Linear Logic and Naive Set Theory

$\sim$ *Make our garden grow* $\sim$

Kazushige Terui

terui@nii.ac.jp

National Institute of Informatics

Fundamental question

- Contraction inference:

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

  "You can use your hypothesis as many times as you like."
- Quite natural and inevitable in reasoning.
- Why then do you study logics without contraction?

Possible reasons

- To understand contraction better.
  (Contraction is available for closed Π_1 provable formulas in 2nd order BCI, etc.)
- To make logic constructive. In BCK,

$$\text{Excluded middle} = \text{Contraction} + \neg\neg A \to A.$$

- Applications in linguistics etc.
- To save naive comprehension in set theory.

Cut-Elimination

- Cut inference: Generalization of *modus ponens*

$$\frac{\Gamma_1 \vdash A \quad A, \Gamma_2 \vdash C}{\Gamma_1, \Gamma_2 \vdash C}$$

- May introduce redundancy:

$$\dfrac{\dfrac{\dfrac{\vdots\ \pi_1}{\vdash A} \quad \dfrac{\vdots\ \pi_2}{\vdash B}}{\vdash A \wedge B} \qquad \dfrac{\dfrac{\vdots\ \pi_3}{A \vdash C}}{A \wedge B \vdash C}}{\vdash C}$$

- Cut-Elimination Theorem (Genten 1934): There is a concrete procedure to eliminate all cuts from a given proof in sequent calculus.

$$\dfrac{\dfrac{\dfrac{\vdots\ \pi_1}{\vdash A} \quad \dfrac{\vdots\ \pi_2}{\vdash B}}{\vdash A \wedge B} \qquad \dfrac{\dfrac{\vdots\ \pi_3}{A \vdash C}}{A \wedge B \vdash C}}{\vdash C} \quad \Longrightarrow \quad \dfrac{\dfrac{\vdots\ \pi_1}{\vdash A} \qquad \dfrac{\vdots\ \pi_3}{A \vdash C}}{\vdash C}$$

Proofs-as-Programs correspondence

- Formulas = Types (Specifications)
- Proofs = Programs (with Verifications)
- Cut-elimination = Computation
- "A logic without cut-elimination is like a car without an engine." (Jean-Yves Girard)

Feasibility

- A useful program must be feasible (executable in, say, polynomial time).
- Unrestricted use of contraction leads to exponential explosion of cut-elimination (=computation).

$$\dfrac{\begin{array}{c}\vdots\ \pi_1\\ A\vdash B\end{array} \qquad \dfrac{\begin{array}{c}\vdots\ \pi_2\\ B,B\vdash C\end{array}}{B\vdash C}}{A\vdash C} \quad\Longrightarrow\quad \dfrac{\dfrac{\begin{array}{c}\vdots\ \pi_1\\ A\vdash B\end{array} \qquad \dfrac{\begin{array}{c}\vdots\ \pi_1\\ A\vdash B\end{array} \qquad \begin{array}{c}\vdots\ \pi_2\\ B,B\vdash C\end{array}}{B,A\vdash C}}{A,A\vdash C}}{A\vdash C}$$

Contraction has to be restricted

Contraction is

- Perfectly sound in reasoning
- Problematic in computation.
- "A logic with untamed contraction is like a car with a rocket engine."

Naive set theory

- Naive comprehension principle: For any property $A(x)$ there exists a set $\{x|A(x)\}$ such that for any t

$$t \in \{x|A(x)\} \iff A(t)$$

- Intuitive and powerful.
- Compatible with cut-elimination procedure.
- Inconsistent.

Russell's paradox $\Rightarrow$ Contradiction

- Let $R = \{x | x \notin x\}$ and $A \equiv R \in R$. Then $A \vdash \neg A$ and $\neg A \vdash A$.

$$\cfrac{\cfrac{\cfrac{A \vdash \neg A \qquad \cfrac{\overline{A \vdash A}}{\neg A, A \vdash}}{A, A \vdash}}{A \vdash}\,(Contr) \qquad \cfrac{\cfrac{\neg A \vdash A \qquad \cfrac{\overline{A \vdash A}}{\neg A, A \vdash}}{\neg A, \neg A \vdash}}{\neg A \vdash}\,(Contr)}{\vdash}$$

- It requires of contraction to derive contradiction from the paradox.
- Naive comprehension is consistent when contraction is restricted in the underlying logic (Grishin 74).

Naive set theories with restricted contraction

- Grishin's set theory (1974),
- BCK set theory (White 1987, Komori 1989),
- Light linear set theory (Girard 1998)
- Light affine set theory (Terui 2001),
- Elementary affine set theory.

BCK set theory

- Terms: x, $\{x|A\}$
  (when x a variable, A a formula.)
- Formulas: $t \in u$, $A \multimap B$, $\forall x.A$
  (when t, u terms, A, B formulas, x a variable.)
- Axioms and inference rules:

$$(A \multimap B) \multimap ((C \multimap A) \multimap (C \multimap B)) \qquad A \multimap (B \multimap A)$$

$$(A \multimap (B \multimap C)) \multimap (B \multimap (A \multimap C)) \qquad \forall x A \multimap A[t/x]$$

$$\forall x(A \multimap B) \multimap (A \multimap \forall x B) \quad \text{(x is not free in A.)}$$

$$\frac{A \quad A \multimap B}{B} \qquad \frac{A}{\forall x A}$$

$$A[t/x] \multimap t \in \{x|A\} \qquad t \in \{x|A\} \multimap A[t/x]$$

Sequent calculus for BCK set theory

Identity and Cut:

$$\frac{}{A \vdash A}\ (Id) \qquad \frac{\Gamma_1 \vdash A \quad A, \Gamma_2 \vdash C}{\Gamma_1, \Gamma_2 \vdash C}\ (Cut)$$

Weakening:

$$\frac{\Gamma \vdash C}{A, \Gamma \vdash C}\ (Weak)$$

Implication:

$$\frac{\Gamma_1 \vdash A \quad B, \Gamma_2 \vdash C}{A \multimap B, \Gamma_1, \Gamma_2 \vdash C}\ (\multimap l) \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap B}\ (\multimap r)$$

Set Quantifiers:

$$\frac{A[t/x], \Gamma \vdash C}{\forall x.A, \Gamma \vdash C}\ (\forall l) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ (\forall r),\ x \text{ is not free in } \Gamma$$

Comprehension:

$$\frac{A[t/x], \Gamma \vdash C}{t \in \{x|A\}, \Gamma \vdash C}\ (\in l) \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash t \in \{x|A\}}\ (\in r)$$

Defined Connectives

$$
\begin{array}{rcl}
A \otimes B & \equiv & \forall x.((A \multimap B \multimap t_0 \in x) \multimap t_0 \in x); \\
A \oplus B & \equiv & \forall x.((A \multimap t_0 \in x) \multimap (B \multimap t_0 \in x) \multimap t_0 \in x); \\
\mathbf{0} & \equiv & \forall x. t_0 \in x; \\
\exists y.A & \equiv & \forall x.(\forall y.(A \multimap t_0 \in x) \multimap t_0 \in x),
\end{array}
$$

where t_0 is a fixed closed term and x is a fresh variable.

$A \multimap B \multimap A \otimes B$	$(A \multimap B \multimap C) \multimap (A \otimes B \multimap C)$
$A \multimap A \oplus B$	$(A \multimap C) \multimap (B \multimap C) \multimap (A \oplus B \multimap C)$
$A \multimap \neg A \multimap \mathbf{0}$	$\mathbf{0} \multimap A$
$A[t/x] \multimap \exists x.A$	$A \multimap C$ implies $(\exists x.A) \multimap C$ if $x \notin FV(C)$.

Cut-elimination for BCK set theory

Principal cut for naive comprehension:

$$\dfrac{\dfrac{\Gamma \vdash A[t/x]}{\Gamma \vdash t \in \{x|A\}} \quad \dfrac{A[t/x], \Delta \vdash C}{t \in \{x|A\}, \Delta \vdash C}}{\Gamma, \Delta \vdash C} \implies \dfrac{\Gamma \vdash A[t/x] \quad A[t/x], \Delta \vdash C}{\Gamma, \Delta \vdash C}$$

- Elimination of a principal cut always reduces the size of a proof.
- Cut-elimination can be done in linear steps (in terms of proofnets).

Consequences of cut-elimination

- Consistency: BCK set theory is provably consistent (in contrast to the alleged consistency of ZF).
- Disjunction property: If $A \oplus B$ is provable, then either A or B is provable.
- Existential property: If $\exists x.A$ is provable, then $A[t/x]$ is provable for some term t.
- Proof: A cut-free proof of $\exists x.A \equiv \forall x.(\forall y.(A \multimap t_0 \in x) \multimap t_0 \in x)$ looks like:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots \\ \vdash A[u/y]\end{array} \quad t_0 \in x \vdash t_0 \in x}{A[u/y] \multimap t_0 \in x \vdash t_0 \in x}}{\forall y.(A \multimap t_0 \in x) \vdash t_0 \in x}}{\vdash \forall y.(A \multimap t_0 \in x) \multimap t_0 \in x}}{\vdash \forall x.(\forall y.(A \multimap t_0 \in x) \multimap t_0 \in x)}
$$

Identity of BCK sets

- **Equality**: $t = u \equiv \forall x.(t \in x \multimap u \in x)$
- BCK set theory proves
  1. $t = t$.
  2. $t = u \multimap (A[t/x] \multimap A[u/x])$.
  3. $t = u \multimap u = t$.
  4. $t = u \otimes u = r \multimap t = r$.
  5. $t = u \multimap t = u \otimes t = u$.
     (take $A \equiv (t = x \otimes t = x)$ and apply 2, 1.)
- **Proposition**: $t = u$ is provable iff t and u are syntactically identical.
- In particular, $\{x|A \oplus B\} = \{x|B \oplus A\}$ is not provable.

Basic constructions

$$\emptyset \equiv \{x|x \neq x\}; \qquad \{t\} \equiv \{x|x = t\};$$

$$\{t, u\} \equiv \{x|x = t \oplus x = u\};$$

$$t \cup u \equiv \{x|x \in t \oplus x \in u\}; \qquad \langle t, u\rangle \equiv \{\{t\}, \{t, u\}\};$$

BCK set theory proves

1. $t \not\in \emptyset$.
2. $t \in \{u\} \multimapboth t = u$.
3. $t \in \{u, v\} \multimapboth t = u \oplus t = v$.
4. $\langle t, u\rangle = \langle r, s\rangle \multimapboth t = r \otimes u = s$.
   (The standard proof applies, since contraction is available for equational formulas.)

Axioms of ZF (1)

- Proposition(Grishin 74): Extensionality principle

$$\forall x.(x \in t \multimapboth x \in u) \multimap t = u$$

  implies Contraction. Thus BCK set theory $+$ Extensionality is inconsistent.

- Proof. We have contraction for equational formulas. So it suffices to show that every formula A is equivalent to an equational formula $t = u$.

- Let $t \equiv \{x | x = x\}$ and $u \equiv \{x | x = x \otimes A\}$.
  $A \multimapboth (x = x \multimapboth x = x \otimes A)$, x not free in A
  $A \multimapboth (x \in t \multimapboth x \in u)$
  $A \multimapboth \forall x.(x \in t \multimapboth x \in u)$
  $A \multimapboth t = u$

- A weaker form of extensionality is also inconsistent. See [?].

Axioms of ZF (2)

- Constructive axioms: Ok, but uniqueness is not guaranteed.
- Separation, Replacement: Part of naive comprehension.
- Regularity: Inconsistent. Let $V \equiv \{x|x = x\}$. Then

$$\cdots V \in V \in V$$

- Infinity: Provable, but “infinity” no more means infinity...
- Let $suc(t) \equiv t \cup \{t\}$ and

$$N' \equiv \{n|\forall\alpha.(\emptyset \in \alpha \otimes \forall x.(x \in \alpha \multimap suc(x) \in \alpha)) \multimap n \in \alpha\}$$

Then $\emptyset, suc(\emptyset) \in N'$ holds, but $suc(suc(\emptyset)) \in N'$ does not hold.

Booleans in BCK set theory

$$
\begin{aligned}
\mathsf{true} &\equiv \emptyset \\
\mathsf{false} &\equiv \{\emptyset\} \\
\mathsf{B} &\equiv \{x|x = \mathsf{true} \oplus x = \mathsf{false}\} \\
neg(x,y) &\equiv (x = \mathsf{true} \otimes y = \mathsf{false}) \oplus (x = \mathsf{false} \otimes y = \mathsf{true}) \\
disj(x,y,z) &\equiv (x = \mathsf{true} \otimes z = \mathsf{true}) \oplus (x = \mathsf{false} \otimes y = z)
\end{aligned}
$$

We have contraction for booleans: $x \in \mathsf{B} \multimap x \in \mathsf{B} \otimes x \in \mathsf{B}$.

Theorem: For any boolean circuit $C(x_1, \ldots, x_n)$, there exists a formula $F_C(x_1, \ldots, x_n, y)$ such that it represents C and

$$\vdash \forall x_1, \ldots, x_n \in \mathsf{B}.\exists y \in \mathsf{B}.F_C(x_1, \ldots, x_n, y)$$

has a proof of size $O(|C|)$ in BCK set theory.

P-completeness of Disjunction Property

Disjunction Property Problem: Given a proof of $\vdash C \oplus D$, determine which one of $\vdash C$ or $\vdash D$ holds.

Theorem: DPP is P-complete (under logspace-reducibility).

Proof:
(In P) By cut-elimination (in quadratic time).
(P-hard) Reduction of Circuit Value Problem; given a circuit C and truth values $b_1, \dots, b_n$, construct a proof of

$$\vdash A_C(b_1, \dots, b_n, \mathsf{true}) \oplus A_C(b_1, \dots, b_n, \mathsf{false})$$

in logspace, by noting that

$\exists y \in \mathsf{B}.A_C(\vec{b}, y) \multimapboth A_C(\vec{b}, \mathsf{true}) \oplus A_C(\vec{b}, \mathsf{false})$.

Fixpoint theorems

Fixpoint theorem 1: For every formula $A(\alpha)$ with a propositional variable α, there exists a formula B such that $B \multimapboth A(B)$.

Proof: Let $B \equiv \{x|A(x \in x)\} \in \{x|A(x \in x)\}$.

Fixpoint theorem 2: For every formula $A(x, y)$ with term variables x, y, there exists a term (set) f such that $x \in f \multimapboth A(x, f)$.

Proof: Let

$$\begin{aligned} s &\equiv \{z \mid \exists u \exists v (z = \langle u, v\rangle \otimes A[\{w \mid \langle w, v\rangle \in v\}/y, u/x])\}; \\ f &\equiv \{w \mid \langle w, s\rangle \in s\}, \end{aligned}$$

where u, v and w are fresh variables.

Natural numbers (1)

- Numerals:

$$\underline{0} \equiv \emptyset, \qquad S(t) \equiv \langle \emptyset, t \rangle, \qquad \underline{n} \equiv S^n(\underline{0}).$$

- Inequality: $\langle x, y \rangle \in$ leq $\circ\!\!-\!\!\circ\ x = y \oplus \exists y'(\langle x, y' \rangle \in$ leq $\otimes\ y = S(y'))$
- The set of natural numbers:
  $x \in N \circ\!\!-\!\!\circ\ x = \underline{0} \oplus \exists y \in N. x = S(y)$
- **Proposition**: BCK set theory proves
  1. $S(t) \neq \underline{0}$.
  2. $S(t) = S(u) \circ\!\!-\!\!\circ\ t = u$.
- **Proposition**: $\underline{n} \neq \underline{m}$ is provable iff $n \neq m$.
- **Proposition**: $\langle x, \underline{n} \rangle \in$ leq $\circ\!\!-\!\!\circ\ x = \underline{0} \oplus \cdots \oplus x = \underline{n}$ is provable.

Natural Numbers (2)

Proposition: $t \in N$ is provable iff t is a numeral.

Proof:

($\Leftarrow$): By induction on n such that $t \equiv \underline{n}$.

($\Rightarrow$): By induction on the size of term t. If $\vdash t \in N^*$ is provable, then either $\vdash t = \underline{0}$ or $\vdash \exists y \in N^*(t = S(y))$ is provable by DPP. In the former case, $t \equiv \underline{0}$. In the latter case, there is some term u such that $\vdash u \in N^*$ and $\vdash t = S(u)$ are provable by the existential property. Thus $t \equiv S(u)$, and hence the induction hypothesis applies to u, as it means that u is smaller than t. It follows that $u \equiv \underline{m}$ for some $m \in \mathbb{N}$. Therefore $t \equiv \underline{m+1}$.

Addition and multiplication (1)

- Addition:

  $\langle x, y, z\rangle \in \mathsf{add} \multimap (y = \underline{0} \otimes x = z) \oplus \exists y' \exists z' (y = S(y') \otimes z = S(z') \otimes \langle x, y', z'\rangle \in \mathsf{add})$.

- Multiplication: $\langle x, y, z\rangle \in \mathsf{mult} \multimap$

  $(y = \underline{0} \otimes z = \underline{0}) \oplus \exists y' \exists z' (y = S(y') \otimes \langle x, y', z'\rangle \in \mathsf{mult} \otimes \langle z', x, z\rangle \in \mathsf{add})$.

- **Proposition**: BCK set theory proves

  1. $\langle x, \underline{0}, z\rangle \in \mathsf{add} \multimap x = z$.
  2. $\langle x, S(y), z\rangle \in \mathsf{add} \multimap \exists z' (z = S(z') \otimes \langle x, y, z'\rangle \in \mathsf{add})$.
  3. $\langle x, \underline{0}, z\rangle \in \mathsf{mult} \multimap z = \underline{0}$.
  4. $\langle x, S(y), z\rangle \in \mathsf{mult} \multimap \exists z' (\langle z', x, z\rangle \in \mathsf{add} \otimes \langle x, y, z'\rangle \in \mathsf{mult})$.

Addition and multiplication (2)

- Proofs of (1) and (2):

$$\begin{array}{rcl} \langle x, \underline{0}, z\rangle \in \mathsf{add} & \multimap\!\circ & (\underline{0} = \underline{0} \otimes x = z) \oplus \exists y' \exists z' (\underline{0} = S(y') \otimes z = S(z') \otimes \langle x, y', z' \rangle \\ & \multimap\!\circ & x = z \\ \langle x, S(y), z\rangle \in \mathsf{add} & \multimap\!\circ & (S(y) = \underline{0} \otimes x = z) \oplus \exists y' \exists z' (S(y) = S(y') \otimes z = S(z') \otimes \langle x \\ & \multimap\!\circ & \exists z' (z = S(z') \otimes \langle x, y, z' \rangle \in \mathsf{add}) \end{array}$$

- **Proposition**: Let $n + m = k$, $n \cdot m = l$. BCK set theory proves
  1. $\langle \underline{n}, \underline{m}, \underline{k} \rangle \in \mathsf{add}$
  2. $\forall z. \langle \underline{n}, \underline{m}, z \rangle \in \mathsf{add} \multimap z = \underline{k}$
  3. $\langle \underline{n}, \underline{m}, \underline{l} \rangle \in \mathsf{mult}$
  4. $\forall z. \langle \underline{n}, \underline{m}, z \rangle \in \mathsf{mult} \multimap z = \underline{l}$
- Proof: By induction on m.

Embedding classical arithmetic (1)

- **Arithmetical terms**: $x, 0, s(a), a + b, a \cdot b$
- Δ_0 **formulas**:
  $a = b, \neg F, F \wedge G, F \vee G, F \rightarrow G, \exists x \leq a.F, \forall x \leq a.G$
  (where x does not occur in a.)
- Σ_1 **formulas**: $\exists x_1 \cdots \exists x_n.F$ where F is Δ_0.
- Truth values of closed Σ_1 formulas: naturally defined.

Embedding classical arithmetic (2)

- For each arithmetical term a whose variables are from $\vec{x} = x_1, \ldots, x_k$, define a BCK formula $Val_a(\vec{x}, y)$ as follows:

$$
\begin{array}{rcl}
Val_{x_i}(\vec{x}, y) & \equiv & y = x_i, \quad Val_0(\vec{x}, y) \equiv y = \underline{0} \\
Val_{s(a)}(\vec{x}, y) & \equiv & \exists y'.Val_a(\vec{x}, y') \otimes y = S(y') \\
Val_{a+b}(\vec{x}, y) & \equiv & \exists y_1 \exists y_2.Val_a(\vec{x}, y_1) \otimes Val_b(\vec{x}, y_2) \otimes \langle y_1, y_2, y \rangle \in \mathsf{add} \\
Val_{a \cdot b}(\vec{x}, y) & \equiv & \exists y_1 \exists y_2.Val_a(\vec{x}, y_1) \otimes Val_b(\vec{x}, y_2) \otimes \langle y_1, y_2, y \rangle \in \mathsf{mult}
\end{array}
$$

- **Proposition**: For any arithmetical term a and $\vec{m} = m_1, \ldots, m_k$, if the value of $a[\vec{m}/\vec{x}]$ is n, then BCK set theory proves

$$Val_a(\underline{\vec{m}}, \underline{n}) \otimes \forall z.Val_a(\underline{\vec{m}}, z) \multimap z = \underline{n}.$$

Embedding classical arithmetic (3)

- **Proof**: By induction on a.
  - $a \equiv x_i$: $\underline{m_i} = \underline{m_i} \otimes \forall z.z = \underline{m_i} \multimap z = \underline{m_i}$
  - $a \equiv 0$: $\underline{0} = \underline{0} \otimes \forall z.z = \underline{0} \multimap z = \underline{0}$
  - $a \equiv b + c$: when the values of b and c are n_1 and n_2, we have

$$Val_b(\underline{\vec{m}}, \underline{n_1}) \otimes Val_c(\underline{\vec{m}}, \underline{n_2}) \otimes \langle \underline{n_1}, \underline{n_2}, \underline{n} \rangle \in \mathsf{add},$$

from which $Val_a(\underline{\vec{m}}, \underline{n})$ follows. Now, working within BCK set theory, suppose $Val_a(\underline{\vec{m}}, z)$. Then there are y_1, y_2 such that $Val_b(\underline{\vec{m}}, y_1)$, $Val_b(\underline{\vec{m}}, y_2)$ and $\langle y_1, y_2, z \rangle \in \mathsf{add}$. By IH, $y_1 = \underline{n_1}$ and $y_2 = \underline{n_2}$, so $z = \underline{n}$ by what precedes.

Embedding classical arithmetic (4)

- For each Δ_0 formula F whose free variables are from $\vec{x} = x_1, \ldots, x_k$, define a BCK formula $Sat_F(\vec{x})$ as follows:

$$
\begin{array}{rcl}
Sat_{a=b}(\vec{x}) & \equiv & \exists z. Val_a(\vec{x}, z) \otimes Val_b(\vec{x}, z) \\
Sat_{\neg F}(\vec{x}) & \equiv & \neg Sat_F(\vec{x}) \\
Sat_{F \wedge G}(\vec{x}) & \equiv & Sat_F(\vec{x}) \otimes Sat_G(\vec{x}) \\
Sat_{F \vee G}(\vec{x}) & \equiv & Sat_F(\vec{x}) \oplus Sat_G(\vec{x}) \\
Sat_{F \to G}(\vec{x}) & \equiv & Sat_F(\vec{x}) \multimap Sat_G(\vec{x}) \\
Sat_{\exists y \leq a. F}(\vec{x}) & \equiv & \exists z (Val_a(\vec{x}, z) \otimes \exists y (\langle y, z \rangle \in \mathsf{leq} \otimes Sat_F(\vec{x}, y))) \\
Sat_{\forall y \leq a. F}(\vec{x}) & \equiv & \exists z (Val_a(\vec{x}, z) \otimes \forall y (\langle y, z \rangle \in \mathsf{leq} \multimap Sat_F(\vec{x}, y)))
\end{array}
$$

- **Theorem**: For any Δ_0 formula F and $\vec{m} = m_1, \ldots, m_k$,
$F[\vec{m}/\vec{x}]$ is true $\iff$ $Sat_F(\underline{\vec{m}})$ is provable,
$F[\vec{m}/\vec{x}]$ is false $\iff$ $\neg Sat_F(\underline{\vec{m}})$ is provable.

Embedding classical arithmetic (5)

- **Proof**: By induction on F.
  - $F \equiv (a = b)$: If $a[\vec{m}/\vec{x}] = b[\vec{m}/\vec{x}] = n$, we have $Val_a(\underline{\vec{m}}, \underline{n}) \otimes Val_b(\underline{\vec{m}}, \underline{n})$.
    If $a[\vec{m}/\vec{x}] = n_1$, $b[\vec{m}/\vec{x}] = n_2$ and $n_1 \neq n_2$, we have
    $$Val_a(\underline{\vec{m}}, z) \vdash z = \underline{n_1} \text{ and } Val_b(\underline{\vec{m}}, z) \vdash z = \underline{n_2},$$
    from which $Sat_F(\underline{\vec{m}}) \vdash \underline{n_1} = \underline{n_2} \vdash \mathbf{0}$ follows.
  - $F \equiv \neg G$: Immediate.
  - $F \equiv G \wedge H$: The case $F[\vec{m}/\vec{x}]$ true is obvious. If it is false, one of the conjuncts, say $G[\vec{m}/\vec{x}]$, is false. By IH, $\neg Sat_G(\underline{\vec{m}})$ is provable, which implies $\neg(Sat_G(\underline{\vec{m}}) \otimes Sat_H(\underline{\vec{m}}))$.
  - $F \equiv \forall y \leq a.G$: Use $x \leq \underline{n} \multimap x = \underline{0} \oplus \cdots \oplus x = \underline{n}$.

Embedding classical arithmetic (6)

- For each Σ_1 formula F whose free variables are from $\vec{x} = x_1, \ldots, x_k$, define a BCK formula $Sat_F(\vec{x})$ by:

$$Sat_{\exists y.F}(\vec{x}) \equiv \exists y(y \in N \otimes Sat_F(\vec{x}, y)).$$

- **Theorem**: For any Σ_1 formula F and $\vec{m} = m_1, \ldots, m_k$, $F[\vec{m}/\vec{x}]$ is true $\Longleftrightarrow$ $Sat_F(\underline{\vec{m}})$ is provable.
- **Proof**: By induction on F
  $\exists y.F[\vec{m}/\vec{x}]$ is true
  $\Longleftrightarrow$ $F[\vec{m}/\vec{x}, n/y]$ is true for some n
  $\Longleftrightarrow$ $Sat_F(\underline{\vec{m}}, \underline{n})$ and $\underline{n} \in N$ are provable for some n
  $\Longleftrightarrow$ $\exists y(y \in N \otimes Sat_F(\underline{\vec{m}}, y))$ is provable.

Embedding classical arithmetic (7)

- **Corollary**: Every r.e. predicate is weakly numeralwise representable in BCK set theory. Namely, for every r.e. predicate $\psi \subseteq \mathbb{N}$, there exists a formula $A(x)$ such that for any $n \in \mathbb{N}$

$$\psi(n) \iff \vdash A(\underline{n}) \text{ is provable in BCK set theory.}$$

- **Corollary**: BCK set theory is undecidable.
- **Corollary**: For any closed Δ_0 formula F, BCK set theory proves $Sat_F \oplus \neg Sat_F$.
- Question: To what extent we may have excluded middle in BCK set theory? Is the above result related to the availability of contraction for closed provable Π_1 formulas in 2nd order MLL?

Expressivity of BCK set theory

- Definability is rich (as it weakly numeralwise represents all r.e. predicates)
- Computability is too weak (as cut-elimination can be done in linear steps)
- In analogy, BCK set theory corresponds to Robinson's Q in arithmetic. We need to strengthen it to get a computationally more interesting system (like S^1_2, $I\Delta_0 + exp$, $I\Sigma_1$, PA, etc.).
- $\Rightarrow$ Light affine set theory (**LAST**) and Elementary affine set theory (**EAST**).

Background on LAST and EAST (1)

- Light linear logic (**LLL**, Girard 1998): subsystem of linear logic corresponding to polynomial time complexity.
  - Proofs of **LLL** precisely captures the polynomial time functions via the Curry-Howard correspondence.
- Light linear set theory: **LLL**$+$ Naive comprehension.
  - Considered as a basis of "polytime mathematics". But formal justification is not given enough.
  - Complexity is light, but syntax is "heavy".

Background on LAST and EAST (2)

- Intuitionistic light affine logic (**ILAL**, Asperti 1998): Intuitionistic **LLL** $+$ Weakening.
  - Drastic simplification of **LLL** with the same computational power.
  - Set theory has not been developed on it.
- NB. Multiplicative **LLL** is already complete for PTIME (Mairson-Terui, ICTCS 2003)
- Cf. Elementary linear logic (Girard 1998): Subsystem of linear logic corresponding to the elementary recursive functions.

Our contributions

- Light affine set theory (**LAST**): **ILAL**$+$ Naive comprehension.
  - Every provably total function in **LAST** is polynomial time computable and vice versa. $\Rightarrow$ **LAST** as a formalization of polynomial time mathematics.
- Elementary affine set theory (**EAST**): Elementary version of **LAST**.
  - Every provably total function in **EAST** is (Kalmar-) elementary recursive and vice versa.

Elementary affine set theory

- Extend BCK set theory with modally controlled Contraction.
- Contraction inference rule controlled by modality !:

$$\frac{!A, !A, \Gamma \vdash C}{!A, \Gamma \vdash C}$$

- **EAST**: BCK set theory $+$ K-controlled contraction
- K: $!(A \multimap B) \multimap !A \multimap !B$
- In sequent calculus,

$$\frac{A_1, \ldots, A_n \vdash B}{!A_1, \ldots, !A_n \vdash !B}$$

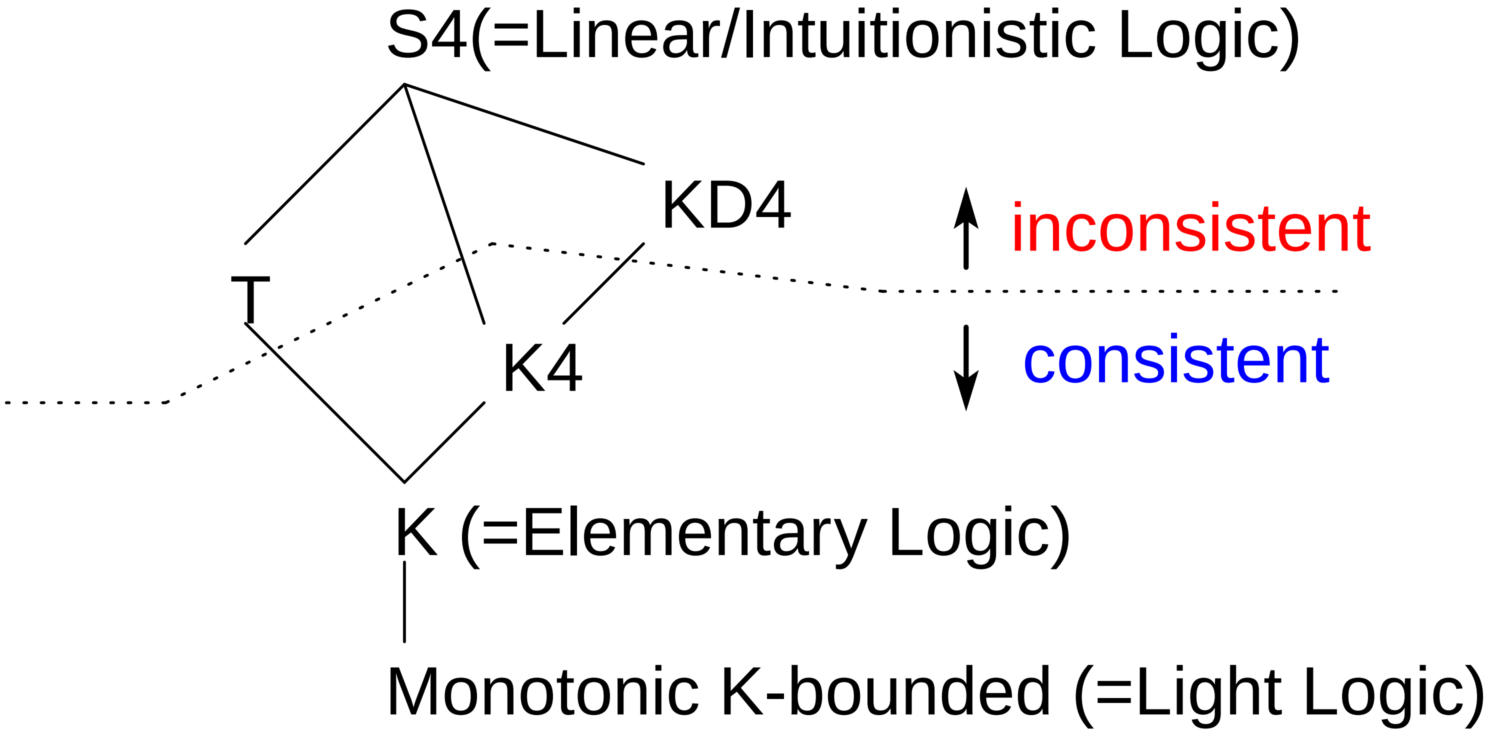
Naive comprehension is inconsistent with T-Contraction

- $T :!A \multimap A$

$$\dfrac{\dfrac{\dfrac{\dfrac{D \vdash !\neg D \qquad \dfrac{\dfrac{\dfrac{!\neg D \vdash D}{\neg D, !\neg D \vdash}}{!\neg D, !\neg D \vdash}\,(T)}{!\neg D \vdash}\,(Contr)}{D \vdash}}{\vdash \neg D}}{\vdash !\neg D} \qquad \dfrac{\dfrac{\dfrac{!\neg D \vdash D}{\neg D, !\neg D \vdash}}{!\neg D, !\neg D \vdash}\,(T)}{!\neg D \vdash}\,(Contr)}{\vdash}$$

- Also inconsistent with $KD4$
- $D :!A \multimap ?A$
- $4 :!A \multimap !!A$

Hierarchy of Naive Set Theories



Expressivity of EAST

Define N by

$$x \in \mathsf{N} \multimapboth \forall \alpha.!\forall y.(y \in \alpha \multimap S(y) \in \alpha) \multimap !(0 \in \alpha \multimap x \in \alpha)$$

A numeric function ϕ is provably total in **EAST** if there is a term f which represents ϕ and for some $d \geq 0$,

$$\vdash \forall x \in \mathsf{N}.!^d(\exists^! y \in \mathsf{N}.\langle x, y \rangle \in f)$$

is provable in **EAST**.

Theorem: ϕ is provably total in **EAST**

$\Longleftrightarrow$ ϕ is an elementary recursive function (i.e. the runtime of ϕ is bounded by a tower of exponentials).

Light affine set theory

- **LAST**: BCK set theory $+$ monotonic K-bounded Contraction
- Multi-modal system with two modalities $\S, !$, where $!$ controls Contraction.
- K: $\S(A \multimap B) \multimap \S A \multimap \S B$
- K-boundedness: $!A \multimap \S A$
- Monotonicity: $A \vdash B$ implies $!A \vdash !B$.

$$\frac{B \vdash A}{!B \vdash !A}\ (!),\quad B \text{ can be absent.} \qquad \frac{\Gamma, \Delta \vdash A}{!\Gamma, \S\Delta \vdash \S A}\ (\S)$$

$$\frac{!A, !A, \Gamma \vdash C}{!A, \Gamma \vdash C}\ (Contr)$$

Natural Numbers in LAST

Define

$$\mathsf{N} \;\equiv\; \{x | \forall \alpha . ! \forall y (y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap x \in \alpha)\}.$$

Then **LAST** proves

1. $\underline{0} \in \mathsf{N}$.
2. $t \in \mathsf{N} \multimap S(t) \in \mathsf{N}$.

LAST proves $t \in \mathsf{N}$ iff $t \equiv \underline{n}$ for some $n \in N$.

Proof of “0 is a natural number”

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\underline{0} \in \alpha \vdash \underline{0} \in \alpha}{\vdash \underline{0} \in \alpha \multimap \underline{0} \in \alpha}}{\vdash \S(\underline{0} \in \alpha \multimap \underline{0} \in \alpha)}}{!\forall y(y \in \alpha \multimap S(y) \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap \underline{0} \in \alpha)}}{\vdash !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap \underline{0} \in \alpha)}}{\vdash \forall \alpha . !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap \underline{0} \in \alpha)}}{\vdash \underline{0} \in \mathsf{N}}
$$

Proof of “2 is a natural number”

$$
\begin{array}{c}
\hline
\underline{0} \in \alpha \multimap \underline{S(0)} \in \alpha, \underline{S(0)} \in \alpha \multimap \underline{S(S(0))} \in \alpha \vdash \underline{0} \in \alpha \multimap \underline{S(S(0))} \in \alpha \\
\hline\hline
\forall y(y \in \alpha \multimap S(y) \in \alpha), \forall y(y \in \alpha \multimap S(y) \in \alpha) \vdash \underline{0} \in \alpha \multimap \underline{S(S(0))} \in \alpha \\
\hline
!\forall y(y \in \alpha \multimap S(y) \in \alpha), !\forall y(y \in \alpha \multimap S(y) \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap \underline{S(S(0))} \in \alpha \\
\hline
!\forall y(y \in \alpha \multimap S(y) \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap \underline{S(S(0))} \in \alpha) \\
\hline
\vdash !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap \underline{S(S(0))} \in \alpha) \\
\hline
\vdash \forall \alpha.!\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap \underline{S(S(0))} \in \alpha) \\
\hline
\vdash \underline{S(S(0))} \in \mathsf{N}
\end{array}
$$

Proof of “Successor of a natural number is a natural number”

$$
\begin{array}{c}
t \in \alpha \vdash t \in \alpha \qquad S(t) \in \alpha \vdash S(t) \in \alpha \\
\hline
t \in \alpha \multimap S(t) \in \alpha, t \in \alpha \vdash S(t) \in \alpha \\
\hline
\underline{0} \in \alpha \vdash \underline{0} \in \alpha \qquad \forall y(y \in \alpha \multimap S(y) \in \alpha), t \in \alpha \vdash S(t) \in \alpha \\
\hline
\underline{0} \in \alpha, \forall y(y \in \alpha \multimap S(y) \in \alpha), \underline{0} \in \alpha \multimap t \in \alpha \vdash S(t) \in \alpha \\
\hline
\forall y(y \in \alpha \multimap S(y) \in \alpha), \underline{0} \in \alpha \multimap t \in \alpha \vdash \underline{0} \in \alpha \multimap S(t) \in \alpha \\
\hline
!\forall y(y \in \alpha \multimap S(y) \in \alpha), \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap S(t) \in \alpha) \\
\hline\hline
!\forall y(y \in \alpha \multimap S(y) \in \alpha)^2, !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap S(t) \in \\
\hline\hline
!\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap S(t) \in \\
\hline\hline
\forall \alpha. !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \forall \alpha. !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap S(\\
\hline\hline
t \in \mathsf{N} \vdash S(t) \in \mathsf{N}
\end{array}
$$

Light Induction

The Light induction principle

$$\frac{\vdash A(\underline{0}) \quad B, A(y)) \vdash A(S(y))}{!B, \vdash \forall x \in \mathsf{N}.\S A(x)}$$

is available in **LAST**.

Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{B, A[y/x] \vdash A[S(y)/x]}{B, y \in \{x|A\} \vdash S(y) \in \{x|A\}}}{B \vdash \forall y(y \in \{x|A\} \multimap S(y) \in \{x|A\})}}{!B \vdash !\forall y(y \in \{x|A\} \multimap S(y) \in \{x|A\})} \quad \dfrac{\dfrac{\dfrac{\Gamma \vdash A[\underline{0}/x]}{\Gamma \vdash \underline{0} \in \{x|A\}} \quad \dfrac{A[t/x] \vdash A[t/x]}{t \in \{x|A\} \vdash A[t/x]}}{\Gamma, \underline{0} \in \{x|A\} \multimap t \in \{x|A\} \vdash A[t/x]}}{\S\Gamma, \S(\underline{0} \in \{x|A\} \multimap t \in \{x|A\}) \vdash \S A[t/x]}}{\dfrac{\S\Gamma, !B, !\forall y(y \in \{x|A\} \multimap S(y) \in \{x|A\}) \multimap \S(\underline{0} \in \{x|A\} \multimap t \in \{x|A\}) \vdash \S A[t/x]}{\S\Gamma, !B, \forall \alpha.!\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \S A[t/x]}}}{\S\Gamma, !B, t \in \mathsf{N} \vdash \S A[t/x]}$$

Totality of addition

Prove

(i) $\vdash \forall x \in \mathsf{N}.\exists^! z \in \mathsf{N}(\langle x, \underline{0}, z\rangle \in \mathsf{add})$ and

(ii) $\forall x \in \mathsf{N}.\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{add}) \vdash \forall x \in \mathsf{N}.\exists^! z \in \mathsf{N}(\langle x, S(y), z\rangle \in \mathsf{add})$.

By light induction on y,

(*) $y \in \mathsf{N} \vdash \S(\forall x \in \mathsf{N}.\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{add}))$.

Therefore,

$$\forall x \in \mathsf{N}.\forall y \in \mathsf{N}.\S\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{add}).$$

Totality of multiplication

We have $\langle x, y, z\rangle \in \mathsf{mult}, \langle z, x, w\rangle \in \mathsf{add} \vdash \langle x, \underline{S}(y), w\rangle \in \mathsf{mult}$.

$\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{mult}), \forall z \in \mathsf{N}.\exists^! w \in \mathsf{N}(\langle z, x, w\rangle \in \mathsf{add})$
$\qquad \vdash \exists^! w \in \mathsf{N}(\langle x, \underline{S}(y), w\rangle \in \mathsf{mult})$.

$\S\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{mult}), \S\forall z \in \mathsf{N}.\exists^! w \in \mathsf{N}(\langle z, x, w\rangle \in \mathsf{add})$
$\qquad \vdash \S\exists^! w \in \mathsf{N}(\langle x, \underline{S}(y), w\rangle \in \mathsf{mult})$.

By (*),

$x \in \mathsf{N}, \S\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{mult}) \vdash \S\exists^! w \in \mathsf{N}(\langle x, S(y), w\rangle \in \mathsf{mult})$.

On the other hand,

$\vdash \S\exists^! z \in \mathsf{N}(\langle x, \underline{0}, z\rangle \in \mathsf{mult})$

By Light Induction,

$$!x \in \mathsf{N}, y \in \mathsf{N} \vdash \S^2\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{mult}).$$

Hence,

$$\forall x \in \mathsf{N}.\forall y \in \mathsf{N}.\S\S\S\exists^! z \in \mathsf{N}(\langle x, y, z\rangle \in \mathsf{mult}).$$

Exponentiation is not total

Define by fixpoint: $\langle y, z\rangle \in \mathsf{exp} \multimap (y = \underline{0} \otimes z = \underline{1}) \oplus$
$\exists y' \exists x (y = S(y') \otimes \langle y', x\rangle \in \mathsf{exp} \otimes \langle x, x, z\rangle \in \mathsf{add})$.
(based on:

$$
\begin{array}{rcl}
2^0 & = & 1 \\
2^{n+1} & = & 2^n + 2^n\ )
\end{array}
$$

Then we have

(i) $\vdash \exists^! z \in \mathsf{N}(\langle \underline{0}, z\rangle \in \mathsf{exp})$

(ii) $\exists^! z \in \mathsf{N}.\S\S(\langle y, z\rangle \in \mathsf{exp}) \vdash \S\S\exists^! z \in \mathsf{N}(\langle S(y), z\rangle \in \mathsf{exp})$.

But light induction cannot be applied!

Expressivity of **LAST**

The set of 0-1 words: $x \in \mathsf{W} \circ\!\!-\!\!\circ$

$\forall \alpha.!\forall y.(y \in \alpha \multimap S_0(y) \in \alpha) \multimap !\forall y.(y \in \alpha \multimap S_1(y) \in \alpha) \multimap \S(\underline{\epsilon} \in \alpha \multimap x \in \alpha)$,
where $\underline{\epsilon} \equiv \emptyset$ and $S_i(t) \equiv \langle \underline{i}, t \rangle$ for $i = 0, 1$.

A function ϕ over $\{0, 1\}^*$ is provably total in **LAST** if there is a term f which represents ϕ and for some $d \geq 0$,

$$\forall x \in \mathsf{W}.\S^d(\exists^! y \in \mathsf{W}.\langle x, y \rangle \in f)$$

is provable in **LAST**.

Theorem: If ϕ is a polynomial time function, then ϕ is provably total in **LAST**.

Interpretation of LAST proofs as λ terms

$$\frac{}{\mathtt{x}:A \vdash \mathtt{x}:A}\ Id \qquad \frac{\Gamma_1 \vdash \mathtt{N}:A \quad \mathtt{x}:A,\Gamma_2 \vdash \mathtt{M}:C}{\Gamma_1,\Gamma_2 \vdash \mathtt{M[N/x]}:C}\ Cut$$

$$\frac{\Gamma \vdash \mathtt{M}:C}{x:A,\Gamma \vdash \mathtt{M}:C}\ Weak \qquad \frac{\mathtt{x}:!A,\mathtt{y}:!A,\Gamma \vdash \mathtt{M}:C}{\mathtt{z}:!A,\Gamma \vdash \mathtt{M[z/x,z/y]}:C}\ Cntr$$

$$\frac{\Gamma_1 \vdash \mathtt{N}:A_1 \quad \mathtt{x}:A_2,\Gamma_2 \vdash \mathtt{M}:C}{\Gamma_1,\mathtt{y}:A_1 \multimap A_2,\Gamma_2 \vdash \mathtt{M[yN/x]}:C}\ \multimap l \qquad \frac{\mathtt{x}:A_1,\Gamma \vdash \mathtt{M}:A_2}{\Gamma \vdash \lambda\mathtt{x.M}:A_1 \multimap A_2}\ \multimap r$$

$$\frac{\mathtt{x}:B \vdash \mathtt{M}:A}{\mathtt{x}:!B \vdash \mathtt{M}:!A}\ ! \qquad \frac{\Gamma,\Delta \vdash \mathtt{M}:A}{!\Gamma,\S\Delta \vdash \mathtt{M}:\S A}\ \S$$

$$\frac{\mathtt{x}:A[u/x],\Gamma \vdash \mathtt{M}:C}{\mathtt{x}:\forall x.A,\Gamma \vdash \mathtt{M}:C}\ \forall l \qquad \frac{\Gamma \vdash \mathtt{M}:A}{\Gamma \vdash \mathtt{M}:\forall x.A}\ \forall r$$

$$\frac{\mathtt{x}:A[u/x],\Gamma \vdash \mathtt{M}:C}{\mathtt{x}:u \in \{x|A\},\Gamma \vdash \mathtt{M}:C}\ \in l \qquad \frac{\Gamma \vdash \mathtt{M}:A[u/x]}{\Gamma \vdash \mathtt{M}:u \in \{x|A\}}\ \in r$$

Example of Proof Interpretation

$$
\dfrac{
  \dfrac{0 \in \alpha \vdash 0 \in \alpha
    \qquad
    \dfrac{\dfrac{t \in \alpha \vdash t \in \alpha \qquad S(t) \in \alpha \vdash S(t) \in \alpha}{t \in \alpha \multimap S(t) \in \alpha, t \in \alpha \vdash S(t) \in \alpha}}{\forall y(y \in \alpha \multimap S(y) \in \alpha), t \in \alpha \vdash S(t) \in \alpha}}
  {\underline{0} \in \alpha, \forall y(y \in \alpha \multimap S(y) \in \alpha), \underline{0} \in \alpha \multimap t \in \alpha \vdash S(t) \in \alpha}
}{\forall y(y \in \alpha \multimap S(y) \in \alpha), \underline{0} \in \alpha \multimap t \in \alpha \vdash \underline{0} \in \alpha \multimap S(t) \in \alpha}
$$

$$
\dfrac{}{!\forall y(y \in \alpha \multimap S(y) \in \alpha), \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap S(t) \in \alpha)}
$$

$$
!\forall y(y \in \alpha \multimap S(y) \in \alpha)^2, !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \S(\underline{0} \in \alpha \multimap S(t) \in
$$

$$
!\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash !\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap S(t) \in
$$

$$
\forall \alpha.!\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap t \in \alpha) \vdash \forall \alpha.!\forall y(y \in \alpha \multimap S(y) \in \alpha) \multimap \S(\underline{0} \in \alpha \multimap S(
$$

$$
t \in \mathsf{N} \vdash S(t) \in \mathsf{N}
$$

$\Downarrow$ interpreted by

$$
Suc(n) \equiv \lambda fx.f(nfx)
$$

Main Properties of Interpretation

- A proof in **LAST** is canonical if it does not contain $A \multimap !B$, $!!B$, $\S!B$ (! always appears as $!A \multimap B$).
- In what follows, we assume that all proofs are canonical.
- Subject Reduction: $\Gamma \vdash \mathtt{M} : C,\ \mathtt{M} \rightarrow_\beta \mathtt{M}' \implies \Gamma \vdash \mathtt{M}' : C$.
- Church-Rosser: $M_1 \longleftarrow^* M_0 \longrightarrow^* M_2$ implies $M_1 \longrightarrow^* M_3 \longleftarrow^* M_2$ for some term M_3.
- Polynomial Time Strong Normalization: Let A be a Π_1 type of depth d (d counts the nesting of $!, \S$). Then any term $M : A$ reduces to its normal form within $O(|M|^{2^{d+1}})$ reduction steps. This result holds independently of which reduction strategy we take.

Program Extraction

Program extraction theorem: If

$$Total(f) \equiv \forall x \in \mathsf{W}.\S^d(\exists^! y \in \mathsf{W}.\langle x, y\rangle \in f)$$

has a (canonical) proof in **LAST**, then we can extract from that proof a λ term corresponding to f.

Corollary: $\phi : \{0,1\}^* \longrightarrow \{0,1\}^*$ is a polynomial time function $\Longleftrightarrow \phi$ is provably total in **LAST**.

Conclusion

- Restricting Contraction is reasonable when feasible constructivity is concerned.
- When Contraction is restricted, naive comprehension is fully available. Naive comprehension endows a system with rich definitional power (but not computational power).
- **LAST**: A formalization of feasible mathematics.
- Problem 1: Extend **EAST** (to primitive recursive functions, etc.) Are there "strongest" naive set theories?
- Problem 2: Intuitive semantics (cf. Komori 89, Shirahata 9?).
- Problem 3: Find a concrete example of mathematical theorems provable in **LAST** and extract a polynomial time program from the proof.