CSC_51051_EP: First-order logic

Samuel Mimram

2024

École polytechnique

Part I

First-order logic

First-order logic

Recall that in the first part of the course we have defined a natural deduction calculus for propositional logic.

We are ultimately going to extend this calculus for dependent types
(the core of Agda).

For now, we begin by looking at first order logic
(which should be familiar from INF412).

This is a first kind of dependency where types can depend on terms.

First order logic

There are two syntactic classes in first-order logic:

- **terms** construct elements of the model,
- **formulas** express logical properties,

and **predicate** allow constructing formulas form terms.

For instance, we can express associativity of a multiplication (e.g. in a group) with

$$\underbrace{\forall x.\forall y.\forall z.\quad \underbrace{(x \times y) \times z}_{\text{term}} \underbrace{=}_{\text{pred.}} \underbrace{x \times (y \times z)}_{\text{term}}}_{\text{formula}}$$

Signatures and terms

A **signature** Σ is a set of *function symbols* together with an *arity* for each symbol.

For instance, the signature for groups is

Signatures and terms

A **signature** Σ is a set of *function symbols* together with an *arity* for each symbol.

For instance, the signature for groups is

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

Signatures and terms

A **signature** Σ is a set of *function symbols* together with an *arity* for each symbol.

For instance, the signature for groups is

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

We write $\mathcal{T}_\Sigma$ for the **terms** generated by the signature, e.g.

$$m(m(e, x), m(x, i(y)))$$

which is what we would usually write

$$(1 \times x) \times (x \times y^{-1})$$

Terms

We suppose fixed an infinite countable set of variables:

$$\mathcal{X} \quad = \quad \{x, y, z, \ldots\}$$

The set $\mathcal{T}_\Sigma$ of **terms** over Σ is the smallest set such that

- every variable is a term:

$$\mathcal{X} \subseteq \mathcal{T}_\Sigma$$

- terms are closed under the operations:
  if $f \in \Sigma$ is a function symbol of arity n and $t_1, \ldots, t_n$ are terms then

$$f(t_1, \ldots, t_n)$$

  is also a term (this is a *formal* application).

Terms

We suppose fixed an infinite countable set of variables:

$$\mathcal{X} \quad = \quad \{x, y, z, \ldots\}$$

The set $\mathcal{T}_\Sigma$ of **terms** over Σ is the smallest set such that

- every variable is a term:

$$\mathcal{X} \subseteq \mathcal{T}_\Sigma$$

- terms are closed under the operations:
  if $f \in \Sigma$ is a function symbol of arity n and $t_1, \ldots, t_n$ are terms then

$$f(t_1, \ldots, t_n)$$

  is also a term (this is a *formal* application).

In short, terms are generated by the grammar: $t ::= x \mid f(t_1, \ldots, t_n)$

Terms

The "λ-terms" are the terms over the signature

Terms

The "λ-terms" are the terms over the signature

$$\Sigma \quad = \quad \{\mathsf{app} : 2, \lambda_x : 1 \mid x \in \mathit{Var}\}$$

Terms

The "λ-terms" are the terms over the signature

$$\Sigma \quad = \quad \{\mathsf{app} : 2, \lambda_x : 1 \mid x \in \mathit{Var}\}$$

For instance,

$$\lambda_x(\mathsf{app}(x, \lambda_y(y)))$$

which is simply another notation for

$$\lambda x.x(\lambda y.y)$$

Terms

The "λ-terms" are the terms over the signature

$$\Sigma \quad = \quad \{\mathsf{app} : 2, \lambda_x : 1 \mid x \in \mathit{Var}\}$$

not really: we don't take α-conversion in account.

For instance,

$$\lambda_x(\mathsf{app}(x, \lambda_y(y)))$$

which is simply another notation for

$$\lambda x.x(\lambda y.y)$$

Free variables

We write $\mathrm{FV}(t)$ for the set of **variables** occurring in a term (no variable is bound).

For instance,

$$\mathrm{FV}(m(m(e, x), m(x, i(y)))) =$$

Free variables

We write $\mathrm{FV}(t)$ for the set of **variables** occurring in a term (no variable is bound).

For instance,

$$\mathrm{FV}(m(m(e,x),m(x,i(y)))) = \{x,y\}$$

Free variables

We write $\mathrm{FV}(t)$ for the set of **variables** occurring in a term (no variable is bound).

For instance,

$$\mathrm{FV}(m(m(e,x),m(x,i(y)))) = \{x,y\}$$

Formally, this is defined by induction by

$$\mathrm{FV}(x) =$$

$$\mathrm{FV}(f(t_1,\ldots,t_n)) =$$

Free variables

We write $\mathrm{FV}(t)$ for the set of **variables** occurring in a term (no variable is bound).

For instance,

$$\mathrm{FV}(m(m(e,x),m(x,i(y)))) = \{x,y\}$$

Formally, this is defined by induction by

$$\mathrm{FV}(x) = \{x\}$$

$$\mathrm{FV}(f(t_1,\ldots,t_n)) =$$

Free variables

We write $\mathrm{FV}(t)$ for the set of **variables** occurring in a term (no variable is bound).

For instance,

$$\mathrm{FV}(m(m(e,x),m(x,i(y)))) = \{x,y\}$$

Formally, this is defined by induction by

$$\mathrm{FV}(x) = \{x\}$$

$$\mathrm{FV}(f(t_1,\ldots,t_n)) = \bigcup_{i=1}^{n} \mathrm{FV}(t_i)$$

Free variables

We write $\mathrm{FV}(t)$ for the set of **variables** occurring in a term (no variable is bound).

For instance,

$$\mathrm{FV}(m(m(e,x),m(x,i(y)))) = \{x,y\}$$

Formally, this is defined by induction by

$$\mathrm{FV}(x) = \{x\}$$

$$\mathrm{FV}(f(t_1,\ldots,t_n)) = \bigcup_{i=1}^{n} \mathrm{FV}(t_i)$$

A term t is **closed** when $\mathrm{FV}(t) = \emptyset$.

Terms

For instance, natural numbers can be defined as the set of closed terms over

$$\Sigma \quad = \quad \{Z : 0, S : 1\}$$

Namely, the closed terms are

$$Z() \qquad S(Z()) \qquad S(S(Z()) \qquad \ldots$$

(a non-closed term is $S(S(x))$)

Formulas

We suppose fixed set $\mathcal{P}$ of **predicates** together with an arity.

For instance,

$$\mathcal{P} \quad = \quad \{= : 2, \mathsf{even} : 1, \ldots\}$$

Formulas

We suppose fixed set $\mathcal{P}$ of **predicates** together with an arity.

For instance,

$$\mathcal{P} \quad = \quad \{= : 2, \mathsf{even} : 1, \ldots\}$$

The set of **formulas** (or *propositions*) is generated by

$$A ::= P(t_1, \ldots, t_n) \mid A \Rightarrow B \mid A \wedge B \mid \top \mid A \vee B \mid \bot \mid \neg A \mid \exists x.A \mid \forall x.A$$

where P is a predicate of arity n, the t_i are terms and $x \in \mathcal{X}$ is a variable.

Formulas

For instance, in the signature of groups

$$\Sigma = \{m : 2, e : 0, i : 1\} \qquad \mathcal{P} = \{= : 2, \ldots\}$$

we have the formula

$$\forall x.\forall y.\forall z. \quad m(m(x,y),z) = m(x,m(y,z)) \wedge m(e,x) = x \wedge m(x,e) = x$$

Formulas

With

$$\mathcal{P} = \{D : 1, \ldots\}$$

the **drinker formula** is

$$\exists x.(D(x) \Rightarrow \forall y.D(y))$$

α-equivalence

In a formula of the form $\exists x.A$ or $\forall x.A$, the variable x is **bound** in A (a variable which is not bound is **free**).

As usual, we consider formulas up to renaming of bound variables.

α-equivalence

In a formula of the form $\exists x.A$ or $\forall x.A$, the variable x is **bound** in A
(a variable which is not bound is **free**).

As usual, we consider formulas up to renaming of bound variables.

Formally, we define set $\mathrm{FV}(A)$ of **free variables** of A by

$$\mathrm{FV}(P(t_1, \ldots, t_n)) = \mathrm{FV}(t_1) \cup \ldots \cup \mathrm{FV}(t_n)$$
$$\mathrm{FV}(A \Rightarrow B) = \mathrm{FV}(A \times B) = \mathrm{FV}(A + B) = \mathrm{FV}(A) \cup \mathrm{FV}(B)$$
$$\mathrm{FV}(\top) = \mathrm{FV}(\bot) = \emptyset$$
$$\mathrm{FV}(\neg A) = \mathrm{FV}(A)$$
$$\mathrm{FV}(\forall x.A) = \mathrm{FV}(\exists x.A) = \mathrm{FV}(A) \setminus \{x\}$$

Substitution

Given a formula A, a term t and a variable x, we write

$$A[t/x]$$

for the formula A where all the free occurrences of x have been substituted by t

$$A \quad = \quad (\exists y.x + x = y) \vee (\exists x.x = y)$$

Substitution

Given a formula A, a term t and a variable x, we write

$$A[t/x]$$

for the formula A where all the free occurrences of x have been substituted by t

$$\begin{aligned} A &= (\exists y.x + x = y) \vee (\exists x.x = y) \\ A[z + z/x] &= \end{aligned}$$

Substitution

Given a formula A, a term t and a variable x, we write

$$A[t/x]$$

for the formula A where all the free occurrences of x have been substituted by t

$$\begin{array}{rcl} A & = & (\exists y.x + x = y) \vee (\exists x.x = y) \\ A[z + z/x] & = & (\exists y.(z + z) + (z + z) = y) \vee (\exists x.x = y) \end{array}$$

Substitution

Given a formula A, a term t and a variable x, we write

$$A[t/x]$$

for the formula A where all the free occurrences of x have been substituted by t

$$\begin{aligned} A &= (\exists y.x + x = y) \vee (\exists x.x = y) \\ A[z + z/x] &= (\exists y.(z + z) + (z + z) = y) \vee (\exists x.x = y) \\ A[y + y/x] &= \end{aligned}$$

Substitution

Given a formula A, a term t and a variable x, we write

$$A[t/x]$$

for the formula A where all the free occurrences of x have been substituted by t

$$\begin{array}{rcl} A & = & (\exists y.x + x = y) \vee (\exists x.x = y) \\ A[z + z/x] & = & (\exists y.(z + z) + (z + z) = y) \vee (\exists x.x = y) \\ A[y + y/x] & = & (\exists z.(y + y) + (y + y) = z) \vee (\exists x.x = y) \end{array}$$

Substitution

Given a formula A, a term t and a variable x, we write

$$A[t/x]$$

for the formula A where all the free occurrences of x have been substituted by t

$$\begin{array}{rcl} A & = & (\exists y.x + x = y) \vee (\exists x.x = y) \\ A[z + z/x] & = & (\exists y.(z + z) + (z + z) = y) \vee (\exists x.x = y) \\ A[y + y/x] & = & (\exists z.(y + y) + (y + y) = z) \vee (\exists x.x = y) \\ A[y + y/x] & \neq & (\exists y.(y + y) + (y + y) = y) \vee (\exists x.x = y) \end{array}$$

As usual, we might have to rename variables to avoid captures!

Rules

The rules of (intuitionistic) logic are the usual ones:

$$\frac{}{\Gamma, A, \Gamma' \vdash A}(\mathsf{ax})$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}(\Rightarrow_{\mathsf{E}}) \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}(\Rightarrow_{\mathsf{I}})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}(\wedge^{\mathsf{l}}_{\mathsf{E}}) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}(\wedge^{\mathsf{r}}_{\mathsf{E}}) \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}(\wedge_{\mathsf{I}})$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}(\vee_{\mathsf{E}}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}(\vee^{\mathsf{l}}_{\mathsf{I}}) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}(\vee^{\mathsf{r}}_{\mathsf{I}})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}(\bot_{\mathsf{E}}) \qquad \frac{}{\Gamma \vdash \top}(\top_{\mathsf{I}})$$

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}(\neg_{\mathsf{E}}) \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}(\neg_{\mathsf{I}})$$

Rules

Together with four new rules:

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_{\mathsf{I}})$$

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}(\exists_{\mathsf{E}}) \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}(\exists_{\mathsf{I}})$$

These rules are subject to the following (important!) side conditions:

- in $(\forall_{\mathsf{I}})$, we suppose $x \notin \mathsf{FV}(\Gamma)$,
- in $(\exists_{\mathsf{E}})$, we suppose $x \notin \mathsf{FV}(\Gamma) \cup \mathsf{FV}(B)$.

Rules

For instance,

$$\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)$$

Rules

For instance,

$$\frac{\forall x.\neg A \vdash \neg(\exists x.A)}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)} \; (\Rightarrow_{\mathrm{I}})$$

Rules

For instance,

$$\dfrac{\dfrac{\forall x.\neg A, \exists x.A \vdash \bot}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_{\mathrm{I}})}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\mathrm{I}})$$

Rules

For instance,

$$\dfrac{\dfrac{\dfrac{\forall x.\neg A, \exists x.A \vdash \exists x.A \qquad \forall x.\neg A, \exists x.A, A \vdash \bot}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_E)}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_I)}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_I)$$

Rules

For instance,

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A \vdash \exists x.A}\,(\mathsf{ax}) \qquad \forall x.\neg A, \exists x.A, A \vdash \bot}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_{\mathsf{E}})}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_{\mathsf{I}})}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\mathsf{I}})$$

Rules

For instance,

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A \vdash \exists x.A}\,(\mathrm{ax}) \qquad \dfrac{}{\forall x.\neg A, \exists x.A, A \vdash \neg A}\qquad \dfrac{}{\forall x.\neg A, \exists x.A, A \vdash A}}{\forall x.\neg A, \exists x.A, A \vdash \bot}\,(\neg_{\mathsf{E}})}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_{\mathsf{E}})}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_{\mathsf{I}})}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\mathsf{I}})$$

Rules

For instance,

$$\dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A \vdash \exists x.A}\,(\mathrm{ax}) \qquad \dfrac{\dfrac{\forall x.\neg A, \exists x.A, A \vdash \forall x.\neg A}{\forall x.\neg A, \exists x.A, A \vdash \neg A}\,(\forall_E) \qquad \forall x.\neg A, \exists x.A, A \vdash A}{\forall x.\neg A, \exists x.A, A \vdash \bot}\,(\neg_E)}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_E)}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_I)}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_I)$$

Rules

For instance,

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A \vdash \exists x.A}\,(\mathsf{ax})\qquad \dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A, A \vdash \forall x.\neg A}\,(\mathsf{ax})}{\forall x.\neg A, \exists x.A, A \vdash \neg A}\,(\forall_{\mathsf{E}})\qquad \forall x.\neg A, \exists x.A, A \vdash A}{\forall x.\neg A, \exists x.A, A \vdash \bot}\,(\neg_{\mathsf{E}})}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_{\mathsf{E}})}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_{\mathsf{I}})}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\mathsf{I}})$$

Rules

For instance,

$$\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A \vdash \exists x.A}\,(\mathrm{ax})}{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A, A \vdash \forall x.\neg A}\,(\mathrm{ax})}{\forall x.\neg A, \exists x.A, A \vdash \neg A}\,(\forall_{\mathsf{E}}) \qquad \dfrac{}{\forall x.\neg A, \exists x.A, A \vdash A}\,(\mathrm{ax})}{\forall x.\neg A, \exists x.A, A \vdash \bot}\,(\neg_{\mathsf{E}})}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_{\mathsf{E}})}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_{\mathsf{I}})}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\mathsf{I}})$$

Rules

The side conditions

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_{\mathsf{I}}) \qquad \text{with } x \notin \mathsf{FV}(\Gamma)$$

avoid clearly problematic proofs:

$$\vdash A(t) \Rightarrow \forall x.A(x)$$

Rules

The side conditions

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_{\mathsf{I}}) \qquad \text{with } x \notin \mathsf{FV}(\Gamma)$$

avoid clearly problematic proofs:

$$\frac{\vdash \forall x.(A(x) \Rightarrow \forall x.A(x))}{\vdash A(t) \Rightarrow \forall x.A(x)}\ (\forall_{\mathsf{E}})$$

Rules

The side conditions

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_{\mathsf{I}}) \qquad \text{with } x \notin \mathsf{FV}(\Gamma)$$

avoid clearly problematic proofs:

$$\dfrac{\dfrac{\vdash A(x) \Rightarrow \forall x.A(x)}{\vdash \forall x.(A(x) \Rightarrow \forall x.A(x))}\,(\forall_{\mathsf{I}})}{\vdash A(t) \Rightarrow \forall x.A(x)}\,(\forall_{\mathsf{E}})$$

Rules

The side conditions

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_{\mathsf{I}}) \qquad \text{with } x \notin \mathsf{FV}(\Gamma)$$

avoid clearly problematic proofs:

$$\dfrac{\dfrac{\dfrac{A(x) \vdash \forall x.A(x)}{\vdash A(x) \Rightarrow \forall x.A(x)}\,(\Rightarrow_{\mathsf{I}})}{\vdash \forall x.(A(x) \Rightarrow \forall x.A(x))}\,(\forall_{\mathsf{I}})}{\vdash A(t) \Rightarrow \forall x.A(x)}\,(\forall_{\mathsf{E}})$$

Rules

The side conditions

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_\mathsf{I}) \qquad \text{with } x \notin \mathsf{FV}(\Gamma)$$

avoid clearly problematic proofs:

$$\dfrac{\dfrac{\dfrac{\dfrac{A(x) \vdash A(x)}{A(x) \vdash \forall x.A(x)}(\forall_\mathsf{I})}{\vdash A(x) \Rightarrow \forall x.A(x)}(\Rightarrow_\mathsf{I})}{\vdash \forall x.(A(x) \Rightarrow \forall x.A(x))}(\forall_\mathsf{I})}{\vdash A(t) \Rightarrow \forall x.A(x)}(\forall_\mathsf{E})$$

We have $x \in \mathsf{FV}(A(x))$!

Rules

The side conditions

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}(\forall_{\mathsf{I}}) \qquad \text{with } x \notin \mathsf{FV}(\Gamma)$$

avoid clearly problematic proofs:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A(x) \vdash A(x)}\,(\mathsf{ax})}{A(x) \vdash \forall x.A(x)}\,(\forall_{\mathsf{I}})}{\vdash A(x) \Rightarrow \forall x.A(x)}\,(\Rightarrow_{\mathsf{I}})}{\vdash \forall x.(A(x) \Rightarrow \forall x.A(x))}\,(\forall_{\mathsf{I}})}{\vdash A(t) \Rightarrow \forall x.A(x)}\,(\forall_{\mathsf{E}})$$

We have $x \in \mathsf{FV}(A(x))$!

Rules

The rules are not completely satisfactory, for instance we can prove:

$$\dfrac{\dfrac{}{\vdash \top}\,(\top_{\mathrm{I}})}{\vdash \exists x.\top}\,(\exists_{\mathrm{I}})$$

(this can be fixed but we will simply ignore it)

Rules

The rules are not completely satisfactory, for instance we can prove:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.A \vdash \forall x.A}\,(\mathsf{ax})}{\forall x.A \vdash A}\,(\forall_{\mathsf{E}})}{\forall x.A \vdash \exists x.A}\,(\exists_{\mathsf{I}})}{\vdash (\forall x.A) \Rightarrow \exists x.A}\,(\Rightarrow_{\mathsf{I}})$$

(this can be fixed but we will simply ignore it)

Cut-elimination

As for predicate logic, when a proof contains cuts, we can eliminate those.

A cut means that

- you prove a general theorem,
- then you use it in a very particular case.

For instance,

- $\forall x.x \neq 0 \Rightarrow \exists y.(y + 1 = x)$,
- therefore $\exists y.(y + 1 = 5)$.

But we could have directly said $y = 4$ shows the result!

Cut-elimination

As for predicate logic, when a proof contains cuts, we can eliminate those.

A cut means that

- you use an introduction rule,
- followed by an elimination rule for the introduced connective.

Cut-elimination

We still have the cut elimination property: the two new cases are

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A[t/x]}}{\Gamma \vdash \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, A \vdash B}}{\Gamma \vdash B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow$$

Cut-elimination

We still have the cut elimination property: the two new cases are

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash \forall x.A}\,(\forall_{\mathsf{E}})}{\Gamma \vdash A[t/x]} \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash A[t/x]}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A[t/x]}\,(\exists_{\mathsf{I}})}{\Gamma \vdash \exists x.A} \qquad \dfrac{\pi'}{\Gamma, A \vdash B}}{\Gamma \vdash B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow$$

Cut-elimination

We still have the cut elimination property: the two new cases are

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash \forall x.A}\,(\forall_{\mathsf{E}})}{\Gamma \vdash A[t/x]} \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash A[t/x]}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A[t/x]}\,(\exists_{\mathsf{I}})}{\Gamma \vdash \exists x.A} \qquad \dfrac{\pi'}{\Gamma, A \vdash B}}{\Gamma \vdash B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash B}$$

Cut-elimination

Theorem
If $\Gamma \vdash A$ is provable then it admits a cut-free proof.

The witness property

As before, we have

Proposition
A cut-free intuitionistic proof of $\vdash A$ *necessarily ends with an introduction rule.*

The witness property

As before, we have

Proposition
A cut-free intuitionistic proof of $\vdash A$ *necessarily ends with an introduction rule.*

In particular,

Theorem (Coherence)
The logic is coherent.

Proof.

□

The witness property

As before, we have

Proposition
A cut-free intuitionistic proof of $\vdash A$ *necessarily ends with an introduction rule.*

In particular,

Theorem (Coherence)
The logic is coherent.

Proof.
If there was a proof of $\bot$, we would have a cut-free one, and thus one ending with an introduction rule, but there is no introduction rule for $\bot$. □

The witness property

As before, we have

Proposition
A cut-free intuitionistic proof of $\vdash A$ *necessarily ends with an introduction rule.*

In particular,

Theorem (Witness property)
If $\vdash \exists x.A$ *is provable intuitionistically then there exists* t *such that* $A[t/x]$ *is provable.*

Proof.

□

The witness property

As before, we have

Proposition
A cut-free intuitionistic proof of $\vdash A$ *necessarily ends with an introduction rule.*

In particular,

Theorem (Witness property)
If $\vdash \exists x.A$ *is provable intuitionistically then there exists* t *such that* $A[t/x]$ *is provable.*

Proof.

The proof can be supposed to be cut-free and then necessarily ends on $\dfrac{\vdash A[t/x]}{\vdash \exists x.A}\ (\exists_{\mathrm{I}})$.

□

Curry-Howard

We can easily extend the Curry-Howard correspondence to first-order logic.

The expressions e corresponding to programs are

$$e ::= \ldots$$

and typing rules are

$$\frac{\Gamma \vdash \quad A}{\Gamma \vdash \quad \forall x.A}(\forall_{\mathsf{I}}) \qquad \frac{\Gamma \vdash \quad A[t/x]}{\Gamma \vdash \quad \exists x.A}(\exists_{\mathsf{I}})$$

and

$$\frac{\Gamma \vdash \quad \forall x.A}{\Gamma \vdash \quad A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash \quad \exists x.A \qquad \Gamma, y : A \vdash \quad B}{\Gamma \vdash \quad B}(\exists_{\mathsf{E}})$$

Curry-Howard

We can easily extend the Curry-Howard correspondence to first-order logic.

The expressions e corresponding to programs are

$$e ::= \ldots$$

and typing rules are

$$\frac{\Gamma \vdash e : A}{\Gamma \vdash \qquad \forall x.A}(\forall_{\mathsf{I}}) \qquad \frac{\Gamma \vdash e : A[t/x]}{\Gamma \vdash \qquad \exists x.A}(\exists_{\mathsf{I}})$$

and

$$\frac{\Gamma \vdash e : \forall x.A}{\Gamma \vdash \qquad A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash e : \exists x.A \qquad \Gamma, y : A \vdash e' : B}{\Gamma \vdash \qquad\qquad B}(\exists_{\mathsf{E}})$$

Curry-Howard

We can easily extend the Curry-Howard correspondence to first-order logic.

The expressions e corresponding to programs are

$$e ::= \ldots \mid \lambda x.e$$

and typing rules are

$$\frac{\Gamma \vdash e : A}{\Gamma \vdash \lambda x.e : \forall x.A}(\forall_{\mathsf{I}}) \qquad \frac{\Gamma \vdash e : A[t/x]}{\Gamma \vdash \exists x.A}(\exists_{\mathsf{I}})$$

and

$$\frac{\Gamma \vdash e : \forall x.A}{\Gamma \vdash A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash e : \exists x.A \qquad \Gamma, y : A \vdash e' : B}{\Gamma \vdash B}(\exists_{\mathsf{E}})$$

Curry-Howard

We can easily extend the Curry-Howard correspondence to first-order logic.

The expressions e corresponding to programs are

$$e ::= \ldots \mid \lambda x.e \qquad \mid \langle t, e \rangle$$

and typing rules are

$$\frac{\Gamma \vdash e : A}{\Gamma \vdash \lambda x.e : \forall x.A}(\forall_{\mathsf{I}}) \qquad \frac{\Gamma \vdash e : A[t/x]}{\Gamma \vdash \langle t, e \rangle : \exists x.A}(\exists_{\mathsf{I}})$$

and

$$\frac{\Gamma \vdash e : \forall x.A}{\Gamma \vdash \qquad A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash e : \exists x.A \qquad \Gamma, y : A \vdash e' : B}{\Gamma \vdash \qquad\qquad\qquad B}(\exists_{\mathsf{E}})$$

Curry-Howard

We can easily extend the Curry-Howard correspondence to first-order logic.

The expressions e corresponding to programs are

$$e ::= \ldots \mid \lambda x.e \mid e\,t \mid \langle t, e \rangle$$

and typing rules are

$$\frac{\Gamma \vdash e : A}{\Gamma \vdash \lambda x.e : \forall x.A}(\forall_{\mathsf{I}}) \qquad \frac{\Gamma \vdash e : A[t/x]}{\Gamma \vdash \langle t, e \rangle : \exists x.A}(\exists_{\mathsf{I}})$$

and

$$\frac{\Gamma \vdash e : \forall x.A}{\Gamma \vdash e\,t : A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash e : \exists x.A \qquad \Gamma, y : A \vdash e' : B}{\Gamma \vdash \qquad\qquad B}(\exists_{\mathsf{E}})$$

Curry-Howard

We can easily extend the Curry-Howard correspondence to first-order logic.

The expressions e corresponding to programs are

$$e ::= \ldots \mid \lambda x.e \mid e\,t \mid \langle t, e\rangle \mid \mathtt{let}\,\langle x, y\rangle = e\,\mathtt{in}\,e'$$

and typing rules are

$$\frac{\Gamma \vdash e : A}{\Gamma \vdash \lambda x.e : \forall x.A}(\forall_{\mathsf{I}}) \qquad \frac{\Gamma \vdash e : A[t/x]}{\Gamma \vdash \langle t, e\rangle : \exists x.A}(\exists_{\mathsf{I}})$$

and

$$\frac{\Gamma \vdash e : \forall x.A}{\Gamma \vdash e\,t : A[t/x]}(\forall_{\mathsf{E}}) \qquad \frac{\Gamma \vdash e : \exists x.A \qquad \Gamma, y : A \vdash e' : B}{\Gamma \vdash \mathtt{let}\,\langle x, y\rangle = e\,\mathtt{in}\,e' : B}(\exists_{\mathsf{E}})$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash A[t/x]}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A}}{\Gamma \vdash \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash A[t/x]}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A}}{\Gamma \vdash \lambda x.e : \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash A[t/x]}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A}}{\Gamma \vdash \lambda x.e : \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash (\lambda x.e)t : A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash A[t/x]}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A}}{\Gamma \vdash \lambda x.e : \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash (\lambda x.e)t : A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash e[t/x] : A[t/x]}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A}}{\Gamma \vdash \lambda x.e : \forall x.A}\,(\forall_{\mathsf{I}})}{\Gamma \vdash (\lambda x.e)t : A[t/x]}\,(\forall_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[t/x]}{\Gamma \vdash e[t/x] : A[t/x]}$$

i.e.

$$(\lambda x.e)t \quad \longrightarrow_{\beta} \quad e[t/x]$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A[t/x]}}{\Gamma \vdash \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, y : A \vdash B}}{\Gamma \vdash B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash B}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A[t/x]}}{\Gamma \vdash \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, y : A \vdash e' : B}}{\Gamma \vdash B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash B}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A[t/x]}}{\Gamma \vdash \langle t, e\rangle : \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, y : A \vdash e' : B}}{\Gamma \vdash \qquad\qquad\qquad B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash \qquad\qquad B}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A[t/x]}}{\Gamma \vdash \langle t, e\rangle : \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, y : A \vdash e' : B}}{\Gamma \vdash \mathtt{let}\ \langle x, y\rangle = \langle t, e\rangle\ \mathtt{in}\ e' : B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash B}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A[t/x]}}{\Gamma \vdash \langle t, e\rangle : \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, y : A \vdash e' : B}}{\Gamma \vdash \mathtt{let}\ \langle x, y\rangle = \langle t, e\rangle\ \mathtt{in}\ e' : B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash e'[t/x, e/y] : B}$$

Curry-Howard

Reduction rules correspond to cut-elimination:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash e : A[t/x]}}{\Gamma \vdash \langle t, e\rangle : \exists x.A}\,(\exists_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma, y : A \vdash e' : B}}{\Gamma \vdash \mathtt{let}\ \langle x, y\rangle = \langle t, e\rangle\ \mathtt{in}\ e' : B}\,(\exists_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[t/x][\pi/A]}{\Gamma \vdash e'[t/x, e/y] : B}$$

i.e.

$$\mathtt{let}\ \langle x, y\rangle = \langle t, e\rangle\ \mathtt{in}\ e' \qquad \longrightarrow_{\beta} \qquad e'[t/x, e/y]$$

Curry-Howard

Note that there are two abstractions:

- $\lambda x^A.e : A \Rightarrow B$
- $\lambda x.e : \forall x.A$

Curry-Howard

Note that there are two abstractions:

- $\lambda x^A.e : A \Rightarrow B$
- $\lambda x.e : \forall x.A$

Similarly, there are two pairs:

- $\langle e, e' \rangle : A \wedge B$
- $\langle t, e \rangle : \exists x.A$

They behave similarly but they are not the same (we should write them differently).

They will become the same in dependent types!

Curry-Howard

For instance, recall our proof of $(\forall x.\neg A) \Rightarrow \neg(\exists x.A)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A \vdash \exists x.A}\,(\text{ax})}{\dfrac{\dfrac{}{\forall x.\neg A, \exists x.A, A \vdash \forall x.\neg A}\,(\text{ax})}{\forall x.\neg A, \exists x.A, A \vdash \neg A}\,(\forall_{\mathsf{E}})} \qquad \dfrac{}{\forall x.\neg A, \exists x.A, A \vdash A}\,(\text{ax})}{\forall x.\neg A, \exists x.A, A \vdash \bot}\,(\neg_{\mathsf{E}})}{\forall x.\neg A, \exists x.A \vdash \bot}\,(\exists_{\mathsf{E}})}{\forall x.\neg A \vdash \neg(\exists x.A)}\,(\neg_{\mathsf{I}})}{\vdash (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\mathsf{I}})$$

Curry-Howard

For instance, recall our proof of $(\forall x.\neg A) \Rightarrow \neg(\exists x.A)$:

$$\dfrac{\dfrac{}{f : \forall x.\neg A, e : \exists x.A \vdash e : \exists x.A}\,(\text{ax}) \qquad \dfrac{\dfrac{\dfrac{}{f : \forall x.\neg A, e : \exists x.A, a : A \vdash f : \forall x.\neg A}\,(\text{ax})}{f : \forall x.\neg A, e : \exists x.A, a : A \vdash f\ x : \neg A}\,(\forall_{\text{E}}) \qquad \dfrac{}{f : \forall x.\neg A, e : \exists x.A, a : A \vdash a : A}\,(\text{ax})}{f : \forall x.\neg A, e : \exists x.A, a : A \vdash f\ x\ a : \bot}\,(\neg_{\text{E}})}{f : \forall x.\neg A, e : \exists x.A \vdash \texttt{let}\ \langle x, a\rangle = e\ \texttt{in}\ f\ x\ a : \bot}\,(\exists_{\text{E}})$$

$$\dfrac{f : \forall x.\neg A, e : \exists x.A \vdash \texttt{let}\ \langle x, a\rangle = e\ \texttt{in}\ f\ x\ a : \bot}{f : \forall x.\neg A \vdash \lambda e.\texttt{let}\ \langle x, a\rangle = e\ \texttt{in}\ f\ x\ a : \neg(\exists x.A)}\,(\neg_{\text{I}})$$

$$\dfrac{f : \forall x.\neg A \vdash \lambda e.\texttt{let}\ \langle x, a\rangle = e\ \texttt{in}\ f\ x\ a : \neg(\exists x.A)}{\vdash \lambda f.\lambda e.\texttt{let}\ \langle x, a\rangle = e\ \texttt{in}\ f\ x\ a : (\forall x.\neg A) \Rightarrow \neg(\exists x.A)}\,(\Rightarrow_{\text{I}})$$

The corresponding term is

$$\lambda f.\lambda e.\texttt{let}\ \langle x, a\rangle = e\ \texttt{in}\ f\ x\ a \qquad : \qquad (\forall x.(A \Rightarrow \bot)) \Rightarrow (\exists x.A) \Rightarrow \bot$$

Classical first-order logic

As before, the rules we have presented implement **intuitionistic** first-order logic.

Classical first order logic can be obtained by adding the usual axioms, e.g.

$$\neg\neg A \Rightarrow A$$

Classical first-order logic

A typical formula which is only provable classically:

$$\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)$$

Classical first-order logic

A typical formula which is only provable classically:

$$\frac{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}\ (\Rightarrow_{\mathrm{I}})$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}\,(\neg\neg_{\mathsf{E}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}\,(\Rightarrow_{\mathsf{I}})$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}\,(\neg_{\mathrm{I}})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}\,(\neg\neg_{\mathrm{E}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}\,(\Rightarrow_{\mathrm{I}})$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\ldots \qquad \neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}(\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}(\neg\neg_{\mathsf{E}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}(\Rightarrow_{\mathsf{I}})$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \neg A(x_0)}\,(\forall_{\mathsf{I}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}\,(\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}\,(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}\,(\neg\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}\,(\Rightarrow_{\mathsf{I}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \bot}(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \neg A(x_0)}(\forall_{\mathsf{I}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}(\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}(\neg\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}(\Rightarrow_{\mathsf{I}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}$$

$\dots$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dots \quad \neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \exists x.A(x)}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \bot}(\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \neg A(x_0)}(\neg_{\mathsf{I}})}{\dots \quad \neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}(\forall_{\mathsf{I}})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}(\neg\neg_{\mathsf{E}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}(\Rightarrow_{\mathsf{I}})$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash A(x_0)}\,(\exists_{\mathsf{I}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \exists x.A(x)}\,(\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \bot}\,(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \neg A(x_0)}\,(\forall_{\mathsf{I}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}\,(\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}\,(\neg_{\mathsf{I}})}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}\,(\neg\neg_{\mathsf{E}})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}\,(\Rightarrow_{\mathsf{I}})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash A(x_0)}(\mathsf{ax})}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \exists x.A(x)}(\exists_\mathsf{I})}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \bot}(\neg_\mathsf{E})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \neg A(x_0)}(\neg_\mathsf{I})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}(\forall_\mathsf{I})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}(\neg_\mathsf{E})}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}(\neg_\mathsf{I})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}(\neg\neg_\mathsf{E})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}(\Rightarrow_\mathsf{I})$$

Classical first-order logic

A typical formula which is only provable classically:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash A(x_0)}(\mathsf{ax})}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \exists x.A(x)}(\exists_\mathsf{I})}{\neg\forall x.\neg A(x), \neg\exists x.A(x), A(x_0) \vdash \bot}(\neg_\mathsf{E})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \neg A(x_0)}(\neg_\mathsf{I})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \forall x.\neg A(x)}(\forall_\mathsf{I})}{\neg\forall x.\neg A(x), \neg\exists x.A(x) \vdash \bot}(\neg_\mathsf{E})}{\neg\forall x.\neg A(x) \vdash \neg\neg\exists x.A(x)}(\neg_\mathsf{I})}{\neg\forall x.\neg A(x) \vdash \exists x.A(x)}(\neg\neg_\mathsf{E})}{\vdash \neg(\forall x.\neg A(x)) \Rightarrow \exists x.A(x)}(\Rightarrow_\mathsf{I})$$

We see that we cannot expect the witness property in classical first-order logic!

The Drinker formula

Another one is the Drinker formula $A = \exists x.(D(x) \Rightarrow (\forall y.D(y)))$:

The Drinker formula

Another one is the Drinker formula $A = \exists x.(D(x) \Rightarrow (\forall y.D(y)))$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, \neg D(y) \vdash \neg D(y)}\,(\mathsf{ax}) \quad \dfrac{}{\ldots, D(y) \vdash D(y)}\,(\mathsf{ax})}{\neg A, D(x), \neg D(y), D(y) \vdash \bot}\,(\neg_{\mathsf{E}})}{\neg A, D(x), \neg D(y), D(y) \vdash \forall y.D(y)}\,(\bot_{\mathsf{E}})}{\neg A, D(x), \neg D(y) \vdash D(y) \Rightarrow (\forall y.D(y))}\,(\Rightarrow_{\mathsf{I}})}{\neg A, D(x), \neg D(y) \vdash \exists x.(D(x) \Rightarrow (\forall y.D(y)))}\,(\exists_{\mathsf{I}})}{\neg A, D(x), \neg D(y) \vdash \bot}\,(\neg_{\mathsf{E}})}{\neg A, D(x) \vdash \neg\neg D(y)}\,(\neg_{\mathsf{I}})}{\neg A, D(x) \vdash D(y)}\,(\neg\neg_{\mathsf{E}})}{\neg A, D(x) \vdash \forall y.D(y)}\,(\forall_{\mathsf{I}})}{\neg A \vdash D(x) \Rightarrow \forall y.D(y)}\,(\Rightarrow_{\mathsf{I}})}{\neg A \vdash \exists x.(D(x) \Rightarrow \forall y.D(y))}\,(\exists_{\mathsf{I}})}{\vdash A}\,(\mathsf{raa})$$

Part II

Theories

Theory

A **theory** consists of

- a signature Σ,
- a set $\mathcal{P}$ of predicates,
- a set $\mathcal{T}$ of axioms (formulas that are supposed to be true).

Groups

For instance, the theory of **groups** has

- signature

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

- predicates

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

- predicates

$$\mathcal{P} \quad = \quad \{= : 2\}$$

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

- predicates

$$\mathcal{P} \quad = \quad \{= : 2\}$$

- axioms:

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

- predicates

$$\mathcal{P} \quad = \quad \{= : 2\}$$

- axioms:

$$\forall x.\forall y.\forall z.m(m(x,y),z) = m(x,m(y,z))$$

$$\forall x.m(e,x) = x \qquad \forall x.m(x,e) = x$$

$$\forall x.m(i(x),x) = e \qquad \forall x.m(x,i(x)) = e$$

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

- predicates

$$\mathcal{P} \quad = \quad \{= : 2\}$$

- axioms:

$$\forall x.x = x$$

$$\forall x.\forall y.(x = y) \Rightarrow (y = x)$$

$$\forall x.\forall y.\forall z.(x = y) \Rightarrow (y = z) \Rightarrow (x = z)$$

Groups

For instance, the theory of **groups** has

- signature

$$\Sigma \quad = \quad \{m : 2, e : 0, i : 1\}$$

- predicates

$$\mathcal{P} \quad = \quad \{= : 2\}$$

- axioms:

$$\forall x.\forall x'.\forall y.\forall y'.(x = x') \Rightarrow (y = y') \Rightarrow (m(x, y) = m(x', y'))$$
$$\forall x.\forall x'.(x = x') \Rightarrow (i(x) = i(x'))$$

(we generally omit congruence axioms in the following)

Theory

A formula is provable in a theory $\mathcal{T}$ when it can be proved in using the rules of logic extended with one rule

$$\frac{}{\vdash A}\ (\text{axiom})$$

for each $A \in \mathcal{T}$.

Models

Let us quickly recall (see INF412) that a **model** of a theory consists of

- a set M,
- a function $[\![f]\!] : M^n \to M$ for every function symbol f of arity n,
- a relation $[\![P]\!] \subseteq M^n$ for every relation symbol R of arity n,

such that the interpretation of every axiom is true.

For instance, a model of a the theory of groups is... a group!

Correctness

The following (not very difficult) theorem ensures that our syntax is alright:

Theorem (Correctness)
If a formula can be derived in a theory then it is true in every model of the theory.

Correctness

In the theory of groups, one can show

$$\forall x.\forall y.(m(x,y) = e) \Rightarrow (y = i(x))$$

In traditional notation:

$$\begin{aligned} x \times y &= 1 \\ x^{-1} \times (x \times y) &= x^{-1} \times 1 \\ x^{-1} \times (x \times y) &= x^{-1} \\ (x^{-1} \times x) \times y &= x^{-1} \\ 1 \times y &= x^{-1} \\ y &= x^{-1} \end{aligned}$$

By correctness, it holds in every group!

Correctness

In the theory of groups, the following formula cannot be shown:

$$\forall x.\forall y.m(x,y) = m(y,x)$$

Correctness

In the theory of groups, the following formula cannot be shown:

$$\forall x.\forall y.m(x,y) = m(y,x)$$

Namely, any non-commutative group (look in a math book to have a concrete example) is a model of the theory and does not satisfy the above formula and we would have a contradiction by correctness.

Consistency

A theory is **consistent** if it does not allow to prove $\bot$.

Consistency

A theory is **consistent** if it does not allow to prove $\bot$.

Theorem
A theory with a model is consistent.

Proof.

Consistency

A theory is **consistent** if it does not allow to prove $\bot$.

Theorem
A theory with a model is consistent.

Proof.

Suppose that $\bot$ can be proved in the theory. By correctness, this means that $\bot$ is true in the model, but it is not by definition of a model, contradiction. $\square$

Presburger arithmetic

The **Presburger arithmetic** is the theory over

$$\Sigma = \{0 : 0, S : 1, + : 2\} \qquad \mathcal{P} = \{= : 2\}$$

with axioms

Presburger arithmetic

The **Presburger arithmetic** is the theory over

$$\Sigma = \{0 : 0, S : 1, + : 2\} \qquad \mathcal{P} = \{= : 2\}$$

with axioms

$$\forall x.0 = S(x) \Rightarrow \bot$$

$$\forall x.\forall y.S(x) = S(y) \Rightarrow x = y$$

$$\forall x.0 + x = x$$

$$\forall x.\forall y.S(x) + y = S(x + y)$$

together with, for every formula $A(x)$,

$$A(0) \Rightarrow (\forall x.A(x) \Rightarrow A(S(x))) \Rightarrow \forall x.A(x)$$

Presburger arithmetic

It is

- decidable
- coherent

and the expected formulas are derivable, e.g.

$$\forall x.x + 0 = x$$
$$\forall x.\forall y.\forall z.(x + y) + z = x + (y + z)$$
$$\forall x.\forall y.x + y = y + x$$

Presburger arithmetic

It is

- decidable (in $O(2^{2^{cn}})$)
- coherent

and the expected formulas are derivable, e.g.

$$\forall x.x + 0 = x$$
$$\forall x.\forall y.\forall z.(x + y) + z = x + (y + z)$$
$$\forall x.\forall y.x + y = y + x$$

Presburger arithmetic

It is

- decidable (in $O(2^{2^{cn}})$)
- coherent

and the expected formulas are derivable, e.g.

$$\forall x.x + 0 = x$$
$$\forall x.\forall y.\forall z.(x + y) + z = x + (y + z)$$
$$\forall x.\forall y.x + y = y + x$$

It admits $(\mathbb{N}, 0, \_+1, +)$ as a model but this is not the only model.

Presburger arithmetic

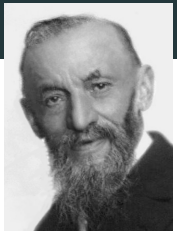
For instance, $\forall x.x + 0 = x$ can be proved by recurrence on x.

Consider the formula $A(x)$ being $x + 0 = x$. We have

- $A(0)$: $0 + 0 = 0$.
- Suppose $A(x)$, we have $A(S(x))$, namely

$$S(x) + 0 = S(x + 0) = S(x)$$

Peano arithmetic

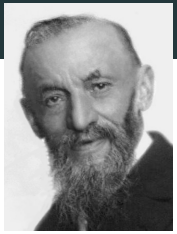


The **Peano arithmetic** is the theory over

$$\Sigma = \{0 : 0, S : 1, + : 2, \times : 2\} \qquad \mathcal{P} = \{= : 2\}$$

with the previous axioms together with

Peano arithmetic



The **Peano arithmetic** is the theory over

$$\Sigma = \{0 : 0, S : 1, + : 2, \times : 2\} \qquad \mathcal{P} = \{= : 2\}$$

with the previous axioms together with

$$\forall x.0 \times x = 0$$
$$\forall x.\forall y.S(x) \times y = y + (x \times y)$$

Peano arithmetic

It is

Peano arithmetic

It is

- undecidable (Hilbert problem #2),
- coherent.

Peano arithmetic

It is

- undecidable (Hilbert problem #2),
- coherent.

For coherence, we can use the fact that $(\mathbb{N}, 0, \_+1, +, \times)$ is a model and use correctness.

Peano arithmetic

It is

- undecidable (Hilbert problem #2),
- coherent.

For coherence, we can use the fact that $(\mathbb{N}, 0, \_+1, +, \times)$ is a model and use correctness.

This is however unsatisfactory because it lives in ZFC.

Peano arithmetic

It is

- undecidable (Hilbert problem #2),
- coherent.

For coherence, we can use the fact that $(\mathbb{N}, 0, \_+1, +, \times)$ is a model and use correctness.

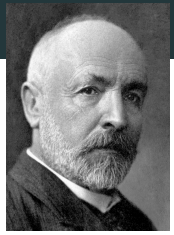
This is however unsatisfactory because it lives in ZFC.

Gentzen introduced cut-elimination in 1936 to show the consistency of PA.
This requires a transfinite induction up to the ordinal ε_0
($\varepsilon_0 = \omega^{\varepsilon_0}$, finite rooted non-planar trees).
By Gödel's second incompleteness theorem, we need more than usual recurrence!

Part III

Set theory

Set theory



An important first order theory is **set theory**, which axiomatizes sets.

This means that every term of the theory should be interpreted as a set.

It was initiated in 1870's by Cantor and Dedekind.

We will need a superficial understanding of it.

Naive set theory

We consider the signature

$$\Sigma = \qquad\qquad \mathcal{P} =$$

together with an axiom

Naive set theory

We consider the signature

$$\Sigma = \{\} \qquad \mathcal{P} = \{\in : 2\}$$

together with an axiom

Naive set theory

We consider the signature

$$\Sigma = \{\} \qquad \mathcal{P} = \{\in : 2\}$$

together with an axiom for every formula $A(x)$:

$$\exists y. \forall x. x \in y \Leftrightarrow A(x)$$

the **unrestricted comprehension scheme**, which states the existence of

$$y = \{x \mid A(x)\}$$

Naive set theory

From this, we can define all the usual operations. For instance,

- the empty set:

$$\emptyset =$$

- union of x and y:

$$x \cup y =$$

- ...

All good!

Naive set theory

From this, we can define all the usual operations. For instance,

- the empty set:

$$\emptyset = \{x \mid \bot\}$$

- union of x and y:

$$x \cup y =$$

- ...

All good!

Naive set theory

From this, we can define all the usual operations. For instance,

- the empty set:

$$\emptyset = \{x \mid \bot\}$$

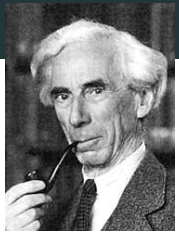
- union of x and y:

$$x \cup y = \{z \mid z \in x \vee z \in y\}$$

- ...

All good!

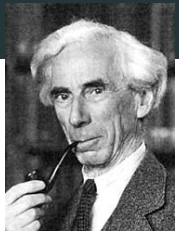
Naive set theory



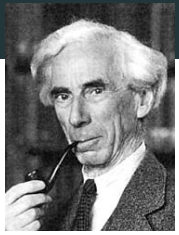
There is a “slight” problem:

Naive set theory

There is a "slight" problem: theory is inconsistent, Russell found a paradox in 1901.



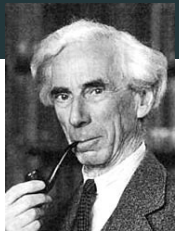
Naive set theory



There is a "slight" problem: theory is inconsistent, Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

Naive set theory

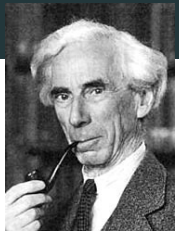


There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

There exists $y = \{x \mid A(x)\}$ such that $\forall x. x \in y \Leftrightarrow \neg(x \in x)$.

Naive set theory



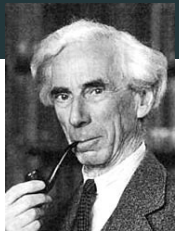
There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

There exists $y = \{x \mid A(x)\}$ such that $\forall x. x \in y \Leftrightarrow \neg(x \in x)$.

In particular, for x being y, we have $y \in y \Leftrightarrow \neg(y \in y)$.

Naive set theory



There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

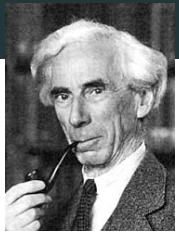
There exists $y = \{x \mid A(x)\}$ such that $\forall x. x \in y \Leftrightarrow \neg(x \in x)$.

In particular, for x being y, we have $y \in y \Leftrightarrow \neg(y \in y)$.

Therefore,

- if $y \in y$, we have $\neg(y \in y)$ and thus $\bot$,
- if $\neg(y \in y)$, we have $y \in y$ and thus $\bot$,

Naive set theory



There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

There exists $y = \{x \mid A(x)\}$ such that $\forall x. x \in y \Leftrightarrow \neg(x \in x)$.

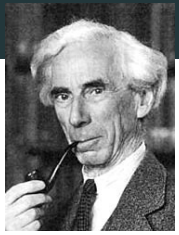
In particular, for x being y, we have $y \in y \Leftrightarrow \neg(y \in y)$.

Therefore,

- if $y \in y$, we have $\neg(y \in y)$ and thus $\bot$,
- if $\neg(y \in y)$, we have $y \in y$ and thus $\bot$,

Can we have an intuitionistic proof?

Naive set theory



There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

There exists $y = \{x \mid A(x)\}$ such that $\forall x. x \in y \Leftrightarrow \neg(x \in x)$.

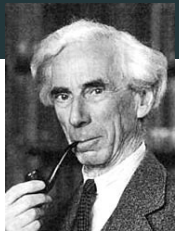
In particular, for x being y, we have $y \in y \Leftrightarrow \neg(y \in y)$.

Therefore,

- if $y \in y$, we have $\neg(y \in y)$ and thus $\bot$,
- if $\neg(y \in y)$, we have $y \in y$ and thus $\bot$,

Can we have an intuitionistic proof? This *is* an intuitionistic proof!

Naive set theory



There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

There exists $y = \{x \mid A(x)\}$ such that $\forall x.x \in y \Leftrightarrow \neg(x \in x)$.

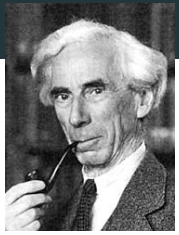
In particular, for x being y, we have $y \in y \Leftrightarrow \neg(y \in y)$.

Therefore,

- if $y \in y$, we have $\neg(y \in y)$ and thus $\bot$, i.e. we have $\neg(y \in y)$,
- if $\neg(y \in y)$, we have $y \in y$ and thus $\bot$,

Can we have an intuitionistic proof? This *is* an intuitionistic proof!

Naive set theory



There is a "slight" problem: theory is inconsistent,
Russell found a paradox in 1901.

Consider $A(x)$ being $\neg(x \in x)$.

There exists $y = \{x \mid A(x)\}$ such that $\forall x. x \in y \Leftrightarrow \neg(x \in x)$.

In particular, for x being y, we have $y \in y \Leftrightarrow \neg(y \in y)$.

Therefore,

- if $y \in y$, we have $\neg(y \in y)$ and thus $\bot$, i.e. we have $\neg(y \in y)$,
- if $\neg(y \in y)$, we have $y \in y$ and thus $\bot$, i.e. we have $\neg\neg(y \in y)$.

Can we have an intuitionistic proof? This *is* an intuitionistic proof!

The core of this proof consists in showing (see TD) that

$$(A \Leftrightarrow \neg A) \Rightarrow \bot$$

or equivalently

$$(A \Rightarrow \neg A) \Rightarrow (\neg A \Rightarrow A) \Rightarrow \bot$$

and conclude using $A = y \in y$.

Naive set theory

The core of this proof consists in showing (see TD) that

$$(A \Leftrightarrow \neg A) \Rightarrow \bot$$

or equivalently

$$(A \Rightarrow \neg A) \Rightarrow (\neg A \Rightarrow A) \Rightarrow \bot$$

and conclude using $A = y \in y$.

Interestingly, the corresponding λ-term is

$$\lambda f.\lambda g.f\,(g\,(\lambda a.f\ a\ a))\,(g\,(\lambda a.f\ a\ a))$$

The core of this proof consists in showing (see TD) that

$$(A \Leftrightarrow \neg A) \Rightarrow \bot$$

or equivalently

$$(A \Rightarrow \neg A) \Rightarrow (\neg A \Rightarrow A) \Rightarrow \bot$$

and conclude using $A = y \in y$.

Interestingly, the corresponding λ-term is

$$\lambda f.\lambda g.f(g(\lambda a.f\ a\ a))(g(\lambda a.f\ a\ a))$$

If we set f and g to be the identity, we recover the looping term

$$\Omega = (\lambda a.a\ a)(\lambda a.a\ a)$$

Recovering the fixpoint combinator

We can think of a set t as a predicate, i.e. $t(u)$ is true when $u \in t$.

Recovering the fixpoint combinator

We can think of a set t as a predicate, i.e. $t(u)$ is true when $u \in t$.

We are thus tempted to adopt the following notations:

instead of	we write
$u \in t$	
$\{x \mid t\}$	

Recovering the fixpoint combinator

We can think of a set t as a predicate, i.e. $t(u)$ is true when $u \in t$.

We are thus tempted to adopt the following notations:

instead of	we write
$u \in t$	$t\ u$
$\{x \mid t\}$	

Recovering the fixpoint combinator

We can think of a set t as a predicate, i.e. $t(u)$ is true when $u \in t$.

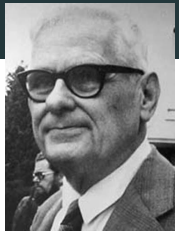
We are thus tempted to adopt the following notations:

instead of	we write
$u \in t$	$t\,u$
$\{x \mid t\}$	$\lambda x.t$

Namely,

$$u \in \{x \mid t(x)\} \quad \Leftrightarrow \quad (\lambda x.t)u \quad \Leftrightarrow \quad t(u)$$

Recovering the fixpoint combinator



We can think of a set t as a predicate, i.e. $t(u)$ is true when $u \in t$.

We are thus tempted to adopt the following notations:

instead of	we write
$u \in t$	$t\,u$
$\{x \mid t\}$	$\lambda x.t$

Namely,

$$u \in \{x \mid t(x)\} \quad \Leftrightarrow \quad (\lambda x.t)u \quad \Leftrightarrow \quad t(u)$$

This was in fact Church initial intuition behind λ-calculus!

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

$$r = \lambda x.\neg(xx)$$

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

$$r = \lambda x.\neg(xx)$$

The fact that $r \in r \Leftrightarrow \neg(r \in r)$ translates as

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

$$r = \lambda x.\neg(xx)$$

The fact that $r \in r \Leftrightarrow \neg(r \in r)$ translates as

$$rr =\!=_\beta \neg(rr)$$

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

$$r = \lambda x.\neg(xx)$$

The fact that $r \in r \Leftrightarrow \neg(r \in r)$ translates as

$$rr =\!=_\beta \neg(rr)$$

In other words rr is

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

$$r = \lambda x.\neg(xx)$$

The fact that $r \in r \Leftrightarrow \neg(r \in r)$ translates as

$$rr =\!=_\beta \neg(rr)$$

In other words rr is a fixpoint for $\neg$!

Recovering the fixpoint combinator

Russell's set $r = \{x \mid \neg(x \in x)\}$ can be written as

$$r = \lambda x.\neg(xx)$$

The fact that $r \in r \Leftrightarrow \neg(r \in r)$ translates as

$$rr =\!=_\beta \neg(rr)$$

In other words rr is a fixpoint for $\neg$!

Generalizing this to any f instead of $\neg$, we recover Church's fixpoint combinator:

$$r = \lambda x.f(xx) \qquad\qquad \mathsf{Y} = \lambda f.rr$$

ZF set theory

In order to avoid this paradox, Zermelo and Fraenkel proposed a new axiomatization of **set theory**, roughly between 1900 and 1925, which is now the "standard".

The idea in order to avoid paradoxes is

ZF set theory

In order to avoid this paradox, Zermelo and Fraenkel proposed a new axiomatization of **set theory**, roughly between 1900 and 1925, which is now the "standard".

The idea in order to avoid paradoxes is that some collections are "too big" to be sets. In particular,

there is no set of all sets.

ZF set theory

In order to avoid this paradox, Zermelo and Fraenkel proposed a new axiomatization of **set theory**, roughly between 1900 and 1925, which is now the "standard".

The idea in order to avoid paradoxes is that some collections are "too big" to be sets. In particular,

there is no set of all sets.

We now list the six axioms (some variants have different axioms, but are equivalent) on

$$\mathcal{P} = \{= : 2, \in : 2\}$$

Axiom of extensionality

Two sets with the same elements are equal:

$$\forall x.\forall y.((\forall z.z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$$

In usual notation,

$$x \subseteq y \wedge y \subseteq x \Rightarrow x = y$$

Axiom of union

The union of a family of sets exists:

$$\forall x.\exists y.\forall z.(z \in y \Leftrightarrow \exists t.(t \in x \wedge z \in t))$$

In usual notation, we can construct

$$y = \bigcup_{t \in x} t = \{z \mid z \in t, t \in x\}$$

Axiom of powerset

There is a set of subsets of a set:

$$\forall x.\exists y.\forall z.(z \in y \Leftrightarrow (\forall t.t \in z \Rightarrow t \in x))$$

In usual notation,

$$\forall x.\exists y.\forall z.(z \in y \Leftrightarrow z \subseteq x)$$

i.e. we can construct

$$y = \mathcal{P}(x) = \{z \mid z \subseteq x\}$$

Axiom schema of replacement

The image of a set under a partial function is a set:

$$(\forall x.\forall y.\forall y'.(A(x,y) \wedge A(x,y') \Rightarrow y = y')) \Rightarrow \forall t.\exists u.\forall y.(y \in u \Leftrightarrow \exists x.(x \in t \wedge A(x,y)))$$

This means that given a relation $A(x,y)$ encoding a partial function we can define the set u of images of t under the partial function:

$$u = \{y \mid \exists x \in t.A(x,y)\}$$

Axiom schema of replacement

The image of a set under a partial function is a set:

$$(\forall x.\forall y.\forall y'.(A(x,y) \wedge A(x,y') \Rightarrow y = y')) \Rightarrow \forall t.\exists u.\forall y.(y \in u \Leftrightarrow \exists x.(x \in t \wedge A(x,y)))$$

This means that given a relation $A(x,y)$ encoding a partial function we can define the set u of images of t under the partial function:

$$u = \{y \mid \exists x \in t.A(x,y)\}$$

For instance, we can define $\emptyset = \{y \mid \exists x \in t.\bot\}$.

Axiom schema of replacement

The image of a set under a partial function is a set:

$$(\forall x.\forall y.\forall y'.(A(x,y) \wedge A(x,y') \Rightarrow y = y')) \Rightarrow \forall t.\exists u.\forall y.(y \in u \Leftrightarrow \exists x.(x \in t \wedge A(x,y)))$$

This means that given a relation $A(x,y)$ encoding a partial function we can define the set u of images of t under the partial function:

$$u = \{y \mid \exists x \in t.A(x,y)\}$$

Given a unary predicate $B(x)$, we can define **restricted comprehension**:

$$\{x \in t \mid B(x)\} = \{y \mid \exists x \in t.\underbrace{y = x \wedge B(x)}_{A(x,y)}\}$$

Axiom schema of replacement

The image of a set under a partial function is a set:

$$(\forall x.\forall y.\forall y'.(A(x,y) \wedge A(x,y') \Rightarrow y = y')) \Rightarrow \forall t.\exists u.\forall y.(y \in u \Leftrightarrow \exists x.(x \in t \wedge A(x,y)))$$

This means that given a relation $A(x,y)$ encoding a partial function we can define the set u of images of t under the partial function:

$$u = \{y \mid \exists x \in t.A(x,y)\}$$

Given a unary predicate $B(x)$, we can define **restricted comprehension**:

$$\{x \in t \mid B(x)\} = \{y \mid \exists x \in t.\underbrace{y = x \wedge B(x)}_{A(x,y)}\}$$

but we cannot construct $\{x \mid \top\}$ or $\{x \mid \neg(x \in x)\}$.

Axiom schema of replacement

The image of a set under a partial function is a set:

$$(\forall x.\forall y.\forall y'.(A(x,y) \wedge A(x,y') \Rightarrow y = y')) \Rightarrow \forall t.\exists u.\forall y.(y \in u \Leftrightarrow \exists x.(x \in t \wedge A(x,y)))$$

This means that given a relation $A(x,y)$ encoding a partial function we can define the set u of images of t under the partial function:

$$u = \{y \mid \exists x \in t.A(x,y)\}$$

This is also why we restrict to *functional* relations:
otherwise, for a given x, $\{y \mid A(x,y)\}$ could be "too big" to be a set.

Axiom of infinity

There exists a set with infinitely many elements:

$$\exists x.\emptyset \in x \wedge \forall y.y \in x \Rightarrow S(y) \in x$$

with $S(y) = y \cup \{y\}$.

Axiom of infinity

There exists a set with infinitely many elements:

$$\exists x.\emptyset \in x \wedge \forall y.y \in x \Rightarrow S(y) \in x$$

with $S(y) = y \cup \{y\}$.

In particular, we can define $\mathbb{N}$ as the intersection of all sets containing $\emptyset$ and closed under S, with the von Newman coding of natural numbers:

$$0 = \{\} \qquad 1 = 0 \cup \{0\} = \{\{\}\} \qquad 2 = 1 \cup \{1\} = \{\{\}, \{\{\}\}\}$$

etc.

Axiom of foundation

Every non-empty set contains a member which is disjoint from the whole set:

$$\forall x.(\exists t.t \in x) \Rightarrow \exists y.(y \in x \wedge \neg\exists z.(z \in y \wedge z \in x))$$

or, in usual notation,

$$\forall x.x \neq \emptyset \Rightarrow \exists y \in x.y \cap x = \emptyset$$

Axiom of foundation

Every non-empty set contains a member which is disjoint from the whole set:

$$\forall x.(\exists t.t \in x) \Rightarrow \exists y.(y \in x \wedge \neg\exists z.(z \in y \wedge z \in x))$$

or, in usual notation,

$$\forall x.x \neq \emptyset \Rightarrow \exists y \in x.y \cap x = \emptyset$$

The main consequence is

Lemma

There is no infinite sequence $(x_i)_{i\in\mathbb{N}}$ *of sets such that* $x_{i+1} \in x_i$.

Axiom of foundation

Every non-empty set contains a member which is disjoint from the whole set:

$$\forall x.(\exists t.t \in x) \Rightarrow \exists y.(y \in x \wedge \neg\exists z.(z \in y \wedge z \in x))$$

or, in usual notation,

$$\forall x.x \neq \emptyset \Rightarrow \exists y \in x.y \cap x = \emptyset$$

Together with other axioms, this is equivalent to the principle of $\in$-induction:

$$(\forall x.(\forall y.y \in x \Rightarrow A(y)) \Rightarrow A(x)) \Rightarrow \forall x.A(x)$$

The axiom of choice

Optionally, one can add the

Axiom of choice

Given a collection of non-empty sets, one can construct a **choice function** which chooses an element in each of the sets:

$$\forall x.\emptyset \notin x \Rightarrow \exists(f : x \to \cup x).\forall y \in x.f(y) \in y$$

The axiom of choice

Optionally, one can add the

Axiom of choice

Given a collection of non-empty sets, one can construct a **choice function** which chooses an element in each of the sets:

$$\forall x.\emptyset \notin x \Rightarrow \exists(f : x \to \cup x).\forall y \in x.f(y) \in y$$

This is very natural at first.

The axiom of choice in question

From a constructivist point of view, the axiom of choice is difficult to accept though. It chooses for us elements in sets, but we do not know how exactly.

The axiom of choice in question

From a constructivist point of view, the axiom of choice is difficult to accept though. It chooses for us elements in sets, but we do not know how exactly.

In particular, given a non-empty set, one can choose an element of it

$$x \neq \emptyset \Rightarrow \exists y.y \in x$$

which is difficult to accept constructively:

$$\neg\neg\exists y.y \in x \Rightarrow \exists y.y \in x$$

The axiom of choice

There are various formulations of the axiom of choice:

- for every set of non-empty sets there is a choice function

$$\forall x.\emptyset \notin x \Rightarrow \exists(f : x \to \cup x).\forall y \in x.f(y) \in y$$

- every surjective function admits a section,
- every set can be well-ordered,
- ...

The axiom of choice

A surjective function

$$f : A \to B$$

is "the same" as a collection of subsets of B (forming a partition):

$$(f^{-1}(y))_{y \in B}$$

The axiom of choice

A surjective function

$$f : A \to B$$

is "the same" as a collection of subsets of B (forming a partition):

$$(f^{-1}(y))_{y \in B}$$

A choice function for this collection is a function

$$g : B \to A$$

such that

$$\forall y. g(y) \in f^{-1}(y)$$

The axiom of choice

A surjective function

$$f : A \to B$$

is "the same" as a collection of subsets of B (forming a partition):

$$(f^{-1}(y))_{y \in B}$$

A choice function for this collection is a function

$$g : B \to A$$

such that

$$\forall y. f(g(y)) = y$$

The axiom of choice

A surjective function

$$f : A \to B$$

is "the same" as a collection of subsets of B (forming a partition):

$$(f^{-1}(y))_{y \in B}$$

A choice function for this collection is a function

$$g : B \to A$$

which is a *section* of f.

The axiom of choice

A surjective function

$$f : A \to B$$

is "the same" as a collection of subsets of B (forming a partition):

$$(f^{-1}(y))_{y \in B}$$

We have the following alternative formulation of the axiom of choice:

every surjective function admits a section.

The axiom of choice

Note that the naive translation of the axiom of choice in constructive type theory is

```
AC : {A B : Set} (f : A → B) →
     ((y : B) → Σ A (λ x → f x ≡ y)) →
     Σ (B → A) (λ g → (y : B) → f (g y) ≡ y)
```

The axiom of choice

Note that the naive translation of the axiom of choice in constructive type theory is provable:

```
AC : {A B : Set} (f : A → B) →
     ((y : B) → Σ A (λ x → f x ≡ y)) →
     Σ (B → A) (λ g → (y : B) → f (g y) ≡ y)
AC f s = (λ y → proj₁ (s y)) , (λ y → proj₂ (s y))
```

The axiom of choice

Note that the naive translation of the axiom of choice in constructive type theory is provable:

```
AC : {A B : Set} (f : A → B) →
     ((y : B) → Σ A (λ x → f x ≡ y)) →
     Σ (B → A) (λ g → (y : B) → f (g y) ≡ y)
AC f s = (λ y → proj₁ (s y)) , (λ y → proj₂ (s y))
```

The axiom of choice would be more like a doubly negated version of that:

```
postulate CAC : {A B : Set} (f : A → B) →
                ¬ ¬ ((y : B) → Σ A (λ x → f x ≡ y)) →
                ¬ ¬ (Σ (B → A) (λ g → (y : B) → f (g y) ≡ y))
```

The axiom of choice

Note that the naive translation of the axiom of choice in constructive type theory is provable:

```
AC : {A B : Set} (f : A → B) →
     ((y : B) → Σ A (λ x → f x ≡ y)) →
     Σ (B → A) (λ g → (y : B) → f (g y) ≡ y)
AC f s = (λ y → proj₁ (s y)) , (λ y → proj₂ (s y))
```

The axiom of choice would be more like a doubly negated version of that:

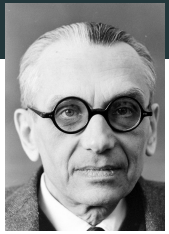
```
postulate CAC : {A B : Set} (f : A → B) →
                ¬ ¬ ((y : B) → Σ A (λ x → f x ≡ y)) →
                ¬ ¬ (Σ (B → A) (λ g → (y : B) → f (g y) ≡ y))
```

although we would rather use an "intuitionistic version of double negation".

The axiom of choice in question

So, people started to investigate the status of AC with respect to ZF.

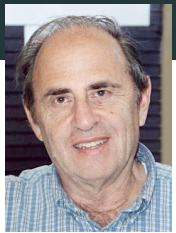
The axiom of choice in question



So, people started to investigate the status of AC with respect to ZF.

In 1938, Gödel, showed that AC is *consistent* with ZF by constructing a model of ZF+AC inside a model of ZF.

The axiom of choice in question

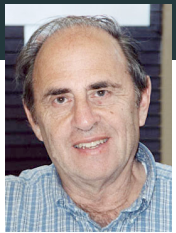


So, people started to investigate the status of AC with respect to ZF.

In 1938, Gödel, showed that AC is *consistent* with ZF by constructing a model of ZF+AC inside a model of ZF.

In 1963, Cohen showed that ZF+$\neg$AC is *consistent* by constructing a model using forcing.

The axiom of choice in question



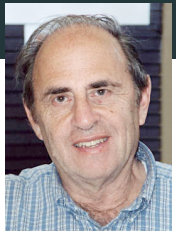
So, people started to investigate the status of AC with respect to ZF.

In 1938, Gödel, showed that AC is *consistent* with ZF by constructing a model of ZF+AC inside a model of ZF.

In 1963, Cohen showed that ZF+$\neg$AC is *consistent* by constructing a model using forcing.

AC is thus *independent* of ZF: we can add it or not.

The axiom of choice in question



So, people started to investigate the status of AC with respect to ZF.

In 1938, Gödel, showed that AC is *consistent* with ZF by constructing a model of ZF+AC inside a model of ZF.

In 1963, Cohen showed that ZF+$\neg$AC is *consistent* by constructing a model using forcing.

AC is thus *independent* of ZF: we can add it or not.

If we are hardcore constructivists, we want to use intuitionistic logic, we will see that in this case we also have to give up (some variants of) AC.

IZF

The theory ZF is usually taken to be in classical logic, but it makes sense in intuitionistic logic (it is then called IZF).

In this world, things do not behave as nicely as usual, but we are constructive!

Let's investigate this.

IZF: deciding membership

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

IZF: deciding membership

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(0 \in x) \Leftrightarrow A$$

IZF: deciding membership

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(0 \in x) \Leftrightarrow A$$

Lemma
In IZF, the formula

$$\forall y.\forall x.(y \in x) \vee \neg(y \in x)$$

is equivalent to the excluded middle.

Proof.

IZF: deciding membership

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(0 \in x) \Leftrightarrow A$$

Lemma
In IZF, the formula

$$\forall y.\forall x.(y \in x) \vee \neg(y \in x)$$

is equivalent to the excluded middle.

Proof.

The right-to-left implication is immediate.

IZF: deciding membership

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(0 \in x) \Leftrightarrow A$$

Lemma
In IZF, the formula

$$\forall y.\forall x.(y \in x) \vee \neg(y \in x)$$

is equivalent to the excluded middle.

Proof.

The right-to-left implication is immediate. For the other implication, given a formula A, take $y = 0$ and $x = \{y \in \mathbb{N} \mid A\}$: the formula is then equivalent to $A \vee \neg A$. □

IZF: deciding membership

What is the intuition behind that?

IZF: deciding membership

What is the intuition behind that?

Take

$$h = \{m \in \mathbb{N} \mid \text{the Turing machine } m \text{ is halting}\}$$

then, if we had a proof of

$$\forall x \in \mathbb{N}.(x \in h) \vee \neg(x \in h)$$

by Curry-Howard, we would have a function which to every program x indicates whether it is halting or not, which is impossible.

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x \Rightarrow 0 \in \emptyset$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x \Rightarrow 0 \in \emptyset \Rightarrow \bot$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x \Rightarrow 0 \in \emptyset \Rightarrow \bot$$

- conversely, if $\neg A$ then

$$y \in x$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x \Rightarrow 0 \in \emptyset \Rightarrow \bot$$

- conversely, if $\neg A$ then

$$y \in x \Rightarrow A$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x \Rightarrow 0 \in \emptyset \Rightarrow \bot$$

- conversely, if $\neg A$ then

$$y \in x \Rightarrow A \Rightarrow \bot$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Namely,

- if $x = \emptyset = \{x \in \mathbb{N} \mid \bot\}$, we have

$$A \Rightarrow 0 \in x \Rightarrow 0 \in \emptyset \Rightarrow \bot$$

- conversely, if $\neg A$ then

$$y \in x \Rightarrow A \Rightarrow \bot \Rightarrow y \in \emptyset$$

IZF: deciding emptyness

Given a proposition A not involving y, consider

$$x = \{y \in \mathbb{N} \mid A\}$$

We have

$$(x = \emptyset) \Leftrightarrow \neg A$$

Lemma
In IZF, the formula

$$\forall x.(x = \emptyset) \vee \neg(x = \emptyset)$$

is equivalent to having

$$\neg A \vee \neg\neg A$$

for every formula A, which does not hold in intuitionistic logic.

IZF: deciding equality

Lemma
In IZF, the formula

$$\forall x.\forall y.(x = y) \vee \neg(x = y)$$

does not hold.

Proof.

□

IZF: deciding equality

Lemma
In IZF, the formula

$$\forall x.\forall y.(x = y) \vee \neg(x = y)$$

does not hold.

Proof.

We have seen that it does not hold in the particular case where $y = \emptyset$. □

IZF: deciding equality

This does not mean that we cannot decide equality for any set!

IZF: deciding equality

This does not mean that we cannot decide equality for any set!

For instance, we define the booleans $\mathbb{B}$ as

$$\mathbb{B} = \{x \mid x = 0 \vee x = 1\} \qquad 0 = \emptyset \qquad 1 = \{\emptyset\}$$

IZF: deciding equality

This does not mean that we cannot decide equality for any set!

For instance, we define the booleans $\mathbb{B}$ as

$$\mathbb{B} = \{x \mid x = 0 \vee x = 1\} \qquad 0 = \emptyset \qquad 1 = \{\emptyset\}$$

We have $0 \neq 1$: namely $0 = 1$ would imply that $\emptyset \in 0$ since $\emptyset \in 1$, thus $\bot$.

IZF: deciding equality

This does not mean that we cannot decide equality for any set!

For instance, we define the booleans $\mathbb{B}$ as

$$\mathbb{B} = \{x \mid x = 0 \vee x = 1\} \qquad 0 = \emptyset \qquad 1 = \{\emptyset\}$$

We have $0 \neq 1$: namely $0 = 1$ would imply that $\emptyset \in 0$ since $\emptyset \in 1$, thus $\bot$.

Every element $x \in \mathbb{B}$ is either 0 or 1 (by definition), so that we can decide equality:

Lemma
The formula $\forall x \in \mathbb{B}.\forall y \in \mathbb{B}.(x = y) \vee (x \neq y)$ *holds.*

IZF: deciding equality

This does not mean that we cannot decide equality for any set!

For instance, we define the booleans $\mathbb{B}$ as

$$\mathbb{B} = \{x \mid x = 0 \vee x = 1\} \qquad 0 = \emptyset \qquad 1 = \{\emptyset\}$$

We have $0 \neq 1$: namely $0 = 1$ would imply that $\emptyset \in 0$ since $\emptyset \in 1$, thus $\bot$.

Every element $x \in \mathbb{B}$ is either 0 or 1 (by definition), so that we can decide equality:

Lemma
The formula $\forall x \in \mathbb{B}.\forall y \in \mathbb{B}.(x = y) \vee (x \neq y)$ *holds.*

Proof.
The booleans x and y are either 0 or 1 and in each of the four cases we can show the result:

	0	1
0	$x = y$	$x \neq y$
1	$x \neq y$	$x = y$

IZF: deciding equality

This does not mean that we cannot decide equality for any set!

For instance, we define the booleans $\mathbb{B}$ as

$$\mathbb{B} = \{x \mid x = 0 \vee x = 1\} \qquad 0 = \emptyset \qquad 1 = \{\emptyset\}$$

We have $0 \neq 1$: namely $0 = 1$ would imply that $\emptyset \in 0$ since $\emptyset \in 1$, thus $\bot$.

Every element $x \in \mathbb{B}$ is either 0 or 1 (by definition), so that we can decide equality:

Lemma
The formula $\forall x \in \mathbb{B}.\forall y \in \mathbb{B}.(x = y) \vee (x \neq y)$ *holds.*

The same would hold for the set $\mathbb{N}$ of natural numbers.

IZF: deciding equality

However, given a proposition $A(b)$, we cannot perform case analysis and say that

$$x = \{b \in \mathbb{B} \mid A(b)\}$$

is either

$$\emptyset \qquad \{0\} \qquad \{1\} \qquad \{0,1\}$$

(thus $A = \emptyset$ or not).

IZF: deciding equality

However, given a proposition $A(b)$, we cannot perform case analysis and say that

$$x = \{b \in \mathbb{B} \mid A(b)\}$$

is either

$$\emptyset \qquad \{0\} \qquad \{1\} \qquad \{0,1\}$$

(thus $A = \emptyset$ or not).

This is because an element of x is more than a boolean: it is

- a boolean b,
- together with a proof that $A(b)$ holds,

and we would have to reason by case analysis on all proofs of $A(b)$ which we can't.

Theorem
IZF+AC implies NNE.

Proof.
Given a formula A, suppose $\neg\neg A$ and consider the set

$$x = \{y \in \mathbb{N} \mid A\}$$

We have $\neg(x = \emptyset)$. Namely, if $x = \emptyset$, then $\neg A$, and therefore $\bot$ (by $\neg\neg A$).

Theorem
IZF+AC implies NNE.

Proof.
Given a formula A, suppose $\neg\neg A$ and consider the set

$$x = \{y \in \mathbb{N} \mid A\}$$

We have $\neg(x = \emptyset)$. Namely, if $x = \emptyset$, then $\neg A$, and therefore $\bot$ (by $\neg\neg A$).
By AC, there is an element $y \in x$ and thus A. □

Theorem
IZF+AC implies NNE.

Proof.
Given a formula A, suppose $\neg\neg A$ and consider the set

$$x = \{y \in \mathbb{N} \mid A\}$$

We have $\neg(x = \emptyset)$. Namely, if $x = \emptyset$, then $\neg A$, and therefore $\bot$ (by $\neg\neg A$).
By AC, there is an element $y \in x$ and thus A. □

We have used the following formulation of AC:

for every family of non-empty sets there is a choice function

Theorem
IZF+AC implies NNE.

Proof.
Given a formula A, suppose $\neg\neg A$ and consider the set

$$x = \{y \in \mathbb{N} \mid A\}$$

We have $\neg(x = \emptyset)$. Namely, if $x = \emptyset$, then $\neg A$, and therefore $\bot$ (by $\neg\neg A$).
By AC, there is an element $y \in x$ and thus A. □

We have used the following formulation of AC:

for every family of non-empty sets there is a choice function

whereas we would rather have:

for every family of sets with an element there is a choice function

Theorem
IZF+AC implies NNE.

Proof.
Given a formula A, suppose $\neg\neg A$ and consider the set

$$x = \{y \in \mathbb{N} \mid A\}$$

We have $\neg(x = \emptyset)$. Namely, if $x = \emptyset$, then $\neg A$, and therefore $\bot$ (by $\neg\neg A$).
By AC, there is an element $y \in x$ and thus A. □

We have used the following formulation of AC:

for every family of non-empty sets there is a choice function

whereas we would rather have:

for every family of sets with an element there is a choice function

The two are classically equivalent, but not intuitionistically so.

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,
- if $f(x) = 0 \neq 1 = f(y)$,

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,
- if $f(x) = 0 \neq 1 = f(y)$, then $x \neq y$ (they would have the same image under f otherwise),

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,
- if $f(x) = 0 \neq 1 = f(y)$, then $x \neq y$ (they would have the same image under f otherwise), if we suppose A then $x = y = \mathbb{B}$,

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,
- if $f(x) = 0 \neq 1 = f(y)$, then $x \neq y$ (they would have the same image under f otherwise), if we suppose A then $x = y = \mathbb{B}$, thus $\bot$,

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,
- if $f(x) = 0 \neq 1 = f(y)$, then $x \neq y$ (they would have the same image under f otherwise), if we suppose A then $x = y = \mathbb{B}$, thus $\bot$, therefore $\neg A$ holds.

Diaconescu's theorem

Theorem
IZF+AC implies LEM.

Proof.
Fix an arbitrary proposition A: we are going to show $A \vee \neg A$.

Consider the sets $x = \{b \in \mathbb{B} \mid (b = 0) \vee A\}$ and $y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$.

They have an element since $0 \in x$ and $1 \in y$.

By AC, there is a function $f : \{x, y\} \to \mathbb{B}$ such that $f(x) \in x$ and $f(y) \in y$.

Now, $f(x)$ and $f(y)$ are booleans so we can reason by case analysis on those:

- if $f(x) = 1$ then $1 \in x$, thus $(1 = 0) \vee A$ holds, thus A holds,
- if $f(y) = 0$ then $0 \in y$, thus $(0 = 1) \vee A$ holds, thus A holds,
- if $f(x) = 0 \neq 1 = f(y)$, then $x \neq y$ (they would have the same image under f otherwise), if we suppose A then $x = y = \mathbb{B}$, thus $\bot$, therefore $\neg A$ holds.

Therefore $A \vee \neg A$. □

Diaconescu's theorem

We have defined

$$x = \{b \in \mathbb{B} \mid (b = 0) \vee A\} \qquad y = \{b \in \mathbb{B} \mid (b = 1) \vee A\}$$

Note that even though $0 \in x$ and $1 \in y$, we cannot say that

$$\begin{aligned} f : \{A, B\} &\to \mathbb{B} \\ x &\mapsto 0 \\ y &\mapsto 1 \end{aligned}$$

is a choice function because it would not be well defined in the case $x = y$.

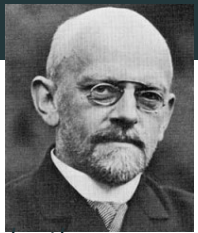
If $x = y$, then $f : x \mapsto 0$ is suitable.

But in order to use those facts to define a function, we would need to decide the equality between x and y in the first place!

Constructive mathematics

Constructive mathematics are hard.

Constructive mathematics

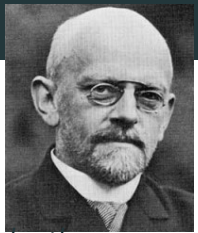


Constructive mathematics are hard.

Hilbert would say

> *Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists. To prohibit existence statements and the principle of excluded middle is tantamount to relinquishing the science of mathematics altogether.*

Constructive mathematics



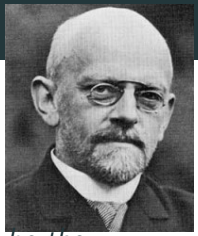
Constructive mathematics are hard.

Hilbert would say

> *Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists. To prohibit existence statements and the principle of excluded middle is tantamount to relinquishing the science of mathematics altogether.*

Without LEM (and thus AC), we have to give away very useful results and tools (we are going to see some of those).

Constructive mathematics



Constructive mathematics are hard.

Hilbert would say

> *Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists. To prohibit existence statements and the principle of excluded middle is tantamount to relinquishing the science of mathematics altogether.*

Without LEM (and thus AC), we have to give away very useful results and tools (we are going to see some of those).

But they are satisfactory: when something is true, we know why.

Life without choice

Let's see what life in IZF looks like.

Subsets of finite sets

A set A is **finite** when there exists $n \in \mathbb{N}$ and an enumeration $(a_i)_{1 \leqslant i \leqslant n}$ of its elements:

$$A = \{a_i \mid 1 \leqslant i \leqslant n\}$$

Subsets of finite sets

A set A is **finite** when there exists $n \in \mathbb{N}$ and an enumeration $(a_i)_{1 \leqslant i \leqslant n}$ of its elements:

$$A = \{a_i \mid 1 \leqslant i \leqslant n\}$$

Theorem
LEM is equivalent to "every subset of a finite set is finite".

Subsets of finite sets

A set A is **finite** when there exists $n \in \mathbb{N}$ and an enumeration $(a_i)_{1 \leqslant i \leqslant n}$ of its elements:

$$A = \{a_i \mid 1 \leqslant i \leqslant n\}$$

Theorem
LEM is equivalent to "every subset of a finite set is finite".

Proof.
Suppose LEM, we are in the usual world: for every element b of the subset either it is in A or not and we can simply reindex the b_i as in A.

Conversely, consider the set $A = \{0\}$ with one element and set $B = \{x \in A \mid P\}$. We have $B = \{b_1, \ldots, b_m\}$ and since equality is decidable on natural numbers we have $m = 0$ or $m \neq 0$, thus either $B = \emptyset$ or $B \neq \emptyset$, thus either $\neg P$ or P. □

Subsets of finite sets

A set A is **finite** when there exists $n \in \mathbb{N}$ and an enumeration $(a_i)_{1 \leqslant i \leqslant n}$ of its elements:

$$A = \{a_i \mid 1 \leqslant i \leqslant n\}$$

Theorem
LEM is equivalent to "every subset of a finite set is finite".

Note that this is not the only possible definition of finite:

- a set A is infinite when it is in bijection with a strict subset (and finite otherwise),
- a set A is finite when for every directed union $B = \bigcup_i B_i$, every function $f : A \to B$ factors as $f : A \to B_i$ for some i,
- ...

These are classically equivalent, but not constructively.

Subsets of finite sets

A set A is **finite** when there exists $n \in \mathbb{N}$ and an enumeration $(a_i)_{1 \leqslant i \leqslant n}$ of its elements:

$$A = \{a_i \mid 1 \leqslant i \leqslant n\}$$

Theorem
LEM is equivalent to "every subset of a finite set is finite".

In the same vein, the axiom of choice is also equivalent to the **trichotomy** principle: two given sets either have the same cardinality or one has smaller cardinality than the other.

Some models of IZF

Some models of IZF satisfy the following properties:

- There is a set that can be partitioned into strictly more equivalence classes than the original set has elements, and a function whose domain is strictly smaller than its range. In fact, this is the case in all known models.

Some models of IZF

Some models of IZF satisfy the following properties:

- There is a set that can be partitioned into strictly more equivalence classes than the original set has elements, and a function whose domain is strictly smaller than its range. In fact, this is the case in all known models.
- There is an infinite set of real numbers without a countably infinite subset.

Some models of IZF

Some models of IZF satisfy the following properties:

- There is a set that can be partitioned into strictly more equivalence classes than the original set has elements, and a function whose domain is strictly smaller than its range. In fact, this is the case in all known models.
- There is an infinite set of real numbers without a countably infinite subset.
- The real numbers are a countable union of countable sets. This does not imply that the real numbers are countable: we need AC to show that a countable union of countable sets is itself countable requires the Axiom of countable choice.

Basis of vector spaces

Another striking property:

Theorem
AC is equivalent to "every vector space has a basis".

In fact, we know models where

- there is a vector space with no basis,
- there is a vector space with two basis of different cardinalities.

Is AC the way to go?

Life without choice is difficult, but this does not necessarily means that AC is the right way to go. In fact it is suspiciously powerful.

Although ZFC is equiconsistent with ZF, we can think of it as the rule

$$\frac{}{\Gamma \vdash A}$$

which would clearly be too powerful.

Banach-Tarski paradox

Two sets A and B of points in $\mathbb{R}^3$ are **congruent** if one can be obtained from the other by an isometry (i.e. by using translations, rotations and reflections).

Banach-Tarski paradox

Two sets A and B of points in $\mathbb{R}^3$ are **congruent** if one can be obtained from the other by an isometry (i.e. by using translations, rotations and reflections).

Theorem (Banach-Tarski)
Given two bounded subsets of $\mathbb{R}^3$ of non-empty interior, there are partitions

$$A = A_1 \uplus \ldots \uplus A_n \qquad B = B_1 \uplus \ldots \uplus B_n$$

such that each A_i is congruent to B_i.
Proof: AC + many other things.

Banach-Tarski paradox

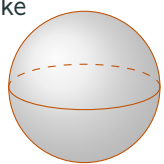
Two sets A and B of points in $\mathbb{R}^3$ are **congruent** if one can be obtained from the other by an isometry (i.e. by using translations, rotations and reflections).

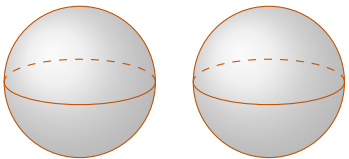
Theorem (Banach-Tarski)
Given two bounded subsets of $\mathbb{R}^3$ of non-empty interior, there are partitions

$$A = A_1 \uplus \ldots \uplus A_n \qquad B = B_1 \uplus \ldots \uplus B_n$$

such that each A_i is congruent to B_i.
Proof: AC + many other things.

In particular, take

$A =$ 

$B =$ 

Less is more

A last remark is that, even if we are not interested in constructivity, it is not entirely fair to think of the proofs in IZF as a subset of the proofs in ZF.

Less is more

A last remark is that, even if we are not interested in constructivity, it is not entirely fair to think of the proofs in IZF as a subset of the proofs in ZF.

Sometimes, less is more.

Computing derivatives

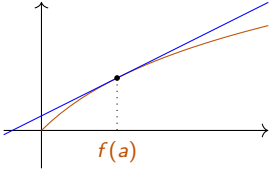
The notion of **infinitesimal** ε is difficult to properly define in mathematics.

Typically, one would like to be able to write something like

$$f'(a) = \frac{f(a+\varepsilon) - f(a)}{\varepsilon}$$

for an arbitrary infinitesimal ε.

The idea is that the derivative of f is the first-order variation of f around a point.



Computing derivatives

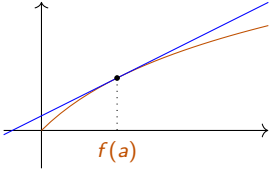
The notion of **infinitesimal** ε is difficult to properly define in mathematics.

Typically, one would like to be able to write something like

$$f(a+\varepsilon) = f(a) + f'(a)\varepsilon$$

for an arbitrary infinitesimal ε.

The idea is that the derivative of f is the first-order variation of f around a point.



Infinitesimals

Consider $f(x) = x^2$. We want to compute $f'(a)$.

Infinitesimals

Consider $f(x) = x^2$. We want to compute $f'(a)$.

Suppose given ε which is *very* small: $\varepsilon^2 = 0$. We have

$$f(a + \varepsilon) = (a + \varepsilon)^2$$

Infinitesimals

Consider $f(x) = x^2$. We want to compute $f'(a)$.

Suppose given ε which is *very* small: $\varepsilon^2 = 0$. We have

$$\begin{aligned} f(a+\varepsilon) &= (a+\varepsilon)^2 \\ &= a^2 + 2a\varepsilon + \varepsilon^2 \end{aligned}$$

Infinitesimals

Consider $f(x) = x^2$. We want to compute $f'(a)$.

Suppose given ε which is *very* small: $\varepsilon^2 = 0$. We have

$$\begin{aligned} f(a+\varepsilon) &= (a+\varepsilon)^2 \\ &= a^2 + 2a\varepsilon + \varepsilon^2 \\ &= a^2 + 2a\varepsilon \end{aligned}$$

Infinitesimals

Consider $f(x) = x^2$. We want to compute $f'(a)$.

Suppose given ε which is *very* small: $\varepsilon^2 = 0$. We have

$$\begin{aligned} f(a+\varepsilon) &= (a+\varepsilon)^2 \\ &= a^2 + 2a\varepsilon + \varepsilon^2 \\ &= a^2 + 2a\varepsilon \end{aligned}$$

Therefore, we can define

$$f'(a) = 2a$$

to be the linear part.

Infinitesimals

This suggests that we define the set of **infinitesimals** as

$$D = \{\varepsilon \in \mathbb{R} \mid \varepsilon^2 = 0\}$$

Infinitesimals

This suggests that we define the set of **infinitesimals** as

$$D = \{\varepsilon \in \mathbb{R} \mid \varepsilon^2 = 0\}$$

and postulate the *principle of microaffineness*:

Axiom (Kock-Lawvere)
Every function $f : D \to \mathbb{R}$ is of the form

$$f(\varepsilon) = a + b\varepsilon$$

for some unique a and b (with a being necessarily $f(0)$).

Infinitesimals

This suggests that we define the set of **infinitesimals** as

$$D = \{\varepsilon \in \mathbb{R} \mid \varepsilon^2 = 0\}$$

and postulate the *principle of microaffineness*:

Axiom (Kock-Lawvere)
Every function $f : D \to \mathbb{R}$ is of the form

$$f(\varepsilon) = a + b\varepsilon$$

for some unique a and b (with a being necessarily $f(0)$).

We can the define $f'(x)$ by writing

$$f(x + \varepsilon) = f(x) + b\varepsilon$$

and defining $f'(x) = b$.

The product rule

We can compute the usual law for deriving products:

$$(f \times g)(a + \varepsilon) = f(a + \varepsilon) \times g(a + \varepsilon)$$

The product rule

We can compute the usual law for deriving products:

$$\begin{aligned}(f \times g)(a + \varepsilon) &= f(a + \varepsilon) \times g(a + \varepsilon) \\ &= (f(a) + f'(a)\varepsilon) \times (g(a) + g'(a)\varepsilon)\end{aligned}$$

The product rule

We can compute the usual law for deriving products:

$$\begin{aligned}(f \times g)(a+\varepsilon) &= f(a+\varepsilon) \times g(a+\varepsilon) \\ &= (f(a) + f'(a)\varepsilon) \times (g(a) + g'(a)\varepsilon) \\ &= f(a)g(a) + (f'(a)g(a) + f(a)g'(a))\varepsilon + f'(a)g'(a)\varepsilon^2\end{aligned}$$

The product rule

We can compute the usual law for deriving products:

$$\begin{aligned}(f \times g)(a+\varepsilon) &= f(a+\varepsilon) \times g(a+\varepsilon) \\ &= (f(a) + f'(a)\varepsilon) \times (g(a) + g'(a)\varepsilon) \\ &= f(a)g(a) + (f'(a)g(a) + f(a)g'(a))\varepsilon + f'(a)g'(a)\varepsilon^2 \\ &= f(a)g(a) + (f'(a)g(a) + f(a)g'(a))\varepsilon\end{aligned}$$

The product rule

We can compute the usual law for deriving products:

$$\begin{aligned}(f \times g)(a+\varepsilon) &= f(a+\varepsilon) \times g(a+\varepsilon) \\ &= (f(a) + f'(a)\varepsilon) \times (g(a) + g'(a)\varepsilon) \\ &= f(a)g(a) + (f'(a)g(a) + f(a)g'(a))\varepsilon + f'(a)g'(a)\varepsilon^2 \\ &= f(a)g(a) + (f'(a)g(a) + f(a)g'(a))\varepsilon\end{aligned}$$

Therefore,

$$(f \times g)'(a) = f'(a) \times g(a) + f(a) \times g'(a)$$

The chain rule

Similarly, we can compute the chain rule by

$$\begin{aligned}(g \circ f)(a + \varepsilon) &= g(f(a) + f'(a)\varepsilon) \\ &= g(f(a)) + g'(f(a)) \times f'(a)\varepsilon\end{aligned}$$

since $f'(a)\varepsilon \in D$.

The chain rule

Similarly, we can compute the chain rule by

$$\begin{aligned}(g \circ f)(a + \varepsilon) &= g(f(a) + f'(a)\varepsilon) \\ &= g(f(a)) + g'(f(a)) \times f'(a)\varepsilon\end{aligned}$$

since $f'(a)\varepsilon \in D$.

Therefore,

$$(g \circ f)'(a) = g'(f(a)) \times f'(a)$$

A bug?

Oh wait, there is a “slight” problem:

A bug?

Oh wait, there is a "slight" problem: our axiom

Axiom
Every function $f : D \to \mathbb{R}$ is of the form $f(\varepsilon) = a + b\varepsilon$ for some unique a and b.

is clearly wrong.

A bug?

Oh wait, there is a "slight" problem: our axiom

Axiom
Every function $f : D \to \mathbb{R}$ is of the form $f(\varepsilon) = a + b\varepsilon$ for some unique a and b.

is clearly wrong.

Namely, we have $D = \{0\}$ and thus

$$f(a + \varepsilon) = f(a) + b\varepsilon \qquad f(a + \varepsilon) = f(a) + c\varepsilon$$

for any b and c since $\varepsilon = 0$.

A bug?

Oh wait, there is a "slight" problem: our axiom

Axiom
Every function $f : D \to \mathbb{R}$ is of the form $f(\varepsilon) = a + b\varepsilon$ for some unique a and b.

is clearly wrong.

Namely, we have $D = \{0\}$ and thus

$$f(a + \varepsilon) = f(a) + b\varepsilon \qquad f(a + \varepsilon) = f(a) + c\varepsilon$$

for any b and c since $\varepsilon = 0$.

Also, our axiom implies that every function is differentiable and we know that's not the way things are.

Synthetic differential geometry

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Well, it's obvious: take any $\varepsilon \in D$, if $\varepsilon \neq 0$ then $\varepsilon^2 > 0$ and therefore $\varepsilon \notin D$.

Synthetic differential geometry

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Well, it's obvious: take any $\varepsilon \in D$, if $\varepsilon \neq 0$ then $\varepsilon^2 > 0$ and therefore $\varepsilon \notin D$.

Oh wait,

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Well, it's obvious: take any $\varepsilon \in D$, if $\varepsilon \neq 0$ then $\varepsilon^2 > 0$ and therefore $\varepsilon \notin D$.

Oh wait, we have used classical logic. Namely, in order to make this reasoning we have implicitly used

Synthetic differential geometry

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Well, it's obvious: take any $\varepsilon \in D$, if $\varepsilon \neq 0$ then $\varepsilon^2 > 0$ and therefore $\varepsilon \notin D$.

Oh wait, we have used classical logic. Namely, in order to make this reasoning we have implicitly used

- nne: we have shown that ε cannot be non-zero, and deduced that $\varepsilon = 0$, or

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Well, it's obvious: take any $\varepsilon \in D$, if $\varepsilon \neq 0$ then $\varepsilon^2 > 0$ and therefore $\varepsilon \notin D$.

Oh wait, we have used classical logic. Namely, in order to make this reasoning we have implicitly used

- nne: we have shown that ε cannot be non-zero, and deduced that $\varepsilon = 0$, or
- lem: either $\varepsilon = 0$ or $\varepsilon \neq 0$, and in the second case we have a contradiction.

Synthetic differential geometry

Why is it the case that $D = \{\varepsilon \mid \varepsilon^2 = 0\} = \{0\}$?

Well, it's obvious: take any $\varepsilon \in D$, if $\varepsilon \neq 0$ then $\varepsilon^2 > 0$ and therefore $\varepsilon \notin D$.

Oh wait, we have used classical logic. Namely, in order to make this reasoning we have implicitly used

- nne: we have shown that ε cannot be non-zero, and deduced that $\varepsilon = 0$, or
- lem: either $\varepsilon = 0$ or $\varepsilon \neq 0$, and in the second case we have a contradiction.

In intuitionistic logic, all we can show is that

$$\forall \varepsilon \in D. \neg\neg(\varepsilon = 0)$$

In this sense, an infinitesimal is "almost 0".

Is it a field?

Is it a field? No: since $\varepsilon^2 = 0$, we would have

$$\varepsilon = \varepsilon^2/\varepsilon = 0/\varepsilon = 0$$

Is it a field? No: since $\varepsilon^2 = 0$, we would have

$$\varepsilon = \varepsilon^2/\varepsilon = 0/\varepsilon = 0$$

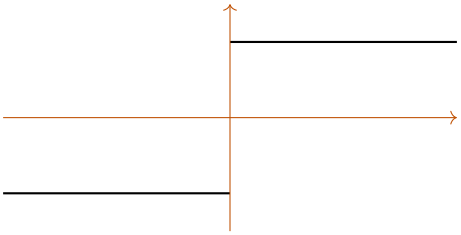
However, we still have the fact that $x \neq 0$ implies that x is invertible, and this is not a problem because we cannot show $\varepsilon \neq 0$, since we have $\neg\neg(\varepsilon = 0)$.

The axiom implies that every function is differentiable.

Synthetic differential geometry

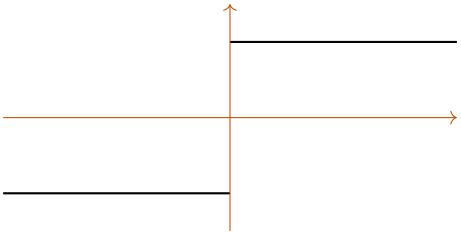
The axiom implies that every function is differentiable.

But this is not the case, for instance,



The axiom implies that every function is differentiable.

But this is not the case, for instance,



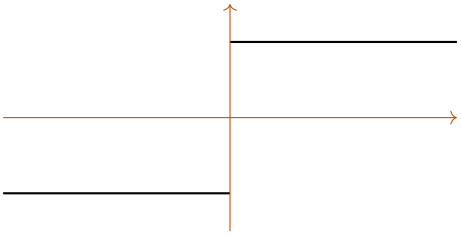
which can be defined by

$$f(x) = \begin{cases} -1 & \text{if } x < 0 \\ 1 & \text{otherwise} \end{cases}$$

Synthetic differential geometry

The axiom implies that every function is differentiable.

But this is not the case, for instance,



which **cannot** be defined by

$$f(x) = \begin{cases} -1 & \text{if } x < 0 \\ 1 & \text{otherwise} \end{cases}$$

Synthetic differential geometry

The field of **synthetic differential geometry** studies differential geometry in this way, by considering infinitesimals in intuitionistic logic.

Synthetic differential geometry

The field of **synthetic differential geometry** studies differential geometry in this way, by considering infinitesimals in intuitionistic logic.

What we did not show here is that we actually have a model satisfying the axioms...

Part IV

Unification

Unification

Suppose fixed a signature Σ, generating a set $\mathcal{T}$ of terms.

We are going to solve systems of equations over $\mathcal{T}$.

For instance, with

$$\Sigma = \{f : 1, g : 2, a : 0\}$$

consider the system of equations

$$\begin{cases} f(x) \stackrel{?}{=} f(f(a)) \\ g(x,x) \stackrel{?}{=} g(x,y) \end{cases}$$

What are the solutions?

The **unification** algorithm solves such equational problems.

Unification

Suppose fixed a signature Σ, generating a set $\mathcal{T}$ of terms.

We are going to solve systems of equations over $\mathcal{T}$.

For instance, with

$$\Sigma = \{f : 1, g : 2, a : 0\}$$

consider the system of equations

$$\begin{cases} f(x) \stackrel{?}{=} f(f(a)) \\ g(x,x) \stackrel{?}{=} g(x,y) \end{cases}$$

What are the solutions?

The **unification** algorithm solves such equational problems.

In particular, we have seen that we could express typing à la Curry in this way.

Substitutions

A **substitution** σ is a function which to some variables associates a term.

Substitutions

A **substitution** σ is a function which to some variables associates a term.

We write $\mathrm{dom}(\sigma)$ for its **domain**, i.e. the variables on which it is defined.

Substitutions

A **substitution** σ is a function which to some variables associates a term.

We write $\mathrm{dom}(\sigma)$ for its **domain**, i.e. the variables on which it is defined.

Given a term t with $\mathrm{FV}(t) \subseteq \mathrm{dom}(\sigma)$, we write $\sigma(t)$ for the term t where each variable x has been replaced by $\sigma(x)$.

Systems of equations

A **system of equations** E is a set

$$E \quad = \quad \{t_1 \stackrel{?}{\neq} u_1, \ldots, t_n \stackrel{?}{\neq} u_n\}$$

of pairs of terms.

Systems of equations

A **system of equations** E is a set

$$E \quad = \quad \{t_1 \stackrel{?}{\neq} u_1, \ldots, t_n \stackrel{?}{\neq} u_n\}$$

of pairs of terms.

A substitution is a **solution** (or **unifier**) of a system of equations E, if for every equation $t_i \stackrel{?}{\neq} u_i$, we have $\mathsf{FV}(t_i) \cup \mathsf{FV}(u_i) \subseteq \mathsf{dom}(\sigma)$ and

$$\sigma(t_i) = \sigma(u_i)$$

Systems of equations

A **system of equations** E is a set

$$E \quad = \quad \{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\}$$

of pairs of terms.

A substitution is a **solution** (or **unifier**) of a system of equations E, if for every equation $t_i \stackrel{?}{=} u_i$, we have $\mathsf{FV}(t_i) \cup \mathsf{FV}(u_i) \subseteq \mathsf{dom}(\sigma)$ and

$$\sigma(t_i) = \sigma(u_i)$$

A solution of our example $\{f(x) \stackrel{?}{=} f(f(a)), g(x,x) \stackrel{?}{=} g(x,y)\}$ is

$$\sigma(x) = \qquad\qquad \sigma(y) =$$

Systems of equations

A **system of equations** E is a set

$$E \quad = \quad \{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\}$$

of pairs of terms.

A substitution is a **solution** (or **unifier**) of a system of equations E, if for every equation $t_i \stackrel{?}{=} u_i$, we have $\mathsf{FV}(t_i) \cup \mathsf{FV}(u_i) \subseteq \mathsf{dom}(\sigma)$ and

$$\sigma(t_i) = \sigma(u_i)$$

A solution of our example $\{f(x) \stackrel{?}{=} f(f(a)), g(x,x) \stackrel{?}{=} g(x,y)\}$ is

$$\sigma(x) = f(a) \qquad\qquad \sigma(y) =$$

Systems of equations

A **system of equations** E is a set

$$E \quad = \quad \{t_1 \stackrel{?}{\neq} u_1, \ldots, t_n \stackrel{?}{\neq} u_n\}$$

of pairs of terms.

A substitution is a **solution** (or **unifier**) of a system of equations E, if for every equation $t_i \stackrel{?}{\neq} u_i$, we have $\mathsf{FV}(t_i) \cup \mathsf{FV}(u_i) \subseteq \mathsf{dom}(\sigma)$ and

$$\sigma(t_i) = \sigma(u_i)$$

A solution of our example $\{f(x) \stackrel{?}{\neq} f(f(a)), g(x,x) \stackrel{?}{\neq} g(x,y)\}$ is

$$\sigma(x) = f(a) \qquad\qquad \sigma(y) = f(a)$$

Solutions?

We first have to explain what we mean by “the solution”:

- $f(x) \not\ni f(a)$ has one solution: $x \mapsto a$,

Solutions?

We first have to explain what we mean by "the solution":

- $f(x) \stackrel{?}{=} f(a)$ has one solution: $x \mapsto a$,
- $x \stackrel{?}{=} f(y)$ has many solutions: $[y \mapsto a, x \mapsto f(a)]$, $[y \mapsto f(a), x \mapsto f(f(a))]$, etc.

Solutions?

We first have to explain what we mean by "the solution":

- $f(x) \stackrel{?}{=} f(a)$ has one solution: $x \mapsto a$,
- $x \stackrel{?}{=} f(y)$ has many solutions: $[y \mapsto a, x \mapsto f(a)]$, $[y \mapsto f(a), x \mapsto f(f(a))]$, etc.
- $f(x) \stackrel{?}{=} g(y, z)$ has no solution,

Solutions?

We first have to explain what we mean by "the solution":

- $f(x) \stackrel{?}{=} f(a)$ has one solution: $x \mapsto a$,
- $x \stackrel{?}{=} f(y)$ has many solutions: $[y \mapsto a, x \mapsto f(a)]$, $[y \mapsto f(a), x \mapsto f(f(a))]$, etc.
- $f(x) \stackrel{?}{=} g(y, z)$ has no solution,
- $x \stackrel{?}{=} f(x)$ has no solution.

Unification

We are going to describe an algorithm which transforms equation systems akin to gaussian elimination:

$$\begin{cases} x + 3y = 0 \\ 2x + 8y = 2z \end{cases}$$

Unification

We are going to describe an algorithm which transforms equation systems akin to gaussian elimination:

$$\begin{cases} x + 3y = 0 \\ 2x + 8y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ \quad 2y = 2z \end{cases}$$

Unification

We are going to describe an algorithm which transforms equation systems akin to gaussian elimination:

$$\begin{cases} x + 3y = 0 \\ 2x + 8y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ 2y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ y = z \end{cases}$$

Unification

We are going to describe an algorithm which transforms equation systems akin to gaussian elimination:

$$\begin{cases} x + 3y = 0 \\ 2x + 8y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ 2y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ y = z \end{cases} \rightsquigarrow \begin{cases} x + 3z = 0 \\ y = z \end{cases}$$

Unification

We are going to describe an algorithm which transforms equation systems akin to gaussian elimination:

$$\begin{cases} x + 3y = 0 \\ 2x + 8y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ 2y = 2z \end{cases} \rightsquigarrow \begin{cases} x + 3y = 0 \\ y = z \end{cases} \rightsquigarrow \begin{cases} x + 3z = 0 \\ y = z \end{cases}$$

$$\rightsquigarrow \begin{cases} x = -3z \\ y = z \end{cases}$$

Solved form

An equation system E is in **solved form** if is of the form

$$E = \{x_1 \stackrel{?}{=} t_1, \ldots, x_n \stackrel{?}{=} t_n\}$$

where

- $x_i \neq x_j$ for $i \neq j$,
- $x_i \notin \mathrm{FV}(t_j)$ for every i and j.

Solved form

An equation system E is in **solved form** if is of the form

$$E = \{x_1 \stackrel{?}{=} t_1, \ldots, x_n \stackrel{?}{=} t_n\}$$

where

- $x_i \neq x_j$ for $i \neq j$,
- $x_i \notin \mathrm{FV}(t_j)$ for every i and j.

For such an equation system, we can consider the substitution such that for every i

$$\sigma(x_i) = t_i$$

and it is easy to see that σ is a solution of E.

Solved form

An equation system E is in **solved form** if is of the form

$$E = \{x_1 \stackrel{?}{=} t_1, \ldots, x_n \stackrel{?}{=} t_n\}$$

where

- $x_i \neq x_j$ for $i \neq j$,
- $x_i \notin \mathrm{FV}(t_j)$ for every i and j.

For instance, the following is in solved form

$$\{x = f(a), y = f(z)\}$$

Solved form

An equation system E is in **solved form** if is of the form

$$E = \{x_1 \stackrel{?}{=} t_1, \ldots, x_n \stackrel{?}{=} t_n\}$$

where

- $x_i \neq x_j$ for $i \neq j$,
- $x_i \notin \mathrm{FV}(t_j)$ for every i and j.

For instance, the following is not in solved form

$$\{x = f(a), y = f(b)\}$$

Solved form

An equation system E is in **solved form** if is of the form

$$E = \{x_1 \stackrel{?}{=} t_1, \ldots, x_n \stackrel{?}{=} t_n\}$$

where

- $x_i \neq x_j$ for $i \neq j$,
- $x_i \notin \mathrm{FV}(t_j)$ for every i and j.

For instance, the following is not in solved form

$$\{x = f(y), y = f(x)\}$$

Solved form

An equation system E is in **solved form** if is of the form

$$E = \{x_1 \stackrel{?}{=} t_1, \ldots, x_n \stackrel{?}{=} t_n\}$$

where

- $x_i \neq x_j$ for $i \neq j$,
- $x_i \notin \mathrm{FV}(t_j)$ for every i and j.

The strategy is thus to transform our equation system

$$E \rightsquigarrow E_1 \rightsquigarrow E_2 \rightsquigarrow \ldots \rightsquigarrow E_n$$

in such a way that

- E_i and E_{i+1} have the same solutions,
- E_n is in solved form.

Unification

The **unification algorithm** consists in applying the following transformations.

Unification

The **unification algorithm** consists in applying the following transformations.

- **Delete**:

$$\{t \stackrel{?}{\neq} t\} \uplus E \quad \rightsquigarrow \quad E$$

Unification

The **unification algorithm** consists in applying the following transformations.

- **Delete**:

$$\{t \stackrel{?}{\neq} t\} \uplus E \quad \rightsquigarrow \quad E$$

- **Decompose**:

$$\{f(t_1, \ldots, t_n) \stackrel{?}{\neq} f(u_1, \ldots, u_n)\} \uplus E \quad \rightsquigarrow \quad \{t_1 \stackrel{?}{\neq} u_1, \ldots, t_n \stackrel{?}{\neq} u_n\} \uplus E$$

Unification

The **unification algorithm** consists in applying the following transformations.

- **Delete**:

$$\{t \stackrel{?}{=} t\} \uplus E \quad \rightsquigarrow \quad E$$

- **Decompose**:

$$\{f(t_1, \ldots, t_n) \stackrel{?}{=} f(u_1, \ldots, u_n)\} \uplus E \quad \rightsquigarrow \quad \{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\} \uplus E$$

- **Orient**: when t is not a variable

$$\{t \stackrel{?}{=} x\} \uplus E \quad \rightsquigarrow \quad \{x \stackrel{?}{=} t\} \uplus E$$

Unification

The **unification algorithm** consists in applying the following transformations.

- **Delete**:

$$\{t \stackrel{?}{=} t\} \uplus E \quad \rightsquigarrow \quad E$$

- **Decompose**:

$$\{f(t_1, \ldots, t_n) \stackrel{?}{=} f(u_1, \ldots, u_n)\} \uplus E \quad \rightsquigarrow \quad \{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\} \uplus E$$

- **Orient**: when t is not a variable

$$\{t \stackrel{?}{=} x\} \uplus E \quad \rightsquigarrow \quad \{x \stackrel{?}{=} t\} \uplus E$$

- **Eliminate**: if $x \in \mathrm{FV}(E) \setminus \mathrm{FV}(t)$,

$$\{x \stackrel{?}{=} t\} \uplus E \quad \rightsquigarrow \quad \{x \stackrel{?}{=} t\} \uplus \sigma(E)$$

Unification

In addition, the algorithm will fail on the following cases:

- **Clash**: for $f \neq g$,

$$\{f(t_1, \ldots, t_n) \stackrel{?}{=} g(u_1, \ldots, u_m)\} \uplus E \quad \rightsquigarrow \quad \text{fail}$$

Unification

In addition, the algorithm will fail on the following cases:

- **Clash**: for $f \neq g$,

$$\{f(t_1, \ldots, t_n) \stackrel{?}{=} g(u_1, \ldots, u_m)\} \uplus E \quad \rightsquigarrow \quad \text{fail}$$

- **Occurs-check**: for $x \in \mathrm{FV}(t)$,

$$\{x \stackrel{?}{=} t\} \uplus E \quad \rightsquigarrow \quad \text{fail}$$

An example

Let's execute our algorithm on

$$\{x \stackrel{?}{=} f(a), g(x, x) \stackrel{?}{=} g(x, y)\}$$

An example

Let's execute our algorithm on

$$\{x \stackrel{?}{=} f(a), g(x,x) \stackrel{?}{=} g(x,y)\}$$
$$\rightsquigarrow \quad \{x \stackrel{?}{=} f(a), g(f(a),f(a)) \stackrel{?}{=} g(f(a),y)\} \quad \text{by Eliminate}$$

An example

Let's execute our algorithm on

$$
\begin{array}{lll}
 & \{x \stackrel{?}{\neq} f(a), g(x,x) \stackrel{?}{\neq} g(x,y)\} & \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), g(f(a),f(a)) \stackrel{?}{\neq} g(f(a),y)\} & \text{by Eliminate} \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} y\} & \text{by Decompose}
\end{array}
$$

An example

Let's execute our algorithm on

$$
\begin{array}{lll}
 & \{x \stackrel{?}{\neq} f(a), g(x,x) \stackrel{?}{\neq} g(x,y)\} & \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), g(f(a),f(a)) \stackrel{?}{\neq} g(f(a),y)\} & \text{by Eliminate} \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} y\} & \text{by Decompose} \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} y\} & \text{by Delete}
\end{array}
$$

An example

Let's execute our algorithm on

$$
\begin{array}{lll}
 & \{x \stackrel{?}{\neq} f(a), g(x,x) \stackrel{?}{\neq} g(x,y)\} & \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), g(f(a),f(a)) \stackrel{?}{\neq} g(f(a),y)\} & \text{by Eliminate} \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} y\} & \text{by Decompose} \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), f(a) \stackrel{?}{\neq} y\} & \text{by Delete} \\
\rightsquigarrow & \{x \stackrel{?}{\neq} f(a), y \stackrel{?}{\neq} f(a)\} & \text{by Orient}
\end{array}
$$

An example

Let's execute our algorithm on

$$
\begin{array}{lll}
 & \{x \stackrel{?}{=} f(a), g(x,x) \stackrel{?}{=} g(x,y)\} & \\
\rightsquigarrow & \{x \stackrel{?}{=} f(a), g(f(a),f(a)) \stackrel{?}{=} g(f(a),y)\} & \text{by Eliminate} \\
\rightsquigarrow & \{x \stackrel{?}{=} f(a), f(a) \stackrel{?}{=} f(a), f(a) \stackrel{?}{=} y\} & \text{by Decompose} \\
\rightsquigarrow & \{x \stackrel{?}{=} f(a), f(a) \stackrel{?}{=} y\} & \text{by Delete} \\
\rightsquigarrow & \{x \stackrel{?}{=} f(a), y \stackrel{?}{=} f(a)\} & \text{by Orient}
\end{array}
$$

A solution is thus

$$\sigma(x) = f(a) \qquad \sigma(y) = f(a)$$

Unification

The **unification algorithm** consists, starting from E, in

- applying a transformation when one applies,
- when no transformation applies anymore and we have not failed, we return the corresponding substitution.

Some remarks

Note that

- we have to show that our transformations preserve the solutions

Some remarks

Note that

- we have to show that our transformations preserve the solutions
- we have to show that if the equation system has a solution then we have a normal form when we stop (without failing)

Some remarks

Note that

- we have to show that our transformations preserve the solutions
- we have to show that if the equation system has a solution then we have a normal form when we stop (without failing)
- the algorithm is not deterministic so that it is not clear that it will always give the same solution

Some remarks

Note that

- we have to show that our transformations preserve the solutions
- we have to show that if the equation system has a solution then we have a normal form when we stop (without failing)
- the algorithm is not deterministic so that it is not clear that it will always give the same solution
- an equation system might have multiple solutions so what is the status of the solution provided by unification?

Some remarks

Note that

- we have to show that our transformations preserve the solutions
- we have to show that if the equation system has a solution then we have a normal form when we stop (without failing)
- the algorithm is not deterministic so that it is not clear that it will always give the same solution
- an equation system might have multiple solutions so what is the status of the solution provided by unification?
- we have to show that the algorithm terminates

Lemma
If $E \rightsquigarrow E'$ then E and E' admit the same solutions.

Proof.
By inspection of the rules.

- Delete: $\{t \stackrel{?}{=} t\} \uplus E \rightsquigarrow E$
- Decompose: $\{f(t_1, \ldots, t_n) \stackrel{?}{=} f(u_1, \ldots, u_n)\} \uplus E \rightsquigarrow \{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\} \uplus E$
- Orient: $\{t \stackrel{?}{=} x\} \uplus E \rightsquigarrow \{x \stackrel{?}{=} t\} \uplus E$ when t is not a variable
- Eliminate: $\{x \stackrel{?}{=} t\} \uplus E \rightsquigarrow \{x \stackrel{?}{=} t\} \uplus \sigma(E)$ if $x \in \mathrm{FV}(E) \setminus \mathrm{FV}(t)$ □

Completeness

Lemma
If $E \not\rightarrow$ then E is in solved form.

Proof.
If E is not in solved form then either

- it contains some $f(t_1, \ldots, t_n) \stackrel{?}{=} u$ with either
  - $u = x$: orient, or
  - $u = f(t_1, \ldots, t_n)$: delete, or
  - $u = f(u_1, \ldots, u_n)$: decompose, or
  - $u = g(u_1, \ldots, u_m)$: clash, or
- there is some $x_i \stackrel{?}{=} t_i$ with $x_i \in \mathrm{FV}(t_j)$: eliminate / occurs-check. □

Termination

How do we show the termination of the algorithm?

Termination

How do we show the termination of the algorithm?

We could associate a natural number n^E to each system of equations such that

$$E \rightsquigarrow E' \qquad \text{implies} \qquad n^E > n^{E'}$$

Termination

How do we show the termination of the algorithm?

We could associate a natural number n^E to each system of equations such that

$$E \rightsquigarrow E' \qquad \text{implies} \qquad n^E > n^{E'}$$

It turns out that it will be more convenient to associate a triple (n_1^E, n_2^E, n_3^3) of natural numbers such that

$$E \rightsquigarrow E' \qquad \text{implies} \qquad (n_1^E, n_2^E, n_3^E) > (n_1^{E'}, n_2^{E'}, n_3^{E'})$$

Termination

How do we show the termination of the algorithm?

We could associate a natural number n^E to each system of equations such that

$$E \rightsquigarrow E' \qquad \text{implies} \qquad n^E > n^{E'}$$

It turns out that it will be more convenient to associate a triple (n_1^E, n_2^E, n_3^3) of natural numbers such that

$$E \rightsquigarrow E' \qquad \text{implies} \qquad (n_1^E, n_2^E, n_3^E) > (n_1^{E'}, n_2^{E'}, n_3^{E'})$$

where $(m_1, m_2, m_3) > (n_1, n_2, n_3)$ when

$m_1 > n_1$ or $m_1 = n_1$ and $m_2 > n_2$ or $m_1 = n_1$ and $m_2 = n_2$ and $m_3 > n_3$

(lexicographic order).

The lexicographic order

We order the set $\mathbb{N} \times \mathbb{N}$ by $(m_1, m_2) > (n_1, n_2)$ whenever

(a) $m_1 > n_1$, or

(b) $m_1 = n_1$ and $m_2 > n_2$.

The lexicographic order

We order the set $\mathbb{N} \times \mathbb{N}$ by $(m_1, m_2) > (n_1, n_2)$ whenever

(a) $m_1 > n_1$, or

(b) $m_1 = n_1$ and $m_2 > n_2$.

A decreasing sequence is

$$(5, 10) > (4, 8) > (3, 18) > (3, 15) > (2, 40) > \dots$$

The lexicographic order

We order the set $\mathbb{N} \times \mathbb{N}$ by $(m_1, m_2) > (n_1, n_2)$ whenever

(a) $m_1 > n_1$, or

(b) $m_1 = n_1$ and $m_2 > n_2$.

A decreasing sequence is

$$(5, 10) > (4, 8) > (3, 18) > (3, 15) > (2, 40) > \dots$$

Proposition
There is no infinite decreasing sequence in $\mathbb{N} \times \mathbb{N}$.

The lexicographic order

We order the set $\mathbb{N} \times \mathbb{N}$ by $(m_1, m_2) > (n_1, n_2)$ whenever

(a) $m_1 > n_1$, or

(b) $m_1 = n_1$ and $m_2 > n_2$.

A decreasing sequence is

$$(5, 10) > (4, 8) > (3, 18) > (3, 15) > (2, 40) > \dots$$

Proposition
There is no infinite decreasing sequence in $\mathbb{N} \times \mathbb{N}$.

Proof.
In the sequence there is an infinite number of (a) or of (b).

(a) This is impossible because the first $\mathbb{N}$ is noetherian.

(b) After the last (a), there is an infinite sequence of (b) which is impossible because the second $\mathbb{N}$ is noetherian.

Termination

We need some terminology.

A variable is **solved** in E when it occurs exactly once, as a left member of an equation.

The **size** of a term is the number of function symbols occurring in it:

$$|f(g(a(), x), y)| = 3$$

Termination

We need some terminology.

A variable is **solved** in E when it occurs exactly once, as a left member of an equation.

The **size** of a term is the number of function symbols occurring in it:

$$|f(g(a(), x), y)| = 3$$

The size of an equation system is the sum of the size of the terms in a left or right member of an equation.

Termination

Theorem
The unification algorithm is terminating for all inputs.

Proof.
To every equation system E, we associate:

- n_1: the number of variables in E which are not solved,
- n_2: the size of E,
- n_3: the number of equations of the form $t \stackrel{?}{=} x$ in E.

We then have

$$n_1 \quad n_2 \quad n_3$$

Termination

Theorem
The unification algorithm is terminating for all inputs.

Proof.
To every equation system E, we associate:

- n_1: the number of variables in E which are not solved,
- n_2: the size of E,
- n_3: the number of equations of the form $t \stackrel{?}{=} x$ in E.

We then have

	n_1	n_2	n_3
Delete	$\geqslant$	$>$	

Termination

Theorem
The unification algorithm is terminating for all inputs.

Proof.
To every equation system E, we associate:

- n_1: the number of variables in E which are not solved,
- n_2: the size of E,
- n_3: the number of equations of the form $t \stackrel{?}{=} x$ in E.

We then have

	n_1	n_2	n_3
Delete	$\geqslant$	$>$	
Decompose	$\geqslant$	$>$	

Termination

Theorem
The unification algorithm is terminating for all inputs.

Proof.
To every equation system E, we associate:

- n_1: the number of variables in E which are not solved,
- n_2: the size of E,
- n_3: the number of equations of the form $t \stackrel{?}{=} x$ in E.

We then have

	n_1	n_2	n_3
Delete	$\geqslant$	$>$	
Decompose	$\geqslant$	$>$	
Orient	$\geqslant$	$=$	$>$

Termination

Theorem
The unification algorithm is terminating for all inputs.

Proof.
To every equation system E, we associate:

- n_1: the number of variables in E which are not solved,
- n_2: the size of E,
- n_3: the number of equations of the form $t \stackrel{?}{=} x$ in E.

We then have

	n_1	n_2	n_3
Delete	$\geqslant$	$>$	
Decompose	$\geqslant$	$>$	
Orient	$\geqslant$	$=$	$>$
Eliminate	$>$		

Composing substitutions

Recall that σ is a partial function from variables to terms.

Composing substitutions

Recall that σ is a partial function from variables to terms.

By convention, we can suppose that it is a total function by declaring that

$$\sigma(x) = x$$

for $x \notin \mathsf{dom}(\sigma)$.

Composing substitutions

Recall that σ is a partial function from variables to terms.

By convention, we can suppose that it is a total function by declaring that

$$\sigma(x) = x$$

for $x \notin \mathsf{dom}(\sigma)$.

Given two substitution σ and τ, we have a **composite** substitution defined by

$$(\tau \circ \sigma)(x) = \tau(\sigma(x))$$

Renamings

A substitution σ is a **renaming** when

- $\sigma(x)$ is a variable for every variable x,
- $\sigma(x) = \sigma(y)$ implies $x = y$.

Renamings

A substitution σ is a **renaming** when

- $\sigma(x)$ is a variable for every variable x,
- $\sigma(x) = \sigma(y)$ implies $x = y$.

In particular, we have the **identity** substitution id defined by

$$\mathrm{id}(x) = x$$

Ordering unifiers

It can be noticed that if σ is a solution of E and τ is an arbitrary substitution then $\tau \circ \sigma$ is also a solution of E.

Ordering unifiers

It can be noticed that if σ is a solution of E and τ is an arbitrary substitution then $\tau \circ \sigma$ is also a solution of E.

We say that σ is **more general** than σ'

$$\sigma \preceq \sigma'$$

when there exists τ such that $\sigma' = \tau \circ \sigma$.

Ordering unifiers

Lemma
The relation $\preceq$ is a preorder.

Proof.
We have

- *Reflexivity.* We have $\sigma \preceq \sigma$ since $\sigma = \mathsf{id} \circ \sigma$.

Ordering unifiers

Lemma
The relation $\preceq$ is a preorder.

Proof.
We have

- *Reflexivity*. We have $\sigma \preceq \sigma$ since $\sigma = \mathsf{id} \circ \sigma$.
- *Transitivity*. Suppose $\sigma \preceq \sigma' \preceq \sigma''$. We have

$$\sigma' = \tau \circ \sigma \qquad \text{and} \qquad \sigma'' = \tau' \circ \sigma'$$

therefore

$$\sigma'' = \tau' \circ \sigma' = \tau' \circ (\tau \circ \sigma) = (\tau' \circ \tau) \circ \sigma$$

□

Ordering unifiers

Is $\preceq$ antisymmetric?

Ordering unifiers

Is $\preceq$ antisymmetric? No.

Ordering unifiers

Is $\preceq$ antisymmetric? No.

Take $\sigma(x) = y$ and $\sigma(y) = x$. We have

- $\mathsf{id} \preceq \sigma$ since $\sigma = \sigma \circ \mathsf{id}$,

Ordering unifiers

Is $\preceq$ antisymmetric? No.

Take $\sigma(x) = y$ and $\sigma(y) = x$. We have

- $\mathsf{id} \preceq \sigma$ since $\sigma = \sigma \circ \mathsf{id}$,
- $\sigma \preceq \mathsf{id}$ since $\mathsf{id} = \sigma \circ \sigma$.

Ordering unifiers

Is $\preceq$ antisymmetric? No.

Take $\sigma(x) = y$ and $\sigma(y) = x$. We have

- $\mathsf{id} \preceq \sigma$ since $\sigma = \sigma \circ \mathsf{id}$,
- $\sigma \preceq \mathsf{id}$ since $\mathsf{id} = \sigma \circ \sigma$.

Lemma
Two substitutions σ and τ are such that $\sigma \preceq \tau$ and $\tau \preceq \sigma$ if and only if they differ by renamings only.

Most general unifiers

A **most general unifier** for E is a solution which is minimal wrt $\preceq$.

Most general unifiers

A **most general unifier** for E is a solution which is minimal wrt $\preceq$.

Theorem
The unification algorithm computes a most general unifier.

A last example

For instance,

$$\{g(x, y) \stackrel{?}{=} g(y, f(z))\}$$

A last example

For instance,

$$\{g(x, y) \stackrel{?}{=} g(y, f(z))\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} y, y \stackrel{?}{=} f(z)\}$$

A last example

For instance,

$$\{g(x,y) \stackrel{?}{=} g(y,f(z))\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} y, y \stackrel{?}{=} f(z)\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} f(z), y \stackrel{?}{=} f(z)\}$$

A last example

For instance,

$$\{g(x,y) \stackrel{?}{=} g(y,f(z))\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} y, y \stackrel{?}{=} f(z)\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} f(z), y \stackrel{?}{=} f(z)\}$$

The most general unifier is thus

$$\sigma(x) = f(z) \qquad\qquad \sigma(y) = f(z)$$

A last example

For instance,

$$\{g(x,y) \neq g(y,f(z))\} \quad \rightsquigarrow \quad \{x \neq y, y \neq f(z)\} \quad \rightsquigarrow \quad \{x \neq f(z), y \neq f(z)\}$$

The most general unifier is thus

$$\sigma(x) = f(z) \qquad \sigma(y) = f(z)$$

Another most general unifier is thus

$$\sigma(x) = f(x) \qquad \sigma(y) = f(x)$$

A last example

For instance,

$$\{g(x,y) \stackrel{?}{=} g(y,f(z))\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} y, y \stackrel{?}{=} f(z)\} \quad \rightsquigarrow \quad \{x \stackrel{?}{=} f(z), y \stackrel{?}{=} f(z)\}$$

The most general unifier is thus

$$\sigma(x) = f(z) \qquad \sigma(y) = f(z)$$

Another most general unifier is thus

$$\sigma(x) = f(x) \qquad \sigma(y) = f(x)$$

A non-minimal solution is

$$\sigma(x) = f(f(a)) \qquad \sigma(y) = f(f(a))$$