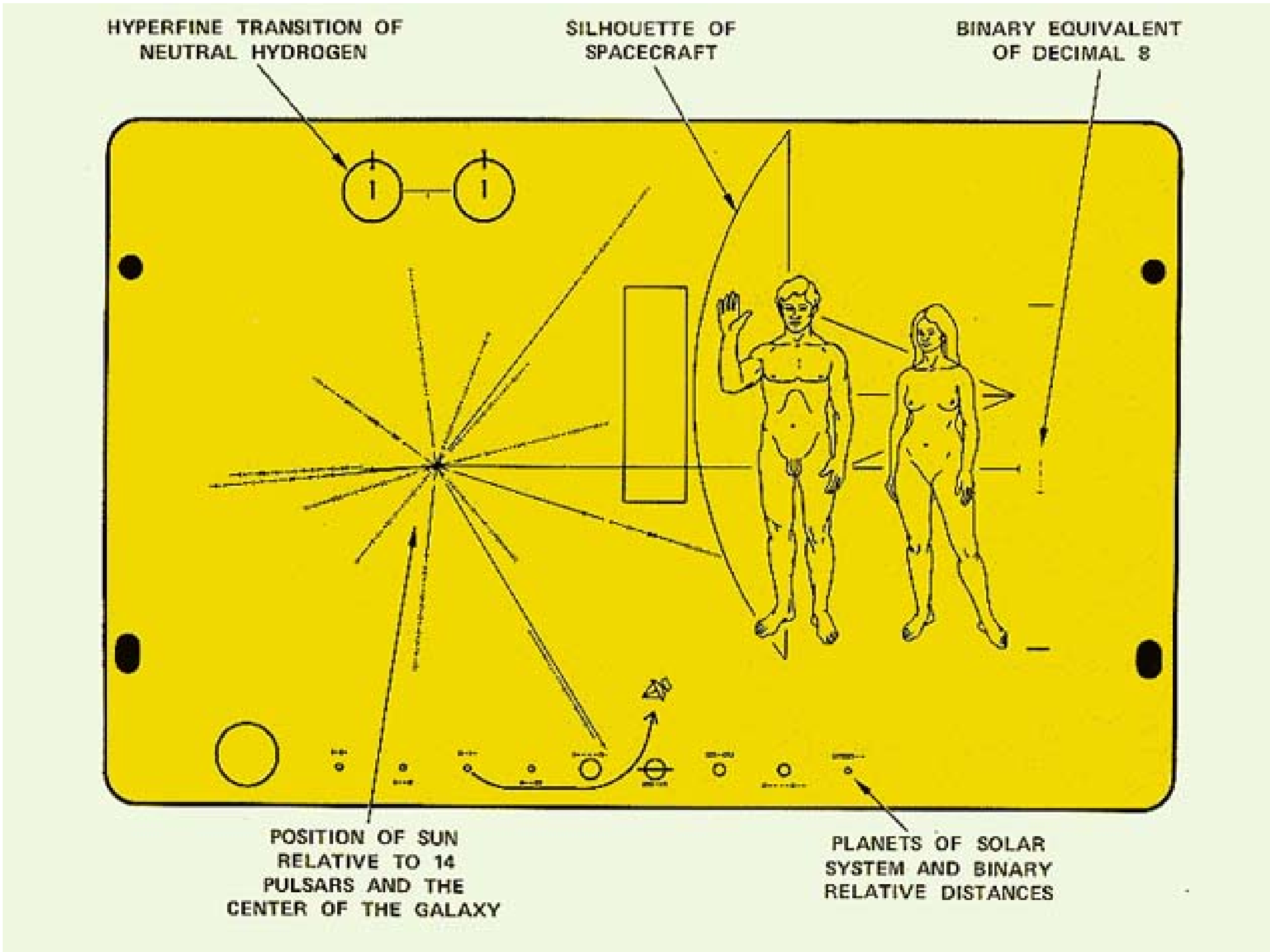
- Automath (de Bruijn, 1970)
- Type Theory (Martin Löf, 1975)
- Mizar (Trybulec, 1975)
- ML/LCF (Milner, Gordon, and Wadsworth, 1979)
- NuPrl (Constable, 1985)
- HOL (Gordon and Melham, 1988)
- Coq (Huet and Coquand, 1988)
- Isabelle (Paulson, 1993)
- Epigram (McBride and McKinna, 2004)
- Agda (Norell, 2005)

Part III

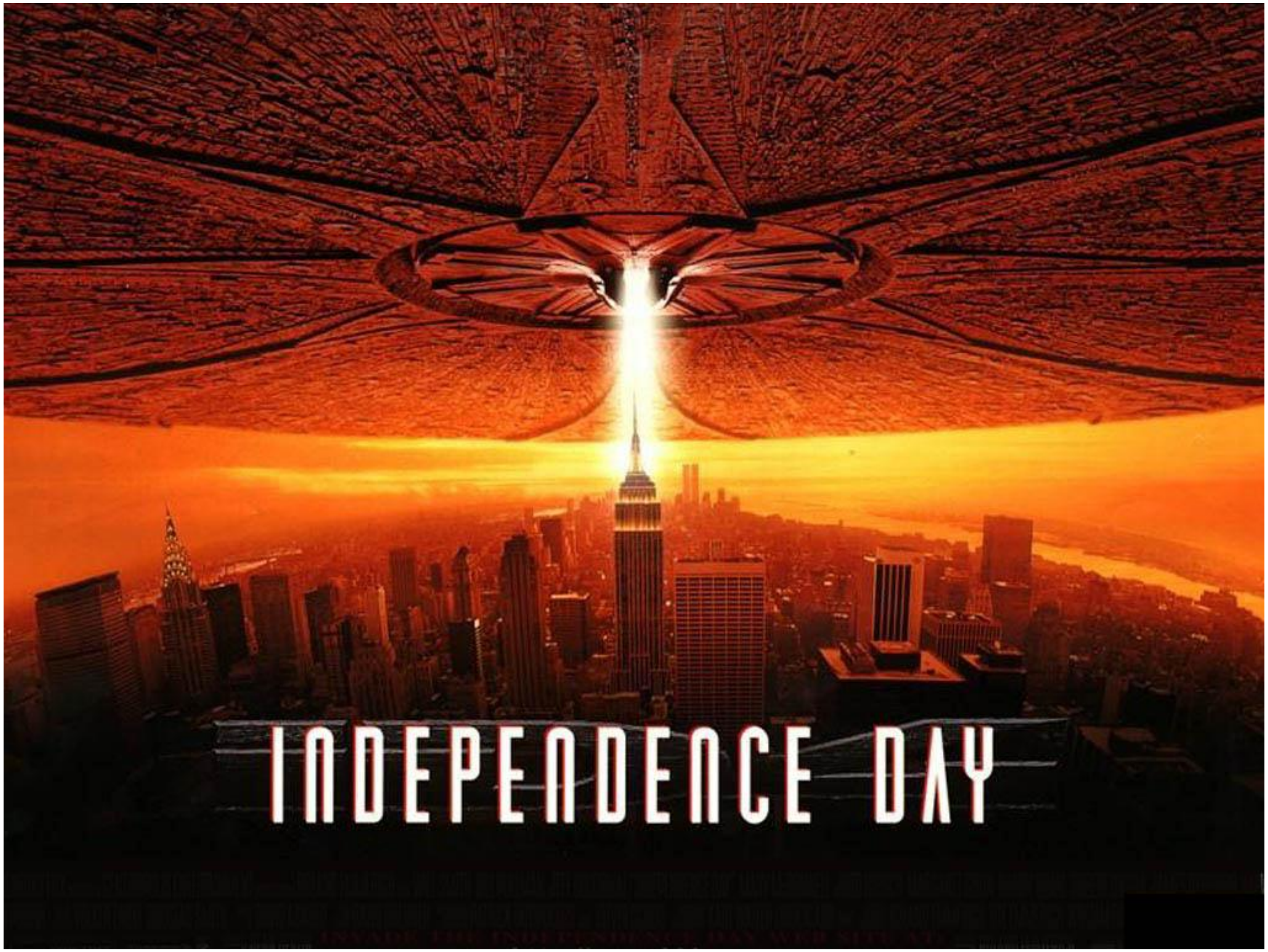
Conclusion:

Philosophy

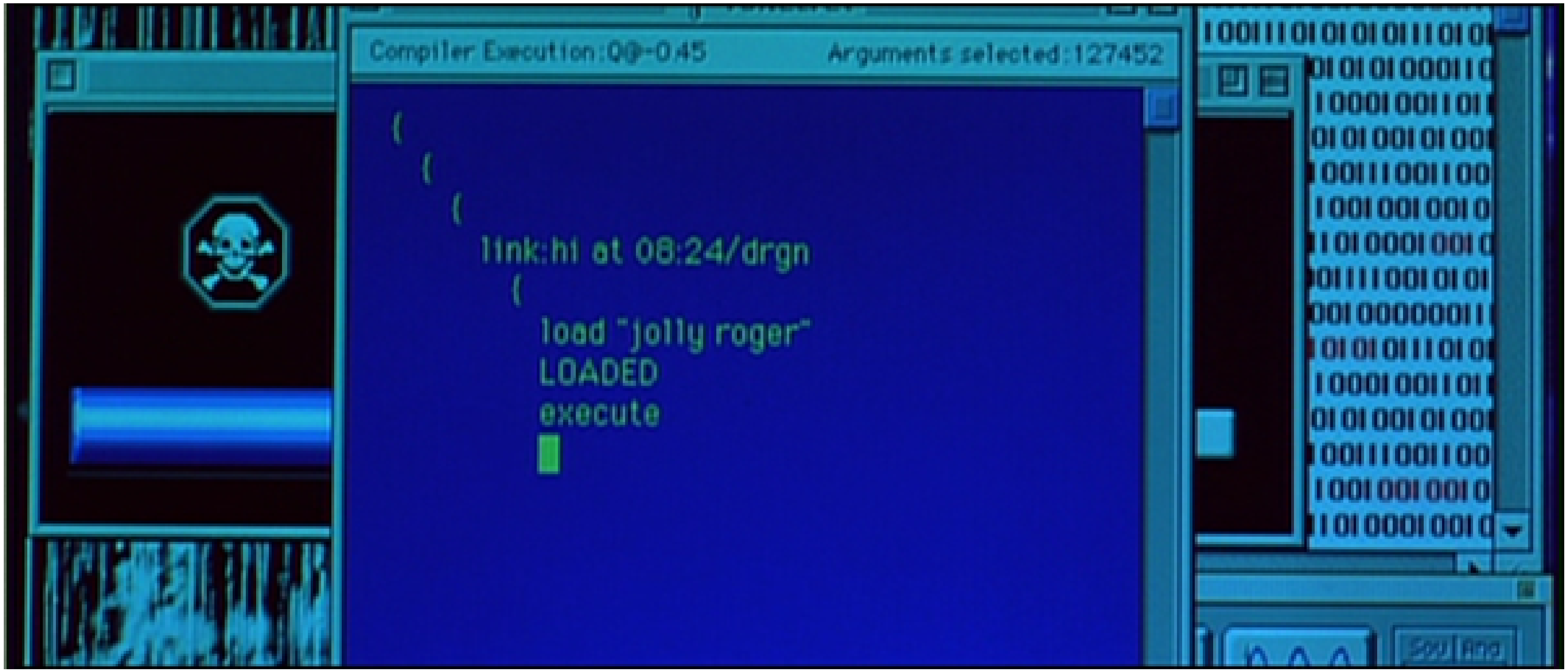
Let's talk to aliens!



Independence Day



A universal programming language?



Multiverses

Lambda is Omniversal