

# Automatsko rezonovanje – beleške sa predavanja Rezonovanje u logici prvog reda sa jednakošću

Milan Banković (po slajdovima Filipa Marića)

\* Matematički fakultet,  
Univerzitet u Beogradu

Prolećni semestar 2023/24.

# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme
- 3 Rezolucija i paramodulacija
- 4 Dedukcija i jednakost
- 5 Jednakosno rezonovanje
- 6 Kongruentno zatvorenje
- 7 Prezapisivanje

## Poseban tretman jednakosti

Kako interpretiramo simbol jednakosti?

Do sada je simbol  $=$  bio tretiran kao bilo koji drugi predikatski simbol.

Primer

*Za očekivati je da je formula*

$$\forall x y z. x = y \wedge y = z \Rightarrow f(x) = f(z)$$

*valjana, međutim, ona to nije. Po do sada izloženom, ova formula se ni po čemu ne razlikuje od formule*

$$\forall x y z. p(x, y) \wedge p(y, z) \Rightarrow p(f(x), f(z)),$$

*za koju je jasno da nije valjana (npr. netačna je kada se  $f$  interpretira identičkom funkcijom, a  $p$  nekom netranzitivnom relacijom).*

# Poseban tretman jednakosti

## Poželjno je da jednakost bude jednakost

- Ipak, uloga jednakosti je centralna u matematici tako da je poželjno posmatrati samo one interpretacije u kojima se simbol '=' interpretira upravo relacijom jednakosti.
- Iako se prethodno opisane procedure jednostavno modifikuju tako da u obzir uzmu samo ovakve modele, moguća je i izrada efikasnijih procedura, specijalizovanih za rezonovanje u prisustvu jednakosti.

# Normalne interpretacije

## Definicija

Ako signatura  $\mathcal{L}$  sadrži simbol  $=$ , za  $\mathcal{L}$ -strukturu (model, interpretaciju) kažemo da je *normalna* ako se simbol  $=$  interpretira relacijom jednakosti odgovarajućeg domena  $D$  (tj. relacijom  $\{(x, x) \mid x \in D\}$ )

## Definicija

*Logika prvog reda sa jednakošću* je fragment logike prvog reda u kome razmatramo samo signature koje sadrže simbol  $=$ , pri čemu se ograničavamo samo na normalne interpretacije.

# Zadovoljivost, valjanost, ...

## Definicija

Formula  $F$  je *valjana* u logici prvog reda sa jednakošću ako je tačna u svim normalnim interpretacijama. Formula  $F$  je *zadovoljiva* u logici prvog reda sa jednakošću ako ima normalni model.

## Definicija

Formula  $F$  je *logička posledica* skupa formula  $\Delta$  u logici prvog reda sa jednakošću (u oznaci  $\Delta \vDash F$  ako je tačna u svim normalnim interpretacijama u kojima su tačne i sve formule iz  $\Delta$ ).

## Definicija

Formule  $F$  i  $G$  su *logički ekvivalentne* (u oznaci  $F \equiv G$ ) ako važi  $F \vDash G$  i  $G \vDash F$ , tj. ako se interpretiraju isto u svim normalnim interpretacijama.

# Aksiome jednakosti

## Aksiome jednakosti

S obzirom da je relacija jednakosti relacija **ekvivalencije**, u svim normalnim interpretacijama naredne formule su tačne.

**refleksivnost** :  $\forall x. x = x$

**simetričnost** :  $\forall x y. x = y \Leftrightarrow y = x$

**tranzitivnost** :  $\forall x y z. x = y \wedge y = z \Rightarrow x = z$

Takođe, za svaki  $n$ -arni funkcijski simbol  $f$  odnosno svaki  $n$ -arni predikatski simbol  $p$  tačne su i formule **kongruentnosti**

$$\forall x_1 \dots x_n y_1 \dots y_n. x_1 = y_1 \wedge \dots \wedge x_n = y_n \Rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$$

$$\forall x_1 \dots x_n y_1 \dots y_n. x_1 = y_1 \wedge \dots \wedge x_n = y_n \Rightarrow p(x_1, \dots, x_n) \Leftrightarrow p(y_1, \dots, y_n)$$

Navedene formule nazivamo **aksiomama jednakosti**. Oznaka  $eqax(\mathcal{L})$  označava aksiome jednakosti jezika  $\mathcal{L}$ .

# Aksiome jednakosti

## Aksiome jednakosti i normalne interpretacije

- Svaka normalna interpretacija zadovoljava aksiome jednakosti.
- Međutim, postoje interpretacije koji nisu normalne, a opet zadovoljavaju aksiome jednakosti.

## Primer

*Ukoliko se jezik  $\mathcal{L} = \{+, \cdot, 0, 1, =\}$  interpretira uobičajeno na skupu prirodnih brojeva, a simbol  $=$  relacijom  $x \equiv y \pmod{2}$ , model zadovoljava aksiome jednakosti, a nije normalan.*

- Na žalost, nije moguće aksiomatski se ograničiti samo na normalne modele.
- Na sreću, to nam, sa stanovišta rezonovanja, nije ni neophodno.



# Veza između normalnih modela i modela aksioma jednakosti

## Stav

*Formula  $F$  jezika  $\mathcal{L}$  ima normalan model akko  $F$  i  $eqax(\mathcal{L})$  imaju model.*

## Dokaz

*Ako  $F$  ima normalan model on je model u kome su i  $F$  i  $eqax(\mathcal{L})$  tačne.*

*Obratno, ako postoji model za  $F$  i  $eqax(\mathcal{L})$  može se definisati relacija  $\sim$  na domenu  $D$  takva da je  $x \sim y$  akko  $x =_{\mathcal{M}} y$ , tj. kada su  $x$  i  $y$  jednaki po interpretaciji  $M$ . Pošto u  $M$  važe  $eqax(\mathcal{L})$  relacija  $\sim$  je relacija ekvivalencije. Traženi normalni model se može jednostavno izgraditi nad klasama ekvivalencije relacije  $\sim$  kao domenom.*

# Veza između normalnih modela i modela aksioma jednakosti

## Stav

- *Formula  $F$  je zadovoljiva u nekom normalnom modelu akko je formula  $F \wedge eqax(\mathcal{L})$  zadovoljiva (u opštoj logici prvog reda).*
- *Formula  $F$  važi u svim normalnim modelima akko je formula  $eqax(\mathcal{L}) \Rightarrow F$  valjana (u smislu opšte logike prvog reda).*

# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme**
- 3 Rezolucija i paramodulacija
- 4 Dedukcija i jednakost
- 5 Jednakosno rezonovanje
- 6 Kongruentno zatvorenje
- 7 Prezapisivanje

# Poluodlučivost i (ne)odlučivost

## Teorema

*Logika prvog reda sa jednakošću je poluodlučiva: za svaku formulu koja je valjana (tj. tačna u svim normalnim modelima) je moguće utvrditi da je valjana.*

## Teorema

*Logika prvog reda sa jednakošću nije odlučiva.*

# Kompaktnost

## Teorema

*Skup formula je zadovoljiv u logici prvog reda sa jednakošću (tj. tačan u nekom normalnom modelu) akko je svaki njegov konačan podskup zadovoljiv (u nekom normalnom modelu).*

# O konačnim modelima

Šta je moguće reći o kardinalnostima?

- U opštoj logici prvog reda nismo mogli da fiksiramo da skup formula ima samo modele neke fiksirane konačne kardinalnosti
- U logici prvog reda sa jednakošću to možemo. Npr. formula  $\exists x_1 x_2 x_3. x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3 \wedge (\forall y. y = x_1 \vee y = x_2 \vee y = x_3)$  ima samo normalne modele kardinalnosti 3
- Medjutim, ne možemo da se ograničimo samo na konačne modele (proizvoljne kardinalnosti)

## Teorema

*Ukoliko skup formula  $\Delta$  ima normalne modele svih mogućih konačnih kardinalnosti, tada ima i normalan model beskonačne kardinalnosti.*

## Dokaz

*Neka je formula  $\phi_n = \exists x_1 x_2 \dots x_n. x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \dots \wedge x_{n-1} \neq x_n$ . Ovu formulu zadovoljavaju svi normalni modeli kardinalnosti veće ili jednake od  $n$ . Posmatrajmo skup formula  $\Phi = \Delta \cup \{\phi_n \mid n \in \mathbb{N}\}$ . Svaki konačan podskup ovog skupa je zadovoljiv (jer po pretpostavci za skup  $\Delta$  postoji konačan model bilo koje kardinalnosti). Na osnovu teoreme kompaktnosti, sledi da je i ceo skup  $\Phi$  zadovoljiv. Medjutim, jasno je da njegov model mora biti beskonačan.*

# Skolem-Lovenhajmova teorema

A šta je sa beskonačnim kardinalnostima?

- Kada su u pitanju beskonačne kardinalnosti, ni ovde ne možemo ni na koji način fiksirati kardinalnost modela.
- Drugim rečima, važe Skolem-Lovenhajmove teoreme (na dole i na gore).

Teorema

*Ukoliko najviše prebrojiv skup formula ima beskonačan normalan model, tada ima  $i$  prebrojiv normalan model.*

Teorema

*Ukoliko najviše prebrojiv skup formula ima prebrojiv normalan model, tada on ima  $i$  normalan model bilo koje veće kardinalnosti.*

# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme
- 3 Rezolucija i paramodulacija**
- 4 Dedukcija i jednakost
- 5 Jednakosno rezonovanje
- 6 Kongruentno zatvorenje
- 7 Prezapisivanje



# Rezolucija u jednakosnoj logici

## Metod rezolucije i jednakost

- Metod rezolucije je bio jedan metod poluodlučivanja za opštu logiku prvog reda
- Ovaj metod se može koristiti i kao procedura poluodlučivanja za logiku prvog reda sa jednakošću
- Za to je dovoljno klauzalnoj formi formule  $F$  čiju zadovoljivost ispitujemo dodati aksiome jednakosti (prethodno konvertovane u klauzalnu formu)

# Rezolucija u jednakosnoj logici

## Primer

*Da bismo dokazali da je formula*

$$\forall x y z. x = y \wedge y = z \Rightarrow f(x) = f(z)$$

*valjana u jednakosnoj logici, možemo je najpre negirati, a zatim njenu negaciju svesti u klauzalni oblik. Dobijamo klauze:*

- 1)  $a = b$
- 2)  $b = c$
- 3)  $f(a) \neq f(c)$  (kraći zapis za  $\neg(f(a) = f(c))$ )

*Dodajmo tome i klauze koje predstavljaju aksiome jednakosti (one koje su nam potrebne ovde):*

- 4)  $x \neq y \vee y \neq z \vee x = z$
- 5)  $u \neq v \vee f(u) = f(v)$

*Sada iz 1 i 4 pravilom rezolucije dobijamo 6)  $b \neq z \vee a = z$ , a iz 2 i 6 dobijamo 7)  $a = c$ . Najzad, iz 7 i 5 dobijamo 8)  $f(a) = f(c)$ , pa iz 3 i 8 dobijamo praznu klauzu.*

# Paramodulacija

## Kako rezoluciju u prisustvu jednakosti učiniti efikasnom?

- Iako je prethodni primer bio prilično jednostavan, u slučaju složenijih tvrdjenja ovakav način dokazivanja postaje prilično neefikasan
- Najveći problem je utvrditi na koji način instancirati aksiome jednakosti
- Bolja ideja je da probamo da metod rezolucije obogatimo dodatnim pravilom koje će omogućiti jednakosno rezonovanje, bez uvođenja aksioma jednakosti
- Jedno takvo pravilo je pravilo **paramodulacije**

# Paramodulacija

## Definicija

*Pravilo paramodulacije glasi:*

$$\frac{C_1 \vee s = t \text{ (ili } t = s) \quad C_2 \vee L[t']}{(C_1 \vee C_2 \vee L[s])\sigma}$$

*gde je  $\sigma$  najopštiji unifikator za termine  $t$  i  $t'$ .*

## Napomene

- Može se pokazati da pravilo paramodulacije ima svojstvo saglasnosti
- Takodje, koristeći samo paramodulaciju i rezoluciju, iz refleksivnosti je moguće dokazati simetričnost i tranzitivnost jednakosti, kao i kongruentnost
- Otuda je za kompletost (za pobijanje) u jednakosnoj logici dovoljan metod rezolucije koji pored pravila paramodulacije implicitno podrazumeva i univerzalno kvantifikovanu jediničnu klauzu  $x = x$

# Paramodulacija

## Primer

*Posmatrajmo ponovo formulu*

$$\forall x y z. x = y \wedge y = z \Rightarrow f(x) = f(z)$$

*za koju dokazujemo da je valjana u jednakosnoj logici, tako što dokazujemo nezadovoljivost skupa klauza:*

- 1)  $a = b$
- 2)  $b = c$
- 3)  $f(a) \neq f(c)$

*Paramodulacijom iz 1) i 2) (za  $s = a$ ,  $t = b$ ,  $t' = b$ ) dobijamo 4)  $a = c$ . Dalje, iz 4) i 3) paramodulacijom (za  $s = a$ ,  $t = c$ ,  $t' = c$ ) dobijamo 5)  $f(a) \neq f(a)$ . Koristeći implicitnu klauzu refleksivnosti  $x = x$ , rezolucijom sa 5) dobijamo praznu klauzu.*

# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme
- 3 Rezolucija i paramodulacija
- 4 Dedukcija i jednakost**
- 5 Jednakosno rezonovanje
- 6 Kongruentno zatvorenje
- 7 Prezapisivanje

# Dedukcija i jednakost

## Deduktivni sistemi za jednakost

- Svi deduktivni sistemi logike prvog reda (Hilbertov sistem, prirodna dedukcija, ...) se mogu koristiti i u logici sa jednakošću
- Jednakost se tretira tako što koristimo aksiome jednakosti kao pretpostavke
- Alternativno, možemo aksiome jednakosti formulisati i kao dodatna pravila deduktivnog sistema

# Pravila dedukcije za jednakost

## Refleksivnost

$$\frac{}{u = u} \textit{ refl}$$

## Simetričnost

$$\frac{u = v}{v = u} \textit{ sym}$$

## Tranzitivnost

$$\frac{u = v \quad v = w}{u = w} \textit{ trans}$$

## Kongruencija

$$\frac{t_1 = s_1 \quad \dots \quad t_n = s_n}{f(t_1, \dots, t_n) = f(s_1, \dots, s_n)} \textit{ congF}$$

$$\frac{t_1 = s_1 \quad \dots \quad t_n = s_n}{p(t_1, \dots, t_n) \Rightarrow p(s_1, \dots, s_n)} \textit{ congP}$$



# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme
- 3 Rezolucija i paramodulacija
- 4 Dedukcija i jednakost
- 5 Jednakosno rezonovanje**
- 6 Kongruentno zatvorenje
- 7 Prezapisivanje

# Jednakosno rezonovanje

## Teorija jednakosti sa neinterpretiranim funkcijskim simbolima

- U prethodnom razmatranju smo podrazumevali da signatura pored jednakosti sadrži i druge predikatske simbole
- Možemo se dalje ograničiti samo na signature koje ne sadrže druge predikatske simbole osim jednakosti
  - sa druge strane, signatura može sadržati funkcijske simbole koji se mogu interpretirati na proizvoljan način (tj. pretpostavljamo da važe samo aksiome jednakosti)
- ovakva logička teorija je poznata i kao **teorija jednakosti sa neinterpretiranim funkcijskim simbolima** (engl. **Equality with Uninterpreted Functions (EUF)**)
  - jedini literali u formulama ove teorije su **jednakosti** i **različitosti** nad termovima koji su izgrađeni nad neinterpretiranim funkcijskim simbolima

# Jednakosno rezonovanje

## Postavka problema

Centralni problem koji ćemo posmatrati je sledeći:

$$\Delta \models s = t$$

gde je  $\Delta$  skup univerzalno kvantifikovanih jednakosti, a  $s = t$  je univerzalno kvantifikovana jednakost.

- Dakle, ispitujemo da li je neka jednakost logička posledica datog skupa jednakosti (podrazumevamo samo normalne interpretacije).
- Univerzalne kvantifikacije su obično implicitne
- Može se pokazati da se možemo ograničiti na slučajeve kada je jednakost  $s = t$  bazna, što ne umanjuje opštost

# Jednakosno rezonovanje

## Stav

*Problem  $\Delta \models s = t$  u kome su sve promenljive koje se pojavljuju u  $s = t$  implicitno univerzalno kvantifikovane ekvivalentan je problemu  $\Delta \models s = t$  u kome se sve promenljive koje se pojavljuju u  $s = t$  tretiraju kao konstante.*

## Dokaz

*Pretpostavimo da jednakost  $s = t$  sadrži promenljive  $x_1, \dots, x_n$  koje su implicitno univerzalno kvantifikovane. Problem  $\Delta \models s = t$  je ekvivalentan problemu ispitivanja (ne)zadovoljivosti skupa formula  $\Delta \cup \{\neg \forall x_1 \dots x_n. s = t\}$ . Negacijom univerzalnog kvantifikatora dobijamo egzistencijalni, pa skolemizacijom dobijamo ekvizadovoljiv skup  $\Delta \cup \{s \neq t\}$  (gde se promenljive  $x_1, \dots, x_n$  nadalje tumače kao konstante). Otuda je gornji problem ekvivalentan problemu ispitivanja logičke posledice  $\Delta \models s = t$ , pri čemu je  $s = t$  sada bazna jednakost.*

# Sintaksno-deduktivni sistemi za jednakost

## Deduktivni sistemi u teoriji jednakosti

- Kako bismo automatizovali rešavanje prethodnog problema, možemo kao i u opštoj logici prvog reda, razmatrati deduktivne sisteme za jednakost
- Ovakvi deduktivni sistemi su jednostavniji od opštih deduktivnih sistema, jer ne moraju sadržati pravila za iskazne veznike, s obzirom na formu problema koji razmatramo
- Jedan takav sistem je **Birkhoffov sistem** koji prikazujemo u nastavku

# Sintaksno-deduktivni sistemi za jednakost — Birkhofova pravila

## Birkhofova pravila

$$\frac{}{\Delta \vdash t = t} \text{ refl}$$

$$\frac{\Delta \vdash s = t}{\Delta \vdash t = s} \text{ sym}$$

$$\frac{\Delta \vdash s = t \quad \Delta \vdash t = u}{\Delta \vdash s = u} \text{ trans}$$

$$\frac{\Delta \vdash s_1 = t_1 \quad \dots \quad \Delta \vdash s_n = t_n}{\Delta \vdash f(s_1, \dots, s_n) = f(t_1, \dots, t_n)} \text{ cong}$$

$$\frac{}{\Delta, s = t \vdash s = t} \text{ ax}$$

$$\frac{\Delta \vdash s = t}{\Delta \vdash (s = t)[x \rightarrow a]} \text{ inst}$$

## Primer

*Dokažimo da važi:*

$$a = b, c = b \vdash f(a) = f(c)$$

*Imamo sledeći dokaz u Birkhofovom sistemu:*

$$\frac{\frac{a = b, c = b \vdash a = b}{ax} \quad \frac{\frac{a = b, c = b \vdash c = b}{sym} \quad \frac{a = b, c = b \vdash b = c}{tran}}{a = b, c = b \vdash a = c} \quad \frac{a = b, c = b \vdash a = c}{a = b, c = b \vdash f(a) = f(c)} \quad cong$$

# Birkofova teorema

## Teorema

$\Delta \models s = t$ , tj. jednačina  $s = t$  važi u svim normalnim modelima skupa jednačina  $\Delta$  akko i samo ako  $\Delta \vdash s = t$ , tj. ako se  $s = t$  može izvesti iz  $\Delta$  primenom Birkofovih pravila.



# Zamenski dokazi

## Definicija

*Neka je dat problem  $E \vdash s = t$ , gde je  $s = t$  bazna jednakost. Pod zamenskim dokazom jednakosti  $s = t$  iz  $E$  podrazumevamo lanac jednakosti  $u_0 = u_1 = \dots = u_n$ , gde je  $u_0 = s$ ,  $u_n = t$ , i važi da je  $u_{i+1} = u_i[l_j \rightarrow r_j]$ , gde je  $l_j = r_j$  (ili  $r_j = l_j$ ) bazna instanca neke jednakosti iz  $E$ .*

## Teorema

*$E \vdash s = t$ , tj.  $s = t$  se može dokazati iz  $E$  u Birkhofovom sistemu akko postoji zamenski dokaz za  $s = t$  iz  $E$ .*

# Zamenski dokazi

## Primer

*Dokažimo da važi*

$$a = b, c = b \vdash f(a) = f(c)$$

*Imamo sledeći zamenski dokaz:  $f(a) = f(b) = f(c)$ , pri čemu smo najpre  $a$  zamenili sa  $b$  (na osnovu jednakosti  $a = b$ ), a zatim smo  $b$  zamenili sa  $c$  (na osnovu jednakosti  $c = b$ ).*

# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme
- 3 Rezolucija i paramodulacija
- 4 Dedukcija i jednakost
- 5 Jednakosno rezonovanje
- 6 Kongruentno zatvorenje**
- 7 Prezapisivanje

# Odlučivanje baznih jednakosti

## Bazni fragment teorije EUF

- Prilikom primene Birkofovih pravila problem predstavlja pravilo instancijacije (nije jasno kako odlučiti koju instancijaciju  $x \rightarrow t$  upotrebiti).
- Ukoliko su sve jednakosti bazne (nemaju slobodnih promenljivih), onda pravilo instancijacije nije potrebno koristiti, što čini ovaj fragment odlučivim.
- Procedure odlučivanja za bazne jednakosti se obično zasnivaju na kongruentnom zatvorenju.

# Kongruentne relacije

## Definicija

Relacija  $\sim$  je *kongruencija* na skupu  $D$  u odnosu na jezik  $\mathcal{L}$  ako je relacija ekvivalencije na domenu  $D$  saglasna (kongruentna) sa svim funkcijskim simbolima jezika  $\mathcal{L}$ , tj. za svako  $f$  važi da ako  $s_1 \sim t_1, \dots, s_n \sim t_n$ , tada  $f(s_1, \dots, s_n) \sim f(t_1, \dots, t_n)$ .

*Kongruentno zatvorenje* relacije je najmanja kongruencija koja sadrži polaznu relaciju.

# Teorema o kongruentnom zatvorenju

## Teorema

*Neka su  $s_i$ ,  $t_i$ ,  $s$  i  $t$  bazni termovi i neka je  $D$  skup svih ovih termova i svih njihovih podtermova. Neka je  $\sim$  kongruentno zatvorenje relacije  $\{(s_1, t_1), \dots, (s_n, t_n)\}$ . Tada*

$$\{s_1 = t_1, \dots, s_n = t_n\} \vDash s = t$$

*akko*

$$\{s_1 = t_1, \dots, s_n = t_n\} \vdash s = t$$

*akko*

$$s \sim t$$

## Teorema o kongruentnom zatvorenju

### Dokaz

*Prva i druga stavka su ekvivalentne na osnovu Birkhofove teoreme. Iz druge stavke sledi treća . . . . Iz treće stavke sledi druga . . . .*

# Nelson-Openov algoritam za određivanje kongruentnog zatvorenja

## Ideja algoritma

- Postupak se zasniva na postepenom proširenju relacije kongruencije počevši od prazne relacije i dodavanjem jedne po jedne jednakosti.
- Kongruencije se predstavljaju klasama ekvivalencije (korišćenjem *union-find* strukture).
- Prilikom spajanja klasa vrši se analiza termova u kojima elementi tih klasa učestvuju i na osnovu kongruentnosti spajaju se odgovarajući termovi. Ukoliko se npr. klase koje sadrže termovi  $s$  i  $t$  spajaju, a postoje npr. termovi  $f(s, g(t))$  i  $f(t, g(s))$ , potrebno je spojiti i klase kojima oni pripadaju.



# Nelson-Openov algoritam za određivanje kongruentnog zatvorenja

## Oznake koje ćemo koristiti:

- Neka je  $E = \{s_1 = t_1, \dots, s_n = t_n\}$  skup baznih jednakosti. Neka je  $T$  skup termova zatvoren za podtermove koji sadrži sve bazne termove  $s_i, t_i$  (i možda još neke druge termove i njihove podtermove).
- Neka  $use(t)$  označava skup svih termova skupa  $T$  čiji je podterm term  $t$ . Ovi skupovi se mogu unapred izračunati.
- Neka  $find(t)$  vraća kanonskog predstavnika klase ekvivalencije kojoj pripada term  $t$ .
- Neka  $union(s, t)$  spaja klasu ekvivalencije terma  $s$  i klasu ekvivalencije terma  $t$ .
- Neka  $cong(s, t)$  označava da je  $s$  oblika  $f(s_1, \dots, s_n)$  i  $t$  oblika  $f(t_1, \dots, t_n)$  pri čemu je  $find(s_i) = find(t_i)$ .

## Nelson-Openov algoritam za određivanje kongruentnog zatvorenja

## Algoritam Nelson-Open

```
function cc( $E, T$ )
begin
  foreach  $t \in T$   $find(t) := t.$ 
  foreach  $s_i = t_i \in E$ 
    if( $find(s_i) \neq find(t_i)$ )
       $merge(s_i, t_i)$ 
end

function merge( $s, t$ )
begin
   $T_s = \bigcup \{use(u) \mid find(u) = find(s)\}$ 
   $T_t = \bigcup \{use(u) \mid find(u) = find(t)\}$ 
  union( $s, t$ )
  foreach  $s' \in T_s, t' \in T_t$ 
    if ( $find(s') \neq find(t') \wedge cong(s', t')$ )
      merge( $s', t'$ )
end
```

## Nelson-Openov algoritam za određivanje kongruentnog zatvorenja — primer

## Primer

Ispitajmo da li važi:  $x = y, y = z \vDash f(x) = f(z)$  (gde su  $x, y, z$  konstante). Potrebno je odrediti kongruentno zatvorenje za skup jednakosti  $E = \{x = y, y = z\}$  nad skupom termova  $T = \{x, y, z, f(x), f(z)\}$  (dakle, svi termovi koji se pojavljuju u  $E$ , kao i u jednakosti  $f(x) = f(z)$  koju dokazujemo).  
 use je određen sa

$$\{x \mapsto \{f(x)\}, y \mapsto \{\}, z \mapsto \{f(z)\}, f(x) \mapsto \{\}, f(z) \mapsto \{\}\}$$

Krećemo od jednočlanih klasa  $\{\{x\}, \{y\}, \{z\}, \{f(x)\}, \{f(z)\}\}$ , tj. find je određen sa:

$$\{x \mapsto x, y \mapsto y, z \mapsto z, f(x) \mapsto f(x), f(z) \mapsto f(z)\}$$

## Primer

- $merge(x, y) - T_x = \{f(x)\}, T_y = \{\}$ . Nakon  $union(x, y)$ , dobijaju se klase  $\{\{x, y\}, \{z\}, \{f(x)\}, \{f(z)\}\}$ , tj.  $find$  je određen sa  $\{x \mapsto x, y \mapsto x, z \mapsto z, f(x) \mapsto f(x), f(z) \mapsto f(z)\}$ . Petlja je prazna.
- $merge(y, z) - T_y = \{f(x)\}, T_z = \{f(z)\}$ . Nakon  $union(y, z)$ , dobijaju se klase  $\{\{x, y, z\}, \{f(x)\}, \{f(z)\}\}$ , tj.  $find$  je određen sa  $\{x \mapsto x, y \mapsto x, z \mapsto x, f(x) \mapsto f(x), f(z) \mapsto f(z)\}$ .  $f(x)$  i  $f(z)$  su kongruentni pa se poziva:
  - $merge(f(x), f(z)) - T_{f(x)} = \{\}, T_{f(z)} = \{\}$ . Nakon  $union(f(x), f(z))$  dobijaju se klase  $\{\{x, y, z\}, \{f(x), f(z)\}\}$ , tj.  $find$  je određen sa  $\{x \mapsto x, y \mapsto x, z \mapsto x, f(x) \mapsto f(x), f(z) \mapsto f(x)\}$ . Petlja je prazna.

## Primer

*Konačna relacija kongruentnog zatvorenja data je skupom klasa  $\{\{x, y, z\}, \{f(x), f(z)\}\}$ . Kako su  $f(x)$  i  $f(z)$  u istoj klasi, to znači da je jednakost  $f(x) = f(z)$  logička posledica skupa jednakosti  $x = y, y = z$ , tj. važi  $x = y, y = z \models f(x) = f(z)$ .*

# Ispitivanje zadovoljivosti bazne EUF formule

## Bazni fragment EUF teorije je odlučiv!

Neka je  $F$  proizvoljna bazna EUF formula (tj. formula bez promenljivih i kvantifikatora u kojoj su svi literali jednakosti i različitosti nad termovima koji sadrže neinterpretirane funkcijske simbole). Njenu zadovoljivost možemo ispitati na sledeći način:

- Formula  $F$  se najpre konvertuje u DNF, a zatim ispitujemo zadovoljivost svake od konjunkcija literala (čim jedna od njih bude zadovoljiva, prekidamo dalji postupak, jer je tada i cela formula zadovoljiva)
- Svaka od konjunkcija je oblika:

$$s_1 = t_1 \wedge \dots \wedge s_n = t_n \wedge s'_1 \neq t'_1 \wedge \dots \wedge s'_{n'} \neq t'_{n'}$$

- Određuje se kongruentno zatvorenje za skup jednakosti  $E = \{s_1 = t_1, \dots, s_n = t_n\}$  i skup termova  $T$  dobijen od  $\{s_1, t_1, \dots, s_n, t_n, s'_1, t'_1, \dots, s'_{n'}, t'_{n'}\}$  i svih njihovih podtermova.
- Konjunkcija je zadovoljiva akko je  $find(s'_i) \neq find(t'_i)$ , za svako  $1 \leq i \leq n'$ .

**NAPOMENA:** Ispitivanje valjanosti se svodi na ispitivanje (ne)zadovoljivosti negacije.

# Odlučivanje univerzalnog fragmenta EUF

## Problem valjanosti univerzalno kvantifikovanih EUF formula

- Razmatrajmo valjanost univerzalno kvantifikovane EUF formule, tj. formula oblika  $\forall x_1 \dots x_n. P(x_1, \dots, x_n)$ , gde je  $P$  EUF formula bez kvantifikatora
- Negacijom i skolemizacijom se dobija bazna formula oblika  $P'(c_1, \dots, c_n)$ .
- Sada se ispitivanje valjanosti polazne univerzalno kvantifikovane EUF formule svodi na ispitivanje zadovoljivosti bazne EUF formule, kao što je malopre opisano

## Napomena

Primetimo da se problem **zadovoljivosti** univerzalno kvantifikovane EUF formule ne može svesti na zadovoljivost bazne formule, jer se u tom slučaju ne mogu ukloniti univerzalni kvantifikatori.

## Odlučivanje univerzalnog fragmenta EUF – primer

## Primer

*Pokažimo da formula*

$$\forall x. f^3(x) = x \wedge f^5(x) = x \Rightarrow f^2(x) = x$$

*važi u svim normalnim modelima, pri čemu je  $f^i(x)$  skraćeni zapis za  $f(f(\dots f(x)))$ , gde se  $f$  primenjuje  $i$  puta. Negiranjem polazne formule i skolemizacijom dobija se formula*

$$f^3(c) = c \wedge f^5(c) = c \wedge f^2(c) \neq c.$$

*Posmatrajmo izvršavanje Nelson-Oppen-ovog algoritma. Skup jednakosti  $E = \{f^3(c) = c, f^5(c) = c\}$ , a skup termova  $T = \{c, f(c), f^2(c), f^3(c), f^4(c), f^5(c)\}$ .*



# Primer

## Primer

- $merge(f^3(c), c) - T_{f^3(c)} = \{f^4(c)\}$ ,  $T_c = \{f(c)\}$ . Nakon izvršetka  $union(f^3(c), c)$  dobijaju se klase  $\{\{c, f^3(c)\}, \{f(c)\}, \{f^2(c)\}, \{f^4(c)\}, \{f^5(c)\}\}$ .  $f^4(c)$  i  $f(c)$  su kongruentni pa se poziva:

- $merge(f^4(c), f(c)) - T_{f^4(c)} = \{f^5(c)\}$ ,  $T_{f(c)} = \{f^2(c)\}$ . Nakon izvršetka  $union(f^4(c), f(c))$  dobijaju se klase  $\{\{c, f^3(c)\}, \{f(c), f^4(c)\}, \{f^2(c)\}, \{f^5(c)\}\}$ .  $f^5(c)$  i  $f^2(c)$  su kongruentni pa se poziva:

- $merge(f^5(c), f^2(c)) - T_{f^5(c)} = \{\}$ ,  $T_{f^2(c)} = \{f^3(c)\}$ . Nakon izvršetka  $union(f^5(c), f^2(c))$  dobijaju se klase  $\{\{c, f^3(c)\}, \{f(c), f^4(c)\}, \{f^2(c), f^5(c)\}\}$ . Petlja je prazna.

# Primer

## Primer

- $merge(f^5(c), c) - T_{f^5(c)} = \{f^3(c)\}, T_c = \{f(c), f^4(c)\}$ .

*Nakon union( $f^5(c), c$ ) dobijaju se klase*

*$\{\{c, f^2(c), f^3(c), f^5(c)\}, \{f(c), f^4(c)\}\}$ .*

*Termovi  $f^3(c)$  i  $f(c)$  su kongruentni pa se poziva*

- $merge(f^3(c), f(c)) - T_{f^3(c)} = \{f(c), f^3(c), f^4(c)\},$   
 $T_{f(c)} = \{f^2(c), f^5(c)\}$ .

*Nakon union( $f^3(c), f(c)$ ) dobijaju se klase*

*$\{\{c, f(c), f^2(c), f^3(c), f^4(c), f^5(c)\}\}$ . Svi termovi su istoj klasi  
 pa nema daljih rekurzivnih poziva.*

*Svi termovi su istoj klasi pa nema daljih rekurzivnih poziva.*

# Odlučivanje univerzalnog fragmenta EUF – primer

## Primer

*Dakle, pošto negirana formula sadrži različitost  $f^2(c) \neq f(c)$ , a na osnovu kongruentnog zatvorenja važi  $f^2(c) = f(c)$ , ona je nezadovoljiva, te polazna formula*

$$\forall x. f^3(x) = x \wedge f^5(x) = x \Rightarrow f^2(x) = x$$

*važi u svim normalnim modelima.*

# Neodlučivost EUF teorije

## Neodlučivost EUF teorije

- Videli smo da su problemi valjanosti i zadovoljivosti odlučivi za bazni fragment EUF teorije
- Takođe, problem valjanosti je odlučiv za univerzalno kvantifikovane EUF formule
- Sa druge strane, problem zadovoljivosti univerzalno kvantifikovanih EUF formula je **neodlučiv**
- Takodje, problemi zadovoljivosti i valjanosti za EUF formule **u opštem obliku** su **neodlučivi**

# Pregled

- 1 Normalni modeli. Aksiome jednakosti
- 2 Metateoreme
- 3 Rezolucija i paramodulacija
- 4 Dedukcija i jednakost
- 5 Jednakosno rezonovanje
- 6 Kongruentno zatvorenje
- 7 Prezapisivanje**

# Zamenski dokazi još jednom

## Zamenski dokazi – podsetnik

- Dokazi tvrdjenja  $E \vdash s = t$  se (neformalno) obično sprovode tako što se se započne od terma  $s$ , a onda se na njega (odnosno njegove podtermove) primenjuju transformacije na osnovu datih jednakosti  $s_i = t_i \in E$ , vršeći pri tom pogodne instancijacije.
- Ukoliko se takvim transformacijama polazeći od  $s$  može dobiti term  $t$ , tada zaključujemo da je  $s = t$  posledica jednakosti iz  $E$
- Ovakve dokaze nazivali smo **zamenskim dokazima**
- Problem zamenskih dokaza je to što ih je teško automatski konstruisati, zbog toga što je teško kontrolisati primenu zamena u termovima i usmeravati je ka pravom cilju

# Prezapisivanje

## Od zamenskih dokaza do prezapisivanja

- U praksi, kada „na papiru” primenjujemo zamenske dokaze, obično date „zakone” iz  $E$  primenjujemo na usmeren način, u cilju uprošćavanja polaznog terma
- Na primer, term  $x \cdot x^{-1}$  se zamenjuje sa  $1$  — zamena u suprotnom smeru je obično neintuitivna, jer ne vodi ka uprošćavanju terma
- Otuda zakon  $x \cdot x^{-1} = 1$  posmatramo kao „usmerenu jednakost”  $x \cdot x^{-1} \rightarrow 1$ , tj. kao pravilo po kome se vrši uprošćavanje
- Sada se tvrdjenje  $E \vdash s = t$  dokazuje tako što se  $s$  i  $t$  uprošćavaju koristeći usmerene jednakosti iz  $E$ , sa ciljem da se svedu na isti term
- Korišćenje transformacija termova na osnovu usmerenih jednakosti naziva se **prezapisivanje**. Usmerene jednakosti nazivamo **pravila prezapisivanja**.

# Usmeravanje jednakosti

## Ali kako da usmerimo jednakosti?

- Postavlja se pitanje na koji način jednakosti  $s_i = t_i \in E$  usmeriti i pretvoriti u pravila prezapisivanja?
- Za svaku jednakost  $s_i = t_i$  imamo dve mogućnosti:  $s_i \rightarrow t_i$  ili  $t_i \rightarrow s_i$
- Jednakosti treba usmeriti tako da u nekom smislu desna strana bude jednostavnija od leve, kako bi se prezapisivanjem dobijali jednostavniji termovi
- Medjutim, pojam jednostavnijeg terma je suptilan. Na primer,  $(x + y) \cdot (w + z)$  je kraći od  $xw + xz + yw + yz$  ali se drugi smatra jednostavnijim jer omogućava dalja skraćivanja
- Otuda problem usmeravanja jednakosti nije ni malo trivijalan



## Definicija

*Pravilo prezapisivanja termova je usmerena jednakost oblika  $l \rightarrow r$  gde su  $l$  i  $r$  termovi takvi da  $l$  nije promenljiva i  $r$  ne uvodi nove slobodne promenljive u odnosu na  $l$  (skup slobodnih promenljivih terma  $r$  je podskup skupa slobodnih promenljivih terma  $l$ ).*

## Definicija

*Ako je  $l \rightarrow r$  pravilo prezapisivanja termova kažemo da se term  $t$  na osnovu ovog pravila prezapisuje u term  $t'$  ako postoji podterm terma  $t$  koji je instanca terma  $l$ , takav da se njegovom zamenom instancom terma  $r$  (pri istoj instancijaciji) dobija term  $t'$ .*

## Definicija

*Sistem prezapisivanja  $R$  termova je skup pravila prezapisivanja termova. Kažemo da  $t \rightarrow_R t'$  ako postoji neko pravilo  $l \rightarrow r \in R$  kojim se  $t$  prezapisuje u  $t'$ . Relacija  $\rightarrow_R$  je relacija prezapisivanja termova.*

# Primer primene prezapisivanja

## Primer

*Prezapisivanjem terma  $(a + a) + (b + b)$  na osnovu pravila  $x + x \rightarrow 2x$  mogu se dobiti  $2a + (b + b)$  i  $(a + a) + 2b$ . Term  $2a + 2b$  se može dobiti nakon dva koraka.*

# Prezapisivanje i Birkhofov sistem

## Teorijski osnov prezapisivanja

- Prezapisivanje ima svoje teoretsko opravdanje (zasnovano na Birkhofovom sistemu).
- Svaki lanac prezapisivanja se može konvertovati u formalni dokaz u Birkhofovom sistemu.
- Važi i obratno.

## Teorema

*Ako je  $\rightarrow_R$  relacija dobijena na osnovu sistema prezapisivanja  $R$ , a  $\leftrightarrow_R^*$  njeno simetrično, refleksivno i tranzitivno zatvorenje, tada za svaka dva terma  $s$  i  $t$  važi  $s \leftrightarrow_R^* t$  ako i samo ako  $R \vdash s = t$ .*

# Kanonski sistemi

## Kanonski sistemi prezapisivanja

- U slučaju jednakosnog rezonovanja na osnovu datih jednakosti  $E$ , reći ćemo da su  $s$  i  $t$  ekvivalentni u odnosu na  $E$ , ako  $E \vdash s = t$
- Da bi sistem za prezapisivanje bio efektivno upotrebljiv za automatizaciju dokazivanja ekvivalentnosti dva terma, poželjno je da ima dva veoma bitna svojstva:
  - svaki lanac prezapisivanja se mora završiti nakon konačno mnogo koraka, tj. mora se stići do terma na koji nije moguće dalje primeniti ni jedno pravilo — za ovakve termine kažemo da su u **normalnoj formi**
  - svaki term ima jedinstvenu normalnu formu
- Ova dva svojstva redom nazivamo **zaustavljanje** i **konfluentnost**
- Sistemi koji imaju ova dva svojstva se nazivaju **kanonski** ili **konvergentni**.
- Ovakvi sistemi se mogu koristiti kao procedure odlučivanja ekvivalentnosti dva terma  $s$  i  $t$  u odnosu na dati sistem jednakosti (proveri se da li se nakon „normalizacije” termina  $s$  i  $t$  dobija ista normalna forma).

# Primer kanonskog sistema

## Primer

$$\{m+0 = m, 0+n = n, m+S(n) = S(m+n), S(m)+n = S(m+n)\}$$

*Utvrdjivanje jednakosti dva terma na osnovu ovog sistema ne zahteva nikakvu kreativnost. Npr.*

$$S(0) + S(S(0)) \rightarrow S(0 + S(S(0))) \rightarrow S(S(S(0)))$$

*Takođe,*

$$S(0) + S(S(0)) \rightarrow S(S(0) + S(0)) \rightarrow S(S(S(0) + 0)) \rightarrow \\ S(S(S(0 + 0))) \rightarrow S(S(S(0)))$$

*Naravno, efikasnost zavisi od redosleda primene pravila, međutim, normalna forma do koje će se stići ne zavisi.*

# Primeri ne-kanonskih sistema — nezaustavljanje

## Primer

*Neka je dato pravilo  $x + y \rightarrow y + x$ . Term  $1 + 2$  nema normalnu formu. Zaista, postoji izvođenje:*

$$1 + 2 \rightarrow 2 + 1 \rightarrow 1 + 2 \rightarrow 2 + 1 \rightarrow \dots$$

*Ovaj sistem očigledno nema svojstvo **zaustavljanja**.*

# Primeri ne-kanonskih sistema — nekonfluentnost

## Primer

$$\{x + 0 \rightarrow x, s(x + y) \rightarrow x + s(y)\}$$

*Term  $s(x + 0)$  se primenom prvog pravila može prezapisati u  $s(x)$ , a primenom drugog pravila u  $x + s(0)$ . Nijedan od ova dva terma nije moguće dalje prezapisivati.*

*Dobijene normalne forme nisu jednake, pa ovaj sistem nema svojstvo konfluentnosti.*

# Primeri ne-kanonskih sistema — nekonfluentnost

## Primer

$$\{x \cdot (y + z) \rightarrow x \cdot y + x \cdot z, (x + y) \cdot z \rightarrow x \cdot z + y \cdot z\}$$

$$\begin{aligned} (a + b) \cdot (c + d) &\rightarrow a \cdot (c + d) + b \cdot (c + d) \\ &\rightarrow (a \cdot c + a \cdot d) + b \cdot (c + d) \\ &\rightarrow (a \cdot c + a \cdot d) + (b \cdot c + b \cdot d) \end{aligned}$$

$$\begin{aligned} (a + b) \cdot (c + d) &\rightarrow (a + b) \cdot c + (a + b) \cdot d \\ &\rightarrow (a \cdot c + b \cdot c) + (a + b) \cdot d \\ &\rightarrow (a \cdot c + b \cdot c) + (a \cdot d + b \cdot d) \end{aligned}$$



# Apstraktni sistemi za prezapisivanje

## Apstraktni sistemi za prezapisivanje

- Najznačajni sistemi za prezapisivanje su sistemi za prezapisivanje termova.
- Ipak, ponekad se posmatraju opštiji sistemi, tzv. **apstraktni sistemi za prezapisivanje**.
- Relacija prezapisivanja  $R$  se posmatra na proizvoljnom skupu  $X$  (ne obavezno skupu termova) i obično se zapisuje infiksno  $x \rightarrow y$ . Ova relacija je apstraktno data i ne definiše se na osnovu skupa jednakosti termova.
- Oznaka  $\rightarrow^+$  označava tranzitivno zatvorenje relacije  $\rightarrow$ , oznaka  $\rightarrow^*$  njeno refleksivno i tranzitivno zatvorenje, dok oznaka  $\leftrightarrow^*$  označava njeno simetrično, refleksivno i tranzitivno zatvorenje.

# Zaustavljanje

## Definicija

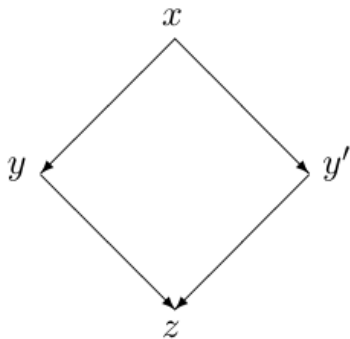
*Relacija  $\rightarrow$  je zaustavljajuća (dobro zasnovana) ako ne postoji beskonačan lanac  $t_1 \rightarrow t_2 \rightarrow t_3 \rightarrow \dots$*

# Oblici konfluentnosti

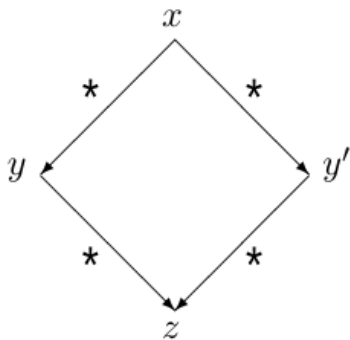
## Definicija

- Relacija  $\rightarrow$  ima *svojstvo dijamanta* ako kada  $x \rightarrow y$  i  $x \rightarrow y'$  tada postoji  $z$  tako da  $y \rightarrow z$  i  $y' \rightarrow z$ .
- $x$  i  $y$  su *spojivi* što označavamo sa  $x \downarrow y$  ako postoji  $z$  tako da  $x \rightarrow^* z$  i  $y \rightarrow^* z$ .
- Relacija je *konfluentna* ako kada  $x \rightarrow^* y$  i  $x \rightarrow^* y'$  tada  $y \downarrow y'$ . Ekvivalentno,  $\rightarrow^*$  ima svojstvo dijamanta.
- Relacija je *slabo konfluentna* ako kada  $x \rightarrow y$  i  $x \rightarrow y'$  tada  $y \downarrow y'$ .
- Relacija ima *Čerč-Roserovo* svojstvo ako kada god  $x \leftrightarrow^* y$ , tada je  $x \downarrow y$ .

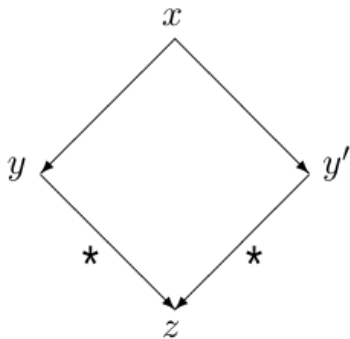
# Svojstvo dijamanta



# Konfluentnost



# Slaba konfluentnost



# Relacija $\leftrightarrow^*$



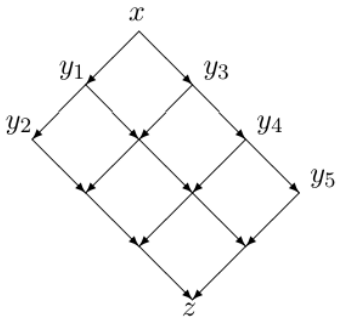
# Oblici konfluentnosti

## Stav

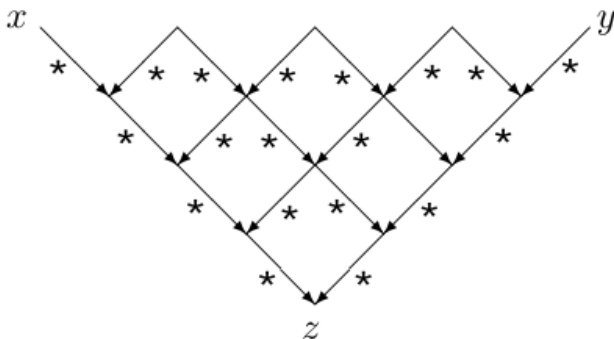
- *Ako je relacija konfluentna ona je slabo konfluentna.*
- *Ako relacija ima svojstvo dijamanta ona je konfluentna.*
- *Ako relacija ima svojstvo dijamanta ona je slabo konfluentna.*
- *Relacija ima Čerč Roserovo svojstvo akko je konfluentna.*



# Svojstvo dijamanta povlači konfluentnost



# Ekvivalentnost Čerč-Roserovog svojstva i konfluentnosti



# Utvrđivanje konfluentnosti

## Primedba

- U praksi je obično znatno lakše utvrditi slabu konfluentnost relacije od konfluentnosti
- Na žalost, slabo konfluentna relacija ne mora biti konfluentna.

## Primer

*Relacija  $b \rightarrow a, b \rightarrow c, c \rightarrow b, c \rightarrow d$  je slabo konfluentna, ali nije konfluentna.*

- Ipak, važi naredna teorema.

## Teorema (Njuman)

*Ako je relacija  $\rightarrow$  zaustavljajuća i slabo konfluentna, ona je i konfluentna.*

- Ove teorema se u praksi koristi za lakše dokazivanje konfluentnosti:
  - Dokaže se slaba konfluentnost (što je lakše)
  - Dokaže se zaustavljanje (koje i onako moramo dokazati da bismo imali efektivno primenljiv sistem prezapisivanja)

# Jedinstvenost normalne forme i konfluentnost

## Definicija

Element  $x \in X$  nazivamo *normalnom formom* u odnosu na relaciju  $\rightarrow$  ako ne postoji  $y \in X$  takvo da je  $x \rightarrow y$ .

Ako je  $x \rightarrow^* y$ , gde je  $y$  normalna forma, tada kažemo da je  $y$  *normalna forma elementa*  $x$ .

## Teorema

Ako je relacija  $\rightarrow$  konfluentna tada svaki element ima najviše jednu normalnu formu.

## Dokaz

Pretpostavimo suprotno: da postoje dve različite normalne forme  $y_1$  i  $y_2$  elementa  $x \in X$ . Kako je  $x \rightarrow^* y_1$  i  $x \rightarrow^* y_2$ , tada bi, zbog konfluentnosti, moralo da važi  $y_1 \downarrow y_2$ , što ne važi jer su ova dva elementa normalne forme. Kontradikcija.

## Posledica

Ako je relacija  $\rightarrow$  konfluentna i zaustavljajuća, tada svaki element  $x \in X$  ima jedinstvenu normalnu formu.

# Spojivost i normalna forma

## Teorema

*Ako je relacija  $\rightarrow$  konfluentna, tada ako za neka dva elementa važi  $x \downarrow y$ , tada ova dva elementa ili oba nemaju normalne forme, ili su im (jedinствене) normalne forme jednake.*

## Dokaz

*Iz  $x \downarrow y$  sledi da postoji neki element  $z$  takav da  $x \rightarrow^* z$  i  $y \rightarrow^* z$ . Ako, npr.  $x$  ima normalnu formu  $x'$ , tada važi  $x \rightarrow^* x'$ , pa zbog konfluentnosti važi  $x' \downarrow z$ . Medjutim, kako je  $x'$  normalna forma, to znači da je  $z \rightarrow^* x'$ . Otuda je i  $y \rightarrow^* x'$ , pa je  $x'$  normalna forma i za  $y$ .*

# Normalne forme i relacija $\leftrightarrow^*$

## Teorema

*Neka je relacija  $\rightarrow$  konfluentna i zaustavljajuća na skupu  $X$ . Tada za svaka dva elementa  $x$  i  $y$  važi  $x \leftrightarrow^* y$  akko  $x$  i  $y$  imaju jednake normalne forme.*

## Dokaz

*Iz konfluentnosti i zaustavljanja sledi da  $x$  i  $y$  imaju jedinstvene normalne forme. Iz konfluentnosti takođe sledi Čerč-Rozeroovo svojstvo, tj.  $x \leftrightarrow^* y$  akko  $x \downarrow y$ . Iz prethodne teoreme sledi da ovo važi akko su normalne forme od  $x$  i  $y$  jednake.*

# Ponovo o prezapisivanju termova

## Teorema

*Neka je dat skup jednakosti  $E$  i neka je orijentacijom ovih jednakosti dobijen sistem prezapisivanja termova  $R$ . Ako je relacija  $\rightarrow_R$  konfluentna i zaustavljajuća, tada za baznu jednakost  $s = t$  važi  $E \models s = t$  akko termovi  $s$  i  $t$  imaju jednake normalne forme u odnosu na relaciju  $\rightarrow_R$ .*

## Dokaz

*Teorema je direktna posledica prethodne teoreme za apstraktne sisteme prezapisivanja.*

## Primedba

Iz ove teoreme sledi da je samo potrebno „pametno“ orijentisati jednakosti iz  $E$  tako da dobijeni sistem prezapisivanja bude konfluentan i zaustavljajući:

- u tom slučaju bismo samo prezapisali  $s$  i  $t$  do svojih normalnih formi (što možemo u konačnom broju koraka), a zatim ispitali da li su te dve normalne forme iste
- otuda bi problem  $E \models s = t$  bio odlučiv

Ipak, ispostavlja se da nije lako utvrditi da li je moguće jednakosti iz  $E$  orijentisati na željeni način.

# Ispitivanje zaustavljanja

## Problem zaustavljanja

- Jedan od fundamentalnih problema je kako za dati sistem prezapisivanja termova utvrditi da li je zaustavljajući.
- Problem ispitivanja zaustavljanja je **neodlučiv!**
- Osnovni metod je pronalaženje dobro zasnovanog uređenja  $\succ$  takvog da iz  $t \rightarrow_R t'$  sledi da  $t \succ t'$ .
- Još je bolje posmatrati dobro-zasnovano  $\succ$  uređenje takvo da za svako pravilo  $l \rightarrow r$  važi  $l \succ r$ . Međutim, da bi se iz ovoga moglo garantovati zaustavljanje potrebno je da uređenje  $\succ$  ima i dodatna svojstva data u sledećoj definiciji.



# Uređenje svođenja

## Definicija

Relacija  $\succ$  je *uređenje prezapisivanja* ako je tranzitivno, irefleksivno i zatvoreno u odnosu na instancijacije i kongruencije, tj.

- *irefleksivno* – Ni za jedan term  $t$  ne važi  $t \succ t$ ,
- *tranzitivno* – Ako je  $s \succ t$  i  $t \succ u$ , tada  $s \succ u$ .
- *stabilno* – Ako je  $s \succ t$  tada je  $s[x \rightarrow t'] \succ t[x \rightarrow t']$ .
- *monotono* – Ako je  $s \succ t$ , tada
 
$$f(u_1, \dots, u_{i-1}, s, u_{i+1}, \dots, u_n) \succ$$

$$f(u_1, \dots, u_{i-1}, t, u_{i+1}, \dots, u_n).$$

Dobro zasnovana uređenja prezapisivanja nazivaju se *uređenja svođenja*.

# Uređenja svođenja

## Lema (Manna, Ness)

*Ako je  $\succ$  uređenje svođenja i za svako  $l \rightarrow r \in R$  važi  $l \succ r$ , tada je  $\rightarrow_R$  zaustavljajuća.*

## Dokaz

*Dovoljno je dokazati da iz  $s \rightarrow_R t$  sledi  $s \succ t$  — pošto je  $\succ$  dobro zasnovano tvrđenje sledi. Iz  $s \rightarrow_R t$  sledi da postoji  $l \rightarrow r \in R$  i instanca  $\bar{l}$  terma  $l$  koja je podterm terma  $s$ , takva da kada se on zameni odgovarajućom instancom  $\bar{r}$  terma  $r$  dobija se term  $t$ . Pošto je  $l \succ r$ , na osnovu svojstva stabilnosti važi da je  $\bar{l} \succ \bar{r}$ . Na osnovu uzastopne primene svojstva monotonosti dobija se i da je  $s \succ t$ .*

# Uređenja pojednostavljivanja

## Definicija

*Relacija  $\succ$  je uređenje pojednostavljivanja ako je irefleksivno, tranzitivno, stabilno, monotono i ima sledeće svojstvo podtermova:*

- *svojstvo podtermova* –  $f(\dots, t_i, \dots) \succ t_i$ .

## Primedba

Uređenje pojednostavljivanja je specijalni tip uređenja prezapisivanja.

## Stav (Deršovic)

*Svako uređenje pojednostavljivanja je dobro uređenje te je i uređenje svođenja.*

## Napomena

Iz prethodnog stava sledi da je u praksi dovoljno naša pravila prezapisivanja „utopiti” u neki poredak pojednostavljivanja. Jedan takav pristup prikazujemo u nastavku.

## Definicija

Neka je data signatura  $\mathcal{L}$ , i neka je  $\succ$  (strogo i potpuno) uređenje skupa funkcijskih simbola  $\Sigma$ . Uređenje leksikografske staze (lexicographic path ordering (LPO))  $\succ_{lpo}$  se definiše rekurzivno sledećim skupom pravila:

$$1 \quad \frac{v \in \text{Vars}(t) \quad t \neq v}{t \succ_{lpo} v}$$

$$2 \quad \frac{}{t \succeq_{lpo} t} \quad , \quad \frac{s \succ_{lpo} t}{s \succeq_{lpo} t}$$

$$3 \quad \frac{\exists i. s_i \succeq_{lpo} t}{f(s_1, \dots, s_m) \succ_{lpo} t}$$

$$4 \quad \frac{f \succ g, \quad \forall i. f(s_1, \dots, s_m) \succ_{lpo} t_i}{f(s_1, \dots, s_m) \succ_{lpo} g(t_1, \dots, t_n)}$$

$$5 \quad \frac{\forall i. f(s_1, \dots, s_m) \succ_{lpo} t_i, \quad (s_1, \dots, s_m) \succ_{lpo}^{lex} (t_1, \dots, t_n)}{f(s_1, \dots, s_m) \succ_{lpo} f(t_1, \dots, t_n)}$$

**NAPOMENA:** Oznaka  $s \succeq_{lpo} t$  znači  $s \succ_{lpo} t \vee s = t$ , a  $\succ_{lpo}^{lex}$  označava leksikografsko poređenje torki.

# Uređenje leksikografske staze

## Primer

Da bismo razjasnili neophodnost dodatnog uslova  $\forall i. f(s_1, \dots, s_m) \succ_{lpo} t_i$  u pravilima 4 i 5, posmatrajmo sledeći primer: pretpostavimo da imamo poredak  $g \succ f \succ h$  među funkcijskim simbolima, gde su  $f$  i  $g$  arnosti 1, a  $h$  arnosti 2. Ako ne bismo imali ovaj dodatni uslov u pravilu 4, tada bismo ovim pravilom mogli da zaključimo da je  $g(x) \succ_{lpo} f(g(x))$  (jer je  $g \succ f$  pa bi bez dodatnog uslova to bilo dovoljno). Dalje bismo mogli da zaključimo da je  $f(g(x)) \succ_{lpo} g(x)$  na osnovu pravila 3. Kako imamo  $g(x) \succ_{lpo} f(g(x)) \succ_{lpo} g(x)$ , sledi da relacija  $\succ_{lpo}$  ne može biti istovremeno i tranzitivna i irefleksivna, kao što bi trebalo da bude.

Slično, ako ne bismo imali dodatni uslov u pravilu 5, tada bismo mogli da izvedemo  $h(g(x), x) \succ_{lpo} h(x, h(g(x), x))$ , jer je  $g(x) \succ_{lpo} x$ , pa bi bez dodatnog uslova to bilo dovoljno. Međutim, na osnovu pravila 3 važi  $h(x, h(g(x), x)) \succ_{lpo} h(g(x), x)$ , pa imamo  $h(g(x), x) \succ_{lpo} h(x, h(g(x), x)) \succ_{lpo} h(g(x), x)$ , odakle imamo isti zaključak kao i malopre.

# Uređenje leksikografske staze

## Stav

*Svako uređenje leksikografske staze je uređenje pojednostavljivanja, pa samim tim i uređenje svođenja.*

# Uređenje leksikografske staze – primeri

## Primer

*Korišćenjem uređenja leksikografske staze pokažimo da je zaustavljajući sistem*

$$\begin{aligned}x + 0 &\rightarrow x \\ -0 &\rightarrow 0 \\ -(x + y) &\rightarrow (-x) + (-y)\end{aligned}$$

*Neka je uređenje simbola  $- \succ + \succ 0$ .*

## Primer

*Tada je:*

- $x + 0 \succ_{lpo} x$  na osnovu pravila 1. jer je  $x \in \text{Vars}(x + 0)$
- $-0 \succ_{lpo} 0$  na osnovu 3. jer je na osnovu 2.  $0 \succeq_{lpo} 0$
- $-(x + y) \succ_{lpo} (-x) + (-y)$  na osnovu pravila 4. jer je  $- \succ +$  i pošto je, kao prvo,  $-(x + y) \succeq_{lpo} -x$  i pošto je, kao drugo,  $-(x + y) \succeq_{lpo} -y$ . Prvo zaista važi na osnovu pravila 5. ukoliko je  $x + y \succ_{lpo}^{lex} x$  a ovo je ispunjeno jer je  $x + y \succ_{lpo} x$  na osnovu pravila 1. Na isti način se pokazuje i drugi uslov.



# Uređenje leksikografske staze – primeri

## Primer

### *Zaustavljanje pravila*

$$(x \cdot y) \cdot z \rightarrow x \cdot (y \cdot z)$$

*se može pokazati uređenjem leksikografske staze. Zaista na osnovu pravila 5. treba pokazati da je  $(x \cdot y, z) \succ_{lpo}^{lex} (x, y \cdot z)$  što je ispunjeno jer je  $x \cdot y \succ_{lpo} x$  na osnovu pravila 1.*

*Dodatno, treba pokazati i da je term  $(x \cdot y) \cdot z$  veći ili jednak od neposrednih podtermova terma  $x \cdot (y \cdot z)$ , a to su  $x$  i  $y \cdot z$ . Prvo je trivijalno na osnovu pravila 1, a drugo se dokazuje slično primenom pravila 5.*

# Zaustavljanje - zaključci

## Zaključci

- LPO uređenje je jednoznačno određeno zadatim poretkom  $\succ$  funkcijskih simbola iz signature  $\mathcal{L}$
- Za fiksiranu signaturu sa konačnim brojem funkcijskih simbola imamo konačno mnogo LPO uređenja
- Ipak, ne mogu se sva uređenja svođenja dobiti na ovakav način, niti je svaka zaustavljajuća relacija prezapisivanja podskup nekog uređenja svođenja
- Otuda, čak i ako pravila prezapisivanja nisu „usmerena” u skladu sa nekim od LPO uređenja datog jezika, to i dalje ne znači da sistem prezapisivanja termova nije zaustavljajući
- Ovo je u skladu sa ranije navedenom činjenicom o neodlučivosti pitanja zaustavljanja

# Ispitivanje konfluentnosti

Pitanje konfluentnosti je takođe neodlučivo!

- Problem ispitivanja konfluentnosti datog sistema prezapisivanja termina je u opštem slučaju **neodlučiv**.
- Ipak, postoje specijalni slučajevi koji su odlučivi:

## Stav

- *Pitanje konfluentnosti baznih sistema za prezapisivanje je odlučivo.*
- *Pitanje konfluentnosti zaustavljajućih sistema za prezapisivanje je odlučivo.*
- Naglasimo da zaustavljanje nije neophodno za konfluentnost:

## Primer

*Sistem  $R = \{a \rightarrow b, b \rightarrow a, a \rightarrow c\}$  je konfluentan, ali nije zaustavljajući.*

# Kritični parovi

## Definicija (Kritični par)

*Neka su  $l_1 \rightarrow r_1$  i  $l_2 \rightarrow r_2$  dva pravila koja nemaju zajedničkih promenljivih (ovo se može uvek postići preimenovanjem). Neka je  $l'_1$  podterm terma  $l_1$  koji nije promenljiva i neka je  $\theta$  najopštiji unifikator termova  $l'_1$  i  $l_2$ . Tada za ova dva pravila prezapisivanja definišemo **kritični par**  $\langle r_1\theta, (l_1[l'_1 \rightarrow r_2])\theta \rangle$ .*

## Primer

*Neka je  $l_1 \rightarrow r_1 \equiv s(x + y) \rightarrow x + s(y)$ , a  $l_2 \rightarrow r_2 \equiv x + 0 \rightarrow x$ . Podterm  $l'_1 \equiv x + y$  se može unifikovati sa  $x + 0$  unifikatorom  $\theta = \{y \mapsto 0\}$ . Otuda imamo kritični par  $\langle x + s(0), s(x) \rangle$ .*

# Knut-Bendiksova teorema

## Teorema

*Sistem za prezapisivanje je lokalno konflentan ako i samo ako su mu svi kritični parovi spojivi tj. ako važi  $u_1 \downarrow u_2$ , za svaki kritični par  $\langle u_1, u_2 \rangle$*

## Napomena

Iz ove teoreme sledi da se ispitivanje lokalne konfluentnosti može svesti na ispitivanje spojivosti kritičnih parova (kojih ima konačno mnogo za dati (konačni) skup pravila prezapisivanja).

# Provera kritičnih parova i ispitivanje konfluentnosti

## Ideja postupka odlučivanja za zaustavljajuće sisteme prezapisivanja

- Da bi se otkrili svi kritični parovi datog sistema za prezapisivanje, svako pravilo se kombinuje sa svakim drugim (uključujući i svoju preimenovanu verziju).
- Pošto u slučaju konačnog sistema za prezapisivanje termova kritičnih parova ima konačno mnogo, da bismo utvrdili da li je sistem lokalno konfluentan, dovoljno je ispitati spojivost konačno mnogo parova termova.
- U slučaju zaustavljajućeg sistema, spojivost kritičnih parova se efektivno može ispitati (dovoljno je termine prezapisati do (nekih) svojih normalnih formi i utvrditi da li su one iste)
- Takodje, usled zaustavljanja, po Njumanovoj lemi važi da je sistem lokalno konfluentan akko je konfluentan.
- Ovo nam daje proceduru odlučivanja za pitanje konfluentnosti konačnih, zaustavljajućih sistema za prezapisivanje termova.

# Knut-Bendiksova procedura upotpunjavanja

## Upotpunjavanje do konfluentnosti

- Iako se ispitivanjem kritičnih parova ponekad ustanovi da određeni sistem za prezapisivanje termova  $R$  nije konfluentan, u nekim slučajevima se, dodavanjem određenih pravila, sistem može učiniti konfluentnim.
- Neka je  $\langle u_1, u_2 \rangle$  kritični par za koji postoje različite normalne forme  $\bar{u}_1$  i  $\bar{u}_2$  termova  $u_1$  i  $u_2$ .
- Jednakost  $\bar{u}_1 = \bar{u}_2$  je posledica sistema  $R$  jer je  $\bar{u}_1 \xleftrightarrow{*}_R \bar{u}_2$  i zbog toga dodavanje pravila  $\bar{u}_1 \rightarrow \bar{u}_2$  ili  $\bar{u}_2 \rightarrow \bar{u}_1$  ne menja odgovarajuću jednakosnu teoriju.
- U ovom proširenom sistemu, par  $\langle u_1, u_2 \rangle$  postaje spojiv.
- Da bi sistem ostao zaustavljajući, potrebno je da je  $\bar{u}_1 \succ \bar{u}_2$  ili  $\bar{u}_2 \succ \bar{u}_1$  u odgovarajućem uređenju svođenja  $\succ$ .

# Knut-Bendiksova procedura upotpunjavanja

## Algoritam

**Ulaz:** skup jednakosti  $E$  i relacija svođenja  $>$

**Izlaz:** konfluentan skup pravila prezapisivanja  $R$  ili *fail*

```
if (  $\exists (s = t) \in E. s \neq t \wedge s \not\approx t \wedge t \not\approx s$  )
  return fail;
```

```
 $R_0 = \{l \rightarrow r \mid (l = r) \in E \cup E^{-1} \wedge l > r\}$ 
```

```
do
```

```
   $R_{i+1} = R_i$ 
```

```
  forall (  $\langle u_1, u_2 \rangle \in CP(R_i)$  )
```

```
     $\bar{u}_1 = u_1 \downarrow; \bar{u}_2 = u_2 \downarrow;$ 
```

```
    if (  $\bar{u}_1 \neq \bar{u}_2 \wedge \bar{u}_1 \not\approx \bar{u}_2 \wedge \bar{u}_2 \not\approx \bar{u}_1$  )
```

```
      return fail;
```

```
    if (  $\bar{u}_1 > \bar{u}_2$  )
```

```
       $R_{i+1} = R_{i+1} \cup \{\bar{u}_1 \rightarrow \bar{u}_2\}$ 
```

```
    else if (  $\bar{u}_2 > \bar{u}_1$  )
```

```
       $R_{i+1} = R_{i+1} \cup \{\bar{u}_2 \rightarrow \bar{u}_1\}$ 
```

```
  i := i+1;
```

```
while (  $R_i \neq R_{i-1}$  );
```

```
return  $R_i$ ;
```



# Konfluentnost – zaključci

## Zaključci o Knut-Bendiksovoj proceduri i konfluentnosti

- Knut-Bendiksova procedura može da nam kao rezultat vrati dopunjeni konfluentan sistem prezapisivanja ekvivalentan sa polaznim (u smislu dobijene jednakosne teorije)
- Alternativno, Knut-Bendiksova procedura može reći da takav sistem ne postoji (pod pretpostavkom fiksiranog uređenja svođenja)
- Najzad, Knut-Bendiksova procedura može da se nikada ne zaustavi
- Otuda, mi ne možemo Knut-Bendiksovu proceduru koristiti kao proceduru odlučivanja za pitanje „da li se dati zaustavljajući sistem prezapisivanja može dopuniti do konfluentnog?“
- I ovo pitanje je u opštem slučaju **neodlučivo**