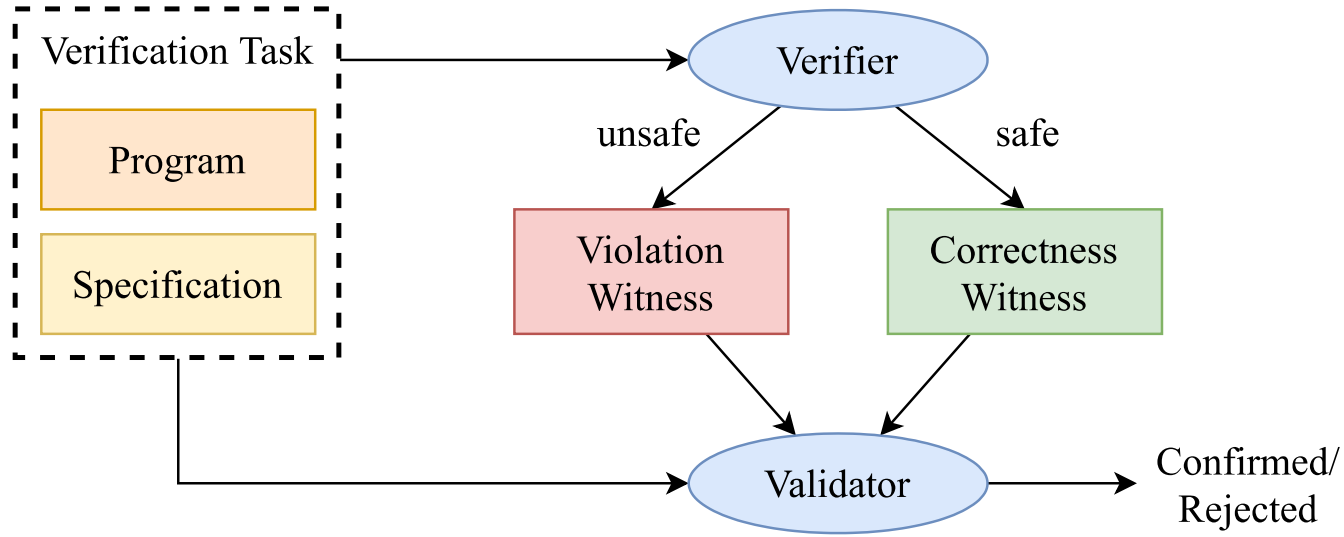
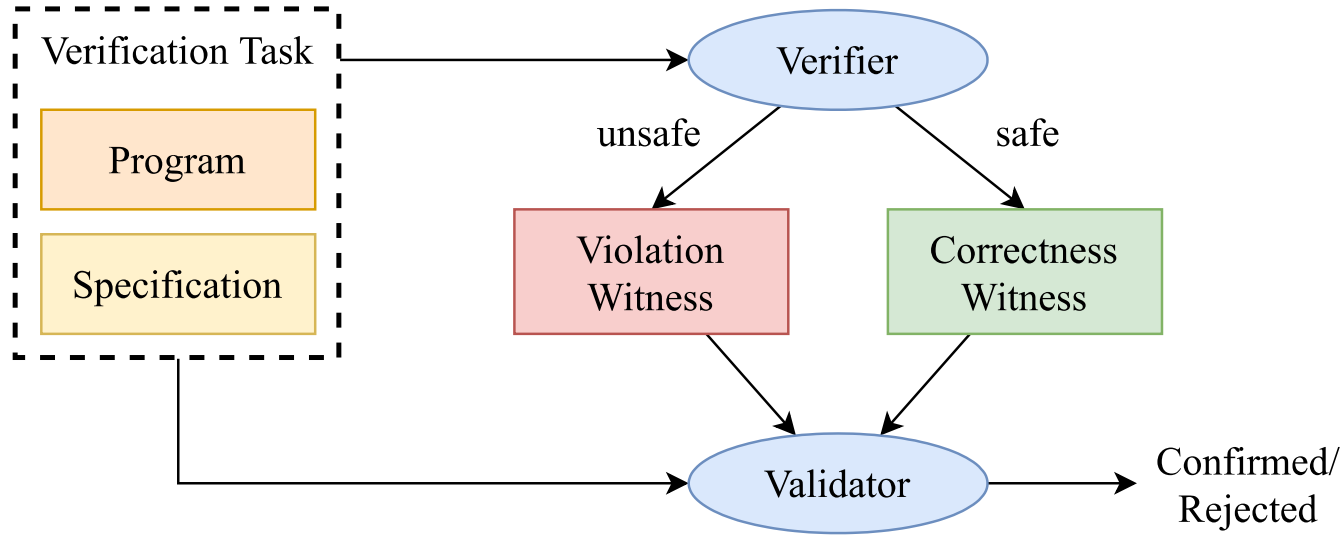


Correctness Witnesses for Concurrent Software Verification



Scheme of verification with witnesses

Correctness Witnesses for Concurrent Software Verification

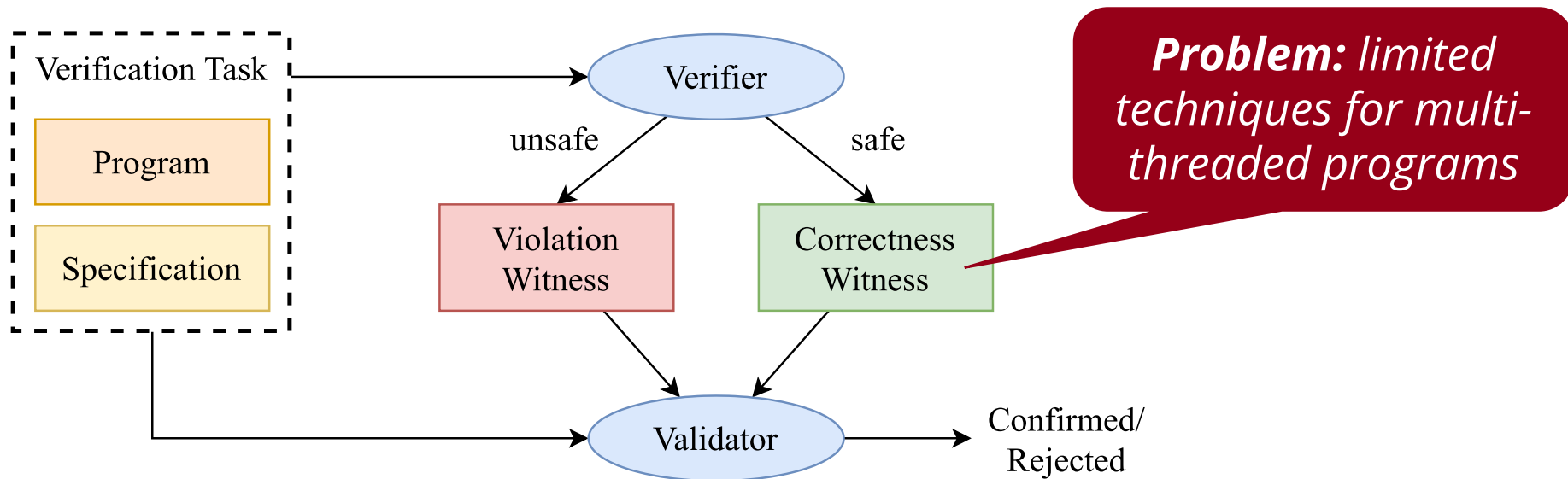


Scheme of verification with witnesses

Advantages:

- More **reliable verdict**
- **Useful insight**
- ...

Correctness Witnesses for Concurrent Software Verification

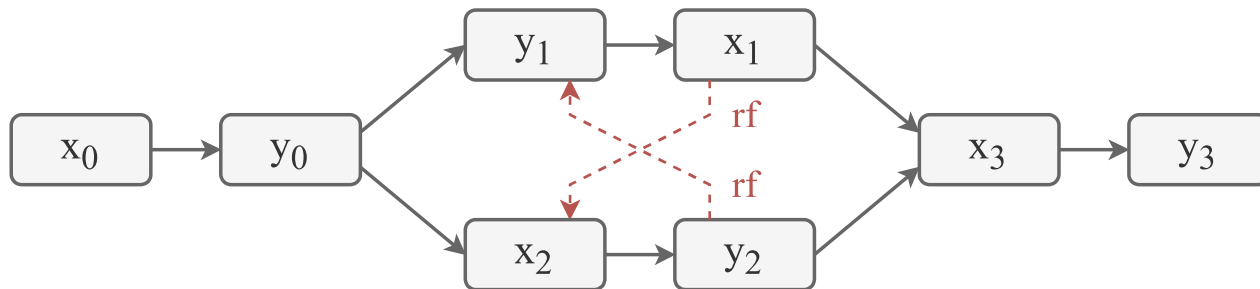


Scheme of verification with witnesses

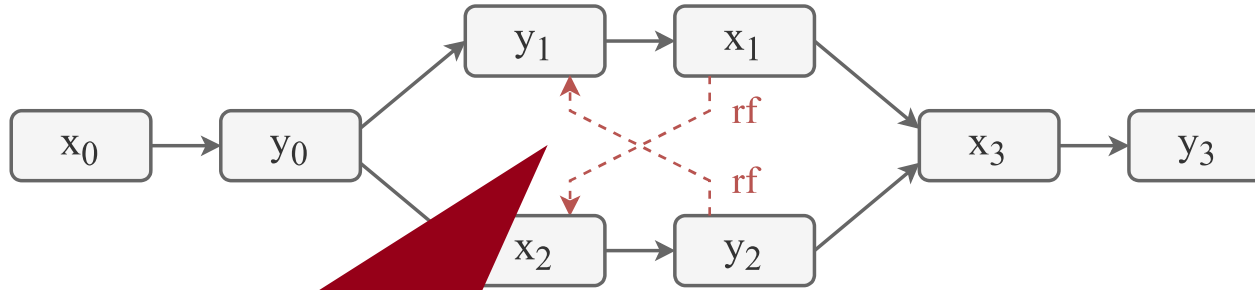
Advantages:

- More **reliable verdict**
- **Useful insight**
- ...

Happens-Before Cycles as Witness

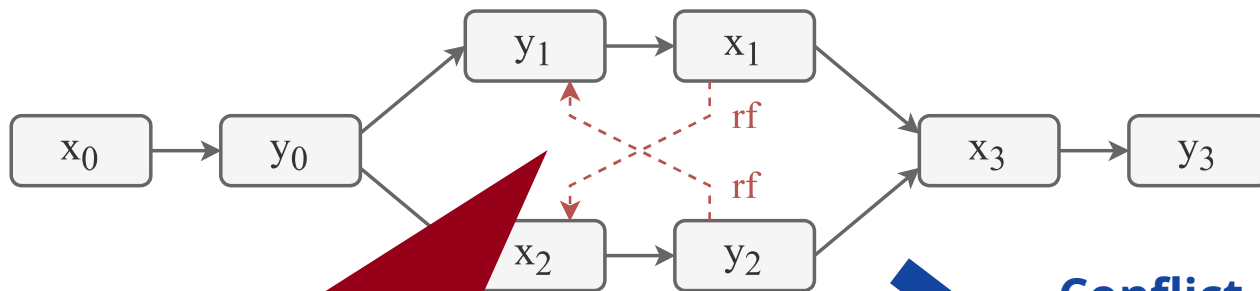


Happens-Before Cycles as Witness



CYCLE in the
happens-before relation:
cannot happen

Happens-Before Cycles as Witness

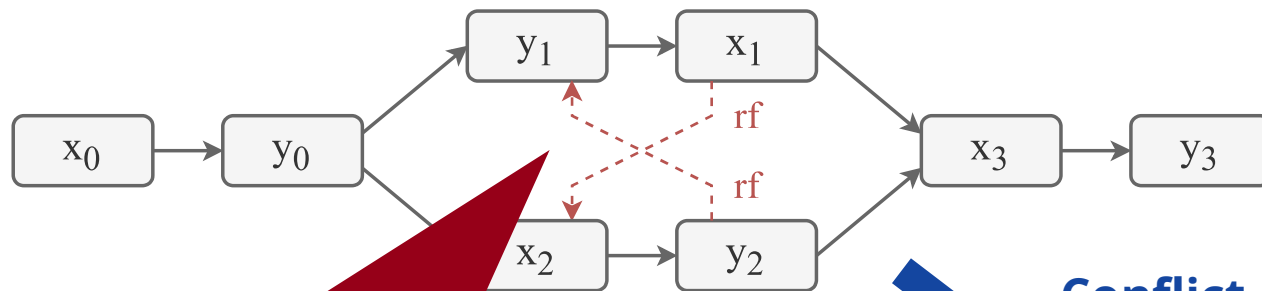


CYCLE in the
happens-before relation:
cannot happen

Conflict clause

$$\neg \left(\boxed{x_1 \prec_{\text{rf}} x_2} \wedge \boxed{x_2 \prec_{\text{po}} y_2} \wedge \boxed{y_2 \prec_{\text{rf}} y_1} \wedge \boxed{y_1 \prec_{\text{po}} x_1} \right)$$

Happens-Before Cycles as Witness



***CYCLE** in the happens-before relation: cannot happen*

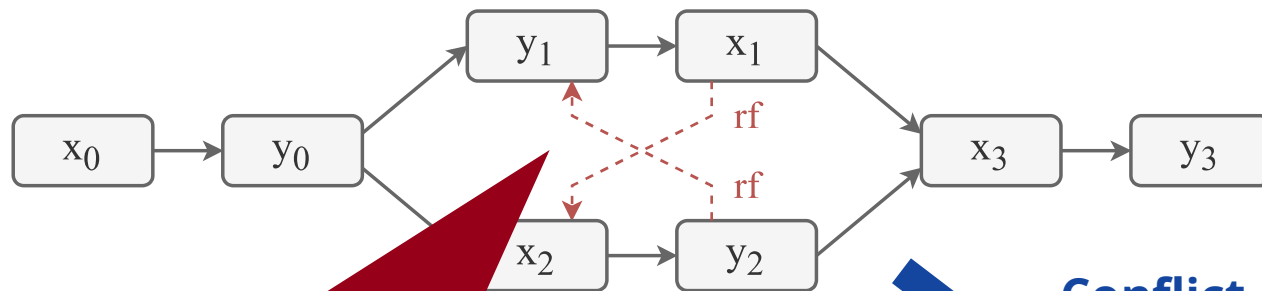
Conflict clause

$$\neg \left(x_1 \prec_{\text{rf}} x_2 \wedge x_2 \prec_{\text{po}} y_2 \wedge y_2 \prec_{\text{rf}} y_1 \wedge y_1 \prec_{\text{po}} x_1 \right)$$

Proposed approach:

- Use **conflict clauses in the witness**
- **Validation** is much **faster** with the extra information of conflict clauses

Happens-Before Cycles as Witness



***CYCLE** in the happens-before relation: cannot happen*

Conflict clause

$$\neg \left(x_1 \prec_{rf} x_2 \wedge x_2 \prec_{po} y_2 \wedge y_2 \prec_{rf} y_1 \wedge y_1 \prec_{po} x_1 \right)$$

Proposed approach:

- Use **conflict clauses in the witness**
- **Validation** is much **faster** with the extra information of conflict clauses

