UNIVERZITET U NOVOM SADU
PRIRODNO–MATEMATIČKI FAKULTET
INSTITUT ZA MATEMATIKU

Igor Dolinka

O identitetima algebri regularnih jezika

– doktorska disertacija –

Novi Sad, 2000.

I like words much better than numbers;
and I always did.

(Volim reči, mnogo više nego brojeve;
i oduvek sam ih voleo.)

P. R. Halmos

U početku bješe riječ...

Jovan I, 1

AZBUKA = skup simbola (**slova**)

REČ = niz slova

PRAZNA REČ = prazan niz, λ

Σ^* = skup svih reči nad Σ

JEZIK = skup reči nad datom azbukom Σ,
tj. $\subseteq \Sigma^*$

$$\Sigma = \{a, b\}$$

$$\Sigma = \{a, b\}$$

a

$$\Sigma = \{a, b\}$$

ab

$$\Sigma = \{a, b\}$$

abb

$$\Sigma = \{a, b\}$$

$abba$

$$\Sigma = \{a, b\}$$

$$abbaa$$

$$\Sigma = \{a, b\}$$

$$abbaaa$$

$$\Sigma = \{a, b\}$$

$$abbaaab$$

$$\Sigma = \{a, b\}$$

$$abbaaaba$$

$$\Sigma = \{a, b\}$$

$$abbaaabaa$$

$$\Sigma = \{a, b\}$$

$$abbaaabaab$$

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, đ, d\check{z}, e, f, g, \ldots\}$$

$$\Sigma = \{a, b, c, č, ć, d, đ, dž, e, f, g, \ldots\}$$

m

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, đ, d\check{z}, e, f, g, \ldots\}$$

$$ma$$

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, đ, d\check{z}, e, f, g, \ldots\}$$

$$mat$$

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, đ, d\check{z}, e, f, g, \ldots\}$$

$$mate$$

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, đ, d\check{z}, e, f, g, \ldots\}$$

$$matem$$

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, đ, d\check{z}, e, f, g, \ldots\}$$

$$matema$$

$$\Sigma = \{a, b, c, č, ć, d, đ, dž, e, f, g, \ldots\}$$

$$matemat$$

$$\Sigma = \{a, b, c, \check{c}, \acute{c}, d, \text{đ}, d\check{z}, e, f, g, \ldots\}$$

$$matemati$$

$$\Sigma = \{a,b,c,\check{c},\acute{c},d,đ,d\check{z},e,f,g,\ldots\}$$

$$matematik$$

$$\Sigma = \{a, b, c, č, ć, d, đ, dž, e, f, g, \ldots\}$$

$$matematika$$

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

`Read`

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

`Read(`

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

`Read(x)`

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

```
Read(x);
Read(y
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y)
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

```
Read(x);
Read(y);
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z:=
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

```
Read(x);
Read(y);
z:=x
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

```
Read(x);
Read(y);
z:=x+
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z:=x+y
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z:=x+y;
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z:=x+y;
Write
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z:=x+y;
Write(
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

```
Read(x);
Read(y);
z:=x+y;
Write(z
```

$$\Sigma = \{\texttt{:=},\texttt{Read},\texttt{Write},\texttt{x},\texttt{y},\texttt{z},\texttt{(},\texttt{)},\texttt{;},\ldots\}$$

```
Read(x);
Read(y);
z:=x+y;
Write(z)
```

$$\Sigma = \{\texttt{:=}, \texttt{Read}, \texttt{Write}, \texttt{x}, \texttt{y}, \texttt{z}, \texttt{(}, \texttt{)}, \texttt{;}, \ldots\}$$

```
Read(x);
Read(y);
z:=x+y;
Write(z);
```

Operacije sa jezicima

- Unija

  $$L_1 + L_2 = L_1 \cup L_2,$$

- Konkatenacija (dopisivanje)

  $$L_1 \cdot L_2 = \{w_1 w_2 : \ w_1 \in L_1, \ w_2 \in L_2\},$$

- Kleenejeva zvezda

  $$L^* = \{\lambda\} + L + L^2 + L^3 + \ldots + L^n + \ldots$$

Osnovni postupci struktuiranog programiranja (N. Wirth):

- selekcija

  `if` p `then` A `else` B

- sekvenca (nizanje komandi)

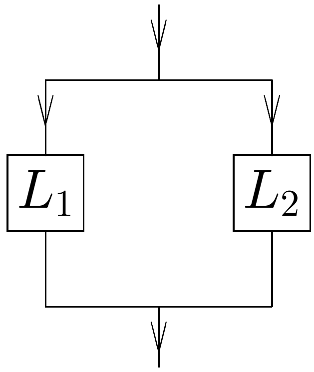
  ```
  Komanda1;Komanda2;...
  ```

- iteracija

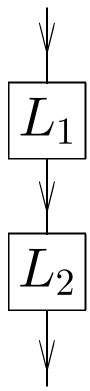
  `while` p `do` A

  `for i:=1 to` n `do` A

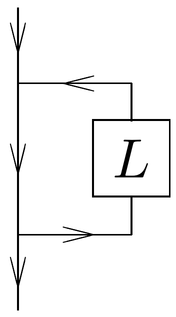
Unija / Selekcija



Konkatenacija / Sekvenca



Zvezda / Iteracija



Algebra jezika

$$\mathbf{Lang}(\Sigma) = \langle \mathcal{P}(\Sigma^*), +, \cdot, ^*, \emptyset, \{\lambda\} \rangle$$

REGULARNI JEZICI

Jezik je **regularan** ako se može dobiti od $\emptyset$, $\{\lambda\}$ i jezika oblika $\{a\}$, $a \in \Sigma$, konačnom primenom operacija $+, \cdot, ^*$.

Algebra regularnih jezika nad Σ:

$$\mathbf{Reg}(\Sigma) = \langle Reg(\Sigma), +, \cdot, ^*, \emptyset, \{\lambda\} \rangle.$$

Regularni jezici i automati

Kleenejeva teorema. Jezik L je regularan akko je L jezik nekog konačnog automata.

$$\begin{tikzcd} {} \arrow[r] & q_0 \arrow[r, leftrightarrow, "a"] \arrow[d, leftrightarrow, "b"'] & q_1 \arrow[d, leftrightarrow, "b"] \\ & q_2 \arrow[r, leftrightarrow, "a"] & q_3 \end{tikzcd}$$

Regularni izrazi

Regularni izrazi su izrazi (termi) sačinjeni od slova $a \in \Sigma$, simbola $0, 1$, i $+, \cdot, ^*$, koji opisuju konstrukciju regularnih jezika.

Primeri:

$(a+b)^* \;\rightarrow\; \{\lambda, a, b, aa, ab, ba, bb, aaa, aab, \ldots\}$
$(ab{+}ba)^*a \;\rightarrow\; \{a, aba, baa, abbaa, baaba, ababa, \ldots\}$
$(a+ba^*b)^* \;\rightarrow$ sve reči sa parno mnogo b-ova
$(a+ab)^*ab+(ba^*b)^* \;\rightarrow\; ?$

Regularni identiteti

Ako regularni izrazi r, s predstavljaju isti jezik, tada par $\langle r, s\rangle$ jeste **regularni identitet**, što pišemo kao

$$r = s.$$

Neki regularni identiteti

$$(a+b)+c = a+(b+c) \qquad 1\cdot a = a\cdot 1 = a$$
$$a+0 = 0+a = a \qquad (ab)c = a(bc)$$
$$a+b = b+a \qquad a(b+c) = ab+ac$$
$$0\cdot a = a\cdot 0 = 0 \qquad (a+b)c = ac+bc$$

$$a^*a^* = a^*$$

$$1 + aa^* = a^*$$

$$a(ba)^* = (ab)^*a$$

$$a^* = (1 + a + a^2 + \ldots + a^{n-1})(a^n)^*$$

Conwayevi identiteti

$$\begin{aligned}(a+b)^* &= (a^*b)^*a^* \\ (ab)^* &= 1 + a(ba)^*b \\ (a^*)^* &= a^*\end{aligned}$$

CONWAYEVI IDENTITETI

$$
\begin{aligned}
(a+b)^* &= (a^*b)^*a^* \\
(ab)^* &= 1 + a(ba)^*b \\
(a^*)^* &= a^*
\end{aligned}
$$

Objašnjenje za prvi identitet:

$$aababaaabbbabaaaa$$

Conwayevi identiteti

$$\begin{aligned}(a+b)^* &= (a^*b)^*a^* \\ (ab)^* &= 1 + a(ba)^*b \\ (a^*)^* &= a^*\end{aligned}$$

Objašnjenje za prvi identitet:

$$aab|ab|aaab|b|b|ab|aaaa$$

Conwayevi identiteti

$$
\begin{aligned}
(a+b)^* &= (a^*b)^*a^* \\
(ab)^* &= 1 + a(ba)^*b \\
(a^*)^* &= a^*
\end{aligned}
$$

Objašnjenje za drugi identitet:

$$ab|ab|ab|ab|ab|ab|ab$$

Conwayevi identiteti

$$
\begin{aligned}
(a+b)^* &= (a^*b)^*a^* \\
(ab)^* &= 1 + a(ba)^*b \\
(a^*)^* &= a^*
\end{aligned}
$$

Objašnjenje za drugi identitet:

$$a|ba|ba|ba|ba|ba|ba|b$$

Veza sa binarnim relacijama

Kleenejeve relacione algebre:

$$\mathbf{Rel}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, {}^{\mathrm{rtc}}, \emptyset, \Delta_A \rangle.$$

Veza sa binarnim relacijama

Kleenejeve relacione algebre:

$$\mathbf{Rel}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_A \rangle.$$

Neka ove algebre generišu varijetet (jednakosnu klasu) $\mathcal{KA}$. Algebre iz $\mathcal{KA}$ zovemo **Kleenejeve algebre**.

Veza sa binarnim relacijama

Kleenejeve relacione algebre:

$$\mathbf{Rel}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, {}^{\mathrm{rtc}}, \emptyset, \Delta_A \rangle.$$

Neka ove algebre generišu varijetet (jednakosnu klasu) $\mathcal{KA}$. Algebre iz $\mathcal{KA}$ zovemo **Kleenejeve algebre**.

Kozen-Németijeva teorema. Algebre regularnih jezika $\mathbf{Reg}(\Sigma)$ su slobodne algebre u klasi $\mathcal{KA}$.

Posledica.

$$\text{regularni identiteti} = \text{zakoni Kleenejevih algebri}$$

Jednakosna logika

Reč je o formalnom sistemu koji omogućava manipulaciju identitetima (zakonima) u okviru matematičke logike.

Jednakosna logika

Reč je o formalnom sistemu koji omogućava manipulaciju identitetima (zakonima) u okviru matematičke logike.

Formule: $p = q$, gde su p, q neki termi (izrazi) po promenljivim $x, y, z, \ldots$.

Jednakosna logika

Reč je o formalnom sistemu koji omogućava manipulaciju identitetima (zakonima) u okviru matematičke logike.

Formule: $p = q$, gde su p, q neki termi (izrazi) po promenljivim $x, y, z, \ldots$.

Aksiome: $x = x$ + sopstvene aksiome ($\mathcal{A}x$).

Jednakosna logika

Reč je o formalnom sistemu koji omogućava manipulaciju identitetima (zakonima) u okviru matematičke logike.

Formule: $p = q$, gde su p, q neki termi (izrazi) po promenljivim $x, y, z, \ldots$.

Aksiome: $x = x$ + sopstvene aksiome ($\mathcal{A}x$).

Dokaz: niz identiteta (formula) koji su svi ili aksiome, ili se dobijaju od prethodnih u nizu putem

pravila izvođenja.

Pravila izvođenja:

$$(Sim):\quad \frac{p=q}{q=p},$$

$$(Tranz):\quad \frac{p=q,\ q=r}{p=r},$$

$$(Zam):\quad \frac{q(x_1,\ldots,x_n)=r(x_1,\ldots,x_n)}{q(p_1,\ldots,p_n)=r(p_1,\ldots,p_n)},$$

$$(Sagl):\quad \frac{p_1=q_1,\ldots,p_n=q_n}{f(p_1,\ldots,p_n)=f(q_1,\ldots,q_n)},$$

gde je f proizvoljan n-aran operacijski simbol.

REDKOVA TEOREMA

Regularni identiteti nemaju konačan sistem aksioma.

V. N. REDKO: *O definišućim relacijama za algebru regularnih događaja* (ruski). Ukrajinski Matematički Žurnal **16** (1964), 120–126.

Ali, *kako* izgleda (beskonačan) sistem aksioma za regularne identitete?

John H. Conway:

Regular Algebra and Finite Machines.

Chapman & Hall, London, 1971.

Conwayeva pretpostavka

Sistem aksioma za regularne identitete je sledeći:

Conwayeva pretpostavka

Sistem aksioma za regularne identitete je sledeći:

- aksiome poluprstena sa jedinicom,

Conwayeva pretpostavka

Sistem aksioma za regularne identitete je sledeći:

- aksiome poluprstena sa jedinicom,
- tri Conwayeva identiteta:

$$
\begin{aligned}
(a+b)^* &= (a^*b)^*a^*, \\
(ab)^* &= 1 + a(ba)^*b, \\
(a^*)^* &= a^*,
\end{aligned}
$$

CONWAYEVA PRETPOSTAVKA

Sistem aksioma za regularne identitete je sledeći:

- aksiome poluprstena sa jedinicom,
- tri Conwayeva identiteta:

$$\begin{aligned}(a+b)^* &= (a^*b)^*a^*,\\ (ab)^* &= 1+a(ba)^*b,\\ (a^*)^* &= a^*,\end{aligned}$$

- identitet $P(G)$ za svaku konačnu grupu G.

$\underline{P(G)}$

Od konačne grupe G se napravi automat, tzv. **grupni automat**, čija su stanja i prelazi obeleženi sa elementima grupe.

$\underline{P(G)}$

Od konačne grupe G se napravi automat, tzv. **grupni automat**, čija su stanja i prelazi obeleženi sa elementima grupe.

Početno stanje je jedinica grupe.

$\underline{P(G)}$

Od konačne grupe G se napravi automat, tzv. **grupni automat**, čija su stanja i prelazi obeleženi elementima grupe.

Početno stanje je jedinica grupe.

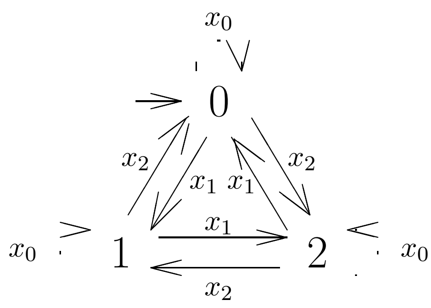
Ako je $g_1 h = g_2$, to ćemo crtati ovako:

$$g_1 \xrightarrow{\quad x_h \quad} g_2$$

Primer grupnog automata

$\mathbf{Z}_3$ – ciklična grupa reda 3:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1



$\underline{P(G)}$

Sada je $P(G)$ sledeći identitet:

$$\boxed{(x_e + x_{g_1} + \ldots + x_{g_{n-1}})^* = E_{e,e} + E_{e,g_1} + \ldots + E_{e,g_{n-1}}}$$

gde je $G = \{e, g_1, \ldots, g_{n-1}\}$ (e je jedinica grupe), dok je

$$E_{e,g_k}$$

regularan izraz koji predstavlja jezik sačinjen od sledećih reči w:

$$\longrightarrow\; e \xrightarrow{\quad w \quad} g_k$$

$\underline{P(G)}$

Identitet $P(G)$ u sebi čuva kompletnu informaciju o strukturi konačne grupe G, odnosno odgovarajućeg grupnog automata.

$\underline{P(G)}$

Identitet $P(G)$ u sebi čuva kompletnu informaciju o strukturi konačne grupe G, odnosno odgovarajućeg grupnog automata.

Po **teoremi Krohn-Rhodesa**, ovim su u stvari opisani svi automati (a time i svi regularni jezici).

Krob

Da je Conwayeva pretpostavka iz 1971. godine tačna, pokazao je **20** godina kasnije **Daniel Krob** (danas direktor Francuske Nacionalne Laboratorije za Informatička Istraživanja).

Krob

Da je Conwayeva pretpostavka iz 1971. godine tačna, pokazao je **20** godina kasnije **Daniel Krob** (danas direktor Francuske Nacionalne Laboratorije za Informatička Istraživanja).

Svoj dokaz Krob je prikazao u radu objavljenom 1991. godine u časopisu *Theoretical Computer Science*. Dokaz je dug **137** strana (!!!)

Krob

Krob je pokazao da je od grupnih identiteta dovoljno uzeti $P(G)$ samo za konačne **proste grupe** G, šta više, dovoljno je uzeti **alternativne grupe permutacija** A_n, $n \geq 5$.

Originalni rezultati

- regularni identiteti sa inverzijom
- regularni identiteti bez +
- komutativni regularni identiteti
- dinamičke algebre

Regularni identiteti sa inverzijom

Inverzija reči i jezika

$$w = a_1 a_2 \ldots a_n \;\Rightarrow\; w^{\vee} = a_n \ldots a_2 a_1$$

Inverzija reči i jezika

$$w = a_1a_2\ldots a_n \;\Rightarrow\; w^{\vee} = a_n\ldots a_2a_1$$

Primeri: $(igor)^{\vee} = rogi$, $(dolinka)^{\vee} = aknilod$
$(siniša)^{\vee} =$*ašinis*, $(crvenković)^{\vee} =$ *ćivoknevrc*
$(anavolimilovana)^{\vee} = anavolimilovana$

Inverzija reči i jezika

$$w = a_1 a_2 \dots a_n \ \Rightarrow \ w^{\vee} = a_n \dots a_2 a_1$$

Primeri: $(igor)^{\vee} = rogi$, $(dolinka)^{\vee} = aknilod$
$(siniša)^{\vee} =$*ašinis*, $(crvenković)^{\vee} =$ *ćivoknevrc*
$(anavolimilovana)^{\vee} = anavolimilovana$

$$L^{\vee} = \{w^{\vee} : w \in L\}$$

Inverzija reči i jezika

$$w = a_1a_2\dots a_n \;\Rightarrow\; w^\vee = a_n\dots a_2a_1$$

Primeri: $(igor)^\vee = rogi$, $(dolinka)^\vee = aknilod$
$(siniša)^\vee =$*ašinis*, $(crvenković)^\vee =$ *ćivoknevrc*
$(anavolimilovana)^\vee = anavolimilovana$

$$L^\vee = \{w^\vee : w \in L\}$$

$$\mathbf{Lang}^\vee(\Sigma) = \langle \mathcal{P}(\Sigma^*), +, \cdot, ^*, ^\vee, \emptyset, \{\lambda\}\rangle$$

Inverzija relacija

$$\varrho^{\vee} = \{\langle b, a\rangle :\ \langle a, b\rangle \in \varrho\}$$

Inverzija relacija

$$\varrho^{\vee} = \{\langle b, a\rangle : \ \langle a, b\rangle \in \varrho\}$$

$$\mathbf{Rel}^{\vee}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, {}^{\mathrm{rtc}}, {}^{\vee}, \emptyset, \Delta_A \rangle$$

Aksiome za inverziju

Bloom, Ésik, Stefanescu (1995): aksiome za inverziju jezika = regularni identiteti +

$$
\begin{array}{ll}
(a+b)^{\vee} = a^{\vee} + b^{\vee} & (a^{\vee})^{\vee} = a \\
(ab)^{\vee} = b^{\vee} a^{\vee} & 0^{\vee} = 0 \\
(a^{*})^{\vee} = (a^{\vee})^{*} & 1^{\vee} = 1
\end{array}
$$

Aksiome za inverziju

Bloom, Ésik, Stefanescu (1995): aksiome za inverziju jezika = regularni identiteti +

$$\begin{array}{ll} (a+b)^\vee = a^\vee + b^\vee & (a^\vee)^\vee = a \\ (ab)^\vee = b^\vee a^\vee & 0^\vee = 0 \\ (a^*)^\vee = (a^\vee)^* & 1^\vee = 1 \end{array}$$

Ésik, Bernátsky (1995): aksiome za inverziju relacija = aksiome za inverziju jezika +

$$a + aa^\vee a = aa^\vee a$$

Problem

Da li identiteti algebri relacija

$$\mathbf{Rel}^{\vee}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, {}^{\mathrm{rtc}}, {}^{\vee}, \emptyset, \Delta_A \rangle$$

imaju konačnu aksiomatizaciju?

(B. Jónsson, 1988)

Srodan problem

Da li regularni identiteti sa inverzijom imaju konačan sistem aksioma?

Involucija

Involucija algebre $\langle A, F \rangle$ = operacija ${}^{\vee} : A \to A$ tako da je $(a^{\vee})^{\vee} = a$ i

$$(f(a_1, \ldots, a_n))^{\vee} = f(a_n^{\vee}, \ldots, a_1^{\vee})$$

za sve $f \in F_n$.

Teorema. Neka za varijetet algebri $\mathcal{V}$, $\widehat{\mathcal{V}}$ označava klasu svih algebri sa involucijom koje zadovoljavaju aksiome za $\mathcal{V}$.

Tada $\mathcal{V}$ i $\widehat{\mathcal{V}}$ zadovoljavaju iste identitete bez involucije ako i samo ako je skup identiteta za $\mathcal{V}$ zatvoren na "obrtanje".

Pri tome $\widehat{\mathcal{V}}$ ima konačan skup aksioma ako i samo ako ga ima $\mathcal{V}$.

$$a + aa^{\vee}a = aa^{\vee}a$$

$$aa^{\vee}a = aa^{\vee}a + a$$

Posledica. Regularni identiteti (kao i identiteti relacija) sa inverzijom nemaju konačan sistem aksioma.

S. Crvenković, I. Dolinka, Z. Ésik,

The variety of Kleene algebras is not finitely based.

Theoretical Computer Science **230** (2000), 235–245.

Elsevier BV, Amsterdam.

Teorema. 13-elementna involutivna polugrupa $I_0^*(B_2^1)$ nema konačnu bazu identiteta.

(*Crvenković, Dolinka, Vinčić, 1998/99*)

S. Crvenković, I. Dolinka, M. Vinčić,

Equational bases for some 0-direct unions of semigroups.

Studia Scientiarum Mathematicarum Hungarica, *u štampi*

MTA & Akadémiai Kiadó, Budapest.

Regularni identiteti bez +

Problem

Da li identiteti algebri relacija
$\mathbf{UFRel}(A) = \langle \mathcal{P}(A \times A), \circ, {}^{\mathrm{rtc}}, \emptyset, \Delta_A \rangle$
imaju konačnu aksiomatizaciju?

(D. A. Bredikhin, 1993)

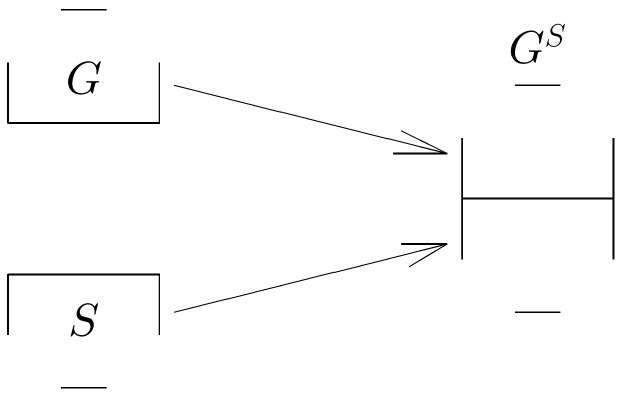
Ekvivalentan problem

Da li regularni identiteti bez + imaju konačnu aksiomatizaciju?

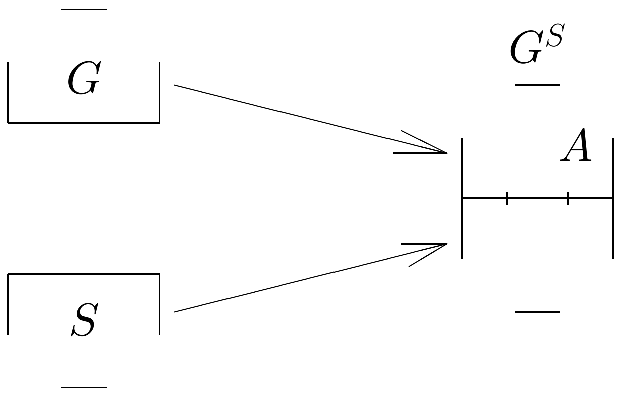
Teorema. Za svaki konačan skup regularnih identiteta E postoji regularni identitet bez simbola $+$ koji se ne može izvesti iz E.

Posledica. Regularni identiteti bez $+$ nemaju konačan sistem aksioma.

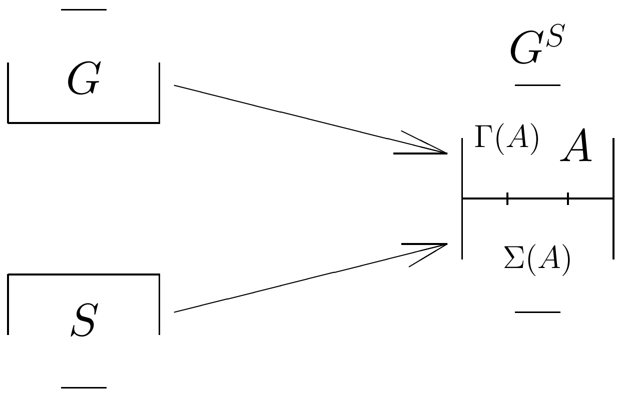
Uopšteni Conwayevi modeli



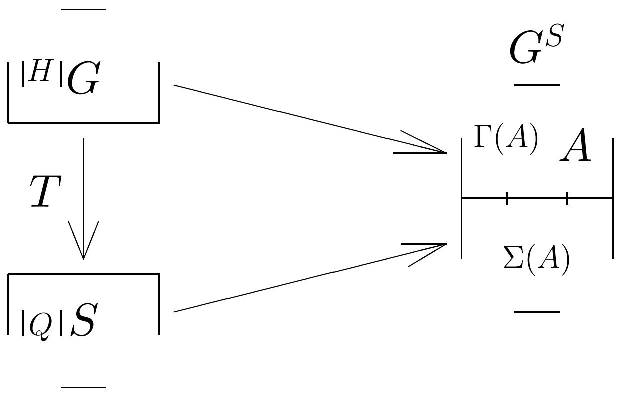
Uopšteni Conwayevi modeli



Uopšteni Conwayevi modeli



Uopšteni Conwayevi modeli



Ideja dokaza

Uopšteni Conwayev model $\mathbf{M}_T(G, S)$ je Conwayev *-poluprsten akko:

- T je monotono ($H \leq K \;\Rightarrow\; T_H \leq T_K$),
- T je stabilno na konjugaciju ($T_{g^{-1}Hg} = T_H$),
- $T : \{1\} \mapsto \emptyset$.

Pretpostavimo:

$$\text{aksiome Conwayevih } {}^*\text{-poluprstena}$$
$$+$$
$$P(G_1), P(G_2), \ldots, P(G_k)$$

dokazuju sve reg. identitete bez +.

Pretpostavimo:

$$\text{aksiome Conwayevih }{}^*\text{-poluprstena}$$

$$+$$

$$P(G_1), P(G_2), \ldots, P(G_k)$$

dokazuju sve reg. identitete bez $+$.

Neka sve grupe G_i imaju $\leq n$ elemenata.

Pretpostavimo:

$$\text{aksiome Conwayevih }^*\text{-poluprstena}$$

$$+$$

$$P(G_1), P(G_2), \ldots, P(G_k)$$

dokazuju sve reg. identitete bez $+$.

Neka sve grupe G_i imaju $\leq n$ elemenata.

Odaberimo proste brojeve p, q tako da je

$$n! < p < q.$$

Polugrupa Ω_3

$$\begin{array}{c|ccc} & a & b & c \\ \hline a & a & a & a \\ b & c & b & c \\ c & c & c & c \end{array}$$

Uz pogodno definisano T, model $\mathbf{M}_T(Z_{pq}, \Omega_3)$:

- jeste Conwayev *-poluprsten,

- zadovoljava $P(G)$ za svaku grupu G sa $\leq n$ elemenata,

- **ali**, ne zadovoljava regularni identitet

$$(x^p)^*(x^q)^* = (x^q)^*(x^p)^*.$$

Problem 1. Naći konkretan, netrivijalan sistem aksioma za regularne identitete bez $+$.

Problem 2. Da li se sistemu aksioma za regularne identitete bez $+$ može dodati neki konačan skup regularnih identiteta, pa da se dobije aksiomatizacija *svih* regularnih identiteta?

Problem 3. (*J. L. Rhodes, 1999*) Dati geometrijsku karakterizaciju automata koji prihvataju jezike predstavljene regularnim izrazima bez $+$.

S. Crvenković, I. Dolinka, Z. Ésik,

On equations for union-free regular languages.

Information & Computation, *u štampi*
Academic Press, London, New York.

Komutativni regularni identiteti

KOMUTATIVNA REČ = niz slova u kojem je dopušteno njihovo permutovanje

$\Sigma^{\oplus}$ = skup svih komutativnih reči nad Σ

KOMUTATIVNI JEZIK = skup komutativnih reči nad Σ, tj. $\subseteq \Sigma^{\oplus}$

Komutativne reči

$$abbaaabaab = a^6b^4,$$
$$matematika = a^3eikm^2t^2,$$
$$igor = gori,$$
$$xyxzxy = x^3y^2z.$$

Algebra komutativnih jezika

$$\mathbf{CLang}(\Sigma) = \langle \mathcal{P}(\Sigma^{\oplus}), +, \cdot, {}^{*}, \emptyset, \{\lambda\} \rangle$$

Algebra komutativnih jezika

$$\mathbf{CLang}(\Sigma) = \langle \mathcal{P}(\Sigma^{\oplus}), +, \cdot, ^*, \emptyset, \{\lambda\} \rangle$$

Polazeći od $\emptyset, \{\lambda\}$ i $\{a\}$ $(a \in \Sigma)$, konačnom primenom $+, \cdot, ^*$ dobijamo **komutativne regularne jezike**.

Algebra komutativnih jezika

$$\mathbf{CLang}(\Sigma) = \langle \mathcal{P}(\Sigma^{\oplus}), +, \cdot, {}^*, \emptyset, \{\lambda\} \rangle$$

Polazeći od $\emptyset, \{\lambda\}$ i $\{a\}$ $(a \in \Sigma)$, konačnom primenom $+, \cdot, {}^*$ dobijamo **komutativne regularne jezike**.

Parovi regularnih izraza koji indukuju iste komutativne regularne jezike čine **komutativne regularne identitete**.

Aksiome za komutativne r.i.

Aksiome za komutativne regularne identitete (Redko, 1964):

- aksiome poluprstena sa jedinicom,

Aksiome za komutativne r.i.

Aksiome za komutativne regularne identitete (Redko, 1964):

- aksiome poluprstena sa jedinicom,
- tri Conwayeva identiteta:

$$(x+y)^* \;=\; (x^*y)^*x^*, \quad (xy)^* \;=\; 1+x(yx)^*y,$$

$$(x^*)^* \;=\; x^*,$$

Aksiome za komutativne r.i.

Aksiome za komutativne regularne identitete (Redko, 1964):

- aksiome poluprstena sa jedinicom,
- tri Conwayeva identiteta:

$$(x+y)^* = (x^*y)^*x^*, \quad (xy)^* = 1 + x(yx)^*y,$$
$$(x^*)^* = x^*,$$

- $x^* = (1 + x + \ldots + x^{p-1})(x^p)^*$ za sve proste p,

Aksiome za komutativne r.i.

Aksiome za komutativne regularne identitete (Redko, 1964):

- aksiome poluprstena sa jedinicom,
- tri Conwayeva identiteta:

$$(x+y)^* = (x^*y)^*x^*, \quad (xy)^* = 1 + x(yx)^*y,$$

$$(x^*)^* = x^*,$$

- $x^* = (1 + x + \ldots + x^{p-1})(x^p)^*$ za sve proste p,
- $xy = yx, \quad x^*y^* = (xy)^*(x^* + y^*)$.

Redkova teorema #2

Komutativni regularni identiteti nemaju konačan sistem aksioma.

V. N. Redko: *O algebri komutativnih događaja* (ruski). Ukrajinski Matematički Žurnal **16** (1964), 185–195.

D. L. Pilling: "The Algebra of Operators for Regular Events". Doktorska disertacija, Cambridge University, 1970.

Problem

Kakva je veza između komutativnih regularnih identiteta i identiteta algebre regularnih jezika **Reg**(1) nad **jednoelementnim** alfabetom?

A. Salomaa: *Theory of Automata* (1969)

Teorema.

Komutativni regularni identiteti

=

identiteti za regularne jezike nad $\Sigma = \{a\}$.

S. Crvenković, I. Dolinka, Z. Ésik,

A note on equations for commutative regular languages.

Information Processing Letters **70** (2000), 265–267.

Elsevier BV, Amsterdam.

<u>Problem 8 iz disertacije</u>

Naći aksiomatizaciju za komutativne regularne identitete bez $+$. Da li ona može biti konačna?

Rešenje Pr.8 (Februar 2000.)

Aksiome komutativnih polugrupa sa 0 i 1, zajedno sa:

$$0^* = 1, \qquad (xy^*)^* = x^*(xyy^*)^*,$$

$$(x^*y)^*x^* = x^*y^*, \qquad (x^*)^* = x^*,$$

$$(xy^*z^*)^* = (xy^*(yz)^*)^*(xz^*(yz)^*)^*,$$

$$(xy^*(uv^*)^*)^* = (xx^*y^*)^*(xux^*y^*u^*v^*)^*,$$

$$(xy^*)^* = (x(y^p)^*)^*(xy(y^p)^*)^* \dots (xy^{p-1}(y^p)^*)^*,$$

za sve proste brojeve p.

Rešenje Pr.8 (Februar 2000.)

Teorema. Komutativni regularni identiteti bez $+$ nemaju konačan sistem aksioma.

S. Crvenković, I. Dolinka

On axioms for commutative regular equations without addition.

Priloženo u: Theoretical Computer Science
Elsevier BV, Amsterdam.

Dinamičke algebre

Osnovni postupci struktuiranog programiranja:

- selekcija

  `if` p `then` A `else` B

- sekvenca (nizanje komandi)

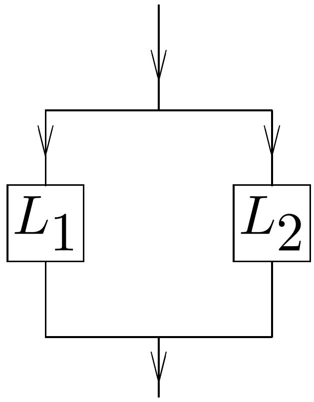
  `Komanda1;Komanda2;...`

- iteracija

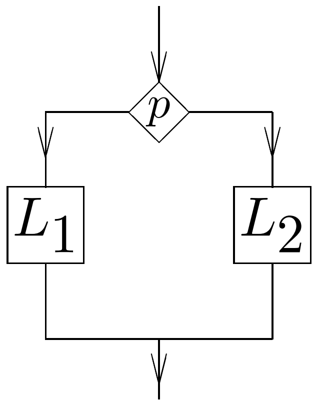
  `while` p `do` A

  `for i:=1 to` n `do` A

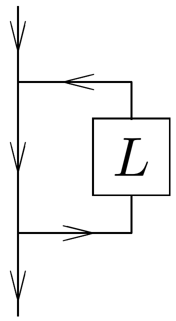
Unija / Selekcija



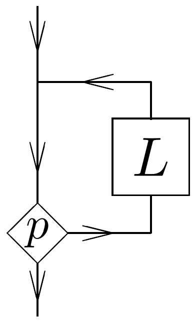
Unija / Selekcija



Zvezda / Iteracija



Zvezda / Iteracija



Dinamičke algebre
= Regularne + Booleove algebre

regularni deo = **akcije** (programi)

Booleov deo = **iskazi** (stanja računara)

$$\langle a \rangle p$$

= iskaz: "akcija a može "proizvesti" stanje (tačnost iskaza) p".

$$\boxed{q} \xrightarrow{\quad a \quad} \boxed{p}$$

Primeri

$$\langle \mathtt{x} := \mathtt{5} \rangle x = 5 \;=\; \top$$

$$\langle \mathtt{x} := \mathtt{x} + \mathtt{1} \rangle x = 5 \;=\; (x = 4)$$

$$\langle (\mathtt{x} := \mathtt{x} - \mathtt{1})^* \rangle x = 0 \;=\; (x \geq 0)$$

Aksiome dinamičkih algebri

$$\langle a \rangle \bot \;=\; \bot$$

Aksiome dinamičkih algebri

$$
\begin{aligned}
\langle a \rangle \bot &= \bot \\
\langle a \rangle (p \vee q) &= \langle a \rangle p \vee \langle a \rangle q
\end{aligned}
$$

Aksiome dinamičkih algebri

$$\begin{aligned}\langle a\rangle\bot &= \bot\\ \langle a\rangle(p\vee q) &= \langle a\rangle p\vee\langle a\rangle q\\ \langle a+b\rangle p &= \langle a\rangle p\vee\langle b\rangle p\end{aligned}$$

Aksiome dinamičkih algebri

$$\begin{aligned}
\langle a\rangle\bot &= \bot\\
\langle a\rangle(p\vee q) &= \langle a\rangle p\vee\langle a\rangle q\\
\langle a+b\rangle p &= \langle a\rangle p\vee\langle b\rangle p\\
\langle ab\rangle p &= \langle a\rangle\langle b\rangle p
\end{aligned}$$

Aksiome dinamičkih algebri

$$\begin{aligned}
\langle a \rangle \bot &= \bot \\
\langle a \rangle (p \vee q) &= \langle a \rangle p \vee \langle a \rangle q \\
\langle a + b \rangle p &= \langle a \rangle p \vee \langle b \rangle p \\
\langle ab \rangle p &= \langle a \rangle \langle b \rangle p \\
\langle 0 \rangle p &= \bot
\end{aligned}$$

Aksiome dinamičkih algebri

$$\begin{aligned}
\langle a\rangle\bot &= \bot\\
\langle a\rangle(p\vee q) &= \langle a\rangle p\vee\langle a\rangle q\\
\langle a+b\rangle p &= \langle a\rangle p\vee\langle b\rangle p\\
\langle ab\rangle p &= \langle a\rangle\langle b\rangle p\\
\langle 0\rangle p &= \bot\\
\langle 1\rangle p &= p
\end{aligned}$$

Aksiome dinamičkih algebri

$$
\begin{aligned}
\langle a \rangle \bot &= \bot \\
\langle a \rangle (p \vee q) &= \langle a \rangle p \vee \langle a \rangle q \\
\langle a + b \rangle p &= \langle a \rangle p \vee \langle b \rangle p \\
\langle ab \rangle p &= \langle a \rangle \langle b \rangle p \\
\langle 0 \rangle p &= \bot \\
\langle 1 \rangle p &= p
\end{aligned}
$$

Aksioma indukcije:

$$p \vee \langle aa^* \rangle p \;\leq\; \langle a^* \rangle p \;\leq\; p \vee \langle a^* \rangle (\neg p \wedge \langle a \rangle p)$$

Dinamičke test algebre

$p?$ – akcija ispitivanja tačnosti iskaza p

$$\langle p? \rangle q \; = \; p \wedge q$$

$\texttt{if}\ p\ \texttt{then}\ A\ \texttt{else}\ B \quad = \quad p?A + (\neg p)?B$

$\texttt{while}\ p\ \texttt{do}\ A \quad = \quad (p?A)^*(\neg p)?$

Kleenejeve test algebre

D. Kozen (1997): modifikacija pojma dinamičke test-algebre.

Teorema. (*Böhm, Jacopini*) Svaki `while` program se može simulirati `while` programom sa najviše jednom "`while`...`do`" petljom, pod uslovom da se dopusti uvođenje novih Booleovih promenljivih.

Jednosortne dinamičke algebre

- $\langle r \rangle t \to f_{\alpha(r)}(t)$

Jednosortne dinamičke algebre

- $\langle r \rangle t \to f_{\alpha(r)}(t)$
- Jónssonove dinamičke algebre: $\langle \mathbf{B}, f_a \rangle_{a \in K}$

Jednosortne dinamičke algebre

- $\langle r \rangle t \to f_{\alpha(r)}(t)$
- Jónssonove dinamičke algebre: $\langle \mathbf{B}, f_a \rangle_{a \in K}$

$$\begin{array}{ll}
f_a(0) = 0 & f_a(x \vee y) = f_a(x) \vee f_a(y) \\
f_{a+b}(x) = f_a(x) \vee f_b(x) & f_{ab}(x) = f_a(f_b(x)) \\
f_0(x) = \perp & f_1(x) = x
\end{array}$$

$$f_{a^*}(x) = x \vee f_{a^*}(\neg x \wedge f_a(x))$$

Kripkeove strukture (KDA)

$$\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle \cdot \rangle \rangle$$

gde je $\mathbf{K} \leq \mathbf{Rel}(A)$, zatim $\mathbf{B} \leq \mathcal{P}(A)$ i

$$\langle \varrho \rangle X = \{ y \in A : \; (\exists x \in X) \; \langle x, y \rangle \in \varrho \}$$

Separabilnost

$$a \neq b \;\Rightarrow\; (\exists p)\ \langle a \rangle p \neq \langle b \rangle p$$

Primer. U KDA važi: ako je za sve $X \subseteq A$

$$\langle \varrho \rangle X = \langle \sigma \rangle X,$$

onda je $\varrho = \sigma$.

Separabilnost – kontraprimer

Conwayev skok:

$$\begin{array}{|l} \infty \\ F \\ 1 \\ 0 \end{array}$$

$$\langle F \rangle p = \langle \infty \rangle p$$

Regularni identiteti – ponovo

Teorema. $r = s$ je regularni identitet ako i samo ako

$$\langle r\rangle x = \langle s\rangle x$$

sledi iz aksioma dinamičkih algebri.

Regularni identiteti – ponovo

Teorema. $r = s$ je regularni identitet ako i samo ako

$$\langle r \rangle x = \langle s \rangle x$$

sledi iz aksioma dinamičkih algebri.

Posledica. Ako je $\mathbf{D}$ separabilna dinamička algebra, tada je njen regularni deo Kleenejeva algebra.

Regularni identiteti – ponovo

Teorema. $r = s$ je regularni identitet ako i samo ako

$$\langle r \rangle x = \langle s \rangle x$$

sledi iz aksioma dinamičkih algebri.

Posledica. Ako je $\mathbf{D}$ separabilna dinamička algebra, tada je njen regularni deo Kleenejeva algebra.

Pitanje. Koje Kleenejeve algebre "forsiraju" separabilnost dinamičih algebri koje ih sadrže?

Teorema. Klasa Kleenejevih komponenti separabilnih dinamičkih algebri je kvazivarijetet, i on sadrži sve Kleenejeve relacione algebre, kao i sve slobodne algebre svih podvarijeteta od $\mathcal{KA}$.

Problem 1. Opisati kvazivarijetet iz prethodne teoreme. Da li je on konačno aksiomatizabilan?

Odlučivost DA

Teorema. *(Fischer, Ladner, 1977)* Jednakosna teorija dinamičkih algebri je odlučiva, i to u determinističkom vremenu $\sim c^{\frac{n}{\log n}}$.

Odlučivost Jónssonovih DA

Teorema. *(Crvenković, Madarász, 1994)* Postoji beskonačno mnogo Kleenejevih algebri **K** za koje jednakosna teorija Jónssonovih **K**-dinamičkih algebri nije odlučiva.

Problem 2. Za koje $\mathbf{K}$ je jednakosna teorija Jónssonovih $\mathbf{K}$-dinamičkih algebri odlučiva? Specijalno, kakva je situacija za konačne $\mathbf{K}$?

Teorema. Odgovor na prethodno pitanje je pozitivan, ukoliko $\mathbf{K}$ ima direktno razlaganje oblika

$$\mathbf{K} \cong \mathbf{F}_{\mathcal{V}_1}(X_1) \times \ldots \times \mathbf{F}_{\mathcal{V}_n}(X_n),$$

gde su varijeteti $\mathcal{V}_i \leq \mathcal{KA}$ generisani Kleene-jevim relacionim algebrama $(1 \leq i \leq n)$.

Posledica. Svaki varijetet dinamičkih algebri generisan (nekim) KDA ima odlučivu jednakosnu teoriju.

Posledica. Svaki varijetet Kleenejevih algebri generisan Kleenejevim relacionim algebrama ima odlučivu jednakosnu teoriju.

S. Crvenković, I. Dolinka,

Separability and decidability results for varieties of Jónsson dynamic algebras.

Algebra Universalis, *u štampi.*
Birkhäuser Verlag, Basel, Boston, Berlin.

Hvala na pažnji!

Pitanja Komisije

dr Rozália Sz. Madarász
redovni profesor PMF-a u Novom Sadu

Pitanja Komisije

dr Miroslav Ćirić
vanredni profesor PMF-a u Nišu
upravnik Studijske grupe za matematiku

Pitanja Komisije

dr Stojan Bogdanović
redovni profesor Ekonomskog fakulteta
u Nišu

Pitanja Komisije

dr Đura Paunić
redovni profesor PMF-a u Novom Sadu
redovni profesor PMF-a u Banja Luci
– *predsednik Komisije* –

Pitanja Komisije

dr Siniša Crvenković
redovni profesor PMF-a u Novom Sadu
redovni profesor PMF-a u Banja Luci
šef Katedre za algebru i diskretnu
matematiku (PMF, Novi Sad)
– mentor –