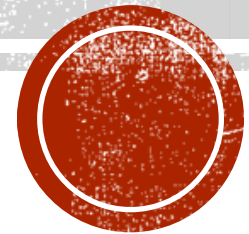# PRIORITIZING LEMMA PUSHING

Hari Govind V K, Arie Gurfinkel, Yakir Vizel and Vijay Ganesh

INCREMENTAL PROOFS

INCREMENTAL PROOFS →
ORDER OF PROVING LEMMAS IS CRITICAL

INCREMENTAL PROOFS ➔
ORDER OF PROVING LEMMAS IS CRITICAL ➔
FIGURE OUT A GOOD ORDERING HEURISTIC

SAFETY

- Given < Init , Tr , P > prove that P holds on all states reachable from Init

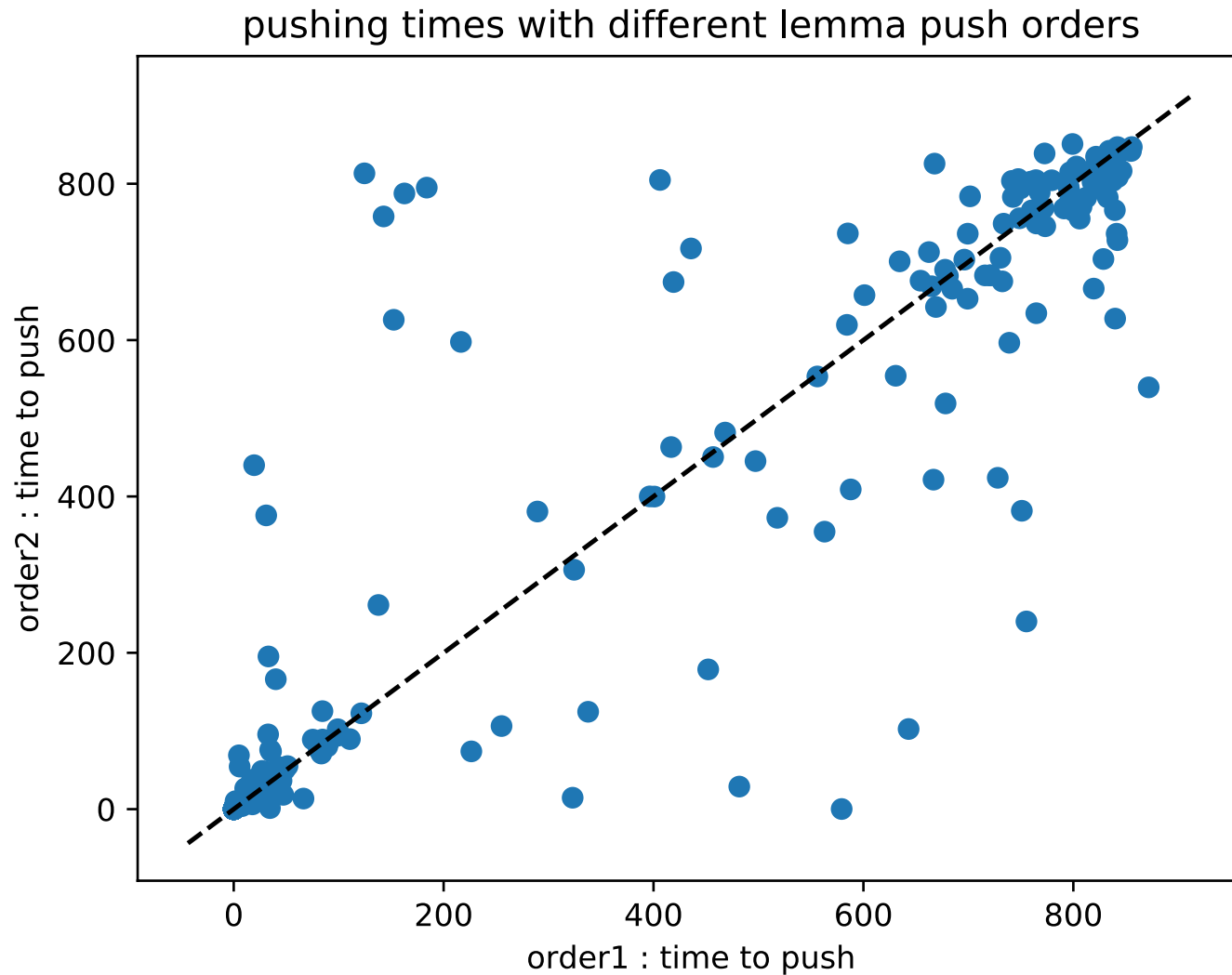# INCREMENTAL PROOF CONSTRUCTION

- Safety can be proven using inductive invariants
  - Init $\rightarrow$ Inv
  - Inv & Tr $\rightarrow$ Inv
  - Inv $\rightarrow$ P

- IC3 based algorithms construct Inv incrementally : conjoin several lemmas to prove the property up to a bound and then push the lemmas forward

ORDER OF PUSHING MATTERS

pushing times with different lemma push orders

WHAT WOULD BE THE RIGHT ORDER ?

- Pushing one lemma depends on many supporting lemmas

- Push support set before pushing this lemma

- Support sets are dynamic

FIGURING OUT THE RIGHT ORDER

- Pushing a lemma is a repetition of previous proofs at higher bounds

- By trial and error, we can learn the correct order

THANK YOU

POSTER 76   PRIORITIZING LEMMA PUSHING