The Girard-Reynolds Isomorphism

Philip Wadler, University of Edinburgh

wadler@inf.ed.ac.uk

Coincidences

Curry-Howard

Hindley-Milner

Girard-Reynolds

John Reynolds (1974)

TOWARDS A THEORY OF TYPE STRUCTURE †

John C. Reynolds

Syracuse University

Syracuse, New York 13210, U.S.A.

Introduction

The type structure of programming languages has been the subject of an active development characterized by continued controversy over basic principles.(1-7) In this paper, we formalize a view of these principles somewhat similar to that of J. H. Morris.(5) We introduce an extension of the typed lambda calculus which permits user-defined types and polymorphic functions, and show that the semantics of this language satisfies a representation theorem which embodies our notion of a "correct" type structure.

Jean-Yves Girard (1972)

UNE EXTENSION DE L'INTERPRETATION DE GÖDEL A L'ANALYSE, ET SON APPLICATION A L'ELIMINATION DES COUPURES DANS L'ANALYSE ET LA THEORIE DES TYPES

Jean-Yves GIRARD

(8, Rue du Moulin d'Amboile, 94-Sucy en Brie, France)

Ce travail comprend (Ch. 1–5) une interprétation de l'Analyse, exprimée dans la logique intuitionniste, dans un système de fonctionnelles Y, décrit Ch. 1, et qui est une extension du système connu de Gödel [Gd]. En gros, le système est obtenu par l'adjonction de deux sortes de types (respectivement existentiels et universels, si les types construits avec → sont considérés comme implicationnels) et de quatre schémas de construction de fonctionelles correspondant à l'introduction et à l'élimination de chacun de ces types, ainsi que par la donnée des règles de calcul (réductions) correspondantes.

John Reynolds (1983)

Types, Abstraction and Parametric Polymorphism

Once upon a time, there was a university with a peculiar tenure policy. All faculty were tenured, and could only be dismissed for moral turpitude. What was peculiar was the definition of moral turpitude: making a false statement in class. Needless to say, the university did not teach computer science. However, it had a renowned department of mathematics.

One semester, there was such a large enrollment in complex variables that two sections were scheduled. In one section, Professor Descartes announced that a complex number was an ordered pair of reals, and that two complex numbers were equal when their corresponding components were equal. He went on to explain how to convert reals into complex numbers, what “i” was, how to add, multiply, and conjugate complex numbers, and how to find their magnitude.

John Reynolds (1983), continued

In the other section, Professor Bessel announced that a complex number was an ordered pair of reals the first of which was nonnegative, and that two complex numbers were equal if their first components were equal and either the first components were zero or the second components differed by a multiple of 2. He then told an entirely different story about converting reals, “i”, addition, multiplication, conjugation, and magnitude.

Then, after their first classes, an unfortunate mistake in the registrar’s office caused the two sections to be interchanged. Despite this, neither Descartes nor Bessel ever committed moral turpitude, even though each was judged by the other’s definitions. The reason was that they both had an intuitive understanding of type. Having defined complex numbers and the primitive operations upon them, thereafter they spoke at a level of abstraction that encompassed both of their definitions.

The moral of this fable is that: *Type structure is a syntactic discipline for enforcing levels of abstraction*.

A tale of Two Theorems

Girard's Representation Theorem

Every function that can be proved total in
second-order Peano arithmetic can be represented in
second-order lambda calculus.

Reynolds's Abstraction Theorem

Terms in second-order lambda calculus take
related arguments to related results,
for a suitable notion of logical relation.

A tale of Two Theorems

Girard's Representation Theorem

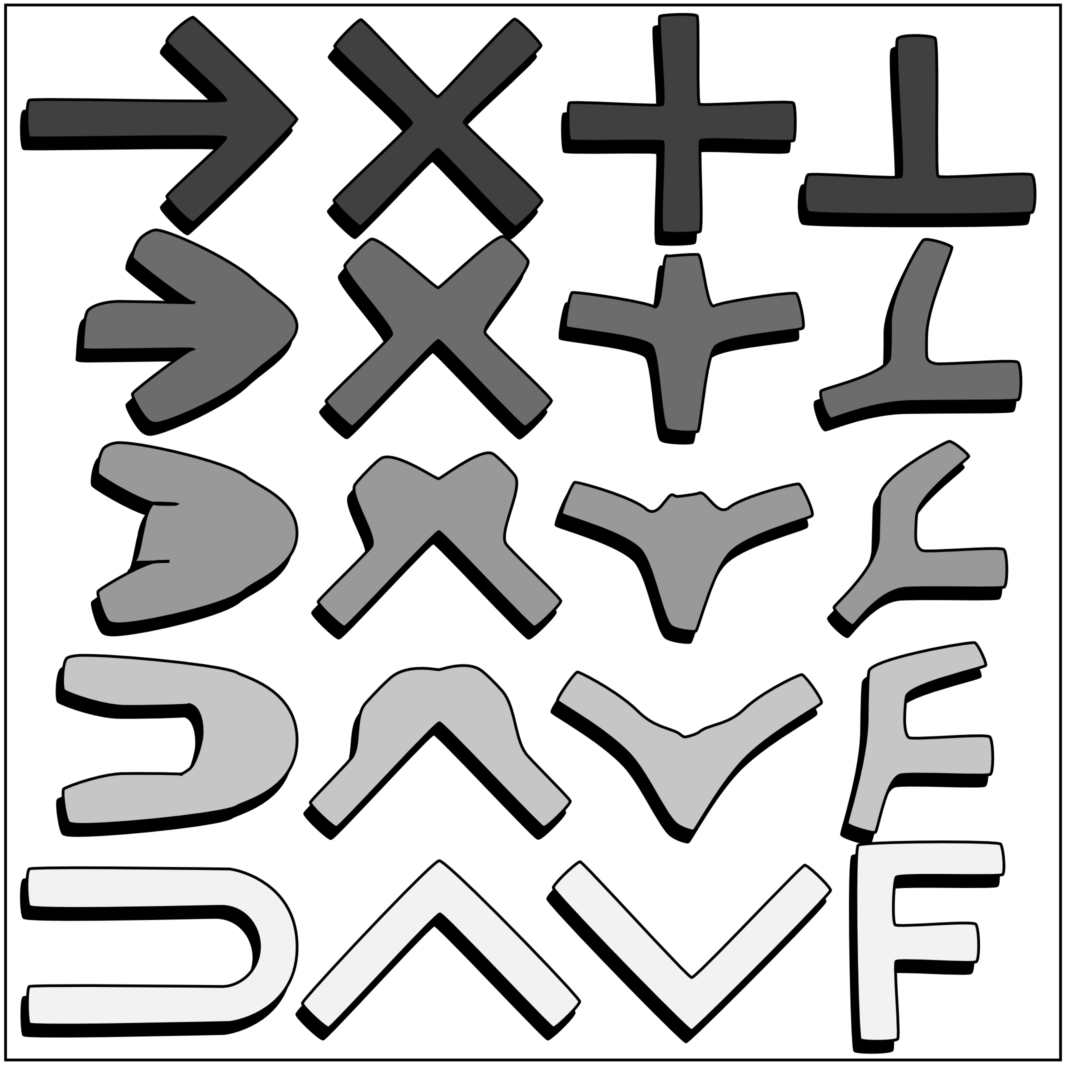
Every function that can be proved total in
second-order Peano arithmetic can be represented in
second-order lambda calculus.

projection : proofs $\longrightarrow$ terms

Reynolds's Abstraction Theorem

Terms in second-order lambda calculus take
related arguments to related results,
for a suitable notion of logical relation.

embedding : terms $\longrightarrow$ proofs



LC'90 *The Curry-Howard homeomorphism*

The Curry-Howard Isomorphism

$$\frac{\forall \quad \supset \quad \wedge \quad \vee \quad F}{\Pi \quad \rightarrow \quad \times \quad + \quad \perp}$$

The Girard-Reynolds Isomorphism

$$\frac{\forall \quad \forall^2 \quad \forall^1 \quad \longrightarrow}{\forall \qquad\qquad\qquad \longrightarrow}$$

The Curry-Howard Isomorphism

$$\begin{array}{ccccc} \forall & \supset & \wedge & \vee & F \\ \hline \Pi & \to & \times & + & \bot \end{array}$$

The Girard-Reynolds Isomorphism

$$\begin{array}{cccc} \forall & \forall^2 & \forall^1 & \longrightarrow \\ \hline \forall & & & \longrightarrow \end{array}$$

Rather than enriching the type systems to match logic,
we impoverish logic to match the type structure.

— Daniel Leivant

Part I

The Girard Projection — from Logic to Lambda

Naturals

A sort and two operations

$$\mathsf{N}, \quad \mathsf{s}^{\mathsf{N}\to\mathsf{N}}, \quad \mathsf{z}^{\mathsf{N}}$$

Define operations by equations

$$(+)^{\mathsf{N}\to\mathsf{N}\to\mathsf{N}}$$

$$\begin{aligned} (\mathsf{s}\,m) + n &= \mathsf{s}\,(m+n) \\ \mathsf{z} + n &= n \end{aligned}$$

Induction

Naturals satisfy induction

$$\mathbf{N} \;\equiv\; \{n^{\mathsf{N}} \mid \forall \mathcal{X}^{\mathsf{N}}.\, (\forall m^{\mathsf{N}}.\, m \in \mathcal{X} \longrightarrow \mathsf{s}\, m \in \mathcal{X}) \longrightarrow \mathsf{z} \in \mathcal{X} \longrightarrow n \in \mathcal{X}\}$$

Three theorems

$$\forall n^{\mathsf{N}}.\, n \in \mathbf{N} \longrightarrow \mathsf{s}\, n \in \mathbf{N}$$

$$\mathsf{z} \in \mathbf{N}$$

$$\forall m^{\mathsf{N}}.\, \forall n^{\mathsf{N}}.\, m \in \mathbf{N} \longrightarrow n \in \mathbf{N} \longrightarrow m + n \in \mathbf{N}$$

Girard projection — from predicates to types

$$\mathbf{N} \;\equiv\; \{n^{\mathsf{N}} \mid \forall \boldsymbol{\mathcal{X}}^{\mathsf{N}}.\, (\forall m^{\mathsf{N}}.\, m \in \boldsymbol{\mathcal{X}} \to \mathsf{s}\, m \in \boldsymbol{\mathcal{X}}) \to \mathsf{z} \in \boldsymbol{\mathcal{X}} \to n \in \boldsymbol{\mathcal{X}}\}$$

$$\downarrow$$

$$\mathsf{N} \;\equiv\; \forall X.\, (X \to X) \to (X \to X)$$

Girard projection — from proofs to terms

$$\forall n^{\mathsf{N}}.\, n \in \mathbf{N} \longrightarrow \mathsf{s}\, n \in \mathbf{N}$$

$$\downarrow$$

$$\mathsf{s}^{\mathsf{N}\to\mathsf{N}} \;\equiv\; \lambda n^{\mathsf{N}}.\, \Lambda X.\, \lambda s^{X\to X}.\, \lambda z^{X}.\, s\;(n\;X\;s\;z)$$

$$\mathsf{z} \in \mathbf{N}$$

$$\downarrow$$

$$\mathsf{z}^{\mathsf{N}} \;\equiv\; \Lambda X.\, \lambda s^{X\to X}.\, \lambda z^{X}.\, z$$

$$\forall m^{\mathsf{N}}.\, \forall n^{\mathsf{N}}.\, m \in \mathbf{N} \longrightarrow n \in \mathbf{N} \longrightarrow m + n \in \mathbf{N}$$

$$\downarrow$$

$$(+)^{\mathsf{N}\to\mathsf{N}\to\mathsf{N}} \;\equiv\; \lambda m^{\mathsf{N}}.\, \lambda n^{\mathsf{N}}.\, m\;\mathsf{N}\;\mathsf{s}\;n$$

Successor: proof

$$\boldsymbol{A}_{\mathsf{s}} \equiv \forall m^{\mathsf{N}}.\, m \in \boldsymbol{\mathcal{X}} \longrightarrow \mathsf{s}\, m \in \boldsymbol{\mathcal{X}} \qquad\qquad \boldsymbol{A}_{\mathsf{z}} \equiv \mathsf{z} \in \boldsymbol{\mathcal{X}}$$

$$
\begin{prooftree}
\AxiomC{$[\boldsymbol{A}_{\mathsf{s}}]^{s}$}
\RightLabel{$\forall^1\mathrm{E}$}
\UnaryInfC{$n \in \boldsymbol{\mathcal{X}} \longrightarrow \mathsf{s}\, n \in \boldsymbol{\mathcal{X}}$}
\AxiomC{$[n \in \mathbf{N}]^{n}$}
\RightLabel{β}
\UnaryInfC{$\forall \boldsymbol{\mathcal{X}}^{\mathsf{N}}.\, \boldsymbol{A}_{\mathsf{s}} \longrightarrow \boldsymbol{A}_{\mathsf{z}} \longrightarrow n \in \boldsymbol{\mathcal{X}}$}
\RightLabel{$\forall\mathbf{E}$}
\UnaryInfC{$\boldsymbol{A}_{\mathsf{s}} \longrightarrow \boldsymbol{A}_{\mathsf{z}} \longrightarrow n \in \boldsymbol{\mathcal{X}}$}
\AxiomC{$[\boldsymbol{A}_{\mathsf{s}}]^{s}$}
\RightLabel{$\longrightarrow\mathbf{E}$}
\BinaryInfC{$\boldsymbol{A}_{\mathsf{z}} \longrightarrow n \in \boldsymbol{\mathcal{X}}$}
\AxiomC{$[\boldsymbol{A}_{\mathsf{z}}]^{z}$}
\RightLabel{$\longrightarrow\mathbf{E}$}
\BinaryInfC{$n \in \boldsymbol{\mathcal{X}}$}
\RightLabel{$\longrightarrow\mathbf{E}$}
\BinaryInfC{$\mathsf{s}\, n \in \boldsymbol{\mathcal{X}}$}
\RightLabel{$\longrightarrow\mathbf{I}^{z}$}
\UnaryInfC{$\boldsymbol{A}_{\mathsf{z}} \longrightarrow \mathsf{s}\, n \in \boldsymbol{\mathcal{X}}$}
\RightLabel{$\longrightarrow\mathbf{I}^{s}$}
\UnaryInfC{$\boldsymbol{A}_{\mathsf{s}} \longrightarrow \boldsymbol{A}_{\mathsf{z}} \longrightarrow \mathsf{s}\, n \in \boldsymbol{\mathcal{X}}$}
\RightLabel{$\forall\mathbf{I}$}
\UnaryInfC{$\forall \boldsymbol{\mathcal{X}}^{\mathsf{N}}.\, \boldsymbol{A}_{\mathsf{s}} \longrightarrow \boldsymbol{A}_{\mathsf{z}} \longrightarrow \mathsf{s}\, n \in \boldsymbol{\mathcal{X}}$}
\RightLabel{β}
\UnaryInfC{$\mathsf{s}\, n \in \mathbf{N}$}
\RightLabel{$\longrightarrow\mathbf{I}^{n}$}
\UnaryInfC{$n \in \mathbf{N} \longrightarrow \mathsf{s}\, n \in \mathbf{N}$}
\RightLabel{$\forall^1\mathrm{I}$}
\UnaryInfC{$\forall n^{\mathsf{N}}.\, n \in \mathbf{N} \longrightarrow \mathsf{s}\, n \in \mathbf{N}$}
\end{prooftree}
$$

Successor: term

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[s^{X\to X}] \qquad \dfrac{\dfrac{\dfrac{[n^{\mathsf{N}}]}{(n\ X)^{(X\to X)\to X\to X}}\ \forall\mathrm{E} \qquad [s^{X\to X}]}{(n\ X\ s)^{X\to X}}\ {\to}\mathrm{E} \qquad [z^{X}]}{(n\ X\ s\ z)^{X}}\ {\to}\mathrm{E}}{(s\ (n\ X\ s\ z))^{X}}\ {\to}\mathrm{E}}{(\lambda z^{X}.\, s\ (n\ X\ s\ z))^{X\to X}}\ {\to}\mathrm{I}^{z}}{(\lambda s^{X\to X}.\, \lambda z^{X}.\, s\ (n\ X\ s\ z))^{(X\to X)\to X\to X}}\ {\to}\mathrm{I}^{s}}{(\Lambda X.\, \lambda s^{X\to X}.\, \lambda z^{X}.\, s\ (n\ X\ s\ z))^{\mathsf{N}}}\ \forall\mathrm{I}}{(\lambda n^{\mathsf{N}}.\, \Lambda X.\, \lambda s^{X\to X}.\, \lambda z^{X}.\, s\ (n\ X\ s\ z))^{\mathsf{N}\to\mathsf{N}}}\ {\to}\mathrm{I}^{n}
$$

Plus: proof

$$\boldsymbol{A}_{\mathsf{s}} \equiv \forall m^{\mathsf{N}}.\, m \in \boldsymbol{\mathcal{X}} \longrightarrow \mathsf{s}\, m \in \boldsymbol{\mathcal{X}} \qquad \boldsymbol{A}_{\mathsf{z}} \equiv \mathsf{z} \in \boldsymbol{\mathcal{X}}$$

$$\boldsymbol{A}_{\mathsf{s}+} \equiv \forall m^{\mathsf{N}}.\, m + n \in \mathbf{N} \longrightarrow (\mathsf{s}\, m) + n \in \mathbf{N} \qquad \boldsymbol{A}_{\mathsf{z}+} \equiv \mathsf{z} + n \in \mathbf{N}$$

$$
\begin{prooftree}
\AxiomC{$[m \in \mathbf{N}]^{\boldsymbol{m}}$}
\RightLabel{β}
\UnaryInfC{$\forall \boldsymbol{\mathcal{X}}^{\mathsf{N}}.\, \boldsymbol{A}_{\mathsf{s}} \longrightarrow \boldsymbol{A}_{\mathsf{z}} \longrightarrow m \in \boldsymbol{\mathcal{X}}$}
\RightLabel{$\forall\mathbf{E}$}
\UnaryInfC{$\boldsymbol{A}_{\mathsf{s}+} \longrightarrow \boldsymbol{A}_{\mathsf{z}+} \longrightarrow m + n \in \mathbf{N}$}
\AxiomC{$\vdots\ \boldsymbol{s}$}
\noLine
\UnaryInfC{$\forall n^{\mathsf{N}}.\, n \in \mathbf{N} \longrightarrow \mathsf{s}\, n \in \mathbf{N}$}
\RightLabel{$\forall^1\mathrm{E}$}
\UnaryInfC{$m + n \in \mathbf{N} \longrightarrow \mathsf{s}\,(m + n) \in \mathbf{N}$}
\RightLabel{β^+}
\UnaryInfC{$m + n \in \mathbf{N} \longrightarrow (\mathsf{s}\, m) + n \in \mathbf{N}$}
\RightLabel{$\forall^1\mathrm{I}$}
\UnaryInfC{$\boldsymbol{A}_{\mathsf{s}+}$}
\RightLabel{$\longrightarrow\mathbf{E}$}
\BinaryInfC{$\boldsymbol{A}_{\mathsf{z}+} \longrightarrow m + n \in \mathbf{N}$}
\AxiomC{$[n \in \mathbf{N}]^{\boldsymbol{n}}$}
\RightLabel{β^+}
\UnaryInfC{$\boldsymbol{A}_{\mathsf{z}+}$}
\RightLabel{$\longrightarrow\mathbf{E}$}
\BinaryInfC{$m + n \in \mathbf{N}$}
\RightLabel{$\longrightarrow\mathbf{I}^{\boldsymbol{n}}$}
\UnaryInfC{$n \in \mathbf{N} \longrightarrow m + n \in \mathbf{N}$}
\RightLabel{$\longrightarrow\mathbf{I}^{\boldsymbol{m}}$}
\UnaryInfC{$m \in \mathbf{N} \longrightarrow n \in \mathbf{N} \longrightarrow m + n \in \mathbf{N}$}
\end{prooftree}
$$

Plus: term

$$
\cfrac{
  \cfrac{
    \cfrac{
      \cfrac{[m^{\mathsf{N}}]}{(m\ \mathsf{N})^{(\mathsf{N}\to\mathsf{N})\to\mathsf{N}\to\mathsf{N}}}\,\forall\mathrm{E}
      \qquad
      \begin{matrix}\vdots\\ \mathsf{s}^{\mathsf{N}\to\mathsf{N}}\end{matrix}
    }{(m\ \mathsf{N}\ \mathsf{s})^{\mathsf{N}\to\mathsf{N}}}\,{\to}\mathrm{E}
    \qquad [n^{\mathsf{N}}]
  }{
    \cfrac{(m\ \mathsf{N}\ \mathsf{s}\ n)^{\mathsf{N}}}{(\lambda n^{\mathsf{N}}.\, m\ \mathsf{N}\ \mathsf{s}\ n)^{\mathsf{N}\to\mathsf{N}}}\,{\to}\mathrm{I}^{n}
  }\,{\to}\mathrm{E}
}{(\lambda m^{\mathsf{N}}.\, \lambda n^{\mathsf{N}}.\, m\ \mathsf{N}\ \mathsf{s}\ n)^{\mathsf{N}\to\mathsf{N}}}\,{\to}\mathrm{I}^{m}
$$

Part II

The Reynolds Embedding
— from Lambda to Logic

The Reynolds embedding — from types to predicates

$$\mathsf{N} \;\equiv\; \forall X.\, (X \to X) \to (X \to X)$$

$$\downarrow$$

$$\begin{aligned}\mathsf{N}^* \;\equiv\; \{n^{\mathsf{N}} \mid \forall X. \forall \boldsymbol{\mathcal{X}}^X. &\\ &\forall s^{X \to X}.\, (\forall m^X.\, m \in \boldsymbol{\mathcal{X}} \longrightarrow s\, m \in \boldsymbol{\mathcal{X}}) \longrightarrow \\ &\quad \forall z^X.\, z \in \boldsymbol{\mathcal{X}} \longrightarrow n\, X\, s\, z \in \boldsymbol{\mathcal{X}}\}\end{aligned}$$

The Reynolds embedding — from terms to proofs

$$\mathsf{s}^{\mathsf{N}\to\mathsf{N}}$$

$$\downarrow$$

$$\forall n^{\mathsf{N}}.\, n \in \mathsf{N}^* \longrightarrow \mathsf{s}\, n \in \mathsf{N}^*$$

$$\mathsf{z}^{\mathsf{N}}$$

$$\downarrow$$

$$\mathsf{z} \in \mathsf{N}^*$$

$$(+)^{\mathsf{N}\to\mathsf{N}\to\mathsf{N}}$$

$$\downarrow$$

$$\forall m^{\mathsf{N}}.\, \forall n^{\mathsf{N}}.\, m \in \mathsf{N}^* \longrightarrow n \in \mathsf{N}^* \longrightarrow m + n \in \mathsf{N}^*$$

Doubling — from predicates to predicates

$$
\begin{array}{l}
\mathsf{N}^* \ \equiv \\
\quad \{n^{\mathsf{N}} \mid \\
\quad\quad \forall X. \forall \boldsymbol{\mathcal{X}}^X. \\
\quad\quad\quad \forall s^{X \to X}. (\forall m^X. m \in \boldsymbol{\mathcal{X}} \to s\, m \in \boldsymbol{\mathcal{X}}) \to \\
\quad\quad\quad\quad \forall z^X. z \in \boldsymbol{\mathcal{X}} \to n\; X\; s\; z \in \boldsymbol{\mathcal{X}}\} \\
\quad\quad\quad\quad \downarrow \\
\mathsf{N}^{*\ddagger} \ \equiv \\
\quad \{(n^{\mathsf{N}}, n'^{\mathsf{N}}) \mid \\
\quad\quad \forall X. \forall X'. \forall \boldsymbol{\mathcal{X}}^{X \times X'}. \\
\quad\quad\quad \forall s^{X \to X}. \forall s'^{X' \to X'}. (\forall m^X. \forall m'^{X'}. (m, m') \in \boldsymbol{\mathcal{X}} \to (s\, m, s'\, m') \in \boldsymbol{\mathcal{X}}) \to \\
\quad\quad\quad\quad \forall z^X. \forall z'^{X'}. (z, z') \in \boldsymbol{\mathcal{X}} \to (n\; X\; s\; z, n'\; X'\; s'\; z') \in \boldsymbol{\mathcal{X}}\}
\end{array}
$$

Doubling — from proofs to proofs

$$\forall n^{\mathsf{N}}.\, n \in \mathsf{N}^* \longrightarrow \mathsf{s}\, n \in \mathsf{N}^*$$

$$\downarrow$$

$$\forall n^{\mathsf{N}}, n'^{\mathsf{N}}.\, (n, n') \in \mathsf{N}^{*\ddagger} \longrightarrow (\mathsf{s}\, n, \mathsf{s}\, n') \in \mathsf{N}^{*\ddagger}$$

$$\mathsf{z} \in \mathsf{N}^*$$

$$\downarrow$$

$$(\mathsf{z}, \mathsf{z}) \in \mathsf{N}^{*\ddagger}$$

$$\forall m^{\mathsf{N}}.\, \forall n^{\mathsf{N}}.\, m \in \mathsf{N}^* \longrightarrow n \in \mathsf{N}^* \longrightarrow m + n \in \mathsf{N}^*$$

$$\downarrow$$

$$\forall m^{\mathsf{N}}, m'^{\mathsf{N}}.\, \forall n^{\mathsf{N}}, n'^{\mathsf{N}}.\, (m, m') \in \mathsf{N}^{*\ddagger} \longrightarrow (n, n') \in \mathsf{N}^{*\ddagger} \longrightarrow (m + n, m' + n') \in \mathsf{N}^{*\ddagger}$$

The Abstraction Theorem — Reynolds then doubling

$$\mathsf{s}^{\mathsf{N}\to\mathsf{N}}$$

$$\downarrow$$

$$\forall n^{\mathsf{N}}, n'^{\mathsf{N}}.\, (n, n') \in \mathsf{N}^{*\ddagger} \longrightarrow (\mathsf{s}\, n, \mathsf{s}\, n') \in \mathsf{N}^{*\ddagger}$$

$$\mathsf{z}^{\mathsf{N}}$$

$$\downarrow$$

$$(\mathsf{z}, \mathsf{z}) \in \mathsf{N}^{*\ddagger}$$

$$(+)^{\mathsf{N}\to\mathsf{N}\to\mathsf{N}}$$

$$\downarrow$$

$$\forall m^{\mathsf{N}}, m'^{\mathsf{N}}.\, \forall n^{\mathsf{N}}, n'^{\mathsf{N}}.\, (m, m') \in \mathsf{N}^{*\ddagger} \longrightarrow (n, n') \in \mathsf{N}^{*\ddagger} \longrightarrow (m + n, m' + n') \in \mathsf{N}^{*\ddagger}$$

Parametricity and weak parametricity

Halving lemma (binary implies unary)

$$\forall n^{\mathsf{N}}, n'^{\mathsf{N}}.\, (n, n') \in \mathsf{N}^{*\ddagger} \longrightarrow n \in \mathsf{N}^{*}$$

Extensiveness

$$\forall n^{\mathsf{N}}, n'^{\mathsf{N}}.\, (n, n') \in \mathsf{N}^{*\ddagger} \longrightarrow n = n'$$

Parametricity

$$\forall n^{\mathsf{N}}.\, (n, n) \in \mathsf{N}^{*\ddagger}$$

Weak parametricity (unary implies binary)

$$\forall n^{\mathsf{N}}.\, n \in \mathsf{N}^{*} \longrightarrow (n, n) \in \mathsf{N}^{*\ddagger}$$

Part III

The Girard-Reynolds Isomorphism

Girard followed by Reynolds

$$\mathbf{N} \;\equiv\; \{n^{\mathsf{N}} \mid \forall \boldsymbol{\mathcal{X}}^{\mathsf{N}}.\, (\forall m^{\mathsf{N}}.\, m \in \boldsymbol{\mathcal{X}} \rightarrow \mathsf{s}\, m \in \boldsymbol{\mathcal{X}}) \rightarrow \mathsf{z} \in \boldsymbol{\mathcal{X}} \rightarrow n \in \boldsymbol{\mathcal{X}}\}$$

$$\downarrow$$

$$\mathbf{N}^{\circ} \;\equiv\; \mathsf{N} \;\equiv\; \forall X.\, (X \rightarrow X) \rightarrow (X \rightarrow X)$$

$$\downarrow$$

$$\mathsf{N}^{\circ *} \;\equiv\; \mathsf{N}^{*} \;\equiv$$

$$\{n^{\mathsf{N}} \mid$$

$$\forall X.\, \forall \boldsymbol{\mathcal{X}}^{X}.$$

$$\forall s^{X \rightarrow X}.\, (\forall m^{X}.\, m \in \boldsymbol{\mathcal{X}} \rightarrow s\, m \in \boldsymbol{\mathcal{X}}) \rightarrow$$

$$\forall z^{X}.\, z \in \boldsymbol{\mathcal{X}} \rightarrow n\; X\; s\; z \in \boldsymbol{\mathcal{X}}\}$$

Girard-Reynolds isomorphism

Induction implies unary parametricity

$$\forall n.\, n \in \mathbf{N} \longrightarrow n \in \mathsf{N}^*$$

Binary parametricity is equivalent to induction

$$\forall n, n'.\, (n, n') \in \mathsf{N}^{*\ddagger} \leftrightarrow n = n' \wedge n \in \mathbf{N}$$

Weak parametricity holds iff
Girard followed by Reynolds is an isomorphism

$$(\forall n.\, n \in \mathsf{N}^* \longrightarrow (n, n) \in \mathsf{N}^{*\ddagger}) \leftrightarrow (\forall n.\, n \in \mathsf{N}^* \leftrightarrow n \in \mathbf{N})$$

Part IV

Conclusion

Related work

Girard 1972

Reynolds 1974, 1983

Böhm and Beararducci 1985

Leivant 1990

Krivine and Parigot 1990

Mairson 1991

Plotkin and Abadi 1993

Hasegawa 1994

Takeuti 1998

Related work: Models

Moggi 1986

Breazu-Tannen and Coquand 1988

Freyd 1989

Hyland, Robinson, and Rosolini 1990

Rummelhoff 2003

Møgelberg 2004

Conclusion

The Girard-Reynolds type system is
the basis for generics in Java 1.5.

Conclusion

The Girard-Reynolds type system is
the basis for generics in Java 1.5.

Girard and Reynolds will be remembered
long after Java is forgotten.

Part V

Details

Second-order lambda calculus (F2)

$$
\begin{array}{llcl}
\text{Type variables} & X, Y, Z & & \\
\text{Types} & A, B, C & ::= & X \\
 & & \mid & A \to B \\
 & & \mid & \forall X.\, B \\
\text{Individual variables} & x, y, z & & \\
\text{Terms} & s, t, u & ::= & x^A \\
 & & \mid & \lambda x^A.\, u \\
 & & \mid & s\ t \\
 & & \mid & \Lambda X.\, u \\
 & & \mid & s\ A
\end{array}
$$

Second-order lambda calculus (F2)

$$\dfrac{\begin{array}{c}[x^A]\\ \vdots\\ u^B\end{array}}{(\lambda x^A.\, u)^{A \to B}} \to \mathrm{I}^x \qquad \dfrac{s^{A\to B} \qquad t^A}{(s\ t)^B} \to \mathrm{E}$$

$$\dfrac{u^B}{(\Lambda X.\, u)^{\forall X.\, B}} \forall \mathrm{I} \quad X \text{ does not escape} \qquad \dfrac{s^{\forall X.\, B}}{(s\ A)^{B[A/X]}} \forall \mathrm{E}$$

Second-order propositional logic (P2)

Predicate variables	$\boldsymbol{\mathcal{X}}, \boldsymbol{\mathcal{Y}}, \boldsymbol{\mathcal{Z}}$		
Propositions	$\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$	$::=$	$t^C \in \boldsymbol{\mathcal{A}}^C$
		$\mid$	$\boldsymbol{A} \rightarrow \boldsymbol{B}$
		$\mid$	$\forall \boldsymbol{\mathcal{X}}^C \boldsymbol{.}\, \boldsymbol{B}$
		$\mid$	$\forall x^C .\, \boldsymbol{B}$
		$\mid$	$\forall X .\, \boldsymbol{B}$
Predicates	$\boldsymbol{\mathcal{A}}, \boldsymbol{\mathcal{B}}, \boldsymbol{\mathcal{C}}$	$::=$	$\boldsymbol{\mathcal{X}}^C$
		$\mid$	$\{x^C \mid \boldsymbol{A}\}$
Hypothesis labels	$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$		
Proofs	$\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{u}$		

Second-order propositional logic (P2)

$$\dfrac{\begin{matrix}[\boldsymbol{A}]^{\boldsymbol{x}} \\ \vdots \\ \boldsymbol{B}\end{matrix}}{\boldsymbol{A} \to \boldsymbol{B}} \to\!\mathbf{I}^{\boldsymbol{x}} \qquad \dfrac{\boldsymbol{A} \to \boldsymbol{B} \qquad \boldsymbol{A}}{\boldsymbol{B}} \to\!\mathbf{E}$$

$$\dfrac{\boldsymbol{B}}{\forall \boldsymbol{\mathcal{X}}^{C}.\,\boldsymbol{B}} \,\forall\mathbf{I} \quad \boldsymbol{\mathcal{X}} \text{ does not escape} \qquad \dfrac{\forall \boldsymbol{\mathcal{X}}^{C}.\,\boldsymbol{B}}{\boldsymbol{B}[\boldsymbol{\mathcal{A}}^{C}/\boldsymbol{\mathcal{X}}]} \,\forall\mathbf{E}$$

$$\dfrac{\boldsymbol{B}}{\forall x^{C}.\,\boldsymbol{B}} \,\forall^1\mathrm{I} \quad x \text{ does not escape} \qquad \dfrac{\forall x^{C}.\,\boldsymbol{B}}{\boldsymbol{B}[t^{C}/x]} \,\forall^1\mathrm{E}$$

$$\dfrac{\boldsymbol{B}}{\forall X.\,\boldsymbol{B}} \,\forall^2\mathrm{I} \quad X \text{ does not escape} \qquad \dfrac{\forall X.\,\boldsymbol{B}}{\boldsymbol{B}[A/X]} \,\forall^2\mathrm{E}$$

β rules

$$
\begin{array}{lcl}
(\lambda x^T.\, u)\; t & =_\beta & u[t/x] \\
(\Lambda X.\, u)\; A & =_\beta & u[A/X] \\
t^C \in \{x^C \mid \boldsymbol{A}\} & =_\beta & \boldsymbol{A}[t/x]
\end{array}
$$

$$
\frac{\boldsymbol{A}}{\boldsymbol{B}}\,\beta \qquad \boldsymbol{A} =_\beta \boldsymbol{B}
$$

Part VI

Girard projection

Girard projection

Propositions

$$
\begin{aligned}
(t^C \in \boldsymbol{\mathcal{A}}^C)^\circ &\equiv \boldsymbol{\mathcal{A}}^\circ \\
(\boldsymbol{A} \to \boldsymbol{B})^\circ &\equiv \boldsymbol{A}^\circ \to \boldsymbol{B}^\circ \\
(\forall \boldsymbol{\mathcal{X}}^C.\, \boldsymbol{B})^\circ &\equiv \forall X.\, \boldsymbol{B}^\circ \\
(\forall x^C.\, \boldsymbol{B})^\circ &\equiv \boldsymbol{B}^\circ \\
(\forall X.\, \boldsymbol{B})^\circ &\equiv \boldsymbol{B}^\circ
\end{aligned}
$$

Predicates

$$
\begin{aligned}
(\boldsymbol{\mathcal{X}}^C)^\circ &\equiv X \\
(\{x^C \mid \boldsymbol{A}\})^\circ &\equiv \boldsymbol{A}^\circ
\end{aligned}
$$

Girard projection

$$\left(\dfrac{\begin{matrix} [\boldsymbol{A}]^{\boldsymbol{x}} \\ \vdots\ \boldsymbol{u} \\ \boldsymbol{B} \end{matrix}}{\boldsymbol{A} \to \boldsymbol{B}} \longrightarrow\mathbf{I}^{\boldsymbol{x}} \right)^{\circ} \equiv \dfrac{\begin{matrix} [x^{\boldsymbol{A}^{\circ}}] \\ \vdots \\ \boldsymbol{u}^{\circ\,\boldsymbol{B}^{\circ}} \end{matrix}}{(\lambda x^{\boldsymbol{A}^{\circ}}\boldsymbol{.}\,\boldsymbol{u}^{\circ})^{\boldsymbol{A}^{\circ}\to\boldsymbol{B}^{\circ}}} \longrightarrow\mathrm{I}^{x}$$

$$\left(\dfrac{\begin{matrix} \vdots\ \boldsymbol{s} \\ \boldsymbol{A} \to \boldsymbol{B} \end{matrix} \qquad \begin{matrix} \vdots\ \boldsymbol{t} \\ \boldsymbol{A} \end{matrix}}{\boldsymbol{B}} \longrightarrow\mathbf{E} \right)^{\circ} \equiv \dfrac{\begin{matrix} \vdots \\ \boldsymbol{s}^{\circ\,\boldsymbol{A}^{\circ}\to\boldsymbol{B}^{\circ}} \end{matrix} \qquad \begin{matrix} \vdots \\ \boldsymbol{t}^{\circ\,\boldsymbol{A}^{\circ}} \end{matrix}}{(\boldsymbol{s}^{\circ}\ \boldsymbol{t}^{\circ})^{\boldsymbol{B}^{\circ}}} \longrightarrow\mathrm{E}$$

Girard projection

$$\left(\dfrac{\begin{array}{c}\vdots\, \boldsymbol{u} \\ \boldsymbol{B}\end{array}}{\forall \boldsymbol{\mathcal{X}}^{C}.\, \boldsymbol{B}}\, \forall\mathbf{I} \right)^{\circ} \equiv \dfrac{\begin{array}{c}\vdots \\ \boldsymbol{u}^{\circ\, \boldsymbol{B}^{\circ}}\end{array}}{(\Lambda X.\, \boldsymbol{u}^{\circ})^{\forall X.\, \boldsymbol{B}^{\circ}}}\, \forall\mathrm{I}$$

$$\left(\dfrac{\begin{array}{c}\vdots\, \boldsymbol{s} \\ \forall \boldsymbol{\mathcal{X}}^{C}.\, \boldsymbol{B}\end{array}}{\boldsymbol{B}[\boldsymbol{\mathcal{A}}^{C}/\boldsymbol{\mathcal{X}}]}\, \forall\mathbf{E} \right)^{\circ} \equiv \dfrac{\begin{array}{c}\vdots \\ \boldsymbol{s}^{\circ\, \forall X.\, \boldsymbol{B}^{\circ}}\end{array}}{(\boldsymbol{s}^{\circ}\ \boldsymbol{\mathcal{A}}^{\circ})^{\boldsymbol{B}^{\circ}[\boldsymbol{\mathcal{A}}^{\circ}/X]}}\, \forall\mathrm{E}$$

Girard projection

$$\left(\begin{array}{c}\vdots\, \boldsymbol{u} \\ \boldsymbol{B} \\ \hline \forall x^C .\, \boldsymbol{B}\end{array}\ \forall^1\mathrm{I}\right)^{\circ} \equiv \begin{array}{c}\vdots \\ \boldsymbol{u}^{\circ}\, \boldsymbol{B}^{\circ}\end{array} \qquad \left(\begin{array}{c}\vdots\, \boldsymbol{s} \\ \forall x^C .\, \boldsymbol{B} \\ \hline \boldsymbol{B}[t^C/x]\end{array}\ \forall^1\mathrm{E}\right)^{\circ} \equiv \begin{array}{c}\vdots \\ \boldsymbol{s}^{\circ}\, \boldsymbol{B}^{\circ}\end{array}$$

$$\left(\begin{array}{c}\vdots\, \boldsymbol{u} \\ \boldsymbol{B} \\ \hline \forall X .\, \boldsymbol{B}\end{array}\ \forall^2\mathrm{I}\right)^{\circ} \equiv \begin{array}{c}\vdots \\ \boldsymbol{u}^{\circ}\, \boldsymbol{B}^{\circ}\end{array} \qquad \left(\begin{array}{c}\vdots\, \boldsymbol{s} \\ \forall X .\, \boldsymbol{B} \\ \hline \boldsymbol{B}[A/X]\end{array}\ \forall^2\mathrm{E}\right)^{\circ} \equiv \begin{array}{c}\vdots \\ \boldsymbol{s}^{\circ}\, \boldsymbol{B}^{\circ}\end{array}$$

$$\left(\begin{array}{c}\vdots\, \boldsymbol{t} \\ \boldsymbol{A} \\ \hline \boldsymbol{B}\end{array}\ \beta\right)^{\circ} \equiv \begin{array}{c}\vdots \\ \boldsymbol{t}^{\circ}\, \boldsymbol{A}^{\circ}\end{array}$$

Part VII

Reynolds embedding

Reynolds embedding

Types

$$
\begin{array}{lcl}
(X)^* & \equiv & \boldsymbol{\mathcal{X}}^X \\
(A \to B)^* & \equiv & \{z^{A \to B} \mid \forall x^A.\, x \in A^* \longrightarrow z\, x \in B^*\} \\
(\forall X.\, B)^* & \equiv & \{z^{\forall X.\, B} \mid \forall X.\, \forall \boldsymbol{\mathcal{X}}^X \boldsymbol{.}\, z\, X \in B^*\}
\end{array}
$$

Reynolds embedding

$$\left(\dfrac{\begin{matrix}[x^A]\\ \vdots \\ u^B\end{matrix}}{(\lambda x^A.\, u)^{A\to B}}\to\mathrm{I}^x\right)^* \equiv \dfrac{\dfrac{\dfrac{\begin{matrix}[x\in A^*]^{\boldsymbol{x}}\\ \vdots\; u^*\\ u\in B^*\end{matrix}}{(\lambda x^A.\,u)\,x\in B^*}\,\beta}{x\in A^*\to(\lambda x^A.\,u)\,x\in B^*}\to\mathbf{I}^{\boldsymbol{x}}}{\forall x^A.\, x\in A^*\to(\lambda x^A.\,u)\,x\in B^*}\,\forall^1\mathrm{I}$$

$$\left(\dfrac{\begin{matrix}\vdots\\ s^{A\to B}\end{matrix}\qquad\begin{matrix}\vdots\\ t^A\end{matrix}}{(s\,t)^B}\to\mathbf{E}\right)^*\equiv \dfrac{\dfrac{\begin{matrix}\vdots\; s^*\\ \forall x^A.\,x\in A^*\to s\,x\in B^*\end{matrix}}{t\in A^*\to s\,t\in B^*}\,\forall^1\mathrm{E}\qquad\begin{matrix}\vdots\; t^*\\ t\in A^*\end{matrix}}{s\,t\in B^*}\to\mathbf{E}$$

Reynolds embedding

$$\left(\dfrac{\begin{array}{c}\vdots\\ u^{B}\end{array}}{(\Lambda X.\,u)^{\forall X.\,B}}\;\forall\mathrm{I}\right)^{*} \equiv \dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\; u^{*}\\ u \in B^{*}\end{array}}{(\Lambda X.\,u)\;X \in B^{*}}\;\beta}{\forall \boldsymbol{\mathcal{X}}^{X}\boldsymbol{.}\,(\Lambda X.\,u)\;X \in B^{*}}\;\forall\mathbf{I}}{\forall X.\,\forall \boldsymbol{\mathcal{X}}^{X}\boldsymbol{.}\,(\Lambda X.\,u)\;X \in B^{*}}\;\forall^{2}\mathrm{I}$$

$$\left(\dfrac{\begin{array}{c}\vdots\\ s^{\forall X.\,B}\end{array}}{(s\;A)^{B[A/X]}}\;\forall\mathrm{E}\right)^{*} \equiv \dfrac{\dfrac{\begin{array}{c}\vdots\; s^{*}\\ \forall X.\,\forall \boldsymbol{\mathcal{X}}^{X}\boldsymbol{.}\,s\;X \in B^{*}\end{array}}{\forall \boldsymbol{\mathcal{X}}^{A}\boldsymbol{.}\,s\;A \in B^{*}[A/X]}\;\forall^{2}\mathrm{E}}{s\;A \in B^{*}[A/X,\,A^{*}/\boldsymbol{\mathcal{X}}]}\;\forall\mathbf{E}$$

Part VIII

Doubling

Doubling

Propositions

$$
\begin{aligned}
(t^C \in \boldsymbol{\mathcal{A}}^C)^\ddagger &\equiv (t^C, t'^{C'}) \in \boldsymbol{\mathcal{A}}^{\ddagger C \times C'} \\
(\boldsymbol{A} \longrightarrow \boldsymbol{B})^\ddagger &\equiv \boldsymbol{A}^\ddagger \longrightarrow \boldsymbol{B}^\ddagger \\
(\forall \boldsymbol{\mathcal{X}}^C .\, \boldsymbol{B})^\ddagger &\equiv \forall \boldsymbol{\mathcal{X}}^{C \times C'} .\, \boldsymbol{B}^\ddagger \\
(\forall x^C .\, \boldsymbol{B})^\ddagger &\equiv \forall x^C, x'^{C'} .\, \boldsymbol{B}^\ddagger \\
(\forall X .\, \boldsymbol{B})^\ddagger &\equiv \forall X, X' .\, \boldsymbol{B}^\ddagger
\end{aligned}
$$

Predicates

$$
\begin{aligned}
(\boldsymbol{\mathcal{X}}^C)^\ddagger &\equiv \boldsymbol{\mathcal{X}}^{C \times C'} \\
(\{x^C \mid \boldsymbol{A}\})^\ddagger &\equiv \{(x^C, x'^{C'}) \mid \boldsymbol{A}^\ddagger\}
\end{aligned}
$$

Doubling

$$\left(\dfrac{\begin{array}{c}[A]^{x}\\ \vdots\; u\\ B\end{array}}{A \to B}\,{\to}\mathbf{I}^{x}\right)^{\ddagger} \equiv \dfrac{\begin{array}{c}[A^{\ddagger}]^{x}\\ \vdots\; u^{\ddagger}\\ B^{\ddagger}\end{array}}{A^{\ddagger} \to B^{\ddagger}}\,{\to}\mathbf{I}^{x}$$

$$\left(\dfrac{\begin{array}{c}\vdots\; s\\ A \to B\end{array} \qquad \begin{array}{c}\vdots\; t\\ A\end{array}}{B}\,{\to}\mathbf{E}\right)^{\ddagger} \equiv \dfrac{\begin{array}{c}\vdots\; s^{\ddagger}\\ A^{\ddagger} \to B^{\ddagger}\end{array} \qquad \begin{array}{c}\vdots\; t^{\ddagger}\\ A^{\ddagger}\end{array}}{B^{\ddagger}}\,{\to}\mathbf{E}$$

Doubling

$$\left(\dfrac{\begin{array}{c}\vdots\; u\\ B\end{array}}{\forall \mathcal{X}^{C}.\, B}\;\forall\mathbf{I}\right)^{\ddagger} \equiv \dfrac{\begin{array}{c}\vdots\; u^{\ddagger}\\ B^{\ddagger}\end{array}}{\forall \mathcal{X}^{C\times C'}.\, B^{\ddagger}}\;\forall\mathbf{I}$$

$$\left(\dfrac{\begin{array}{c}\vdots\; s\\ \forall \mathcal{X}^{C}.\, B\end{array}}{B[\mathcal{A}^{C}/\mathcal{X}]}\;\forall\mathbf{E}\right)^{\ddagger} \equiv \dfrac{\begin{array}{c}\vdots\; s^{\ddagger}\\ \forall \mathcal{X}^{C\times C'}.\, B^{\ddagger}\end{array}}{B^{\ddagger}[\mathcal{A}^{\ddagger\, C\times C'}/\mathcal{X}]}\;\forall\mathbf{E}$$

Doubling

$$\left(\frac{\begin{array}{c} \vdots\ \boldsymbol{u} \\ \boldsymbol{B} \end{array}}{\forall x^{C}.\, \boldsymbol{B}}\ \forall^1\mathrm{I} \right)^{\ddagger} \equiv \frac{\begin{array}{c} \vdots\ \boldsymbol{u}^{\ddagger} \\ \boldsymbol{B}^{\ddagger} \end{array}}{\forall x^{C}, x'^{C'}.\, \boldsymbol{B}^{\ddagger}}\ \forall^1\mathrm{I}\ \text{twice}$$

$$\left(\frac{\begin{array}{c} \vdots\ \boldsymbol{s} \\ \forall x^{C}.\, \boldsymbol{B} \end{array}}{\boldsymbol{B}[t^{C}/x]}\ \forall^1\mathrm{E} \right)^{\ddagger} \equiv \frac{\begin{array}{c} \vdots\ \boldsymbol{s}^{\ddagger} \\ \forall x^{C}, x'^{C'}.\, \boldsymbol{B}^{\ddagger} \end{array}}{\boldsymbol{B}^{\ddagger}[t^{C}/x, t'^{C'}/x']}\ \forall^1\mathrm{E}\ \text{twice}$$

Doubling

$$\left(\begin{array}{c} \vdots\ \boldsymbol{u} \\ \boldsymbol{B} \\ \hline \forall X.\,\boldsymbol{B} \end{array}\ \forall^2\mathrm{I}\right)^{\ddagger} \equiv \begin{array}{c} \vdots\ \boldsymbol{u}^{\ddagger} \\ \boldsymbol{B}^{\ddagger} \\ \hline \forall X, X'.\,\boldsymbol{B}^{\ddagger} \end{array}\ \forall^2\mathrm{I}\text{ twice}$$

$$\left(\begin{array}{c} \vdots\ \boldsymbol{s} \\ \forall X.\,\boldsymbol{B} \\ \hline \boldsymbol{B}[A/X] \end{array}\ \forall^2\mathrm{E}\right)^{\ddagger} \equiv \begin{array}{c} \vdots\ \boldsymbol{s}^{\ddagger} \\ \forall X, X'.\,\boldsymbol{B}^{\ddagger} \\ \hline \boldsymbol{B}^{\ddagger}[A/X, A'/X'] \end{array}\ \forall^2\mathrm{E}\text{ twice}$$

Doubling

$$\left(\dfrac{\begin{array}{c} \vdots\, \boldsymbol{t} \\ \boldsymbol{A} \end{array}}{\boldsymbol{B}}\,\beta \right)^{\ddagger} \equiv \dfrac{\begin{array}{c} \vdots\, \boldsymbol{t}^{\ddagger} \\ \boldsymbol{A}^{\ddagger} \end{array}}{\boldsymbol{B}^{\ddagger}}\,\beta \text{ twice}$$