JAVA PROGRAMMIDE VERIFITSEERIMINE MUDELIKONTROLLI ABIL

Bandera näitel

Juhan Ernits
Küberneetika Instituut / TTÜ arvutiteaduse instituut

Arulas 3-5 veebruaril 2003

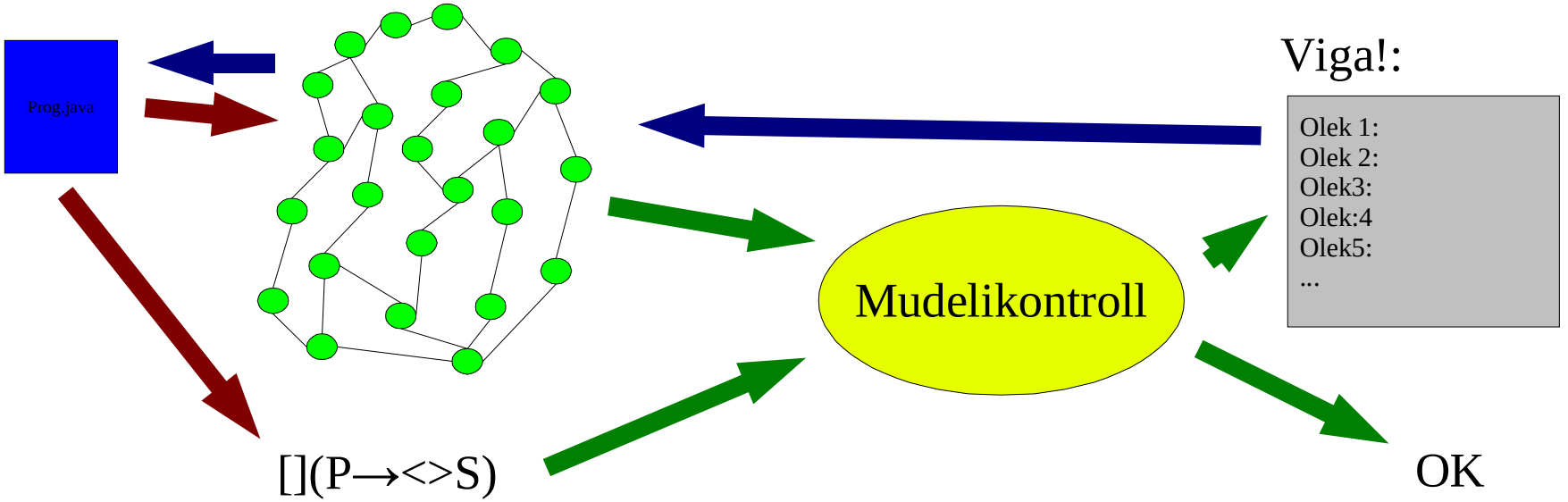
Ülevaade

- Eesmärk:
  - Anda põgus ülevaade ühest võimalikust metoodikast, kuidas kontrollida programmide omadusi.
  - Uurimisobjektiks on Bandera. (võimalikke variante on rohkem: JPL, SLAM, Alloy ...)
- Ajakava:
  - 10 slaidi sissejuhatust (~ 15 min);
  - Bandera demo (kuni õhtusöögini);

Miks üldse üritada uurida programmide omadusi mudelikontrolli abil?

- Kontrollida automaatselt:
  - invariantide, lihtsate turvalisus- ning elusustingimuste kehtivust;
  - tupikute mitteolemasolu;
  - keerukate sündmusjadade kehtivusomadusi.
- Vastupidiselt simulatsioonidele ning testimisele vaadatakse programmi kõik võimalikud jooksud;
- Mudelikontrolli on juba pikka aega edukalt kasutatud mitmesuguste (riistvara taseme) protokollide arendamisel. See lubab loota, et mudelikontroll täiendab olemasolevaid tarkvara kvaliteedi tagamise tehnikaid.

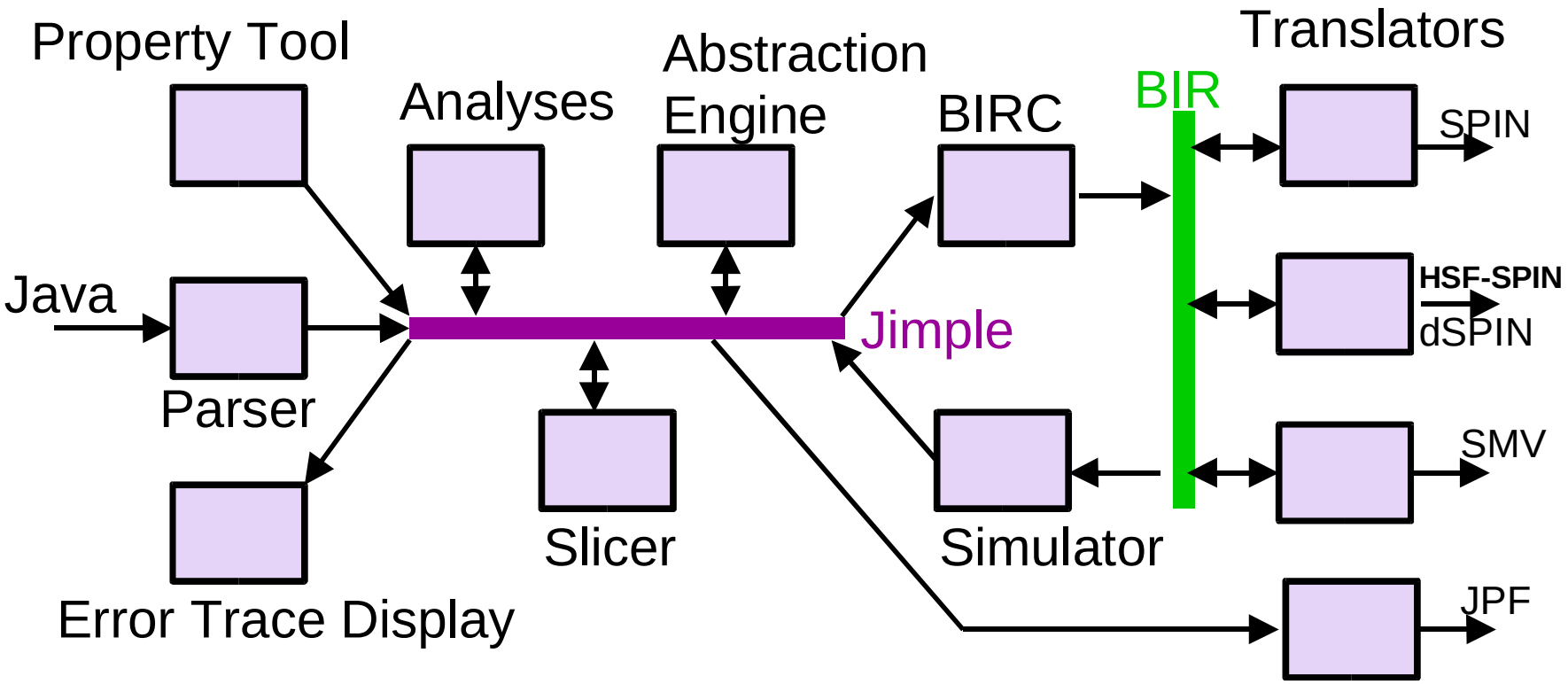
Programmide mudelikontroll



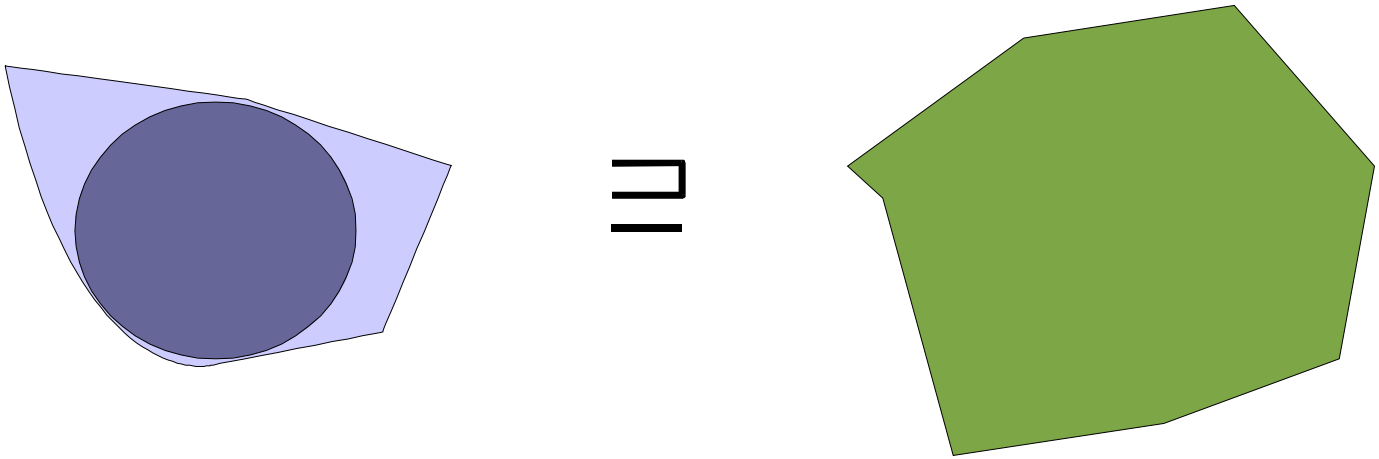
Probleemiks on:

- Mudeli koostamine programmist;
- Olekuruumi plahvatuslik suurenemine;
- Omaduste formuleerimine modaalloogikas;
- Tulemuse tõlgendamine lähtekoodi tasandil.

Bandera arhitektuur



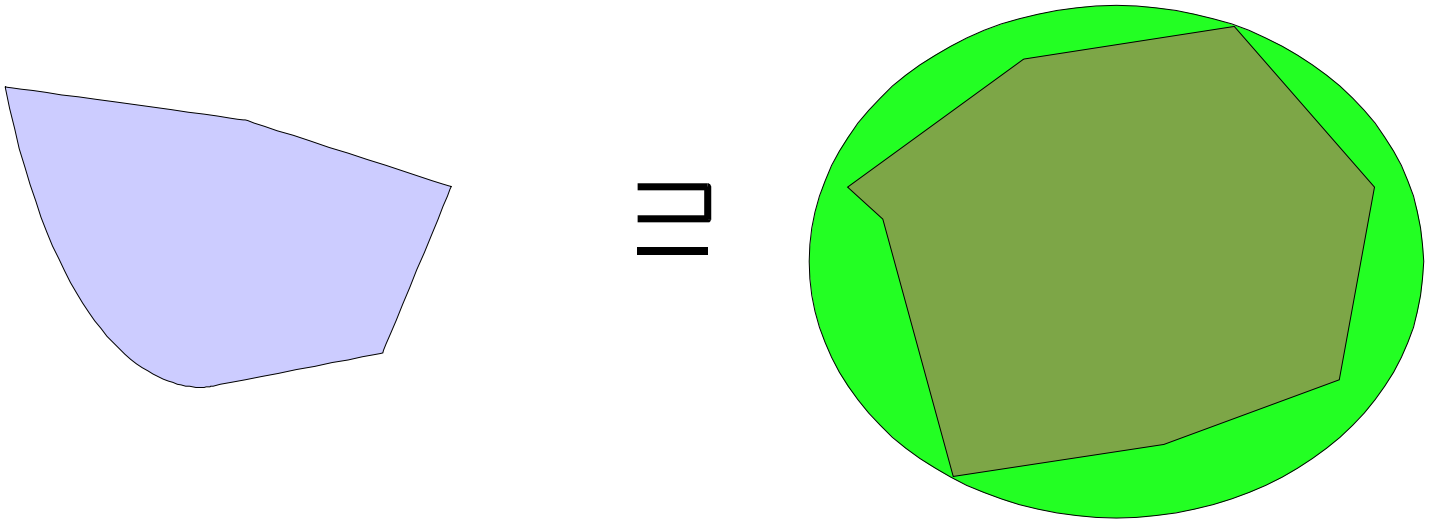
Alaaproksimeerimine



Nõuded

Mudel

Üleaproksimeerimine



Nõuded

Mudel

Kokkuvõte

- Bandera on avatud arhitektuur katsetamiseks.
- Võimaldab mudeli kirjeldamist sõltumatult konkreetsest mudelikontrolliprogrammist (toetab mitut erinevat mudelikontrolliprogrammi).
- Modifitseerib mudelit lähtudes analüüsitavast omadusest (lõiked, abstraktsioonid, ...).
- Ei toeta:
  - Rekursiivseid meetodeid;
  - Erandeid, sisemisi klasse, süsteemimeetodite väljakutseid.

Arengusuunad

- Mudelikontroll ei sobi hästi andmete omaduste analüüsiks. Sobib juhtimiskäskude ja saavutatavuse kontrolliks.
- Suur potentsiaal liideste ja sündmuste taseme analüüsiks (Cadena, Eclipse-i plugin).