CoLoSL

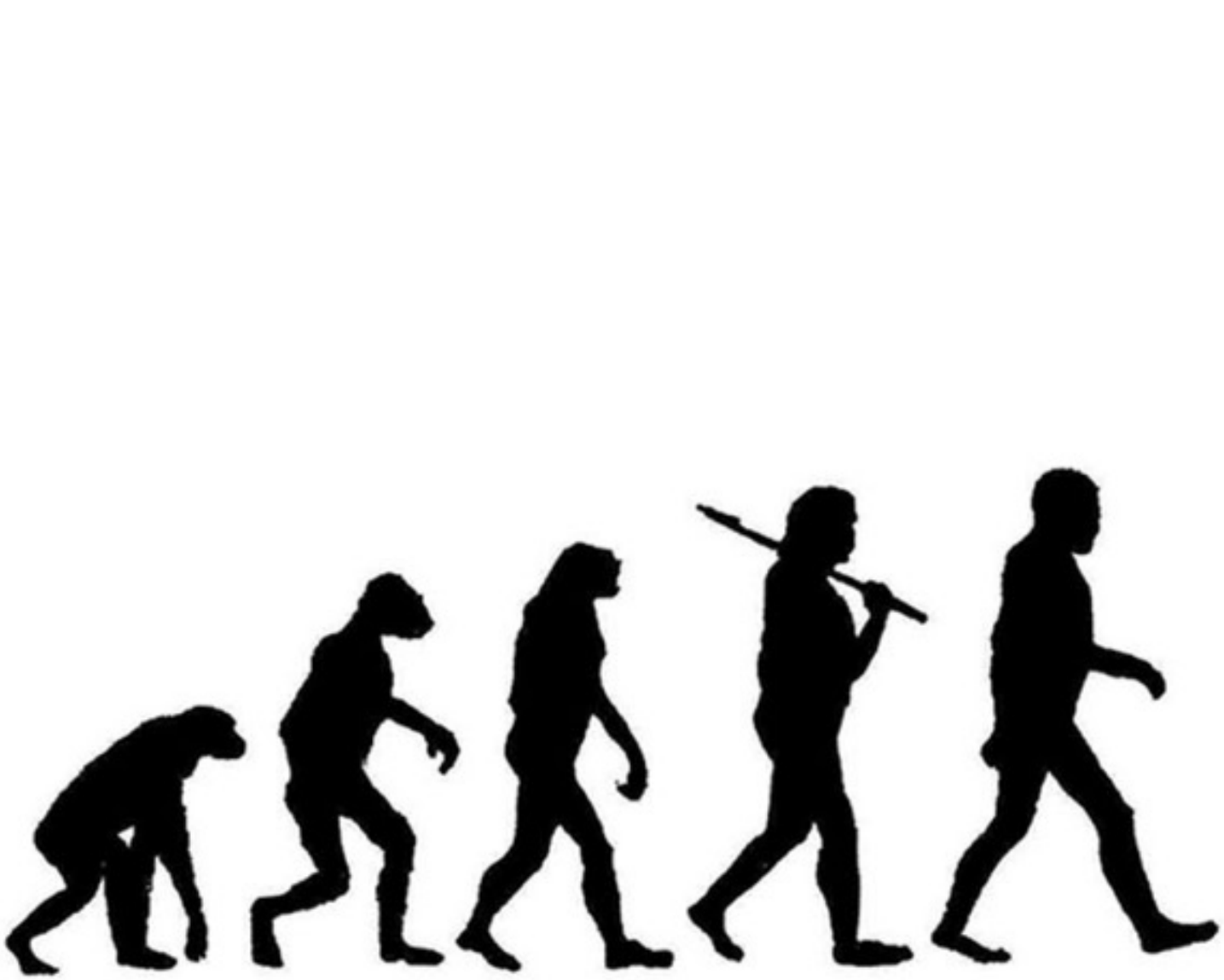
Why Not Frame All the Way?

Azalea Raad Jules Villard Philippa Gardner

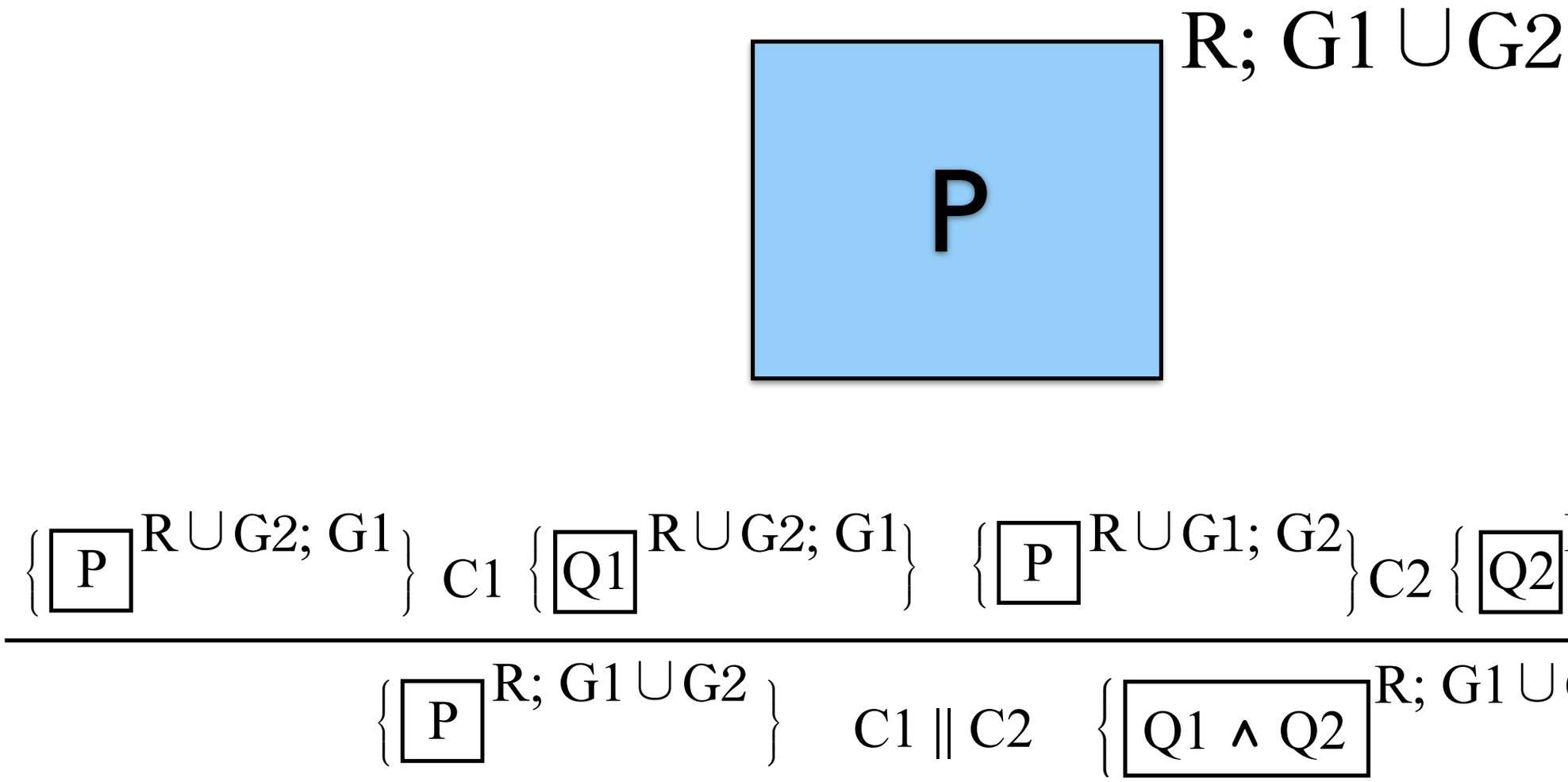
Imperial College London

23 June 2015

One Logic to Rule Them All…



Global Reasoning



Rely-Guarantee (Owicki-Gries)

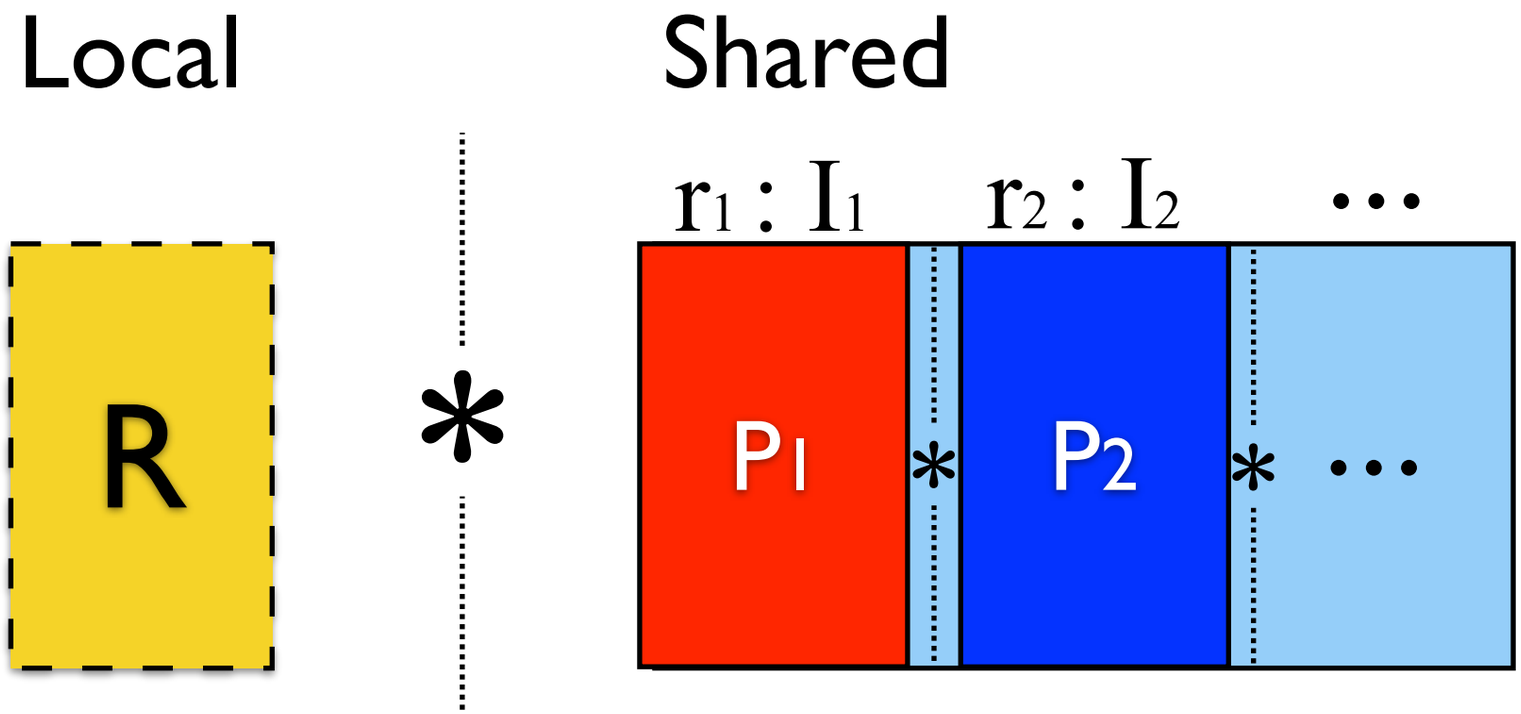
Global Reasoning

$$\frac{\{\boxed{P}^{R;\,G}\}\ C1\ \{\boxed{Q1}^{R;\,G}\} \qquad \{\boxed{P}^{R;\,G}\}\ C2\ \{\boxed{Q2}^{R;\,G}\}}{\{\boxed{P}^{R;\,G}\}\ C1 \parallel C2\ \{\boxed{Q1 \wedge Q2}^{R;\,G}\}}$$

- **No framing on shared resources / interference**
  - Reasoning on GLOBAL resources
  - Interference on ALL resources considered

Rely-Guarantee (Owicki-Gries)

Local Reasoning (Disjoint)



$$\frac{\left\{\boxed{P}^{r_1}_{I_1}\right\} \;C\; \left\{\boxed{P'}^{r_1}_{I_1}\right\}}{\left\{\boxed{P}^{r_1}_{I_1} * \boxed{Q}^{r_2}_{I_2}\right\} \;C\; \left\{\boxed{P'}^{r_1}_{I_1} * \boxed{Q}^{r_2}_{I_2}\right\}} \text{(FRAME)}$$

CSL, RGSep, DG, CAP, HOCAP, iCAP, FCSL, TaDA

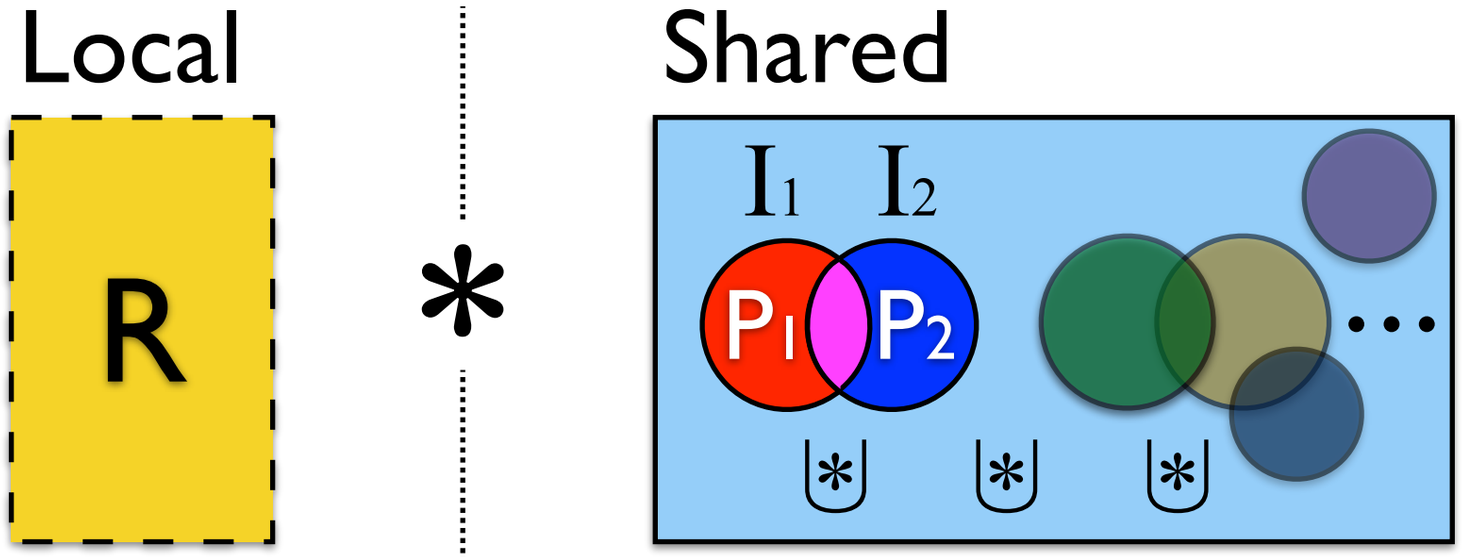
Local Reasoning (Disjoint)

$$\frac{\left\{\boxed{P}_{I1}^{r1}\right\} \; C \; \left\{\boxed{P'}_{I1}^{r1}\right\}}{\left\{\boxed{P}_{I1}^{r1} * \boxed{Q}_{I2}^{r2}\right\} \; C \; \left\{\boxed{P'}_{I1}^{r1} * \boxed{Q}_{I2}^{r2}\right\}} \text{(FRAME)}$$

- **<u>Limited framing on shared resources / interference</u>**
  - **Static** (pre-determined) frames (regions/ invariants)
  - **Physically** disjoint frames

CSL, RGSep, DG, CAP, HOCAP, iCAP, FCSL, TaDA

CoLoSL: Concurrent Local Subjective Logic



$$\frac{\{\boxed{P}_{I}\}\ C\ \{\boxed{P'}_{I}\} \qquad I \cup I' \sqsubseteq^{P} I}{\{\boxed{P \circledast Q}_{I \cup I'}\}\ C\ \{\boxed{P' \circledast Q}_{I \cup I'}\}}\ (\textsc{Frame})$$

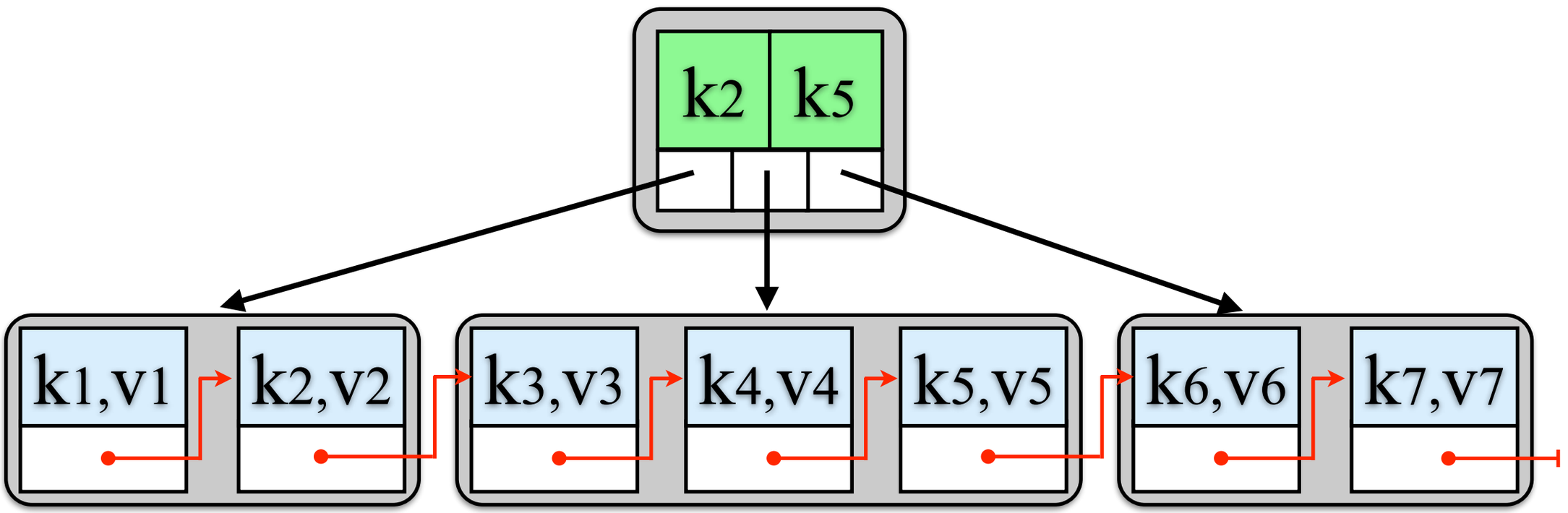
CoLoSL

CoLoSL: Concurrent Local Subjective Logic

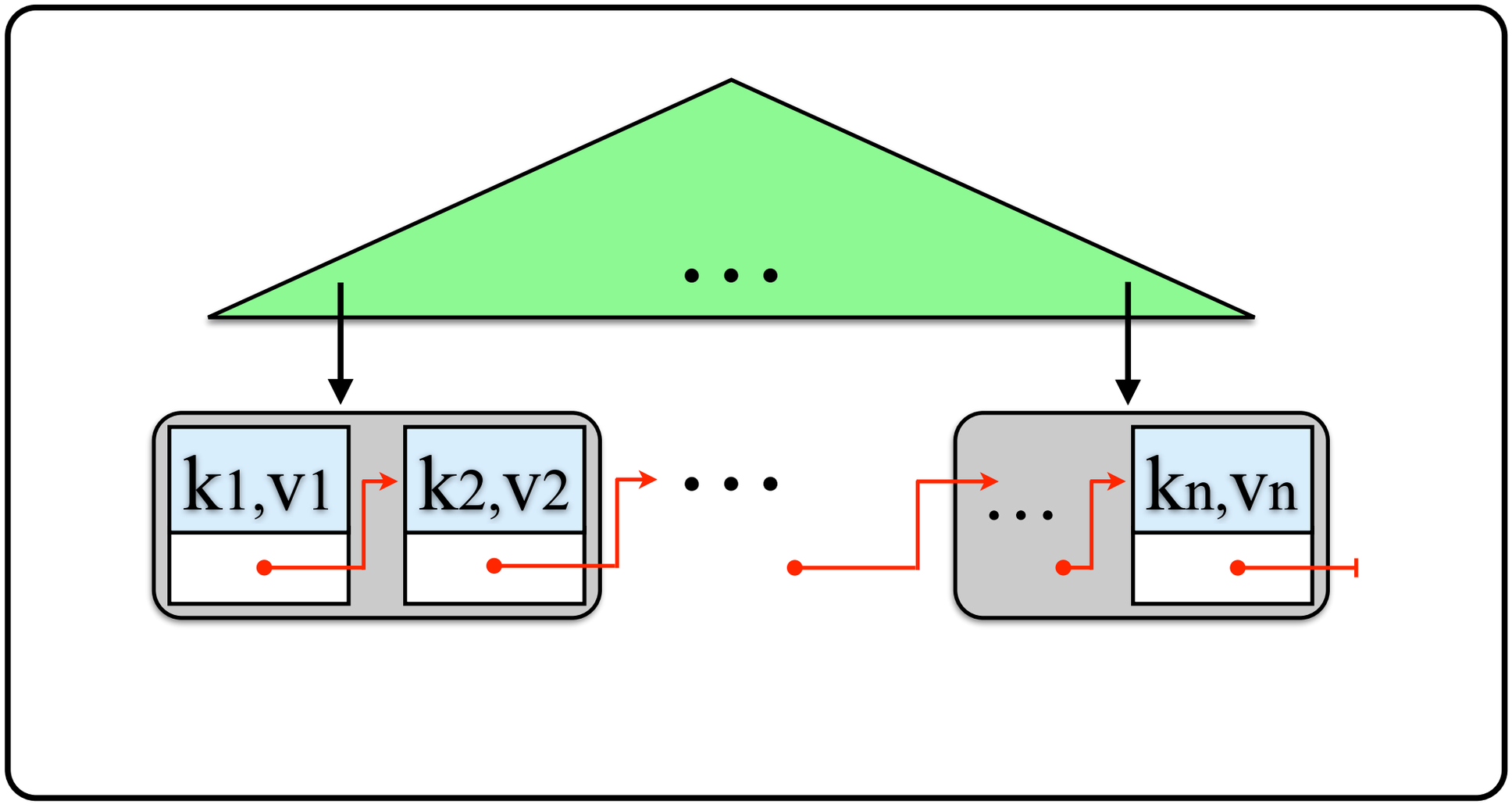
$$\frac{\{\boxed{P}_I\}\ C\ \{\boxed{P'}_I\} \qquad I \cup I' \sqsubseteq^P I}{\{\boxed{P \circledast Q}_{I \cup I'}\}\ C\ \{\boxed{P' \circledast Q}_{I \cup I'}\}}\ (\textsc{Frame})$$

- **Flexible framing on shared resources/invariants**
  - **Overlapping** frames
  - **Flexible** framing/rewriting of interference

Concurrent B+ Tree



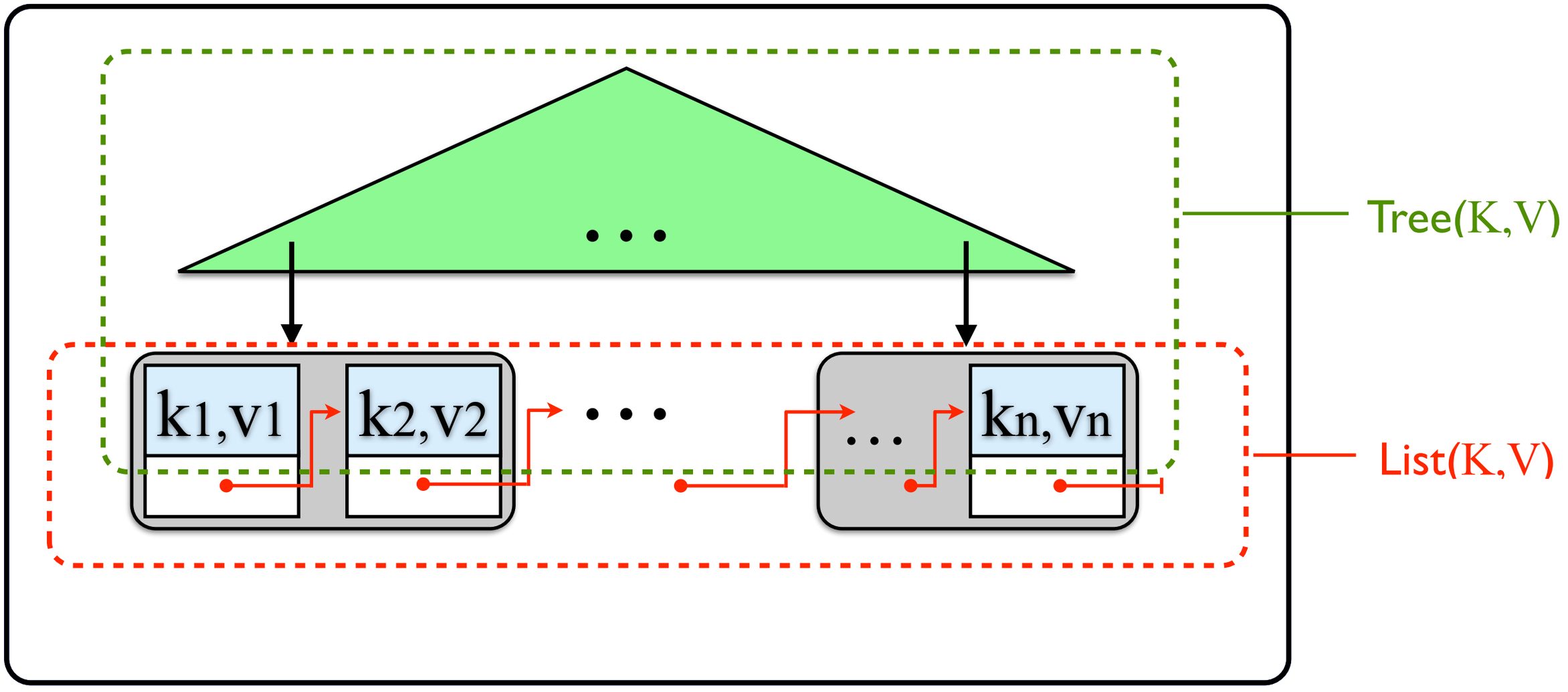
Concurrent B+ Tree



I_{B^+} = I[illegible]

- **B+Tree operations**
  - find(k); update(k, v); updateAll(V); add(k,v);

Concurrent B+ Tree: Quest for Small Axioms



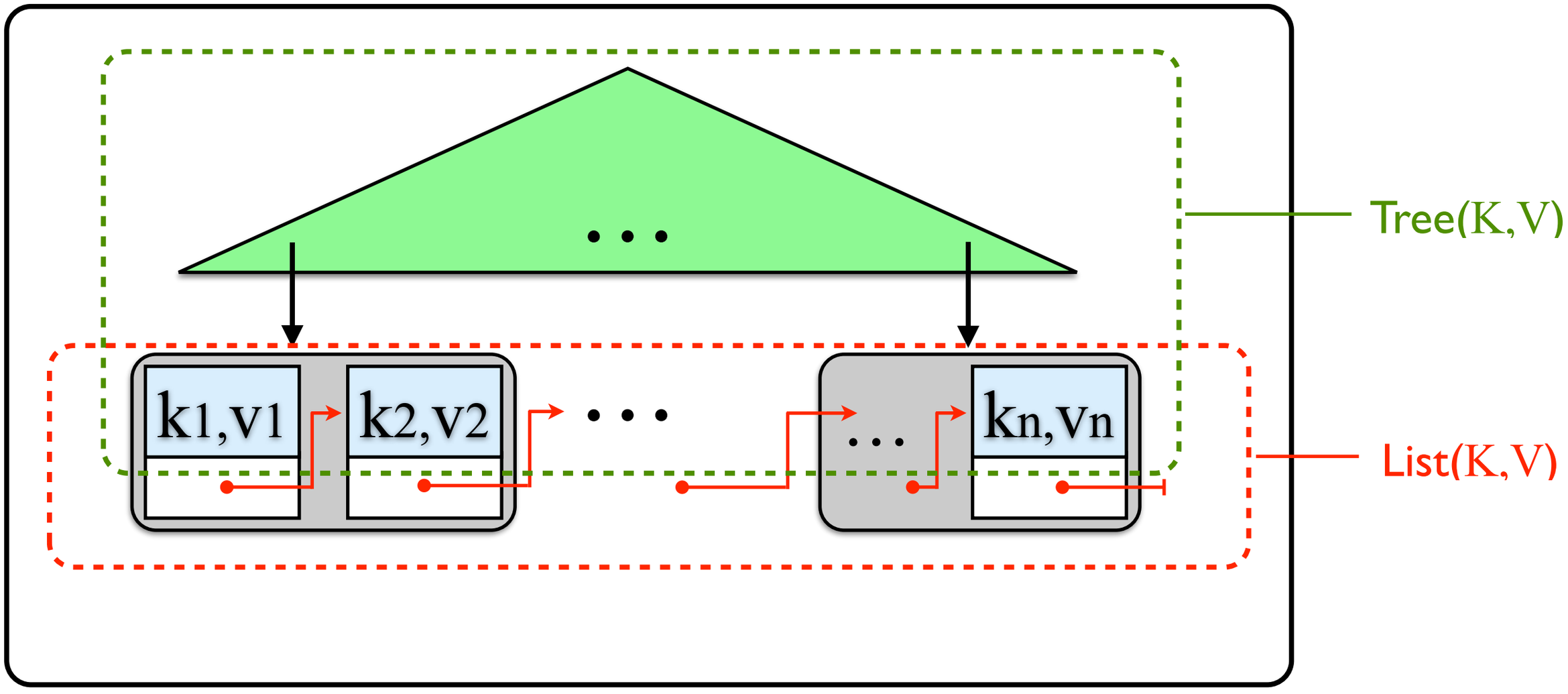
$$I_{B^+} = I_{find} \cup I_{up} \cup I_{add\_L} \cup I_{add\_T}$$

- **B+Tree operations**
  - find(k); update(k, v); updateAll(V); add(k,v);

$I_T = I_{find} \cup I_{up} \cup I_{add\_T}$ $I_L = I_{up} \cup I_{add\_L}$ $I_{B^+} = I_T \cup I_L$

||

Concurrent B+ Tree: Quest for Small Axioms

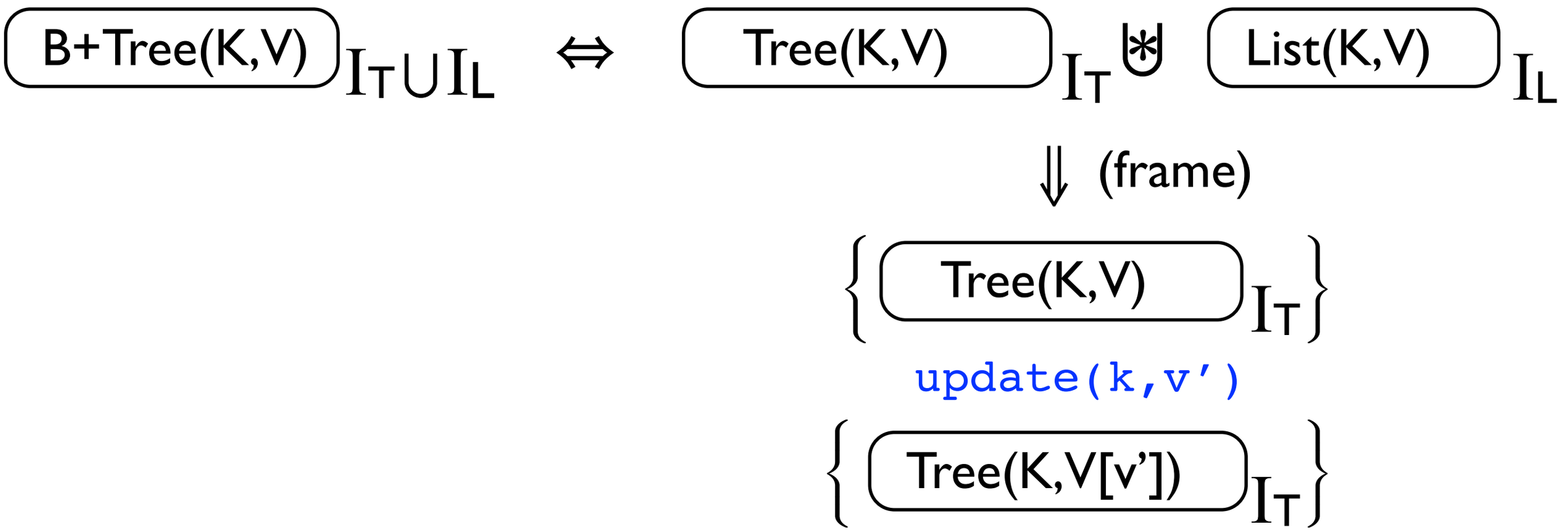


$$I_{B^+} = I_{find} \cup I_{up} \cup I_{add\_L} \cup I_{add\_T}$$

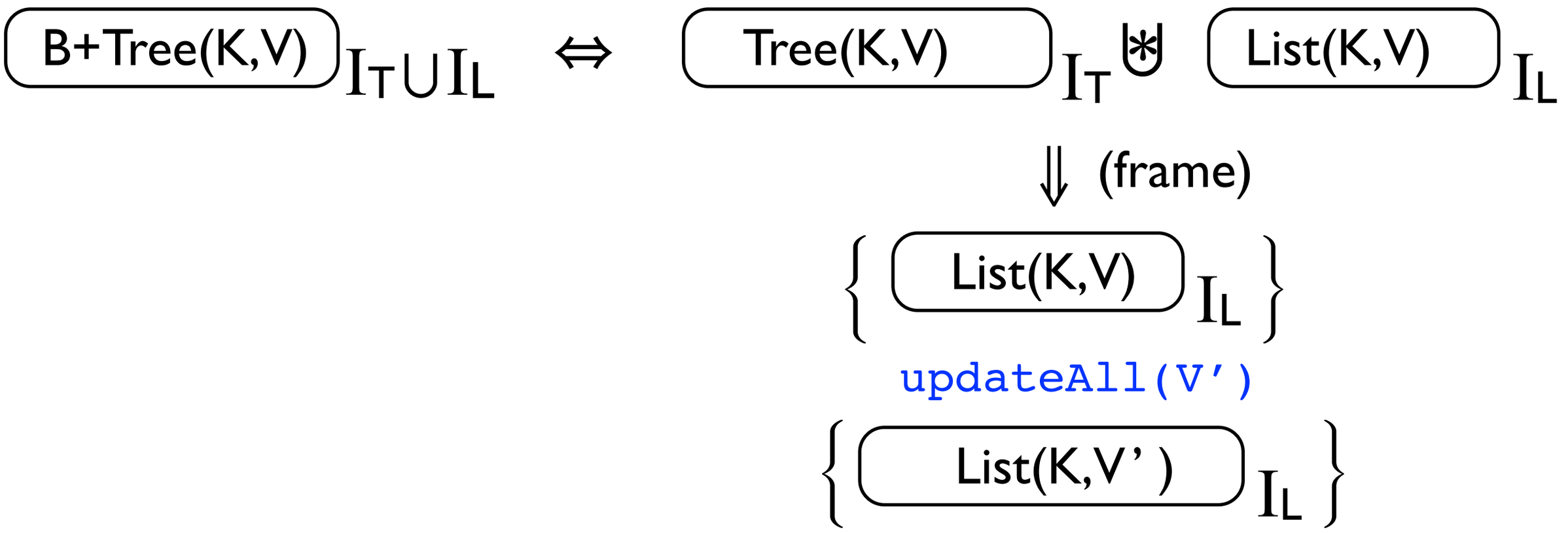
B+Tree(K,V) ⇔ Tree(K,V) * List(K,V)

$I_T \cup I_L$ I_T I_L

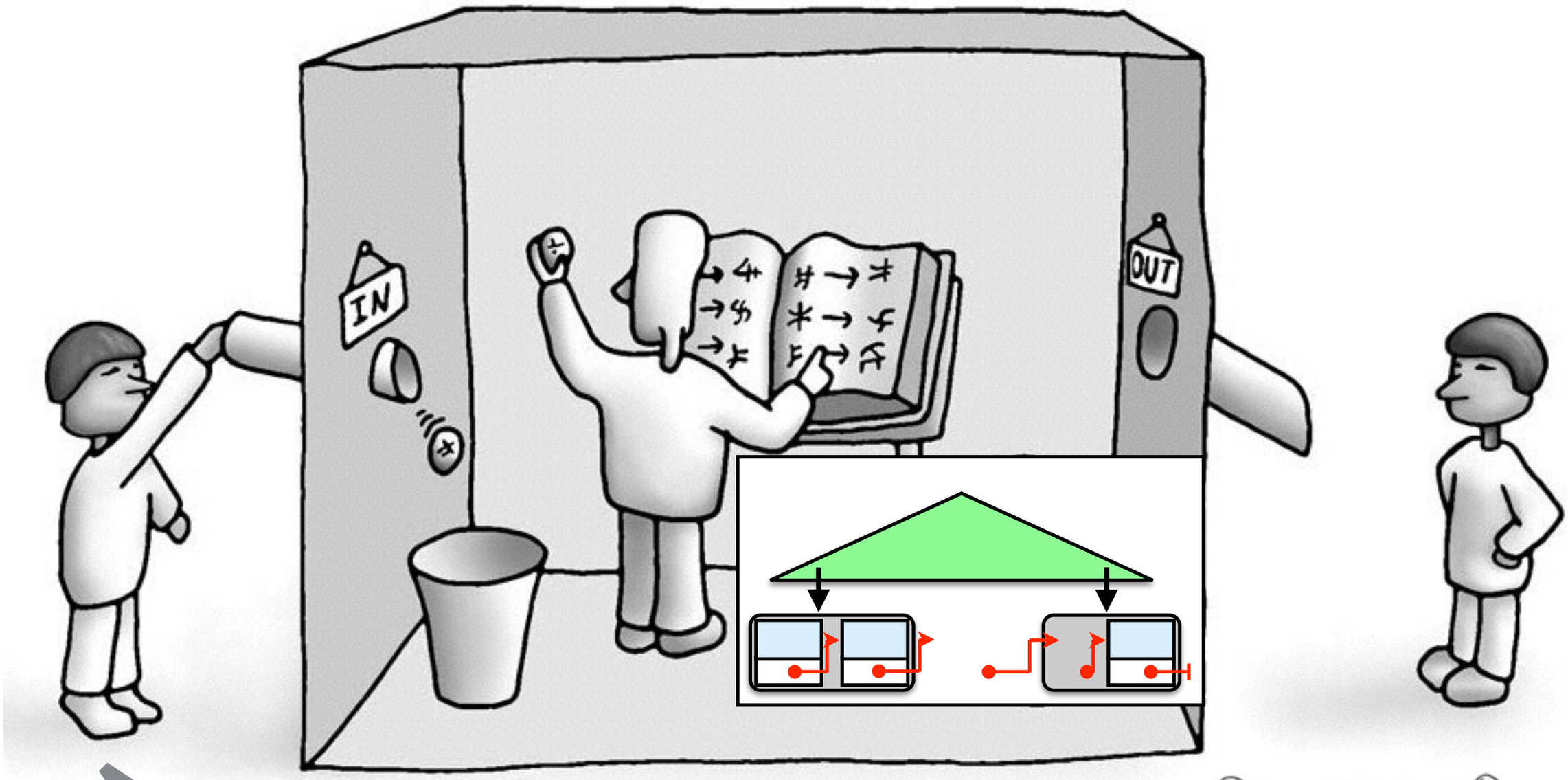
Concurrent B+ Tree Wish List



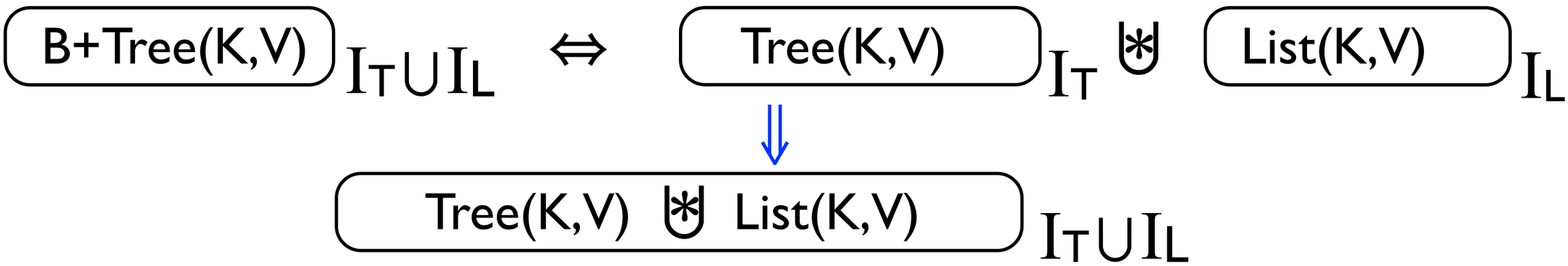
Concurrent B+ Tree Wish List



Chinese Room of Concurrent Interfaces

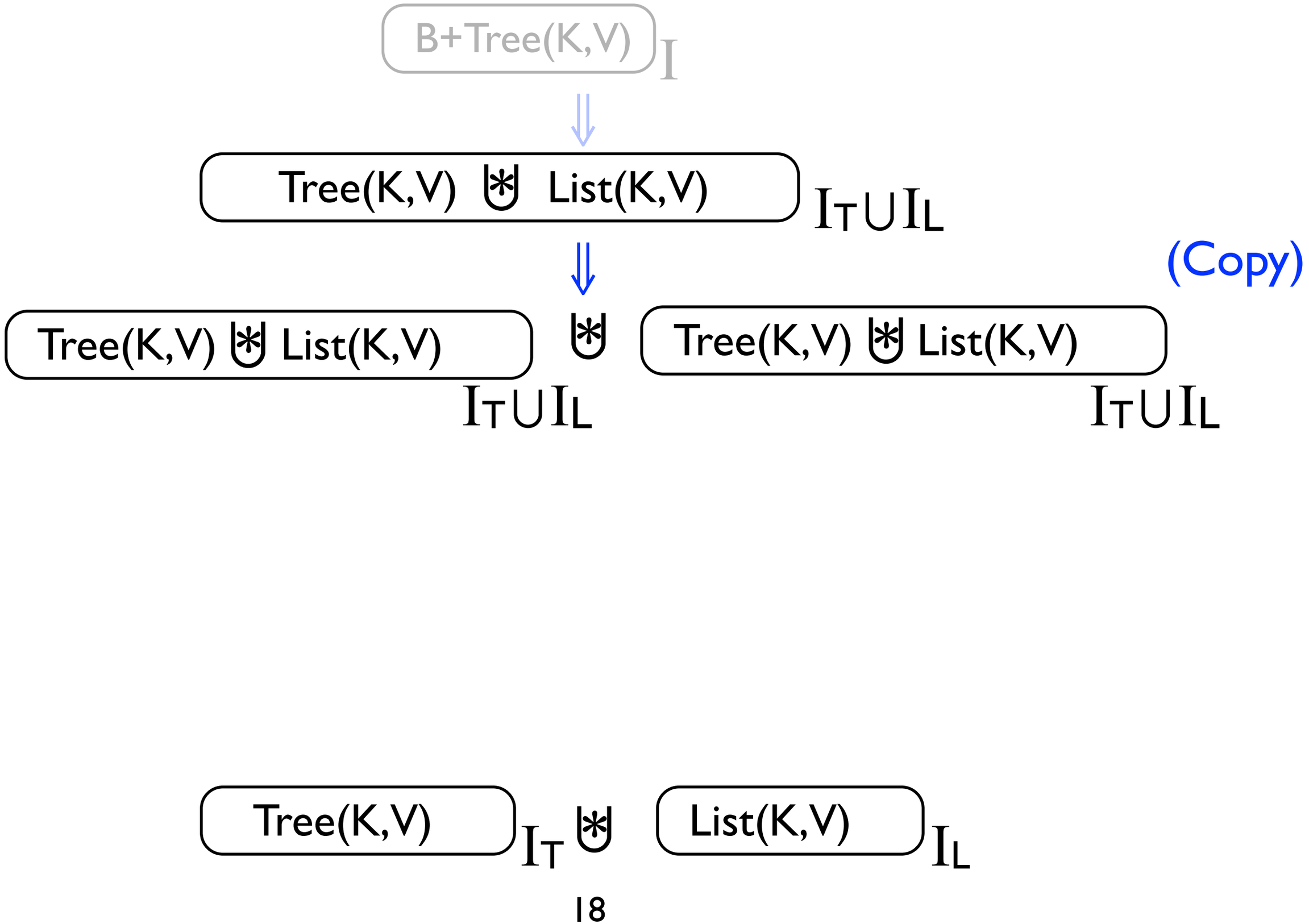


CoLoSL Principles

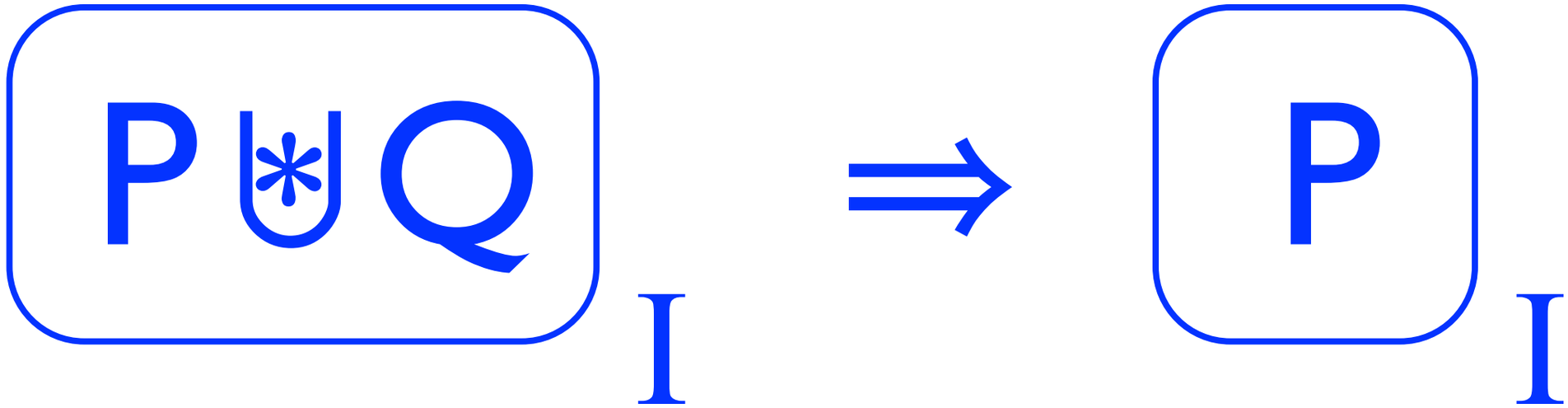


Duplicating Resources

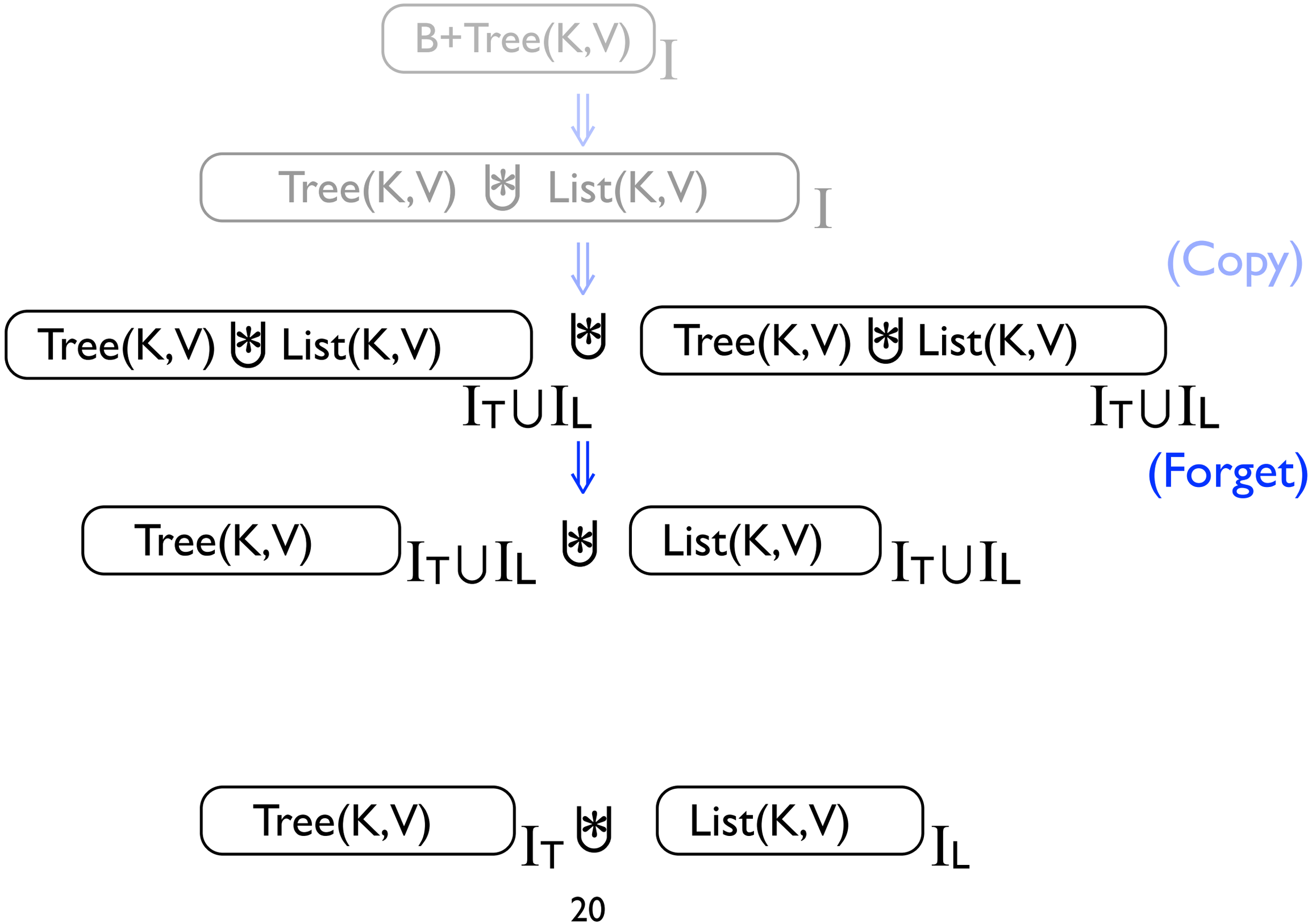
CoLoSL Principles



Forgetting Resources



CoLoSL Principles

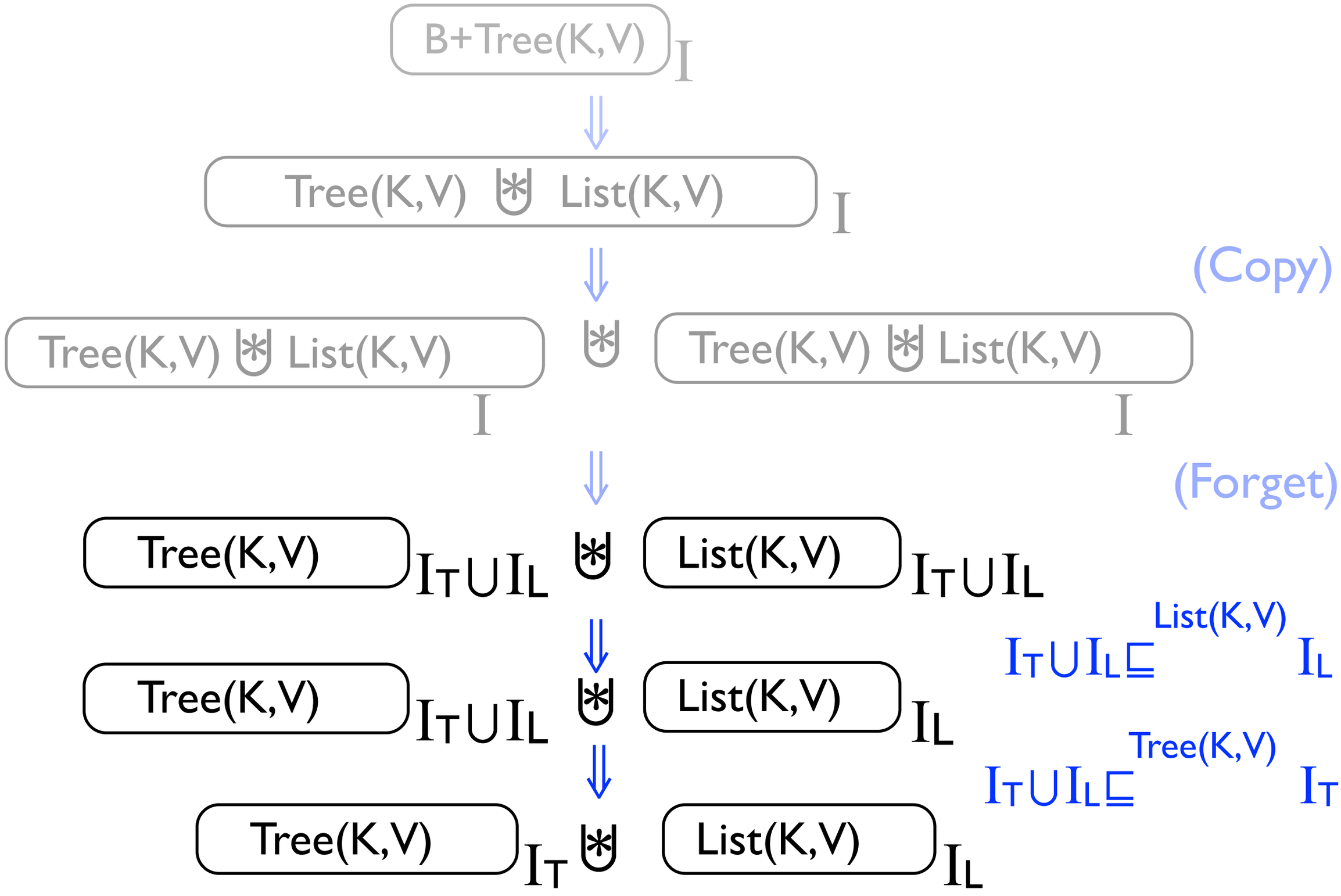


Forgetting Interference (Shift)

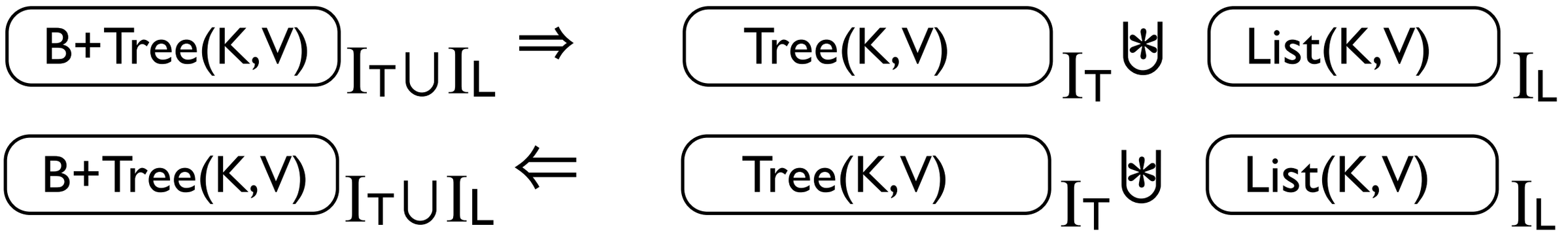
if $I \sqsubseteq^{P} I'$

then $\boxed{P}_{I} \Rightarrow \boxed{P}_{I'}$

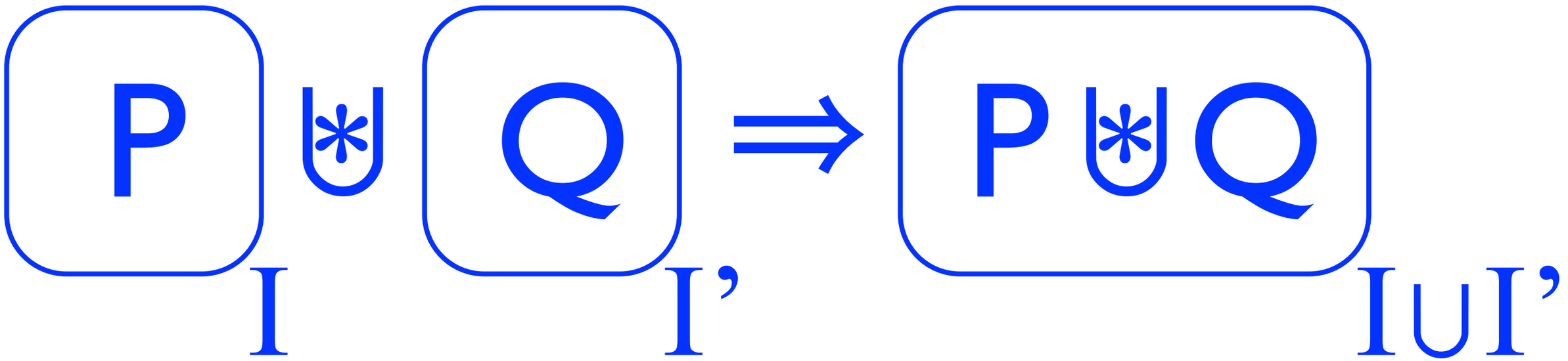
CoLoSL Principles



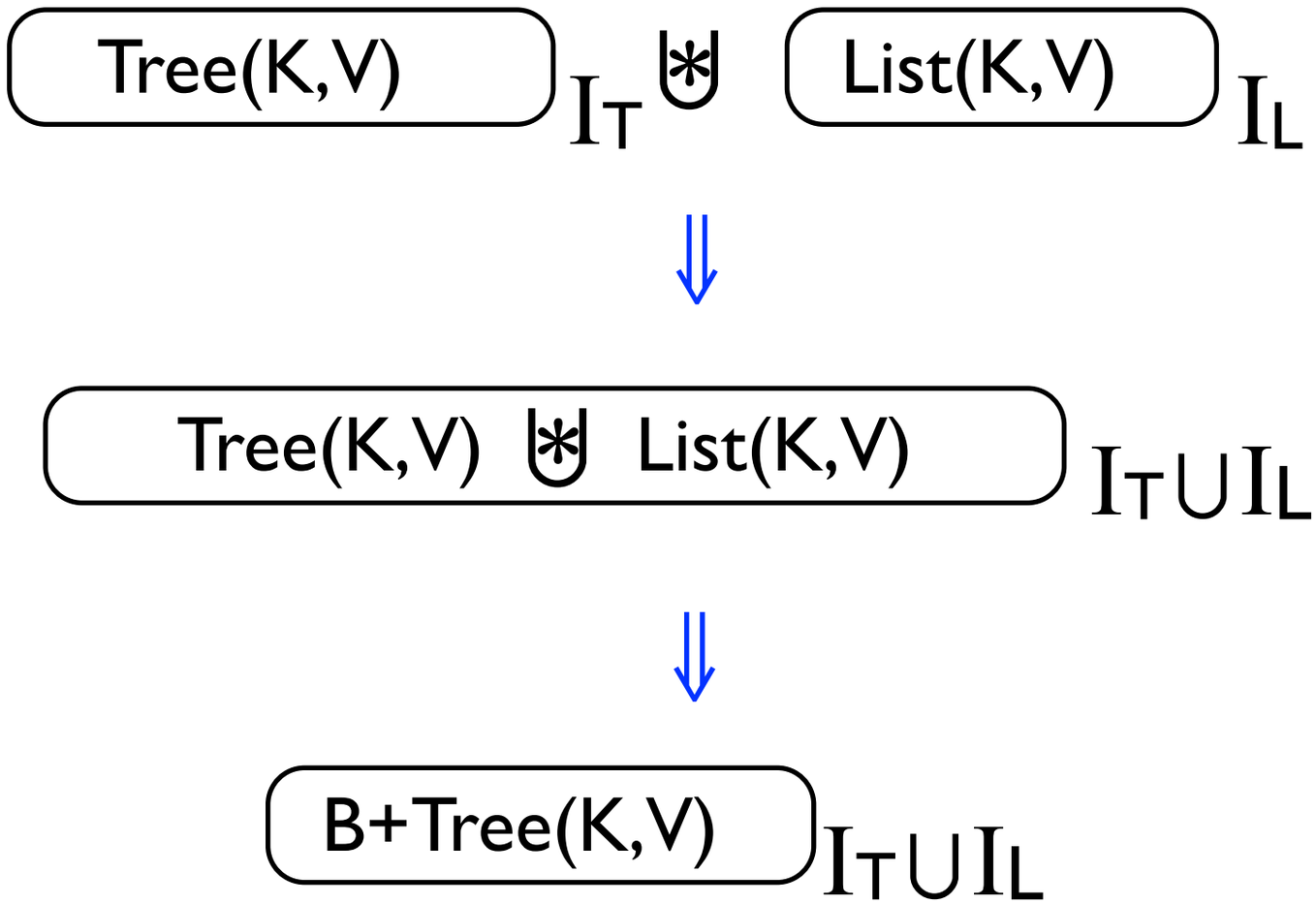
CoLoSL Principles



Merging Resources



CoLoSL Principles



Why Not Frame All the Way?

- **Sequential Reasoning (no interference)**
  - Frame resources ☞ local reasoning
- **Concurrent Reasoning (so far)**
  - Frame resources; no interference framing
  - Locality achieved per example by:
    - Verify examples w.r.t local interference
    - Prove lemmas to show extension to larger interference
- **CoLoSL**
  - Frame resources AND interference ☞ local reasoning

Conclusions and Future Work

- CoLoSL
  - Subjective/overlapping views
  - **Interference composition** ☞ more flexible framing
  - Are we there yet? No!
- Future Work
  - Abstract predicates, abstract atomicity, …
  - CoLoSL in Iris (monoid/invariant to split the interference)

Thank you for listening!