MARIA: Saavutettavuusanalysaattori korkean tason verkoille

Sovellusalue

MARIA on suunniteltu insinöörien apuvälineeksi helpottamaan esimerkiksi tiedonsiirtoprotokollissa esiintyvien rinnakkaisuuteen liittyvien ongelmien mallintamista ja ratkaisemista.

Työkalu on tehty Teknillisen korkeakoulun Tietojenkäsittelyteorian laboratoriossa. Monet ajatukset perustuvat aiempaan PROD-työkaluun, mutta MARIA on rakennettu täysin modulaariseksi.

Etuja

- Sanallisten määrittelyjen epäselvyydet häviävät tai ratkeavat formaalin määrittelyn avulla
- Virheet löytyvät suunnitteluvaiheessa ennen ohjelmoinnin aloittamista
- Tehokas mallinnuskieli helpottaa sekä ihmisten että automaattisten kääntäjien työtä
- Ohjelmisto on saatavissa ja hyödynnettävissä vapaasti GNU-lisenssin ehdoilla
- C++-kielinen ohjelmisto toimii niin pienissä kuin suurissakin laitteistoissa

Ominaisuuksia

- Perustuu *formaaliin* korkean tason Petri-verkkoluokkaan, algebrallisiin järjestelmäverkkoihin
- Monipuoliset tietotyypit, tehokkaat operaatiot ja tarkat virheentarkistukset antavat lisäturvaa
- Tekstimuotoinen syötekieli, jota EMACS tukee
- Sekä tekstimuotoinen että graafinen käyttöliittymä
- Tila-avaruuksien ja virhepolkujen vuorovaikutteinen simulointi ja havainnollistaminen
- Kattava saavutettavuusanalyysi ja reiluusoletuksellinen LTL-mallintarkistus
- Probabilistinen turvallisuustarkistus
- Analyysin nopeuttamiseksi mallit voi kääntää C-kielisiksi

Teollisten järjestelmien analysointia

MARIAn mallinnuskielen ilmaisuvoima on lähellä korkean tason ohjelmointi- ja spesifiointikieliä (kuten Java ja SDL). Kielen tehokkaat jono- ja pino-operaatiot mahdollistavat monimutkaisenkin kommunikaation kuvaamisen lisäämättä malliin turhia, analyysiä hankaloittavia välitiloja.

Käyttäjien ei tarvitse tuntea analysaattorimme formalismia. *Sovellusalakohtainen etupää* sovittaa syötteen

- kääntämällä käyttäjän ohjelmat tai spesifikaatiot analysaattorin omaan formalismiin,
- mahdollistamalla haluttujen ominaisuuksien kuvaamisen sovelluksen omalla kielellä ja
- esittämällä löydetyt virheelliset käyttäytymiset sovelluksen suorituskaaviona.

Yleisellä formalismilla on joitakin etuja sovelluskohtaisiin formalismeihin nähden. Tehokkaampien analyysimenetelmien toteuttaminen hyödyttää heti kaikkia niitä kieliä, joille on käännös.

Olemme toteuttaneet etupään CCITT:n SDL-kielelle, ja Java-etupää on suunnitteilla. MARIAn monipuolisen tyyppijärjestelmän ansiosta lausekkeiden ja sanomanvälityksen kääntäminen on helppoa.

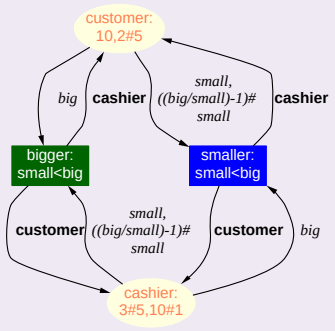
Yleiskuva

Työkalua voi käyttää sekä vuorovaikutteisesti (komentoriviltä ja graafisesti) että eräajona. Toimintatapoja on monia:

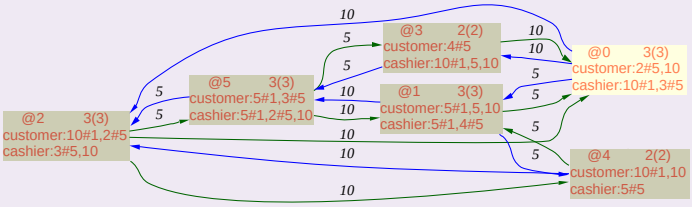
- täysi saavutettavuusanalyysi: tutkitaan kaikki saavutettavissa olevat tilat
- vuorovaikutteinen simulaatio: laske käyttäjän valitsemien tilojen seuraajat
- aikalogiikan kaavalla annetun turvallisuus- ja elävyysominaisuuden tarkistaminen
- mallin kääntäminen matalan tason Petri-verkoksi, haluttaessa kutistettuna

Työkalu hallitsee saavutettavuusgraafia (saavutettavia tiloja ja tilojen välisiä siirtymiä) levytiedostoissa. Keskusmuistin säästämisen ansiosta

```
typedef unsigned (1,5,10,50,100,500) money_t;

place customer money_t: 10,2#5;
place cashier money_t: 3#5,10#1;

trans smaller
in {
  place customer: big;
  place cashier: small, (big/small-1)#small;
}
gate big > small
out {
  place cashier: place customer;
  place customer: place cashier;
};

trans bigger
in {
  place customer: small, (big/small-1)#small;
  place cashier: big;
}
gate big > small
out {
  place customer: place cashier;
  place cashier: place customer;
};
```



Kuva 1: Eräs rahanvaihtoalgoritmi



Kuva 2: Rahanvaihtoalgoritmin tilat

- analyysi voidaan keskeyttää ja sitä voidaan jatkaa myöhemmin,
- luotua saavutettavuusgraafia voidaan tutkia toisella tietokoneella ja
- yksi rajoitus poistuu: erään 15 866 988-tilaisen ja 61 156 129-siirtymäisen mallin analyysi vei 5 megatavua muistia (ja 1,55 gigatavua levyä).

Kehittelemämme probabilistinen verifiointimenetelmä käyttää levyn sijasta rajoitettua muistialuetta saavutettavissa olevan tilajoukon esittämiseen. Se on hyödyllisimmillään tarkistettaessa turvallisuusominaisuuksia eräajona.

Graafin tutkiminen

Saavutettavuusgraafia voi tutkia ja selata monin tavoin. Tiloissa voi laskea lausekkeita ja aikalogiikan kaavoja. On mahdollista etsiä lyhin polku annetun tilan ja tilajoukon välillä. MARIA osaa laskea graafin vahvasti yhtenäiset komponentit.

Jos osittaisessa saavutettavuusgraafissa tarkistetaan aikalogiikan kaavaa, työkalu lisää graafiin uusia tiloja, kunnes se löytää vastaesimerkin tai toteaa, että kaavan ominaisuus pätee.

Simulaatio voi helpottaa mallintamistyötä. MARIA simuloi malleja hyvin läpinäkyvästi. Kun käyttäjä haluaa nähdä jonkin ennestään tutkimattoman tilan seuraajat, työkalumme lisää tilat saavutettavuusgraafiin ja näyttää ne käyttäjälle.

Kuva **??** esittää erästä yksinkertaista järjestelmää sekä MARIAn syötekielellä (EMACSin värittämänä) että graafisessa muodossa. Kuvassa **??** on järjestelmän tilaavaruus. Kuvien graafit on tuotettu MARIAlla ja muokattu käsin ennen niiden syöttämistä GRAPHVIZille.

Tehokkaat algebralliset operaatiot

Ohjelmointikielten perusrakenteiden lisäksi mallinnuskielessä on valmiita operaatioita

- jonojen ja pinojen käsittelemiseen,
- monijoukkojen perustoimituksiin (leikkaus, liitto, erotus, erilaiset kuvaukset) ja
- ryhmittämiseen (eksistentiaali- ja universaalikvantifiointi sekä monijoukkosummat).

Ryhmitysoperaatioiden indeksimuuttujien arvojen rajoittaminen dynaamisilla ehdoilla on erityisen tehokas rakenne hajautettujen algoritmien mallintamiseen. Palvelinta, joka lähettää viestin kaikille muille paitsi itselleen, voidaan kuvata lyhyellä lausekkeella. Palvelinten määrän muuttamiseksi riittää kajota yhteen ainoaan tietotyyppimääritykseen.

Peruslaskutoimitukset tarkistavat poikkeukset kuten ylivuodot ja nollalla jakamisen. Kaikki operaatiot tarkistavat rajoiterikkeet. Myös rakenteisten tietotyyppien arvoaluetta voi rajoittaa täysin mielivaltaisesti.

Saatavuus

MARIA on kehitetty UNIX-ympäristössä. Osa siitä toimii missä tahansa järjestelmässä, jolle on saatavissa standardin mukainen C++-kääntäjä. Työkalu on saatavissa osoitteesta `http://www.tcs.hut.fi/maria/`.

Vaikka lähestymistapamme oudoksuttaisikin hieman, älä epäröi ottaa meihin yhteyttä. Etsimme jatkuvasti kiinnostavia järjestelmiä, joiden mallintaminen ja analysoiminen auttavat kehittämään työkaluamme.