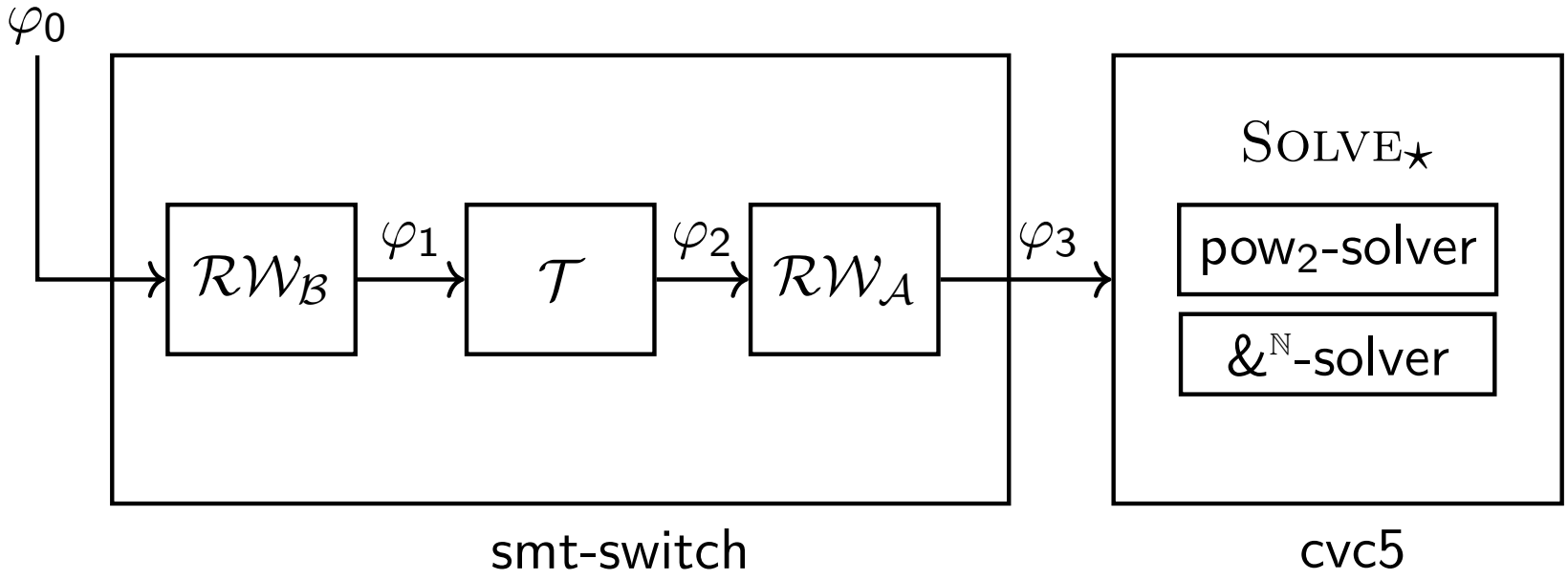
Department of
Computer Science
Faculty of Exact Sciences
Bar-Ilan University

Integrating Parametric Bit-vectors into cvc5

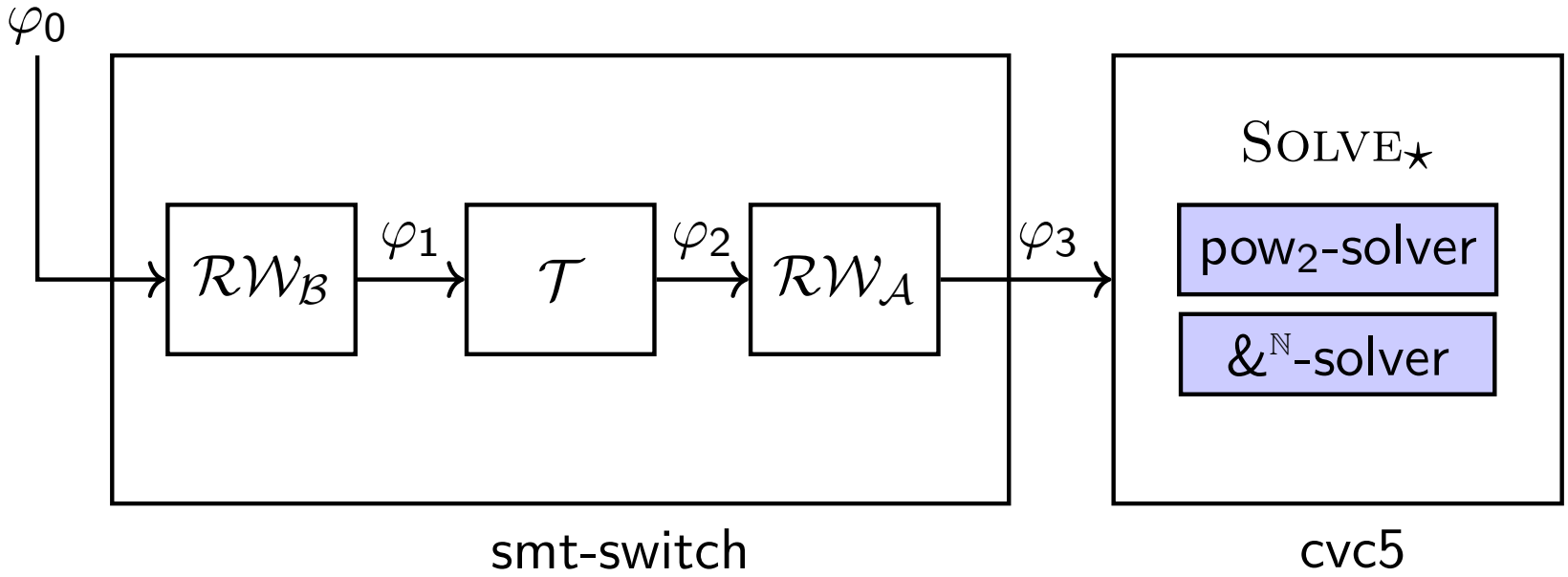
Zvika Berger

cvc5 summit

Current Architecture

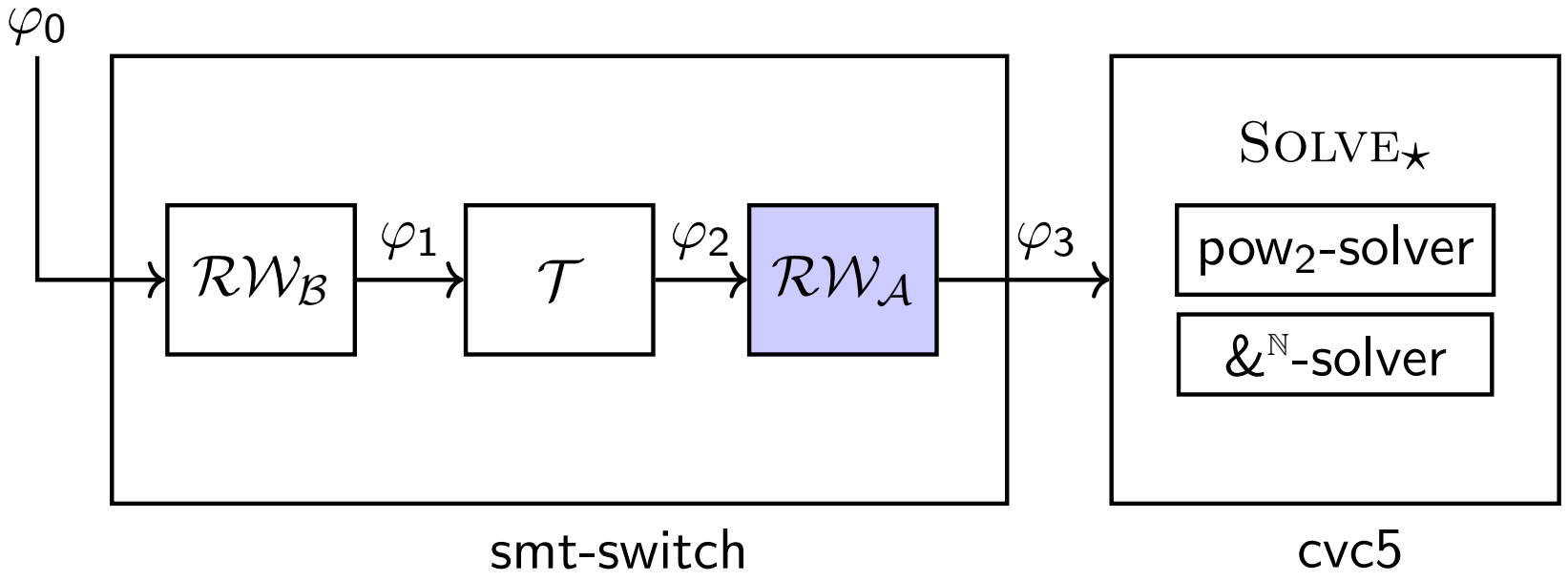


Integration into cvc5 - Phase 1 (theory solvers)



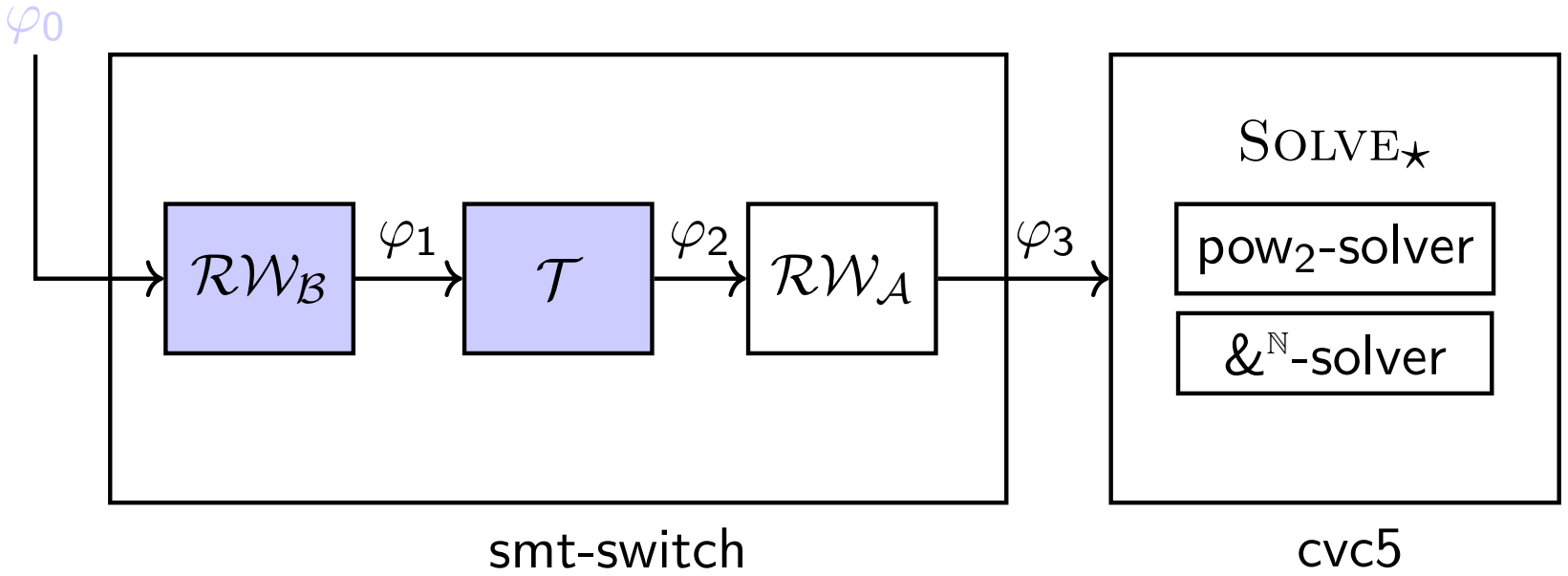
- New lemmas for `pow2`.
  - Pull request submitted.
- `piand` operator, rewriter, and solver.
  - Pull request coming soon.

Integration into cvc5 - Phase 2 (arithmetic rewriter)



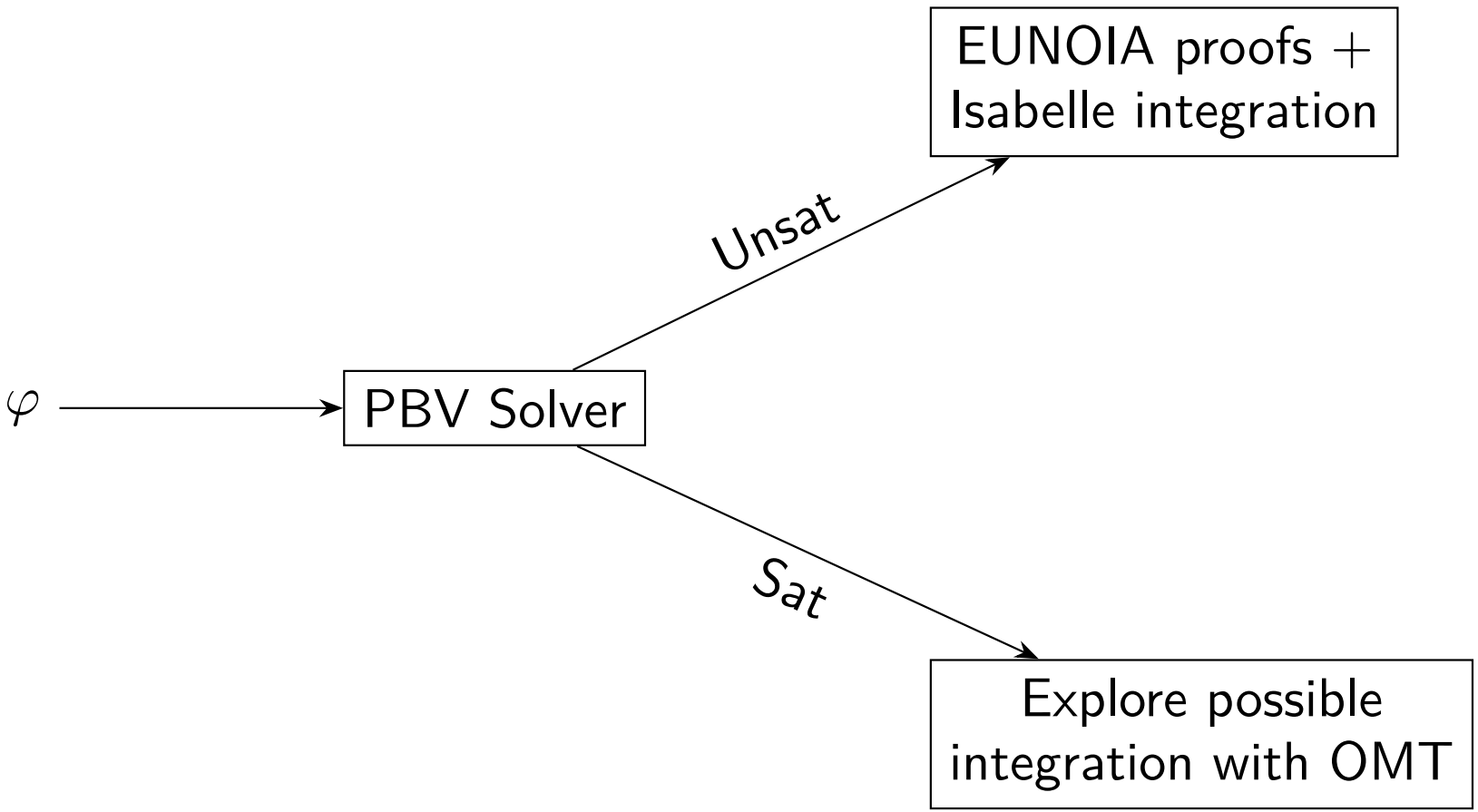
- New rewrite rules for `mod` in the cvc5 arithmetic rewriter.
  - Implement as a static rewriter.

Integration into cvc5 - Phase 3 (new theory)



- Add a new sort (PBV) and many new operators.
- Implement a PBV rewriter.
- Reimplement int-blasting to support PBV.
- Eliminate `iand` as a special case.

Integration into cvc5 - Phase 4 (General PBV)



Parametric Bit-Vectors Theory

- $T_{PBV} = (\Sigma_{PBV}, I_{PBV})$
- The set $\Sigma_{PBV} = \Sigma_{IA} +$ the following operators:

Symbol	**SMT-LIB Syntax**	**Sort**
$\approx_{\text{PBV}}, \not\approx_{\text{PBV}}$	`=, distinct`	PBV $\times$ PBV $\rightarrow$ Bool
$<_{\text{u}}, >_{\text{u}}, <_{\text{s}}, >_{\text{s}}$	`bvult, bvugt, bvslt, bvsgt`	PBV $\times$ PBV $\rightarrow$ Bool
$\leq_{\text{u}}, \geq_{\text{u}}, \leq_{\text{s}}, \geq_{\text{s}}$	`bvule, bvuge, bvsle, bvsge`	PBV $\times$ PBV $\rightarrow$ Bool
$\sim, -^{\mathcal{B}}$	`bvnot, bvneg`	PBV $\rightarrow$ PBV
$\&, \mid, \oplus$	`bvand, bvor, bvxor`	PBV $\times$ PBV $\rightarrow$ PBV
$\ll, \gg, \gg_a$	`bvshl, bvlshr, bvashr`	PBV $\times$ PBV $\rightarrow$ PBV
$+^{\mathcal{B}}, -^{\mathcal{B}}$	`bvadd, bvsub`	PBV $\times$ PBV $\rightarrow$ PBV
$\cdot^{\mathcal{B}}$, mod$^{\mathcal{B}}$, div$^{\mathcal{B}}$	`bvmul, bvurem, bvudiv`	PBV $\times$ PBV $\rightarrow$ PBV
$\_[\_:\_]$	`pextract`	PBV $\times$ Int $\times$ Int $\rightarrow$ PBV
$\circ$	`concat`	PBV $\times$ PBV $\rightarrow$ PBV
ext_z	`pzero_extend`	Int $\times$ PBV $\rightarrow$ PBV
ext_s	`psign_extend`	Int $\times$ PBV $\rightarrow$ PBV
$\lvert\_\rvert$	`bvsize`	PBV $\rightarrow$ Int
topbv	`int_to_pbv`	Int $\times$ Int $\rightarrow$ PBV