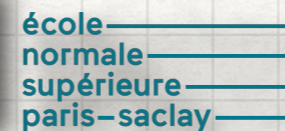


# Integrating Automated Provers in Proof Assistants

---

Mohamed Yacine EL HADDAD

14 Novembre 2018





## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo



## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo





## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo



Proof Checker



## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo





## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo



✓ More Powerful

✗ Hard to check



## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo



✓ More Powerful

✗ Hard to check



✗ Less powerful

✓ Easily to check



## Theorem Provers :

- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo



✓ More Powerful

✗ Hard to check



✗ Less powerful

✓ Easily to check

?



## Theorem Provers :

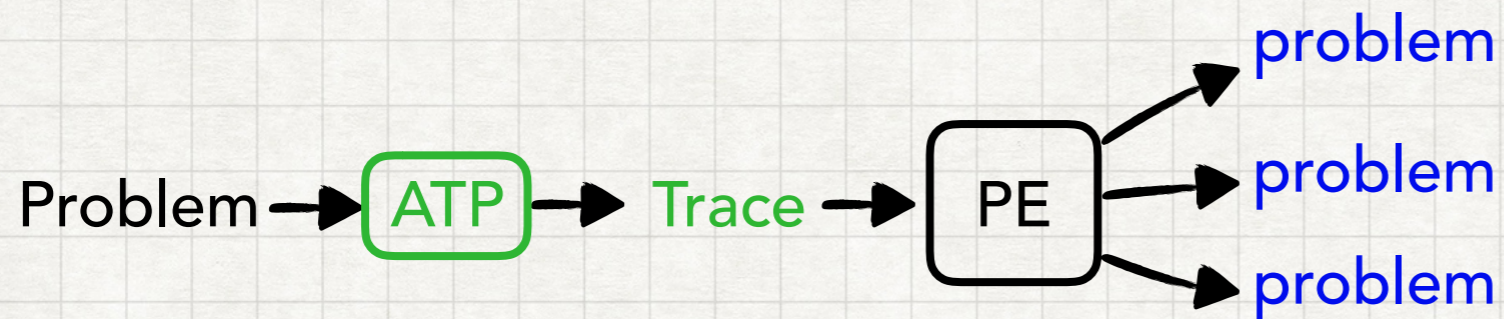
- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo





## Theorem Provers :

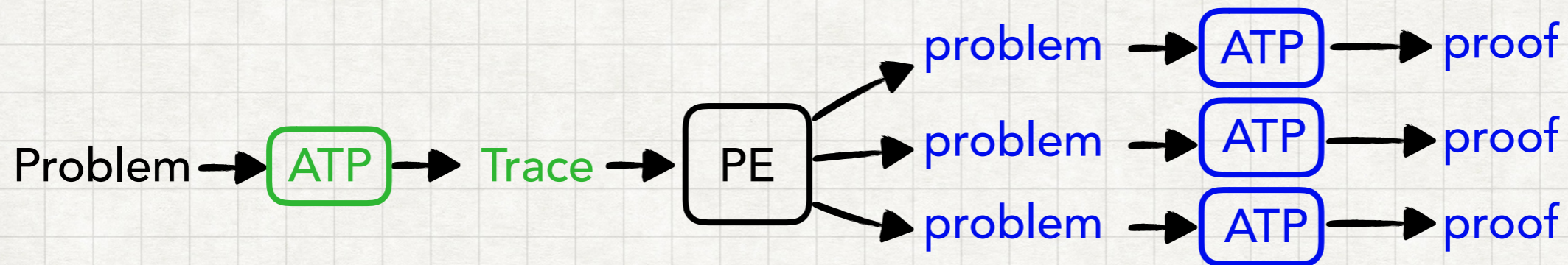
- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo





## Theorem Provers :

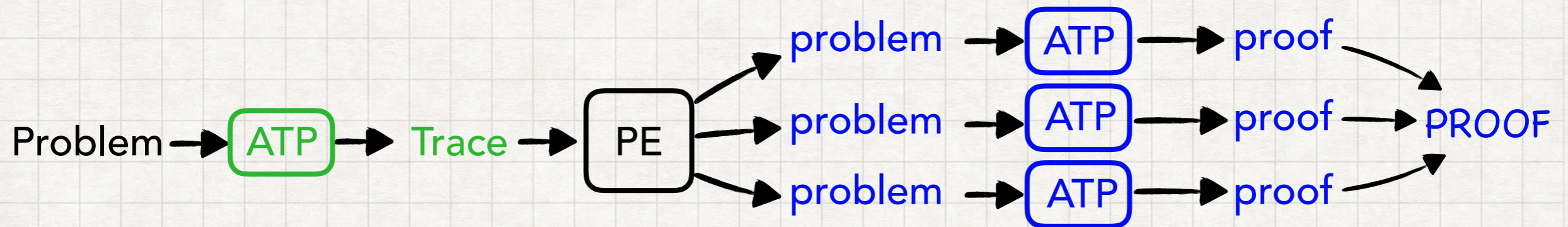
- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo





## Theorem Provers :

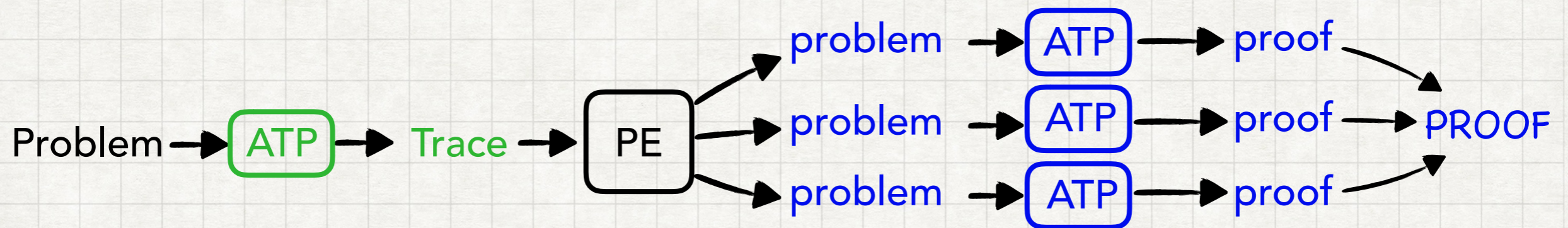
- **Interactive** : Coq, Isabelle, Matita, Dedukti ?...
- **Automated (ATP)** : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo





## Theorem Provers :

- Interactive : Coq, Isabelle, Matita, Dedukti ?...
- Automated (ATP) : Z3, E-prover, Vampire, Zenon, ZenonModulo, iProverModulo



## Gain :

- Complete proof
- Independent ATPs
- Parallel proving

	E	ZenonModulo	E+ZenonModulo
TSTP / Dedukti	55%	15%	34%
Checkability	No	Yes	Yes
Time/Problem	5mn	5mn	5mn + 10s/problem