

Fibrational IA-FC Coincidence over Initial Algebras: Turning Verification Witnesses Upside Down

Mayuko Kori^{1, 2}, Ichiro Hasuo^{1, 2}, Shin-ya Katsumata²

¹The Graduate University for Advanced Studies (SOKENDAI), Kanagawa, Japan

²National Institute of Informatics, Tokyo, Japan

in CONCUR 2021

Initial Algebra (IA) & Final Coalgebra (FC)

- Algebra: $FX \rightarrow X$, Coalgebra: $X \rightarrow FX$

where $F : \mathbb{C} \rightarrow \mathbb{C}$

- Initial Algebra (IA):

$$\begin{array}{ccc} F(\mu F) & \xrightarrow{\quad} & FX \\ \text{init.} \downarrow \cong & & \downarrow \\ \mu F & \xrightarrow{\quad} & X \end{array}$$

- Final Coalgebra (FC):

$$\begin{array}{ccc} X & \xrightarrow{\quad} & \nu F \\ \downarrow & & \cong \downarrow \text{final.} \\ FX & \xrightarrow{\quad} & F(\nu F) \end{array}$$

	In Set-like categories	In Posets as categories
IA (finite)	Inductive datatype e.g. finite lists	“lfp property” e.g. liveness
FC (infinite)	coinductive datatype e.g. finite & infinite lists	“gfp property” e.g. safety

IA-FC coincidence in Computer Science

IA-FC coincidence may be unlikely but ...

- Domain theory:

Recursive domain equations of mixed variance [Fiore, 96],
[Freyd, LICS'90], [Smyth&Plotkin, SIAM'82]

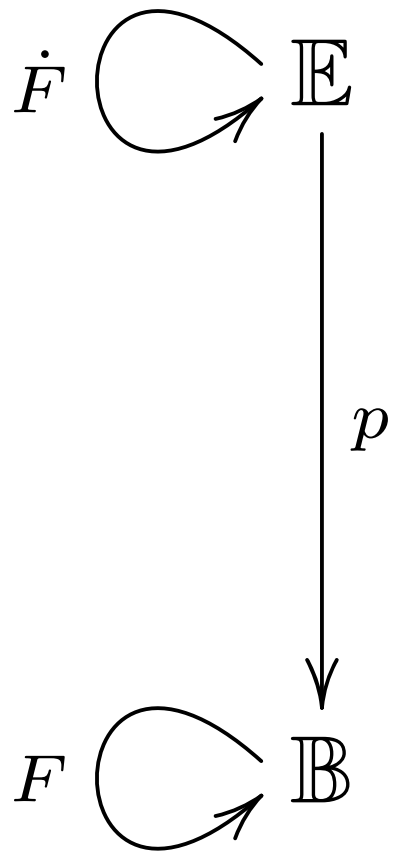
- Process semantics:

Coalgebraic characterization of finite trace semantics
[Hasuo+, LMCS'07]

- Program semantics:

Interpretation of various recursive types in functional
programming

IA-FC coincidence over base IAs



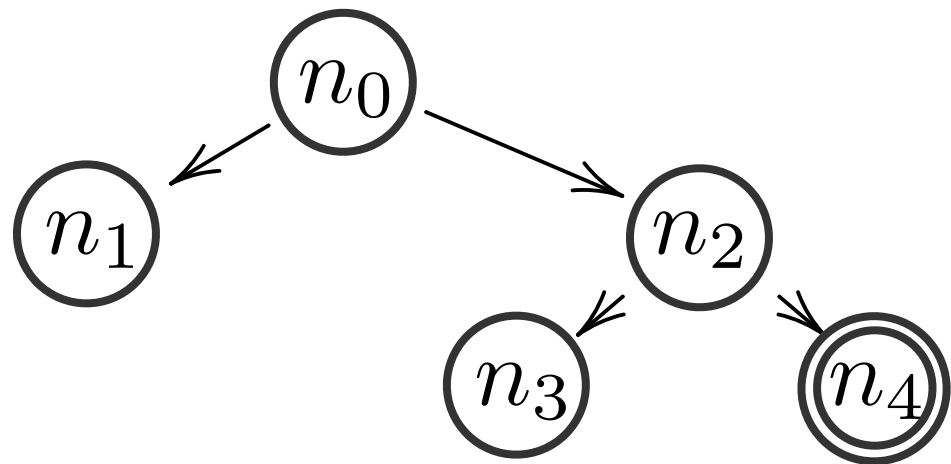
Initial $\dot{F}$ -alg.
= lfp property

$\cong$

Final $\dot{F}$ -coalg.
= gfp property

Initial F -algebra
(algebraic datatype)

Simple example for IA-FC coincidence over IAs



Consider T , which is a set of finite trees with circles $\bigcirc$ and $\bigcirc\bigcirc$.

Def. T is a "reachability invariant" if for each $t \in T$ satisfies the root of t is $\bigcirc\bigcirc$ or $(t = \begin{array}{c} n \\ \swarrow \quad \searrow \\ t_1 \quad t_2 \end{array} \text{ and } t_1 \in T \text{ or } t_2 \in T)$.

Thm. Every tree in a reachability invariant T has a node with $\bigcirc\bigcirc$.

Key: Finiteness

Background: IA-FC coincidence over Initial Algebras

Contributions

- **IF/I coincidence:**

Fibrational framework for IA-FC coincidence over IAs

- We give mild conditions to ensure IF/I coincidence.
 - Fibredness of liftings
 - Stability of chain colimits
- Application to verification witnesses
 - Coinductive witness notions for inductive properties

Outline

1. Background: Fibrations and liftings
2. IF/I coincidence
3. Conditions to ensure IF/I coincidence
for $\text{CLat}_\wedge$ -fibrations
4. Application to verification witness
5. Conclusion

Outline

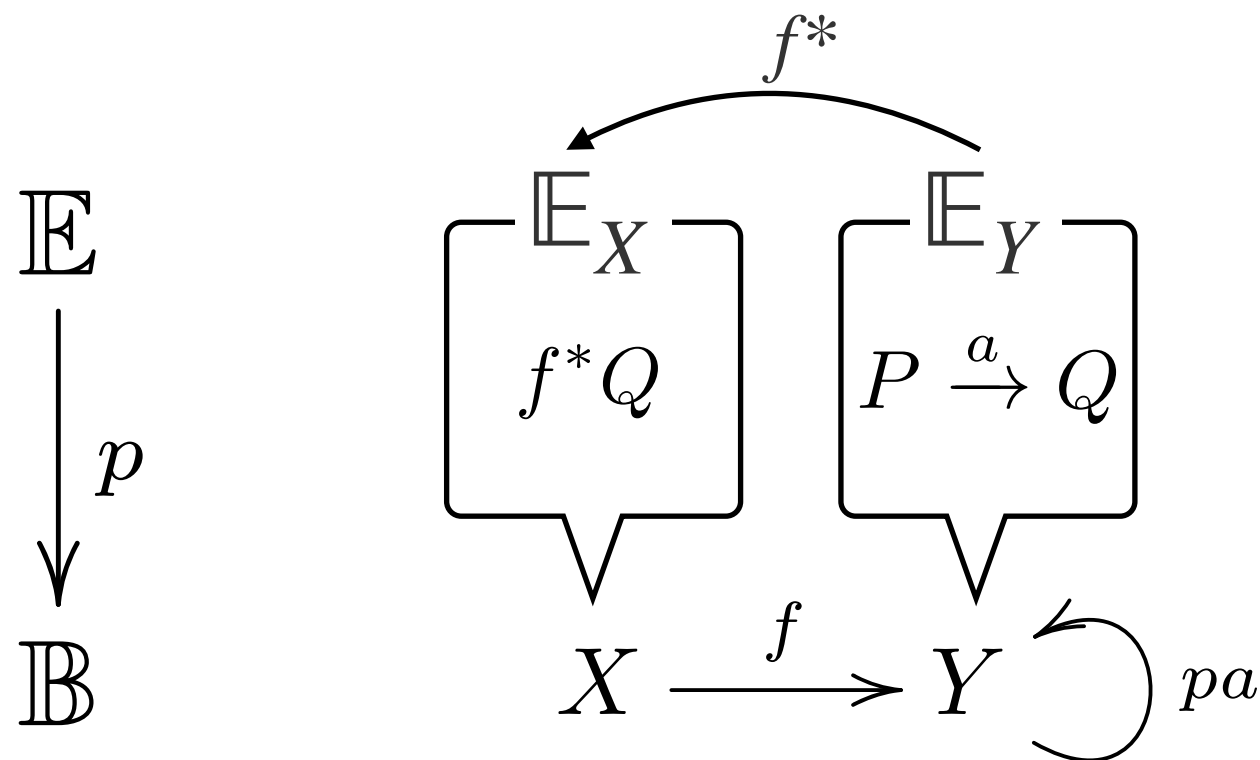
1. Background: Fibrations and liftings
2. IF/I coincidence
3. Conditions to ensure IF/I coincidence
for $\text{CLat}_\wedge$ -fibrations
4. Application to verification witness
5. Conclusion

Background: fibration

A fibration p is a functor that models indexing and substitution

fibre categories $(\mathbb{E}_X)_{X \in \mathbb{B}}$

+ substitution functors $(f^* : \mathbb{E}_Y \rightarrow \mathbb{E}_X)_{f \text{ in } \mathbb{B}}$



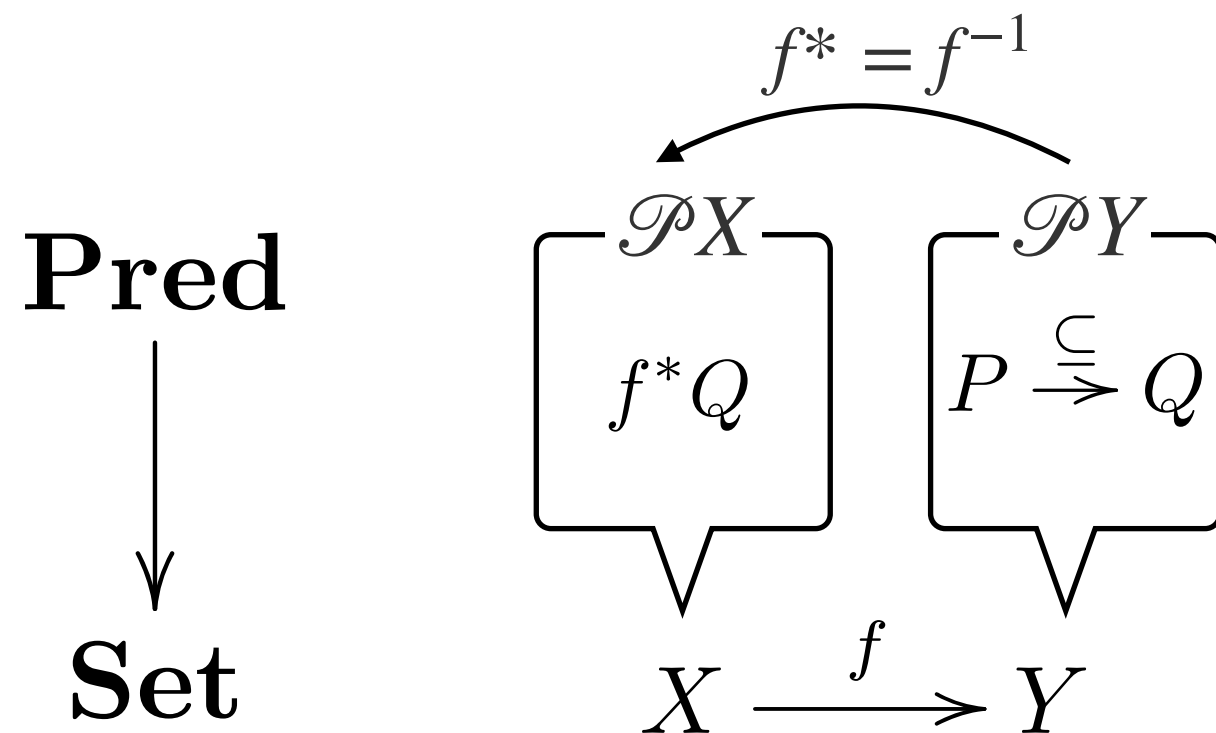
cartesian lifting

$$f^*Q \overset{\bar{f}}{\dashrightarrow} Q$$

$$X \xrightarrow{f} Y$$

Background: fibration

e.g. **Pred** $\rightarrow$ **Set** where **Pred** has objects $(Y, Q \subseteq Y)$



cartesian lifting

$$(f^{-1}Q \subseteq X) \xrightarrow{f} (Q \subseteq Y)$$

$$X \xrightarrow{f} Y$$

Our examples often use $\mathbb{B} = \mathbf{Set}$,
and $\mathbb{E}$ which models “predicates” over sets in $\mathbb{B}$

Background: (fibred) lifting

Def. $\dot{F} : \mathbb{E} \rightarrow \mathbb{E}$ is a **lifting** of $F : \mathbb{B} \rightarrow \mathbb{B}$ along p if

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{\dot{F}} & \mathbb{E} \\ \downarrow p & & \downarrow p \\ \mathbb{B} & \xrightarrow{F} & \mathbb{B} \end{array}$$

A lifting $\dot{F}$ is **fibred** if $\dot{F}$ preserves cartesian
i.e. for each $f : X \rightarrow Y$ in $\mathbb{B}$,

$$\begin{array}{ccc} \dot{F} \circlearrowleft \mathbb{E} & & \dot{F} f^* P \xrightarrow{\dot{F} \bar{f}} \dot{F} P \\ \downarrow p & \cong \downarrow & \downarrow \\ F \circlearrowleft \mathbb{B} & & (F f)^* \dot{F} P \xrightarrow{\overline{F f}} \dot{F} P \\ & & \downarrow \\ & & F X \xrightarrow{F f} F Y \end{array}$$

Outline

1. Background: Fibrations and liftings
2. IF/I coincidence
3. Conditions to ensure IF/I coincidence
for $\text{CLat}_\wedge$ -fibrations
4. Application to verification witness
5. Conclusion

IF/I coincidence

IA-FC coincidence over an init alg

Def. $(p, F, \dot{F})$ satisfies the **IF/I coincidence** if

1. There exists an init F -alg $\beta : F(\mu F) \xrightarrow{\cong} \mu F$;
2. There exists an init $\dot{F}$ -alg $\dot{\beta} : \dot{F}(\mu \dot{F}) \xrightarrow{\cong} \mu \dot{F}$ above β ;
3. $\dot{\beta}^{-1}$ is final over β^{-1} .

$$\begin{array}{ccc}
 \begin{array}{c} \dot{F} \curvearrowright \mathbb{E} \\ \downarrow p \\ F \curvearrowright \mathbb{B} \end{array} & \dot{F}P \xleftarrow{\gamma} P & \implies \begin{array}{c} \dot{F}(\mu \dot{F}) \xleftarrow[\cong]{\dot{\beta}^{-1}} \mu \dot{F} \\ \dot{F}f \uparrow \quad \uparrow f \\ \dot{F}P \xleftarrow{\gamma} P \end{array} \\
 & F(\mu F) \xleftarrow[\cong]{\beta^{-1}} \mu F; & F(\mu F) \xleftarrow[\cong]{\beta^{-1}} \mu F;
 \end{array}$$

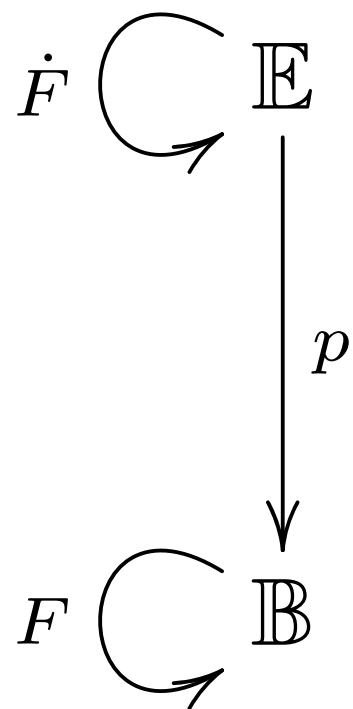
Intuition of IF/I coincidence

- Cond 1 & 2 are norm

Def. $(p, F, \dot{F})$ satisfies the **IF/I coincidence** if

1. There exists an init F -alg $\beta : F(\mu F) \xrightarrow{\cong} \mu F$;
2. There exists an init $\dot{F}$ -alg $\dot{\beta} : \dot{F}(\mu \dot{F}) \xrightarrow{\cong} \mu \dot{F}$ above β ;
3. $\dot{\beta}^{-1}$ is final over β^{-1} .

- Cond 3:



$$\dot{F}(\mu \dot{F}) \xleftarrow[\cong]{\dot{\beta}^{-1}} \mu \dot{F}$$

Greatest invariant

$$\dot{F}P \xleftarrow[\gamma]{\quad} P$$

Invariant preserved by β^{-1}
 $P \leq (\beta^{-1})^* \dot{F}P$

$$F(\mu F) \xleftarrow[\cong]{\beta^{-1}} \mu F$$

Transition system

so $\dot{\beta}$ is an inductive and coinductive predicate.

Outline

1. Background: Fibrations and liftings
2. IF/I coincidence
3. Conditions to ensure IF/I coincidence
for $\text{CLat}_\wedge$ -fibrations
4. Application to verification witness
5. Conclusion

$\mathbf{CLat}_\wedge$ -fibration

Def. $p : \mathbb{E} \rightarrow \mathbf{Set}$ is a $\mathbf{CLat}_\wedge$ -fibration if each $\mathbb{E}_X$ is a complete lattice and each f^* preserves all meets.

cf. [Komorida+, LICS19], [Sprunger+, CMCS18]

They model sets with predicates.

e.g. forgetful functors $\mathbb{E} \rightarrow \mathbf{Set}$

- $\mathbb{E} = \mathbf{Pred}$, the category of predicates $(X, P \subseteq X)$
- $\mathbb{E} = \mathbf{ERel}$, the category of binary rels $(X, R \subseteq X \times X)$
- $\mathbb{E} = \mathbf{Set}/\Omega$, lax slice category with obj f and morph h :

$$\begin{array}{ccc} X & \xrightarrow{h} & Y \\ & \searrow \scriptstyle \leq_X \swarrow & \\ f & & g \\ & \searrow \swarrow & \\ & \Omega & \end{array}$$

IF/I coincidence in a $\mathbf{CLat}_\wedge$ -fibration

Def. $(p, F, \dot{F})$ satisfies the **IF/I coincidence** if

1. There exists an init F -alg $\beta : F(\mu F) \xrightarrow{\cong} \mu F$;
2. There exists an init $\dot{F}$ -alg $\dot{\beta} : \dot{F}(\mu \dot{F}) \xrightarrow{\cong} \mu \dot{F}$ above β ;
3. $\dot{\beta}^{-1}$ is final over β^{-1} .

$$\mathbb{E}_{\mu F} \xrightarrow{\dot{F}} \mathbb{E}_{F \mu F} \xrightarrow{(\beta^{-1})^*} \mathbb{E}_{\mu F}$$

Cond 2, 3 are simplified to

- Cond 2': There exists a lfp $\mu \dot{F} \in \mathbb{E}_{\mu F}$ of $(\beta^{-1})^* \dot{F}$
- Cond 3': $\mu \dot{F}$ is a gfp of $(\beta^{-1})^* \dot{F}$

IF/I coincidence yields a unique fixed-point $\mu \dot{F}$ of $(\beta^{-1})^* \dot{F}$.

Outline

1. Background: Fibrations and liftings
2. IF/I coincidence
3. Conditions to ensure IF/I coincidence
for $\text{CLat}_\wedge$ -fibrations
4. Application to verification witness
5. Conclusion

Stable chain colimit

Fibrational stability under pullback for chain colimits

Def. $p : \mathbb{E} \rightarrow \mathbb{B}$ has **stable chain colimits** if for each $D : \mathbf{Ord}_{<\lambda} \rightarrow \mathbb{B}$,

1. $\mathbb{B}$ has a colimit of D ;
2. for each $P \in \mathbb{E}_{\text{colim } D}$, the yellow chain forms a colimit diagram.

$$\begin{array}{ccc}
 \begin{array}{c} \dot{F} \circlearrowleft \mathbb{E} \\ \downarrow p \\ F \circlearrowleft \mathbb{B} \end{array} & \kappa_0^* P \longrightarrow \kappa_1^* P \longrightarrow \dots \longrightarrow P \cong \text{colim}_{i < \lambda} \kappa_i^* P & \\
 & \begin{array}{c} D0 \longrightarrow D1 \longrightarrow \dots \longrightarrow \text{colim } D \\ \searrow \quad \quad \quad \nearrow \kappa_1 \\ \quad \quad \quad \kappa_0 \end{array} &
 \end{array}$$

This works well in Adamek's chain construction of IAs.

e.g. $\mathbf{Pred} \rightarrow \mathbf{Set}$, $\mathbf{ERel} \rightarrow \mathbf{Set}$, $\mathbf{Set}/\Omega \rightarrow \mathbf{Set}$

$$\mathbb{C} \rightarrow \xrightarrow{\text{cod}} \mathbb{C}$$

if chain colimits in $\mathbb{C}$ are stable under pullback. (cf. [Lurie, Ann. Math. Stud. '09])

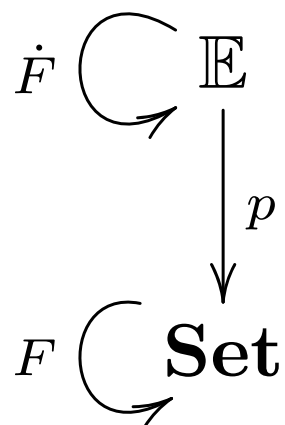
Main result

Here are mild sufficient conditions for IF/I coincidence

Thm. Consider a $\mathbf{CLat}_\wedge$ -fibration $p : \mathbb{E} \rightarrow \mathbf{Set}$.

Then $(p, F, \dot{F})$ satisfies the IF/I coincidence if

1. there exists an init F -alg;
2. $\dot{F}$ is a **fibred lifting** of F ;
3. p has **stable chain colimits**.



$$F(\mu F) \xrightarrow[\cong]{\beta} \mu F$$

Def. $(p, F, \dot{F})$ satisfies the **IF/I coincidence** if

1. There exists an init F -alg $\beta : F(\mu F) \xrightarrow{\cong} \mu F$;
2. There exists an init $\dot{F}$ -alg $\dot{\beta} : \dot{F}(\mu \dot{F}) \xrightarrow{\cong} \mu \dot{F}$ above β ;
3. $\dot{\beta}^{-1}$ is final over β^{-1} .

More information about the main result

Our paper includes ...

- Conditions for general (not $\text{CLat}_\wedge$) fibrations
 - we need more conditions
about preservation of chain colimits
- (technical) Non-example for main result:
 - $(p, F, \dot{F})$
s.t. $\times$ IF/I coincidence, $\times$ stable chain colimits

Outline

1. Background: Fibrations and liftings
2. IF/I coincidence
3. Conditions to ensure IF/I coincidence
for $\text{CLat}_\wedge$ -fibrations
4. Application to verification witness
5. Conclusion

Verification problems using fixed-points

Revisiting the theory of fixed-points...

Liveness checking: $P \leq \mu F$ (or dually $\nu F \leq P$)

- often use Cousot-Cousot theorem
 - $P \leq \mu F$ if $P \leq F^\alpha(\perp)$ for some α
- witness: ranking function

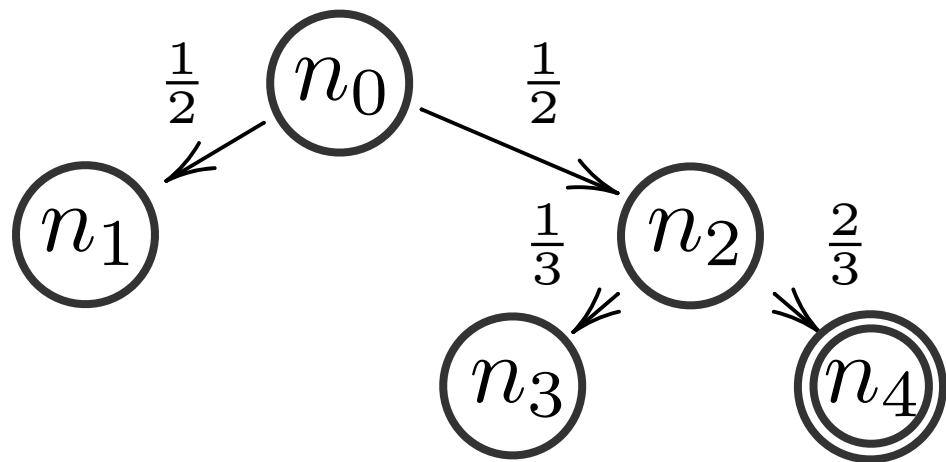
safety checking: $P \leq \nu F$ (or dually $\mu F \leq P$)

- often use Knaster-Tarski theorem
 - $P \leq \nu F$ if $P \leq FP$
- witness: invariant

IF/I coincidence yields

invariant-type witness for **liveness checking**.

Example: probabilistic liveness



Consider a finite tree t with circles $\bigcirc$ and $\bigcirc\bigcirc$.

Liveness problem: $\lambda \leq \Pr(\text{eventually reaching } \bigcirc\bigcirc \text{ in } t)$.

To prove the liveness problem,

- ordinary witness: ranking supermartingale [Fioriti&Hermanns, POPL'15]
- witness by IF/I coincidence: **invariant-like submartingale**

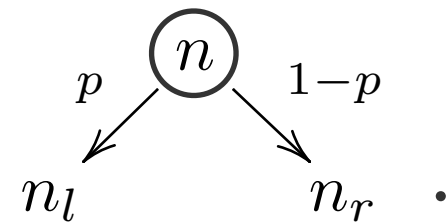
Invariant-like submartingale witness

Def. Let N be the set of nodes of t .

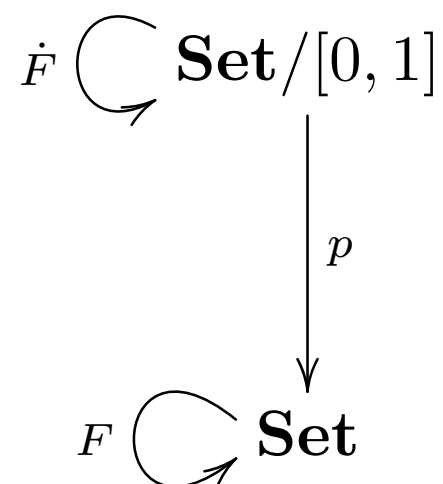
$f: N \rightarrow [0,1]$ is an **IF/I submartingale** if

1. $f(n) = 0$ for each leaf n ;

2. $f(n) \leq p f(n_l) + (1 - p) f(n_r)$ for each



Thm. For a finite tree t , an IF/I submartingale f yields $f(\text{the root}) \leq \text{Pr}(\text{eventually reaching } \odot)$.



$$\dot{F}(\mu \dot{F}) \xleftarrow[\cong]{\dot{\beta}^{-1}} \mu \dot{F} \dots \text{root} \mapsto \text{Pr}(\text{eventually reaching } \odot)$$

$$\begin{array}{c} \uparrow \dots \uparrow \\ \dot{F} f \xleftarrow[\gamma]{} f \dots \text{IF/I submartingale} \end{array}$$

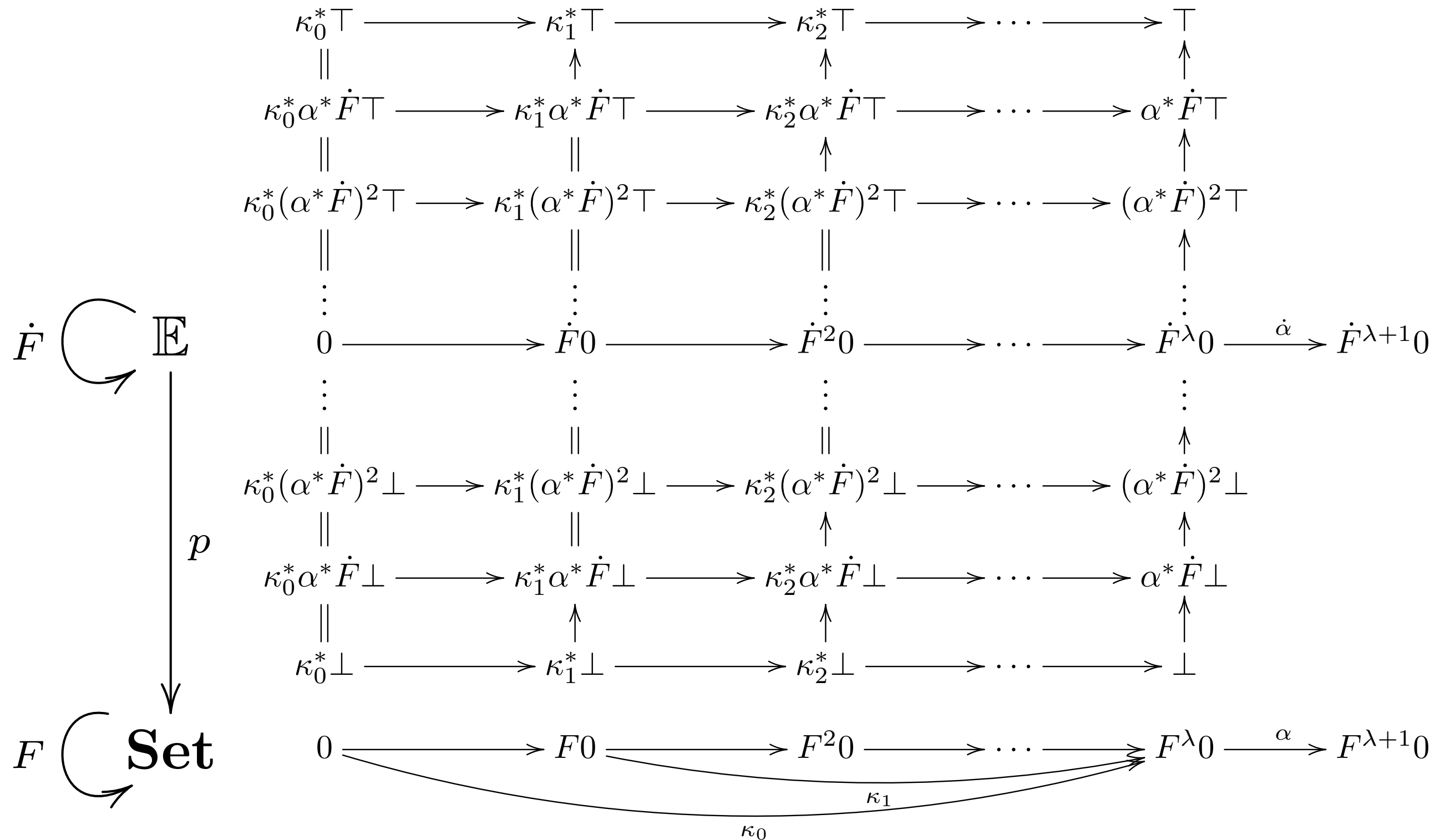
$$F(\mu F) \xleftarrow[\cong]{\beta^{-1}} \mu F = \text{finite trees}$$

Conclusion

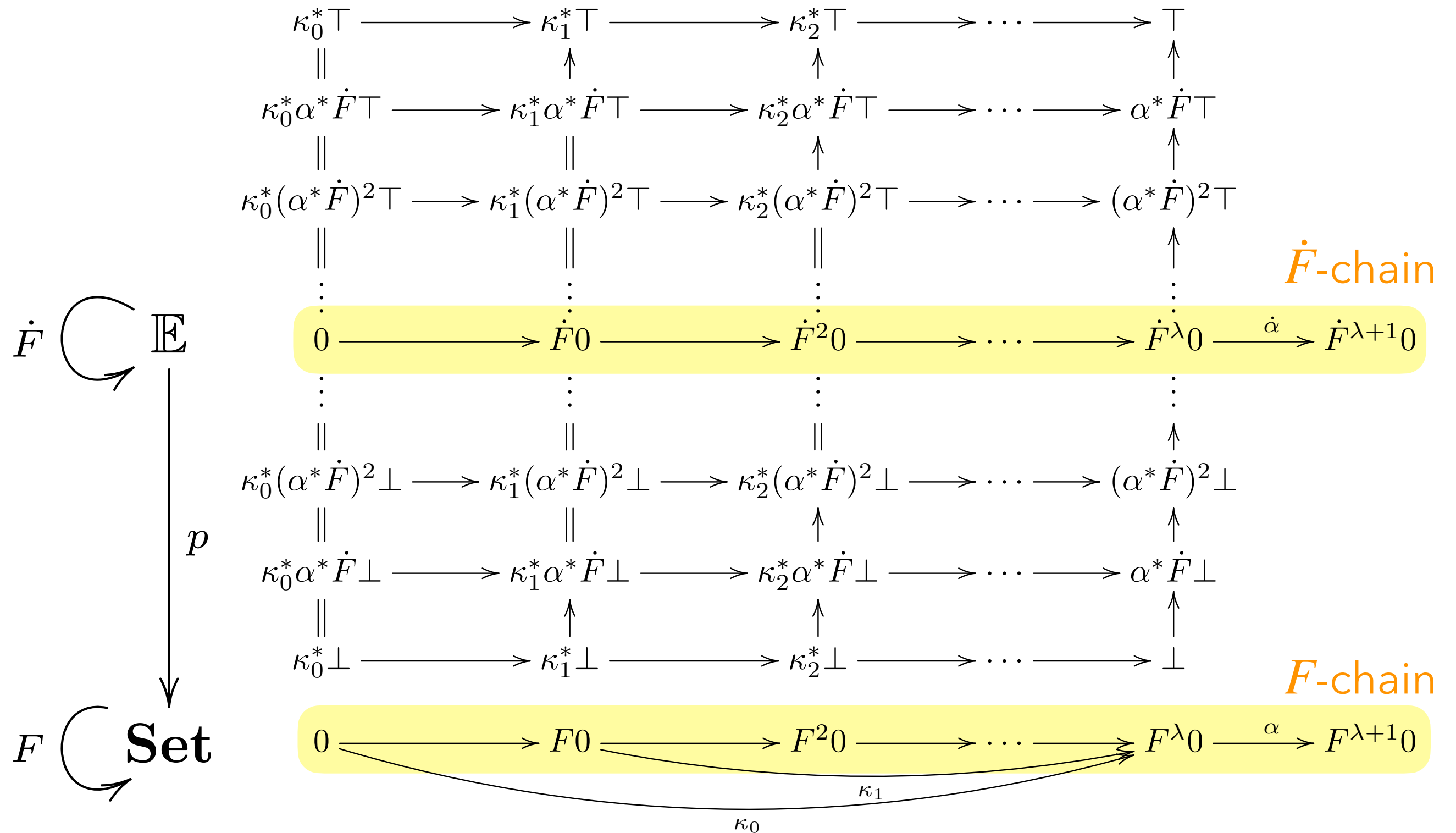
- IF/I coincidence: a fibrational framework for IA-FC coincidence over IAs,
- Mild conditions to ensure IF/I coincidence
 - Fibredness of liftings and Stability of chain colimits
 - not rely on enrichment (cf. [Pitts, Inf Comput.'96], [Barr, J. Pure Appl. Algebra'92])
- Coinductive verification witnesses for inductive properties.
 - probabilistic liveness & tree automata
- Future work: relationship to other homset enrichment approaches[Pitts, Inf Comput.'96], [Barr, J. Pure Appl. Algebra'92].

Additional slides

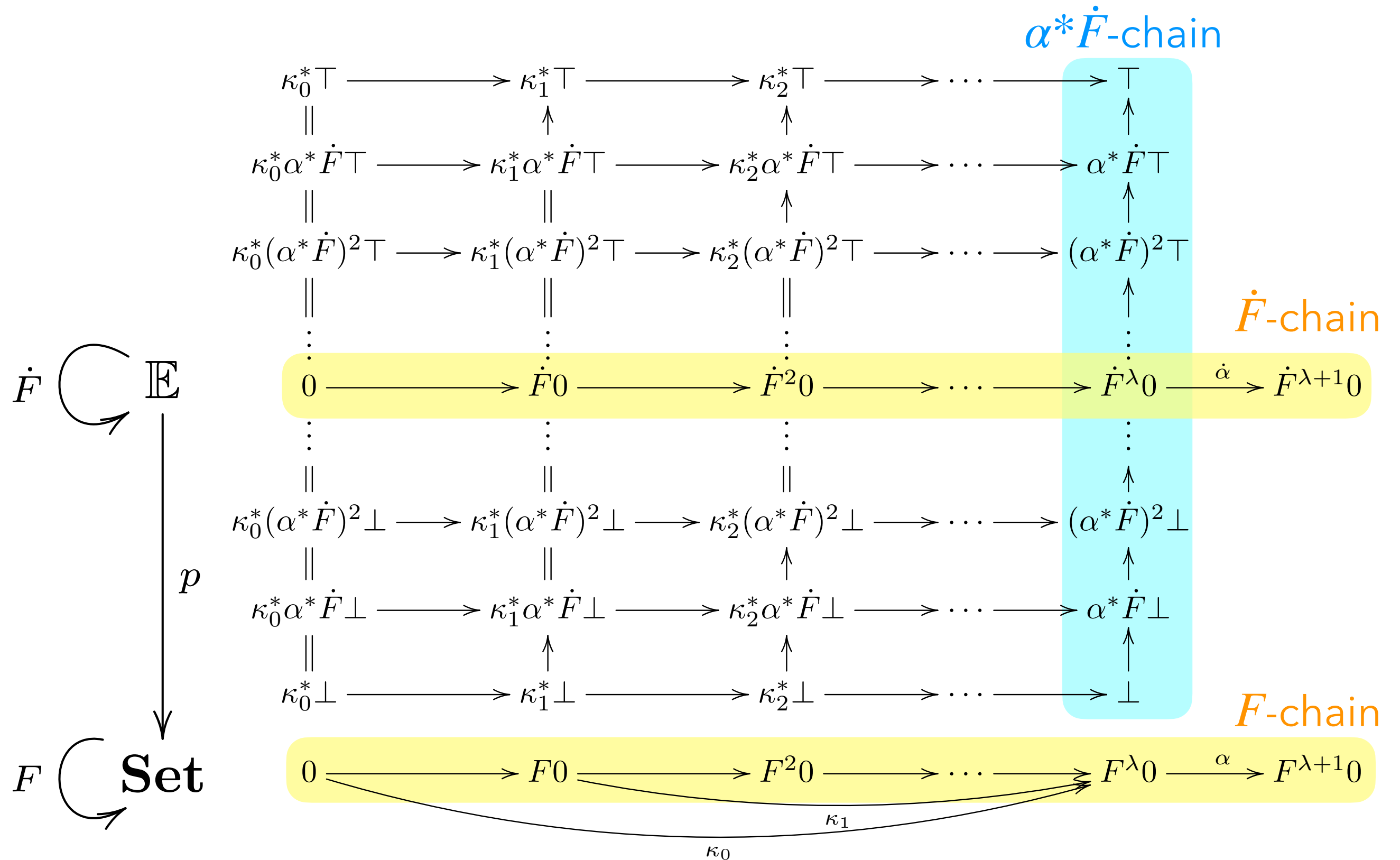
Main diagram for the proof



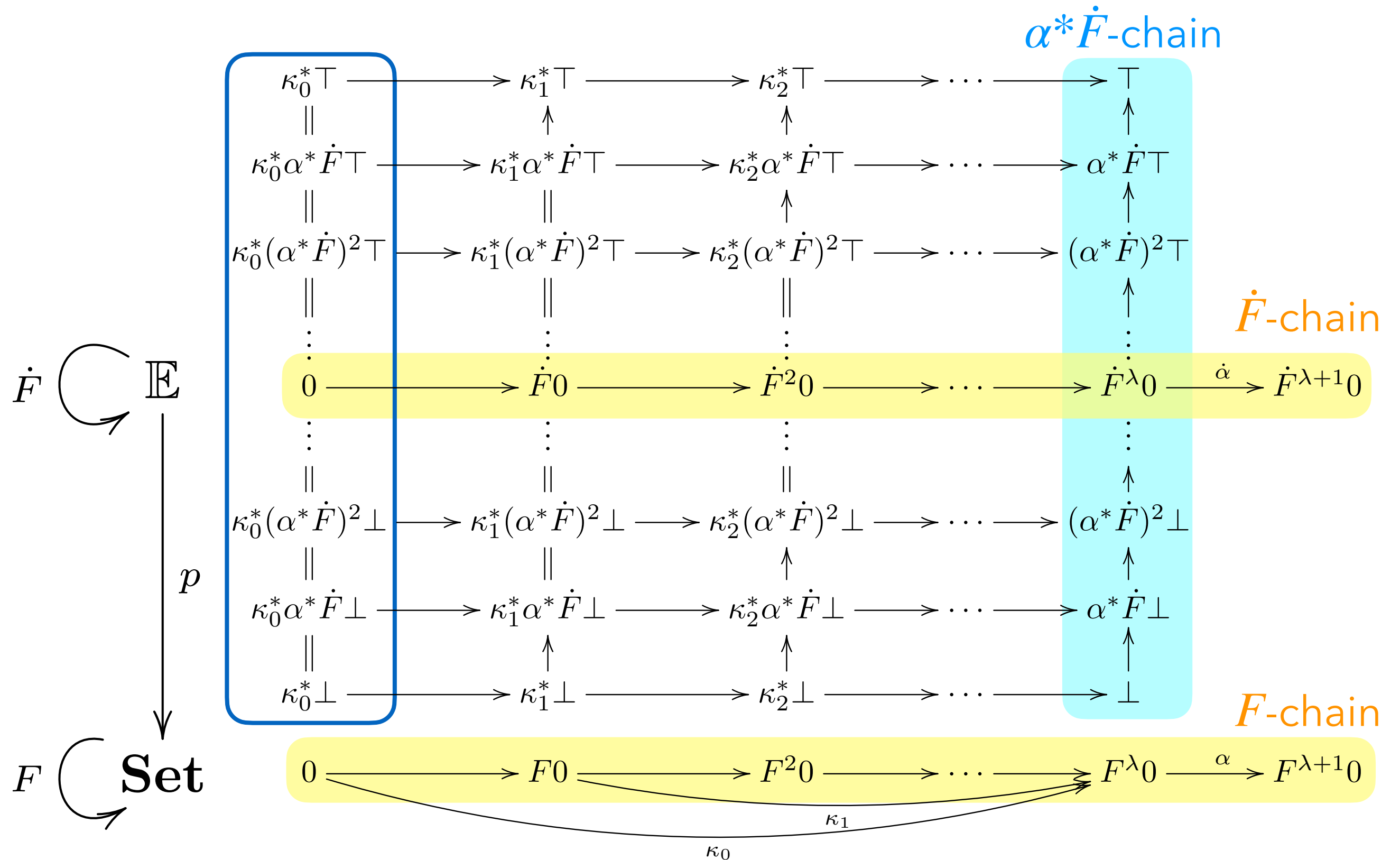
Main diagram for the proof



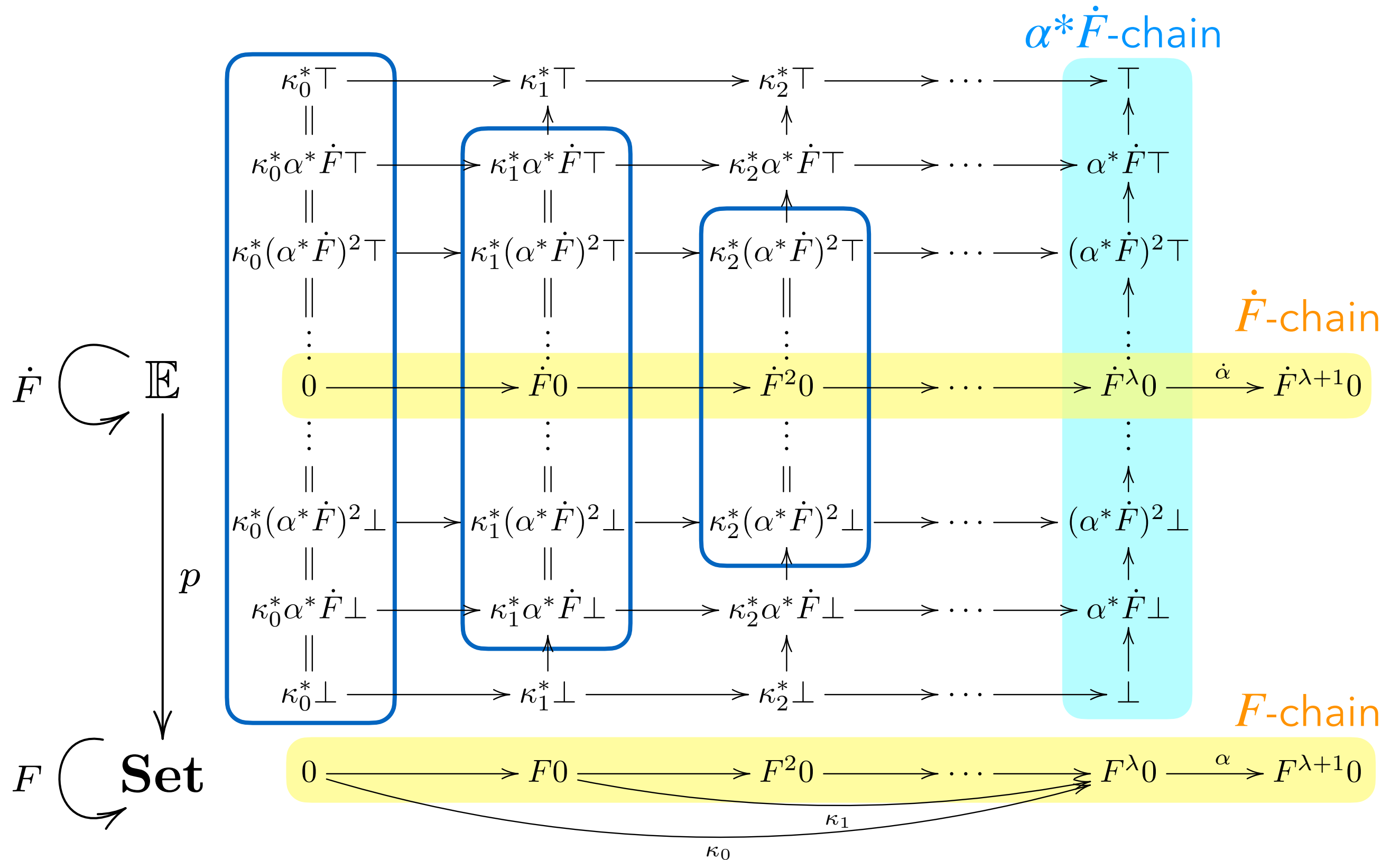
Main diagram for the proof



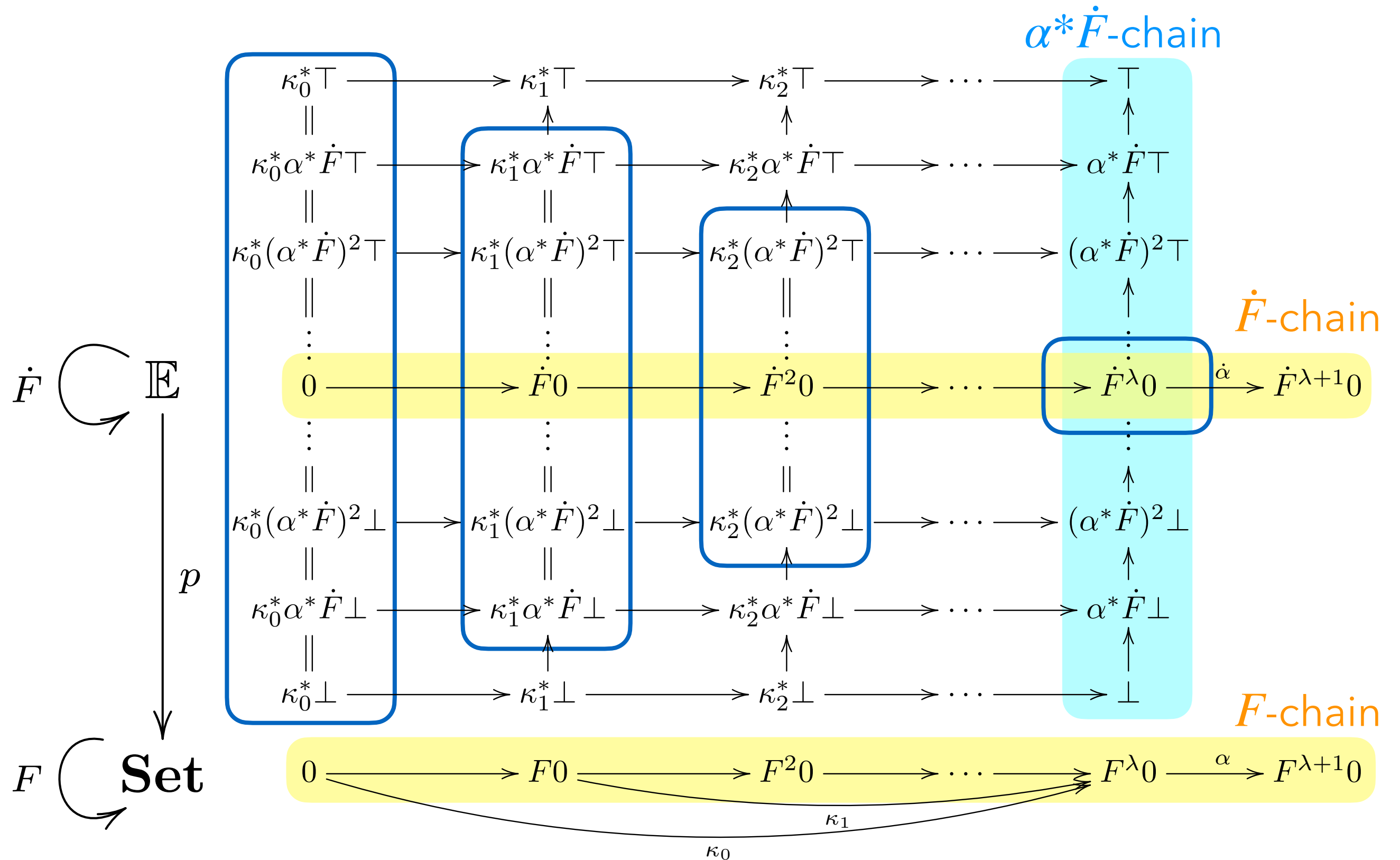
Main diagram for the proof



Main diagram for the proof



Main diagram for the proof



Initial algebra construction by chains

Def.

Let $\mathbb{C}$ be a chain-cocomplete category.

The **initial chain** of $F : \mathbb{C} \rightarrow \mathbb{C}$ is

$$0 \xrightarrow{\exists! u} F0 \xrightarrow{Fu} F^2 0 \xrightarrow{F^2 u} \dots \rightarrow F^\lambda 0 \rightarrow \dots$$

where $F^i 0 = F(F^{i-1} 0)$ (if i : succ)

$F^i 0 = \text{colim}_{j < i} F^j 0$ (if i : limit).

Prop. [Adamek, '74]

If $F^\lambda 0 \xrightarrow{\cong} F^{\lambda+1} 0$ in the init chain (or it converges in λ steps)
then its inverse is an initial algebra.

Initial chain coincidence

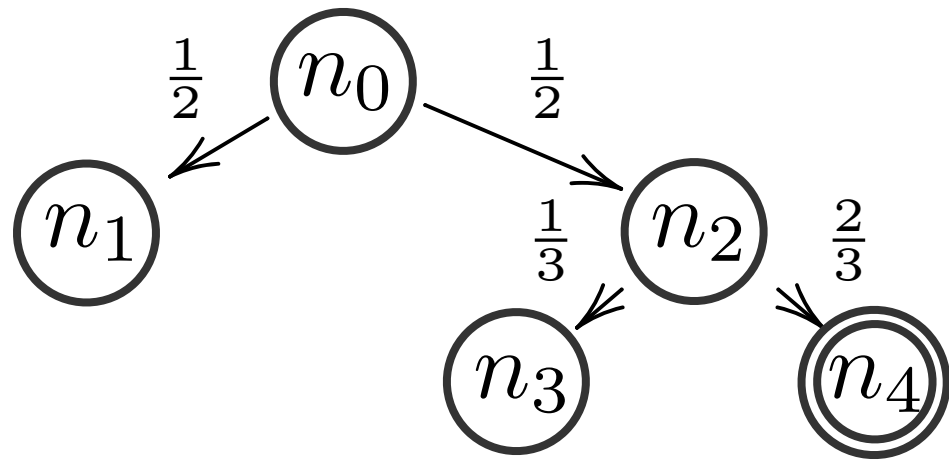
Lem.

Assume $\mathbb{E}, \mathbb{B}$ are chain-cocomplete and
 $p : \mathbb{E} \rightarrow \mathbb{B}$ strictly preserves chain colimits.
 Then the init chain of $\dot{F}$ is above that of F .

$$\begin{array}{ccc}
 \dot{F} \begin{array}{c} \curvearrowright \\ \mathbb{E} \end{array} & & 0 \longrightarrow \dot{F}0 \longrightarrow \dots \longrightarrow \dot{F}^\lambda 0 \xrightarrow{\cong} \dot{F}^{\lambda+1} 0 \longrightarrow \dots \\
 \downarrow p & & \\
 F \begin{array}{c} \curvearrowright \\ \mathbb{B} \end{array} & & 0 \longrightarrow F0 \longrightarrow \dots \longrightarrow F^\lambda 0 \xrightarrow{\cong} F^{\lambda+1} 0 \longrightarrow \dots
 \end{array}$$

If $\dot{F}$ has an initial algebra by the initial chain,
 then $\text{init } \dot{F}\text{-alg}$ is above $\text{init } F\text{-alg}$.

Example: probabilistic liveness



Let $N = \{n_i \mid i = 0, \dots, 4\}$ and we define $\dot{F} : [0, 1]^N \rightarrow [0, 1]^N$ by

$$\dot{F}(N \xrightarrow{f} [0, 1]) = (n \in N) \mapsto \begin{cases} 1 & \text{if } \textcircled{\textcircled{n}} \\ 0 & \text{if } \textcircled{n} \text{ and it is a leaf} \\ pf(n_l) + (1-p)f(n_r) & \text{if } \begin{array}{c} \textcircled{n} \\ \swarrow \quad \searrow \\ n_l \quad n_r \end{array} \end{cases}$$

then $\mu\dot{F}(n_0) = \text{Pr}(\text{eventually reaching } \textcircled{\textcircled{}})$.

To prove liveness problem $f \leq \mu\dot{F}$,

- ordinary witness: ranking supermartingale [Fioriti&Hermanns, POPL'15]
- witness by IF/I coincidence: **invariant-like submartingale**