Proof systems for the (modal) mu-calculus

- Kozen, results on the propositional mu-calculus, 83 (finite axiomatization)
- Walukiewicz, completeness of the mu-calculus, ~95... (tableaux and completeness proof)
- Studer, on the proof theory of the modal mu-calculus, 2008
- Jäger, Kretz, Studer, canonical completeness for infinintary mu, 2009
- Afshari, Leigh, Cut-free completeness for the modal-mu-calculus, 2017
- Baelde, Doumane, Saurin, Infinitary proof-theory, 2016

- Kozen's proofs
- infinitary proofs with omega rule
- circular proofs

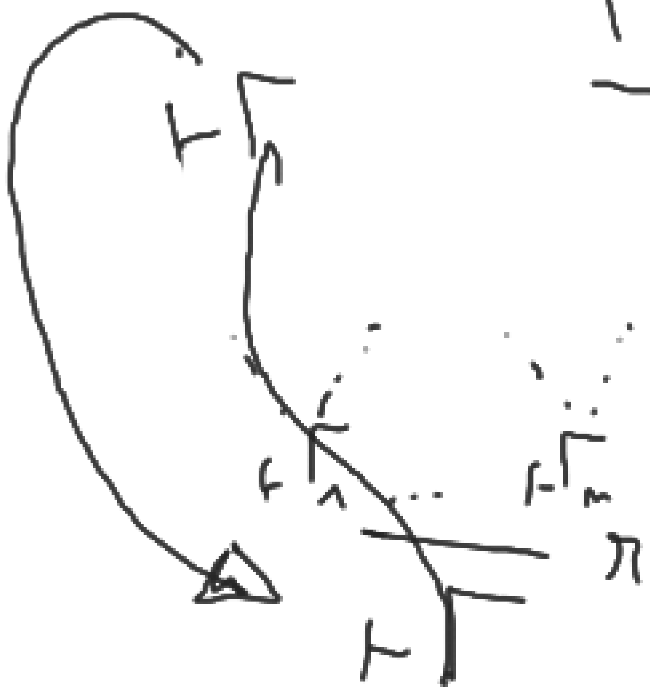
mu X. F <-> F[mu X.F / X]

|- F[nu X.F / X], Gamma

--------------------------------------(nu)

|- nu X.F, Gamma

$$\frac{\left(\vdash A(k), \Gamma\right)_{k \geq 0}}{\vdash \forall n, A, \Gamma}\ (\Omega)$$



infinite

The set of *μ-formulæ* is given by the grammar $\bar{p} / \sim p / \neg p$.

$$A := p \mid p \mid \mathsf{x} \mid A \wedge A \mid A \vee A \mid [\mathfrak{a}]A \mid \langle\mathfrak{a}\rangle A \mid \mu\mathsf{x}A \mid \nu\mathsf{x}A$$

$\mathfrak{a} \in \mathfrak{Act}$

We define the following operations on μ-formulæ. Set $\bot = p \wedge \overline{p}$ and $\top = \overline{p} \vee p$ for some fixed $p \in Prop$ and define $A \to B = \overline{A} \vee B$ where $\overline{A}$ denotes the *dual* of A, given by

$$\overline{A \wedge B} = \overline{A} \vee \overline{B} \qquad \overline{[\mathfrak{a}]A} = \langle\mathfrak{a}\rangle\overline{A} \qquad \overline{\mu\mathsf{x}A} = \nu\mathsf{x}\overline{A} \qquad \overline{\mathsf{x}} = \mathsf{x}$$

$$\overline{A \vee B} = \overline{A} \wedge \overline{B} \qquad \overline{\langle\mathfrak{a}\rangle A} = [\mathfrak{a}]\overline{A} \qquad \overline{\nu\mathsf{x}A} = \mu\mathsf{x}\overline{A} \qquad \overline{\overline{p}} = p$$

$\boxed{\mu x.\,(A \vee x)} \mapsto A$ $\qquad (x \notin FV(A))$,

$\nu x.\,(A \vee x) \mapsto \top$

$\overline{\mu x(A \vee x)} = \nu x.\,(\overline{A} \wedge x) \mapsto \overline{A}$

$$\mathsf{Ax1}\colon p, \bar{p} \qquad \frac{\Gamma, B, C}{\Gamma, B \vee C}\vee \qquad \frac{\Gamma, B \quad \Gamma, C}{\Gamma, B \wedge C}\wedge$$

$$\frac{\Gamma, A}{\langle\mathfrak{a}\rangle\Gamma, [\mathfrak{a}]A}\mathsf{mod} \qquad \frac{\Gamma, A(\sigma\mathsf{x}A(\mathsf{x}))}{\Gamma, \sigma\mathsf{x}A}\sigma \qquad \frac{\Gamma}{\Gamma, A}\mathsf{weak}$$

Figure 1: Rules and axioms of *fixed point logic*, Fix.

Semantics for the modal μ-calculus is a direct extension of Kripke semantics for (multi-)modal logic incorporating variables and quantifiers. A *frame*, or *labelled transition system*, is a tuple $\mathscr{K} = \langle K, R, \lambda\rangle$ where $R\colon \mathfrak{Act} \to K \times K$ and $\lambda\colon Prop \to 2^K$. The set K is called the *domain* of $\mathscr{K}$. A *valuation* (over $\mathscr{K}$) is a function $v\colon \mathsf{Var} \to 2^K$.

Given a frame $\mathscr{K} = \langle K, R, \lambda\rangle$, μ-formula A and valuation v over $\mathscr{K}$, we define $\|A\|_v^{\mathscr{K}}$ by induction on A:

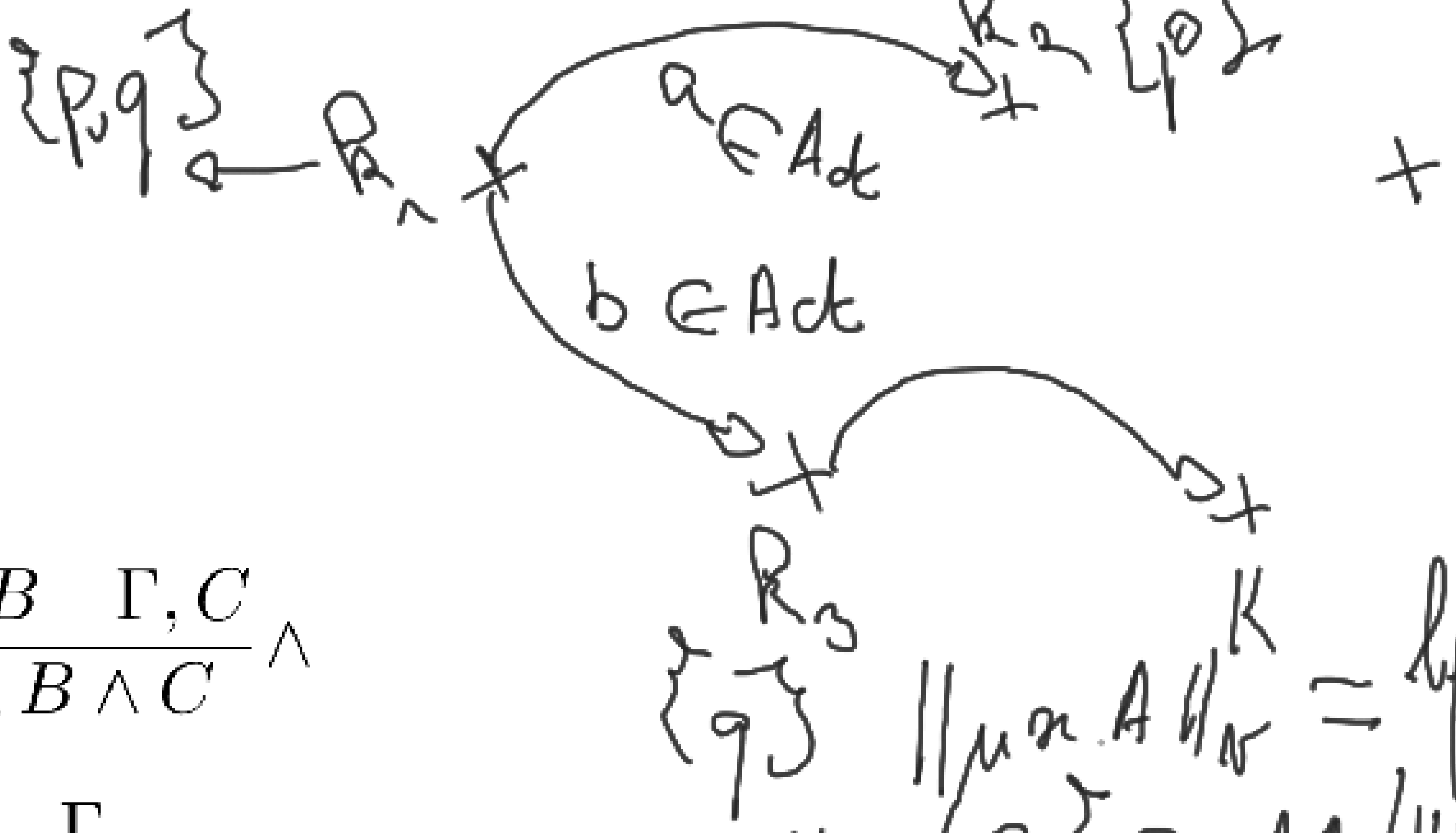
$$\|\mathsf{x}\|_v^{\mathscr{K}} = v(\mathsf{x})$$

$$\|p\|_v^{\mathscr{K}} = \lambda(p) \qquad \|[\mathfrak{a}]A\|_v^{\mathscr{K}} = \{s \in K \mid \forall t \in K((s,t) \in R(\mathfrak{a}) \to t \in \|A\|_v^{\mathscr{K}})\}$$

$$\|\overline{p}\|_v^{\mathscr{K}} = K \setminus \lambda(p) \qquad \|\langle\mathfrak{a}\rangle A\|_v^{\mathscr{K}} = \{s \in K \mid \exists t \in K((s,t) \in R(\mathfrak{a}) \wedge t \in \|A\|_v^{\mathscr{K}})\}$$

$$\|A \wedge B\|_v^{\mathscr{K}} = \|A\|_v^{\mathscr{K}} \cap \|B\|_v^{\mathscr{K}} \qquad \|\mu\mathsf{x}A\|_v^{\mathscr{K}} = \bigcap\{S \subseteq K \mid \|A\|_{v[\mathsf{x}\mapsto S]}^{\mathscr{K}} \subseteq S\}$$

$$\|A \vee B\|_v^{\mathscr{K}} = \|A\|_v^{\mathscr{K}} \cup \|B\|_v^{\mathscr{K}} \qquad \|\nu\mathsf{x}A\|_v^{\mathscr{K}} = \bigcup\{S \subseteq K \mid S \subseteq \|A\|_{v[\mathsf{x}\mapsto S]}^{\mathscr{K}}\}$$



$\|\mu x.A\|_v^K = \mathrm{lfp}\,\varphi$,

$\bigcap\{S \subseteq K / \|A\|_{v[x\to S]} \subseteq S\}$

$\varphi : S \mapsto \|A\|^K_{v[x\mapsto S]}$

$[\![B A]\!]^K_v = K \rightsquigarrow [\![\langle a \rangle B, [a]A]\!]^K_v$

Δ

$s \in K$

$$\{s \in K \mid \exists t, s \xrightarrow{a} t \in [\![B]\!]\} \qquad \{s \in K \mid \forall t, s \xrightarrow{a} t, t \in [\![A]\!]\}$$

K

$\|$

$$[\![\Delta]\!] = [\![\langle a \rangle B]\!]^K \cup [\![[a]A]\!]^K$$

$s \in$ $\qquad$ $s \notin$

$s \xrightarrow{a} t$, $t \notin [\![A]\!]^K_v$

$t \in [\![B]\!]^K_v$

$$\mu x. (A \vee x) \leftrightarrow A \quad (x \notin FV(A)),$$

$$\nu x. (A \vee a) \leftrightarrow \top$$

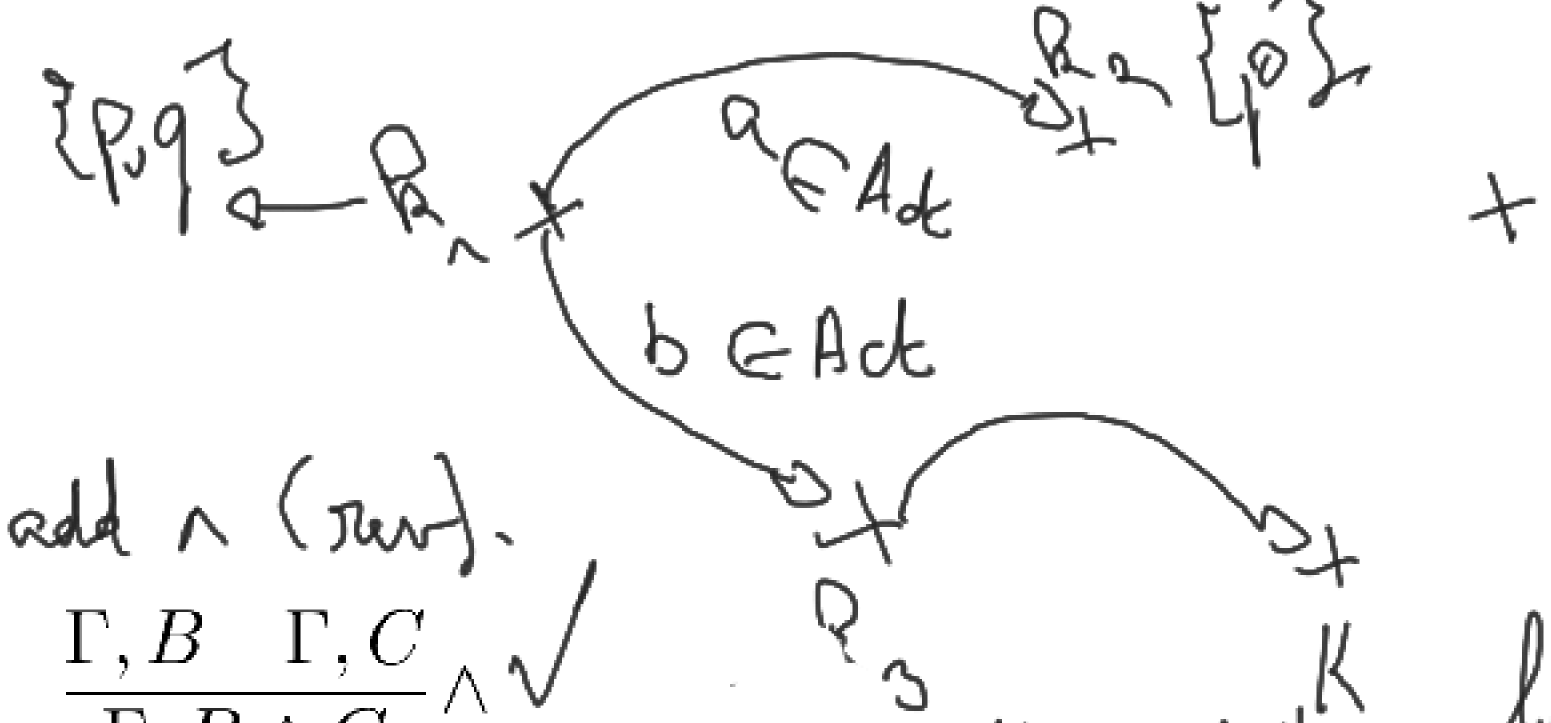
$$\overline{\mu x (A \vee x)} = \nu x. (\overline{A} \wedge x) \leftrightarrow \overline{A}$$

Ax2: $\mu x A, \nu x \overline{A}$ $\quad$ mult $\vee$ (rev) $\quad$ add $\wedge$ (rev).

Semantics for the modal μ-calculus is a direct extension of Kripke semantics for (multi-)modal logic incorporating variables and quantifiers. A *frame*, or *labelled transition system*, is a tuple $\mathscr{K} = \langle K, R, \lambda \rangle$ where $R: \mathfrak{Act} \to K \times K$ and $\lambda: Prop \to 2^K$. The set K is called the *domain* of $\mathscr{K}$. A *valuation* (over $\mathscr{K}$) is a function $v: \mathsf{Var} \to 2^K$.

Given a frame $\mathscr{K} = \langle K, R, \lambda \rangle$, μ-formula A and valuation v over $\mathscr{K}$, we define $\|A\|^{\mathscr{K}}_v$ by induction on A:

$$\begin{array}{ll}
\|\mathsf{x}\|^{\mathscr{K}}_v = v(\mathsf{x}) & \\
\|p\|^{\mathscr{K}}_v = \lambda(p) & \|[\mathfrak{a}]A\|^{\mathscr{K}}_v = \{s \in K \mid \forall t \in K((s,t) \in R(\mathfrak{a}) \to t \in \|A\|^{\mathscr{K}}_v)\} \\
\|\overline{p}\|^{\mathscr{K}}_v = K \setminus \lambda(p) & \|\langle \mathfrak{a} \rangle A\|^{\mathscr{K}}_v = \{s \in K \mid \exists t \in K((s,t) \in R(\mathfrak{a}) \wedge t \in \|A\|^{\mathscr{K}}_v)\} \\
\|A \wedge B\|^{\mathscr{K}}_v = \|A\|^{\mathscr{K}}_v \cap \|B\|^{\mathscr{K}}_v & \|\mu \mathsf{x} A\|^{\mathscr{K}}_v = \bigcap\{S \subseteq K \mid \|A\|^{\mathscr{K}}_{v[\mathsf{x} \mapsto S]} \subseteq S\} \\
\|A \vee B\|^{\mathscr{K}}_v = \|A\|^{\mathscr{K}}_v \cup \|B\|^{\mathscr{K}}_v & \|\nu \mathsf{x} A\|^{\mathscr{K}}_v = \bigcup\{S \subseteq K \mid S \subseteq \|A\|^{\mathscr{K}}_{v[\mathsf{x} \mapsto S]}\}
\end{array}$$



Ax1: $p, \bar{p}$ ✓ $\qquad \dfrac{\Gamma, B, C}{\Gamma, B \vee C} \vee$ ✓ $\qquad \dfrac{\Gamma, B \quad \Gamma, C}{\Gamma, B \wedge C} \wedge$ ✓

$\dfrac{\Gamma, A}{\langle \mathfrak{a} \rangle \Gamma, [\mathfrak{a}]A}$ mod $\qquad \dfrac{\Gamma, A(\sigma \mathsf{x} A(\mathsf{x}))}{\Gamma, \sigma \mathsf{x} A} \sigma \in \{\mu, \nu\}$ $\qquad \dfrac{\Gamma}{\Gamma, A}$ weak

Figure 1: Rules and axioms of *fixed point logic*, Fix.

$$\frac{?\Gamma, A}{?\Gamma, !A} \qquad \frac{\vdash \Gamma, ??A}{\vdash \Gamma, ?A} \qquad \frac{\Gamma, A}{?\Gamma, !A}$$

$$\|\mu x. A\|^K_v = \mathrm{lfp}\, \varphi$$

$$\bigcap\{S \subseteq K \mid \|A\|_{v[x \mapsto S]} \subseteq S\}$$

$v[x \mapsto S]$

x ∈ C . prefixed points .

$F(x) \sqsubseteq x$.

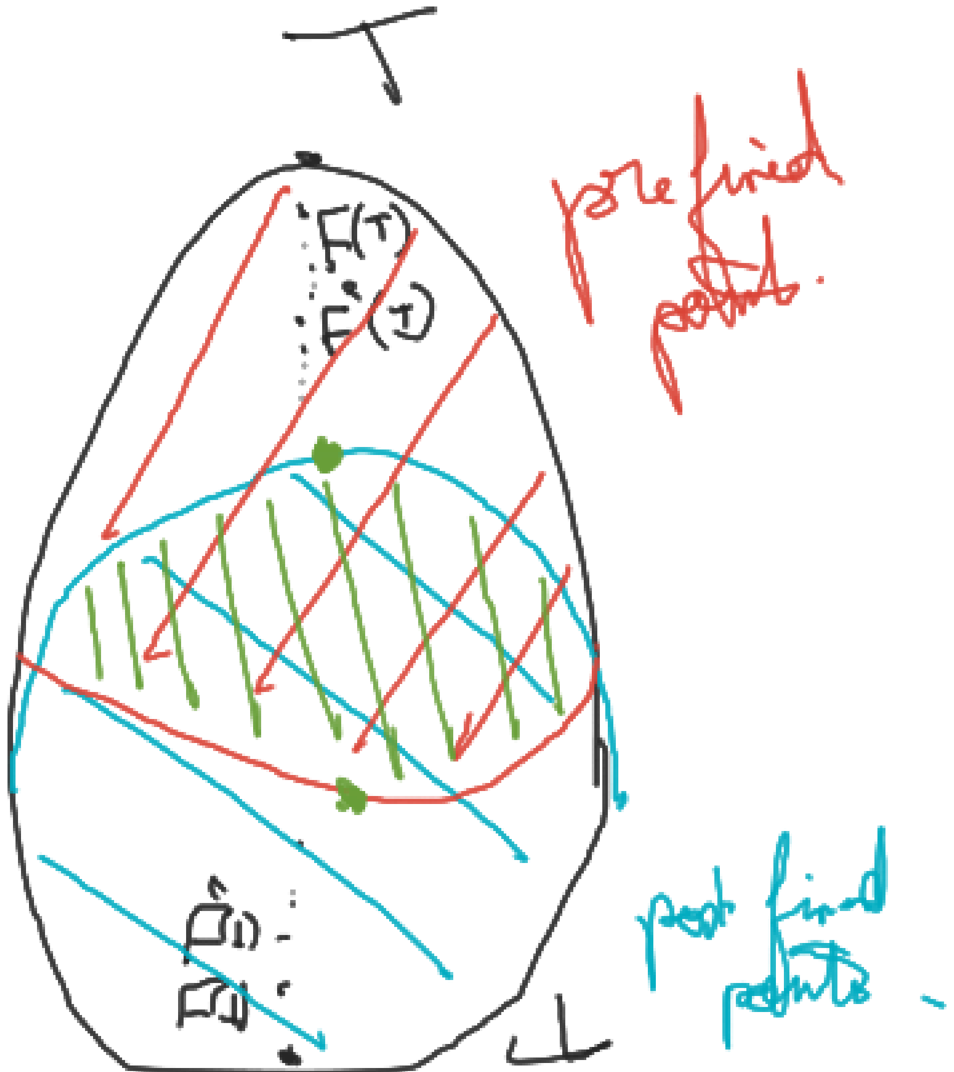
---

x ∈ C, post fixed point

$x \sqsubseteq F(x)$.

$x \sqsubseteq y \Longrightarrow F(x) \sqsubseteq F(y)$.

$\bot \sqsubseteq F(\bot) \mid F(\top) \sqsubseteq \top$



Knaster-Tarski fixed-point theorem

$\mu F \sqsubseteq$

$\varphi : X \longrightarrow \{0\} \cup \{s(x) \mid \forall x \in X\}$.

Let C be a complete lattice and F a monotonic operator on C.

Theorem

F has a **least** fixed-point μF.

μF is the **least prefixed**-point:

- $\boxed{F(\mu F) \sqsubseteq \mu F}$ and pre
- $\forall S, F(S) \sqsubseteq S \Rightarrow \mu F \sqsubseteq S$. least

≠ in general.

Theorem

F has a **greatest** fixed-point νF.

νF is the greatest postfixed-point:

- $\nu F \sqsubseteq F(\nu F)$ and
- $\forall S, S \sqsubseteq F(S) \Rightarrow S \sqsubseteq \nu F$.

Proof by induction:

To prove that $\mu F \subseteq P$, it is sufficient to find some $S \subseteq P$ and to prove that $\forall x \in F(S), x \in S$.

$\varphi(S) \subseteq S$.

$0 \in S$.

$\forall x \in \varphi(S)$ $x \in S$

$y \in S$ st. $x = s(y)$.

Proof by coinduction:

To prove that $P \subseteq \nu F$, it is sufficient to find some $S \supseteq P$ and to prove that $\forall x \in S, x \in F(S)$.

Knaster-Tarski fixed-point theorem

$$\boxed{\bar{\Gamma} = \bigwedge_{F\in\Gamma}(\bar{F})}$$

$$\frac{\vdash \Gamma, \bar{S} \qquad \vdash S, F[S/x]}{\vdash \Gamma, \nu X.F}\ \nu$$

Let C be a complete lattice and F a monotonic operator on C.

Theorem

F has a **least** fixed-point μF.

μF is the **least prefixed**-point:
- $F(\mu F) \sqsubseteq \mu F$ and
- $\forall S, F(S) \sqsubseteq S \Rightarrow \mu F \sqsubseteq S$.

Theorem

F has a **greatest** fixed-point νF.

νF is the **greatest postfixed**-point:
- $\nu F \sqsubseteq F(\nu F)$ and
- $\forall S, S \sqsubseteq F(S) \Rightarrow S \sqsubseteq \nu F$.

Proof by induction:

To prove that $\mu F \subseteq P$, it is sufficient to find some $S \subseteq P$ and to prove that $\forall x \in F(S), x \in S$.

$$\frac{H \vdash F[\mu X.F/X]}{H \vdash \mu X.F}\,[\mu_r] \qquad \frac{F[S/X] \vdash S}{\mu X.F \vdash S}\,[\mu_l]$$

$\vdash \Gamma, \nu X.F$

$$\boxed{\frac{\vdash \Gamma, F[\bar{\Gamma}/x]}{\vdash \Gamma, \nu X.F}}$$

Proof by coinduction:

To prove that $P \subseteq \nu F$, it is sufficient to find some $S \supseteq P$ and to prove that $\forall x \in S, x \in F(S)$.

$$\frac{F[\nu X.F/X] \vdash H}{\nu X.F \vdash H}\,[\nu_l] \qquad \frac{S \vdash F[S/X]}{S \vdash \nu X.F}\,[\nu_r]$$

$$\frac{\vdash \Gamma, F[\mu X.F/x]}{\vdash \Gamma, \mu X.F}\ \mu$$

Kozen's axiomatization

Previous inferences plus the following (Koz- is the cut-free fragment):

$$\frac{\Gamma, A(\overline{\Gamma})}{\Gamma, \nu \mathsf{x} A(\mathsf{x})}\,\text{ind} \qquad \boxed{\mathsf{Ax2}: \nu \mathsf{x} A, \mu \mathsf{x} \bar{A}} \qquad \xcancel{\frac{\Gamma, A(B), A(C)}{\Gamma, A(B \vee C)}\vee_d} \qquad \frac{\Gamma, A \quad \Gamma, \overline{A}}{\Gamma}\,\text{cut}$$

Figure 2: Additional rules present in Koz^-.

$$\frac{}{\vdash A, \bar{A}}\,\text{Ax.}$$

Theorem 3.1. Koz *is sound and complete for the* μ*-calculus.*

Lemma 3.2. *Let* $A(\mathsf{x}_0, \dots, \mathsf{x}_{k-1})$ *be a formula with at most the designated variables free.*

If B_i *and* C_i *are closed formulæ for each* $i < k$, *then*

$$\{B_i, C_i\}_{i<k} \vdash_{\mathsf{Koz}^-} \overline{A}(B_0, \dots, B_{k-1}), A(C_0, \dots, C_{k-1}).$$

$$\left[\begin{array}{l} \vdash B_0, C_0 \quad \dots \quad \vdash B_{k-1}, C_{k-1}. \\ A(x_0, \dots x_{k-1}). \\ \\ \vdash A(B_0, B_1 \dots B_{k-1}), \bar{A}(C_0, \dots C_{k-1}) \end{array}\right.$$

Proof. The proof proceeds by induction on A. We present the case $A = \nu \mathsf{x}_k A_0(\mathsf{x}_0, \dots, \mathsf{x}_{k-1}, \mathsf{x}_k)$. The remaining cases are straightforward. Let $B_k = \overline{A}(B_0, \dots, B_{k-1})$. As the sequent $B_k, \overline{B_k}$ is an instance of Ax2, the induction hypothesis implies

$$\{B_i, C_i\}_{i<k} \vdash_{\mathsf{Koz}^-} \overline{A_0}(B_0, \dots, B_k), A_0(C_0, \dots, C_{k-1}, \overline{B_k}),$$

whereby an application of μ yields

$$\{B_i, C_i\}_{i<k} \vdash_{\mathsf{Koz}^-} B_k, A_0(C_0, \dots, C_{k-1}, B_k)$$

and an application of ind completes the proof. □

Fixed-point logics and (co)induction

Some examples from (co)inductive predicates to μ-calculus

- $Nat(x) \triangleq_{ind} (x = 0) \vee \exists y. x = s(y) \wedge Nat(y)$
- $ListNat(l) \triangleq_{ind} (l = nil) \vee \exists h, t. l = h :: t \wedge (Nat(h) \wedge ListNat(t))$
- $StreamNat(l) \triangleq_{coind} \exists h, t. l = h :: t \wedge (Nat(h) \wedge StreamNat(t))$

- $Nat(x) \triangleq \mu N.(x = 0) \vee \exists y. x = s(y) \wedge N(y)$
- $ListNat(l) \triangleq \mu L.(l = nil) \vee \exists h, t. l = h :: t \wedge (Nat(h) \wedge L(t))$
- $StreamNat(l) \triangleq \nu S. \exists h, t. l = h :: t \wedge (Nat(h) \wedge S(t))$

- $Nat \triangleq \mu N. \top \vee N$
- $ListNat \triangleq \mu L. \top \vee (Nat \wedge L)$
- $StreamNat \triangleq \nu S. Nat \wedge S$

$\Rightarrow$ in the following,
the propositional
μ-calculus only.

Interleavings of inductive/coinductives behaviours; *eg.* allowing to express fairness properties:

$\nu X. \mu Y. (P \wedge \bigcirc X) \vee \bigcirc Y.$ $\nu X. \mu Y. (P \wedge \langle a \rangle X) \vee \langle a \rangle Y.$ --> P holds "infinitely often".

$\mu Y. \nu X. (P \wedge \bigcirc X) \vee \bigcirc Y.$ $\mu Y. \nu X. (P \wedge \langle a \rangle X) \vee \langle a \rangle Y.$ --> P holds "almost always".

Example 3.1. Recall the valid sequent $\{\nu\mathsf{x}\mu\mathsf{y}\overline{B}, \nu\mathsf{y}\mu\mathsf{x}B\}$ from Example 2.1. Let $C = \nu\mathsf{x}\mu\mathsf{y}\overline{B}$ and $D = \nu\mathsf{y}\mu\mathsf{x}B$. The following derivation, which we denote π_{koz}, is the Koz-proof of this sequent motivated by the semantic validity argument:

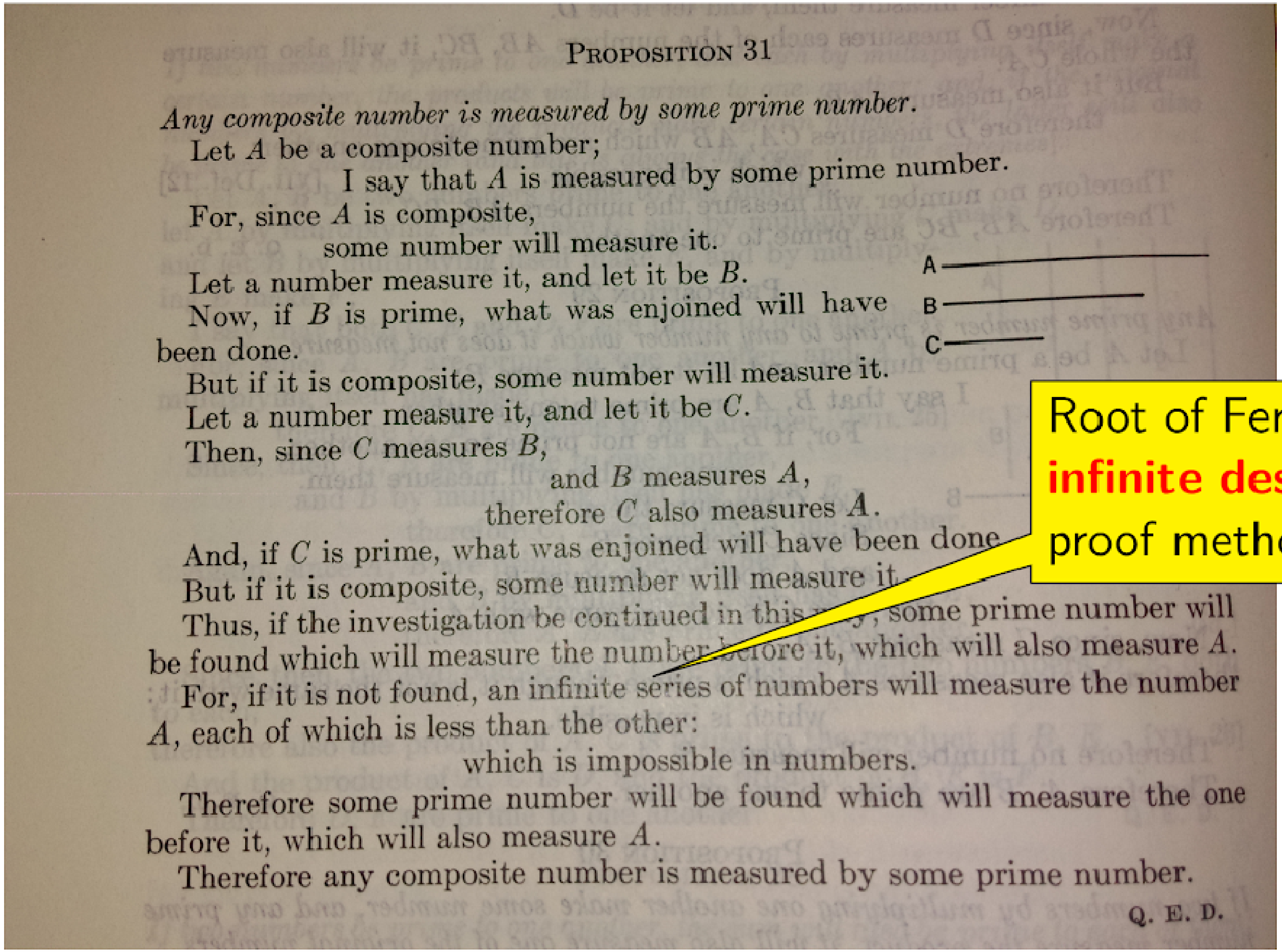
$$
\dfrac{\dfrac{\dfrac{
\begin{array}{c}
\nu\mathsf{x}\overline{B}(\mathsf{x},C), \mu\mathsf{x}B(\mathsf{x},\overline{C}) \qquad
\dfrac{
\begin{array}{c}
\dfrac{\dfrac{\dfrac{
\begin{array}{c}
C,\overline{C} \qquad
\dfrac{
\begin{array}{c}
C,\overline{C} \\ \hdashline
\vdots\ \text{Lemma 3.2} \\
\mu\mathsf{y}\overline{B}(C,\mathsf{y}), \nu\mathsf{y}B(\overline{C},\mathsf{y})
\end{array}
}{C, \nu\mathsf{y}B(\overline{C},\mathsf{y})}\,\nu \\ \hdashline
\vdots\ \text{Lemma 3.2} \\
\overline{B}(C,C), B(\overline{C}, \nu\mathsf{y}B(\overline{C},\mathsf{y}))
\end{array}
}{\overline{B}(C,C), \nu\mathsf{y}B(\overline{C},\mathsf{y})}\,\nu}{\overline{B}(C,C), \overline{C}}\,\mu}{\nu\mathsf{x}\overline{B}(\mathsf{x},C), \overline{C}}\,\mathsf{ind} \\ \hdashline
\vdots\ \text{Lemma 3.2} \\
\mu\mathsf{y}\overline{B}(\nu\mathsf{x}\overline{B}(\mathsf{x},C),\mathsf{y}), \nu\mathsf{y}B(\overline{C},\mathsf{y})
\end{array}
}{\mu\mathsf{y}\overline{B}(\nu\mathsf{x}\overline{B}(\mathsf{x},C),\mathsf{y}), \overline{C}}\,\mu \\ \hdashline
\vdots\ \text{Lemma 3.2} \\
\overline{B}(\nu\mathsf{x}\overline{B}(\mathsf{x},C), \mu\mathsf{y}\overline{B}(\nu\mathsf{x}\overline{B}(\mathsf{x},C),\mathsf{y})), B(\mu\mathsf{x}B(\mathsf{x},\overline{C}), \overline{C})
\end{array}
}{\mu\mathsf{y}\overline{B}(\nu\mathsf{x}\overline{B}(\mathsf{x},C),\mathsf{y}), \mu\mathsf{x}B(\mathsf{x},\overline{C})}\,\mu,\mu}{C, \mu\mathsf{x}B(\mathsf{x},\overline{C})}\,\mathsf{ind}}{C, D}\,\mathsf{ind}
$$

Circular & non-wellfounded proofs

Circular proofs: an old mathematical story

Back to Euclid's *Elements* (Book VII)

another example



PROPOSITION 31

Any composite number is measured by some prime number.

Let A be a composite number;

I say that A is measured by some prime number.

For, since A is composite,

some number will measure it.

Let a number measure it, and let it be B.

Now, if B is prime, what was enjoined will have been done.

But if it is composite, some number will measure it.

Let a number measure it, and let it be C.

Then, since C measures B,

and B measures A,

therefore C also measures A.

And, if C is prime, what was enjoined will have been done.

But if it is composite, some number will measure it.

Thus, if the investigation be continued in this way, some prime number will be found which will measure the number before it, which will also measure A.

For, if it is not found, an infinite series of numbers will measure the number A, each of which is less than the other:

which is impossible in numbers.

Therefore some prime number will be found which will measure the one before it, which will also measure A.

Therefore any composite number is measured by some prime number.

Q. E. D.

Root of Fermat's **infinite descent** proof method.

For any integer m, $\sqrt{m}$ is either an integer, or irrational.

Another example of infinite descent

another example

Proof

Let $m \in \mathbb{N}$ and for the sake of contradiction, assume $\sqrt{m} \in \mathbb{Q} \setminus \mathbb{N}$.

1. Choose $q, a_0, b_0 \in \mathbb{N}$ st. $0 < \sqrt{m} - q < 1$ and $\sqrt{m} = a_0/b_0$. One has $b_0\sqrt{m} = a_0 \in \mathbb{N}$ and $a_0\sqrt{m} = mb_0 \in \mathbb{N}$.
2. Therefore by setting $a_1 \triangleq mb_0 - a_0 q = a_0(\sqrt{m} - q)$ and $b_1 \triangleq a_0 - b_0 q = b_0(\sqrt{m} - q)$, we have
   - a_0, a_1 are integers,
   - $0 < a_1 < a_0, \quad 0 < b_1 < b_0$ and
   - $\sqrt{m} = a_1/b_1$.
3. In a similar way, one can build $(a_i)_{i \in \mathbb{N}}$ and $(b_i)_{i \in \mathbb{N}}$ infinite sequences of integers, *which are strictly decreasing*.
4. This is impossible. Therefore $\sqrt{m}$ is either integer or irrational.

□

Non-Wellfounded Sequent Calculus

Consider your favourite logic $\mathscr{L}$ & add fixed points as in the μ-calculus

Pre-proofs are the trees **coinductively** generated by:

- $\mathscr{L}$ inference rules
- inference for μ, ν:

$$\frac{\Gamma, F[\mu X.F/X] \vdash \Delta}{\Gamma, \mu X.F \vdash \Delta}\,[\mu_l] \qquad \frac{\Gamma, F[\nu X.F/X] \vdash \Delta}{\Gamma, \nu X.F \vdash \Delta}\,[\nu_l]$$

$$\frac{\Gamma \vdash F[\mu X.F/X], \Delta}{\Gamma \vdash \mu X.F, \Delta}\,[\mu_r] \qquad \frac{\Gamma \vdash F[\nu X.F/X], \Delta}{\Gamma \vdash \nu X.F, \Delta}\,[\nu_r]$$

Circular (pre-)proofs: the regular fragment of infinite (pre-)proofs, ie finitely many sub-(pre)proofs.

Pre-proofs are unsound!! ***Need for a validity condition***

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,[\mu]}{\vdash \mu X.X}\,[\mu] \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\,[\nu]}{\vdash \nu X.X, F}\,[\nu]}{\vdash F}\,[\text{Cut}]$$

Fischer-Ladner subformulas

$FL(F)$ is the least set of formula occurrences such that:

- $F \in FL(F)$;
- $G_1 \star G_2 \in FL(F) \Rightarrow G_1, G_2 \in FL(F)$ for $\star \in \{\vee, \wedge\}$;
- $\sigma X.B \in FL(F) \Rightarrow B[\sigma X.B/X] \in FL(F)$ for $\sigma \in \{\mu, \nu\}$;
- $mG \in FL(F) \Rightarrow G \in FL(F)$ for $m \in \{[a], \langle a \rangle\}$.

Fact

$FL(F)$ is a finite set for any formula F.

Example: $F = \nu X.((a \vee a^{\perp}) \wedge (X \wedge \mu Y.X))$

$$FL(F) = \{F\,,\ (a \vee a^{\perp}) \wedge (F \wedge \mu Y.F)\,,\ \begin{array}{cc} a \vee a^{\perp}\ , & \begin{array}{c} a \\ a^{\perp} \end{array} \\ F \wedge \mu Y.F\ , & \mu Y.F \end{array}\ \}$$

Fischer-Ladner subformulas

$FL(F)$ is the least set of formula occurrences such that:

- $F \in FL(F)$;
- $G_1 \star G_2 \in FL(F) \Rightarrow G_1, G_2 \in FL(F)$ for $\star \in \{\vee, \wedge\}$;
- $\sigma X.B \in FL(F) \Rightarrow B[\sigma X.B/X] \in FL(F)$ for $\sigma \in \{\mu, \nu\}$;
- $mG \in FL(F) \Rightarrow G \in FL(F)$ for $m \in \{[a], \langle a \rangle\}$.

Fact

$FL(F)$ is a finite set for any formula F.

Example: $F = \nu X.((a \vee a^\perp) \wedge (X \wedge \mu Y.X))$

$$\begin{tikzcd}
 & & a \vee a^\perp \arrow[r] \arrow[dr] & a \\
FL(F) = F \arrow[r] & (a \vee a^\perp) \wedge (F \wedge \mu Y.F) \arrow[ur] \arrow[dr] & & a^\perp \\
 & & F \wedge \mu Y.F \arrow[r] \arrow[ull, bend left] & \mu Y.F \arrow[ulll, bend left]
\end{tikzcd}$$

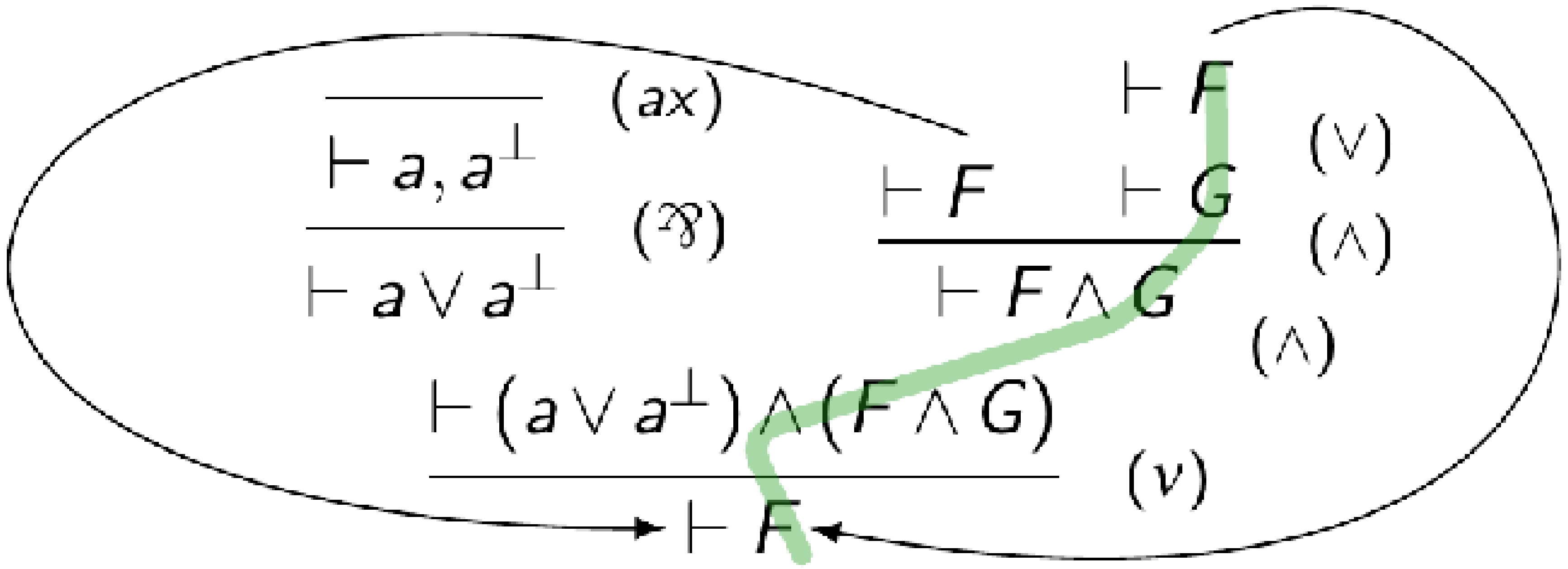
Infinite threads, validity

A ***thread*** on an infinite branch $(\Gamma_i)_{i\in\omega}$ is an infinite sequence of formula occurrences $(F_i)_{i\geq k}$ such that for any $i \geq k$, $F_i \in \Gamma_i$ and F_{i+1} is an immediate ancestor of F_i.

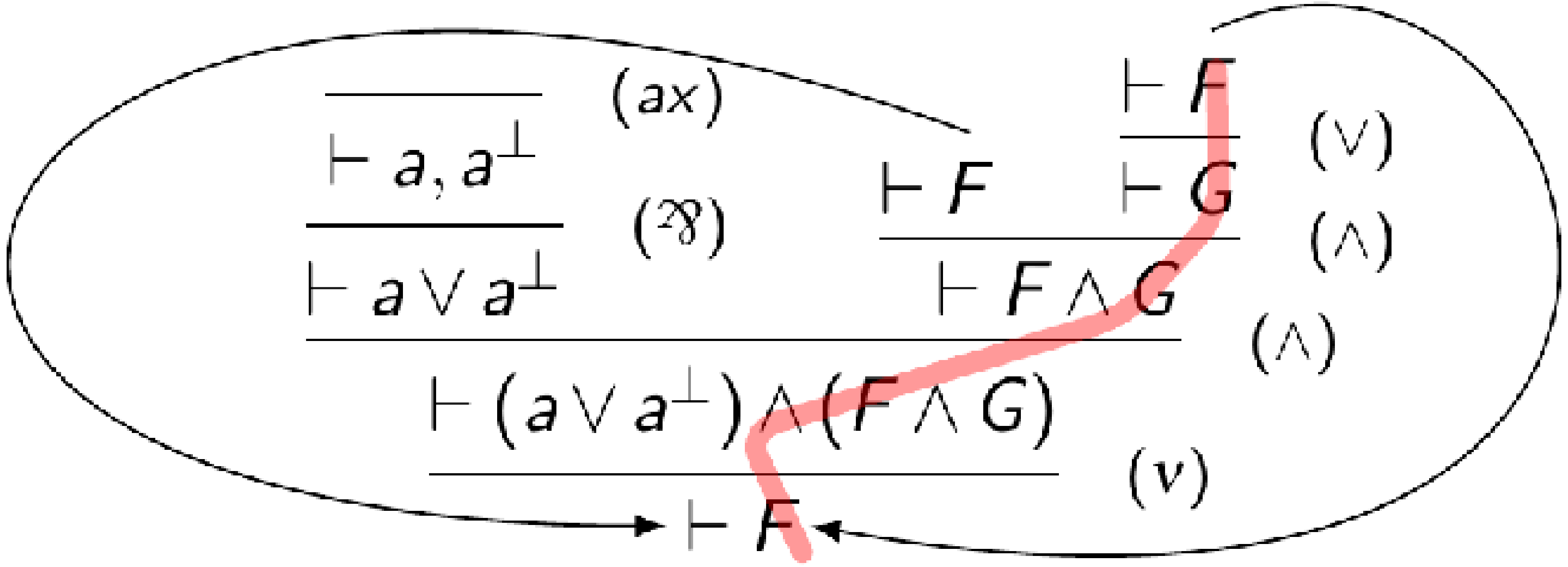
A thread is valid if it unfolds infinitely many ν. More precisely, if the minimal ***recurring*** principal formula of the thread is a ν-formula.

A proof is valid if every infinite branch contains a valid thread.

$$F = \nu X.((a \vee a^{\perp}) \wedge (X \wedge \mu Y.X)).$$
$$G = \mu Y.F$$



$$F = \nu X.((a \vee a^{\perp}) \wedge (X \wedge G))$$
$$G = \mu Y.\nu X.((a \vee a^{\perp}) \wedge (X \wedge Y))$$



Examples of circular proofs

- **Inductive and coinductive definitions**

$$\mathsf{N} = \mu X.1 \oplus X \qquad\qquad \mathsf{S} = \nu X.(1 \,\&\, (N \otimes X))$$

- **Proofs-programs over these data types**

$$\begin{array}{lcll} \mathit{double} & : & N \to N & \\ \mathit{double}(n) & = & 0 & \text{if } n = 0 \\ & = & \mathit{succ}(\mathit{succ}(\mathit{double}(m))) & \text{if } n = \mathit{succ}(m) \end{array}$$

$$\pi_0 = \cfrac{\cfrac{\cfrac{}{\vdash 1}\,(\mathbf{1})}{\vdash 1 \oplus N}\,(\oplus_1)}{\vdash N}\,(\mu)$$

$$\pi_{k+1} = \cfrac{\cfrac{\cfrac{\pi_k}{\vdash N}}{\vdash 1 \oplus N}\,(\oplus_2)}{\vdash N}\,(\mu)$$

$$\Pi_{double} \quad = \quad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\vdash 1}\,(\mathbf{1})}{\vdash 1 \oplus N}\,(\oplus_1)}{\vdash N}\,(\mu)}{1 \vdash N}\,(\bot) \qquad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\Pi_{double}}{N \vdash N}}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)}{1 \oplus N \vdash N}\,(\&)}{N \vdash N}\,(\nu)$$

Examples of circular proofs

- **Inductive and coinductive definitions**

$$\mathsf{N} = \mu X.1 \oplus X \qquad\qquad \mathsf{S} = \nu X.1 \,\&\, (N \otimes X)$$

- **Proofs-programs over these data types**

$$\begin{array}{lcl} enum & : & N \to S \\ enum(n) & = & n :: enum(succ(n)) \end{array}$$

$$\pi_{\mathrm{succ}} = \dfrac{\dfrac{\dfrac{}{N \vdash N}\,(ax)}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)$$

$$\Pi_{enum} = \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 1}\,(1)}{!N \vdash 1}\,(w) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{N \vdash N}\,(ax)}{!N \vdash N}\,(?) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\pi_{\mathrm{succ}}}{N \vdash N}}{!N \vdash N}\,(?)}{!N \vdash !N}\,(!) \qquad \dfrac{\Pi_{enum}}{!N \vdash S}}{!N \vdash S}\,(cut)}{!N, !N \vdash N \otimes S}\,(\otimes)}{!N \vdash N \otimes S}\,(c)}{!N \vdash 1 \,\&\, (N \otimes S)}\,(\&)}{!N \vdash S}\,(\nu)$$

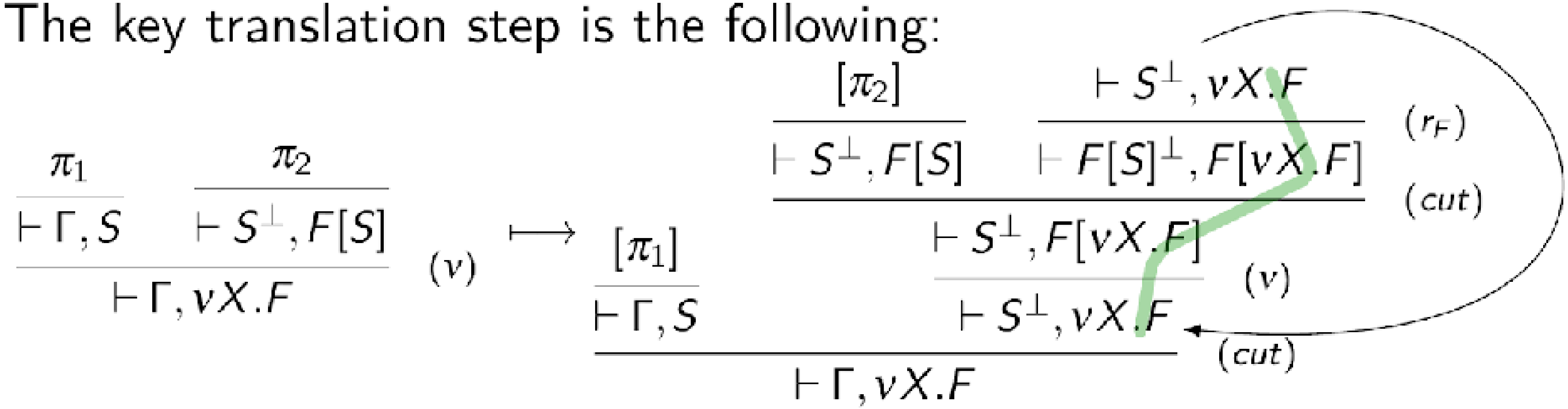
Circular & finitary proofs

From finitary to circular proofs

Theorem

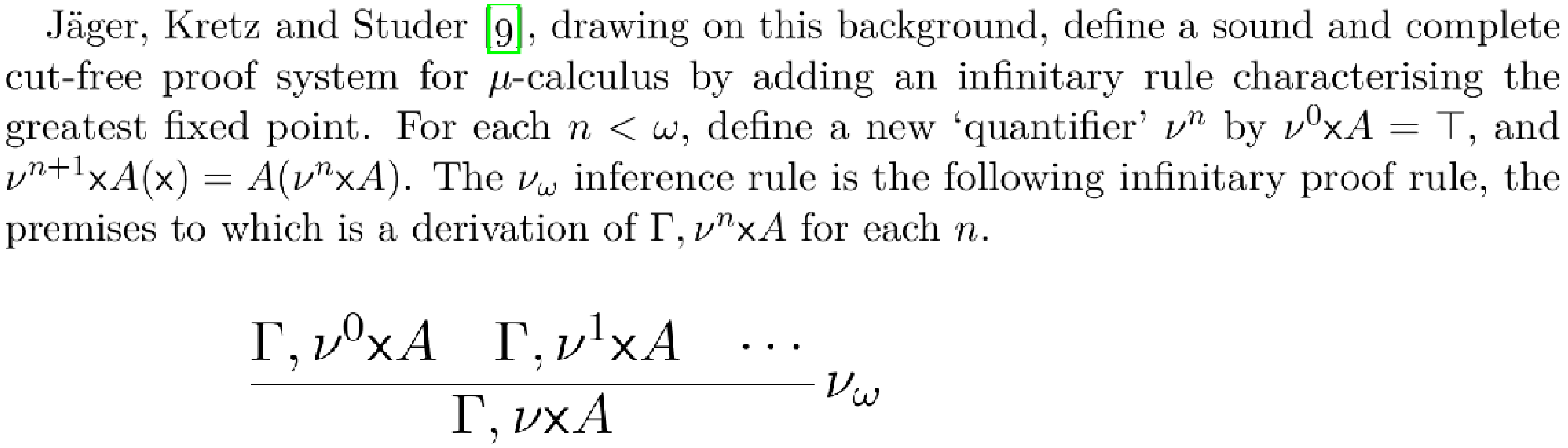
Finitary proofs can be transformed to (valid) circular proofs.

The key translation step is the following:



$$\dfrac{\dfrac{\pi_1}{\vdash \Gamma, S} \qquad \dfrac{\pi_2}{\vdash S^{\perp}, F[S]}}{\vdash \Gamma, \nu X.F}\,(\nu) \quad \longmapsto \quad \dfrac{\dfrac{[\pi_1]}{\vdash \Gamma, S} \qquad \dfrac{\dfrac{\dfrac{[\pi_2]}{\vdash S^{\perp}, F[S]} \qquad \dfrac{\vdash S^{\perp}, \nu X.F}{\vdash F[S]^{\perp}, F[\nu X.F]}\,(r_F)}{\vdash S^{\perp}, F[\nu X.F]}\,(cut)}{\vdash S^{\perp}, \nu X.F}\,(\nu)}{\vdash \Gamma, \nu X.F}\,(cut)$$

Proof systems with the omega rule



Jäger, Kretz and Studer [9], drawing on this background, define a sound and complete cut-free proof system for μ-calculus by adding an infinitary rule characterising the greatest fixed point. For each $n < \omega$, define a new 'quantifier' ν^n by $\nu^0\mathsf{x}A = \top$, and $\nu^{n+1}\mathsf{x}A(\mathsf{x}) = A(\nu^n\mathsf{x}A)$. The ν_ω inference rule is the following infinitary proof rule, the premises to which is a derivation of $\Gamma, \nu^n\mathsf{x}A$ for each n.

$$\frac{\Gamma, \nu^0\mathsf{x}A \quad \Gamma, \nu^1\mathsf{x}A \quad \cdots}{\Gamma, \nu\mathsf{x}A}\,\nu_\omega$$