Robust Hyperproperty Preservation for Secure Compilation

Deepak Garg[1] Cătălin Hriţcu[2] Marco Patrignani[3]
Marco Stronati[2] David Swasey[1]

13th January 2018

1 MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS

2 Inria inventeurs du monde numérique

3 CISPA Center for IT-Security, Privacy and Accountability

Special Thanks to:




Contents

Background & Motivation

- many criteria imply secure compilation

  preserving memory safety, CFI, non interference, program equivalence

Background & Motivation

- many criteria imply secure compilation

  preserving memory safety, CFI, non interference, program equivalence

Is that all?

Background & Motivation

- many criteria imply secure compilation

  preserving memory safety, CFI, non interference, program equivalence

Goal: study criteria that

Background & Motivation

- many criteria imply secure compilation

  preserving memory safety, CFI, non interference, program equivalence

Goal: study criteria that

- are security-driven and preserve security properties formally

Background & Motivation

- many criteria imply secure compilation

  preserving memory safety, CFI, non interference, program equivalence

Goal: study criteria that

- are security-driven and preserve security properties formally
- are robust (hold for all adversarial context)

Background & Motivation

- many criteria imply secure compilation

  preserving memory safety, CFI, non interference, program equivalence

Relate backtranslation techniques and property preservation

Goal:

- are security-driven and preserve security properties formally
- are robust (hold for all adversarial context)

HyperProperties Clarkson & Schneider '08

HyperProperties Clarkson & Schneider '08

- properties = sets of traces

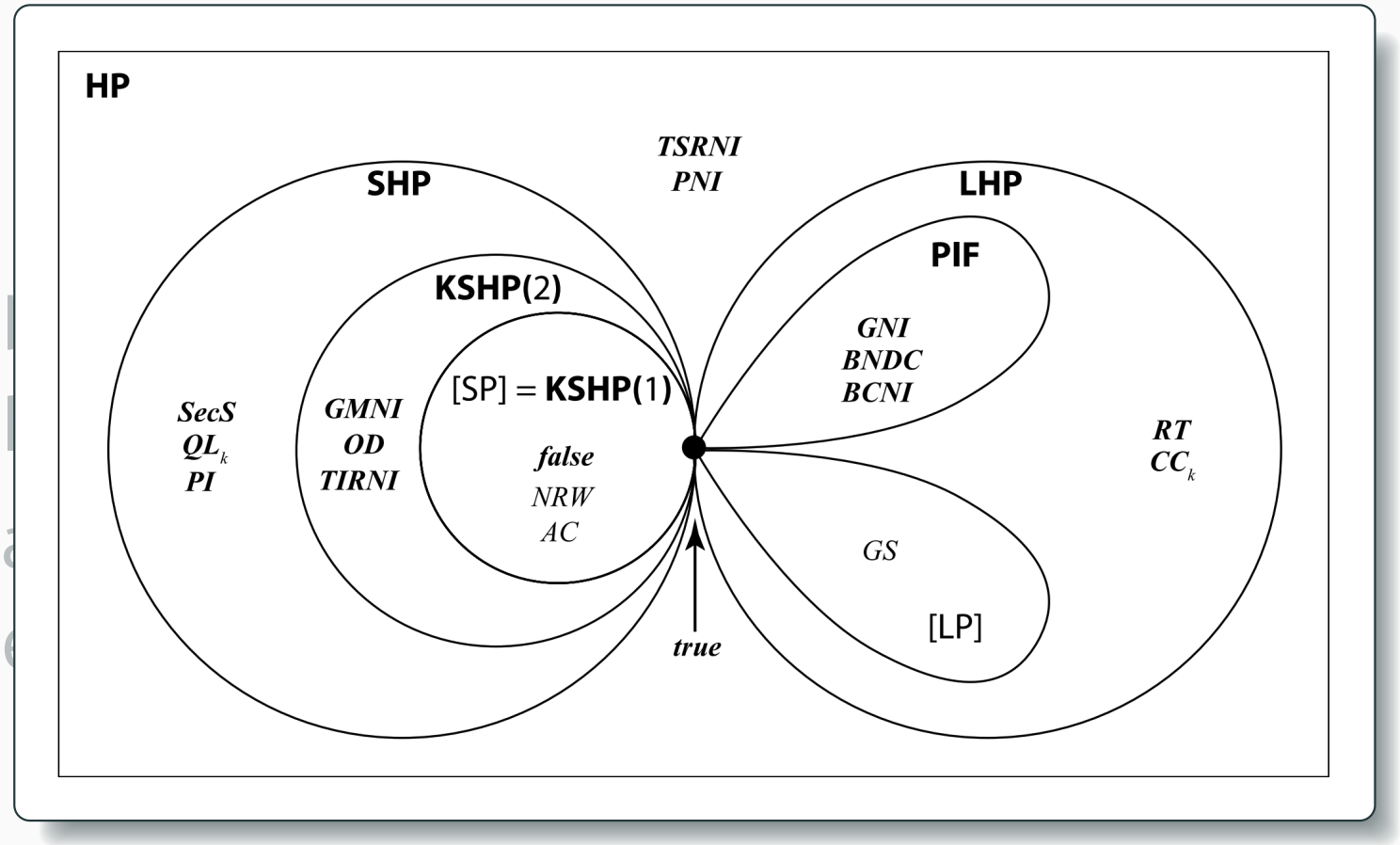
HyperProperties Clarkson & Schneider '08

- properties = sets of traces
- hyperproperties = sets of sets of traces

HyperProperties Clarkson & Schneider '08

- properties = sets of traces
- hyperproperties = sets of sets of traces
- are organised in subclasses for expressiveness

HyperProperties Clarkson & Schneider '08



Robust Compilation Criteria

Robust Compilation Partial Order

In the partial order:

- higher notions are stronger

Robust Compilation Partial Order

In the partial order:

- higher notions are stronger
  - and trickier to achieve

Robust Compilation Partial Order

In the partial order:

- higher notions are stronger
  - and trickier to achieve
- each notion comes in two flavours

Robust Compilation Partial Order

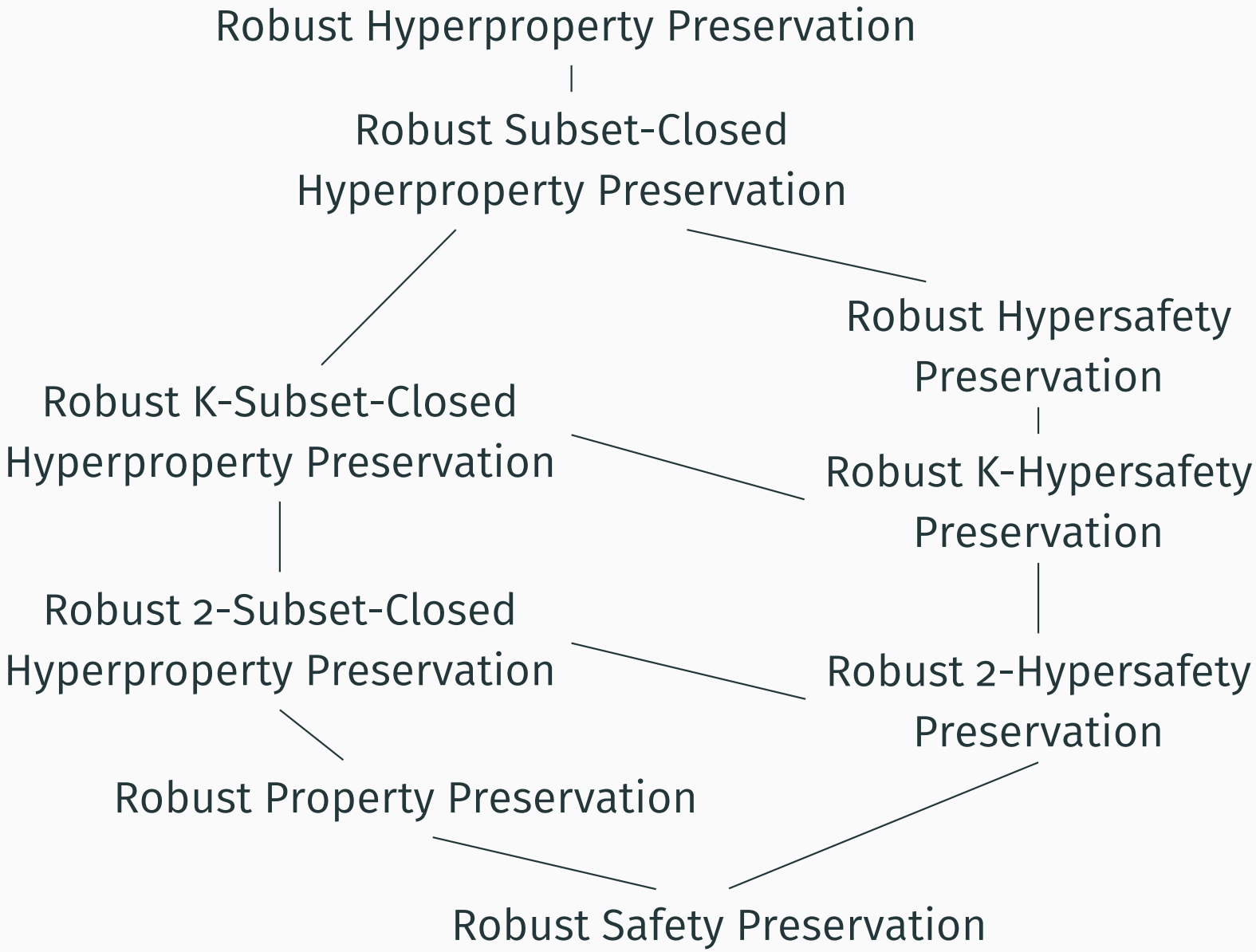
In the partial order:

- higher notions are stronger
  - and trickier to achieve
- each notion comes in two flavours
  - one with clear HP correspondence
  - one for simpler proofs

Notation

- $\mathrm{P_s}, \mathbf{P_t}$: components of S and $\mathbf{T}$
- $\mathbb{C}_\mathrm{s}\cdot, \mathbb{C}_\mathbf{t}\cdot$: contexts
- $\mathbb{C}_\mathrm{s}[\mathrm{P_s}], \mathbb{C}_\mathbf{t}[\mathbf{P_t}]$: whole programs
- $[\![\cdot]\!] : \mathrm{P_s} \to \mathbf{P_t}$: compiler from S to $\mathbf{T}$
- β: traces (possibly infinite), I/O with an environment
- $\mathtt{Behav}(\mathrm{P_s})$: set of traces of $\mathrm{P_s}$
- π: prefix (finite)
- $\prec$: prefixing

Robust Compilation Criteria



RPP: **Robust Property Preservation**

Definition (RPP)

$$[\![\cdot]\!] \in \mathrm{RPP} \stackrel{\mathrm{def}}{=} \forall \mathrm{P_s}, \mathtt{P}.$$
$$\text{if} \quad (\forall \mathbb{C}_s.\mathtt{Behav}\,(\mathbb{C}_s\,[\mathrm{P_s}]) \subseteq \mathtt{P})$$
$$\text{then} \quad (\forall \mathbb{C}_t.\mathtt{Behav}\,(\mathbb{C}_t\,[[\![\mathrm{P_s}]\!]]) \subseteq \mathtt{P})$$

RC: **Robust Compilation**

Definition: (RC)

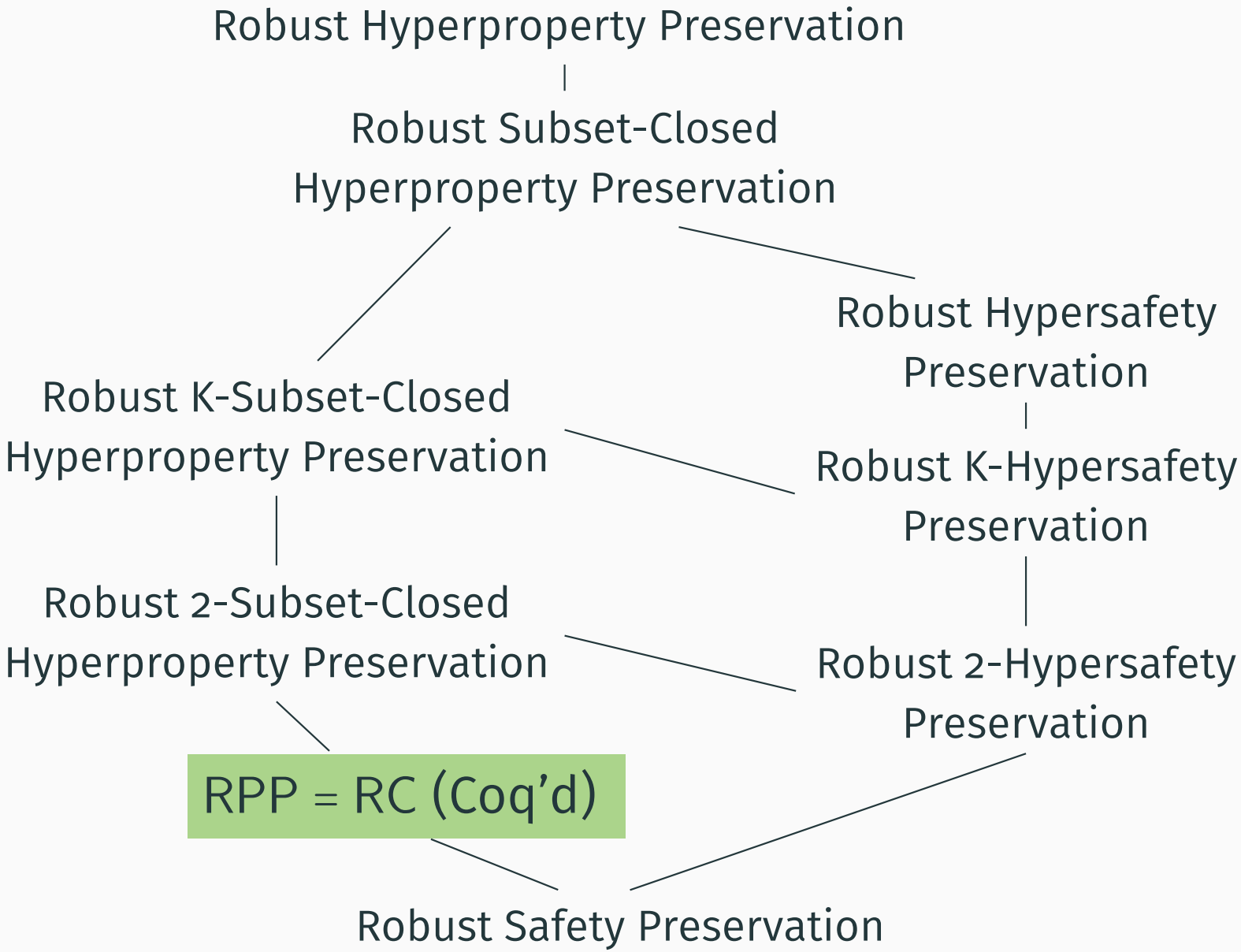
$$[\![\cdot]\!] \in \mathrm{RC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s, \beta. \exists \mathbb{C}_s.$$
$$\text{if} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$
$$\text{then} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

RC: **Robust Compilation**

Definition: (RC)

$$[\![\cdot]\!] \in \mathrm{RC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s, \beta. \exists \mathbb{C}_s.$$
$$\text{if} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$
$$\text{then} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

Robust Compilation Criteria



Robust Safety Property Preservation

Definition (RSPP)

$$[\![\cdot]\!] \in \mathrm{RSPP} \stackrel{\mathrm{def}}{=} \forall \mathrm{P_s}, \mathrm{P} \in SP\ .$$
$$\text{if}\quad (\forall \mathbb{C}_\mathrm{s}.\mathtt{Behav}\,(\mathbb{C}_\mathrm{s}\,[\mathrm{P_s}]) \subseteq \mathrm{P})$$
$$\text{then}\quad (\forall \mathbb{C}_\mathbf{t}.\mathtt{Behav}\,(\mathbb{C}_\mathbf{t}\,[[\![\mathrm{P_s}]\!]]) \subseteq \mathrm{P})$$

Robust Safety Compilation

Definition: (RC)

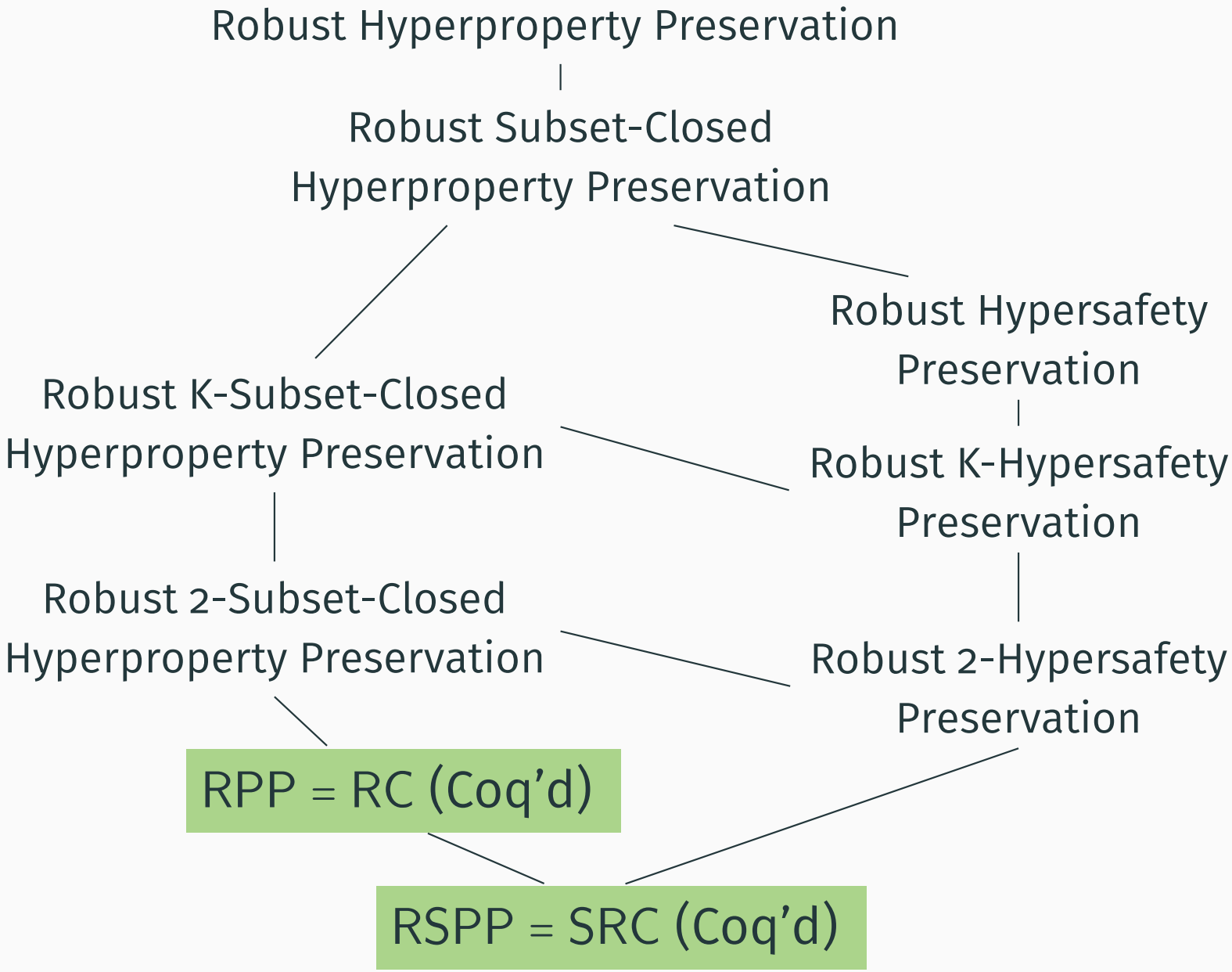
$$[\![\cdot]\!] \in \mathrm{RC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s, \beta. \exists \mathbb{C}_s.$$
$$\text{if} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$
$$\text{then} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

Robust Safety Compilation

Definition: (SRC)

$$[\![\cdot]\!] \in \mathrm{SRC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s, \pi . \exists \mathbb{C}_s .$$
$$\text{if } \pi \prec \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$
$$\text{then } \pi \prec \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

Robust Compilation Criteria



RSHP: **Robust Hypersafery Preservation**

Definition (RPP)

$$[\![\cdot]\!] \in \mathrm{RPP} \stackrel{\mathrm{def}}{=} \forall \mathrm{P_s}, \mathtt{P}.$$
$$\text{if } (\forall \mathbb{C}_\mathrm{s}.\mathtt{Behav}\,(\mathbb{C}_\mathrm{s}\,[\mathrm{P_s}]) \subseteq \mathtt{P})$$
$$\text{then } (\forall \mathbb{C}_\mathbf{t}.\mathtt{Behav}\,(\mathbb{C}_\mathbf{t}\,[[\![\mathrm{P_s}]\!]]) \subseteq \mathtt{P})$$

RSHP: **Robust Hypersafery Preservation**

Definition (RSHP)

$$[\![\cdot]\!] \in \text{RSHP} \stackrel{\text{def}}{=} \forall \mathtt{P_s}, \mathtt{H} \in \mathit{SHP}.$$
$$\text{if} \quad (\forall \mathbb{C}_s.\mathtt{Behav}(\mathbb{C}_s[\mathtt{P_s}]) \in \mathtt{H})$$
$$\text{then} \quad (\forall \mathbb{C}_t.\mathtt{Behav}(\mathbb{C}_t[[\![\mathtt{P_s}]\!]]) \in \mathtt{H})$$

SHRC: **Hypersafety Robust Compilation**

Definition: (RC)

$$[\![\cdot]\!] \in \mathrm{RC} \stackrel{\text{def}}{=} \forall \mathrm{P_s}, \mathbb{C}_\mathbf{t}, \pi.\exists \mathbb{C}_\mathrm{s}.$$
$$\text{if } \pi{\prec}\mathtt{Behav}\left(\mathbb{C}_\mathbf{t}\left[[\![\mathrm{P_s}]\!]\right]\right)$$
$$\text{then } \pi{\prec}\mathtt{Behav}\left(\mathbb{C}_\mathrm{s}\left[\mathrm{P_s}\right]\right)$$

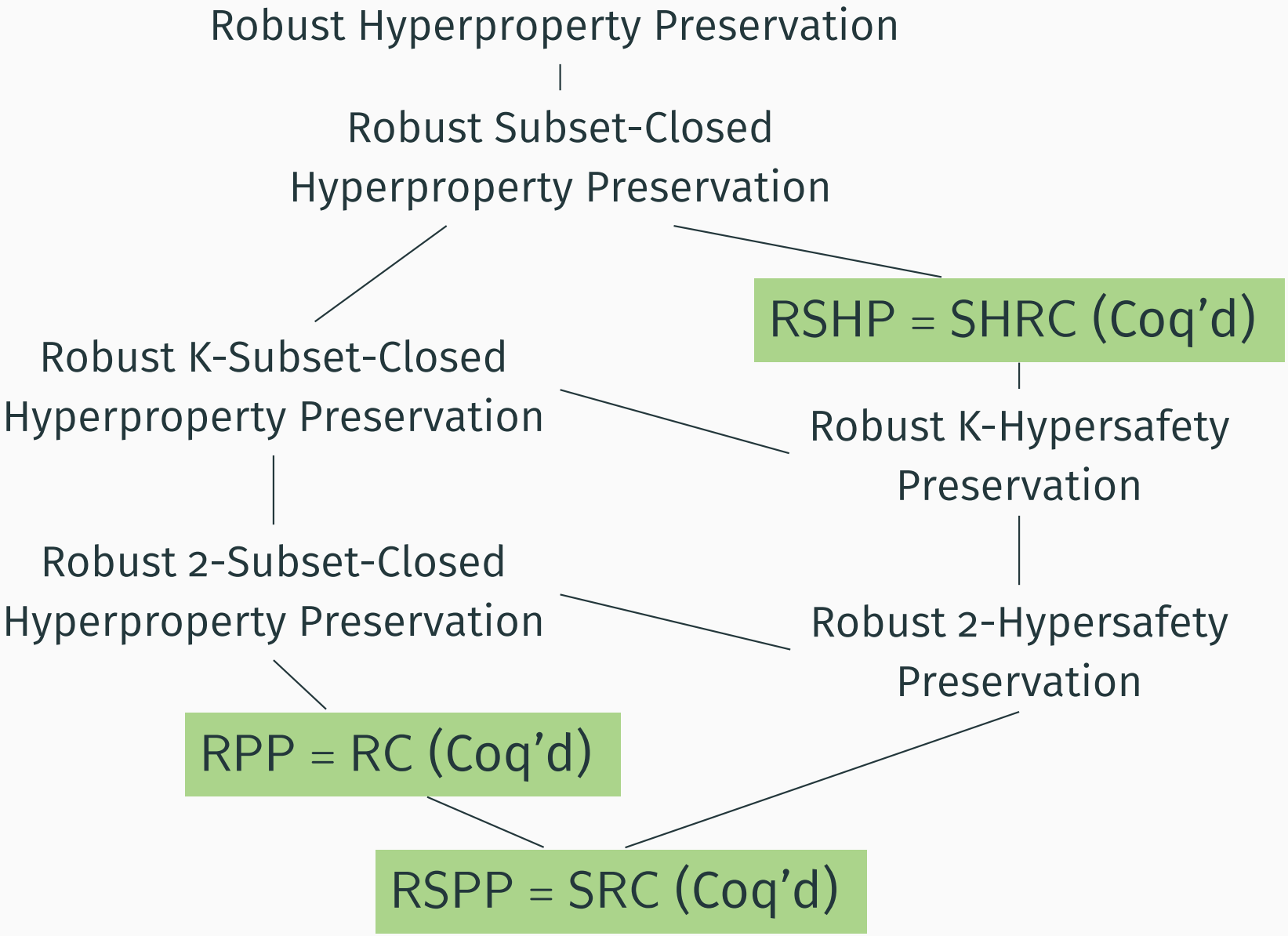
SHRC: **Hypersafety Robust Compilation**

Definition: (SHRC)

$$[\![\cdot]\!] \in \mathsf{SHRC} \stackrel{\text{def}}{=} \forall \mathtt{P_s}, \mathbb{C}_\mathtt{t}, \hat{\pi}.\exists \mathbb{C}_\mathtt{s}.$$
$$\text{if } \hat{\pi} \precsim \mathtt{Behav}\,(\mathbb{C}_\mathtt{t}\,[[\mathtt{P_s}]])$$
$$\text{then } \hat{\pi} \precsim \mathtt{Behav}\,(\mathbb{C}_\mathtt{s}\,[\mathtt{P_s}])$$

$\hat{\pi}$: finite set of prefixes

Robust Compilation Criteria



Robust Hyperproperty Preservation

Definition (RHP)

$$[\![\cdot]\!] \in \mathrm{RHP} \stackrel{\mathrm{def}}{=} \forall \mathrm{P_s}, \mathtt{H}.$$
$$\text{if} \quad (\forall \mathbb{C}_s.\mathtt{Behav}\,(\mathbb{C}_s\,[\mathrm{P_s}]) \in \mathtt{H})$$
$$\text{then} \quad (\forall \mathbb{C}_t.\mathtt{Behav}\,(\mathbb{C}_t\,[[\![\mathrm{P_s}]\!]]) \in \mathtt{H})$$

Hyperproperty Robust Compilation

Definition: (RC)

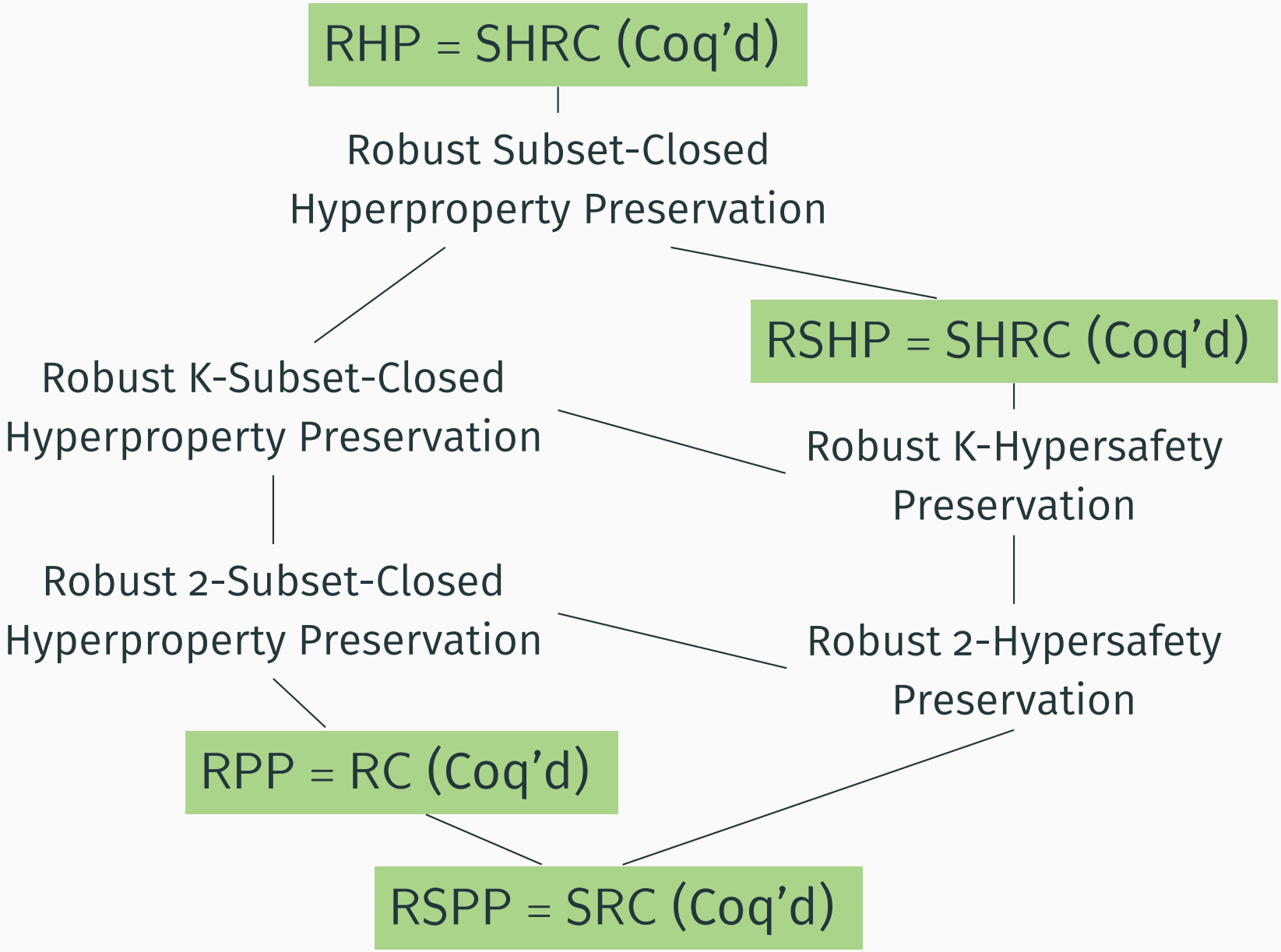
$$[\![\cdot]\!] \in \mathrm{RC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s, \beta. \exists \mathbb{C}_s.$$
$$\text{if} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$
$$\text{then} \quad \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

Hyperproperty Robust Compilation

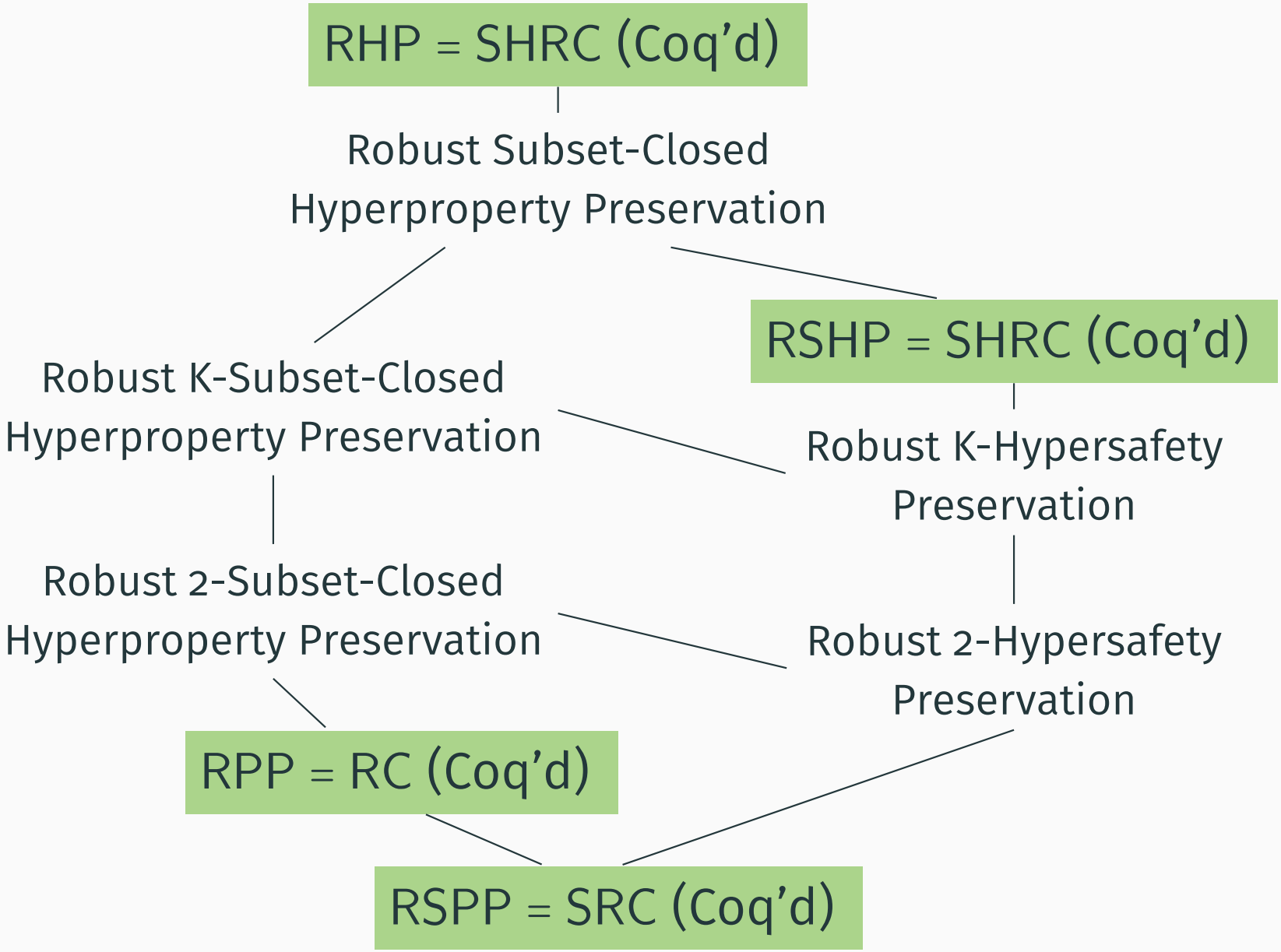
Definition: (HRC)

$$[\![\cdot]\!] \in \mathsf{HRC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s, \exists \mathbb{C}_s. \forall \beta.$$
$$\beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$
$$\iff \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

Robust Compilation Criteria

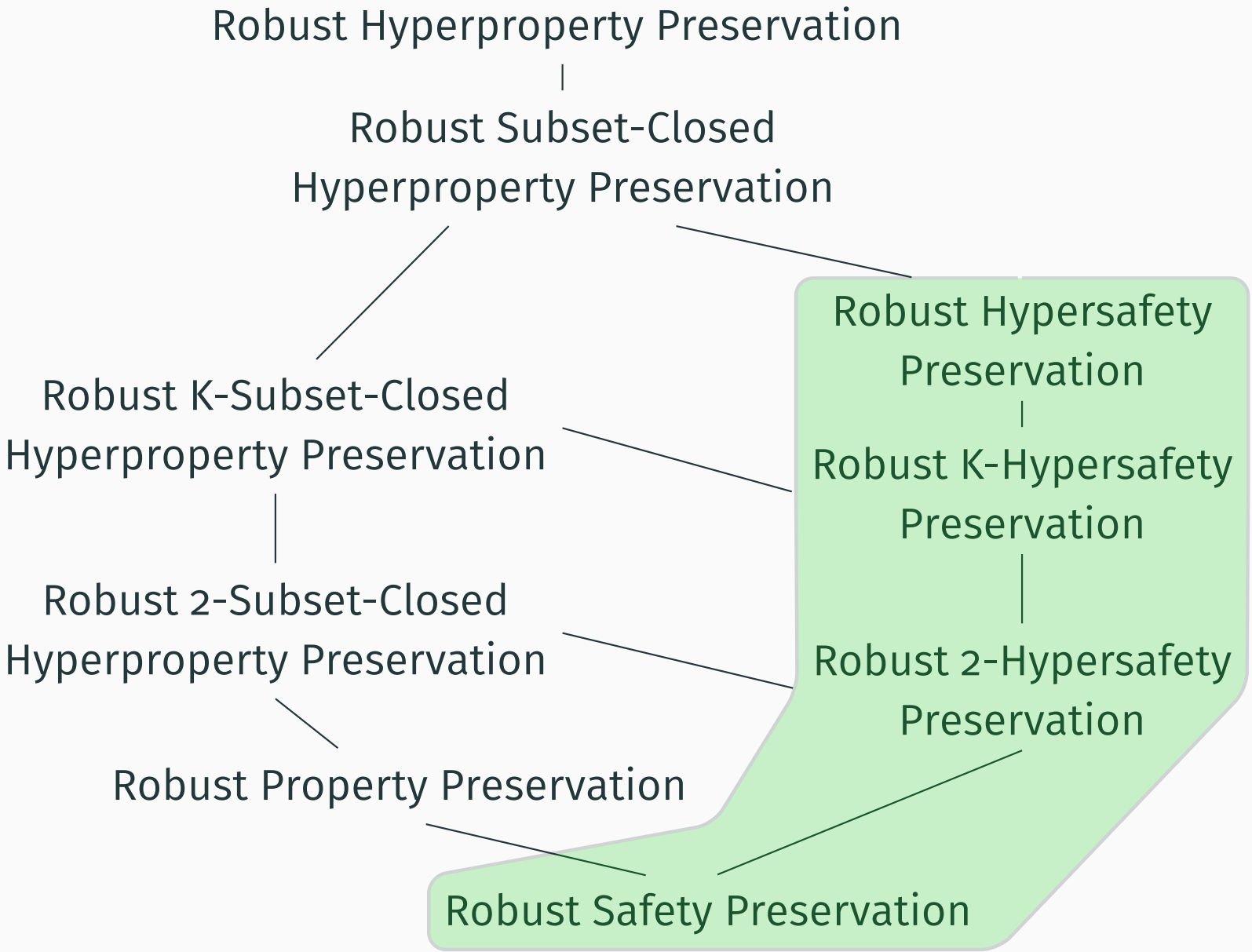


Robust Compilation Criteria

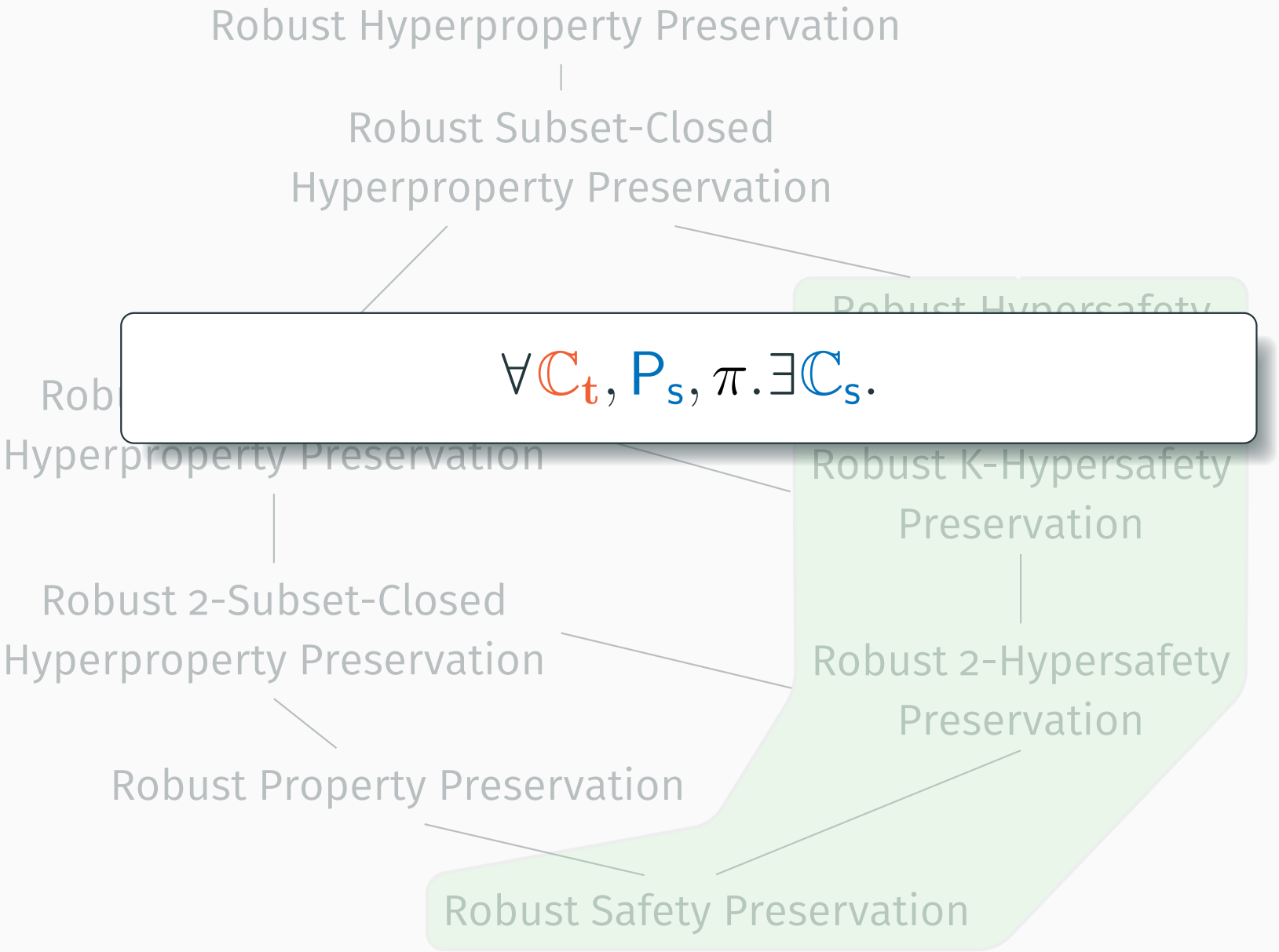


Proof Techniques

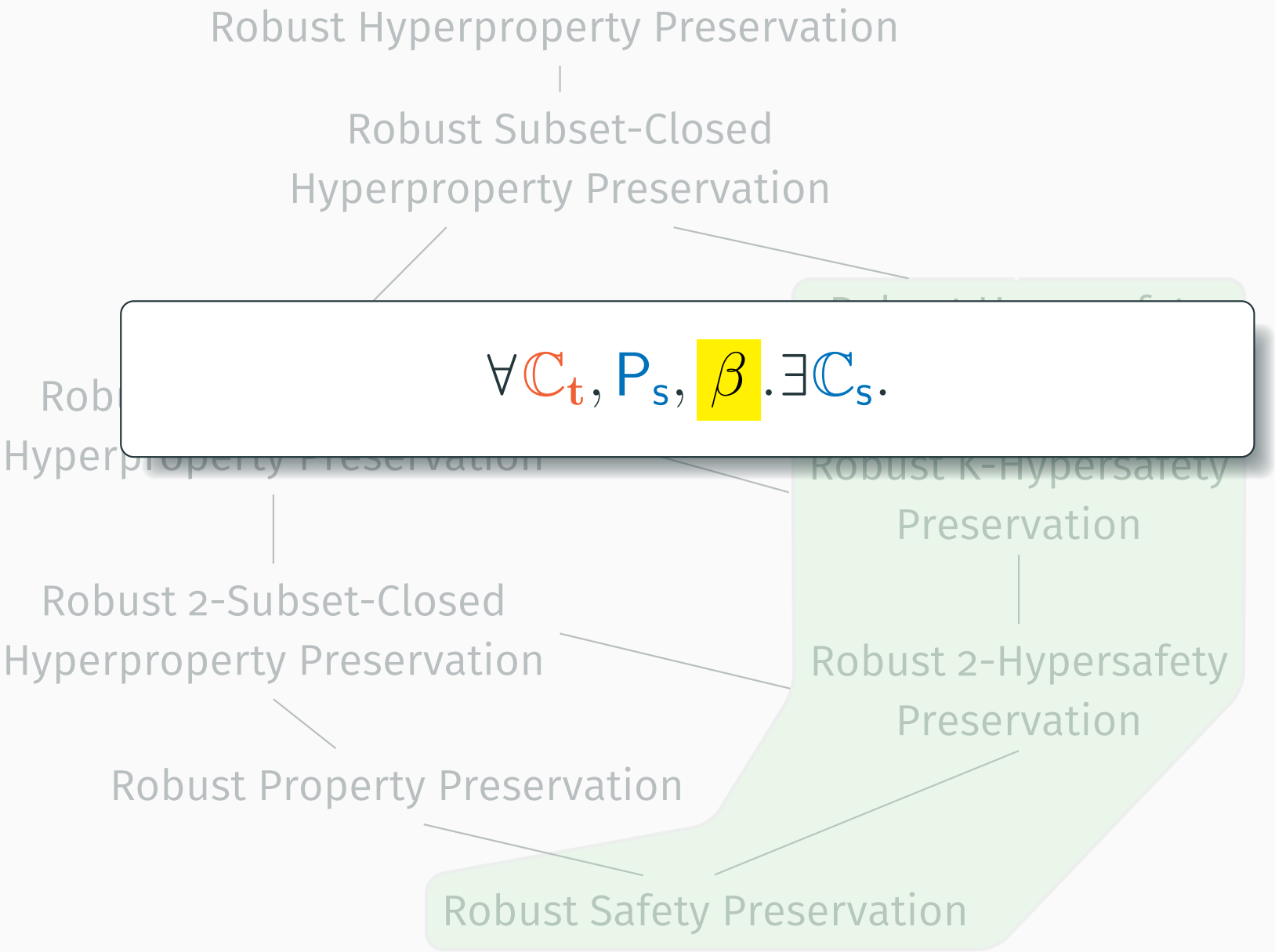
Proof Techniques



Proof Techniques

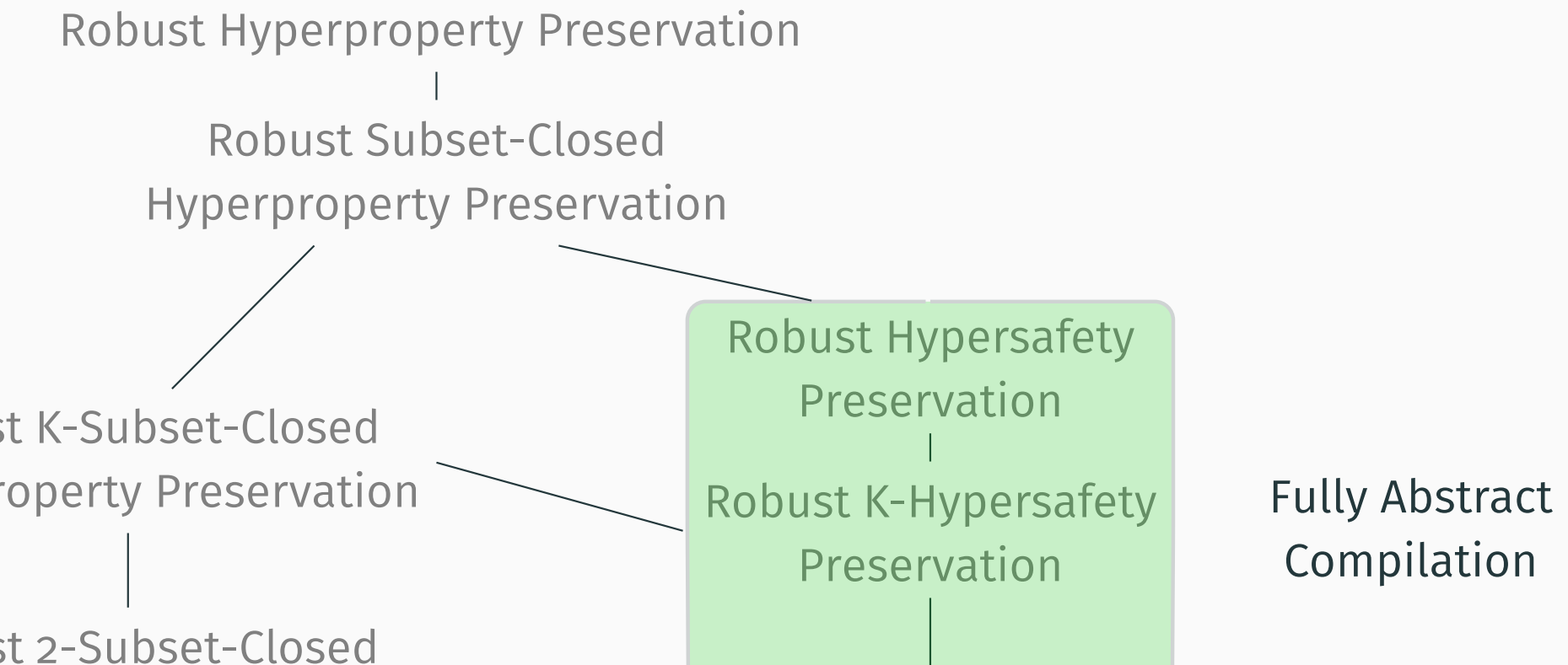


Proof Techniques



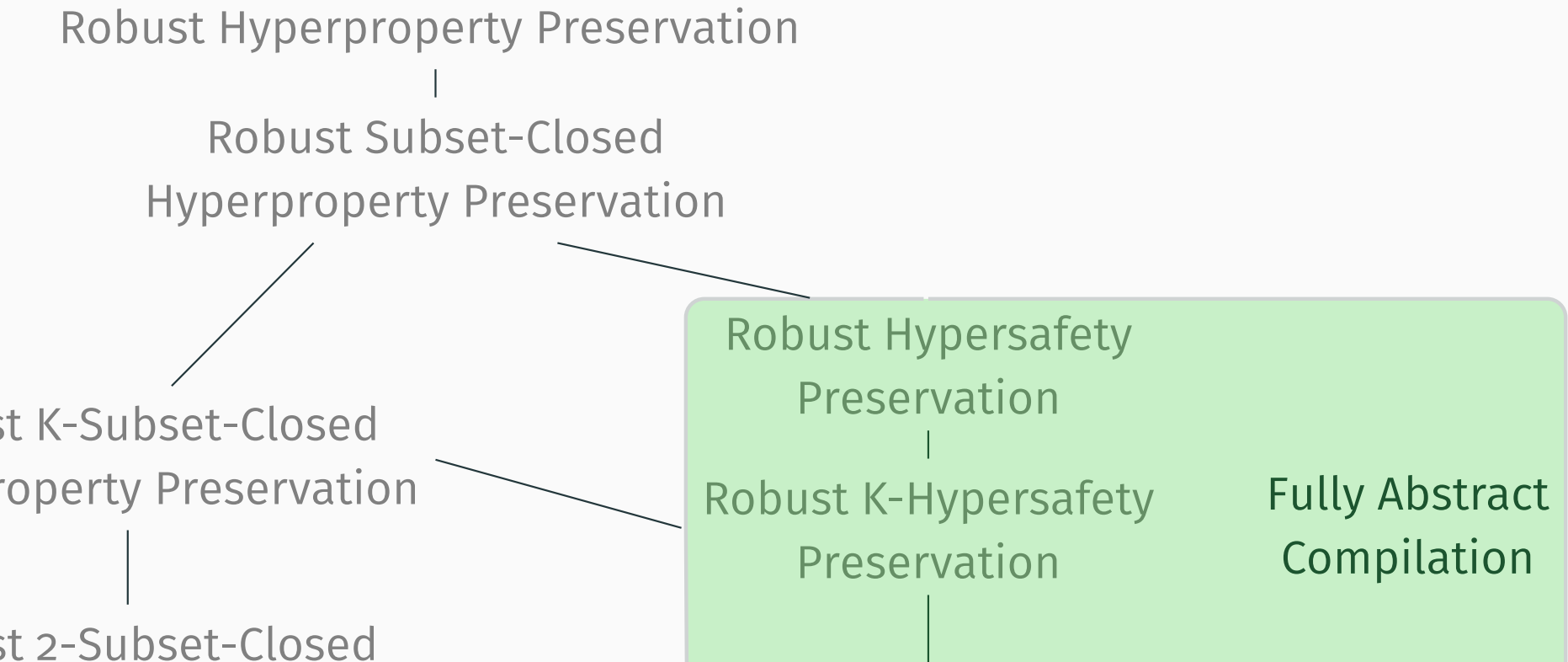
Where is FAC?

There is FAC

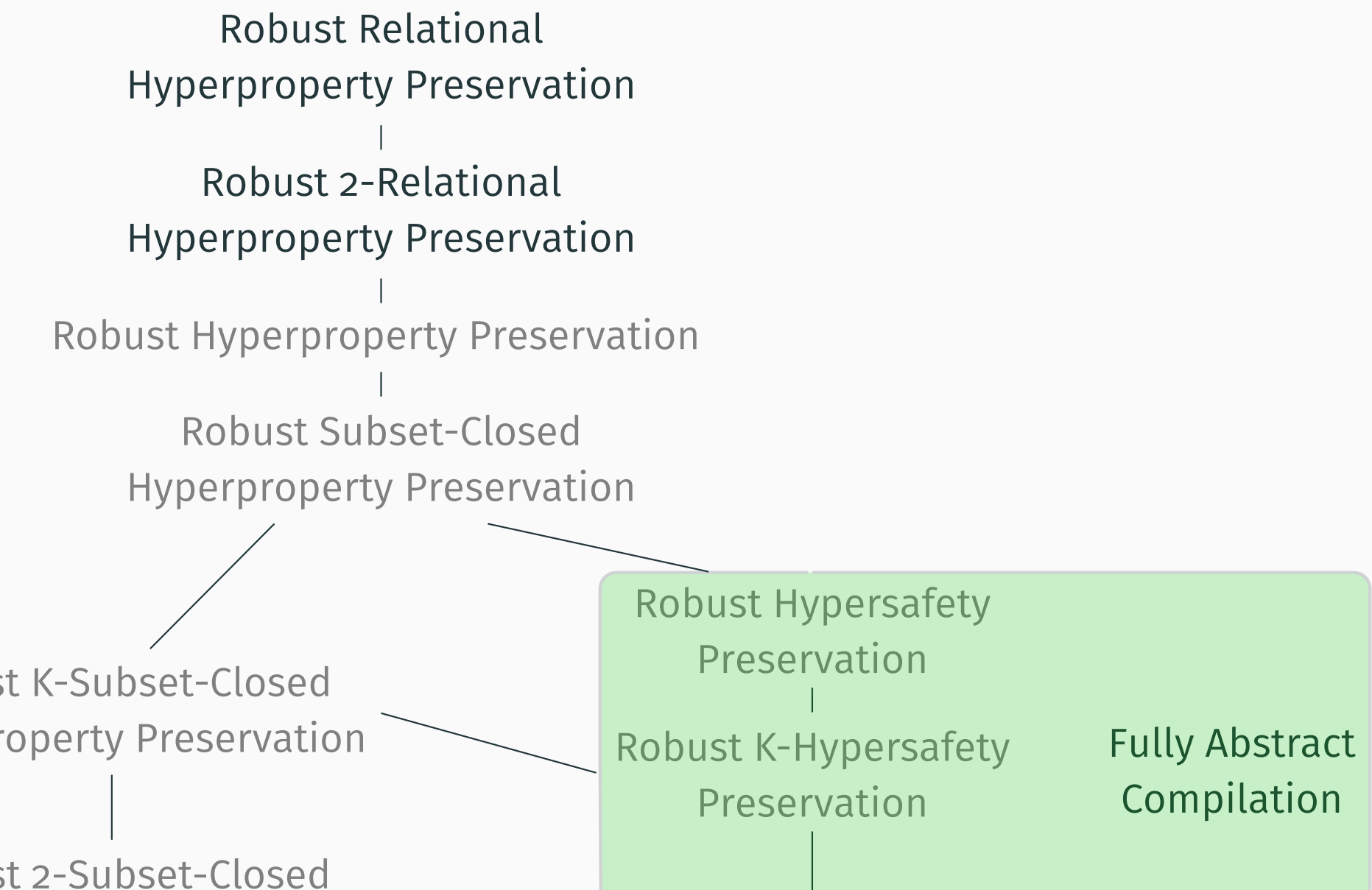


Fully Abstract
Compilation

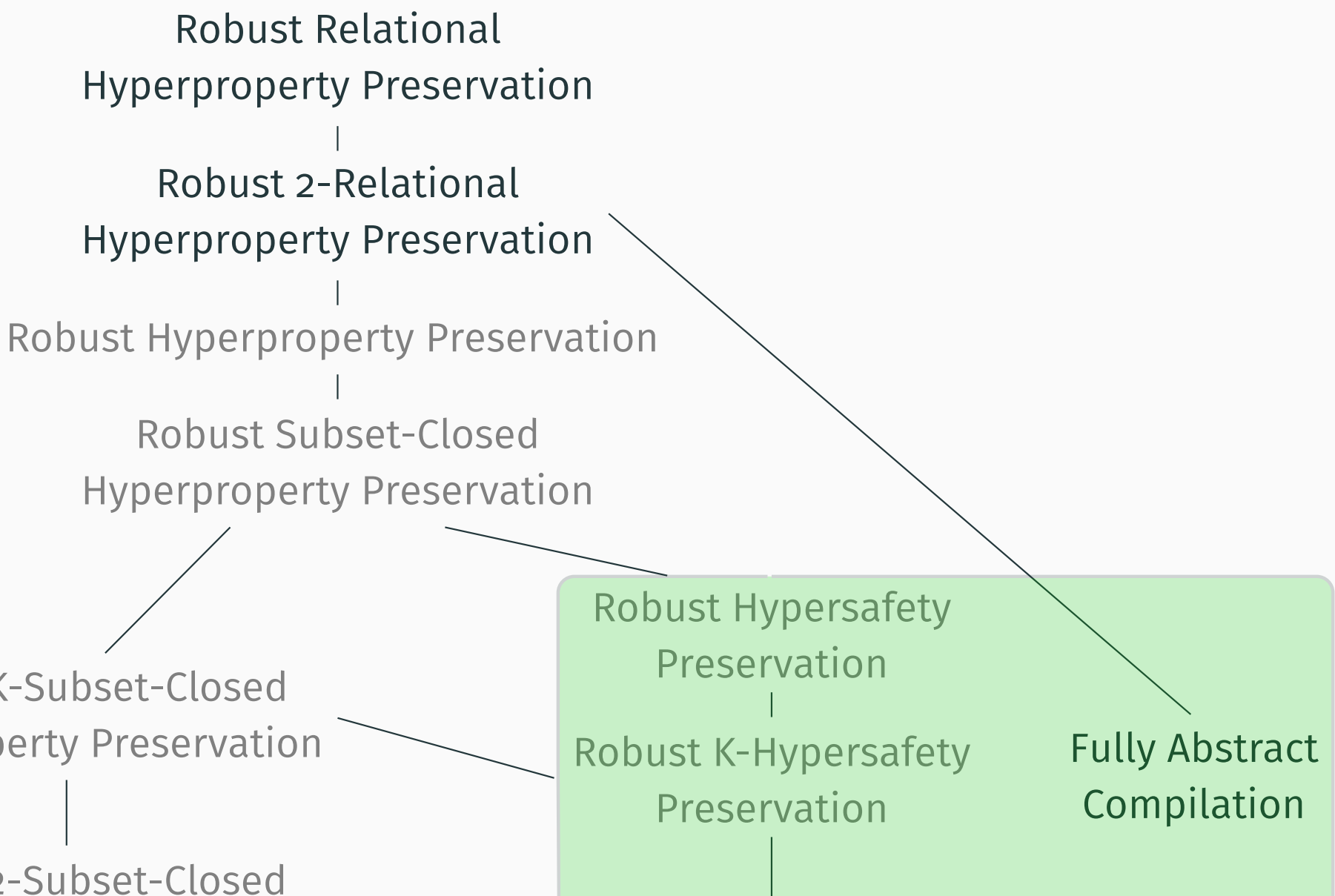
There is FAC


Robust Hyperproperty Preservation
Robust Subset-Closed
Hyperproperty Preservation
st K-Subset-Closed
roperty Preservation
st 2-Subset-Closed
Robust Hypersafety
Preservation
Robust K-Hypersafety
Preservation
Fully Abstract
Compilation

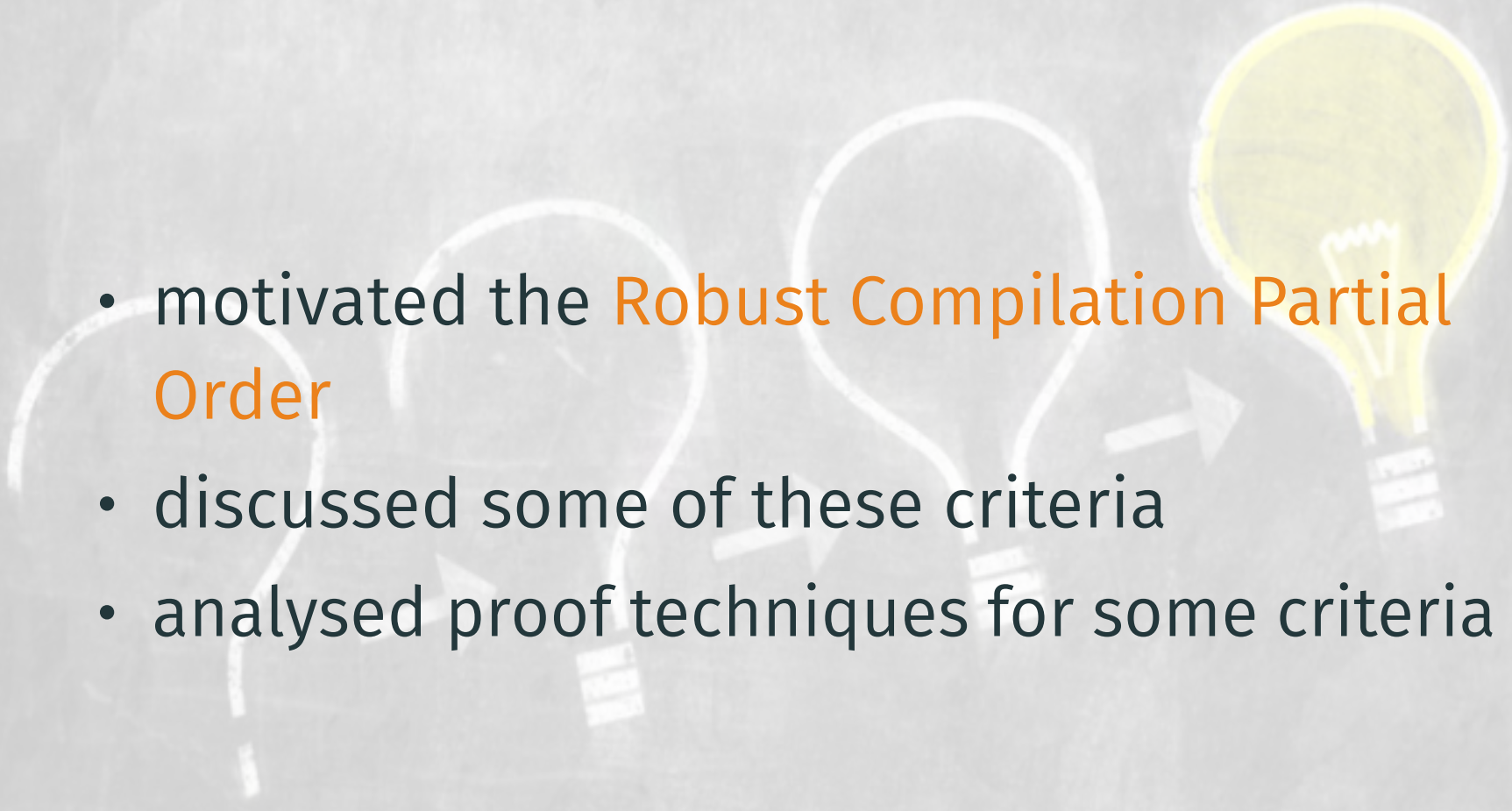
There is FAC


Robust Relational
Hyperproperty Preservation
Robust 2-Relational
Hyperproperty Preservation
Robust Hyperproperty Preservation
Robust Subset-Closed
Hyperproperty Preservation
st K-Subset-Closed
roperty Preservation
st 2-Subset-Closed
Robust Hypersafety
Preservation
Robust K-Hypersafety
Preservation
Fully Abstract
Compilation

There is FAC

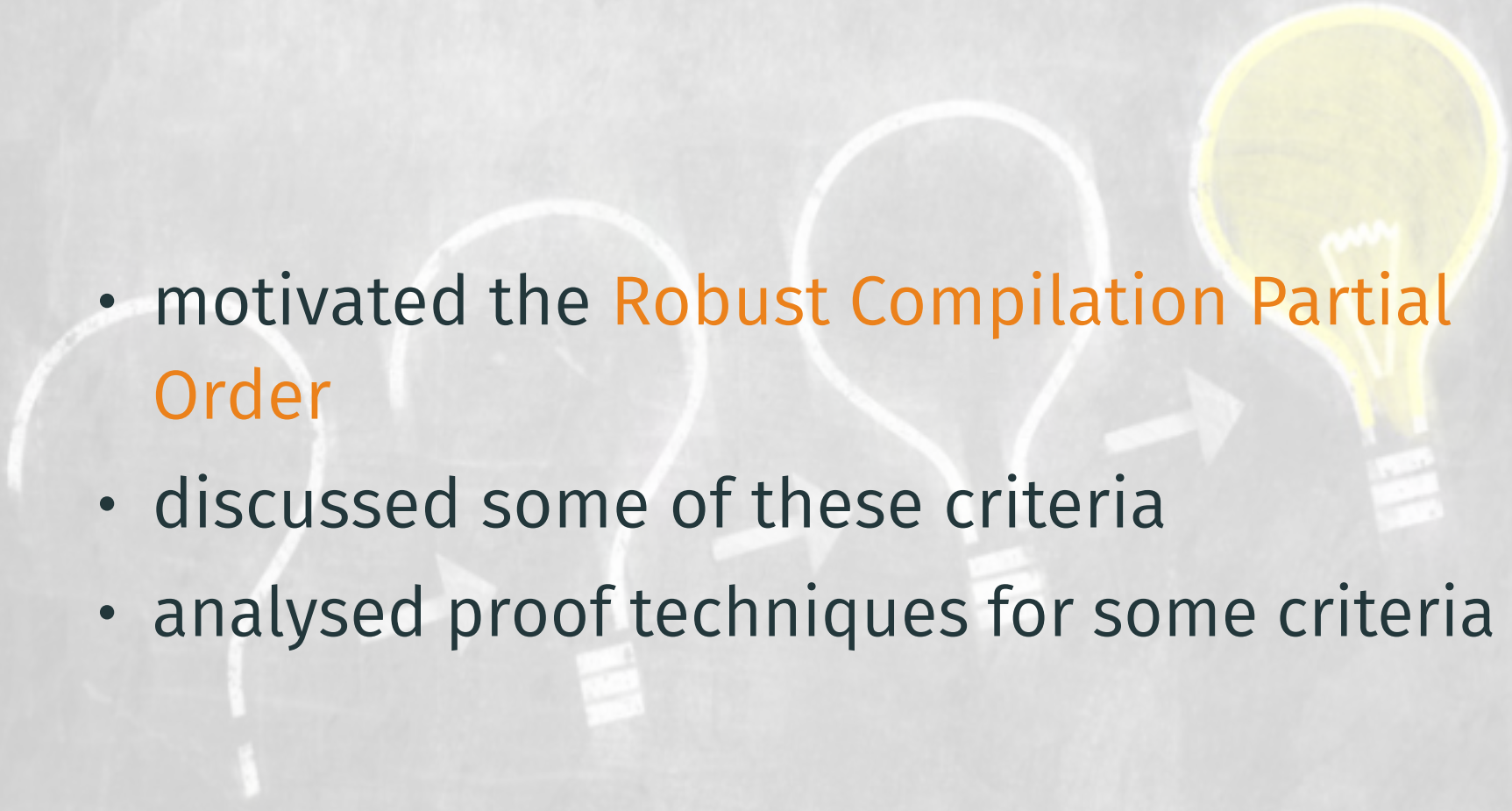

Robust Relational
Hyperproperty Preservation
Robust 2-Relational
Hyperproperty Preservation
Robust Hyperproperty Preservation
Robust Subset-Closed
Hyperproperty Preservation
st K-Subset-Closed
roperty Preservation
st 2-Subset-Closed
Robust Hypersafety
Preservation
Robust K-Hypersafety
Preservation
Fully Abstract
Compilation

Conclusion



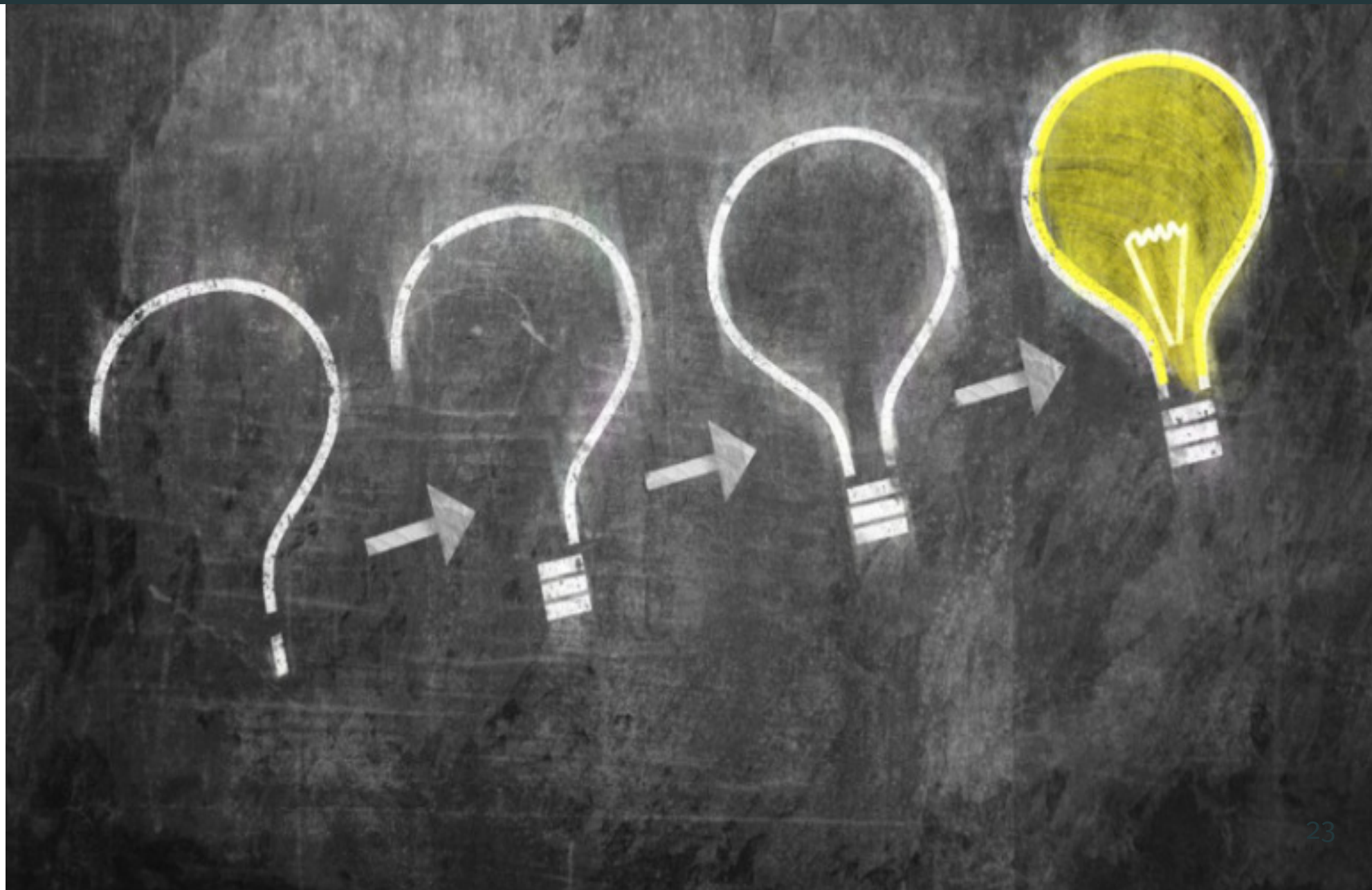
- motivated the Robust Compilation Partial Order
- discussed some of these criteria
- analysed proof techniques for some criteria

Conclusion

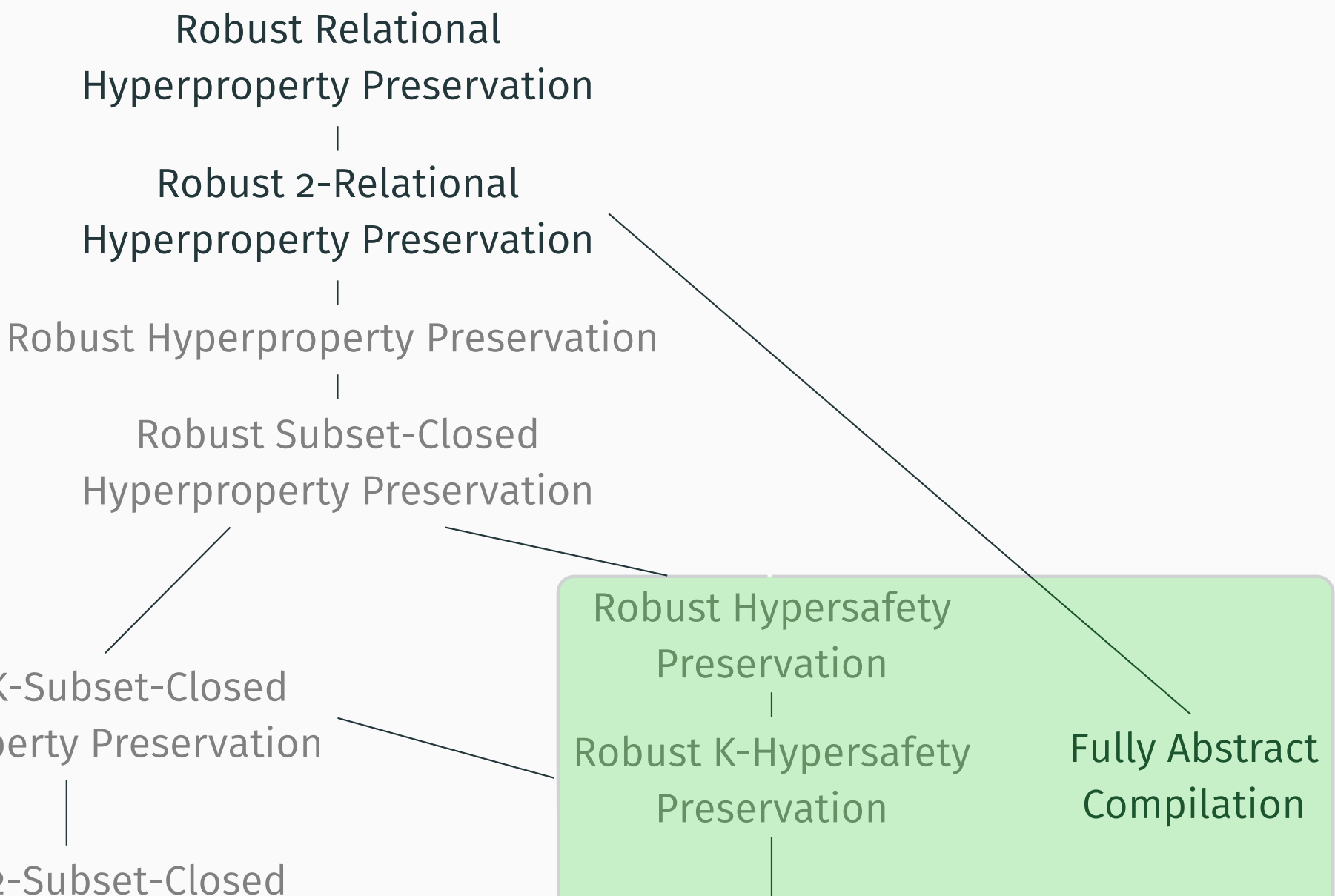


- motivated the Robust Compilation Partial Order
- discussed some of these criteria
- analysed proof techniques for some criteria

Conclusion



Robust Compilation Criteria



Robust Relational Hyperproperty Preservation

Definition: (HRC)

$$[\![\cdot]\!] \in \mathrm{HRC} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \mathrm{P}_s. \exists \mathbb{C}_s. \beta$$

$$\beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right)$$

$$\iff \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right)$$

Robust Relational Hyperproperty Preservation

Definition: (RRHP)

$$[\![\cdot]\!] \in \mathrm{RRHP} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \exists \mathbb{C}_s. \forall P_s, \beta$$
$$\beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![P_s]\!]\right]\right)$$
$$\iff \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[P_s\right]\right)$$

Robust 2-Relational Hyperproperty Preservation

Definition: (RRHP)

$$[\![\cdot]\!] \in \mathrm{RRHP} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \exists \mathbb{C}_s. \forall \mathrm{P}_s. \beta$$

$$\left(\beta \in \mathtt{Behav}\left(\mathbb{C}_t\left[[\![\mathrm{P}_s]\!]\right]\right) \iff \beta \in \mathtt{Behav}\left(\mathbb{C}_s\left[\mathrm{P}_s\right]\right) \right)$$

Robust 2-Relational Hyperproperty Preservation

Definition: (R2RHP**)**

$$[\![\cdot]\!] \in \text{R2RHP} \stackrel{\text{def}}{=} \forall \mathbb{C}_t, \exists \mathbb{C}_s. \forall \, P_s, P'_s. \, \beta$$

$$\left(\beta \in \text{Behav}\left(\mathbb{C}_t\left[[\![P_s]\!]\right]\right) \iff \beta \in \text{Behav}\left(\mathbb{C}_s\left[P_s\right]\right) \right)$$

$$\text{and} \quad \left(\beta \in \text{Behav}\left(\mathbb{C}_t\left[[\![P'_s]\!]\right]\right) \iff \beta \in \text{Behav}\left(\mathbb{C}_s\left[P'_s\right]\right) \right)$$