NuSMV

- sustav za simboličku provjeru modela (SMV -symbolic model verifier), tj. kritičnih dijelova sustava - višedretvenost
- formalno: provjera vrijedi li M I= FI (M Kripke struktura, FI svojstvo u CTL/LTL)
- ulaz: opis programa u NuSMV jeziku i spec. Svojstava u CTL ili LTL, izlaz: T/F
- algoritam za provjeru modela temeljen na BDD-ovima (binarni dijagrami odlučivanja) i SAT-solvera za LTL koji se koristi za ograničenu (bounded) provjeru modela
- program = 1+ modul, jedini posebni modul je **main**
- modul = deklaracija varijabli, dodjeljivanje vrijednosti, svojstva za provjeru
    - k.r. process = asinkrono izvođenje modula
- varijable - tipovi. Boolean, vektor bitova, enum, integer, modul, nizovi, k.r. VAR
- dodjeljivanja - k.r. ASSIGN - na trenutnu vrijednost, inicijalnu (*init*), sljedeću (*next*)
    - može se dodijeliti više vrijednosti, ali samo jednom po *init* ili *next* bloku
    - graf ovisnosti ne smije imati cikluse - mora biti jasna dodjela
- specifikacija svojstava - operatori: &, I, ->, <->, E (egistenc. kvant), A (univ. kvant) puta
    - X - sljedeće stanje, F - kon. stanje, G - cijeli put, [ctlform U ctlform] - na dijelu puta
- nedeterminizam
    - **implicitni** - var. nema poč. vrijednost (ulazna varijabla)
    - **eksplicitni** - varijabli se dodjeluje skup vrijednosti
- modul - instanciranje t.d. se inicijalizira varijabla s imenom modula
    - m.v. - pristup varijabli v u modulu m
- **DEFINE** - k.r. za makro dodjelu (zamjena jedne riječi drugom)
    - ne proširuje prostor stanja, ne radi s nedeterminizmom
- sinkrono izvođenje - potoji globalni sat, svaki takt = paralelno izvođenje ASSIGN blokova
- asinkrono izvođenje - različiti moduli = različite brzine, proizvoljno ispreplitanje (interleaving)
    - unutarnja varijabla ***running*** - izvodi li se modul
    - interleaving - potrebno postaviti k.r. ***process*** kod instanciranja modula
- MUTEX (međusobno isključivanje) - definiramo kritične odsječke (k.o.)
    - svojstva: **sigurnost** - max. 1 proces u k.o., **životnost** - svaki proces će konačno ući u k.o., **neblokiranje** - drugi proces ne smije sprječavati ulaz u k.o. (zahtjevanje ulaza), **nedeterminirani redoslijed** - proizvoljan red ulaska u k.o.
- **pravednost** - svojstvo da je moguće ograničiti pretraživanje prostora stanja na samo one staze izvršavanja duž koje je CTL formula istinita beskonačno često - k.r. JUSTICE
    - JUSTICE running - nedeterminističko određivanje da ili ne izvoditi modul
- NuSMV u stilu ograničenja - INIT umjesto init, TRANS <- next, INVAR <- ekspl. dekl.
    - navodimo logičke tvrdnje koje trbaju vrijediti u modulu
    - rizik nekonzistentnih, mogu imati skriven nedeterminizam
- pokretanje NuSMV
    - uobičajeno (niz naredbi u konzoli)
    - interaktivno