Seminar za formalne metode i primjene

“Automatska verifikacija temporalnih protokola“

Dr.-Ing. Dario Krešić

22. listopada 2008.

Analiza protokola

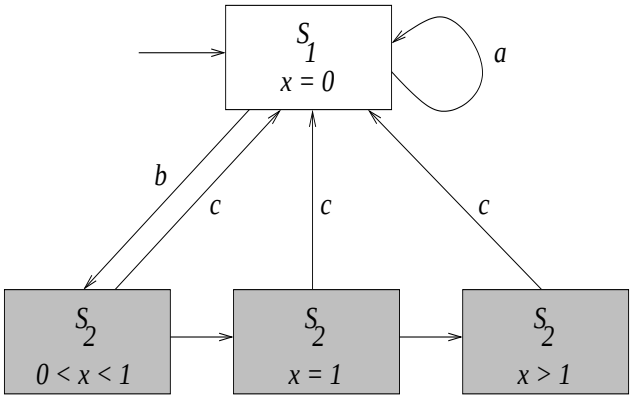
- protokoli: visoki paralelizam
- abstrakcija protokola i modeli
- konačni automat: $FA = (\Sigma, S, S_0, \Delta, F)$, gdje je
  - Σ konačna *abeceda*
  - S konačni skup *stanja*
  - $S_0 \subseteq S$ skup *početnih stanja*
  - Δ *relacija prijelaza*
  - F skup *završnih stanja*

Algoritamska verifikacija

- problem inkluzije: $L(\mathcal{A}) \subseteq L(\mathcal{B})$
- *model checking*: $\mathcal{A} \models \varphi$
- klase svojstava:
  - *safety*
  - *(real-time) liveness*

Prostor stanja

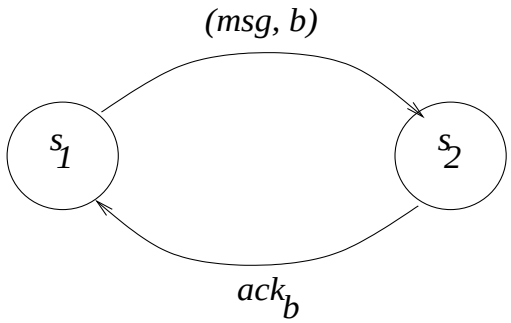
- diskretizacija kroz *regije*
- primjer:



- tzv. “eksplozija prostora stanja“ (*state space explosion*)
- broj regija: $O\left(|C|! \cdot 2^{|C|} \cdot \prod_{x \in C}(2c_x + 2)\right)$

Primjer: komunikacijski protokol (I)

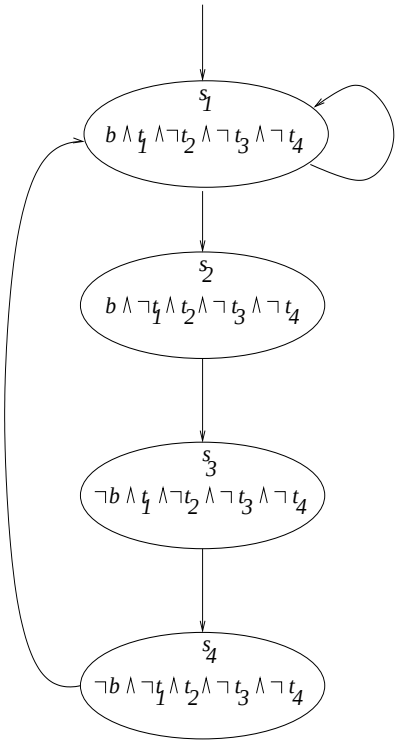
- *alternating bit protocol*:



- cilj: pouzdana komunikacija
- formalni model

Primjer: komunikacijski protokol (II)

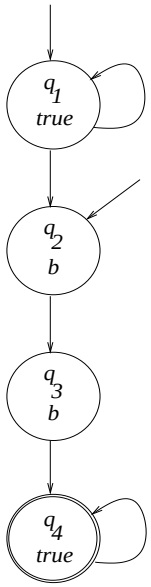
- prostor stanja protokola:



- regije kao propozicije nad satnom varijablom x

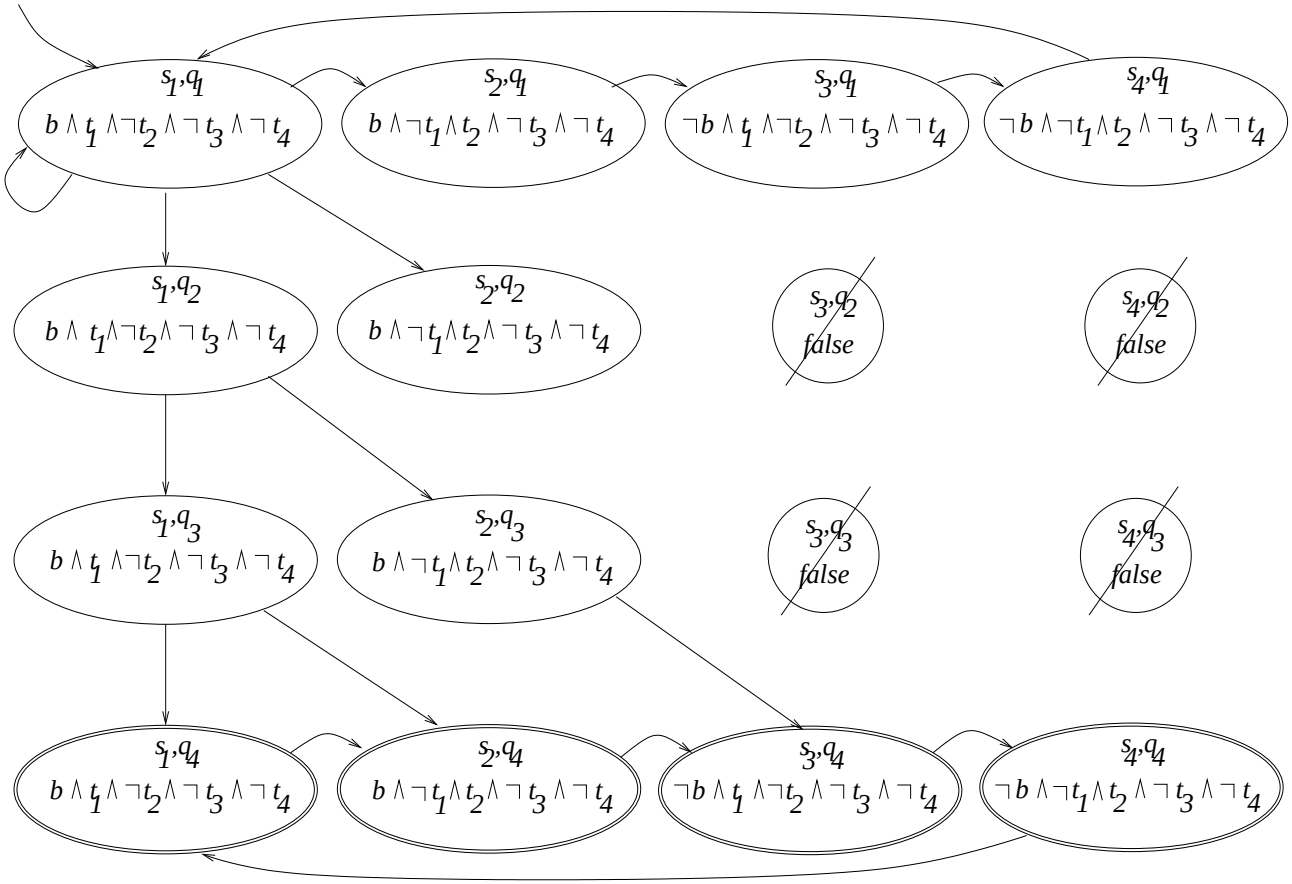
Primjer: komunikacijski protokol (III)

- svojstvo protokola: “*Sa svakom poslanom porukom mijenja se vrijednost potvrdnog bita*“
- specifikacija svojstva (LTL): $\Box(b \rightarrow \bigcirc\neg b)$
- transformacija LTL-formule:



Primjer: komunikacijski protokol (IV)

- konstrukcija presjeka



Primjer: komunikacijski protokol (IV)

- jezik presjeka automata *nije* prazan
- protuprimjer (*counter-example*)
- programska podrška: *UPPAAL* (Uppsala/BRICS)

Zaključak i diskusija

- (mogući) raskorak izmedju modela i stvarnosti
- protokoli s beskonačno mnogo stanja (*infinite state systems*)
- eksplozija prostora stanja
- efikasnost konstrukcije presjeka
- analiza protuprimjera
- . . .