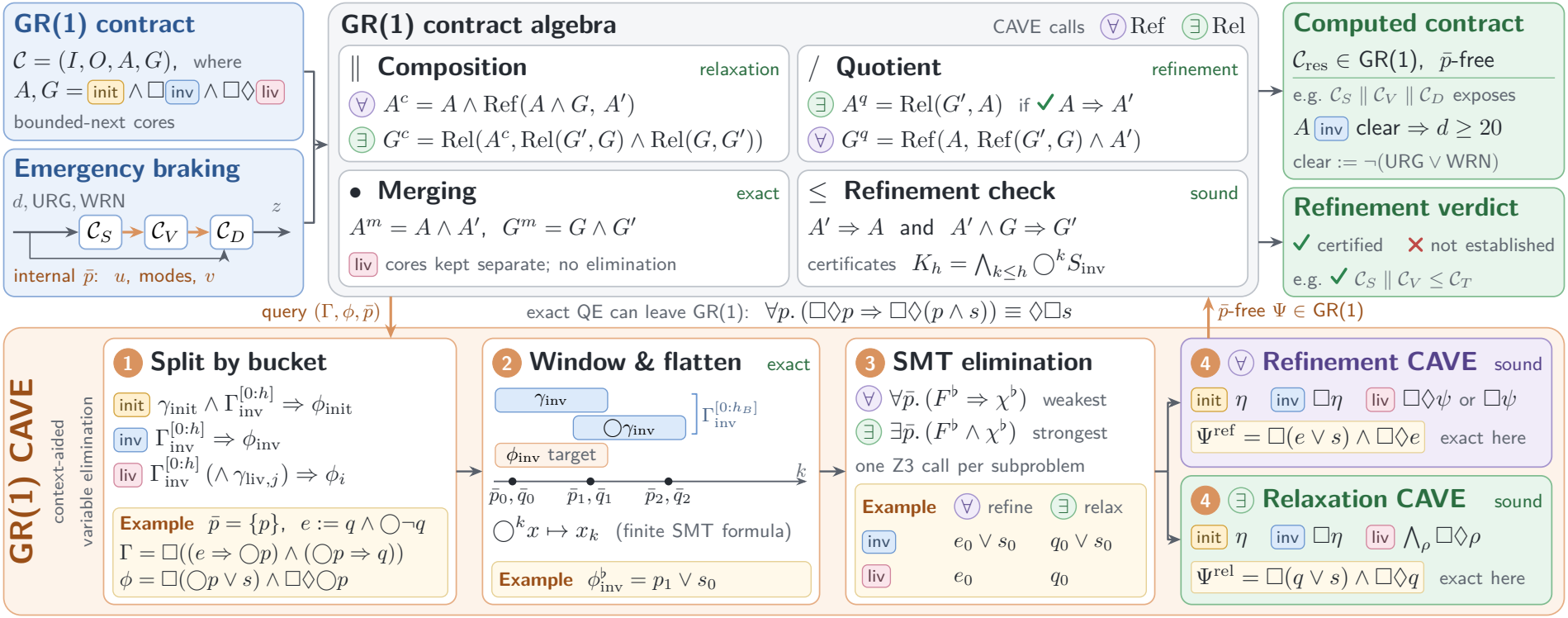

GR(1) contract
$\mathcal{C} = (I, O, A, G)$, where
$A, G =$ init $\wedge \square$ inv $\wedge \square\Diamond$ liv
bounded-next cores
Emergency braking
d, URG, WRN
z
$\mathcal{C}_S$ $\mathcal{C}_V$ $\mathcal{C}_D$
internal $\bar{p}$: u, modes, v
GR(1) contract algebra
CAVE calls ∀ Ref ∃ Rel
‖ Composition relaxation
$A^c = A \wedge \mathrm{Ref}(A \wedge G,\ A')$
$G^c = \mathrm{Rel}(A^c, \mathrm{Rel}(G', G) \wedge \mathrm{Rel}(G, G'))$
/ Quotient refinement
$A^q = \mathrm{Rel}(G', A)$ if ✓ $A \Rightarrow A'$
$G^q = \mathrm{Ref}(A,\ \mathrm{Ref}(G', G) \wedge A')$
• Merging exact
$A^m = A \wedge A'$, $G^m = G \wedge G'$
liv cores kept separate; no elimination
≤ Refinement check sound
$A' \Rightarrow A$ and $A' \wedge G \Rightarrow G'$
certificates $K_h = \bigwedge_{k \le h} \bigcirc^k S_{\mathrm{inv}}$
Computed contract
$\mathcal{C}_{\mathrm{res}} \in$ GR(1), $\bar{p}$-free
e.g. $\mathcal{C}_S \parallel \mathcal{C}_V \parallel \mathcal{C}_D$ exposes
A inv clear $\Rightarrow d \ge 20$
clear := ¬(URG ∨ WRN)
Refinement verdict
✓ certified ✗ not established
e.g. ✓ $\mathcal{C}_S \parallel \mathcal{C}_V \le \mathcal{C}_T$
query $(\Gamma, \phi, \bar{p})$
exact QE can leave GR(1): $\forall p.\ (\square\Diamond p \Rightarrow \square\Diamond(p \wedge s)) \equiv \Diamond\square s$
$\bar{p}$-free $\Psi \in$ GR(1)
GR(1) CAVE
context-aided variable elimination
1 Split by bucket
init $\gamma_{\mathrm{init}} \wedge \Gamma_{\mathrm{inv}}^{[0:h]} \Rightarrow \phi_{\mathrm{init}}$
inv $\Gamma_{\mathrm{inv}}^{[0:h]} \Rightarrow \phi_{\mathrm{inv}}$
liv $\Gamma_{\mathrm{inv}}^{[0:h]}\ (\wedge \gamma_{\mathrm{liv},j}) \Rightarrow \phi_i$
Example $\bar{p} = \{p\}$, $e := q \wedge \bigcirc\neg q$
$\Gamma = \square((e \Rightarrow \bigcirc p) \wedge (\bigcirc p \Rightarrow q))$
$\phi = \square(\bigcirc p \vee s) \wedge \square\Diamond\bigcirc p$
2 Window & flatten exact
γ_{inv}
$\bigcirc\gamma_{\mathrm{inv}}$
$\Gamma_{\mathrm{inv}}^{[0:h_B]}$
ϕ_{inv} target
k
$\bar{p}_0, \bar{q}_0$ $\bar{p}_1, \bar{q}_1$ $\bar{p}_2, \bar{q}_2$
$\bigcirc^k x \mapsto x_k$ (finite SMT formula)
Example $\phi_{\mathrm{inv}}^{\flat} = p_1 \vee s_0$
3 SMT elimination
∀ $\forall\bar{p}.\ (F^{\flat} \Rightarrow \chi^{\flat})$ weakest
∃ $\exists\bar{p}.\ (F^{\flat} \wedge \chi^{\flat})$ strongest
one Z3 call per subproblem
Example ∀ refine ∃ relax
inv $e_0 \vee s_0$ $q_0 \vee s_0$
liv e_0 q_0
4 ∀ Refinement CAVE sound
init η inv $\square\eta$ liv $\square\Diamond\psi$ or $\square\psi$
$\Psi^{\mathrm{ref}} = \square(e \vee s) \wedge \square\Diamond e$ exact here
4 ∃ Relaxation CAVE sound
init η inv $\square\eta$ liv $\bigwedge_\rho \square\Diamond\rho$
$\Psi^{\mathrm{rel}} = \square(q \vee s) \wedge \square\Diamond q$ exact here