Высказывания и типы

Николай Кудасов
МГУ им. Ломоносова

Москва, 15 марта 2016

По мотивам доклада Филипа Вадлера в Сент-Луисе 25 августа 2015

Филип Вадлер (1956 г.р.)

Филип Вадлер (2015) – Propositions as Types

Propositions as Types *

Philip Wadler

University of Edinburgh

wadler@inf.ed.ac.uk

Propositions as Types is a notion with many names and many origins. It is closely related to the BHK Interpretation, a view of logic developed by the intuitionists Brouwer, Heyting, and Kolmogorov in the 1930s. It is often referred to as the Curry-Howard Isomorphism, referring to a correspondence observed by Curry in 1934 and refined by Howard in 1969 (though not published until 1980, in a Festschrift dedicated to Curry). Others draw attention to significant contributions from de Bruijn's Automath and Martin-Löf's Type Theory in the 1970s. Many variant names appear in the literature, including Formulae as Types, Curry-Howard-de Bruijn Correspondence, Brouwer's Dictum, and others.

Евклид (325–265 до н.э)

Аль-Хорезми (780–846 н.э)

Вычислимость

- **Алонзо Чёрч:** ***Лямбда-исчисление***
An unsolvable problem of elementary number theory
Bulletin the American Mathematical Society, May 1935
- **Курт Гёдель: Рекурсивные функции**
Stephen Kleene, General recursive functions of natural numbers
Bulletin the American Mathematical Society, July 1935
- **Алан Тьюринг: Машины Тьюринга**
On computable numbers, with an application to the *Entscheidungsproblem*
Proceedings of the London Mathematical Society, received 25 May 1936

СБ24
Сладкая жизнь
СОТОВЫЕ
АКСЕССУАРЫ
СКИДКА 50 %
52
55

Давид Гильберт (1862–1943)

Давид Гильберт (1928) – Entscheidungsproblem

- Найти алгоритм, который бы принимал в качестве входных данных описание любой проблемы разрешимости (формального языка и математического утверждения S на этом языке), и после конечного числа шагов останавливался бы и выдавал один из двух ответов: «истина» или «ложь», в зависимости от того, истинно или ложно утверждение S.

Курт Гёдель (1906–1978)

Курт Гёдель (1931) – Теорема о неполноте

42. $isAxiom(x) \Leftrightarrow peanoAxiom(x) \vee propAxiom(x) \vee$
$quantor1Axiom(x) \vee quantor2Axiom(x) \vee reduAxiom(x) \vee$
$setAxiom(x)$

x is an AXIOM.

43. $immConseq(x, y, z) \Leftrightarrow y = imp(z, x) \vee \exists v \leq x \,.\, isVar(v) \wedge x = forall(v, y)$

x is an IMMEDIATE CONSEQUENCE of y and z.

44. $isProofFigure(x) \Leftrightarrow \big(\forall 0 < n \leq length(x) \,.$
$isAxiom(item(n, x)) \vee \exists 0 < p, q < n \,.$
$immConseq(item(n, x), item(p, x), item(q, x))\big) \wedge$
$length(x) > 0$

x is a PROOF FIGURE (a finite sequence of FORMULAE, each of which is either an AXIOM or the IMMEDIATE CONSEQUENCE of two of the preceding ones).

45. $proofFor(x, y) \Leftrightarrow isProofFigure(x) \wedge item(length(x), x) = y$

x is a PROOF for the FORMULA y.

46. $provable(x) \Leftrightarrow \exists y \,.\, proofFor(y, x)$

x is a PROVABLE FORMULA. ($provable(x)$ is the only one among the concepts 1-46 for which we can not assert that it is primitive recursive).

«Это высказывание не доказуемо»

Метод пристального взгляда

Алонзо Чёрч (1903–1995)

Алонзо Чёрч (1935) – Лямбда-исчисление

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 $\lambda ab \cdot a(a(\cdot\cdot\cdot a(b) \cdot\cdot\cdot))$.

Алонзо Чёрч (1935) – λ-исчисление

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

Курт Гёдель (1906–1978)

Курт Гёдель (1936) – Рекурсивные функции

General recursive functions of natural numbers[1]).

Von

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

The substitution

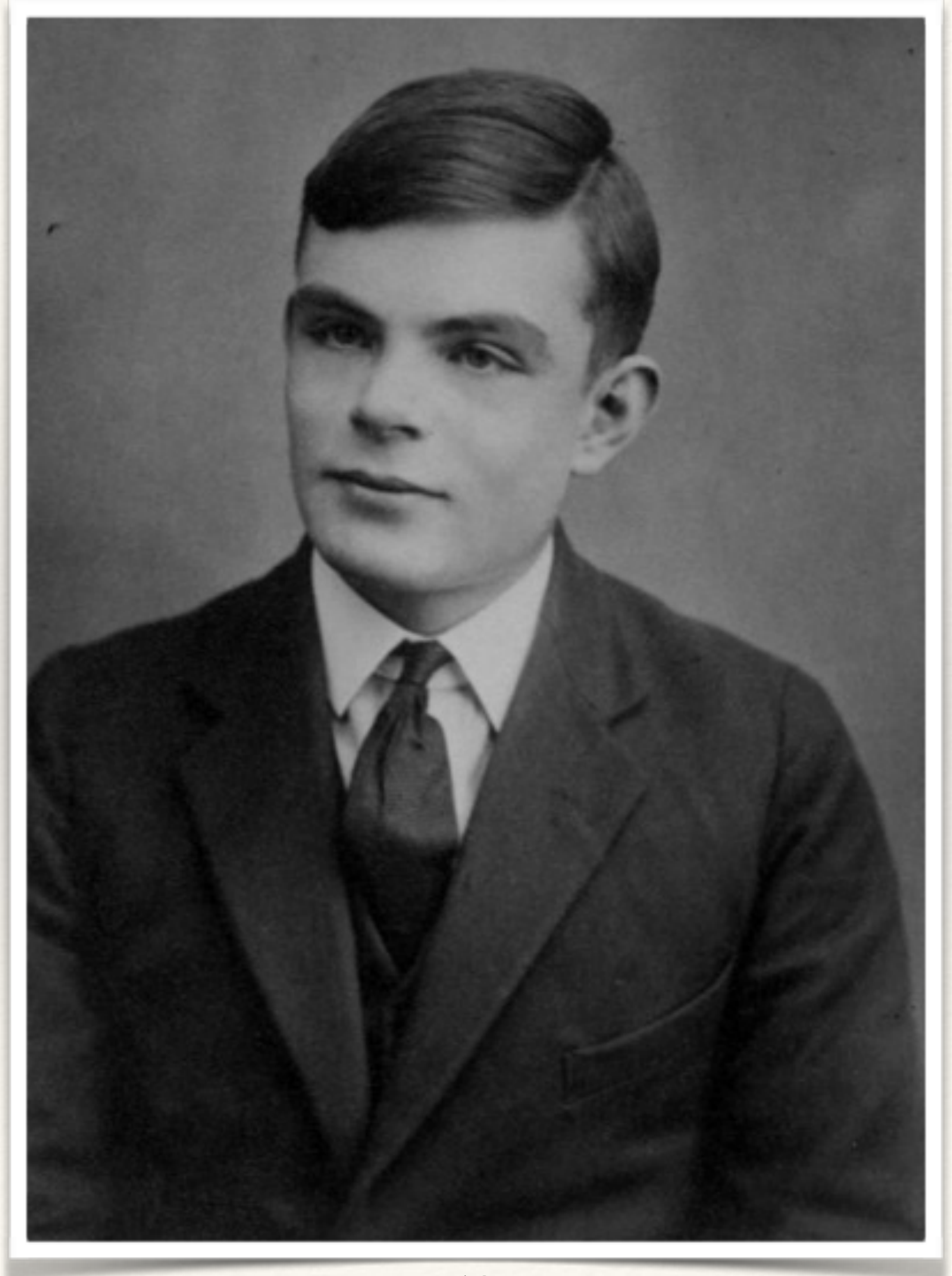
$$\varphi(x_1, \ldots, x_n) = \theta(\chi_1(x_1, \ldots, x_n), \ldots, \chi_m(x_1, \ldots, x_n)), \tag{1}$$

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.

Алан Тьюринг (1912–1954)



Алан Тьюринг (1936) – Машины Тьюринга

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

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

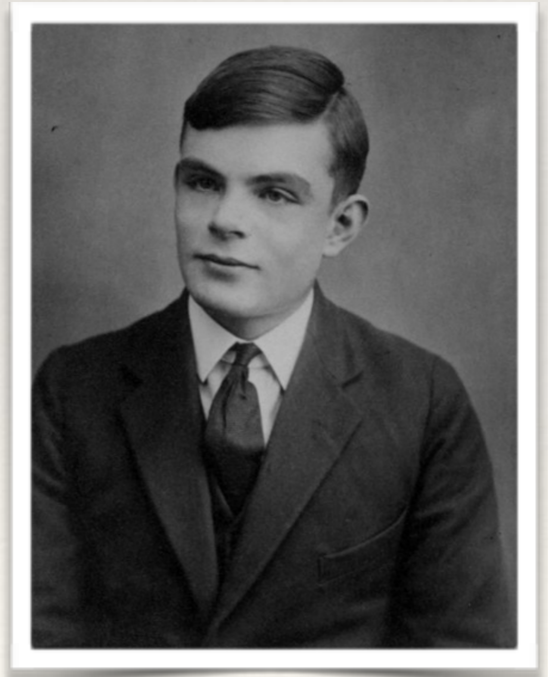
The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means.

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.

Математика – открытие или изобретение?

Курт Гёдель, 28

Давид Гильберт, 68



Алан Тьюринг, 23

Алонзо Чёрч, 33

Курт Гёдель, 30

Часть 2

Высказывания и типы

Герхард Генцен (1909–1945)

Герхард Генцен (1935) – Естественный вывод

UE	UB		OE		OB
$\dfrac{\mathfrak{A} \quad \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}}$	$\dfrac{\mathfrak{A} \,\&\, \mathfrak{B}}{\mathfrak{A}}$	$\dfrac{\mathfrak{A} \,\&\, \mathfrak{B}}{\mathfrak{B}}$	$\dfrac{\mathfrak{A}}{\mathfrak{A} \vee \mathfrak{B}}$	$\dfrac{\mathfrak{B}}{\mathfrak{A} \vee \mathfrak{B}}$	$\dfrac{\mathfrak{A} \vee \mathfrak{B} \quad \begin{matrix}[\mathfrak{A}] \\ \mathfrak{C}\end{matrix} \quad \begin{matrix}[\mathfrak{B}] \\ \mathfrak{C}\end{matrix}}{\mathfrak{C}}$

AE	AB	EE	EB
$\dfrac{\mathfrak{F}\mathfrak{a}}{\forall \mathfrak{x} \mathfrak{F}\mathfrak{x}}$	$\dfrac{\forall \mathfrak{x} \mathfrak{F}\mathfrak{x}}{\mathfrak{F}\mathfrak{a}}$	$\dfrac{\mathfrak{F}\mathfrak{a}}{\exists \mathfrak{x} \mathfrak{F}\mathfrak{x}}$	$\dfrac{\exists \mathfrak{x} \mathfrak{F}\mathfrak{x} \quad \begin{matrix}[\mathfrak{F}\mathfrak{a}] \\ \mathfrak{C}\end{matrix}}{\mathfrak{C}}$

FE	FB	NE	NB	
$\dfrac{\begin{matrix}[\mathfrak{A}] \\ \mathfrak{B}\end{matrix}}{\mathfrak{A} \supset \mathfrak{B}}$	$\dfrac{\mathfrak{A} \quad \mathfrak{A} \supset \mathfrak{B}}{\mathfrak{B}}$	$\dfrac{\begin{matrix}[\mathfrak{A}] \\ \curlywedge\end{matrix}}{\neg \mathfrak{A}}$	$\dfrac{\mathfrak{A} \quad \neg \mathfrak{A}}{\curlywedge}$	$\dfrac{\curlywedge}{\mathfrak{D}}$

Герхард Генцен (1935) – Естественный вывод

$$\frac{\begin{array}{c}[A]^x \\ \vdots \\ B\end{array}}{A \to B}\ (\to \mathrm{I}^x) \qquad \frac{A \to B \quad A}{B}\ (\to \mathrm{E})$$

$$\frac{A \quad B}{A \,\&\, B}\ (\&\mathrm{I}) \qquad \frac{A \,\&\, B}{A}\ (\&\mathrm{E}_l) \qquad \frac{A \,\&\, B}{B}\ (\&\mathrm{E}_r)$$

Доказательство

$$\dfrac{\dfrac{\dfrac{[B \mathbin{\&} A]^z}{A}\,(\&\mathrm{E}_r) \qquad \dfrac{[B \mathbin{\&} A]^z}{B}\,(\&\mathrm{E}_l)}{A \mathbin{\&} B}\,(\&\mathrm{I})}{(B \mathbin{\&} A) \to (A \mathbin{\&} B)}\,(\to \mathrm{I}^z)$$

Упрощение доказательств

$$\dfrac{\dfrac{\begin{matrix}[A]^x \\ \vdots \\ B\end{matrix}}{A \to B}\,(\to \mathrm{I}^x) \qquad \begin{matrix}\vdots \\ A\end{matrix}}{B}\,(\to \mathrm{E}) \qquad \Rightarrow \qquad \begin{matrix}\vdots \\ A \\ \vdots \\ B\end{matrix}$$

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ A\end{matrix} \quad \begin{matrix}\vdots \\ B\end{matrix}}{A \mathbin{\&} B}\,(\&\mathrm{I})}{A}\,(\&\mathrm{E}_l) \qquad \Rightarrow \qquad \begin{matrix}\vdots \\ A\end{matrix}$$

Упрощение доказательства

$$\dfrac{\dfrac{\dfrac{\dfrac{[B \,\&\, A]^z}{A}\,(\&\mathrm{E}_r) \qquad \dfrac{[B \,\&\, A]^z}{B}\,(\&\mathrm{E}_l)}{A \,\&\, B}\,(\&\mathrm{I})}{(B \,\&\, A) \to (A \,\&\, B)}\,(\to \mathrm{I}^z) \qquad \dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{A \,\&\, B}\,(\to \mathrm{E})$$

Упрощение доказательства

$$
\dfrac{\dfrac{\dfrac{\dfrac{[B \,\&\, A]^z}{A}\,(\&\mathrm{E}_r) \qquad \dfrac{[B \,\&\, A]^z}{B}\,(\&\mathrm{E}_l)}{A \,\&\, B}\,(\&\mathrm{I})}{(B \,\&\, A) \to (A \,\&\, B)}\,(\to \mathrm{I}^z) \qquad \dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{A \,\&\, B}\,(\to \mathrm{E})
$$

$$\Downarrow$$

$$
\dfrac{\dfrac{\dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{A}\,(\&\mathrm{E}_r) \qquad \dfrac{\dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{B}\,(\&\mathrm{E}_l)}{A \,\&\, B}\,(\&\mathrm{I})
$$

Упрощение доказательства

$$\dfrac{\dfrac{\dfrac{\dfrac{[B \,\&\, A]^z}{A}\,(\&\mathrm{E}_r) \qquad \dfrac{[B \,\&\, A]^z}{B}\,(\&\mathrm{E}_l)}{A \,\&\, B}\,(\&\mathrm{I})}{(B \,\&\, A) \to (A \,\&\, B)}\,(\to \mathrm{I}^z) \qquad \dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{A \,\&\, B}\,(\to \mathrm{E})$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{A}\,(\&\mathrm{E}_r) \qquad \dfrac{\dfrac{[B]^y \quad [A]^x}{B \,\&\, A}\,(\&\mathrm{I})}{B}\,(\&\mathrm{E}_l)}{A \,\&\, B}\,(\&\mathrm{I})$$

$$\Downarrow$$

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

Алонзо Чёрч (1903–1995)

Алонзо Чёрч (1940) – Типизированное λ-исчисление

$$\dfrac{\begin{array}{c}[x : A]^x \\ \vdots \\ N : B\end{array}}{\lambda x.\, N : A \to B}\ (\to \mathrm{I}^x) \qquad \dfrac{L : A \to B \quad M : A}{L\ M : B}\ (\to \mathrm{E})$$

$$\dfrac{M : A \quad N : B}{(M, N) : A \,\&\, B}\ (\&\mathrm{I}) \qquad \dfrac{L : A \,\&\, B}{\mathrm{fst}\ L : A}\ (\&\mathrm{E}_l) \qquad \dfrac{L : A \,\&\, B}{\mathrm{snd}\ L : B}\ (\&\mathrm{E}_r)$$

Программа

$$
\dfrac{\dfrac{\dfrac{[z : B \mathbin{\&} A]^z}{\mathrm{snd}\ z : A}\ (\&\mathrm{E}_r) \qquad \dfrac{[z : B \mathbin{\&} A]^z}{\mathrm{fst}\ z : B}\ (\&\mathrm{E}_l)}{(\mathrm{snd}\ z, \mathrm{fst}\ z) : A \mathbin{\&} B}\ (\&\mathrm{I})}{\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z) : (B \mathbin{\&} A) \to (A \mathbin{\&} B)}\ (\to \mathrm{I}^z)
$$

Вычисление программ

$$
\dfrac{\dfrac{\begin{matrix}[x : A]^x \\ \vdots \\ N : B\end{matrix}}{\lambda x.\, N : A \to B}\,(\to \mathrm{I}^x) \qquad \begin{matrix}\vdots \\ M : A\end{matrix}}{(\lambda x.\, N)\; M : B}\,(\to \mathrm{E}) \qquad \Rightarrow \qquad \begin{matrix}\vdots \\ M : A \\ \vdots \\ N\{M/x\} : B\end{matrix}
$$

$$
\dfrac{\dfrac{\begin{matrix}\vdots \\ M : A\end{matrix} \quad \begin{matrix}\vdots \\ N : B\end{matrix}}{(M, N) : A \,\&\, B}\,(\&\mathrm{I})}{\mathrm{fst}\ (M, N) : A}\,(\&\mathrm{E}_l) \qquad \Rightarrow \qquad \begin{matrix}\vdots \\ M : A\end{matrix}
$$

Алан Тьюринг (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).

Вычисление программы

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{[z : B \mathbin{\&} A]^z}{\mathrm{snd}\ z : A}\,(\&\mathrm{E}_r)
      \quad
      \dfrac{[z : B \mathbin{\&} A]^z}{\mathrm{fst}\ z : B}\,(\&\mathrm{E}_l)
    }{(\mathrm{snd}\ z, \mathrm{fst}\ z) : A \mathbin{\&} B}\,(\&\mathrm{I})
  }{\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z) : (B \mathbin{\&} A) \to (A \mathbin{\&} B)}\,(\to \mathrm{I}^z)
  \quad
  \dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \mathbin{\&} A}\,(\&\mathrm{I})
}{(\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z))\ (y, x) : A \mathbin{\&} B}\,(\to \mathrm{E})
$$

Вычисление программы

$$\dfrac{\dfrac{\dfrac{\dfrac{[z : B \,\&\, A]^z}{\mathrm{snd}\ z : A}\,(\&\mathrm{E}_r) \qquad \dfrac{[z : B \,\&\, A]^z}{\mathrm{fst}\ z : B}\,(\&\mathrm{E}_l)}{(\mathrm{snd}\ z, \mathrm{fst}\ z) : A \,\&\, B}\,(\&\mathrm{I})}{\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z) : (B \,\&\, A) \to (A \,\&\, B)}\,(\to \mathrm{I}^z) \qquad \dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \,\&\, A}\,(\&\mathrm{I})}{(\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z))\ (y, x) : A \,\&\, B}\,(\to \mathrm{E})$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \,\&\, A}\,(\&\mathrm{I})}{\mathrm{snd}\ (y, x) : A}\,(\&\mathrm{E}_r) \qquad \dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \,\&\, A}\,(\&\mathrm{I})}{\mathrm{fst}\ (y, x) : B}\,(\&\mathrm{E}_l)}{(\mathrm{snd}\ (y, x), \mathrm{fst}\ (y, x)) : A \,\&\, B}\,(\&\mathrm{I})$$

Вычисление программы

$$\dfrac{\dfrac{\dfrac{\dfrac{[z : B \mathbin{\&} A]^z}{\mathrm{snd}\ z : A}\,(\&\mathrm{E}_r) \quad \dfrac{[z : B \mathbin{\&} A]^z}{\mathrm{fst}\ z : B}\,(\&\mathrm{E}_l)}{(\mathrm{snd}\ z, \mathrm{fst}\ z) : A \mathbin{\&} B}\,(\&\mathrm{I})}{\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z) : (B \mathbin{\&} A) \to (A \mathbin{\&} B)}\,(\to \mathrm{I}^z) \quad \dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \mathbin{\&} A}\,(\&\mathrm{I})}{(\lambda z.\ (\mathrm{snd}\ z, \mathrm{fst}\ z))\ (y, x) : A \mathbin{\&} B}\,(\to \mathrm{E})$$

$$\Downarrow$$

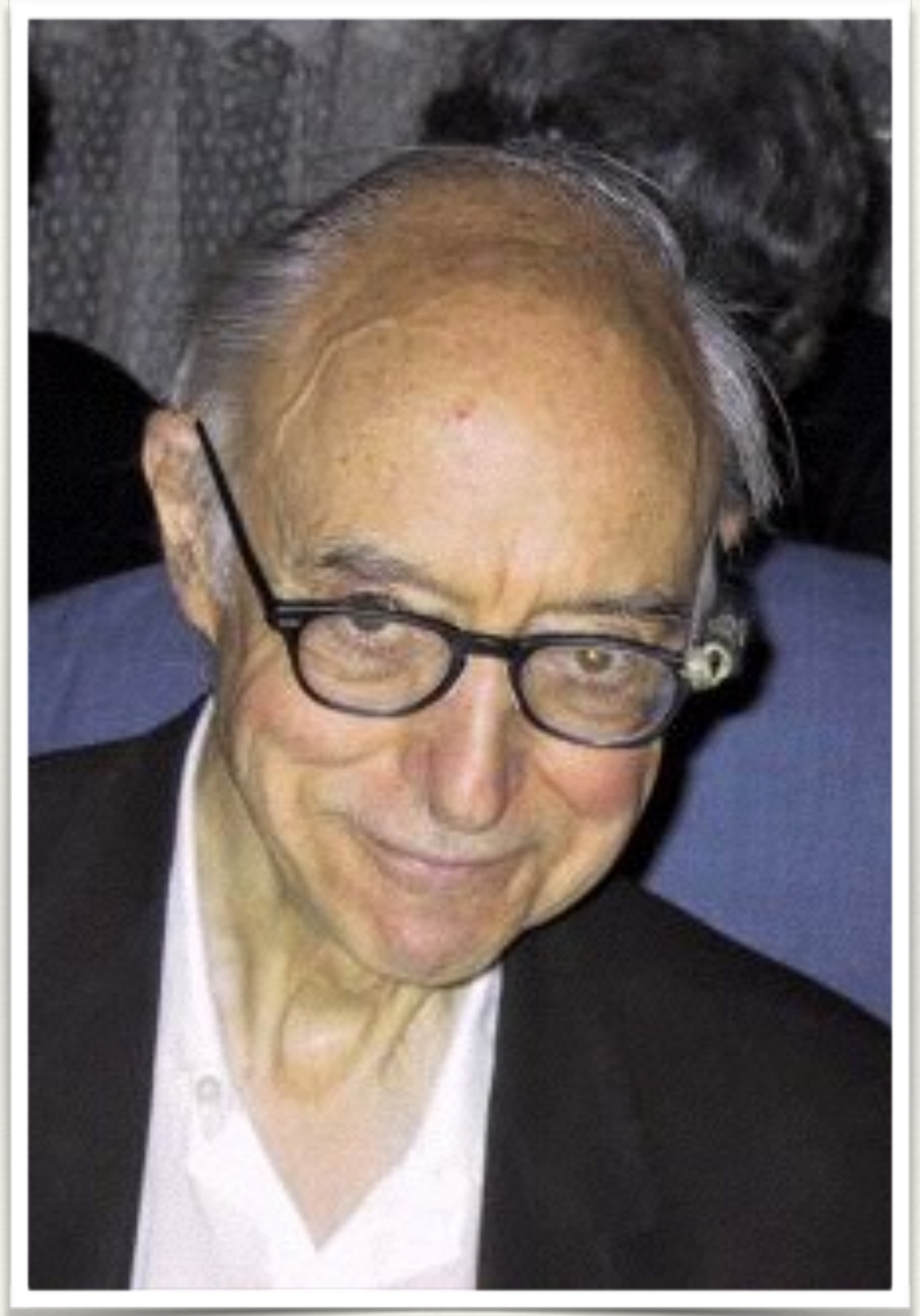
$$\dfrac{\dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \mathbin{\&} A}\,(\&\mathrm{I})}{\mathrm{snd}\ (y, x) : A}\,(\&\mathrm{E}_r) \quad \dfrac{\dfrac{[y : B]^y \quad [x : A]^x}{(y, x) : B \mathbin{\&} A}\,(\&\mathrm{I})}{\mathrm{fst}\ (y, x) : B}\,(\&\mathrm{E}_l)}{(\mathrm{snd}\ (y, x), \mathrm{fst}\ (y, x)) : A \mathbin{\&} B}\,(\&\mathrm{I})$$

$$\Downarrow$$

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

Хаскелл Карри (1900–1982)

Вильям Говард (1926–)



Говард (1980) – Высказывания как Типы

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.

Соответствие Карри-Говарда

высказывания	—	типы
доказательства	—	программы
упрощение доказательств	—	вычисление программ

Соответствие Карри-Говарда

Естественный вывод Генцен (1935)	⇔	**Типизированное λ-исчисление** Чёрч (1940)
Схемы типов Хиндли (1969)	⇔	**Система типов ML** Милнер (1975)
Система F Жирар (1972)	⇔	**Полиморфное λ-исчисление** Рейнольдс (1974)
Модальная логика Льюис (1910)	⇔	**Монады (состояние, исключения)** Клейсли (1965), Могги (1987)
Теорема Гёделя-Генцена о дизъюнкции Гёдель (1932), Генцен(1935)	⇔	**Континуации** Рейнольдс (1972)

Функциональные языки программирования

- Lisp (Маккарти, 1958)
- ISWIM (Лэндин, 1966)
- Scheme (Стил и Сассман, 1970)
- ML (Милнер и др., 1973)
- Haskell (Худак, Пейтон Джонс, Вадлер, 1987)
- Erlang (Армстронг, Вирдинг, Вильямс, 1987)
- OCaml (Лерой, 1996)
- Scala (Одерски, 2003)
- F# (Сайм, 2005)

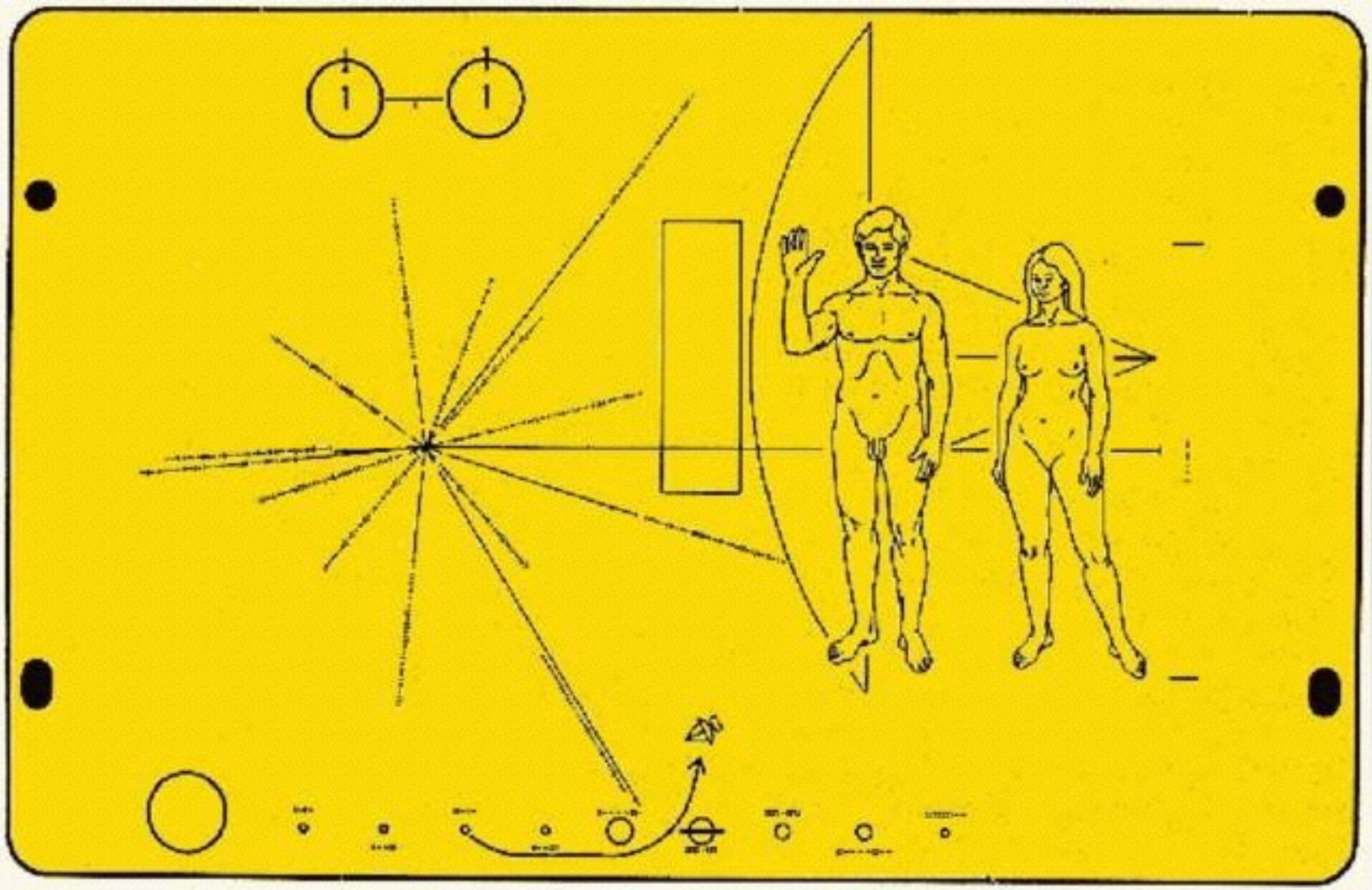
Доказыватели теорем (Theorem provers)

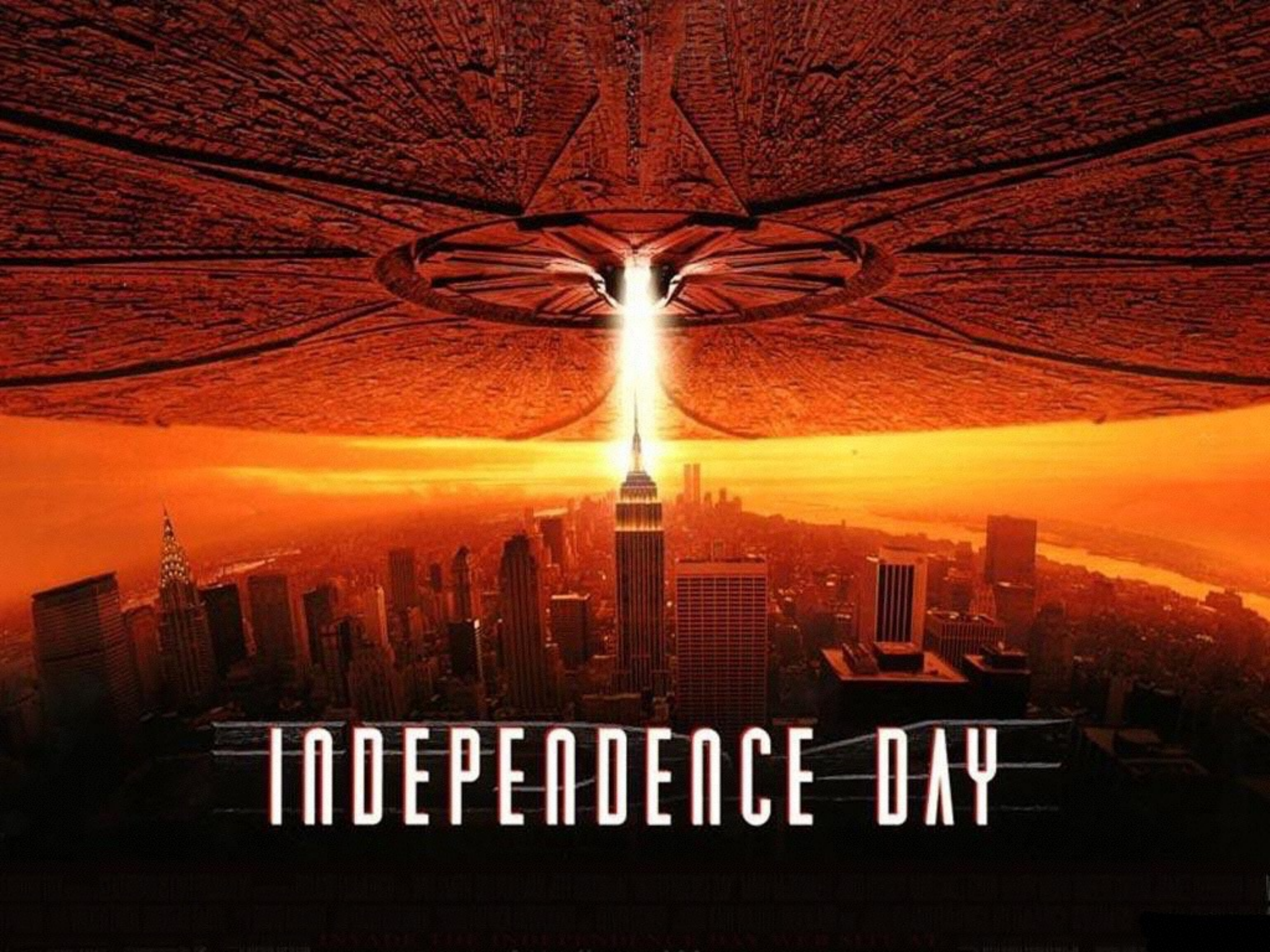
- Automath (де Брёйн, 1970)
- ML/LCF (Милнер и др., 1973)
- Type Theory (Мартин Лёф, 1975)
- Mizar (Трибулек, 1975)
- NuPrl (Констебл, 1985)
- HOL (Гордон и Мелхам, 1988)
- Coq (Хью и Кокан, 1988)
- Isabelle (Полсон, 1993)
- Epigram (Макбрайд и Маккинна, 2004)
- Agda (Норелл, 2005)

Часть 3

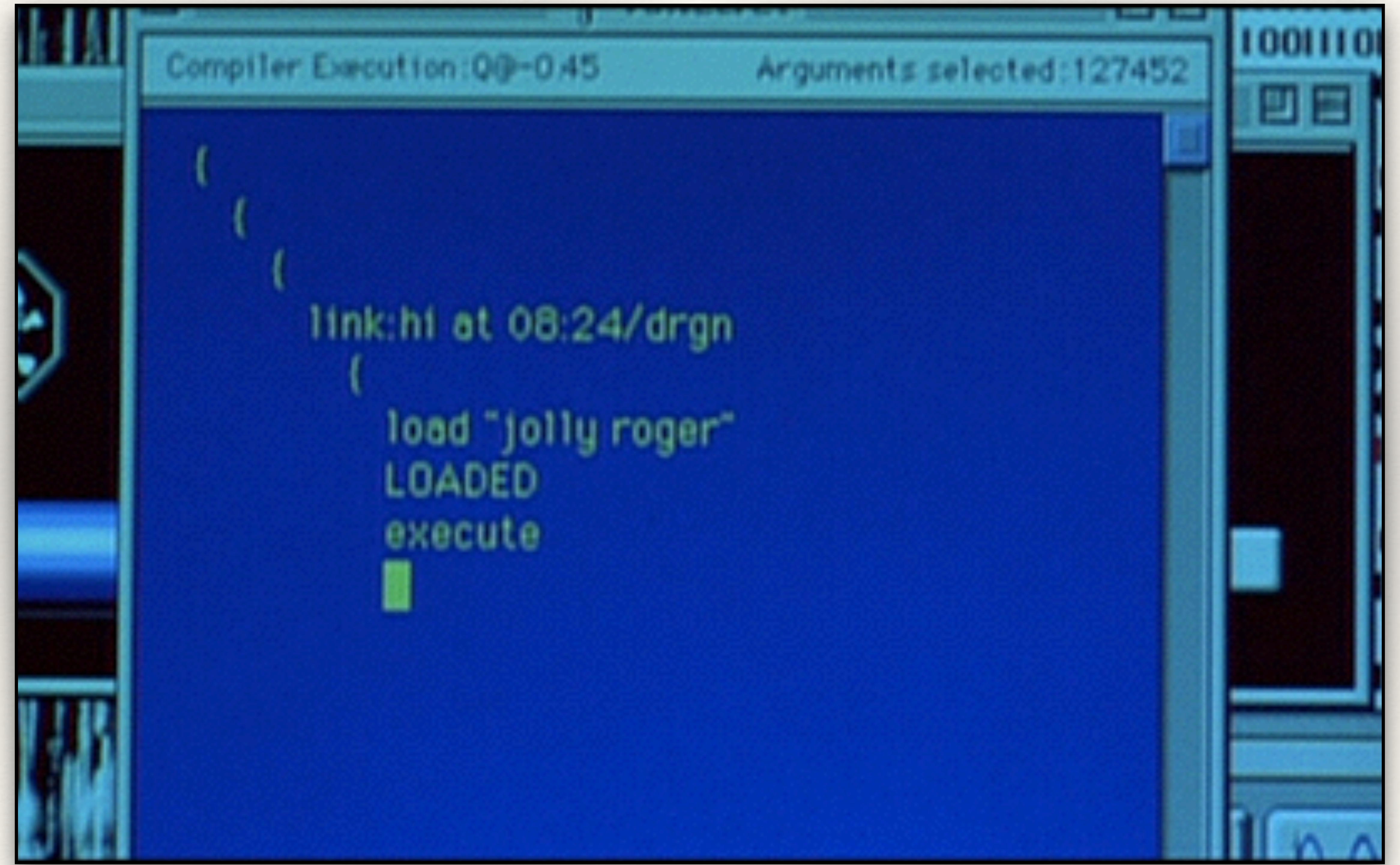
Заключение: Философия

Привет, космос!




INDEPENDENCE DAY

Язык программирования Вселенной?



λ-исчисление – язык **всех** вселенных!