УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ"

ПРИРОДНО-МАТЕМАТИЧКИ ФАКУЛТЕТ - СКОПЈЕ

ИНСТИТУТ ЗА ИНФОРМАТИКА

Ана Соколова

ПРОБЛЕМ НА ЗБОРОВИ

- МАГИСТЕРСКИ ТРУД -

СКОПЈЕ, 1999

РЕПУБЛИКА МАКЕДОНИЈА

Содржина

1 Вовед

Во изминатите 60 години, голем дел од научните истражувања во математиката и теориската информатика се однесуваат на проблеми на одлучување. Најопшто, под проблем на одлучување се подразбира проблем на кој одговорот е "да" или "не". Голем дел од овие истражувања се должат на основните резултати од теоријата на пресметливост поставени од Turing, Post, Markov, Church и други. Притоа под *одлучив* проблем се подразбира "да-не" проблем за кој постои алгоритам со кој се доаѓа до одговорот, додека неодлучив е оној "да-не" проблем за кој не постои таков алгоритам. Но, се поставува прашањето: што е алгоритам? Поимот алгоритам можеби е интуитивно јасен, но е далеку од она што се очекува од формална прецизна математичка гледна точка. Токму затоа и поимот одлучивост се појавува заедно со основите на теоријата на пресметливост. Затоа, овде, и секаде кога станува збор за одлучивост, под алгоритам подразбираме алгоритам во смисла на тезата на Church, односно Тјуринговa машина или рекурзивна функција или граматика или нормален алгоритам.

Голем број од истражувањата во врска со проблемите на одлучување се однесуваат на проблеми на одлучување во универзалната алгебра, таканаречени алгоритамски проблеми за алгебрите, меѓу кои е и проблемот на зборови. Притоа, постојат две нивоа на проблем на зборови. Проблем на зборови на ниво на многуобразие и проблем на зборови за дадена алгебра.

Нека $\mathcal{V}$ е многуобразие алгебри од даден тип. Проблемот на зборови за дадена $\mathcal{V}$-алгебра дефинирана со конечно множество слободни генератори B и конечно множество дефинирачки равенства е решен ако постои алгоритам за одлучување дали два збора од апсолутно слободната алгебра со слободна база B од исти тип, се еквивалентни во дадената алгебра при конгруенцијата генерирана од идентитетите на многуобразието и дефинирачките равенства.

Проблемот на зборови е решен за многуобразие $\mathcal{V}$ доколку постои алгоритам кој може да се примени на секоја $\mathcal{V}$- алгебра дефинирана со конечно множество слободни генератори и конечно множество дефинирачки релации за да се определи дали два збора од апсолутно слободната алгебра со ист јазик се еквивалентни во дадената алгебра.

Основна тема на трудот е проблемот на зборови. Дадени се некои општи резултати во врска со решливоста на проблемот на зборови на прво и на второ ниво, како и примери на алгебри со решлив и нерешлив проблем на зборови, и примери на многуобразија со решлив и нерешлив проблем на зборови на ниво на многуобразие.

Интересно е да се напомене дека прв проблемот на зборови за многуобразието полугрупи го поставил Axel Thue во 1914 година, кога воопшто не бил прецизиран поимот алгоритам ниту пак идејата за неодлучивост. Затоа разбирливо е што оригиналниот проблем на Thue гласел вака:

За дадена конечно презентирана полугрупа и два збора над азбуката од генераторите, определи дали зборовите се еквивалентни

Сличен проблем бил поставен од Dehn неколку години претходно, познат како проблем на Dehn за конечно презентираните групи. И двата проблеми биле "позитивно зададени", во смисла "најди метод за ...". Проблемот на Dehn бил решен во 1932 година од Magnus за случајот на групи презентирани со едно дефинирачко равенство.

Со настанокот на теоријата на пресметливост во 30-тите години од овој век, ситуацијата се изменила, се појавиле првите примери на алгоритамски нерешливи проблеми, како и нова можност за приод кон проблемот на зборови и евентуално докажување на негативен резултат. Така, за полугрупите, во 1947 година е докажано од Markov и Post дека проблемот на зборови и на ниво на многуобразие и на ниво на алгебра е нерешлив, имено докажано е следново тврдење:

Постои конечно презентирана полугрупа S и збор w такви што не постои алгоритам кој одлучува, за даден збор v, дали v е еквивалентен на w или не.

Всушност проблемот на Thue е првиот проблем на одлучување кој се појавил во алгебрата и за кој е докажана алгоритамска неодлучивост.

Голем придонес во врска со истражувањето на алгебарските услови за решливост на проблемот на зборови дал Trevor Evans во чии неколку статии се дадени општи резултати во врска со решливост на проблемот на зборови на ниво на многуобразие, базирани на неговиот главен резултат:

Ако $\mathcal{V}$ е многуобразие со својството дека секоја делумна $\mathcal{V}$ алгебра може да се смести во $\mathcal{V}$ алгебра, тогаш проблемот на зборови е решлив за $\mathcal{V}$.

Разработувањето на овие резултати исто така ќе заземе голем дел од трудот. Всушност вториот дел (по воведот) е посветен на дефиниции на основните поими: алгебра, многуобразие, слободна алгебра, апсолутно слободна алгебра, алгебра на зборови (терми), презентација на алгебра, проблем на зборови на ниво на алгебра и проблем на зборови на ниво на многуобразие, како и на општите резултати на Evans кои имаат големо теоретско значење, но од друга страна, самиот алгоритам на Evans е многу комплексен.

Третиот дел од трудот е посветен на теоријата на пресметливост, односно на прецизирање на поимот алгоритам. Дадена е дефиниција на Тјурингова машина, на Тјуринг-одлучив и Тјуринг-прифатлив јазик, дефиниција на граматика, одредени својства во врска со наведените поими, и доказ за постоење на јазик кој не е Тјуринг-одлучив, врз кој се базира и доказот на наведениот резултат на Markov во врска со неодлучивоста на проблемот на зборови за полугрупите, на што е посветен значаен дел.

Во поново време, со воведувањето на поимите препишувачки систем и препишувања, како и добивањето на основните резултати во врска со препишувачките системи (бројни трудови на Huet, Klop, Jouannaud, Knuth, Bendix, Dershovitz и други) овозможено е решавање на проблемот на зборови во одредени алгебри и/или многуобразија со далеку помала комплексност, а проблемот се сведува на дизајн на соодветен препишувачки систем со одредени пожелни својства. На препишувачките системи е посветен четвртиот дел од трудот.

Препишувачките системи или системите од редукции имаат широка примена во теоретската информатика. Симболичкото манипулирање со синтаксни објекти е базирано на фактот што тие даваат модели за пресметување во оперативна околина. Теоријата на препишување потекнува од алгебрата, теоријата на докази и теоријата на пресметливост, и е фокусирана околу поимот "нормална форма" - израз кој понатаму не може да се редуцира.

Употребата на равенства е традиционална во математиката. Равенствата може да се употребуваат за резонирање (замена на еднакво со еднакво) на крајно недетерминистички начин. За разлика од нив, препишувачките системи прават нешто како "употреба на равенствата во една насока" при што се губи еден извор на недетерминизам. Ваквата еднонасочна употреба се базира на препишување според добро основано подредување на термите и се нарекува редукција. Да го цитираме Evans: "Редукција е секоја трансформација што намалува должина". Другите извори на недетерминизам како што е изборот на правило и подтерм на кој тоа се применува може да се елиминираат ако секој израз има единствена нормална форма.

Како пример за употреба на препишувачки систем наместо равенства ги наведуваме групите. Општо е познато дека групите се дефинирани со следните три равенства:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),\ x \cdot x^{-} = 1,\ x \cdot 1 = x,$$

но, исто така и со следново множество од 10 правила за препишување кои определуваат нормални форми:

$(x \cdot y) \cdot z \to x \cdot (y \cdot z),\ x \cdot x^{-} \to 1,\ x \cdot 1 \to x,\ x^{--} \to x,\ x \cdot (x^{-} \cdot y) \to y,\ (x \cdot y)^{-} \to y^{-} \cdot x^{-},\ x^{-} \cdot x \to 1,\ 1 \cdot x \to x,\ 1^{-} \to 1,\ x^{-} \cdot (x \cdot y) \to y.$

Препишувачките системи имаат голема улога во повеќе области, како што се спецификации на апстрактни податочни типови, имплементација на функционални програмски јазици и автоматско заклучување. Од наш интерес овде е пред се употребата на препишувачки системи во решавањето на проблемот на зборови во универзална алгебра. Тие се атрактивни пред се заради нивната едноставна синтакса и семантика.

Конечно, последниот дел од трудот ќе биде посветен на решавањето на проблемот на зборови во едно конкретно многуобразие, многуобразието Штајнерови лупи или слупи. Конкретното многуобразие е интересно бидејќи постои обратно еднозначно соодветство помеѓу класата конечни слупи и класата Штајнерови системи тројки. Во тој дел е даден опис на слободните објекти во ова многуобразие, и тоа директен опис и опис со канонични претставници, со помош на редукција на терми. Потоа, со помош на дефинираната редукција е даден алгоритам за решавање на проблемот на зборови за слупи, имено, е дефиниран соодветен препишувачки систем кој ја има особината на единствена нормална форма. Наведениот алгоритам задржува идеи од општиот алгоритам на Evans, но е базиран на препишувачки систем. Една битна разлика е тоа што во дефиницијата на препишувачкиот систем влегуваат само дефинирачките равенства на дадена конечно презентирана слупа, а потоа истиот може да се употребува за испитување на еквивалентност на произволни зборови. Овој дел е всушност резултат на оригинални истражувања на проф. Смиле Марковски и на авторот на овој труд.

2 Проблем на зборови - дефиниција и алгебарски пристап во решавањето

Овој дел воглавно се однесува на универзалната алгебра. Даваме дефиниции на основните поими неопходни за дефинирање на проблемот на зборови, како и некои познати општи резултати од универзалната алгебра. Го дефинираме проблемот на зборови на двете нивоа, како и некои други проблеми на одлучивост за алгебрите и даваме врски меѓу нив, како и преглед на решливост односно нерешливост на проблемот на зборови во одредени познати класи алгебри. Исто така детално се задржуваме на општите резултати на Trevor Evans во врска со алгебарските услови за решливост на проблемот на зборови на ниво на многуобразие. Во овој дел не го прецизираме поимот алгоритам (иако го употребуваме), тоа ќе биде направено во третиот дел од трудот.

2.1 Воведни поими и резултати од универзална алгебра

Во овој дел ознаките и дефинициите на поимите се воглавно како во [17]. Доказите на теоремите кои не се дадени, се наоѓаат во секоја стандардна книга за универзална алгебра, на пример [17, 18, 19].

Дефиниција 1 *Алгебра* е подреден пар $\mathbf{A} =< A, F >$ каде A е непразно множество и $F =< F_i; i \in I >$ каде F_i е финитарна операција на A (т.е. пресликување од A^n во A за некој $n \in \mathbb{N}$) за секој $i \in I$. A е *носител*, F_i *основна операција*, за секој $i \in I$, I е *индексно множество* или *множество операциски симболи* или *сигнатура* на алгебрата. △

Ги користиме и следниве ознаки. Ако Q е операциски симбол на $\mathbf{A}$, тогаш со Q^A ја означуваме основната операција на A индексирана со Q. Q^A се нарекува *интерпретација* на Q во $\mathbf{A}$.

За дадена алгебра $\mathbf{A}$ и индексно множество I, дефинирана е функција ρ наречена *ранг функција* од I во множеството природни броеви $\mathbb{N}$, дефинирана со: за секој $Q \in I$, $\rho(Q) = n_Q$ ако рангот на Q^A е n_Q, т.е. $Q^A : A^{n_Q} \to A$. Ранг функцијата уште се нарекува и *тип на сличност на алгебрата* или само *тип*. За две алгебри велиме дека се *слични* ако имаат ист тип.

Дефиниција 2 Нека F е операција од ранг r на множество A и нека X е подмножество на A. *X е затворено за F* ако и само ако за секои $a_0, \ldots, a_{r-1} \in X$, $F(a_0, \ldots, a_{r-1}) \in X$. Едно подмножество X на носителот на алгебра $\mathbf{A}$ е *под-носител* на $\mathbf{A}$ ако е затворено за сите основни операции на $\mathbf{A}$. △

Нека $\mathbf{A}$ е алгебра. За алгебрата $\mathbf{B}$ велиме дека е *подалгебра* на $\mathbf{A}$ ако и само ако $\mathbf{A}$ и $\mathbf{B}$ се слични, носителот B на $\mathbf{B}$ е под-носител на носителот на $\mathbf{A}$ и за секој операциски симбол Q од сигнатурата, Q^B е рестрикцијата на Q^A над B.

Дефиниција 3 Нека $\mathbf{A}$ е алгебра и $X \subseteq A$. *Под-носител на* $\mathbf{A}$ *генериран од* X е множеството $S_g^A(X) = \bigcap\{B | X \subseteq B$ и B е под-носител а $A\}$. △

Својство 1 Нека $\mathbf{A}$ е алгебра и $X \subseteq A$. Дефинираме индуктивно подмножества X_n од A со:

$X_0 = X$

$X_{n+1} = X_n \cup \{F(a_0, \ldots, a_{r-1}) |\ F$ е основна операција на $\mathbf{A}$ со ранг r и $a_0, \ldots, a_{r-1} \in X_n\}$.

Тогаш $S_g^A(X) = \bigcup\{X_n |\ n \in \mathbb{N}\}$. $\square$

Дефиниција 4 Алгебрата $\mathbf{A}$ е *е генерирана од* $X \subseteq A$ ако $A = S_g^A(X)$. Една алгебра $\mathbf{A}$ е *конечно генерирана* ако $\mathbf{A} = S_g^A(Y)$ за некое конечно $Y \subseteq A$. $\triangle$

Дефиниција 5 Нека $\mathbf{A}$ и $\mathbf{B}$ се алгебри од исти тип, Q е операциски симбол од нивната сигнатура со ранг r. Една функција $h : A \to B$ е *согласна со интерпретацијата* на Q ако, за сите $a_0, \ldots, a_{r-1} \in A$, $h(Q^A(a_0, \ldots, a_{r-1}) = Q^B(h(a_0), \ldots, h(a_{r-1}))$. $\triangle$

Една функција $h : A \to B$ велиме дека е *хомоморфизам* од $\mathbf{A}$ во $\mathbf{B}$ ако h е согласна со интерпретацијата на секој операциски симбол на $\mathbf{A}$. Сурјективен хомоморфизам се нарекува *епиморфизам* и притоа $\mathbf{B}$ се вика *хомоморфна слика* на $\mathbf{A}$. Инјективен хомоморфизам се нарекува *мономорфизам* или *сместување*, а биективен хомоморфизам се вика *изоморфизам*. За хомоморфизам од $\mathbf{A}$ во $\mathbf{A}$ велиме дека е *ендоморфизам* на $\mathbf{A}$, биективен ендоморфизам е *автоморфизам*.

Дефиниција 6 Нека $\mathbf{A} =< \mathbf{A}_i, i \in I >$ е систем слични алгебри. *Директен производ* на $< \mathbf{A}_i, i \in I >$ е алгебра, ознака $\Pi_I \mathbf{A}_i = \Pi\mathbf{A}$, од ист тип, со носител $\Pi_I A_i$ таква што за секој операциски симбол од ранг r и секои $f^0, \ldots, f^{r-1} \in \Pi_I A_i$, $(Q^{\Pi A}(f^0, \ldots, f^{r-1}))_i = Q^{A_i}(f_i^0, \ldots, f_i^{r-1})$, за секој $i \in I$. $\triangle$

Дефиниција 7 Нака $\mathbf{A}$ е алгебра и θ е бинарна релација на A. θ е *согласна со основна операција* F на $\mathbf{A}$ од ранг r ако за секои $a_0, \ldots, a_{r-1}, b_0, \ldots, b_{r-1} \in A$, од $a_i \theta b_i$ за $0 \leq i \leq r-1$ следува $F(a_0, \ldots, a_{r-1}) \theta F(b_0, \ldots, b_{r-1})$.

Конгруенција на $\mathbf{A}$ е еквивалентност на A согласна со секоја основна операција на $\mathbf{A}$. Со $Con\mathbf{A}$ се означува множеството од сите конгруенции на $\mathbf{A}$. $\triangle$

Дефиниција 8 Нека $\mathbf{A}$ е алгебра и θ е конгруенција на $\mathbf{A}$. *Фактор алгебра* $\mathbf{A}/\theta$ е алгебра слична на $\mathbf{A}$, со носител A/θ, во која интерпретација на секој операциски симбол Q (со ранг r) на $\mathbf{A}$ е Q_0^A, каде $Q_0^A(a_0/\theta, \ldots, a_{r-1}/\theta) = (Q^A(a_0, \ldots, a_{r-1}))/\theta$. $\triangle$

Теорема 1 (Теорема за хомоморфизам)

Нека $\mathbf{A}$ и $\mathbf{B}$ се две слични алгебри и h е епиморфизам од $\mathbf{A}$ на $\mathbf{B}$, нека θ е конгруенција на $\mathbf{A}$ и g е природното пресликување од $\mathbf{A}$ на $\mathbf{A}/\theta$ ($g(a) = a/\theta$, за секој $a \in A$). Тогаш

(i) Јадрото $kerh$ на h е конгруенција на $\mathbf{A}$. ($a \ker h b$ ако и само ако $h(a) = h(b)$).

(ii) Природното пресликување g е епиморфизам од $\mathbf{A}$ на $\mathbf{A}/\theta$.

(iii) Ако $\theta = kerh$, тогаш постои единствено пресликување f од A/θ во B со својство $f \circ g = h$, и тоа е изоморфизам меѓу $\mathbf{A}/\theta$ и $\mathbf{B}$. $\square$

Дефиниција 9 Нека $\mathbf{A}$ е алгебра и $X \subseteq A \times A$. *Конгруенција генерирана од* X е $C_g^A(X) = \bigcap\{\theta \mid X \subseteq \theta$ и θ е конгруенција на $\mathbf{A}\}$. Ако X е конечно, $C_g^A(X)$ е *конечно генерирана*. $\triangle$

Функции кои пресликуваат класа (слични) алгебри во класа (слични) алгебри се нарекуваат *оператори на класи*. Дефинираме неколку оператори на класи.

Дефиниција 10 Нека $\mathcal{K}$ е класа алгебри.

$\mathbf{A} \in \mathbf{I}(\mathcal{K})$ ако и само ако $\mathbf{A}$ е изоморфна на некоја алгебра од $\mathcal{K}$.

$\mathbf{A} \in \mathbf{H}(\mathcal{K})$ ако и само ако $\mathbf{A}$ е изоморфна на хомоморфна слика на алгебра од $\mathcal{K}$.

$\mathbf{A} \in \mathbf{S}(\mathcal{K})$ ако и само ако $\mathbf{A}$ е изоморфна на подалгебра на алгебра од $\mathcal{K}$.

$\mathbf{A} \in \mathbf{P}(\mathcal{K})$ ако и само ако $\mathbf{A}$ е изоморфна на директен производ на систем алгебри од $\mathcal{K}$. $\triangle$

Велиме дека $\mathcal{K}$ е класа *затворена за оператор на класи* $\mathbf{Q}$ ако $\mathbf{Q}(\mathcal{K}) \subseteq \mathcal{K}$.

Секој од дефинираните оператори на класи $\mathbf{Q}$, при рестрикција на класи слични алгебри, е *растечки* односно $\mathbf{Q}(\mathcal{K}) \supseteq \mathcal{K}$, *запазува подредување*, т.е. $\mathbf{Q}(\mathcal{K}_0) \subseteq \mathbf{Q}(\mathcal{K}_1)$ ако $\mathcal{K}_0 \subseteq \mathcal{K}_1$, и е *идемпотентен*, т.е. $\mathbf{Q}(\mathbf{Q}(\mathcal{K})) = \mathbf{Q}(\mathcal{K})$.

Дефиниција 11 Една класа $\mathcal{K}$ алгебри од ист тип е *многуобразие* ако е затворена за $\mathbf{H}$, $\mathbf{S}$ и $\mathbf{P}$. $\triangle$

Дефиниција 12 Нека $\mathcal{K}$ е класа слични алгебри. $\mathbf{V}(\mathcal{K})$ го означува најмалото многуобразие кое ја содржи $\mathcal{K}$ и се нарекува *многуобразие генерирано од* $\mathcal{K}$. $\triangle$

Теорема 2 $\mathbf{V} = \mathbf{HSP}$. $\square$

Дефиниција 13 Нека $\mathcal{K}$ е класа алгебри од исти тип и $\mathbf{U}$ е алгебра од истиот тип. Нека X е подмножество од U. $\mathbf{U}$ има *својство на универзално пресликување* за $\mathcal{K}$ над X ако и само ако за секоја $\mathbf{A} \in \mathcal{K}$ и секое пресликување $f : X \to A$ постои хомоморфизам $h : \mathbf{U} \to \mathbf{A}$ кој е проширување на f, т.е. $f(x) = h(x)$, за $x \in X$. $\triangle$

Велиме дека $\mathbf{U}$ е *слободна за* $\mathcal{K}$ над X ако $\mathbf{U}$ е генерирана од X и $\mathbf{U}$ има својство на универзално пресликување за $\mathcal{K}$ над X.

Велиме дека $\mathbf{U}$ е *слободна во* $\mathcal{K}$ над X ако $\mathbf{U} \in \mathcal{K}$ и $\mathbf{U}$ е слободна за $\mathcal{K}$ над X. Ако $\mathbf{U}$ е слободна во $\mathcal{K}$ над X, тогаш X се нарекува *слободно генераторно множество* за $\mathbf{U}$, и $\mathbf{U}$ се нарекува слободно генерирана од X. Ако $\mathcal{K}$ е класата од сите алгебри со одреден тип на сличност и $\mathbf{U}$ е слободна алгебра во $\mathcal{K}$ над X, за $\mathbf{U}$ велиме дека е *апсолутно слободна алгебра*.

Својство 2 Ако $\mathcal{K}_0 \subseteq \mathcal{K}_1$ и $\mathbf{U}$ е слободна за $\mathcal{K}_1$ над X, тогаш $\mathbf{U}$ е слободна за $\mathcal{K}_0$ над X. $\square$

Својство 3 Ако $\mathbf{U}$ е слободна за $\mathcal{K}$ над X, тогаш $\mathbf{U}$ е слободна за $\mathbf{V}(\mathcal{K})$ над X. $\square$

Својство 4 Нека $\mathbf{U}_1$ и $\mathbf{U}_2$ се слободни во $\mathcal{K}$ над X_1 и X_2 соодветно. Ако, $|X_1| = |X_2|$, тогаш $\mathbf{U}_1 \cong \mathbf{U}_2$. $\square$

Дефиниција 14 Нека $\mathcal{K}$ е класа алгебри и $\mathbf{A}$ е алгебра, сите од ист тип. Тогаш

$$\Theta_A(\mathcal{K}) = \bigcap\{\theta \in Con\mathbf{A} |\ \mathbf{A}/\theta \in \mathbf{S}(\mathcal{K})\}. \qquad \triangle$$

Својство 5 Нека $\mathbf{U}$ е слободна за $\mathcal{K}$ над X. Тогаш $\bar{\mathbf{U}} = \mathbf{U}/\Theta_U(\mathcal{K})$ е слободна во $\mathbf{V}(\mathcal{K})$ над $\bar{X} = \{x/\Theta_U(\mathcal{K})|\ x \in X\}$. $\square$

Нека ρ е тип на сличност и I е соодветно множество операциски симболи. Нека X е множество дисјунтно со I. За $n \in \mathbb{N}$, означуваме $I_n = \{Q \in I|\rho(Q) = n\}$, всушност I_n е множеството n-арни операциски симболи од I. Под *низа од* $X \cup I$ подразбираме конечна низа $< s_0, \ldots, s_k >$ чии членови припаѓаат на $X \cup I$. Ваквата низа уште се нарекува и *збор над азбука* $X \cup I$ и се запишува како $s_0 \ldots s_k$. *Производ* на два збора $a = a_0 \ldots a_{n-1}$ и $b = b_0 \ldots b_{m-1}$ е зборот $ab = a_0 \ldots a_{n-1} b_0 \ldots b_{m-1}$. Јасно, кога пишуваме "зборот u" за $u \in X \cup I$, всушност мислиме на низата $< u >$.

Дефиниција 15 Множеството $\mathcal{T}_\rho(X)$ од *терми од тип* ρ *над* X е најмалото множество $\mathcal{T}$ од зборови над азбука $X \cup I$ така што:

1. $X \cup I_0 \subseteq \mathcal{T}$,
2. Ако $p_0, \ldots, p_{n-1} \in \mathcal{T}$ и $Q \in I_n$, тогаш зборот $Qp_0p_1 \ldots p_{n-1} \in \mathcal{T}$.

$\triangle$

Притоа, воведуваме договор за означување на термите. Наместо терм $Qp_0p_1 \ldots p_{n-1}$ пишуваме $Q(p_0, p_1, \ldots, p_{n-1})$, бинарните операциски симболи во термите ги пишуваме инфиксно. Да уочиме дека $\mathcal{T}_\rho(X)$ е празно ако и само ако $X \cup I_0$ е празно.

Дефиниција 16 Ако $\mathcal{T}_\rho(X) \neq \emptyset$, тогаш *алгебра терми од тип* ρ *над* X, со ознака $\mathbf{T}_\rho(X)$, е алгебрата од тип ρ со носител $\mathcal{T}_\rho(X)$ за чии основни операции важи

$$Q^{\mathbf{T}_\rho(X)}(p_0,\ldots,p_{n-1}) = Q(p_0,\ldots,p_{n-1})$$

за секој $Q \in I_n,\ p_i \in \mathcal{T}_\rho(X)$. $\triangle$

Теорема 3 Нека ρ е тип на сличност, I е соодветно множество операциски симболи, и X е множество такво што $|X| \geq 1$ ако $I_0 = \emptyset$. Нека $\mathcal{V}$ е многуобразие алгебри од тип ρ.

(i) Ако $X \cap I = \emptyset$, тогаш алгебрата терми $\mathbf{T}_\rho(X)$ е апсолутно слободна алгебра од тип ρ генерирана од множеството $\{< x > \mid x \in X\}$ (или велиме, генерирана од X).

(ii) Ако $X \cap I = \emptyset$, тогаш $\mathbf{T}_\rho(X)/\Theta(\mathcal{V})$ е слободна во $\mathcal{V}$ над множеството $\{< x > /\Theta(\mathcal{V}) \mid x \in X\}$.

(iii) Ако $\mathcal{V}$ има нетривијални членови, тогаш постои слободна алгебра во $\mathcal{V}$ над множеството X. $\square$

Дефиниција 17 Со $\mathbf{F}_\mathcal{K}(X)$ означуваме слободна алгебра во $\mathbf{V}(\mathcal{K})$ со слободно генераторно множество X. $\mathbf{F}_\mathcal{K}(\kappa)$ означува алгебра $\mathbf{F}_\mathcal{K}(X)$ за $|X| = \kappa$. $\triangle$

Да забележиме дека: $\mathbf{F}_\mathcal{K}(X)$, ако постои, е определена до изоморфизам; $\mathbf{F}_\mathcal{K}(\kappa)$ е определена до изоморфизам; $\mathbf{F}_\mathcal{K}(0)$ постои ако и само ако типот содржи нуларни операции; $\mathbf{F}_\mathcal{K}(1)$ постои; ако $\kappa > 1$, $\mathbf{F}_\mathcal{K}(\kappa)$ постои ако и само ако $\mathcal{K}$ има нетривијални членови.

Последица 1 Нека X е множество и $\mathcal{K}$ е класа алгебри од тип ρ така што $\mathbf{F}_\mathcal{K}(X)$ постои. Тогаш $\mathbf{F}_\mathcal{K}(X)$ припаѓа на $\mathbf{SP}(\mathcal{K})$ и

$$\mathbf{F}_{\mathbf{V}(\mathcal{K})}(X) \cong \mathbf{F}_\mathcal{K}(X) \cong \mathbf{T}_\rho(X)/\Theta(\mathcal{K}). \qquad \square$$

Во продолжение даваме поопшта дефиниција на терм. Притоа, сметаме дека секое множество операциски симболи I од секој тип ρ е такво што $I \cap \mathbb{N} = \emptyset$.

Дефиниција 18 Нека ρ е тип. Под *терм (од тип ρ)* подразбираме елемент од алгебрата терми $\mathbf{T}_\rho(\mathbb{N})$. Ставаме $v_n =< n >$ и термите v_n, за $n \in \mathbb{N}$, ги нарекуваме *променливи.* $\triangle$

За секој $n \in \mathbb{N}$, алгебрата терми $\mathbf{T}_\rho(n)$ е подалгебра од $\mathbf{T}_\rho(\mathbb{N})$ генерирана од $v_0, \ldots, v_{n-1}$. Потоа, $\mathbf{T}_\rho(\mathbb{N}) = \bigcup_{n\in\mathbb{N}} \mathbf{T}_\rho(n)$ и $\mathbf{T}_\rho(1) \subseteq \mathbf{T}_\rho(2) \subseteq \ldots$.

Дефиниција 19 Нека $\mathbf{A}$ е алгебра од тип ρ и $p \in \mathbf{T}_\rho(n)$. Дефинираме n-арна операција p^A на A со индукција по должината на p. Ако $p = v_i$, ставаме $p^A(a_0, \ldots, a_{n-1}) = a_i$. Ако q^A е дефинирано за сите терми q со должина помала од p, и ако $p = Q(p_1, \ldots, p_{m-1})$, каде Q е m-арен операциски симбол, тогаш ставаме

$$p^A(a_0, \ldots, a_{n-1}) = Q^A(p_0^A(a_0, \ldots, a_{n-1}), \ldots, p_{m-1}^A(a_0, \ldots, a_{n-1})).$$

$\triangle$

Дефиниција 20 *Идентитет* или *равенство* од тип ρ е збор од облик $p \approx q$ каде p и q се ρ- терми. $\triangle$

Нека $\mathbf{A}$ е алгебра и $p \approx q$ е идентитет (и двете од тип ρ) и нека $p, q \in \mathbf{T}_\rho(n)$. Ако $\bar{a} \in A^n$, тогаш велиме дека $\bar{a}$ *го задоволува* $p \approx q$ ако и само ако $p^A(\bar{a}) = q^A(\bar{a})$. Означуваме $\mathbf{A}, \bar{a} \models p \approx q$.

Велиме дека идентитетот $p \approx q$ *е вистинит* во $\mathbf{A}$ ако и само ако $p^A = q^A$. Означуваме $\mathbf{A} \models p \approx q$.

Велиме дека идентитетот $p \approx q$ *е вистинит во класа* $\mathcal{K}$ од тип ρ ако и само ако е вистинит во секој член на $\mathcal{K}$. Означуваме $\mathcal{K} \models p \approx q$.

Ако Σ е множество идентитети од тип ρ и $\mathcal{K}$ е класа алгебри од тип ρ, велиме дека Σ е вистинито во $\mathcal{K}$, ознака $\mathcal{K} \models \Sigma$, ако и само ако секој елемент на Σ е вистинит во $\mathcal{K}$.

Својство 6 Нека $\mathbf{A}$ е алгебра и $p \approx q$ е идентитет (и двете од тип ρ). Следните услови се еквивалентни.

(i) $\mathbf{A} \models p \approx q$.

(ii) Ако $p, q \in \mathbf{T}_\rho(n)$, тогаш $\mathbf{A}, \bar{a} \models p \approx q$ за секој $\bar{a} \in A^n$.

(iii) За секој хомоморфизам f од $\mathbf{T}_\rho(\mathbb{N})$ во $\mathbf{A}$ важи $f(p) = f(q)$.

(iv) Ако $p, q \in \mathbf{T}_\rho(n)$ и $x_0, \ldots, x_{n-1}$ се n различни променливи, тогаш $\mathbf{A} \models p(x_0, \ldots, x_{n-1}) \approx q(x_0, \ldots, x_{n-1})$. $\square$

Теорема 4 Нека $\mathcal{K}$ е класа алгебри од тип ρ, нека $p, q \in \mathbf{T}_\rho(n)$, нека X е множество и $x_0, \ldots, x_{n-1} \in X$. Следните услови се еквивалентни:

(i) $\mathcal{K} \models p \approx q$.

(ii) $< p, q >$ припаѓа во конгруенцијата $\Theta(\mathcal{K})$ на $\mathbf{T}_\rho(\mathbb{N})$.

(iii) Ако $\mathbf{F}_\mathcal{K}(X)$ постои, тогаш $\mathbf{F}_\mathcal{K}(X) \models p \approx q$.

(iv) Ако $\mathbf{F}_\mathcal{K}(X)$ постои, тогаш $p^{\mathbf{F}_\mathcal{K}(X)}(x_0, \ldots, x_{n-1}) = q^{\mathbf{F}_\mathcal{K}(X)}(x_0, \ldots, x_{n-1})$.

$\square$

Својство 7 Нека $\mathcal{K}$ е класа алгебри од исти тип. Множествата идентитети вистинити во класите $\mathcal{K}$, $\mathbf{H}(\mathcal{K})$, $\mathbf{S}(\mathcal{K})$, $\mathbf{P}(\mathcal{K})$, $\mathbf{V}(\mathcal{K})$ се еднакви.

$\square$

Дефиниција 21 Нека $\mathcal{K}$ е класа алгебри од тип ρ и Σ е множество идентитети од тип ρ. Означуваме $\Theta(\mathcal{K}) = \{p \approx q |\ \mathcal{K} \models p \approx q\}$ и $\mathbf{Mod}(\Sigma) = \{\mathbf{A}|\ \mathbf{A} \models \Sigma\}$. $\triangle$

Класата $\mathcal{K}$ се нарекува *еднаквосӣна класа* ако и само ако $\mathcal{K} = \mathbf{Mod}(\Gamma)$ за некое множество идентитети Γ. Кога ова важи велиме дека $\mathcal{K}$ е *дефинирана* или *аксиомаӣизирана* од Γ.

Множеството Σ се нарекува *еднаквосӣна ӣеорија* ако и само ако $\Sigma = \Theta(\mathcal{L})$ за некоја класа алгебри $\mathcal{L}$ од тип ρ. Кога ова важи Σ се вика *еднаквосӣна ӣеорија на* $\mathcal{L}$.

Својство 8 Нека $\mathcal{K}$ е класа алгебри од тип ρ, $\mathbf{A}$ е алгебра од истиот тип и X е множество такво што $|X| \geq |A|$.

(i) Ако $\mathcal{K}$ се состои од тривијални алгебри, тогаш $\mathbf{A} \models \Theta(\mathcal{K})$ ако и само ако $|A| = 1$.

(ii) Ако $\mathcal{K}$ содржи нетривијална алгебра, тогаш $\mathbf{A} \models \Theta(\mathcal{K})$ ако и само ако $\mathbf{A} \in \mathbf{H}(\mathbf{F}_{\mathcal{K}}(X))$. $\square$

Теорема 5 (G. Birkhoff)

За секоја класа $\mathcal{K}$ од слични алгебри, $\mathbf{HSP}(\mathcal{K}) = \mathbf{Mod}\Theta(\mathcal{K})$. (Значи, $\mathcal{K}$ е многуобразие ако и само ако е еднаквостна класа.) $\square$

Својство 9 Ако $\mathcal{V}$ е многуобразие кое содржи нетривијална алгебра и X е множество кое е најмалку преброиво, тогаш $\mathcal{V} = \mathbf{V}(\mathbf{F}_{\mathcal{V}}(X))$. $\square$

Значи, нека $\mathcal{V}$ е многуобразие од тип ρ кое содржи нетривијални алгебри. $\mathcal{V}$ е генерирано од својата слободна алгебра $\mathbf{F}_{\mathcal{V}}(\omega)$, која може да се конструира како фактор алгебра на $\mathbf{T}_{\rho}(\mathbb{N})$. Два терми p и q се во иста класа во фактор структурата ако и само ако идентитетот $p \approx q$ е вистинит во $\mathcal{V}$. Така, еднаквостната теорија на $\mathcal{V}$ ја определува $\mathbf{F}_{\mathcal{V}}(\omega)$ и самото $\mathcal{V}$ може да се дефинира како класата од сите модели на својата еднаквостна теорија. Слично, конечно генерирана слободна алгебра $\mathbf{F}_{\mathcal{V}}(n), n \in \mathbb{N}$, е фактор алгебра на $\mathbf{T}_{\rho}(n)$ и два n-арни терми p и q се идентификуваат во $\mathbf{F}_{\mathcal{V}}(n)$ ако и само ако термовските операции p^A и q^A се еднакви за секоја $\mathbf{A} \in \mathcal{V}$.

Конструктивен опис на слободните алгебри во многуобразие $\mathcal{V}$ е исто што и конструктивен опис на конгруенцијата $\Theta(\mathcal{V})$ на $\mathbf{T}_{\rho}(\mathbb{N})$ за која $\mathbf{F}_{\mathcal{V}}(\omega) \cong \mathbf{T}_{\rho}(\mathbb{N})/\Theta(\mathcal{V})$ или пак на еднаквостната теорија на $\mathcal{V}$, бидејќи $< p, q > \in \Theta(\mathcal{V})$ ако и само ако $p \approx q \in \Theta(\mathcal{V})$. Еден пристап за описот на слободните алгебри е определување на подмножество од $\mathbf{T}_{\rho}(\mathbb{N})$ составено точно од по еден елемент од секоја класа на еквивалентност. Елементите од такво множество често се нарекуваат *редуцирани терми* или *нормални форми*. Се обидуваме да определиме алгоритам кој за секој терм го определува единствениот редуциран терм, еквивалентен на него. Ако ваков алгоритам постои, тој веднаш води кон дефиниција на операциите на множеството редуцирани терми, при кои ова множество станува алгебра изоморфна на $\mathbf{F}_{\mathcal{V}}(\omega)$.

Тоа е направено за многуобразието слупи во петтиот дел на трудот.

2.2 Проблем на зборови и други проблеми на одлучивост за алгебрите

Во овој дел го дефинираме проблемот на зборови, давајќи претходно неколку неопходни дефиниции во врска со презентациите на алгебрите. Дефинициите на поимите и теоремите се според [13]. Притоа, секаде ќе ги користиме следниве ознаки. Ако I е сигнатура од тип ρ, $\mathbf{A}$ е алгебра од тип ρ и G е подмножество од носителот на $\mathbf{A}$, со ρ' ќе го означуваме рангот на $I \cup G$ (при општа претпоставка $I \cap G = \emptyset$), т.е. на сигнатурата се додаваат како нови константи (нуларни операции) елементите од G. Потоа, со $\mathbf{A}_G$ ќе ја означуваме алгебрата која настанува од $\mathbf{A}$, додавајќи само уште основни нуларни операции од G.

Дефиниција 22 Нека R е множество идентитети од тип ρ', во сигнатура $I \cup G$. Подредениот пар (G, R) е *презентација* од тип ρ' во сигнатура $I \cup G$. Една презентација (G, R) е *конечна* ако и G и R се конечни множество. $\triangle$

Дефиниција 23 Нека Θ е множество идентитети од тип ρ, $\mathcal{V} = \mathbf{Mod}(\Theta)$ и нека (G, R) е презентација од тип ρ'. Алгебра $\mathbf{A}$ од тип ρ *е презентирана* од (G, R) во $\mathcal{V}$, ако важат следниве услови:

(i) $\mathbf{A} = S_g^A(G)$;

(ii) $\mathbf{A}_G \models \Theta \cup R$; и

(iii) За секој идентитет без променливи $p \approx q$ од тип ρ', од $\mathbf{A}_G \models p \approx q$ следува $\Theta \cup R \models p \approx q$. $\triangle$

За една алгебра велиме дека е *конечно презентирана*, ако е презентирана со конечна презентација.

Алгебра презентирана со (G, R) во $\mathcal{V}$ е единствена до изоморфизам.

Нека (G, R) е презентација од тип ρ', Θ е множество идентитети од тип ρ и $\bar{\mathcal{V}}$ е многуобразието дефинирано со $\Theta \cup R$. Тогаш редуктот до тип ρ (од сигнатурата отстранети нуларните операции од G) на слободната алгебра $\mathbf{F}_{\bar{\mathcal{V}}}(0)$ е алгебра презентирана со (G, R) во $\mathcal{V}$.

Дефиниција 24 Нека Θ е множество идентитети од тип ρ, $\mathcal{V} = \mathbf{Mod}(\Theta)$ и $\mathbf{A}$ е алгебра конечно презентирана со (G, R) во $\mathcal{V}$. *Проблемот на зборови* за $\mathbf{A}$ во $\mathcal{V}$ прашува дали постои алгоритам кој одлучува за произволен идентитет $p \approx q$ од тип ρ', без променливи, дали $\mathbf{A}_G \models p \approx q$ или не. $\triangle$

Ако ваков алгоритам постои велиме дека проблемот на зборови за $\mathbf{A}$ е *решлив*, инаку е *нерешлив*.

Дефиниција 25 Нека Θ е множество идентитети од тип ρ и $\mathcal{V} = \mathbf{Mod}(\Theta)$.

Проблем на зборови за $\mathcal{V}$ на прво ниво $(WP1)$ е прашањето дали постои алгоритам кој го решава проблемот на зборови за сите конечно презентирани алгебри во $\mathcal{V}$.

Проблем на зборови за $\mathcal{V}$ на второ ниво $(WP2)$ е прашањето дали за секоја конечно презентирана алгебра $\mathbf{A}$ во $\mathcal{V}$, постои алгоритам кој го решава проблемот на зборови за $\mathbf{A}$ во $\mathcal{V}$. $\triangle$

Јасно е дека решливоста на проблемот на зборови на прво ниво, за некое многуобразие, повлекува решливост и на второ ниво.

Како што веќе споменавме во воведот, пред развитокот на теоријата на пресметливост поимот алгоритамски нерешлив проблем, па и нерешлив проблем на зборови не бил познат. Во 1947 Марков и Post докажале дека проблемот на зборови за полугрупите е нерешлив (на второ ниво, а со тоа и на прво). Доказот на тоа тврдење е детално разработен во вториот дел на трудот. Во 1955 Boone и Новиков докажале исто за многуобразието групи, а Hutchinson и Lipshitz за модуларните мрежи.

За преглед ја даваме следнава табела (според [13]).

Нерешлив $WP1$	Решлив $WP1$
групи	Абелови групи квазигрупи
прстени	комутативни прстени неасоцијативни прстени
полугрупи	комутативни полугрупи
модуларни мрежи	мрежи

Во трудот нема да се задржуваме на докажување на сите резултати наведени во овој преглед. Интересно е како додавањето на комутативниот закон влијае на решливоста на проблемот на зборови, и одземањето на асоцијативниот исто така. Во последниот ред од табелата не е содржана никаква контрадикција. Постои конечно презентирана модуларна мрежа во многуобразието модуларни мрежи со нережлив проблем на зборови која не е конечно презентирана во многуобразието мрежи.

Да споменеме дека решливост на $WP2$ не повлекува решливост на $WP1$, но ова тврдење е далеку од едноставно да се докаже.

Пример 1 (Wells, според [13])

Нека $\mathcal{V}$ е многуобразие со една нуларна операција 0, една бинарна $\cdot$ и преброиво многу унарни операции $h_n,\ n \in \mathbb{N}$, кое е дефинирано со следниве идентитети:

$$x \cdot y \approx y \cdot x,\ x \cdot (y \cdot z) \approx (x \cdot y) \cdot z, x \cdot 0 \approx 0,\ x \cdot x \approx 0,$$

$$x \cdot h_n(y) \approx 0,\ h_n(h_n(x)) \approx h_n(x),\ n \in \mathbb{N},$$

$$h_n(h_k(x)) \approx 0,\ n \neq k,\ \ n, k \in \mathbb{N},$$

$$h^n_{m_n}(x_1 \cdot x_2 \cdot \cdots \cdot x_{m_n}) \approx 0,$$

каде $\{m_n | n \in \mathbb{N}\}$ е некое рекурзивно набројување на некое нерекурзивно множество X. Тогаш $\mathcal{V}$ има решлив $WP2$, а нерешлив $WP1$.

Друг проблем на одлучивост за алгебрите е таканаречениот *проблем на еднаквостна теорија* кој, според дефиницијата, е тесно поврзан со проблемот на зборови.

Дефиниција 26 Нека $\mathcal{V}$ е многуобразие алгебри од тип ρ. Проблем на еднаквостна теорија за $\mathcal{V}$ е проблемот на одлучивост на јазикот $Eq(\mathcal{V}) = \{p \approx q |\ \mathcal{V} \models p \approx q,\ p \approx q$ е идентитет од тип $\rho\}$. △

Нека Θ е множество идентитети од тип ρ и $\mathcal{V}$ е многуобразието дефинирано со Θ. Нека $\mathbf{A}$ е алгебра презентирана со $(G, \emptyset)$ во $\mathcal{V}$, каде G е преброиво множество од (нови) константи. Јасно, $\mathbf{A}$ не е конечно презентирана, но ако проблемот на зборови го дефинираме за $\mathbf{A}$ аналогно како за конечно презентирана алгебра од $\mathcal{V}$, тогаш проблемот на зборови за $\mathbf{A}$ во $\mathcal{V}$ е еквивалентен на проблемот на одлучивост на еднаквостната теорија за $\mathcal{V}$. Бидејќи вака дефинираната алгебра $\mathbf{A}$ е изоморфна на $\mathbf{F}_{\mathcal{V}}(\omega)$, често проблемот на еднаквостна теорија за $\mathcal{V}$ се нарекува и *проблем на зборови за слободните објекти во* $\mathcal{V}$.

Да се задржиме на врските помеѓу проблемот на зборови за едно многуобразие и проблемот на еднаквостна теорија. Во општ случај од нерешливоста на проблемот на зборови на прво или на второ ниво за многуобразие $\mathcal{V}$ не следува неодлучивост на еднаквостната теорија за $\mathcal{V}$. Пример за ова е многуобразието групи во кое $WP1$ и $WP2$ се нерешливи но еднаквостната теорија е одлучива - препишувачки систем на Knuth и Bendix наведен во воведот.

Исто така, во општ случај, неодлучивост на еднаквостната теорија на некое многуобразие не повлекува неодлучивост на $WP2$ за истото многуобразие, што и се очекува од дефиницијата, бидејќи неодлучива еднаквостна теорија значи дека проблемот на зборови е нерешлив за $\mathbf{F}_{\mathcal{V}}(\omega)$, но оваа алгебра не е конечно презентирана во $\mathcal{V}$. Пример за тоа е многуобразието од *Пример 1* кое има неодлучива еднаквостна теорија ([13]).

Она што важи е дека решливост на $WP1$ за дадено многубразие повлекува одлучивост на еднаквостната теорија за истото. Доказот на ова тврдење е доста сложен, истиот може да се најде во [13]. Овде даваме само преглед на некои поими и својства од кои истото следува, а кои се интересни и сами по себе.

Дефиниција 27 Нека $\mathcal{K}$ е класа модели на јазик од прв ред $\mathcal{L}$. Велиме дека *елементарната теорија на* $\mathcal{K}$ е одлучива ако е одлучиво множеството $Th(\mathcal{K}) = \{\phi |\ \mathcal{K} \models \phi,\ \phi$ е формула во јазикот $\mathcal{L}\}$. $\triangle$

Јасно, одлучивост на елементарната теорија повлекува одлучивост на еднаквостната теорија за некое многуобразие.

Ако $\mathcal{V}$ е многуобразие, тогаш , според теоремата на Birkhoff, тоа е класа модели на множество идентитети на јазик од прв ред со равенство кој нема предикатни симболи, па, според тоа, може да зборуваме за одлучивост на елементарната теорија на $\mathcal{V}$.

Дефиниција 28 Ако $p_1 \approx q_1, \ldots, p_n \approx q_n, p \approx q$ се идентитети од тип ρ во сигнатура I, тогаш формулата $p_1 \approx q_1 \wedge \cdots \wedge p_n \approx q_n \implies p \approx q$ е *квази-идентитет од тип* ρ (во сигнатура I). $\triangle$

Нека $\mathcal{V}$ е многуобразие од тип ρ. Велиме дека *проблемот на квази-идентитети* на $\mathcal{V}$ е одлучив ако е одлучиво множеството $Q(\mathcal{V}) = \{q |\ \mathcal{V} \models q,\ q$ е квази-идентитет од тип $\rho\}$.

Теорема 6 Нека $\mathcal{V}$ е многуобразие. Проблемот на квази-идентитети за $\mathcal{V}$ е еквивалентен со $WP1$ за $\mathcal{V}$. $\square$

Тврдењето искажано со претходната теорема е интересно, бидејќи со тоа проблемот на зборови на прво ниво за некое многуобразие директно се сведува на проблем на одлучивост на одредено множество. Исто така, од ова тврдење следува дека одлучивост на $WP1$ за некое многуобразие повлекува одлучивост на еднаквостна теорија на истото, бидејќи $\mathcal{K} \models p \approx q$ ако и само ако $\mathcal{K} \models p \approx p \implies p \approx q$.

Последица 2 За секое многуобразие $\mathcal{V}$ неодлучивост на $WP1$ имплицира неодлучивост на неговата елементарна теорија. $\square$

2.3 Резултати на Evans за одлучивост на $WP1$

Во овој дел се задржуваме на неколку теореми на Evans ([5, 6, 7, 8]) кои даваат битни критериуми за решливост на проблемот на зборови на прво ниво за произволно многуобразие.

Нека $\mathcal{V}$ е многуобразие алгебри од тип ρ. Со $\mathcal{V}_\rho$ го означуваме многуобразието од сите алгебри од тип ρ.

Дефиниција 29 Нека P е множество. *Делумна операција* на P со ранг r е пресликување $f : D \to P$, каде $D \subseteq P^r$ е *домен* на на f.

Нека I е индексно множество од тип ρ. *Делумна* или *некомплетна* $\mathcal{V}_\rho$ - алгебра е тројка $\mathbf{P} =< P, F, \mathcal{S} >$, каде P е множество, F е множество делумни операции, интерпретации на операциските симболи од I, и $\mathcal{S}$ е фамилија множества од P, индексирана со I, т.е. S_Q е доменот на делумната операција $Q^P \in F$. $\triangle$

Дефиниција 30 *Делумна* или *некомплетна* $\mathcal{V}$-алгебра е делумна $\mathcal{V}_\rho$-алгебра $\mathbf{P} =< P, F, \mathcal{S} >$ за која важи:

(1) Кога идентитетите на $\mathcal{V}$ се применливи на $\mathbf{P}$, тие се задоволени во $\mathbf{P}$, односно, ако $p \approx q$ е идентитет од $\mathcal{V}$, каде $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n)$ и $a_1, \ldots, a_n$ се елементи од P за кои делумните операции дозволуваат да се пресметаат вредностите на $p^P(a_1, \ldots, a_n)$ и $q^P(a_1, \ldots, a_n)$, тогаш $p^P(a_1, \ldots, a_n) = q^P(a_1, \ldots, a_n)$.

(2) Делумните операции на $\mathbf{P}$ и идентитетите на $\mathcal{V}$ не дозволуваат зголемување на доменот на делумните операции, односно, ако $p \approx q$ е идентитет во $\mathcal{V}$ каде $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n)$ и, од друга страна, $q = Q(r_1, \ldots, r_m), Q \in I$ и $a_1, \ldots a_n$ се елементи од P за кои се дефинирани вредностите на $p^P(a_1, \ldots, a_n)$ и $r_i^P(a_1, \ldots, a_n)$, за $1 \leq i \leq m$, тогаш и $Q^P(r_1^P(a_1, \ldots, a_n), \ldots, r_m^P(a_1, \ldots, a_n))$ има дефинирана вредност во $\mathbf{P}$ и важи $Q^P(r_1^P(a_1, \ldots, a_n), \ldots, r_m^P(a_1, \ldots, a_n)) = p^P(a_1, \ldots, a_n)$. $\triangle$

Дефиниција 31 Една делумна $\mathcal{V}$-алгебра $\mathbf{P} =< P, F, \mathcal{S} >$ е *сместлива* во $\mathcal{V}$-алгебра $\mathbf{A}$, ако постои инјекција $f : P \to A$, така што за секој операциски симбол Q од сигнатурата на $\mathbf{P}$, $f \circ Q^P = Q^A | f(S_Q)$. $\triangle$

Бидејќи секогаш може да работиме со минималната подалгебра од $\mathcal{V}$-алгебра $\mathbf{A}$ во која се сместува делумна $\mathcal{V}$ алгебра $\mathbf{P}$, без губење општост може да сметаме дека $\mathbf{A}$ е генерирана од $f(P)$, а и дека е генерирана од P.

Лема 1 Нека $\mathbf{P}$ е делумна $\mathcal{V}$-алгебра. Нека $\mathbf{A}$ е $\mathcal{V}$ алгебра презентирана со (P, R), каде $R = \{Q^A(a_{i_1}, \ldots, a_{i_r}) \approx a_t | \ \rho(Q) = r, < a_{i_1}, \ldots, a_{i_r} > \in S_Q, Q^P(a_{i_1}, \ldots, a_{i_r}) = a_t\}$. Тогаш ако постои сместување на $\mathbf{P}$ во $\mathcal{V}$-алгебра, постои сместување на $\mathbf{P}$ во $\mathbf{A}$ и секоја $\mathcal{V}$-алгебра во која може да се смести $\mathbf{P}$ е хомоморфна слика на $\mathbf{A}$.

Доказ. Нека $\mathbf{B}$ е произволна $\mathcal{V}$ алгебра во која се сместува $\mathbf{P}$. Имаме $\mathbf{B} \cong \mathcal{T}_\rho(P)/\beta$ и $\mathbf{A} \cong \mathcal{T}_\rho(P)/\alpha$ каде $\alpha \in \mathbf{C}on\mathcal{T}_\rho(P)$ и α е генерирана од идентитетите на $\mathcal{V}$ и дефинирачките релации од R. Од инјективноста на сместувањето $i \neq j \implies i/\beta \neq j/\beta$. Потоа $\alpha \subseteq \beta$ од дефинирачките равенства на $\mathbf{A}$ и од тоа што $\mathbf{P}$ е сместена во $\mathbf{B}$. Пресликувањето $\phi : \mathcal{T}_\rho(P)/\alpha \to \mathcal{T}_\rho(P)/\beta$ определено со $\phi(u/\alpha) = u/\beta$ е хомоморфизам од $\mathbf{A}$ во $\mathbf{B}$. Пресликувањето $i \mapsto i/\alpha$ е сместување на $\mathbf{P}$ во $\mathbf{A}$. Имено, за секоја делумна операција Q^P на $\mathbf{P}$ со ранг r и секој $< i_1, \ldots, i_r > \in S_Q$ имаме $Q^P(i_1, \ldots, i_r) = s \mapsto s/\alpha = Q^{\mathcal{T}_\rho(J)/\alpha}(i_1/\alpha, \ldots, i_r/\alpha)$ и $i/\alpha = j/\alpha$ повлекува $i/\beta = j/\beta$ од каде $i = j$. $\square$

Дефиниција 32 $\mathcal{V}$-алгебра $\mathbf{A}$ од тип ρ и индексно множество I, презентирана со $(G, R), G = \{a_i | \; i \in J\}$, е *е дефинирана со затворен систем од релации* ако:

(1) Секоја релација од R е од облик $Q^A(a_{i_1}, \ldots, a_{i_r}) \approx a_t$, каде Q е операциски симбол со ранг r.

(2) Системот $\mathbf{P} =< G, F_I, \mathcal{S}_I >$, каде $< a_{i_1}, \ldots, a_{i_r} > \in S_Q$ ако и само ако $Q^A(a_{i_1}, \ldots, a_{i_r}) \approx a_t \in R$ и тогаш $Q^P(a_{i_1}, \ldots, a_{i_r}) = a_t$, е делумна $\mathcal{V}$-алгебра. (Притоа $\mathbf{P}$ е *делумна алгебра соодветна на* $\mathbf{A}$.) $\triangle$

Лема 2 Нека $\mathcal{V}$ е многуобразие со својството дека секоја делумна $\mathcal{V}$-алгебра може да се смести во $\mathcal{V}$-алгебра. Ако $\mathbf{A}$ е $\mathcal{V}$-алгебра презентирана со (G, R), каде R е затворен систем дефинирачки релации, тогаш ниедни два генераторни елементи од G не се еквивалентни во $\mathbf{A}$.

Доказ. Нека $\mathbf{A}$ е дефинирана со затворен систем дефинирачки релации. Тогаш $\mathbf{A} \cong \mathcal{T}_\rho(G)/\alpha$. Нека $\mathbf{P}$ е делумна $\mathcal{V}$ алгебра соодветна на $\mathbf{A}$. Од

Лема 1 пресликувањето $i \mapsto i/\alpha, i \in G$ е сместување на $\mathbf{P}$ во $\mathbf{A}$. Од инјективноста следува тврдењето. $\square$

Теорема 7 Нека $\mathcal{V}$ е многуобразие алгебри со својството дека секоја (конечна) делумна $\mathcal{V}$-алгебра може да се смести во $\mathcal{V}$-алгебра. Тогаш $WP1$ е решлив за $\mathcal{V}$.

Доказ Нека $\mathcal{V}$ е многуобразие со својството дека секоја делумна $\mathcal{V}$-алгебра може да се смести во $\mathcal{V}$ алгебра и нека $\mathbf{A}$ е конечно презентирана $\mathcal{V}$ алгебра со презентација (G_A, R). Јасно, $\mathbf{A} \cong \mathcal{T}_\rho(G_A)/\alpha$ каде $\alpha \in \mathbf{C}on\mathcal{T}_\rho(G_A)$ и α е генерирана од идентитетите на $\mathcal{V}$ и дефинирачките релации од R. Нека $u, v \in \mathcal{T}_\rho(G_A)$. Ќе конструираме $\mathcal{V}$ алгебра $\mathbf{B}$ дефинирана со затворен систем дефинирачки релации т.ш. $\mathbf{B} \cong \mathbf{A}$. Алгебрата $\mathbf{B}$ ќе има презентација (G_B, C_B) т.е. $\mathbf{B} \cong \mathcal{T}_\rho(G_B)/\beta$ каде $\beta \in \mathbf{C}on\mathcal{T}_\rho(G_B), \beta$ е генерирана од C_B. Притоа при изоморфизмот u/α и v/α ќе соодветствуваат на g_1/β и g_2/β соодветно, за некои генератори $g_1, g_2 \in G_B$. Тогаш од *Лема 2* и од изоморфизмот се добива $g_1 = g_2$ ако и само ако $u/\alpha = v/\alpha$. Ги конструираме G_B и C_B на следниот начин. Со индукција по сложеност на терми, дефинираме пресликување $P : \mathcal{T}_\rho(G_A) \to \mathcal{B}(\mathcal{T}_\rho(G_A)$ со:

$$P(t) := \begin{cases} \{t\} & t \in G_A \\ \{t\} \cup P(t_1) \cup \cdots \cup P(t_r) & t = Q(t_1, \ldots, t_r) \end{cases}$$

Нека

$$X = P(u) \cup P(v) \cup (\bigcup_{i=1}^{q} P(l_i)) \cup (\bigcup_{i=1}^{q} P(r_i)))$$

каде $R = \{l_i \approx r_i | i = 1, \dots, q\}$.

X е конечно множество, нека $|X| = n$ и нека $G'_B = \{b_1, \dots, b_n\}$ е множество т.ш. $G'_B \cap X = \emptyset$ и $b : X \to G'_B$ е биекција, при која $b_1 = b(u), b_2 = b(v)$. Ставаме

$$R_B = \{Q(b_{i_1}, \dots, b_{i_r}) \approx b_t | b_t = b(Q(t_{i_1}, \dots, t_{i_r})), b(t_{i_j}) = b_{i_j}, j = 1, \dots, r\}$$
$$\cup \{b_s \approx b_t | b_s = b(l_i), b_t = b(r_i), l_i \approx r_i \in R\}.$$

Тогаш алгебрата $\mathbf{B}$ презентирана со (G'_B, R_B) е изоморфна со $\mathbf{A}$. Имено, $\mathbf{B} \cong \mathcal{T}_\rho(G_B)/\beta$, за $\beta \in \mathbf{C}on\mathcal{T}_\rho(G_B)$, β е генерирана од идентитетите на $\mathcal{V}$ и дефинирачките релации од R_B. Пресликувањето $u/\alpha \mapsto b'(u)/\beta$ за секој $u \in \mathcal{T}_\rho(G_B)$ каде $b'(u) = b(u)$ за $u \in X$ и $b'(u) = Q^{\mathcal{T}_\rho(G_B)}(b'(t_1), \dots, b'(t_r))$ ако $u \notin X, u = Q^{\mathcal{T}_\rho(G_A)}(t_1, \dots, t_r)$ е изоморфизам од $\mathbf{A}$ во $\mathbf{B}$. Да забележиме дека може да сметаме дека $G_A \subseteq X$ од аспект на проблемот на зборови, бидејќи $\mathbf{A} \models u \approx v$ ако и само ако $u \approx v$ е вистинит во алгебрата презентирана со (G'_A, R) каде $G'_A = G_A \cap X$, а со тоа и горното пресликување е добро дефинирано.

Со постапката наведена во продолжение од G'_B и R_B формираме $G_B \subseteq G'_B$ и затворен систем дефинирачки релации C_B така што (G_B, C_B) е повторно презентација на $\mathbf{B}$. Постапката се состои од:

I. **Отстранување генератори и релации.** Ако $b_s \approx b_t$ е дефинирачка релација при $s < t$, истата ја отстрануваме од множеството дефинирачки релации, го отстрануваме b_t одмножеството генератори и во сите останати релации секое појавување на b_t го заменуваме со b_s.

II. **Додавање релации.** Постојат три случаи:

1. Ако постојат две релации $Q_1(b_{i_1}, \ldots, b_{i_r}) \approx b_s$ и $Q_1(b_{i_1}, \ldots, b_{i_r}) \approx b_t$ при $s \neq t$, додаваме релација $b_s \approx b_t$.

2. Ако за некоја замена на генератори на место на променливи во аксиома $p \approx q$ од $\mathcal{V}$ на двата добиени збора (лева и десна страна) може да им се додели вредност b_s и b_t соодветно при $s \neq t$, додаваме релација $b_s \approx b_t$.

3. Ако $p \approx q$ е аксиома на $\mathcal{V}$ каде $q = Q(q_1, \ldots, q_r)$ и ако за некоја замена на генератори на место на променливи во p може да се додели вредност b_s, а во $q_1, \ldots, q_r$ може да се доделат соодветно вредности $b_{i_1}, \ldots, b_{i_r}$ додаваме релација $Q(b_{i_1}, \ldots, b_{i_r}) \approx b_s$.

Потребен и доволен услов за едно множество дефинирачки релации да претставува затворен систем е примена на $I.$ и $II.$ да не го менува.

Ги применуваме $I.$ и $II.$ на генераторите и дефинирачките релации на B. Она што се добива со примена на $I.$ или $II.$ повторно е презентација на B. Исто така B е конечно презентирана па по конечен број чекори се добива конечна презентација на B со затворен систем дефинирачки релации. Имено, со $I.$ се намалува бројот на генератори и дефинирачки релации, $II1$ намалува генератори и дефинирачки релации при следна примена на $I.$ Бидејќи $\mathcal{V}$ е дефинирано со конечно можество идентитети со $II2$ и $II3$ евентуално се додаваат конечно многу нови релации. Генераторот b_1 секогаш останува во множеството генератори, по конечна последователна примена на I и II се добива некое множество дефинирачки релации во кои нема релации од облик $b_s \approx b_t, s \neq t$. Тогаш веќе со I и II не се добива ништо ново и дефинирачките релации формираат затворен систем. Останатото множество генератори го означуваме со G_B, а множеството дефинирачки релации со C_B.

Според претходно направената дискусија, ако $b_2 \in G_B$ тогаш $\mathbf{A} \models u \approx v$, инаку u и v не се еквивалентни во $\mathbf{A}$. $\square$

Со примена на оваа теорема се добива решливост на WPI за многу многуобразија алгебри, како што се многуобразието лупи од тип $< 2, 2, 2 >$ (G.E. Bates, G. Birkhoff) и многуобразието мрежи - како последица од теорема на G. Birkhoff според која секое делумно подредено множество може да се смести во мрежа така што сите инфимуми и супремуми во подреденото множество се запазени во мрежата. Во четвртиот дел на трудот, користејќи ја претходната теорема на Evans, докажуваме дека проблемот на зборови е решлив за многуобразието слупи од тип $< 2, 0 >$.

Дефиниција 33 *Проблемот на сместување* е решлив за многуобразие $\mathcal{V}$ ако е одлучиво дали секоја конечна делумна $\mathcal{V}$-алгебра може да се смести во $\mathcal{V}$-алгебра. $\triangle$

Теорема 8 Проблемот на сместување е решлив за многуобразие $\mathcal{V}$ ако и само ако $WP1$ е решлив за $\mathcal{V}$.

Доказ Нека WPI е решлив за $\mathcal{V}$ и нека $\mathbf{P}$ е конечна делумна $\mathcal{V}$-алгебра. Од *Лема 1* ако постои сместување на $\mathbf{P}$ во некоја $\mathcal{V}$-алгебра, постои сместување на $\mathbf{P}$ во $\mathcal{T}_\rho(P)/\alpha$ каде α е конгруенцијата на $\mathcal{T}_\rho(P)$ генерирана од дефинирачки равенства кои соодветствуваат на делумните операции од $\mathbf{P}$ и идентитетите од $\mathcal{V}$. Притоа $\mathcal{T}_\rho(P)/\alpha$ изоморфно ја содржи $\mathbf{P}$ ако и само ако $x/\alpha \neq y/\alpha$ за $x, y \in P, x \neq y$ т.е. $x \not\alpha y$. Значи, бидејќи по претпоствка за произволни два збора $u, v \in \mathcal{T}_\rho$ може да утврдиме дали $u\alpha v$, може да утврдиме и дали $\mathbf{P}$ може да се смести.

Обратно, нека проблемот на сместување е решлив за $\mathcal{V}$. Нека $\mathbf{A}$ е конечно презентирана во $\mathcal{V}$ со (G, R). Нека $u, v \in \mathcal{T}_\rho(G)$ се произволни два збора. Сакаме да утврдиме дали $u\alpha v$ каде α е конгруенцијата на $\mathcal{T}_\rho(G)$ генерирана од идентитетите на $\mathcal{V}$ и дефинирачките равенства од R. Како во доказот на *Теорема 7* конструираме конечно презентирана $\mathcal{V}$ алгебра $\mathbf{B}$ со презентација (G_B, C_B), каде C_B е затворен систем дефинирачки релации која е изоморфна на $\mathbf{A}$, и при овој изоморфизам u/α и v/α соодветствуваат на класи на генератори од $\mathbf{B}$. Нека $\mathbf{P}$ е делумната алгебра соодветна на $\mathbf{B}$ (ваква постои бидејќи $\mathbf{B}$ е дефинирана со затворен систем дефинирачки релации). Во конструкцијата на $\mathbf{B}$ може да се случи u/α и v/α да соодветствуваат на класа на еден (преостанат) генератор. Во овој случај јасно е дека $u\alpha v$. Нека u/α соодветствува на класата на b_1, а v/α на класата на b_2, каде $b_1, b_2 \in G_B, b_1 \neq b_2$. Од *Лема 2* ако $\mathbf{P}$ може да се смести во $\mathcal{V}$-алгебра, тогаш b_1 и b_2 не се еквивалентни во $\mathbf{B}$, па u и v не се еквивалентни во $\mathbf{A}$.

Останува уште случајот кога $\mathbf{P}$ не може да се смести во $\mathcal{V}$-алгебра. Тогаш некои од генераторите на $\mathbf{B}$ се еквивалентни во $\mathbf{B}$. За да утврдиме дали b_1 и b_2 се еквивалентни, конструираме хомоморфни слики на $\mathbf{B}$ на различни начини но секогаш b_1 и b_2 ги оставаме различни. Ако генераторите и дефинирачките релации од овие хомоморфни слики соодветствуваат на делумна $\mathcal{V}$ алгебра која може да се смести, тогаш b_1 и b_2, бидејќи не се еквивалентни во соодветната хомоморфна слика, не се еквивалентни ни во $\mathbf{B}$.

Имено, нека е дадена партиција на генераторите на $\mathbf{B}$, $G_B = G_B^1 \cup \cdots \cup G_B^s$. Нека $\mathbf{B}'$ е $\mathcal{V}$ алгебра со презентација

$$(G_B, C_B \cup \{b_i \approx b_j | (\exists k \in \{1, \ldots, s\} b_i, b_j \in G_B^k\}).$$

На ист начин како во доказот на *Теорема 7* за $\mathbf{B}'$ добиваме затворен систем дефинирачки равенства C'_B, т.е. $\mathbf{B}'$ е презентирана со (G'_B, C'_B). Јасно, во G'_B се наоѓа најмногу по еден генератор од секоја од класите $G_B^1, \ldots, G_B^s$. Всушност ќе има точно по еден од секоја класа (оној со најмал индекс) кога секоја класа од партицијата содржи еквивалентни генератори од $\mathbf{B}$ и ниедни два генератори од различни класи не се еквивалентни во $\mathbf{B}$.

Ако π е една партиција на генераторите на $\mathbf{B}$, тогаш $\mathcal{V}$ алгебрата $\mathbf{B}'$ се нарекува π-хомоморфна слика на $\mathbf{B}$. Притоа важи следното тврдење.

Ако $\mathbf{B}$ е $\mathcal{V}$ алгебра генерирана од $G_B = \{b_1, \ldots, b_m\}$ и дефинирана со затворен систем дефинирачки релации т. ш. b_1 и b_2 не се еквивалентни во $\mathbf{B}$, тогаш постои π - хомоморфна слика $\mathbf{B}'$ на $\mathbf{B}$ која ги содржи b_1 и b_2 меѓу своите нееквивалентни генератори и соодветната делумна алгебра може да се смести.

Навистина, нека π е партиција на G_B при која два генератори се во иста класа ако и само ако се еквивалентни во $\mathbf{B}$. Партицијата има барем две класи (b_1 и b_2 по претпоставка се нееквивалентни). Нека $\mathbf{B}'$ е π - хомоморфна слика на $\mathbf{B}$. Тогаш ниедни два генератори на $\mathbf{B}'$ не се еквивалентни во $\mathbf{B}'$, па соодветната делумна $\mathcal{V}$ алгебра може да се смести.

Значи методот за определување дали генераторите b_1 и b_2 на $\mathbf{B}$ се еквивалентни е следниот: ги разгледуваме сите партиции на генераторите на $\mathbf{B}$. Вакви има конечно многу. По претпоставка одлучиво е дали делумна $\mathcal{V}$ алгебра може да се смести, па може да ги најдеме сите π - хомоморфни слики на $\mathbf{B}$ кои соодветствуваат на делумни алгебри кои можат да се сместат. Ако во некоја од нив b_1 и b_2 се различни генератори, тогаш тие не се еквивалентни во $\mathbf{B}$, инаку се еквивалентни. $\square$

Еден можен начин за одлучување на проблемот на сместување за многуобразие $\mathcal{V}$ е да се докаже дека ако конечна делумна алгебра може да се смести, тогаш таа може да се смести во конечна $\mathcal{V}$-алгебра и да се добие некаква оценка за големината на $\mathcal{V}$-алгебрата која ја содржи. За жал, многу многуобразија го немаат ова својство.

Дефиниција 34 Една алгебра $\mathbf{A}$ е *резидуално конечна* ако за секои $x \neq y \in A$, постои хомоморфизам h од $\mathbf{A}$ на конечна алгебра при кој $h(x) \neq h(y)$. $\triangle$

Дефиниција 35 Една $\mathcal{V}$-алгебра $\mathbf{A}$ има својство на *конечно смес̄тување* ако секоја конечна делумна $\mathcal{V}$-алгебра, содржана во $\mathbf{A}$, може да се смести во конечна $\mathcal{V}$-алгебра.

Едно многуобразие $\mathcal{V}$ има својство на *конечно смес̄тување* ако секоја конечна делумна $\mathcal{V}$-алгебра, која може да се смести, може да се смести во конечна $\mathcal{V}$-алгебра. $\triangle$

Својство 10 Многуобразие $\mathcal{V}$ има својство на конечно сместување ако секоја конечно генерирана алгебра од $\mathcal{V}$ го има истото својство.

Доказ Нека $\mathcal{V}$ е многуобразие во кое секоја конечно генерирана алгебра има својство на конечно сместување и нека $\mathbf{A}$ е $\mathcal{V}$ алгебра и $\mathbf{P}$ е конечна делумна алгебра содржана во $\mathbf{A}$. Нека $\mathbf{B}$ е $\mathcal{V}$ алгебрата во која се сместува $\mathbf{P}$ од *Лема 1*. Алгебрата $\mathbf{B}$ ја содржи $\mathbf{P}$ изоморфно и е конечно генерирана, па по претпоставка $\mathbf{P}$ може конечно да се смести. Добиваме дека $\mathcal{V}$ има својство на конечно сместување. $\square$

Теорема 9 Конечно презентираните алгебри од многуобразие $\mathcal{V}$ се резидуално конечни ако и само ако $\mathcal{V}$ има својство на конечно сместување.

Доказ Нека конечно презентираните алгебри на $\mathcal{V}$ се резидуално конечни. Нека $\mathbf{A}$ е конечно презентирана алгебра на $\mathcal{V}$. Значи $\mathbf{A}$ е резидуално конечна. Нека $\mathbf{P}$ е конечна делумна $\mathcal{V}$ алгебра содржана во $\mathbf{A}$. За секој пар $x, y \in P, x \neq y$, нека $\alpha_{x,y}$ е хомоморфизам од $\mathbf{A}$ во конечна $\mathcal{V}$-алгебра $\mathbf{A}_{x,y}$ т.ш. $\alpha_{x,y}(x) \neq \alpha_{x,y}(y)$. Пресликувањето $h : \mathbf{A} \to \Pi\mathbf{A}_{x,y}$ кое го пресликува секој $a \in \mathbf{A}$ во елемент од $\Pi\mathbf{A}_{x,y}$ со компонента $\alpha_{x,y}(a)$ во $\mathbf{A}_{x,y}$ е хомоморфизам кој е инјективен на P. Множеството $\Pi A_{x,y}$ е конечно, па значи $\mathbf{P}$ е сместена во конечна $\mathcal{V}$-алгебра и од *Својство 10*, $\mathcal{V}$ има својство на конечно сместување.

Обратно, нека $\mathcal{V}$ има својство на конечно сместување и нека $x \neq y$ се два елементи од конечно презентирана алгебра $\mathbf{A}$ во $\mathcal{V}$. Нека $\mathbf{B}$ е алгебрата изоморфна на $\mathbf{A}$ презентирана со затворен систем дефинирачки релации при кој изоморфизам на x и y соодветствуваат различни генераторни елементи од $\mathbf{B}$ (како во доказот на *Теорема 7*). Нека $\mathbf{P}$ е конечната делумна алгебра соодветна на $\mathbf{B}$. По претпоставка постои конечна алгебра **C** во која се сместува **P**. Од *Лема 1*, **C** е хомоморфна слика на **A** и при овој хомоморфизам x и y се пресликуваат во различни елементи од **C** (бидејќи **P** е сместена во **C**). Значи, **A** е резидуално конечна. □

Теорема 10 Ако конечно презентирана алгебра **A** од многуобразие $\mathcal{V}$ е резидуално конечна (или има својство на конечно сместување), тогаш проблемот на зборови е решлив за **A**.

Доказ Нека **A** е конечно презентирана $\mathcal{V}$ алгебра со презентација (G, R). По претпоставка **A** е резидуално конечна. Нека $u, v \in \mathcal{T}_\rho(G)$. Ако u и v не се еквивалентни во **A**, тогаш постои конечна хомоморфна слика на **A** (при хомоморфизам h) во која $h(u), h(v) \in \mathcal{T}_\rho(h(G))$ не се еквивалентни. Би можеле да ги наброиме сите конечни алгебри генерирани со $h(G)$ во кои се задоволени дефинирачките релации од R (соодветни на R всушност) и да проверуваме дали $h(u)$ е еквивалентен со $h(v)$ во секоја ваква. Ако u и v не се еквивалентни во **A** ќе најдеме по конечен број чекори ваква алгебра **B**.

Од друга страна, ако u и v се еквивалентни во **A**, тогаш $u \approx v$ е последица од дефинирачките релации на **A** т.е. $\bigwedge R \implies u \approx v$ може да се докаже во елементарната теорија на $\mathcal{V}$. Може да ги набројуваме и сите последици од дефинирачките релации на **A**. Значи ако $u \approx v$ во **A**, таква формула ќе се појави во нашето набројување.

Со наизменично набројување на конечните $\mathcal{V}$-алгебри и вистинитите $\mathcal{V}$ формули некогаш ќе утврдиме дали u е еквивалентен со v или не, т.е. проблемот на зборови е решлив за **A**. □

Последица 3 Ако $\mathcal{V}$ е многуобразие со својство на конечно сместување, тогаш $WP1$ е решлив за $\mathcal{V}$ (т.е. проблемот на сместување е одлучив за $\mathcal{V}$). $\square$

Претходната теорема повторно дава униформен метод за одлучување решливост на проблемот на зборови за Абеловите групи, лупите, мрежите, квазигрупите, но методот на решавање на истиот е далеку неефикасен.

2.4 Нерешливост на проблемот на зборови

На кратко даваме осврт на докажувањето на неодлучивост на проблемот на зборови, според [13]. Постојат разни методи за истото, но сите тие може да се поделат во две главни групи:

- Директни методи, кои ги користат резултатите за неодлучивост од теоријата на пресметливост.
- Индиректни методи, кои користат сместувања и интерпретации на некои основни неодлучиви многуобразија.

Секако, вторите се појавиле по добивањето на резултати од првите, односно по битните резултати за неодлучивост добиени во теоријата за пресметливост. Во третиот дел се задржуваме на теоријата на пресметливост и на директен доказ за нарешливост на $WP2$, а со тоа и $WP1$ за многуобразието полугрупи.

Својство 11 Ако $\mathcal{V}_1$ и $\mathcal{V}_2$ се класи алгебри такви што:

(i) $\mathcal{V}_1 \subseteq \mathcal{V}_2$,

(ii) секоја алгебра од $\mathcal{V}_2$ може да се смести во некоја алгебра од $\mathcal{V}_1$,

тогаш теориите на квази-идентитети на класите $\mathcal{V}_1$ и $\mathcal{V}_2$ се поклопуваат.

Доказ Од $\mathcal{V}_1 \subseteq \mathcal{V}_2$, имаме $Q(\mathcal{V}_2) \subseteq Q(\mathcal{V}_1)$. Нека $\phi \in Q(\mathcal{V}_1), \phi \notin Q(\mathcal{V}_2)$. Значи постои алгебра $\mathbf{A}$ од $\mathcal{V}_2$ т.ш. $\mathbf{A} \not\models \phi$. Од (ii) постои алгебра $\mathbf{B}$ од $\mathcal{V}_1$ т.ш. $\mathbf{A}$ може да се смести во $\mathbf{B}$. Но, $\mathbf{B} \models \phi$ и ϕ е универзална формула, па мора $\mathbf{A} \models \phi$ што е контрадикција. Значи $Q(\mathcal{V}_2) = Q(\mathcal{V}_1)$. $\square$

Последица 4 Нека $\mathcal{V}_1$ и $\mathcal{V}_2$ се класи алгебри такви што $\mathcal{V}_1 \subseteq \mathcal{V}_2$ и секоја $\mathcal{V}_2$-алгебра може да се смести во некоја $\mathcal{V}_1$-алгебра. Тогаш $WP1$ за $\mathcal{V}_1$ е еквивалентен со $WP1$ за $\mathcal{V}_2$. $\square$

Така, ако $\mathcal{V}_2$ е многуобразието полугрупи и $\mathcal{V}_1$ е некое многуобразие такво што класата од некои редукти на алгебри од $\mathcal{V}_1$ ги задоволува условите од претходната последица, тогаш $\mathcal{V}_1$ има нерешлив $WP1$.

Следната теорема искажува појако тврдење од претходната последица, во случај кога $\mathcal{V}_2$ е многуобразието полугрупи.

Теорема 11 Нека $\mathcal{V}$ е многуобразие од тип ρ, со сигнатура I која содржи бинарна асоцијативна операција $*$. Ако секоја полугрупа може да се смести во $*$ - редукт на некоја алгебра од $\mathcal{V}$, тогаш $WP2$ е нерешлив за $\mathcal{V}$.

Доказ Нека $\mathcal{S}$ е многуобразието од сите полугрупи. $WP2$ е нерешлив за $\mathcal{S}$. Нека $\mathbf{S}$ е конечно презентирана полугрупа, со презентација (G, R), со нерешлив проблем на зборови. Нека Θ е множеството од сите дефинирачки идентитети на $\mathcal{V}$, т.е. $\mathcal{V} = \mathbf{Mod}\Theta$. Нека $\hat{\mathcal{V}}$ е многуобразие во сигнатура $I \cup G$ т.ш. $\hat{\mathcal{V}} = \mathbf{Mod}(\Theta \cup R)$ и $\mathbf{F}_{\hat{\mathcal{V}}}(\emptyset)$ е слободната $\hat{\mathcal{V}}$ алгебра со празно множество генератори. Нека $\mathbf{A}$ е редукт на $\mathbf{F}_{\hat{\mathcal{V}}}(\emptyset)$ до сигнатура I. Ќе докажеме дека $\mathbf{A}$ е конечно презентирана во $\mathcal{V}$ со нерешлив проблем на зборови.

Според *Дефиниција 23*, $\mathbf{A}$ е презентирана со (G, R) во $\mathcal{V}$. Нека претпоставиме дека $\mathbf{A}$ има решлив проблем на зборови т.е. дека постои алгоритам кој за секој идентитет $u \approx v$ без променливи во сигнатура $I \cup G$ одлучува дали $\mathbf{A}_G \models u \approx v$. Тогаш би имале алгоритам и за идентитетите без променливи во сигнатура $\{*\} \cup G$, па проблемот на зборови за $\mathbf{S}$ би бил решлив.

За секој идентитет $u \approx v$ во сигнатура $\{*\} \cup G$ важи:

$$\mathbf{S}_G \models u \approx v \text{ ако и само ако } \mathbf{A}_G \models u \approx v.$$

Навистина, нека $\mathbf{A}_G \models u \approx v$. Тогаш $\mathbf{F}_{\hat{\mathcal{V}}}(\emptyset) \models u \approx v$, па $\hat{\mathcal{V}} \models u \approx v$ и $\Theta \cup R \models u \approx v$. Нека претпоставиме дека $\mathbf{S}_G \not\models u \approx v$. При претпоставките од теоремата $\mathbf{S}$ може да се смести во некоја алгебра $\mathbf{B}$ од $\mathcal{V}$. Ако соодветните елементи на елементите од $G \subseteq S$ ги означиме исто и во $\mathbf{B}$ имаме $\mathbf{B}_G \models R$ и $\mathbf{B}_G \not\models u \approx v$, од каде $\mathbf{B}_G \models \Theta \cup R$ но $\mathbf{B}_G \not\models u \approx v$ што е контрадикција со $\Theta \cup R \models u \approx v$. Обратно, ако $\mathbf{S}_G \models u \approx v$, тогаш од асоцијативноста и од дефинирачките релации на R е последица $u \approx v$, но како асоцијативноста е последица од Θ, се добива $\Theta \cup R \models u \approx v$, од каде следува $\mathbf{A}_G \models u \approx v$. $\square$

Ако се има предвид доказот на претходната теорема јасно е дека важи всушност следното тврдење.

Теорема 12 Нека $\mathcal{V}$ е многуобразие од тип ρ, со сигнатура I која содржи бинарна асоцијативна операција $*$. Ако некоја конечно презентирана полугрупа со нерешлив проблем на зборови може да се смести во $*$ - редукт на некоја алгебра од $\mathcal{V}$, тогаш $WP2$ е нерешлив за $\mathcal{V}$. $\square$

Сепак, ова појако тврдење поретко се употребува, бидејќи нема многу познати примери на конечно презентирани полугрупи со нерешлив проблем на зборови и истите тешко се конструираат.

Следната теорема дава некои услови за сместување на една алгебра во некој редукт на некоја алгебра од друго многуобразие.

Теорема 13 Нека $\mathcal{V}_1$ и $\mathcal{V}_2$ се многуобразија од тип ρ_1 и ρ_2 и сигнатури I_1 и I_2, соодветно, така што $I_1 \subseteq I_2$ и $\rho_1 = \rho_2|I_1$. Една алгебра $\mathbf{A}$ од $\mathcal{V}_1$ може да се смести во (некој I_1 редукт на) некоја алгебра од $\mathcal{V}_2$ ако и само ако $\mathbf{A}$ ги задоволува сите квази-идентитети во сигнатура I_1 кои се последици од дефинирачките идентитети на многуобразието $\mathcal{V}_2$. $\square$

Доказ Нека $\phi : A \to B$ е сместување на $\mathbf{A}$ од $\mathcal{V}_1$ во (некој I_1 редукт на) некоја алгебра $\mathbf{B}$ од $\mathcal{V}_2$. Тогаш бидејќи секој квази-идентитет е универзална формула, $\mathbf{A}$ ги задоволува сите квази-идентитети кои ги задоволува $\mathbf{B}$.

Обратно, нека Θ е множеството дефинирачки идентитети на $\mathcal{V}_2$ и $Diag(\mathbf{A})$ е множеството од сите атомарни формули и нивни негации на јазик $I_1 \cup A$ кои се вистинити во $\mathbf{A}$ (т.е. $Diag(\mathbf{A})$ е диаграмот на $\mathbf{A}$). Нека $\mathbf{B}$ е $\mathcal{V}_2$ алгебра, презентирана со $(A, Diag(\mathbf{A}))$. Ќе докажеме дека пресликувањето $\phi : A \to B$ дефинирано со $\phi(a) = a, a \in A$ е сместување. Од $\mathbf{B}_A \models Diag(\mathbf{A})$ следува дека ϕ е хомоморфизам. Останува да се докаже дека е инјективно. Нека претпоставиме дека постојат $a, b \in A$, т.ш.

$$\mathbf{A}_A \models a \not\approx b, \text{ но } \mathbf{B}_A \models a \approx b. \tag{1}$$

Од последново и од дефиницијата на $\mathbf{B}_A$ имаме дека $\Theta \cup Diag(A) \vdash a \approx b$. Значи постојат конечно многу идентитети $i_1, \ldots, i_n$ на $I_1 \cup S$ без променливи, т.ш. $Diag(A) \vdash i_1 \wedge i_2 \wedge \cdots \wedge i_n$ и $\Theta \vdash (i_1 \wedge \cdots \wedge i_n) \implies a \approx b$. Сега од условите на теоремата $\mathbf{A}_A \models (i_1 \wedge \cdots \wedge i_n) \implies a \approx b$ па од $\mathbf{A}_A \models Diag(A)$ и $Diag(A) \vdash i_1 \wedge i_2 \wedge \cdots \wedge i_n$ добиваме дека $\mathbf{A}_A \models a \approx b$ што е контрадикција со (1). □

Наведената теорема е всушност обопштување на теорема на A. Maljcev, која дава услов кога една полугрупа може да се смести во група.

Теорема 14 Полугрупа $\mathbf{S} =< S, \cdot >$ може да се смести во некоја група ако и само ако $\mathbf{S}$ ги задоволува сите квази-идентитети во сигнатура $\{\cdot\}$ кои се последица од аксиомите за групи. □

3 Елементи од теоријата на пресметливост

Во овој дел се задржуваме на елементи од теоријата на пресметливост со цел да го прецизираме поимот на одлучивост. Имено, во дефиницијата на проблемот на одлучување, главна улога има поимот алгоритам под кој подразбираме, во смисла на тезата на Church, Тјурингова машина или граматика или рекурзивна функција или нормален алгоритам. Ќе бидат изнесени неопходните дефиниции на Тјурингови машини и граматики, како и одредени својства на истите, за конечно да презентираме и пример на неодлучив проблем на зборови на прво и на второ ниво. Ова е блиску поврзано со проблемот на запирање на Тјурингова машина. Дефинициите на поимите и теоремите во овој дел се според [10, 11].

3.1 Тјурингови машини

Постојат повеќе еквивалентни дефиниции на Тјурингова машина, овде ја изнесуваме дефиницијата како во [10]. Пред да дадеме формална дефиниција, неколку зборови за интуитивно разбирање. Тјуринговата машина обработува зборови над некоја конечна азбука, која го содржи и празниот симбол #. Притоа зборовите се запишани на лента - еден симбол во една келија. Лентата има лев крај, а на десна страна е потенцијално бесконечна. Машината има внатрешна контрола (множество внатрешни состојби) и глава за движење, читање и запишување. Работата на машината (поточно на главата) е управувана од функција на премин.

Тјуринговите машини името го добиле по англискиот математичар Alan Turing и заедно со граматиките, рекурзивните функции и нормалните алгоритми претставуваат најмоќен (досега познат) вид на автомат.

Дефиниција 36 *Тјуринѓова машина* е четворка (K, Σ, δ, s), каде:

K е конечно множество чии елементи се нарекуваат состојби, $h \notin K$;

Σ е конечно множество, наречено азбука, празниот симбол $\# \in \Sigma$, симболите $L, R \notin \Sigma$;

$s \in K$ и се нарекува почетна состојба;

δ е пресликување од $K \times \Sigma$ во $(K \cup \{h\}) \times (\Sigma \cup \{L, R\})$, ($h$ се нарекува завршна состојба). $\triangle$

Дефиниција 37 *Конфиѓурација* на Тјуринговa машина $M = (K, \Sigma, \delta, s)$ е елемент од $(K \cup \{h\}) \times \Sigma^* \times \Sigma \times (\Sigma^*(\Sigma - \{\#\}) \cup \{e\})$, каде e е ознака за празниот збор. $\triangle$

Конфигурација чиј прв елемент е h се нарекува *завршна конфиѓурација*.

Интуитивно може да сметаме дека конфигурацијата ја опишува моменталната состојба на машината, односно првата компонента е состојбата во која машината се наоѓа, а останатите три го опишуваат зборот кој во моментот се обработува, при што тековна позиција на замислената глава за читање и пишување е третата компонента (буква од азбуката).

Често, кога не ни е битна состојбата во една конфигурација, наместо четворка (q, w, a, u) пишуваме $w\underline{a}u$ или, дури и ако е битна состојбата, истата конфигурација наместо како четворка, може да се претстави со пар $(q, w\underline{a}u)$.

Во продолжение дефинираме релација $\vdash_M$ (*преминува во еден чекор*) на множеството конфигурации на една Тјурингова машина, M.

Дефиниција 38 Нека $M = (K, \Sigma, \delta, s)$ е Тјурингова машина и нека $(q_1, w_1, a_1, u_1), (q_2, w_2, a_2, u_2)$ се две конфигурации на M. Тогаш

$$(q_1, w_1, a_1, u_1) \vdash (q_2, w_2, a_2, u_2)$$

ако и само ако, за некој $b \in \Sigma \cup \{L, R\}, \delta(q_1, a_1) = (q_2, b)$ и важи еден од следниве услови:

(1) $b \in \Sigma,\ w_1 = w_2,\ u_1 = u_2,\ a_2 = b$;

(2) $b = L,\ w_1 = w_2 a_2$ и

(2.1) $u_2 = a_1 u_1$, ако $a_1 \neq \#$ или $u_1 \neq e$, или

(2.2) $u_2 = e$, ако $a_1 = \#$ и $u_1 = e$;

(3) $b = R,\ w_2 = w_1 a_1$ и

(3.1) $u_1 = a_2 u_2$, или

(3.2) $u_1 = u_2 = e, a_2 = \#$.

Да воведеме некои понеформални поими, но често употребувани во врска со Тјуринговите машини и премините. Во случајот (1) велиме дека M запишува симбол без да ја помесува главата. При (2) велиме дека главата се придвижува за едно место лево, при што ако се бара движење на лево кога главата е на десниот крај на лентата, едноставно, празниот симбол на скенираната келија исчезнува од конфигурацијата.

Во случајот (3) се движи за едно место на десно, при тоа ако се бара движење на крајот од зборот едноставно се појавува нова празна келија на десно.

Да уочиме дека ако $b = L, w_1 = e$, тогаш ниедна конфигурација (q_1, w_1, a_1, u_1) не преминува во еден чекор во ниедна друга. Во секој друг случај од една конфигурација во еден чекор се преминува во точно една конфигурација.

За конфигурацијата (q_1, e, a_1, u_1), при $\delta(q_1, a_1) = (q_2, L)$ велиме дека е *висечка конфигурација*.

Дефиниција 39 За дадена Тјурингова машина со $\vdash_M^*$ се означува рефлексивното и транзитивно проширување на $\vdash_M$. Конфигурацијата C_1 *преминува* во конфигурација C_2 ако $C_1 \vdash_M^* C_2$. *Пресметување* на M со *должина* n е низа од конфигурации $C_0, \ldots, C_n$, за некој $n \in \mathbb{N}$, т.ш. $C_0 \vdash_M \cdots \vdash_M C_n$. $\triangle$

Следните неколку дефиниции ја опишуваат работата на Тјуринговите машини.

Дефиниција 40 Нека $M = (K, \Sigma, \delta, s), w \in \Sigma^*$. M *запира на влез* w ако постои завршна конфигурација C_h таква што $(s, \#w\underline{\#}) \vdash_M C_h$. Аналогно, M *виси на влез* w ако постои висечка конфигурација C_v таква што $(s, \#w\underline{\#}) \vdash_M C_v$. $\triangle$

Дефиниција 41 Нека Σ_0 и Σ_1 се азбуки кои не го содржат празниот симбол $\#$ и нека f е функција од Σ_0^* во Σ_1^*. Тјуринговата машина $M = (K, \Sigma, \delta, s)$ *ја пресметува* f ако $\Sigma_0, \Sigma_1 \subseteq \Sigma$ и за секој $w \in \Sigma_0^*$,

$(s, \#w\underline{\#}) \vdash_M^* (h, \#f(w)\underline{\#})$. Ако ваква Тјурингова машина постои, тогаш f е *Тјуринг-пресметлива* функција. $\triangle$

Претходната дефиниција може лесно да се прошири на функции од повеќе променливи. Имено, за $f : \Sigma_0^k \to \Sigma_1$ велиме дека е Тјуринг-пресметлива ако постои Тјурингова машина $M = (K, \Sigma, \delta, s)$ таква што за секој $(w_1, \ldots, w_k) \in \Sigma_0^k$, $(s, \#w_1\# \ldots \#w_k\underline{\#}) \vdash_M^* (h, \#f(w_1, \ldots, w_k)\underline{\#})$.

Потоа, една бројна функција $f : \mathbb{N} \to \mathbb{N}$ велиме дека е Тјуринг пресметлива ако постои Тјурингова машина која ја пресметува функцијата $f' : \{|\}^* \to \{|\}^*$, каде $f'(|^n) = |^{f(n)}$, за секој $n \in \mathbb{N}$.

Друг битен поим кој произлегува од дефиницијата на Тјуринг-пресметлива функција е поимот за Тјуринг-одлучив јазик.

Дефиниција 42 Нека Σ_0 е азбука која не го содржи празниот симбол $\#$ и нека Y и N се два фиксни симболи кои не се во Σ_0. Јазикот $L \subseteq \Sigma_0^*$ е *Тјуринг-одлучив* ако неговата карактеристична функција $\chi_L : \Sigma_0^* \to \{Y, N\}$ е Тјуринг пресметлива. $\triangle$

За секој $w \in \Sigma_0^*$,

$$\chi_L(w) = \begin{cases} Y & w \in L \\ N & w \notin L \end{cases}$$

Ако χ_L ја пресметува Тјурингова машина M, тогаш M се нарекува *процедура за одлучување* на L.

Значи, Тјуринговите машини може да се користат како одлучувачи или препознавачи на јазици. Освен ова, тие можат да се користат и како прифаќачи на јазици, согласно следната дефиниција.

Дефиниција 43 Една Тјурингова машина M *го прифаќа* зборот $w \in \Sigma_0^*$, ако таа запира на влез w. M *го прифаќа* јазикот $L \subseteq \Sigma_0^*$ ако и само ако $L = \{w \in \Sigma_0^* \mid M \text{ го прифаќа } w\}$. Еден јазик е *Тјуринг-прифатлив*, ако постои Тјурингова машина која го прифаќа. $\triangle$

Постојат повеќе проширувања на поимот Тјурингова машина како на пример: дозволување лентата да е бесконечна во двете насоки, а не само на десно; употреба на повеќе ленти; употреба на повеќе глави наместо една; употреба на дводимензионална лента и разни комбинации од овие. Овде нема да се задржуваме на нивните прецизни дефиниции. Во секој од досега направените обиди за проширувања се докажало дека во суштина не се добива никакво подобрување, т.е. добиената машина може да се симулира со стандардната Тјурингова машина. Всушност еквивалентноста се докажува конструирајќи стандардна Тјурингова машина за дадена Тјурингова машина од проширен тип а потоа се докажува дека новоконструираната машина соодветно ја имитира дадената.

Друго можно проширување е со дозволување недетерминизам. Овде сепак ќе ја дадеме дефиницијата на недетерминистичка Тјурингова машина.

Дефиниција 44 *Недетерминистичка Тјурингова машина* е четворка (K, Σ, Δ, s), каде K, Σ, s ги имаат истите значења како кај стандардната Тјурингова машина, додека

$$\Delta \subseteq (K \times \Sigma) \times ((K \cup \{h\}) \times (\Sigma \cup \{L, R\})). \qquad \triangle$$

Конфигурациите и релациите $\vdash_M$ и $\vdash_M^*$ се дефинираат вообичаено.

Јасно, бидејќи недетерминистичка Тјурингова машина може да даде два различни излези за ист влез, треба некако да определиме што е излез од ваква машина, односно што не интересира од однесувањето на ваквата машина. Затоа, недетерминистички Тјурингови машини конструираме само како прифаќачи на јазици. Без доказ ја даваме следнава теорема.

Теорема 15 За секоја недетерминистичка Тјурингова машина M_1 може да се конструира стандардна Тјурингова машина M_2 така што, за секој збор w кој не содржи празен карактер, M_1 запира на влез w ако и само ако M_2 запира на влез w. $\square$

Значи, секој јазик кој е прифатлив од недетерминистичка Тјурингова машина се прифаќа и од детерминистичка Тјурингова машина.

3.2 Граматики

Во овој дел се задржуваме на дефиниција на општи граматики, и еквивалентност на граматиките и Тјуринговите машини, која ќе ни биде потребна за примерот на неодлучивост што сакаме натаму да го презентираме.

Дефиниција 45 *Граматика* е четворка $G = (V, \Sigma, R, S)$, каде

V е азбука;

$\Sigma \subseteq V$ е множество *терминални* симболи, $V - \Sigma$ е множество *нетерминални* симболи;

$S \in V - \Sigma$ е *почетен нетерминал*;

R е конечно подмножество од $(V^*(V - \Sigma)V^*) \times V^*$, наречено множество *правила*. $\triangle$

Наместо $(u, v) \in R$, користиме ознака $u \to v$. Потоа, за два збора $u, v \in V^*$, $u \Rightarrow_G v$ ако и само ако за некои $w_1, w_2 \in V^*, u' \to u'' \in R, u = w_1 u' w_2, v = w_1 u'' w_2$. Со $\Rightarrow_G^*$ се означува рефлексивното и транзитивно затварање на $\Rightarrow_G$.

За еден збор $w \in \Sigma^*$ велиме дека *е генериран* од G ако $S \Rightarrow_G^* w$. Со $L(G)$ се означува множеството од сите зборови генерирани од G, и истото се нарекува *јазик генериран од граматиката* G.

Под *извод* со *должина* n се подразбира низа од облик $w_0 \Rightarrow_G w_1 \Rightarrow_G \cdots \Rightarrow_G w_n$, каде $w_1, \ldots, w_n \in V^*$, $n \in \mathbb{N}$.

Следната лема дава начин за симулирање на Тјурингова машина со граматика.

Лема 3 Нема $M = (K, \Sigma, \delta, s)$ е Тјурингова машина и $K \cap \Sigma = \emptyset$. Тогаш постои граматика G таква што, за секои конфигурации (q, u, a, v), (q', u', a', v') на M,

$$(q, u, a, v) \vdash_M^* (q', u', a', v')$$

ако и само ако

$$[uqav] \Rightarrow_G^* [u'q'a'v'].$$

Притоа, [и] се нови симболи кои не се во Σ, ни во K.

Доказ.

Идејата е секоја конфигурација (q, u, a, v) да се претстави со збор $[uqav]$. Притоа, позицијата на состојбата во зборот укажува на позицијата на главата. Симболот $]$ е битен за да се разреши проблемот на празна лента на десен крај, додека $[$ е употребена само заради читливост.

Дефинираме граматика $G = (V, \Sigma, R, S)$, каде $V = K \cup \Sigma \cup \{[,], h, S\}$ и R содржи правила од три типа.

(1) За секој $q \in K, a \in \Sigma$, ако $\delta(q, a) = (p, b)$, каде $p \in K \cup \{h\}, b \in \Sigma$, тогаш

$$qa \to pb \in R.$$

(2) За секој $q \in K, a \in \Sigma$, ако $\delta(q, a) = (p, R)$, каде $p \in K \cup \{h\}$, тогаш за секој $b \in \Sigma$,

$$qab \to apb \in R$$

и

$$qa] \to ap\#] \in R.$$

(3) За секој $q \in K, a \in \Sigma$, ако $\delta(q, a) = (p, L)$, каде $p \in K \cup \{h\}$, тогаш за секои $b \in \Sigma, c \in \Sigma \cup \{]\}$

$$bqac \to pbac \in R$$

каде $a \neq \#$ или $c \neq]$; и за секој $b \in \Sigma$

$$bq\#] \to pb].$$

Директно се проверува дека $(q, u, a, v) \vdash_M (q', u', a', v')$ ако и само ако $[uqav] \Rightarrow_G [u'q'a'v']$, од каде следува тврдењето и за соодветните рефлексивни и транзитивни затворачи. $\square$

Граматиките ги дефиниравме како генератори на јазици, но, според претходната лема, истите може да се третираат и како пресметувачи на функции.

Дефиниција 46

(1) Нека Σ_0, Σ_1 се азбуки кои не го содржат празниот симбол $\#$, $f : \Sigma_0^* \to \Sigma_1^*$ и нека $G = (V, \Sigma, R, S)$ е граматика т.ш. $\Sigma_0, \Sigma_1 \subseteq \Sigma$. *$G$ ја пресметува f* ако постојат зборови $x, y, x', y' \in V^*$ такви што за секој $u \in \Sigma_0^*, v \in \Sigma_1^*$

$$f(u) = v \Leftrightarrow xuy \Rightarrow_G^* x'vy'$$

Функцијата f е *граматички пресметлива* ако постои граматика која ја пресметува.

(2) Една бројна функција $f : \mathbb{N} \to \mathbb{N}$ е *граматички пресметлива* ако функцијата $f' : \{|\}^* \to \{|\}^*$ е граматички пресметлива, каде $f'(|^n) = |^{f(n)}$ за секој $n \in \mathbb{N}$. $\triangle$

Сега може да ја искажеме следната теорема.

Теорема 16 Секоја Тјуринг пресметлива функција (од зборови или бројна функција) е граматички пресметлива.

Доказ Доказот следува од дефиницијата и од претходната лема, при $x = [\#,\ y = s\#],\ x' = [\#,\ y' = h\#]$. $\square$

Да напоменеме дека се задржавме на доказите на претходните својства од причини што конструкцијата на граматиката во доказот на претходната лема ни е потребна понатаму. Инаку, важи и поопшта теорема која ја искажуваме без доказ, и која е дел од поткрепата на тезата на Church.

Теорема 17 Класата од Тјуринг пресметливи функции е еднаква со класата граматички пресметливи функции. $\square$

3.3 Претставување на Тјурингови машини. Универзална Тјурингова машина

Во овој дел презентираме дефиниција на универзална Тјурингова машина која, за разлика од претходната дефиниција на машина со специјална намена, ја опишува секоја Тјурингова машина. Исто така, дефинираме претставување на произволна Тјурингова машина со збор од азбука $\{c, |\}$.

Фиксираме две преброиви множества $K_\infty = \{q_1, q_2, \dots\}$ и $\Sigma_\infty = \{a_1, a_2, \dots\}$, и сметаме дека за секоја Тјурингова машина множеството состојби е конечно подмножество од K_∞ и азбуката е конечно подмножество од Σ_∞.

На секој симбол σ од дефиницијата на една Тјурингова машина му придружуваме збор $\lambda(\sigma)$ од $\{|\}^*$, на следниот начин:

$$\lambda(q_i) = |^{i+1},\ \lambda(h) = |,\ \lambda(L) = |,\ \lambda(R) = ||,\ \lambda(a_i) = |^{i+2}.$$

Да забележиме дека на секои два различни елементи од $K_\infty \cup \{h\}$ им се придружени различни зборови, истото важи и за елементите на $\Sigma_\infty \cup \{L, R\}$.

Потоа, дефинираме претставување на секоја Тјурингова машина со збор од азбука $\{c, |\}$, каде c е нов симбол.

Нека $M = (K, \Sigma, \delta, s)$ е Тјурингова машина, каде $K \subseteq K_\infty, \Sigma \subseteq \Sigma_\infty$. Може да сметаме дека $K = \{q_{i_1}, q_{i_2}, \ldots, q_{i_k}\},\ i_1 < i_2 < \cdots < i_k, \Sigma = \{a_{j_1}, a_{j_2}, \ldots, a_{j_l}\},\ j_1 < j_2 < \cdots < j_l$ и $s = q_{i_m}$ за некој $m,\ 1 \leq m \leq k$.

За секој $p \in \{1, \ldots, k\}$ и за секој $r \in \{1, \ldots l\}$ дефинираме по еден збор $S_{pr} = cw_1cw_2cw_3cw_4c$, каде $w_1 = \lambda(q_{i_p}), w_2 = \lambda(a_{j_r}), w_3 = \lambda(q'), w_4 = \lambda(b)$ и $\delta(q_{i_p}, a_{j_r}) = (q', b)$. Значи, со секој ваков збор S_{pr} е претставен по еден премин од функцијата на премин δ.

Конечно, презентацијата на M е зборот

$$p(M) = cS_0cS_{11}S_{12}\ldots S_{1l}S_{21}S_{22}\ldots S_{2l}\ldots S_{k1}S_{k2}\ldots S_{kl}c$$

каде $S_0 = \lambda(s)$.

На овој начин на секоја Тјурингова машина и одговара еднозначно определен збор од $\{c, |\}$ и за даден таков збор едноставно се проверува дали е претставување на Тјурингова машина, и доколку е, на која е.

Исто така дефинираме претставување на збор $w = b_1b_2\ldots b_n \in \Sigma_\infty^*$ со $p(w) = c\lambda(b_1)c\lambda(b_2)c\ldots c\lambda(b_n)$.

Од универзална Тјурингова машина $U = (K_U, \Sigma_U, \delta_U, s_U)$ се очекува за секоја Тјурингова машина $M = (K, \Sigma, \delta, s)$ и за секој збор $w \in \Sigma^*$

(1) ако $(h, u\underline{a}v)$ е завршна конфигурација на M, таква што $(s, \#w\underline{\#}) \vdash_M^* (h, u\underline{a}v)$, тогаш $(s_U, \#p(M)p(w)\underline{\#}) \vdash_U^* (h, \#p(uav)\underline{\#})$;

(2) ако $(s_U, \#p(M)p(w)\underline{\#}) \vdash_U^* (h', u'\underline{a}'v')$ за некоја завршна конфигурација $(h', u'\underline{a}'v')$ на U, тогаш $a' = \#, v' = e, u' = \#p(uav)$ за

некои u, a, v такви што $(h, u\underline{a}v)$ е завршна конфигурација на M и $(s, \#w\underline{\#}) \vdash_M^* (h, u\underline{a}v)$.

Нема детално да ја дефинираме универзалната машина M, бидејќи тоа би било прегломазно. Накратко (повторно без детална дефиниција), ќе опишеме машина U' со три ленти за читање и пишување која ја извршува бараната работа, а како што претходно спомнавме, постои стандардна машина која ја симулира работата на U' и тоа би била бараната машина U. Машината U' ги користи своите три ленти на следниот начин. На првата лента останува запишано претставувањето на w, на втората се запишува претставувањето на M, а на третата се запишува претставувањето на состојбата на M во тековниот момент на симулирана обработка.

Машината U' започнува со работа со збор $\#p(M)p(w)$ на првата лента и останатите две ленти празни. Веднаш U' го пренесува зборот $p(M)$ на втората лента, а на првата (од почетокот на десно) се запишува $\#c\lambda(\#)$, до кој се шифтира (налево) $p(w)$ и се допишува $\lambda(\#)c$. Така, во овој момент на првата лента се наоѓа зборот $\#p(\#w\#)$. Потоа, од $p(M)$, U' ја зема презентацијата на почетната состојба на M и ја запишува на третата лента. Сега почнува да се одвива симулацијата на M чекор по чекор. Помеѓу чекорите, главите на U се позиционирани на следниот начин. Главите на втората и третата лента се на крајот на зборот а главата на првата лента е на симболот c кој го означува крајот на претставувањето на симболот кој M би го сканирала во дадениот момент. Како изгледа симулацијата на еден чекор: машината U' наоѓа на втората лента блок од облик $cc|^ic|^jc|^kc|^lcc$, таков што $|^i$ е низа од $|$

запишана на третата лента, а $|^j$ е лево од главата на првата лента, и ја менува првата лента соодветно. Ако $|^l$ е $\lambda(L)$ или $\lambda(R)$ нема поголеми проблеми, се движи по првата лента одреден број келии лево или десно (до следното c), ако е пак претставување на буква потребно е одредено шифтирање на целиот збор од првата лента. Конечно U' запишува $|^k$ на третата лента, проверува дали новозапишаниот збор на третата лента е $\lambda(h)$, ако не е продолжува со следниот чекор, ако е ја придвижува главата на првата лента до првиот празен симбол на десно од зборот и самата завршува со работа.

3.4 Непресметливост и неодлучивост. Проблем на запирање

Досега веќе рековме дека Тјуринговата машина треба да се смета за математичка формализација на поимот алгоритам. Според тоа, од интерес е наоѓање на јазици кои не се Тјуринг-одлучиви т.е. се *неодлучиви* со кој било алгоритам, односно функции кои не се Тјуринг-пресметливи т.е. се *алгоритамски непресметливи*. Во овој дел ќе се задржиме на такви примери, како и на врските помеѓу Тјуринг-одлучивост и Тјуринг - прифатливост на јазиците. Еден од неодлучивите проблеми е точно проблемот на запирање на Тјурингова машина на кој детално ќе се задржиме, а кој е и корисен, бидејќи докажувањето на неодлучивост на многу проблеми често се изведува преку сведување на конкретниот проблем на проблем на запирање.

Теорема 18 Секој Тјуринг-одлучив јазик е Тјуринг-прифатлив. □

Теорема 19 Ако L е Тјуринг-одлучив јазик, тогаш и неговиот комплемент е Тјуринг-одлучив. $\square$

Кога би биле во можност за произволна Тјурингова машина M и за произволен влезен збор w да предвидиме дали M ќе запре на влез w, тогаш секој Тјуринг-прифатлив јазик би бил Тјуринг-одлучив.

Со K_0 го означуваме јазикот

$K_0 = \{p(M)p(w)|$ Тјуринговата машина M го прифаќа зборот $w\}$.

Својство 12 K_0 е Тјуринг-прифатлив.

Доказ K_0 го прифаќа варијанта на универзалната Тјурингова машина, за која стана збор претходно. $\square$

Нека M_1 и M_2 се две Тјурингови машини. *Состав* на Тјуринговите машини M_1 и M_2 е Тјурингова машина, која ја означуваме со M_1M_2. За произволен влез w M_1M_2 се однесува како M_1 на влез w, а откако M_1 заврши со работа се однесува како M_2 на влез - она што е останато на лентата од работата на M_1.

Својство 13 Секој Тјуринг-прифатлив јазик е Тјуринг-одлучив ако и само ако K_0 е Тјуринг-одлучив.

Доказ Нека K_0 е Тјуринг-одлучив, и нека го одлучува машина M_0. Нека L е произволен Тјуринг-прифатлив јазик и M_1 е Тјурингова машина која го прифаќа L.

Прво конструираме Тјурингова машина M_1^* која произволен влезен збор w т.е. $\#w\underline{\#}$ го трансформира во $\#p(M_1)p(w)\underline{\#}$. Всушност, M_1^* го поместува влезот за $|p(M_1)|$ места на десно, го претставува во азбука $\{c, |\}$ и потоа лево од него го запишува фиксниот збор $p(M_1)$. Нека $M_2 = M_1^* M_0$, односно е составот на овие две машини. Значи M_2 го трансформира влезот $\#w\underline{\#}$ во $\#p(M_1)p(w)\underline{\#}$, а потоа и ја предава контролата на M_0 која по претпоставка одлучува дали M_1 го прифаќа w или не. Добивме дека L е Тјуринг-одлучив.

Обратната насока е тривијална последица од претходното својство.

$\square$

Својство 14 K_0 не е Тјуринг-одлучив.

Доказ Ако K_0 е Тјуринг-одлучив, тогаш и јазикот

$K_1 = \{p(M)|$ Тјуринговата машина M го прифаќа зборот $p(M)\}$

би бил Тјуринг - одлучив. Имено, нека M_0 го одлучува K_0 и нека M_1 е машина која го трансформира својот влез $\#w\underline{\#}$ во $\#wp(w)\underline{\#}$, а потоа ја предава контролата на M_0. Значи M_1 го дава истиот резултат на влез $\#w\underline{\#}$, кој M_0 го дава на влез $\#wp(w)\underline{\#}$. Сега, од дефиницијата на K_0, M_0 дава резултат Y на влез $\#wp(w)\underline{\#}$ ако и само ако важат следниве две работи:

(1) $w = p(M)$ за некоја Тјурингова машина M; и

(2) Тјуринговата машина M го прифаќа влезниот збор $p(M)$.

Значи, M_1 го одлучува K_1. Од таму, доволно е да се докаже дека K_1 не е Тјуринг-одлучив.

Ако K_1 е Тјуринг-одлучив, тогаш и неговиот комплемент е исто така Тјуринг-одлучив. $\bar{K}_1 = \{w \in \{c, |\}|w$ не е претставување на ниедна Тјурингова машина M или $w = p(M)$ за некоја Тјурингова машина M

која не го прифаќа зборот $p(M)\}$.

Но, $\bar{K}_1$ не е дури ни Тјуринг-прифатлив. Имено, нека M' е Тјурингова машина која го прифаќа $\bar{K}_1$. Тогаш M' го прифаќа $p(M')$ ако и само ако M' не го прифаќа $p(M')$, што е апсурд. $\square$

Теорема 20 Не секој Тјуринг-прифатлив јазик е Тјуринг-одлучив.

$\square$

Ова е воедно и најпознатиот нерешлив (алгоритамски неодлучив) проблем, односно *проблемот на запирање* кој се состои во следново: за произволна дадена Тјурингова машина M и збор w да се утврди дали M запира на влез w. Уште повеќе постојат конкретни Тјурингови машини за кои не постои општ метод за утврдување дали машината запира на произволен влез w или не. Ова произлегува од фактот што K_0 е Тјуринг-прифатлив, но не е Тјуринг-одлучив. Имено, таква Тјурингова машина е машината M_0 која го прифаќа K_0. Нерешливоста на проблемот на запирање е искажана во следната теорема.

Теорема 21

(i) Не постои алгоритам за одлучување, за произволна Тјурингова машина M и произволен влезен збор w, дали M го прифаќа w.

(ii) Постои Тјурингова машина M_0 за која не постои алгоритам за одлучување, дали M_0 прифаќа произволен влезен збор w. $\square$

Во остатокот од овој дел, заради комплетност, наведуваме уште некои својства во врска со Тјуринг-одлучивост и Тјуринг-прифатливост на јазиците.

Теорема 22 Комплемент на Тјуринг-прифатлив јазик не мора да е Тјуринг-прифатлив. $\square$

Теорема 23 Еден јазик L е Тјуринг-одлучив ако и само ако и L и $\bar{L}$ се Тјуринг-прифатливи. $\square$

Дефиниција 47 Нека Σ_0 е азбука која не го содржи празниот симбол $\#$. Јазикот $L \subseteq \Sigma_0^*$ е *излезен јазик* на една Тјурингова машина $M = (K, \Sigma, \delta, s), \Sigma_0 \subseteq \Sigma$, ако и само ако

$$L = \{w \in \Sigma_0^* | (\exists u \in \Sigma_0^*)(s, \#u\underline{\#}) \vdash_M^* (h, \#w\underline{\#})\}. \qquad \triangle$$

Теорема 24 Еден јазик е Тјуринг-прифатлив ако и само ако е излезен јазик од некоја Тјурингова машина. $\square$

И Тјуринговите машини може да се користат како генератори на јазици.

Дефиниција 48 Тјуринговата машина $M = (K, \Sigma, \delta, s)$ го *набројува* јазикот L ако и само ако, за некоја фиксна состојба q на M, важи

$$L = \{w| \text{ за некој збор } u,\ (s, \underline{\#}) \vdash_M^* (q, \#w\underline{\#}u)\}.$$

Еден јазик е *Тјуринг-наброив* ако постои Тјурингова машина што го набројува. $\triangle$

Теорема 25 Еден јазик е Тјуринг-прифатлив ако и само ако е Тјуринг-наброив, ако и само ако е генериран од некоја граматика. $\square$

Ќе се задржиме уште малку на некои примери на неодлучиви проблеми.

Теорема 26 Следните проблеми во врска со Тјуринговите машини се неодлучиви:

(1) За произволна Тјурингова машина M и произволен влезен збор w, дали M запира на влез w?

(2) За фиксна Тјурингова машина M и произволен влезен збор w, дали M запира на влез w?

(3) За дадена Тјурингова машина M, дали M запира на празен влез?

(4) За дадена Тјурингова машина M, дали воопшто постои збор на кој M запира?

(5) За дадена Тјурингова машина M, дали M запира на секој збор?

(6) За дадени две Тјурингови машини M_1 и M_2, дали тие запираат на истите влезни зборови?

(7) За дадена Тјурингова машина M, дали јазикот кој M го прифаќа е регуларен? Дали е контестно-слободен? Дали е Тјуринг-одлучив?

Доказ Тврдењата (1) и (2) се претходно докажани. За илустрација на начинот на докажување неодлучивост, ќе дадеме докази на (3) и (5).

(3) Нека претпоставиме дека M_0 е машина која го одлучува јазикот $\{p(M)|M$ запира на влез $e\}$. Ќе докажеме дека тогаш M_0 може да се искористи за одлучување на K_0. Прво, за дадена Тјурингова машина M и збор w, со M_w ја означуваме следната Тјурингова машина. M_w на влез e, т.е. во конфигурација $(s, \#\underline{\#})$ го запишува w (конфигурација $(s, \#w\underline{\#})$) на лентата, а потоа се однесува како M. Сега, за произволна Тјурингова машина M и влезен збор w, ја конструираме M_w, го определуваме $p(M_w)$, а потоа го обработуваме $p(M_w)$ со M_0. Тогаш M_0 запира со Y на

својата лента ако и само ако M го прифаќа w, т.е. ако T е Тјурингова машина која на влез $\#p(M)p(w)\underline{\#}$ запира со $\#p(M_w)\underline{\#}$ на лентата (а ваква секако постои), тогаш TM_0 го одлучува K_0, што не е можно.

(5) Нека E е Тјурингова машина која го брише секој влезен збор, имено го трансформира $\#w\underline{\#}$ во $\underline{\#}$. Нека T_1 е Тјурингова машина која за секоја Тјурингова машина M го трансформира $\#p(M)\underline{\#}$ во $\#p(ERM)\underline{\#}$. (R е Тјурингова машина која само ја движи главата за едно место на десно, ERM е составот од трите машини). Тогаш ако M_1 е машина која го одлучува јазикот $\{p(M)|M$ запира на секој влез$\}$, T_1M_1 би го одлучувала $\{p(M)|M$ го прифаќа $e\}$, што е спротивно на (3). $\square$

Од еквивалентноста (еднаквата пресметувачка моќ) на граматиките и Тјуринговите машини следува неодлучивост на низа проблеми поврзани со граматики.

Теорема 27 Следните проблеми во врска со граматиките се неодлучиви:
(1) За произволна граматика G и збор w, дали $w \in L(G)$?
(2) За фиксна граматика G_0 и произволен збор w, дали $w \in L(G_0)$?
(3) За произволни две граматики G_1 и G_2, дали $L(G_1) = L(G_2)$?
(4) За произволна граматика G, дали $L(G) = \emptyset$? $\square$

3.5 Неодлучивост на проблемот на зборови за полугрупите

Многуобразието полугрупи е многуобразие групоиди со идентитет

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Во овој дел ќе докажеме дека проблемот на зборови за полугрупите е нерешлив (неодлучив и на прво и на второ ниво), односно неодлучиво е дали за произволна конечно презентирана полугрупа S зададена со конечно множество генератори B и дефинирачки равенства $E = \{u_1 \approx v_1, \ldots, u_n \approx v_n\},\ u_i, v_i \in \mathcal{T}_{\{\cdot\}}(B)$ и дадени два збора $x, y \in \mathcal{T}_{\{\cdot\}}(B)$, $x \equiv_S y$ каде $\equiv_S$ е конгруенцијата на $\mathcal{T}_{\{\cdot\}}(B)$ генерирана од E и од идентитетот. Уште повеќе, постои конечно презентирана полугрупа S_0 и збор $w_0 \in \mathcal{T}_{\{\cdot\}}(B)$ за кои е неодлучиво дали, за произволен збор $u \in \mathcal{T}_{\{\cdot\}}(B), w_0 \equiv_{S_0} u$.

Иако со препишувачки системи ќе се занимаваме повеќе во наредното поглавје, да споменеме дека презентација на полугрупа (B, R) често се поистоветува со така наречен препишувачки систем на Thue (B^*, R') (според Axel Thue кој во 1914 година прв го поставил проблемот на зборови за полугрупите) на множество B^* со множество правила за препишување $R' = \{u \to v | u \approx v \in R \vee v \approx u \in R\}$. Притоа, имајќи на ум дека B^* е слободен моноид со слободна база B, го имаме следново едноставно својство.

Својство 15 Проблемот на зборови за полугрупа S со презентација (B, R) е решлив ако и само ако за произволни два збора $u, v \in B^*$ е одлучиво дали $u \leftrightarrow^* v$ во соодветниот систем (B^*, R') на Thue. $\square$

Теорема 28 (А.А. Марков, 1947)

Проблемот на зборови е неодлучив за многуобразието полугрупи, уште повеќе постои полугрупа $\mathbf{S}_0$ и збор z_0 така што за произволен збор z не е одлучиво дали $z \equiv_{S_0} z_0$.

Доказ Прво да уочиме дека следната варијанта на проблемот на запирање е неодлучива. За дадена азбука Σ_0, дадена Тјурингова машина M и даден збор $w \in \Sigma_0^*$, дали M за влез w запира со празна лента т.е. дали $(s, \#w\underline{\#}) \vdash_M^* (h, \underline{\#})$ каде s е почетната состојба на M.

Имено, нека претпоставиме дека Тјуринговата машина M_0 го одлучува јазикот

$$\{p(M)p(w)|(s, \#w\underline{\#}) \vdash_M^* (h, \underline{\#})\} \qquad (1).$$

Значи

$$(s, \#p(M)p(w)\underline{\#}) \vdash_{M_0}^* (h, \#Y\underline{\#}) \Leftrightarrow (s, \#w\underline{\#}) \vdash_M^* (h, \underline{\#}).$$

Нека M_1 е машина која има една лента повеќе од M_0 и работи на следниов начин. M_1 на првата лента се однесува исто како M_0, а на втората лента во секој момент е претставена тековната состојба на проверуваната машина M. M_1 запира со излез Y на првата лента ако и само ако M_0 запира и на втората лента се наоѓа зборот $||$ т.е. $\lambda(h)$, инаку M_1 запира со излез N во секој друг случај (кога M_0 запира). Добиваме дека M_1 го одлучува проблемот на запирање, што не е можно, односно ваква M_0 не постои.

Нека $M = (K, \Sigma, \delta, s)$ е Тјурингова машина и $\Sigma_0 \subseteq \Sigma$. Ја применуваме конструкцијата од *Лема 3* на M и добиваме граматика $G = (V, \Sigma, R, S)$ таква што

$$(\forall w \in \Sigma^*)[\#ws\#] \Rightarrow_G^* [h\#] \Leftrightarrow (s, \#w\underline{\#}) \vdash_M^* (h, \underline{\#})$$

Нека S е полугрупата со презентација (Σ_0, E_R), каде $E_R = \{u \approx v \mid u \to v \in R\}$.

Ќе докажеме дека

$$(\forall w \in \Sigma^*)[\#ws\#] \Rightarrow_G^* [h\#] \Leftrightarrow [\#ws\#] \equiv_S [h\#]$$

што е доволно за да се докаже првото тврдење од теоремата, бидејќи тогаш ако проблемот на зборови е решлив за S би имале Тјуринг-одлучивост на јазикот (1).

Јасно, ако $[\#ws\#] \Rightarrow_G^* [h\#]$, тогаш $[\#ws\#] \equiv_S [h\#]$ бидејќи секое правило од G постои како дефинирачко равенство во E_R.

Нека $[\#ws\#] \equiv_S [h\#]$. Тогаш постои конечна низа зборови w_0, $w_1, \ldots,$ w_n каде

$$w_0 = [\#ws\#], w_n = [h\#], w_i \equiv_S w_{i+1}, i \in \{0, \ldots, n-1\} \qquad (2).$$

Да претпоставиме дека оваа низа е најкратката можна т.е. не постои низа $u_0, \ldots, u_{n'}$ која ги задоволува условите (2) при $n' < n$. Тврдиме дека $w_i \Rightarrow_G w_{i+1}, i \in \{0, \ldots, n-1\}$ т.е. сите дефинирачки равенства се употребени во "вистинска" насока (како во правилата од R). Со докажувањето на ова тврдење ќе биде комплетиран доказот на првиот дел од теоремата.

Пред се, да уочиме дека $w_{n-1} \Rightarrow_G w_n$, бидејќи во секое правило од R, па и во секое дефинирачко равенство од E_R и левата и десната страна содржат состојби, но состојбата во левата страна на кое било правило од R не е h бидејќи M не ја напушта завршната состојба. Сега, нека претпоставиме дека за некој $i \in \{0, \dots, n-1\}$ не важи $w_i \Rightarrow_G w_{i+1}$. Тогаш $w_{i+1} \Rightarrow_G w_i$. Нека i е најголемиот со ова својство. Значи $w_{i+1} \Rightarrow_G w_i$, но $w_{i+1} \Rightarrow_G w_{i+2} \Rightarrow_G \cdots \Rightarrow_G w_n$. Но тогаш $w_i = w_{i+2}$ (бидејќи G е добиена од детерминистичка Тјурингова машина, па само едно правило од G е применливо на произволен збор $[uqav], u, v \in \Sigma^*, q \in K, a \in \Sigma$) и $w_0, \dots, w_{i-1}, w_{i+2}, \dots, w_n$ е пократка низа која ги задоволува условите (2) што е спротивно на минималноста на n.

Што се однесува на вториот дел од тврдењето на теоремата, го имаме следново. Јазикот (1) е Тјуринг-прифатлив. Имено него го прифаќа варијанта на опишаната универзална машина со три ленти, со следнава разлика. Машината има една состојба m вишок од опишаната машина. Оваа состојба е "мртва" т.е. од неа не се излегува со ниеден премин. Откако ќе симулира еден чекор, машината проверува на третата лента дали е запишано $\lambda(h)$ и истовремено дали првата лента е празна. Ако ова е исполнето и самата завршува со работа, ако на третата лента стои $\lambda(h)$ но првата лента не е празна преминува во состојба m, инаку продолжува со симулирање на следниот чекор. Нека стандардната машина еквивалентна на погоре опишаната ја означиме со M_0. Нека $G_0 = (V_0, \Sigma, R_0, S_0)$ е граматиката добиена од M_0 со примена на *Лема 3* и нека $\mathbf{S}_0$ е полугрупата презентирана со (Σ_0, E_{R_0}), каде $E_{R_0} = \{u \approx v \mid u \to v \in R_0\}$. Со сосема аналогни аргументи, како погоре, се утврдува дека

$$[\#ws\#] \Rightarrow_{G_0} [h\#] \Leftrightarrow [\#ws\#] \equiv_{S_0} [h\#].$$

Сега ако со z_0 го означиме зборот $[h\#]$, имаме дека ако за произволен збор $z \in \Sigma_0^*$ е одлучиво дали $z \equiv_{S_0} z_0$ тогаш јазикот (1) би бил одлучив.

$\square$

Во претходната теорема не е експлицитно дадена презентација на полугрупа со неодлучив проблем на зборови. Во 1956 година, А.А.Марков дал пример на презентација со 13 генератори и 33 дефинирачки равенства со неодлучив проблем на зборови. Доказот на Марков е доста сложен и е начелно даден во [11, 12], овде го наведуваме само примерот, како и некои други подоцнежни примери со уште помал број на генератори и дефинирачки равенства.

Пример 2 (А.А. Марков, 1956, според [11])

Полугрупата со презентација (A, E) каде $A = \{a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ \bar{a},\ \bar{b},\ \hat{a},\ \hat{b},\ m\}$ и E содржи 33 дефинирачки равенства од кои 20 изразуваат комутативност на симболите од $\{a, b, c, d\}$ со оние од $\{f, \bar{a}, \bar{b}, \hat{a}, \hat{b}\}$, а останатите 13 се:

$$e\hat{a} = \hat{a}e, e\hat{b} = \hat{b}e, ea = \bar{a}e, eb = \bar{b}e, am = \hat{a}m,$$

$$bm = \hat{b}m, ha\bar{a} = ah, hb\bar{b} = bh, ag\hat{a} = ga, bg\hat{b} = gb,$$

$$df = dh, fd = gd, hc = cg,$$

има нерешлив проблем на зборови.

Пример 3 (G. C. Tzeitin, 1958, според [11])

Следната полугрупа зададена со презентација (A, E), каде $A =$

$\{a, b, c, d, e\}$, а $E = \{ac = ca, ad = da, bc = cb, bd = db, eca = ce, edb = de, cca = ccae\}$ има нерешлив проблем на зборови.

Пример 4 (Ј. Матијашевич , 1967, според [16])

Полугрупата со презентација (A, E), каде A е двоелементна азбука, $A = \{\alpha, \sigma\}$ и E е троелементно множество дефинирачки равенства, имено

$$E = \{\alpha\alpha\sigma\alpha\sigma = \sigma\alpha\alpha, \alpha\alpha\sigma\sigma = \sigma\alpha\alpha, L = M\}$$

каде L и M се специјални долги зборови, имено L има 304 букви, а M 608, има нерешлив проблем на зборови. Очигледно цената на намалувањето на бројот на дефинирачките равенства е зголемување на бројот на букви во иститe. Доказот и начинот на конструкција на ваквиот систем се преобемни, за да најдат свое место овде. Идеата е почнувајќи од презентација на полугрупа со нерешлив проблем на зборови, со соодветно претставување на буквите во двоелементна азбука, и трансформација на дефинирачките равенства да се дојде до овој систем.

Како последица од претходната теорема постои доказ на нерешливоста на проблемот на зборови за групи (П.С. Новиков 1955, W.W. Boone 1959, J. L. Britton 1963, G. Higman 1961). Од друга страна, докажано е од страна на W. Magnus, 1932, дека конечно презентираните групи со едно дефинирачко равенство имаат решлив проблем на зборови. Како што се појавувале примери на полугрупи со нерешливи проблеми на зборови, со се помалку дефинирачки равенства, така се добивани и соодветни примери за групи. Така, најмал досега познат пример е група со презентација на двоелементна азбука и 12 дефинирачки равенства, конструиран од В. В. Борисов, 1969, врз база на претходно наведениот *Пример 3*.

Сеуште е отворен проблемот за полугрупи со едно дефинирачко равенство. Наведуваме неколку резултати добиени во последно време во таа насока, како и некои резултати во врска со алгебарските својства на групи и полугрупи со решлив проблем на зборови *:

- (С. Адян, 1966) Проблемот на зборови е решлив за специјален вид моноиди со презентација $(A, \{w = e\})$ или $(A, \{u = v\})$ каде u и v имаат различни први букви и различни последни букви, e е ознака за празниот збор.

- (С. Адян, Г. Оганесян, 1978) Проблемот на одлучивост на проблемот на зборови за полугрупи со едно дефинирачко равенство се сведува на одлучивост на проблем на зборови за полугрупи со презентација $(A, \{bua = a\})$, и $(A, \{bua = ava\})$ каде $a, b \in A, a \neq b$.

- (Г. Оганесян, 1982) Проблемот на зборови е решлив во полугрупи со презентација $(A, \{bua = a\})$.

- (А. В. Кузнјецов, 1958; W.W. Boone, G. Higman, 1974) Конечно презентирана група [полугрупа] G има решлив проблем на зборови ако и само ако постои мономорфизам $\phi : G \to S$ каде S е ед-

*оригиналните трудови во кои се наогјаат доказите на сите наброени резултати не ми беа достапни, самите резултатите се преземени од [16, 11, 12] каде се нао—аат и скици на докази на дел од наведените тврдеща ноставна подгрупа [подполугрупа без конгруенции] на конечно презентирана група [полугрупа].

- (B.H. Neumann, 1973; R. McKenzie, R.J. Thompson, 1973) Конечно презентирана група [полугрупа] G има одлучив проблем на зборови ако G може да се смести во алгебарски затворена група [полугрупа] S. (S е алгебарски затворена ако секоја равенка со константи од S која е решлива во проширување на S има решенија во S).

4 Препишувачки системи

Во овој дел ќе се задржиме на дефинициите на препишувачки систем и особини на препишувачки системи (терминација, конфлуентност, комплетност, нормални форми), заедно со сите неопходни поими. Ќе бидат дадени основните својства поврзани со особините на препишувачките системи и нивни докази, како и осврт на докажување на терминација на препишувачки систем и осврт на постапката за комплетирање на препишувачки систем, односно од систем равенства добивање на комплетен препишувачки систем, позната како алгоритам на Knuth и Bendix. Всушност, како резултат од таа постапка е добиен примерот за групи наведен во воведот. Дефинициите на поимите и теоремите се дадени според [2, 3, 9, 19].

4.1 Дефиниција на препишувачки системи и релации

Во овој дел ги воведуваме основните дефиниции во врска со препишувачки системи, равенства, препишувачки правила. При тоа се задржуваме само на термовски препишувачки системи, иако поголем дел од наведената теорија се однесува општо на системи на редукција на било кое множество.

Понатаму, со $\mathcal{T}$ го означуваме множеството од сите терми (во некоја сигнатура I), со $\mathcal{G}$ множеството од сите базични терми (терми без променливи).

Секое пресликување од конечно множество променливи во множеството терми се нарекува *супституција*. За супституциите се користат мали грчки букви. Со Σ ќе биде означувано множеството од сите супституции. Нека s е терм и σ е супституција, со $s\sigma$ се означува термот кој се добива од s со истовремена замена на секоја од променливите од доменот на σ во s со соодветна слика при σ. Ако T е множество терми и σ е супституција т.ш. $(\forall s, t \in T)s\sigma = t\sigma$ тогаш велиме дека σ е *унификатор* на T. Унификаторот σ на множество терми T е *најопшт унификатор* ако за секој друг унификатор τ на T постои супституција ρ така што $\tau = \sigma \circ \rho$.

Теорема 29 (Теорема за унификација)

Ако за множество терми T постои унификатор, тогаш постои и најопшт унификатор. $\square$

Нека s е терм со должина (број на симболи) n. За $p \in \{1, \ldots, n\}$ велиме дека е позиција на s ако p-тиот симбол на s е операциски симбол од сигнатурата. Со $\mathcal{P}os(s)$ ќе го означува множеството од сите позиции на терм s, $s|_p$ е ознака за подтермот на s на позиција p, а $s[t]_p$ термот што се добива со замена на $s|_p$ во s со t.

Дефиниција 49 Една бинарна релација $\to$ на множество терми $\mathcal{T}$ е *препишувачка релација* ако е затворена за примена на контекст и инстанцирање, т.е.

$(\forall s, t, u \in \mathcal{T})(\forall p \in \mathcal{P}os(t))(\forall \sigma \in \Sigma)\ s \to t \implies u[s\sigma]_p \to u[t\sigma]_p.$ $\triangle$

Инверзијата, симетричниот затворач, рефлексивниот затворач и транзитивниот затворач на секоја препишувачка релација се исто така препишувачки релации. Јасно, секоја еквиваленција на множество терми која е препишувачка релација е конгруенција на алгебрата терми.

Подредување на терми кое е препишувачка релација се *нарекува препишувачко подредување.*

Дефиниција 50 *Правило за препишување* е пар терми и се запишува $l \to r, (\, l, r \in \mathcal{T})$. Препишувачки систем е пар $(\mathcal{T}, R)$, каде R е множество правила за препишување.

Нека R е множество правила за препишување. Дефинираме препишувачка релација која се добива од R.

За терм s велиме дека *се препишува во еден чекор до* терм t на позиција p со употреба на правило $l \to r \in R$ ако постои супституција σ таква што $s|_p = l\sigma$ и $t = s[r\sigma]_p$. Во тој случај, за $s|_p$ велиме дека е *редекс*. Означуваме $s{\to^p}_{l\to r}t$ или $t{\leftarrow^p}_{l\to r}s$, а понекогаш и ги испуштаме индексите за правилото и позицијата, односно, наместо ${\to^p}_{l\to r}$ пишуваме само $\to_R$.

Рефлексивното проширување на дефинираната релација се означува со ${\to^=}_R$ (*се препишува во нула или еден чекор*), рефлексивното и транзитивно проширување на дефинираната препишувачка релација се нарекува *релација на изведување (се препишува до)* и се означува со ${\to^*}_R$, додека ${\leftrightarrow^*}_R$ е ознака за конгруенцијата генерирана од R. Да забележиме дека $\leftrightarrow^* = (\to \cup \leftarrow)^*$.

Низа од препишувања $s{\leftrightarrow^*}_R t$ се нарекува *доказ* (на еквивалентност на s и t).

Дефиниција 51 Велиме дека термите s и t се *конвертибилни* ако постои доказ $s \leftrightarrow^*{}_R\, t$. $\triangle$

За различни форми на докази, употребуваме соодветни имиња. Така, $s \rightarrow^*{}_R\, u \leftarrow^*{}_R\, t$ се нарекува *долина* или *препишувачки доказ*, во кој случај за s и t велиме дека се *конвергентни*; $s \rightarrow^={}_R\, u \leftarrow^={}_R\, t$ се нарекува *рамен* или *дијамантски* доказ; $s \leftarrow_R u \rightarrow_R t$ се нарекува *врв*; $s \leftarrow^*{}_R\, u \rightarrow^*{}_R\, t$ се вика *планина*.

Дефиниција 52 Терм t е *редуцибилен* ако содржи редекс, а *иредуцибилен (во нормална форма)* инаку. $\triangle$

Терм s *има нормална форма* ако постои иредуцибилен терм t т.ш. $s \rightarrow_R^* t$.

За препишувачкиот систем R велиме дека е *функционален (нормализирачки)* ако секој терм t има нормална форма и постои алгоритам со кој истата се определува.

4.2 Својства на препишувачките системи и релации

Веќе дефиниравме едно својство на препишувачки систем, имено функционалноста. Функционалноста е најпожелната карактеристика на еден препишувачки систем. За жал, таа е неодлучива и често е многу тешко да се оствари. Затоа се задржуваме на неколку својства на препишувачките системи, и врските помеѓу нив. Всушнот дефинираме својства на препишувачките релации, но, понатаму, без посебно нагласување, својство на препишувачка релација го поистоветуваме со својство на препишувачки систем од кој релацијата настанува.

Дефиниција 53 За препишувачката релација $\rightarrow$ велиме дека е:

$Church - Rosser$ ако за секој доказ постои препишувачки доказ:

$(\forall u, v \in \mathcal{T})(u \leftrightarrow^* v \implies (\exists t \in \mathcal{T})\ u \rightarrow^* t \leftarrow^* v)$;

конфлуентна ако за секоја планина постои долина, т.е. препишувачки доказ:

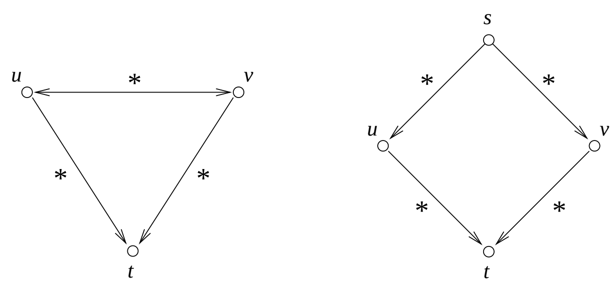
$(\forall u, v, s \in \mathcal{T})(u \leftarrow^* s \rightarrow^* v \implies (\exists t \in \mathcal{T})\ u \rightarrow^* t \leftarrow^* v)$;

локално конфлуентна ако за секој врв постои долина, т.е препишувачки доказ:

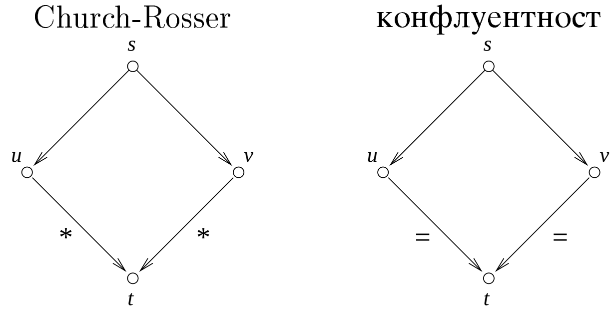
$(\forall u, v, s \in \mathcal{T})(u \leftarrow s \rightarrow v \implies (\exists t \in \mathcal{T})\ u \rightarrow^* t \leftarrow^* v)$;

јако конфлуентна ако за секој врв постои дијамантски доказ:

$(\forall u, v, s \in \mathcal{T})(u \leftarrow s \rightarrow v \implies (\exists t \in \mathcal{T})\ u \rightarrow^= t \leftarrow^= v)$.



Church-Rosser конфлуентност

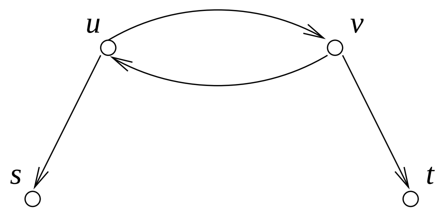


локална конфлуентност јака конфлуентност

Јасно е дека секоја конфлуентна релација е локално конфлуентна, обратното во општ случај не важи.

Пример 5 (Hindly)

Препишувачка релација која е локално конфлуентна но не е конфлуентна.



Својство 16 Препишувачка релација е конфлуентна ако и само ако е Church- Rosser.

Пред да го дадеме доказот на ова тврдење, ќе се задржиме на две помошни својства.

Лема 4 За секои две релации α и β на множество A важи

$$\beta = \Delta_A \cup \alpha \cdot \beta \implies \alpha^* \subseteq \beta.$$

Доказ. Од $\Delta_A \subseteq \beta$, $\alpha \subseteq \alpha \cdot \beta \subseteq \beta$, со индукција тривијално се покажува дека $(\forall n \in \mathbf{N})\alpha^n \subseteq \beta$. $\square$

Лема 5 За произволни две релации α и β на множество A важи: $(\alpha \cup \beta)^* = \alpha^* \cdot (\beta \cdot \alpha^*)^*$.

Доказ. За да се докаже "$\subseteq$" делот, доволно е да се утврди (според *Лема 4*) дека $\gamma = \alpha^* \cdot (\beta \cdot \alpha^*)^*$ задоволува $\gamma = \Delta_A \cup (\alpha \cup \beta) \cdot \gamma$. Имаме,

$$\begin{array}{rcl} \alpha^* \cdot (\beta \cdot \alpha^*)^* & = & (\beta \cdot \alpha^*)^* \cup \alpha \cdot \alpha^* \cdot (\beta \cdot \alpha^*)^* \\ & = & \Delta_A \cup \beta \cdot \alpha^* \cdot (\beta \cdot \alpha^*)^* \cup \alpha \cdot \alpha^* \cdot (\beta \cdot \alpha^*)^* \ \cdot \\ & = & \Delta_A \cup (\alpha \cup \beta) \cdot \alpha^* \cdot (\beta \cdot \alpha^*)^* \end{array}$$

Обратната инклузија следува веднаш од дефиницијата на $(\alpha \cup \beta)^*$. $\square$

Доказ (*Својство 16*) Нека $\rightarrow$ е Church - Rosser. Значи, за секои два терми, имаме: ако се конвертибилни, тогаш се конвергентни. Сега нека $x \leftarrow^* u \rightarrow^* y$. Тогаш x и y се конвертибилни, па и конвергентни.

Обратно, нека $\rightarrow$ е конфлуентна. Според *Лема 5* имаме

$$\leftrightarrow^* = \rightarrow^* \cdot \bigcup((\leftarrow \cdot \rightarrow^*)^n | n \in \mathbf{N}).$$

Со индукција по n ќе докажеме дека

$$(\forall n \in \mathbf{N})(\leftarrow \cdot \rightarrow^*)^n \subseteq \rightarrow^* \cdot \leftarrow^* .$$

За $n = 0$ тврдењето е тривијално исполнето. Ако $(\leftarrow \cdot \rightarrow^*)^n \subseteq \rightarrow^* \cdot \leftarrow^*$, тогаш

$$\begin{array}{rcl} (\leftarrow \cdot \rightarrow^*)^{n+1} & = & \leftarrow \cdot \rightarrow^* \cdot (\leftarrow \cdot \rightarrow^*)^n \\ & \subseteq & \leftarrow \cdot \rightarrow^* \cdot \rightarrow^* \cdot \leftarrow^* \\ & = & \leftarrow \cdot \rightarrow^* \cdot \leftarrow^* \\ & \subseteq & \rightarrow^* \cdot \leftarrow^* \cdot \leftarrow^* \\ & = & \rightarrow^* \cdot \leftarrow^* \end{array}$$

при што последната инклузија е последица од конфлуентноста.

Значи, $\leftrightarrow^* \subseteq \to^* \cdot \leftarrow^*$, т.е. $\to$ е Church-Rosser. $\square$

Дефиниција 54 За препишувачката релација $\to$ велиме дека е *терминирачка (строго нормализирачка)* ако не постои бесконечна низа од облик $t_0 \to t_1 \to \cdots \to t_i \to \ldots$.

Терминирачки и конфлуентен препишувачки систем се нарекува *комплетен*. Јасно е дека секој комплетен систем е функционален, секое препишување води до единствената нормална форма.

Теорема 30 *(*Лема на Newmann)

Нека $\to$ е терминирачка. Тогаш $\to$ е конфлуентна ако и само ако е локално конфлуентна.

Доказ Доволно е да се докаже дека локалната конфлуентност повлекува конфлуентност, при терминирачки препишувачки систем. Нека $(\mathcal{T}, R)$ е терминирачки препишувачки систем кој е локално конфлуентен. Треба да докажеме дека

$$(\forall u, v, s \in \mathcal{T})(u \leftarrow^* \ s \to^* \ v \implies (\exists t \in \mathcal{T})\ u \to^* \ t \leftarrow^* \ v).$$

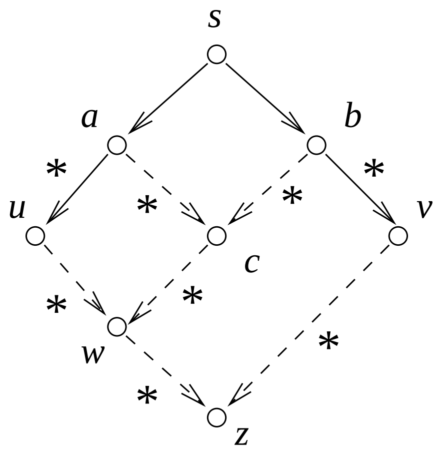
Доказот ќе го изведеме со индукција. Имено, дефинираме:

$\mathcal{P}(s)$ ако и само ако $(\forall u, v \in \mathcal{T})(u \leftarrow^* s \to^* v \implies (\exists t \in \mathcal{T}) u \to^* t \leftarrow^* v)$.

Потребно е да се провери вистинитоста на тврдењето

$$(\forall s \in \mathcal{T})((\forall x \in \mathcal{T})(s \to x \implies \mathcal{P}(x)) \implies \mathcal{P}(s)).$$

Ако $s \in \mathcal{T}$ е иредуцибилен, тогаш $\mathcal{P}(s)$ е секако тривијално исполнета, а со тоа е покажан базниот чекор. Натаму, нека $s \in \mathcal{T}$ и нека $u, v \in \mathcal{T}$ се такви што $s \to^* u, s \to^* v,\ (u \neq v)$. Тогаш постојат елементи $a, b \in \mathcal{T}$ такви што $s \to a \to^* u, s \to b \to^* v$. Сега, од локалната конфлуентност, се добива дека постои $c \in \mathcal{T}$, $a \to^* c, b \to^* c$. Според индуктивната претпоставка важи $\mathcal{P}(a)$. Значи постои $w \in \mathcal{T}$ таков што $c \to^* w \leftarrow^* u$, од каде следува $b \to^* w$. Со уште една примена на индуктивната претпоставка за b важи $\mathcal{P}(b)$, па постои $z \in \mathcal{T}$ таков што $w \to^* z \leftarrow^* v$, што значи дека е исполнето $\mathcal{P}(s)$.



□

Како последица се добива битен критериум за комплетност.

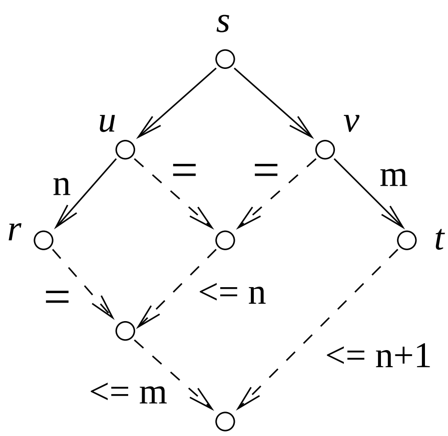
Последица 5 Еден препишувачки систем е комплетен ако и само ако е локално конфлуентен и терминирачки. □

Како алтернатива на терминацијата се користи јаката конфлуентност. Имено, го имаме следниот резултат.

Теорема 31 *(*Лема на Rosen)

Релацијата $\to$ е конфлуентна ако е јако конфлуентна.

Доказ Доказот повторно се изведува едноставно со индукција, користејќи аргументи на поплочување, имено, сосема е јасно ако се има на ум следниот цртеж.



□

4.3 Терминација на термовски препишувачки систем

Ја дефиниравме особината на терминирање на даден препишувачки систем. Исто така, јасна е важноста на оваа особина од лемата на Newmann. За жал, терминацијата е неодлучива во општ случај, освен за препишувачки системи без променливи. Докажувањето терминација исто така, во општ случај, не е едноставна работа и користи голем дел од теоријата на подредувања. Во овој дел ќе се задржиме накратко на некои основни методи и примери за докажување терминација на термовски препишувачки системи. Наведените примери се според [3, 4].

Дефиниција 55 *Редукциско подредување* на множество терми $\mathcal{T}$ е секое добро основано препишувачко подредување на $\mathcal{T}$. (Една релација R е добро основана ако не постои бесконечна низа $a_1 R a_2 R \ldots$.) △

Терминацијата е обезбедена ако $l > r$ за секое правило $l \to r \in R$, каде $>$ е редукциско подредување. Од друга страна, ако $(\mathcal{T}, R)$ терминира, тогаш самата релација $\to_R^+$ е редукциско подредување. Затоа за докажување терминација, потребни ни се доволно силни редукциски подредувања. Во литературата се среќаваат огромен број на различни редукциски подредувања за докажување терминација. Овде ќе се задржиме накратко на некои од нив. Исто така, често пати наместо конкретно редукциско подредување на терми, всушност зборуваме за интерпретација (пресликување) на термите во некое "стандардно" добро подредено множество, така што конкретниот препишувачки систем задоволува $u \to v \Leftrightarrow |u| > |v|$, за секои два терми u и v, каде со $|t|$ е означена интерпретацијата на терм t, а ">" е добро основано подредување на множеството во кое ги интерпретираме термите.

Пример 6 (Лупи)

Следниот систем од 12 правила за препишување е даден од $\mathrm{T.\ Evans}$, 1951 и дава постапка за определување на нормални форми за лупи при сигнатура $\{\cdot, \backslash, /, e\}$.

$x \backslash x \to e$	$x/x \to e$	$e \cdot x \to x$
$x \cdot e \to x$	$e \backslash x \to x$	$x/e \to x$
$x \cdot (x \backslash y) \to y$	$(y/x) \cdot x \to y$	$x \backslash (x \cdot y) \to y$
$(y \cdot x)/x \to y$	$x/(y \backslash x) \to y$	$(x/y) \backslash x \to y$

Системот терминира бидејќи примена на произволно правило на произволен редекс на терм t ја намалува големината (бројот на симболи) на t.

Пример 7 (Дел од теоријата на групи)

Системот

$$
\begin{array}{cc}
\hline
1 \cdot x \to x & x \cdot 1 \to x \\
x^{-} \cdot x \to 1 & x \cdot x^{-} \to 1 \\
1^{-} \to 1 & (x^{-})^{-} \to x \\
x^{-} \cdot (x \cdot y) \to y & x \cdot (x^{-} \cdot y) \to y \\
\hline
\end{array}
$$

терминира од истите причини како и претходниот.

Овде да напоменеме дека не е доволно левата страна на секое правило да е подолга од десната, бидејќи ако имаме правило во кое на десна страна одредена променлива се појавува повеќе пати отколку на лева, на пример $(x \cdot y) \cdot z \to y \cdot y$, тогаш примена од типот $(a \cdot (b \cdot b)) \cdot c \to ((b \cdot b) \cdot (b \cdot b)) \cdot c$ предизвикува зголемување на големината на термот (всушност ова барање е содржано во дефиницијата на препишувачко подредување).

Пример 8 (употреба на полиномна интерпретација, симболичко диференцирање, Lankford, 1979)

Терминација на системот

$$
\begin{aligned}
Dt &\rightarrow 1 \\
D(const) &\rightarrow 0 \\
D(x+y) &\rightarrow Dx+Dy \\
D(x\times y) &\rightarrow (x\times Dy)+(y\times Dx) \\
D(x-y) &\rightarrow Dx-Dy \\
D(-x) &\rightarrow -D(x) \\
D(x/y) &\rightarrow (Dx/y)-(x\times Dy/y^2) \\
D(lnx) &\rightarrow Dx/x \\
D(x^y) &\rightarrow (y\times x^{y-1}\times Dx)+(x^y\times(lnx)\times Dy)
\end{aligned}
$$

се докажува со следната полиномна интерпретација:

$$
\begin{aligned}
\|x+y\| &= \|x\|+\|y\| & \|x-y\| &= \|x\|+\|y\| \\
\|x^y\| &= \|x\|+2\|y\| & \|-x\| &= \|x\|+1 \\
\|const\| &= 2 & \|t\| &= 2 \\
\|x\times y\| &= \|x\|+\|y\| & \|x/y\| &= \|x\|+2\|y\| \\
\|Dx\| &= \|x\|^2 & \|lnx\| &= \|x\|+1
\end{aligned}
$$

Општо идеата за полиномна интерпретација потекнува од Lankford и се состои во следново. На секој n-арен симбол од сигнатурата $\mathcal{F}$ на $\mathcal{T}_{\mathcal{F}}$ му се придружува по еден целоброен полином од n променливи. Изборот на коефициентите мора да го осигура условот на монотоност и термите мора да се пресликуваат во природни броеви. Потоа, мора да се докаже дека секое правило е редуцирачко, односно дека за секое правило $l \rightarrow r$ важи: $|l|-|r|$ е позитивен за сите вредности на променливите поголеми од минималната вредност на базичен терм (каде со $|t|$ е означена интерпретацијата на терм t). Всушност, со оваа интерпретација, променливите се интерпретираат во променливи над множеството природни броеви.

Постојат и повеќе често употребувани методи на дефинирање на посложени препишувачки подредувања, врз база на стандардни добро основани подредувања. На кратко ќе се задржиме на некои од нив. Наједноставен метод е **лексикографско проширување**. Со него n добро основани подредувања $>_1, >_2, \cdots >_n$ на множества $A_1, \ldots, A_n$, соодветно, се трансформираат во добро основано подредување $(>_1, \ldots, >_N)_{lex}$ на директниот производ $A_1 \times \cdots \times A_n$, на следниот начин:

$$(a_1, \ldots, a_n)(>_1, \ldots, >_N)_{lex}(b_1, \ldots, b_n)$$

ако $a_1 >_1 b_1$ или $a_1 = b_1, (a_2, \ldots, a_n)(>_2, \ldots, >_N)_{lex}(b_2, \ldots, b_n)$.

Ако $>_1 = \cdots = >_n$, пишуваме $>_{lex}$.

Пример 9 Даден е препишувачки систем од две правила:

$$f(f(x)) \to g(f(x))$$
$$g(g(x)) \to f(x)$$

Истиот лесно се уочува дека терминира ако се има на ум лексикографското подредување $(>, >)_{lex}$ и интерпретацијата $\|\| : \mathcal{T} \to \mathbb{N} \times \mathbb{N}$ определена со: $\|t\| = (t_1, t_2)$, каде t_1 е големина - број на симболи во t, а t_2 е број на симболи f во термот t.

Пример 10 Во следниот систем се користи пар од интерпретации и лексикографско подредување за докажување на неговата терминација.

$$
\begin{array}{lll}
\hline
x \cdot (y+z) & \to & (x \cdot y) + (x \cdot z) \\
(y+z) \cdot x & \to & (x \cdot y) + (x \cdot z) \\
(x \cdot y) \cdot z & \to & x \cdot (y \cdot z) \\
(x+y)+z & \to & x + (y+z) \\
\hline
\end{array}
$$

Парот интерпретации $(\|t\|, \|t\|')$, е определен со

$$
\begin{aligned}
\|x \cdot y\| &= \|x\| \cdot \|y\| \\
\|x + y\| &= \|x\| + \|y\| + 1 \\
\|const\| &= 2
\end{aligned}
$$

и

$$
\begin{aligned}
\|x \cdot y\|' &= 2\|x\|' + \|y\|' \\
\|x + y\|' &= 2\|x\|' + \|y\|' \\
\|const\|' &= 2
\end{aligned}
$$

Имено, првите две правила ја намалуваат првата интерпретација, а вторите две првата не ја менуваат, а ја намалуваат втората.

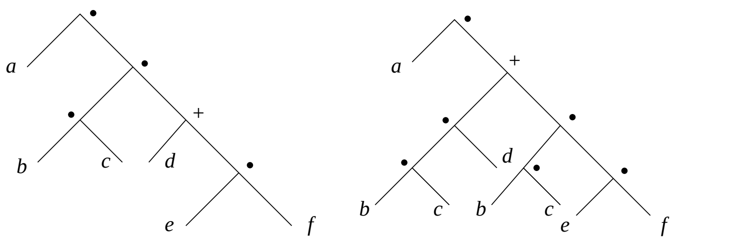
Друг метод е **проширување на мултимножества**. Конечно мултимножество (или вреќа) е пресликување од конечно множество S во множеството природни броеви. Всушност сликата на секој елемент означува број на појавувања на елементот во мултимножеството. Сега, ако $>$ е подредување на S, тогаш подредувањето $>_{mul}$ на мултимножествата со елементите на S се дефинира како транзитивен затворач на релацијата на замена на еден елемент со конечен број (може и нула) елементи кои се помали од него во однос на $>$.

Пример 11 Системот составен од следното правило (дистрибутивност)

$$x \cdot (y + z) \to (x \cdot y) + (x \cdot z)$$

го наведуваме како пример за докажување терминација со помош на мултимножества. Имено, се дефинира редукциско подредување на термите на следниот начин. За секој терм конструираме мултимножество чии елементи се од n -торки од броеви. Термот се претставува со коренско дрво од горе надолу. На секој најдолен симбол "$\cdot$" во коренското стебло, му се придружува по една n-торка броеви на следниот начин. На секој симбол "$\cdot$" на патот од најдолен симбол "$\cdot$" до коренот на стеблото соодветствува по еден број - бројот на јазли во потстеблото чиј коренски симбол е разгледуваниот симбол "$\cdot$". Потоа, n - торките се споредуваат лексикографски, а мултимножествата според соодветното индуцирано подредување.

Така, на пример термите $a\cdot((b\cdot c)\cdot(d+(e\cdot f)))$ и $a\cdot(((b\cdot c)\cdot d)+((b\cdot c)\cdot(e\cdot f)))$ се претставуваат со коренски стебла како на следната слика и со



$a \cdot ((b \cdot c) \cdot (d + (e \cdot f)))$ $\quad$ $a \cdot ((b \cdot c) \cdot d + (b \cdot c) \cdot (e \cdot f))$

мултимножествата $\{< 3, 9, 11 >, < 3, 9, 11.\}$ и $\{< 3, 5, 15 >, < 3, 7, 15 >, < 3, 7, 15 >\}$, соодветно. Притоа второто мултимножество е помало, бидејќи секој негов елемент е лексикографски строго помал од $< 3, 9, 11 >$ кој се појавува во првото мултимножество.

Трет метод е **подредување на патеки**. Овој метод трансформира произволно добро основано подредување $\succeq$ (приоритет) на азбука $\mathcal{F}$ од функциски симболи во препишувачко подредување на множеството базични терми во сигнатура $\mathcal{F}$. Идеата е дека терм s треба да е поголем од секој терм кој е изграден од терми помали од s поврзани со функциски симболи помали (по приоритет) од коренот на s. При тоа, "помали од s" се подразбира рекурзивно, при истото подредување. Два дадени терми s и t, прво се споредуваат по приоритет на коренскиот функциски симбол: ако коренот на s е со поголем приоритет од коренот на t, t може да е поголем од s само ако некој од неговите подтерми е поголем од s. Притоа, постојат два основни типа на подредување на патеки, **лексикографско подредување на патеки** и **подредување на патеки со мултимножества**, како и нивни комбинации, од коишто најчесто е користено така нараченото **рекурзивно подредување на патеки**.

Нека е дадено подредување по приоритет $\succeq$ на азбука $\mathcal{F}$.

Подредувањето на патеки со мултимножества $\succeq_{mul}$ се дефинира на следниот начин:

$f(s_1, \ldots, s_n)$	$\succ_{mul}$	s_i	$1 \leq i \leq n$
$f(s_1, \ldots, s_n)$	$\succ_{mul}$	$g(t_1, \ldots, t_m)$	$f \succ q, f(s_1, \ldots, s_n) \succ_{mul} t_1, \ldots, t_m$
$f(s_1, \ldots, s_i, \ldots, s_n)$	$\succ_{mul}$	$g(s_1, \ldots t_1, \ldots, t_k, \ldots, s_n)$	$f \preceq g, s_i \succ_{mul} t_1, \ldots, t_k, k \geq 0$
$f(s_1, \ldots, s_n)$	$\approx_{mul}$	$g(s_{\pi_1}, \ldots, s_{\pi_n})$	$f \approx q, \pi$ е пермутација

Пример 12 (Дисјунктивна нормална форма, Dershowitz, 1982)

За пример на употреба на подредување на патеки со мултимножества при докажување терминација го даваме следниот препишувачки систем.

$\neg\neg x$	$\to$	x
$\neg(x \vee y)$	$\to$	$\neg x \wedge \neg y$
$\neg(x \wedge y)$	$\to$	$\neg x \vee \neg y$
$x \wedge (y \vee z)$	$\to$	$(x \wedge y) \vee (x \wedge z)$
$(y \vee z) \wedge x$	$\to$	$(x \wedge y) \vee (x \wedge z)$

Притоа, приоритетот е зададен со $\neg \succ \wedge \succ \vee$.

Лексикографското подредување на патеки $\succeq_{lex}$ се дефинира на следниот начин:

$f(s_1,\ldots,s_n) \succ_{lex} s_i$	$1 \leq i \leq n$
$f(s_1,\ldots,s_n) \succ_{lex} g(t_1,\ldots,t_m)$	$f \succ q, f(s_1,\ldots,s_n) \succ_{lex} t_1,\ldots,t_m$
$f(s_1,\ldots,s_i,\ldots,s_n) \succeq_{lex} f(s_1,\ldots,s_{i-1},t_i,\ldots\ldots t_n)$	$s_i \succeq_{lex} t_i,$
	$f(s_1,\ldots,s_n) \succ_{lex} t_{i+1},\ldots,t_n$
$f(s_1,\ldots,s_n) \succ_{lex} g(s_1,\ldots,s_m)$	$f \approx g, m < n$
$f(s_1,\ldots,s_n) \approx_{lex} g(s_1,\ldots,s_n)$	$f \approx g$

Овде, како и во подредувањето со мултимножества, приоритетот индуцира подредување на термите, но подтермите од исти функциски симбол се подредуваат од лево на десно, лексикографски.

Пример 13 За доказ на терминација на системот

$ack(0,y)$	$\to$	$succ(y)$
$ack(succ(x),0)$	$\to$	$ack(x,succ(0))$
$ack(succ(x),succ(y))$	$\to$	$ack(x,ack(succ(x),y))$

за функцијата на $\mathrm{Ackerman}$ се користи лексикографско подредување на патеки, при приоритет $ack \succ succ$.

При **рекурзивното подредување на патеки**, пред се на секој елемент од $\mathcal{F}$ му се доделува статус - лексикографски или на мултимножество, т.е. $\mathcal{F}$ се дели на две подмножества Lex и Mul. Потоа дефиницијата на индуцираното подредување е следната:

$$s = f(s_1, \ldots, s_m) \succeq_{rpo} g(t_1, \ldots, t_n) = t$$

ако важи еден од следните три услови

(i) $s_i \succeq t$, за некој $i \in \{1, \ldots, m\}$,

(ii) $f = g$ и

1. $f \in Lex$ и $s \succ_{rpo} t_1, \ldots, s \succ_{rpo} t_n, (s_1, \ldots, s_n)(\succeq_{rpo})_{lex}(t_1, \ldots, t_n)$,
2. $f \in Mul$ и $(s_1, \ldots, s_n)(\succeq_{rpo})_{mul}(t_1, \ldots, t_n)$,

(iii) $f \succ g$ и $s \succ_{rpo} t_i$, за секој $i \in \{1, \ldots, n\}$.

Кога $\succ$ е линеарно подредување на $\mathcal{F}$, тогаши $\succ_{rpo}$ е линеарно подредување. Индуцираното подредувањето е стриктно ако $Mul = \emptyset$. Ова досега се однесуваше на подредување на базични терми, а за терми со променливи можно е вака дефинираното подредување да се прошири до препишувачко со $s \succeq_{rpo} t$ ако и само ако $s\sigma \succeq_{rpo} t\sigma$, за секоја базична супституција σ, или пак со третирање на променливите како нови константи неспоредливи со ниеден функциски симбол, ниту меѓу себе во $\succ$.

За препишувачкиот систем за групи наведен во воведот, терминацијата се докажува со помош на еден вид рекурзивно подредување на патеки, познато како подредување на Knuth - Bendix.

4.4 Комплетирање на термовски препишувачки систем

Веќе спомнавме дека препишувачките системи ни се од интерес за решавање на проблеми на зборови. Притоа проблемот се сведува на следново: за дадена конгруенција на конечно презентирана алгебра (во случајов алгебра терми) да се дефинира комплетен препишувачки систем кој ја генерира истата конгруенција. Бидејќи, секако, различни препишувачки системи може да генерираат иста релација, потребен ни е поимот за нивна еквивалентност.

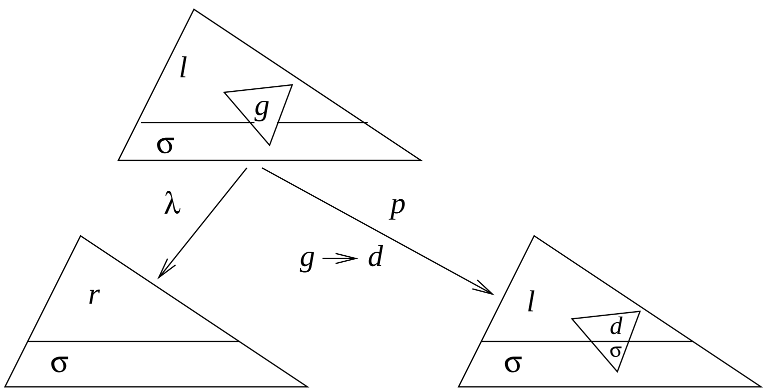
Дефиниција 56 Два термовски препишувачки системи $(\mathcal{T}, \rightarrow), (\mathcal{T}, \Rightarrow)$ се *еквивалентни* ако $\leftrightarrow^* = \Leftrightarrow^*$. $\triangle$

Секој комплетен препишувачки систем еквивалентен на даден препишувачки систем $(\mathcal{T}, \rightarrow)$ се нарекува негово *комплетирање*.

Се поставува прашањето дали секој препишувачки систем има комплетирање. Со употреба на аксиомата на избор се добива позитивен одговор на ова прашање, но во општ случај невозможно е истото да се конструира алгоритамски. Идејата за алгоритамско комплетирање на даден препишувачки систем е базирана на *Последица 5*. Всушност, поаѓајќи од еден препишувачки систем се обидуваме да конструираме негово комлетирање лоцирајќи ги сите ситуации во кои е нарушена локалната конфлуентност. Постапката за комплетирање на препишувачки систем потекнува од Knuth и Bendix, а постојат и повеќе подобрувања на истата во смисла на ефикасност. Накратко, што е идејата: почнуваме со даден терминирачки препишувачки систем $(\mathcal{T}, \to)$ и го определуваме множеството од сите "критични парови" на $\to$, при што $(x, y) \in \mathcal{T} \times \mathcal{T}$ е критичен пар ако ја нарушува локалната конфлуентност т.е. постои $z \in \mathcal{T}$ таков што $z \to x, z \to y$, но x и y не се конвергентни. Јасно, ако ова множество е празно, тогаш системот е комплетен. Но, ако постои критичен пар (x, y), тогаш воспоставуваме локална конфлуентност со додавање на едно од правилата $x \to y$ или $y \to x$ водејќи сметка да не се наруши терминацијата. Ако и двете овие правила ја нарушуваат терминацијата постапката завршува со неуспех, инаку ја повторуваме постапката за вака проширената релација. Притоа повторно има две можности - постапката да заврши со релација која е локално конфлуентна и терминирачка, односно, со комплетирање на системот, или никогаш да не заврши. Инаку, јасно е дека со секое додавање на правило се добива еквивалентен препишувачки систем. При практична имплементација секако е битен и изборот на критичен пар во даден момент, како и многу други детали. Истата постапка е особено погодна од алгебарски аспект, т.е. од аспект на замена на систем од равенства (идентитети) со систем правила за препишување. Почнувајќи од систем равенства доколку истите се насочат и се примени постапката, се добива евентуално препишувачки систем кој е комплетен и кој ја генерира истата конгруенција. Ова е корисно за алгоритамско опишување на слободните алгебарски структури со помош на канонични претставници, како и за решавање на проблемот на зборови во дадено многуобразие алгебри, секако доколку постапката заврши со успех.

Во продолжение ќе ги дадеме основните дефиниции и својства за прецизно определување на постапката за комплетирање, без задржување на многу детали. Постапка е детално обработена во [2, 9, 19].

Дефиниција 57 Нека $l \to r$ и $g \to d$ се две правила за препишување (со дисјунктни променливи - по потреба преименувани) и нека σ е најопшт унификатор на g и подтерм $l|_p$ од l кој не е променлива. Тогаш врвот $r\sigma \xleftarrow{\lambda}_{l\to r} l\sigma \to^{p}_{g\to d} l\sigma[d\sigma]_p$ е *критичен*, а парот $(r\sigma, l\sigma[d\sigma]_p)$ е *критичен пар*. Со $CP(R)$ го означуваме множеството од сите критични парови настанати од правилата на R. △



Критичен врв и критичен пар

Следното својство покажува дека сите критични ситуации до кои може да дојдеме при проверка на локална конфлуентност се инстанци од критични парови, т.е. концептот на критични парови ја опишува критичната ситуација на најопшт начин.

Својство 17 Нека $l_1 \to r_1, l_2 \to r_2$ се две правила од препишувачки систем R. Нека p е позиција на l_1 и подтермот $l_1|_p$ не е променлива. Ако постојат супституции σ_1 и σ_2, такви што $l_1|_p\sigma_1 = l_2\sigma_2$, тогаш постои критичен пар $(t_1, t_2) \in CP(R)$ и супституција σ, така што $t_1\sigma = l_1\sigma_1$ и $t_2\sigma = l_1\sigma_1[r_2\sigma_2]_p$. □

Теорема 32 (Тест на Huet за локална конфлуентност)

Еден препишувачки систем е локално конфлуентен ако и само ако сите негови критични парови се конвергентни. □

Конечен препишувачки систем има конечно множество критични парови, според тоа, локалната конфлуентност е одлучиво својство за конечни препишувачки системи. Исто така е и комплетноста, според лемата на Newman за терминирачки и конечни препишувачки системи. Така, следната теорема е директна последица од претходната и од лемата на Newman.

Теорема 33 (Knuth - Bendix)

Терминирачки препишувачки систем R е конфлуентен ако и само ако секој критичен пар $(t', t'') \in CP(R)$ е конвергентен. □

Во продолжение на кратко ја даваме постапката на Knuth и Bendix за комплетирање, која е базирана на претходната теорема.

Нека R е конечен терминирачки препишувачки систем. Со постапката се генерира низа $(R_n | n \in \mathbf{N})$ конечни множества правила за препишување, кои ги задоволуваат следните два услови:

(1) R_n е терминирачки и еквивалентен на R, и

(2) Секој критичен пар на R е конвергентен во R_{n+1}.

Во постапката за пресметување презентирана во продолжение, истата евентуално завршува со комплетен систем соодветен на спецификација зададена со равенства.

Постапка за комплетирање на Knuth - Bendix

Влез:

- спецификација со равенства $(\mathcal{F}, E)$,
- редукциско подредување на $\mathcal{T}_{\mathcal{F}}$

Излез: комплетен термовски препишувачки систем R со особината

$$(\forall s, t \in \mathcal{T}_{\mathcal{F}} s \leftrightarrow_R t \Leftrightarrow (\mathcal{F}, E) \vdash s \approx t$$

Почни

$R := \emptyset$;

додека $E \neq \emptyset$ прави

избери равенство $s = t$ од E

редуцирај ги s и t до соодветни нормални форми s' и t' (во однос на R)

ако $s' \equiv t'$ тогаш

$E := E - \{s = t\}$

инаку

ако $s' > t'$ тогаш

$\alpha := s', \beta := t'$

инаку ако $t' > s'$ тогаш

$\alpha := t', \beta := s'$

инаку *неуспех*

крај; {ако}

$CP := \{p = q | (p, q)$ критичен пар меѓу

правилата од R и $\alpha \to \beta\}$;

$R = R \cup \{\alpha \to \beta\}$;

$E = E \cup CP - \{s \approx t\}$

крај; {ако}

крај; {додека}

Крај.

Најголем проблем секако е определување на подредувањето, но на тоа во моментов воопшто не се задржуваме. Доказот на коректноста на постапката за комплетирање е прилично сложен и прв го дал Huet, 1981. Детални насоки за докажување на комплетноста се дадени во [2, 9].

5 Слободни слупи и проблем на зборови

Во овој дел се задржуваме на многуобразието слупи, односно Штајнерови лупи. Даваме опис на слободните слупи, и решение на проблемот на зборови во ова многуобразие, односно доказ дека истиот е решлив користејќи ги резултатите на T.Evans и конструкција на препишувачки систем за негово решавање.

5.1 Воведни поими

Штајнерова лупа или слупа е алгебра $(L; \cdot, 1)$, каде $\cdot$ е бинарна операција и 1 е константа, која ги задоволува идентитетите

(S1)	$1 \cdot x = x$
(S2)	$x \cdot y = y \cdot x$
(S3)	$x \cdot (x \cdot y) = y$

Штајнеров систем тројки е пар (L, M) каде L е конечно множество, M е множество триелементни подмножества од L со својството, за секои $a, b \in L$ $(a \neq b)$ постои единствен $c \in L$ така што $\{a, b, c\} \in M$. Јасно е дека секој Штајнеров систем тројки на множество L овозможува конструкција на слупа со носител $L \cup \{1\}$ каде $1 \notin L$, и обратно. Значи постои обратна еднозначна кореспонденција помеѓу Штајнеровите системи тројки и конечните слупи.

Класата инволуторни комутативни лупи е дефинирана со законите: $1x = x,\ xy = yx,\ xx = 1,\ (\forall x, y)(\exists! z, u)(xz = y,\ ux = y)$.

Својство 18 Многуобразието слупи е вистинско подмногуобразие од класата инволуторни комутативни лупи.

Доказ Ако $(L; \cdot, 1)$ е слупа, тогаш равенката $ax = b$ за произволни $a, b \in L$ има единствено решение $x = ab$. Во продолжение даваме пример на инволуторна комутативна лупа која не е слупа:

$\cdot$	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	c	d	e	b
b	b	c	1	e	a	d
c	c	d	e	1	b	a
d	d	e	a	b	1	c
e	e	b	d	a	c	1

$\square$

Понатаму го користиме терминот *база* за минимално генераторно множество на една алгебра, и *слободна база* за база на алгебра со својство на универзално пресликување. Така, множество B велиме дека е слободна база на слупа $\mathbf{S} = (S; \cdot, 1)$ ако B е база и секое пресликување од B во L, каде $\mathbf{L} = (L; \cdot, 1)$ е слупа, може на единствен начин да се прошири до хомоморфизам од $\mathbf{S}$ во $\mathbf{L}$.

5.2 Слободни слупи - конструкција 1

Нека X е дадено множество. Дефинираме верига од множества X_i и множество F со:

(B1) $\quad X_1 = X, \quad X_{i+1} = X_i \cup \{\{u,v\} \mid u \neq v \in X_i,\ u \notin v,\ v \notin u\},$

$F_X = (\cup\ (X_i|\ i \geq 1)) \cup \{1\} \quad 1 \notin \cup\ (X_i|\ i \geq 1).$

Својство 19 Елементот $x \in X_{i+1} \setminus X_i$ ако и само ако $x = \{u,v\}$ за некои еднозначно определени u и v такви што $u \in X_i \setminus X_{i-1}$ или $v \in X_i \setminus X_{i-1}$.

□

Дефинираме операција $*$ на F_X на следниот начин. Ако $u, v \in F_X \setminus \{1\}$, тогаш

$$u * v := \begin{cases} \{u,v\} & u \neq v,\ u \notin v,\ v \notin u \\ 1 & u = v \\ t & v = \{u,t\}\ ili\ u = \{v,t\} \end{cases}$$

и $1 * u := u, \quad u * 1 := u, \quad 1 * 1 := 1.$

Теорема 34 $\mathbf{F}_X = (F_X; *, 1)$ е слободен објект во многуобразието слупи со слободна база X.

Доказ Очигледно е дека $u * v = v * u$. Го проверуваме идентитетот $u * (u * v) = v$ во следните случаи.

1) $u \neq v,\ u \notin v,\ v \notin u: \quad u * (u * v) = u * \{u,v\} = v,$

2) $v = \{u,t\}: \quad u * (u * v) = u * t = \{u,t\} = v,$

3) $u = \{v,t\}: \quad u * (u * v) = u * t = v.$

Во секој друг случај тврдењето директно е исполнето. Значи, $\mathbf{F}_X$ е слупа.

Јасно е дека X е база на $\mathbf{F}_X$ која е слободна. Имено, нека $(L;\cdot,1)$ е слупа и $\phi : X \longrightarrow L$ е пресликување. Дефинираме индуктивно верига од пресликувања $(\phi_i : X_i \longrightarrow L \mid i \geq 1)$ на следниот начин. $\phi_1 = \phi$ и ако ϕ_i е дефинирано, тогаш за $x \in X_{i+1}$,

$$\phi_{i+1}(x) := \begin{cases} \phi_i(x) & x \in X_i \\ \phi_i(u) \cdot \phi_i(v) & x = \{u, v\} \in X_{i+1} \setminus X_i \end{cases}$$

Од *Својство 2*, ϕ_i е добро дефинирано за $i \geq 1$.

Нека $\phi^* := \cup(\phi_i \mid i \geq 1) \cup \{(1,1)\}$. Ќе докажеме дека ϕ^* е хомоморфизам. Ги разгледуваме следните случаи.

1) $u \neq v,\ u \notin v,\ v \notin u$ ($u, v \in X_i$ за некој $i \geq 1$) : $\quad \phi^*(u * v) = \phi^*(\{u,v\}) = \phi_{i+1}(\{u,v\}) = \phi_i(u) \cdot \phi_i(v) = \phi^*(u) \cdot \phi^*(v)$.

2) $u = \{v, t\} \in X_i$ за некој $i > 1$: $\quad \phi^*(u * v) = \phi^*(t) = \phi_{i-1}(t) = (\phi_{i-1}(v) \cdot \phi_{i-1}(t)) \cdot \phi_{i-1}(v) = \phi_i(\{v,t\}) \cdot \phi_{i-1}(v) = \phi^*(u) \cdot \phi^*(v)$.

Останатите случаи се тривијални. □

Сметајќи дека множеството X е добро подредено (т.е. земаме дека важат аксиомите од ZFC теоријата на множества), го прошируваме истото подредување до подредување на F_X, на следниот начин.

Елементот 1 е најмал во F_X. Ако $\alpha, \beta \in F_X$ и α има помал број (парови) загради од β, тогаш $\alpha < \beta$. Ако $\{\alpha, \beta\} \neq \{\gamma, \delta\} \in F_B$, $\{\alpha, \beta\}$, $\{\gamma, \delta\}$ имаат ист број (парови) загради и $\alpha < \beta$, $\gamma < \delta$, тогаш ставаме

$\{\alpha, \beta\} < \{\gamma, \delta\}$ ако $\alpha < \gamma$ или $\alpha = \gamma, \beta < \delta$, и

$\{\gamma, \delta\} < \{\alpha, \beta\}$ ако $\gamma < \alpha$ или $\alpha = \gamma, \delta < \beta$.

Својство 20 $(F_X, \leq)$ е добро подредено множество.

Доказ (Со индукција по броеви на згаради.) Нека $A \subseteq F_X$. Ако A содржи елемент без загради, тогаш најмалиот во $(X \cup \{1\}) \cap A$ е најмал во A. Инаку, нека $k > 0$ е најмалиот број на загради на елемент од A и $A' = \{a \in A \mid$ бројот на загради во a е $k\}$. Го разгледуваме множеството $A'' = \{u \in F_X \mid \{u, v\} \in A', u < v\}$. Според индуктивна претпоставка A'' има најмал елемент α и $A''' = \{v \in F_X \mid \{\alpha, v\} \in A'\}$ има најмал β. Тогаш $\{\alpha, \beta\}$ е најмал во A' т.е. A. $\square$

Да уочиме дека ако X е рекурзивно множество, такво е и F_X.

5.3 Слободни слупи - конструкција 2

Овде даваме друг опис а слободните слупи користејќи ја апсолутно слободната алгебра, т.е. алгебрата базични терми $\mathcal{G}_{\{\cdot,1\}}(X) = \mathcal{G}_X$ со слободна база X, во сигнатура $\{\cdot, 1\}$. Секоја слободна слупа со слободна база X е всушност фактор алгебра на $\mathcal{G}_X$. Меѓутоа, во овој опис користиме подмножество на $\mathcal{G}_X$ како носител на слободна слупа.

На индуктивен начин дефинираме пресликување $d : \mathcal{G}_X \longrightarrow \mathbb{N}$, каде $\mathbb{N}$ е множеството природни броеви, со:

$d(1) := 0, \quad d(x) := 0$ за $x \in X, \quad d(t_1 \cdot t_2) = d(t_1) + d(t_2) + 1.$

Притоа за $d(t)$ велиме дека е *тежина* на термот $t \in \mathcal{G}_X$.

Со индукција по тежината дефинираме пресликување $C : \mathcal{G}_X \longrightarrow F_X$

на следниот начин:

$$C(t) := \begin{cases} 1 & t = 1 \; ili \; t = t_1 \cdot t_2, \; C(t_1) = C(t_2) \\ t & t \in X \\ C(t_1) & t = t_1 \cdot t_2, \; C(t_2) = 1 \\ C(t_2) & t = t_1 \cdot t_2, \; C(t_1) = 1 \\ C(t_3) & t = t_1 \cdot t_2, \; C(t_2) = \{C(t_1), C(t_3)\} \; ili \\ & t = t_1 \cdot t_2, \; C(t_1) = \{C(t_2), C(t_3)\} \\ \{C(t_1), C(t_2)\} & t = t_1 \cdot t_2 \; i \; niedno \; od \; prethodnite \; ne \; vai \end{cases}$$

Својство 21 Пресликувањето C е епиморфизам. □

Сега од теоремата за хомоморфизам имаме $\mathcal{G}_X/kerC \cong \mathbf{F}_X$. Понатаму определуваме каноничен претставник за секоја класа.

Претпоставувајќи дека X е добро подредено, дефинираме пресликување $T : F_X \longrightarrow \mathcal{G}_X$ користејќи го доброто подредување на F_X, со:

$T(1) := 1, \quad T(x) := x$ за $x \in X, \quad T(\{u, v\}) := T(u) \cdot T(v)$ каде $u < v$.

Својство 22 T е инјекција. □

Својство 23 $TCT = T, \; CTC = C.$

Доказ Нека $\alpha \in F_X$. Ако $\alpha = 1$ или $\alpha \in X$, тврдењето е тривијално исполнето. Нека $\alpha = \{u, v\}, \; u, v \in F_X, \; u < v$. Претпоставуваме дека тврдењето важи за секој елемент на F_X помал од α. Значи, $TCT(u) = T(u), \; TCT(v) = T(v)$. Тогаш $CT(u) = u, \; CT(v) = v$ според *Својство 22*, и бидејќи $\alpha \in F_X$ имаме $CT(u) \neq CT(v), \; CT(u) \notin CT(v), \; CT(v) \notin$

$CT(u)$. Следи, $TCT(\alpha) = TC(T(u) \cdot T(v)) = T(\{CT(u), CT(v)\}) = T(\{u, v\}) = T(\alpha)$.

Сега, $CTC = C$ е последица од *Својство 22* и $TCT = T$. $\square$

За елементот $t \in \mathcal{G}_X$ велиме дека е *редуциран* ако $TC(t) = t$. Пресликувањето $R = TC$ го нарекуваме *редукција*. Да забележиме дека $(R(t), t) \in kerC$ и во секоја класа конгруентни елементи постои точно еден редуциран елемент кој ќе биде каноничен претставник на класата.

Пресликувањето R ги има следните својства.

Својство 24 $R^n = R$, за секој $n \geq 2$, и за секои $t, s \in \mathcal{G}_X$ имаме:

(i) $R(1 \cdot t) = R(t)$;

(ii) $R(t \cdot s) = R(s \cdot t)$;

(iii) $R(t \cdot s) = t \cdot s \implies R(t) = t,\ R(s) = s$;

(iv) $R(R(t) \cdot s) = R(t \cdot s)$;

(v) $R(R(t) \cdot R(s)) = R(t \cdot s)$;

(vi) $R(t \cdot (t \cdot s)) = R(s)$.

Доказ (i) и (ii) се директни, (v) е последица од (iv).

(iii) $R(t \cdot s) = TC(t \cdot s) = t \cdot s$ повлекува дека $C(t \cdot s) = \{\alpha, \beta\}$ каде $\alpha < \beta,\ T(\alpha) = t,\ T(\beta) = s$. Сега, $TC(t) = TCT(\alpha) = T(\alpha) = t$, и на ист начин $TC(s) = s$.

(iv) Од $CR(t) = CTC(t) = C(t)$ добиваме

$$C(R(t) \cdot s) = \begin{cases} 1 & C(t) = C(s) \\ C(s) & C(t) = 1 \\ C(t) & C(s) = 1 \\ C(l) & C(t) = \{C(s), C(l)\} \; ili \; C(s) = \{C(t), C(l)\} \\ \{C(t), C(s)\} & inaku \end{cases}$$

односно $C(R(t) \cdot s) = C(t \cdot s)$.

(vi) исто така се добива разгледувајќи ги сите случаи во дефиницијата на R односно C. $\square$

Нека G_X е множеството редуцирани терми т.е. $G_X = R(\mathcal{G}_X) = T(F_X)$. Дефинираме операција $\circ$ на G_X со

$$t \circ s = R(t \cdot s), \; (\forall t, s \in G_X).$$

Теорема 35 $\mathbf{G}_X = (G_X; \circ, 1)$ е слободна слупа со слободна база X.

Доказ Ќе докажеме дека биекцијата T е изоморфизам меѓу $(F_X; *, 1)$ и $(G_X; \circ, 1)$. За секои $t, s \in \mathcal{G}_X$ имаме $t/kerC * s/kerC = (t \cdot s)/kerC = (R(t \cdot s))/kerC = R(R(t) \cdot R(s))/kerC = (R(t) \circ R(s))/kerC$. Од $\mathcal{G}_X/kerC \cong \mathbf{F}_X$ добиваме $C(t) * C(s) = C(R(t) \circ R(s))$ и ако $u = C(t)$, $v = C(s)$, тогаш $T(u * v) = T(C(t) * C(s)) = T(C(R(t) \circ R(s))) = R(R(t) \circ R(s)) = R(t) \circ R(s) = TC(t) \circ TC(s) = T(u) \circ T(v)$. $\square$

Да забележиме дека ако X е рекурзивно множество, тогаш бидејќи C и T се рекурзивно дефинирани и G_X е рекурзивно множество и претходно дефинираното добро подредување на F_X индуцира добро подредување на G_X.

5.4 Проблем на зборови за многуобразието слупи

5.4.1 Воведни поими и резултати

Во продолжение се задржуваме на решавање $WP1$ за многуобразието слупи. Истиот за многуобразието слупи се сведува на следното. Нека X е конечно множество и $(\mathcal{G}_X; \cdot, 1)$ е апсолутно слободната алгебра со база X во сигнатура $\{\cdot, 1\}$, т.е. $\mathcal{G}_X$ е множеството терми во сигнатура $\{\cdot, 1\}$. Дали постои алгоритам со кој за произволни $u, v \in \mathcal{G}_X$, и произволно $E = \{s_i \approx t_i \| \; s_i, t_i \in \mathcal{G}_X, \; 1 \leq i \leq q, q \in \mathbb{N}\}$ кје се утврди дали $u \; \alpha \; v$, каде

$\alpha \in Con\mathcal{G}_X$, α е генерирана од идентитетите за слупи и дефинирачките релации од E.

Според *Теорема 7* ако секоја делумна слупа може да се смести во слупа, тогаш проблемот на зборови е решлив за многуобразието слупи.

Некомплетна или делумна слупа со носител G е четворка $(G, \cdot, 1, D)$, каде $D \subseteq G^2, 1_G \in G, \cdot : D \mapsto G$ е пресликување и следните услови важат:

$$(1) \quad (x, x) \in D \implies x \cdot x = 1_G$$

$$(2) \quad (x, y) \in D \implies (y, x) \in D, \; x \cdot y = y \cdot x$$

$$(3) \quad (x, 1) \in D \implies x \cdot 1 = x$$

$$(4) \quad (x, y) \in D \implies (x, x \cdot y) \in D, \; x \cdot (x \cdot y) = y$$

Својство 25 Секоја некомплетна слупа може да се смести во слупа.

Доказ Нека $(G, \cdot, 1, D)$ е делумна слупа.

Нека $D_0 = D \cup \{(x,x) | x \in G\} \cup \{(1,x),(x,1) | x \in G\}$ и нека $\cdot_0 : D_0 \to G$ е дефинирано со

$$x \cdot_0 y = x \cdot y, (x,y) \in D$$

$$x \cdot_0 x = 1, x \cdot_0 1 = 1 \cdot_0 x = x, x \in G$$

Така добиваме делумна слупа $(G_0, \cdot_0, 1, D_0)$ каде $G_0 = G, D \subseteq D_0 \subseteq G_0^2$.

Ако $(G_i, \cdot_i, 1, D_i)$ е дефинирана делумна слупа, формираме нова на следниот начин. Нека $C_i = \{\{x,y\} | x,y \in G_i, (x,y) \notin D_i\}$, при претпоставка $C_i \cap G_i = \emptyset$ (инаку би земале еквивалентно множество на C_i) и ставаме $G_{i+1} = G_i \cup C_i$.

Дефинираме делумна операција $\cdot_{i+1}$ со:

$(x,y) \in D_i$	$\Longrightarrow$	$x \cdot_{i+1} y = x \cdot_i y$
$(x,y) \in G_i^2 \setminus D_i$	$\Longrightarrow$	$x \cdot_{i+1} y = \{x,y\}$
$x \in G_{i+1}$	$\Longrightarrow$	$x \cdot_{i+1} x = 1, x \cdot_{i+1} 1 = 1 \cdot_{i+1} x = x$
$x \in G_i, \{x,y\} \in C_i$	$\Longrightarrow$	$x \cdot_{i+1} \{x,y\} = y = \{x,y\} \cdot_{i+1} x$

Нека D_{i+1} е множеството од сите парови $(x,y) \in G_{i+1}$ за кои $x \cdot_{i+1} y$ е дефинирано. Значи $G_i^2 \subseteq D_{i+1}$ и $D_i \subseteq D_{i+1}$.

Јасно е дека за $(G_{i+1}, \cdot_{i+1}, 1, D_{i+1})$ важат (1) - (3) од дефиницијата на делумна слупа. Го проверуваме условот (4).

Нека $(x,y) \in D_{i+1}$. Можни се следниве случаи:

- $(x,y) \in D_i$, во кој случај важи (4)
- $x = y \in G_i$, тогаш $x \cdot_{i+1} y = 1$ па $x \cdot_{i+1} (x \cdot_{i+1} y) = x \cdot_{i+1} 1 = x = y$
- $(x,y) \in G_i^2 \setminus D_i$, тогаш $x \cdot_{i+1} y = \{x,y\}$ и $x \cdot_{i+1} (x \cdot_{i+1} y) = x \cdot_{i+1} \{x,y\} = y$

- $x \in G_i, y = \{x, z\} \in C_i$, тогаш $x \cdot_{i+1} y = x \cdot_{i+1} \{x, z\} = z$, па $x \cdot_{i+1} (x \cdot_{i+1} y) = x \cdot_{i+1} z = \{x, z\} = y$.

На овој начин добиваме вериги од множества $(G_i | i \geq 0), (D_i | i \geq 0), (\cdot_i | i \geq 0)$, со својствата:

$$G_i \subseteq G_{i+1}, D_i \subseteq G_i^2 \subseteq D_{i+1}, \cdot_i \subseteq \cdot_{i+1}.$$

Нека

$$G^* = \bigcup_{i \geq 0} G_i, D^* = \bigcup_{i \geq 0} D_i, \cdot^* = \bigcup_{i \geq 0} \cdot_i.$$

Притоа, за $x, y \in G^*$, постои $i \geq 0$ т.ш. $x, y \in G_i$, од каде $(x, y) \in D_{i+1}$, т.е. $(x, y) \in D^*$. Значи $D^* = (G^*)^2$ односно $(G^*, \cdot^*, 1)$ е слупа која е проширување на $(G, \cdot, 1, D)$. □

Од последното својство и од наведениот резултат на Evans директно следува следната теорема.

Теорема 36 Проблемот на зборови е решлив за многуобразието слупи.

□

Притоа, општиот алгоритам на Evans освен неговата добра страна, општоста, прилично е комплексен и не многу погоден за употреба. Во продолжение ќе дадеме директен алгоритам за решавање на проблемот на зборови во многуобразието слупи, кој сепак во голема мера ги задржува идеите од алгоритмот на Evans.

5.4.2 Термовски препишувачки систем за решавање на проблемот на зборови во многуобразието слупи

Нека X е конечно множество, $(\mathcal{G}_X, \cdot, 1)$ е апсолутно алободната алгебра терми во јазик $\{\cdot, 1\}$ и нека $E = \{t_i \approx s_i \mid i = 1, \ldots, q,\ t_i, s_i \in \mathcal{G}_X\}$ е конечно множество дефинирачки равенства.

Со A_X го означуваме множеството $A_X \subseteq \mathcal{G}_X \times \mathcal{G}_X$,

$A_X = \{(t, s) | t\sigma \approx s\sigma$ е примерок од аксиома, за некоја супституција $\sigma\}$.

Нека $\alpha = Cg_{\mathcal{G}_X}(E \cup A_X)$.

Може да сметаме дека $t_i = R(t_i), s_i = R(s_i), i = 1, .., q$ бидејќи ако $\alpha' = Cg_{\mathcal{G}_X}(\{(R(t_i), R(s_i)) | i = 1, \ldots, q\} \cup A_X)$, тогаш $\alpha = \alpha'$.

Имено, $(\forall x \in \mathcal{G}_X)\ x\ \alpha\ R(x),\ x\ \alpha'\ R(x)$.

Со индукција по тежината d, дефинираме пресликување $P : \mathcal{G}_X \to \mathcal{B}(\mathcal{G}_X)$ со:

$$P(t) := \begin{cases} \{t\} & t \in X \cup \{1\} \\ \{t\} \cup P(t_1) \cup P(t_2) & t = t_1 t_2 \end{cases}$$

Нека

$$X' = (X \cup (\bigcup_{i=1}^{q} P(t_i)) \cup (\bigcup_{i=1}^{q} P(s_i))) \setminus \{1\}.$$

Множеството X' е конечно, нека $n = |X'|$ и $B = \{b_1, \ldots, b_n\}$ е множество такво што $B \cap X' = \emptyset$, и нека $b : X' \to B$ е биекција која ја прошируваме до биекција од $X' \cup \{1\}$ во $B \cup \{1\}$ со $b(1) = 1$.

Јасно, $b|_{X \cup \{1\}}$ на единствен начин се проширува до мономорфизам $- : \mathcal{G}_X \to \mathcal{G}_B$ (при кој сликата на $x \in \mathcal{G}_X$ ќе ја означуваме со $\bar{x} \in \mathcal{G}_B$).

Пресликувањето$\bar{\ }$всушност врши транскрипција од азбука X во азбука $b(X)$.

За потребите на конструкцијата што следува во продолжение дефинираме два типа на пресликувања. Тоа се пресликувањата $\rightarrow_{l,k}$: $\mathcal{G}_B \rightarrow \mathcal{G}_B$, за $l, k \in \{1, .., q\}, l > k$ и пресликувањата $\rightarrow_l$: $\mathcal{G}_B \rightarrow \mathcal{G}_B, l \in \{1, .., q\}$ определени индуктивно по d со:

$$\rightarrow_{l,k}(x) := \begin{cases} x & x \neq b_l, x \in B \\ b_k & x = b_l \\ R(\rightarrow_{l,k}(x_1) \cdot \rightarrow_{l,k}(x_2)) & x = x_1 \cdot x_2 \end{cases}$$

$$\rightarrow_l(x) := \begin{cases} x & x \neq b_l, x \in B \\ 1 & x = b_l \\ R(\rightarrow_l(x_1) \cdot \rightarrow_l(x_2)) & x = x_1 \cdot x_2 \end{cases}$$

Да забележиме дека елементот b_l не се појавува во термот $\rightarrow_{l,k}(t)$ ниту во $\rightarrow_l(t)$.

Всушност овие пресликувања извршуваат замени. Пресликувањата од првиот тип се сведуваат на заменување на сите појавувања на b_l со b_k во даден терм и така добиениот терм го редуцираат, додека пресликувањата од вториот тип се сведуваат на замена на секое појавување на b_l со 1, и повторно добиениот терм се редуцира.

Продолжуваме со формиањето на две конечни множества D и V, $D \subseteq (B \cdot B) \cdot B, V \subseteq B \cup B \cdot B$ кои ќе бидат клучни во проверката на еквивалентност на произволни зборови. Слично како во алгоритмот на Evans формираме затворен систем дефинирачки релации. Притоа работиме со елементи од $\mathcal{G}_B$, а не со парови од причина што во произволна слупа S, $x = y$ ако и само ако $xy = 1$. Така всушност $D \cup V$ претставува затворен систем дефинирачки релации (всушност дефинирачки единици) со тоа што наместо пар (x, y), овде е производ xy и наместо пар $(x, 1)$, имаме само елемент x. За дефиниција на $D, V \subseteq \mathcal{G}_B$, претходно дефинираме множества D_i, V_i

Нека $V_0 = \emptyset$ и нека D_0 е множеството

$$\{b_l b_k | l > k, \{b_l, b_k\} = \{b(t_i), b(s_i)\}, (t_i, s_i) \in E\} \cup$$
$$\{b_l | \{b_l, 1\} = \{b(t_i), b(s_i)\}, (t_i, s_i) \in E\} \cup$$
$$\{(b_l b_k) b_j | t = t_1 t_2 \in X', \{b_l, b_k, b_j\} = \{b(t), b(t_1), b(t_2)\}, l > k\}.$$

Ако D_m, V_m се формирани ставаме $D_{m,0} = D_m, V_{m,0} = V_m$. Ако $D_{m,s}$ е дефинирано и ако:

(1) $D_{m,s} \cap B \neq \emptyset$ и $b_l \in D_{m,s} \cap B$ е елементот со најголем индекс, тогаш дефинираме

$$D_{m,s+1} = \to_l (D_{m,s}) \setminus \{1\}, V_{m,s+1} = V_{m,s} \cup \{b_l\}.$$

(Сега b_l не се појавува во термите од $D_{m,s+1}$.)

(2) $D_{m,s} \cap B = \emptyset, D_{m,s} \cap B \cdot B \neq \emptyset$ и $b_l b_k \in D_{m,s} \cap B \cdot B$ е елементот со лексикографски најголем индекс lk, тогаш дефинираме

$$D_{m,s+1} = \to_{l,k} (D_{m,s}) \setminus \{1\}, V_{m,s+1} = \to_{l,k} (V_{m,s}) \cup \{b_l b_k\}.$$

(Пак b_l не се појавува во термите од $D_{m,s+1}$.)

(3) $D_{m,s} \cap B = \emptyset, D_{m,s} \cap B \cdot B = \emptyset$, тогаш ставаме

$$D'_m = D_{m,s}, V_{m+1} = V_{m,s},$$

и завршуваме со формирањето на множествата $D_{m,i}$.

Да уочиме дека по конечен број чекори настапува случајот (3) бидејќи $D_{m,s} \cap B \neq \emptyset$ или $D_{m,s} \cap B \cdot B \neq \emptyset$ имплицира $|D_{m,s+1}| < |D_{m,s}|$.

Сега ставаме $D_{m+1} = D'_m \cup \{b_l b_k |\ l > k,\ (b_{i1}b_{i2})b_{i3},\ (b_{j1}b_{j2})b_{j3} \in D'_m,\ \{i_1, i_2, i_3\} = \{l, i, j\},\ \{j_1, j_2, j_3\} = \{k, i, j\}\}$.

Нека r е најмалиот позитивен цел број таков што $D_{r+1} = D'_r$. Да уочиме дека ваков r постои. Имено, ако се има предвид постапката што се спроведува, јасно е следново: $|D'_m| \leq |D_m|$ и ако $|D_{m+1}| = |D'_m| + p, p > 0$, тогаш $|D'_{m+1}| \leq |D_{m+1}| - 2p \leq |D'_m| - p < |D'_m|$.

Означуваме $D = D_{r+1},\ V = V_r$.

Корисно е да се забележат одредени работи кои следуваат од дефинициите на новоформираните множества.

Својство 26 Следните тврдења важат за D и V:

(i) $D \cap B = D \cap B \cdot B = \emptyset$

(ii) $(b_l b_k)b_j \in D \implies |\{b_l, b_k, b_j\}| = 3$

(iii) $b_l \in V,\ (b_k b_i)b_j \in D \implies l \notin \{k, i, j\}$

(iv) $b_l \in V, b_i b_k \in V \implies l \notin \{i, k\}$

(v) $b_l b_k \in V,\ (b_m b_i)b_j \in D \implies l \notin \{m, i, j\}$

(vi) $b_i b_j \in V, b_l b_k \in V \implies (i \neq l, j \neq l) \vee (j \neq l, j \neq k)$.

□

Да се задржиме малку на појаснување на тврдењето дека множествата D и V соодветствуваат на затворен систем дефинирачки равенства. За таа цел, индуктивно по d, дефинираме пресликување $e : \mathcal{G}_B \to \mathcal{G}_X$, кое ќе го нарекуваме *експанзија* на следниот начин. Нека $x \in \mathcal{G}_B$.

$$e(x) := \begin{cases} b^{-1}(x) & x \in B \cup \{1\} \\ e(x_1)e(x_2) & x = x_1x_2 \end{cases}$$

Својство 27 За секој $xy \in D \cup V$ важи $(e(x), e(y)) \in \alpha$, и за секој $x \in V \cap B$ важи $(e(x), 1) \in \alpha$.

Доказ Нека $(b_l b_k)b_j \in D_0, l > k$ тогаш $e(b_l b_k) = b^{-1}(b_l)b^{-1}(b_k), e(b_j) = b^{-1}(b_j)$ и постои $t \in X', t = t_1t_2, \{b_l, b_k, b_j\} = \{b(t), b(t_1), b(t_2)\}$, при што $t_1t_2 \ \alpha t$ (од рефлексивноста) и $tt_1\alpha t_2, tt_2\alpha t_1, t_1t\alpha t_2, t_2t\alpha t_1$, од $Ax \subseteq \alpha$ и конгруентноста на α. Потоа $b_lb_k \in D_0$ всушност значи $(e(b_l), e(b_k)) \in E$ или $(e(b_k), e(b_l)) \in E$, при што тврдењето секако важи, а идентичен на овој е случајот $b_l \in D_0$ во кој $(e(b_l), 1) \in \alpha$. Значи тврдењето важи за D_0, V_0. Нека важи за D_m, V_m и нека важи и за $D_{m,s}, V_{m,s}$.

Да го уочиме следново. Ако $(b_l, 1) \in \alpha$ тогаш од $A_X \subseteq \alpha$ и α е конгруенција имаме од $x \ \alpha \ y$ следува $\to_l (x) \ \alpha \ \to_l (y)$, и од истите причини ако $(b_l, b_k) \in \alpha$, од $x \ \alpha \ y$ следува $\to_{l,k} (x) \ \alpha \ \to_{l,k} (y)$. Значи тврдењето важи и за $D_{m,s+1}, V_{m,s+1}$.

Потоа, ако $(b_{i_1}b_{i_2})b_{i_3}, (b_{j_1}b_{j_2})b_{j_3} \in D'_m, \{i_1, i_2, i_3\} = \{i, j, k\}, \{j_1, j_2, j_3\} = \{i, j, l\}$, тогаш по индуктивната претпоставка $(b_ib_j, b_k), (b_ib_j, b_l) \in \alpha$, од каде се добива $b_k \ \alpha \ b_l(b_lb_k) \ \alpha \ b_l((b_ib_j)(b_ib_j)) \ \alpha \ b_l$. Значи тврдењето важи и за D_{m+1}, V_{m+1}. $\square$

Дефинираме препишувачки систем на множеството терми со константи од B во сигнатура $\{\cdot, 1\}$ со следните четири шеми правила.

$(WPS1)$	t	$\to$	$R(t)$	$t \in \mathcal{G}_B, t \neq R(t)$
$(WPS2)$	b_i	$\to$	1	$b_i \in V \cap B$
$(WPS3)$	b_i	$\to$	b_j	$b_i b_j \in V \cap B \cdot B$
$(WPS4)$	$b_i \cdot b_j$	$\to$	b_k	$(b_i \cdot b_j) \cdot b_k \in D \cap (B \cdot B) \cdot B$

Својство 28 Релацијата $\to$ е терминирачка, односно не постои бесконечна низа $x_0 \to x_1 \to \ldots$.

Доказ Дефинираме интерпретација на термите од $\mathcal{G}_B$ во множеството $\mathbb{N}^3$, со, $|t| = (n_1, n_2, n_3)$, каде $n_1 = d(t)$, n_2 е збир на индексите на буквите кои се појавуваат во t, n_3 е бројот на редуцирани подтерми на t. Сега лексикографското подредување на $\mathbb{N}^3$ индуцирано од стандардното подредување на $\mathbb{N}$ е препишувачко подредување во кое е содржана релацијата $\to$. $\square$

Својство 29 Релацијата $\to$ е локално конфлуентна, т.е. $(\forall x, y, z \in \mathcal{G}_B)(\exists w \in \mathcal{G}_B)(x \to y \wedge x \to z \implies y \to^* w \wedge z \to^* w)$.

Доказ Нека $x, y, z \in \mathcal{G}_B, x \to y, x \to z$. Ако $y = z$ јасно е дека тврдењето важи. Исто така, важи во сите случаи во кои $x = s[x_1x_2]_p, y = s[x_1'x_2]_p, z = s[x_1x_2']_p$. Секако, тврдењето е исполнето за $x \in B$. Со индукција по тежина ќе докажеме дека важи и во сите останати случаи кои се сведуваат на $x = x_1x_2, y = R(x) = R(R(x_1)R(x_2)), z$ е добиено со примена на $(WPS2)$, $(WPS3)$ или $(WPS4)$ од дефиницијата на $\rightarrow$. Имаме неколку можности

$$y = R(x) := \begin{cases} 1 & R(x_1) = R(x_2) \\ t & R(x_1) = tR(x_2)\ ili \\ & R(x_1) = R(x_2)t\ ili \\ & R(x_2) = tR(x_1)\ ili \\ & R(x_2) = R(x_1)t \\ R(x_1)R(x_2) & R(x_1) < R(x_2)\ i\ prethodnite\ ne\ vaat \\ R(x_1)R(x_2) & inaku \end{cases}$$

и $z = z_1x_2,\ x_1 \rightarrow z_1$ или $z = x_1z_2,\ x_2 \rightarrow z_2$.

Од причини на симетрија доволно е да се разгледаат следните неколку подслучаи.

1. $y = 1, z = z_1x_2$. Имаме $d(x_1) < d(x), x_1 \rightarrow z_1, x_1 \rightarrow R(x_1)$, па од индуктивната претпоставка постои $w_1 \in \mathcal{G}_B, z_1 \rightarrow^* w_1, R(x_1) \rightarrow^* w_1$. Тогаш $z = z_1x_2 \rightarrow z_1R(x_2) \rightarrow^* w_1R(x_2) \rightarrow^* w_1w_1 \rightarrow 1$.

2. $y = t, R(x_1) = tR(x_2)$.

   (а) $z = x_1z_2$.

   Сега, $x_2 \rightarrow z_2, x_2 \rightarrow R(x_2), d(x_2) < d(x)$, па постои $w_2 \in \mathcal{G}_B, z_2 \rightarrow^* w_2, R(x_2) \rightarrow^* w_2$. Тогаш $z \rightarrow (tR(x_2))z_2 \rightarrow^* (tR(x_2))w_2 \rightarrow^* (tw_2)w_2 \rightarrow t$.

   (б) $z = z_1x_2$.

   Притоа $x_1 \rightarrow z_1, x_1 \rightarrow R(x_1) = tR(x_2), d(x_1) < d(x)$, па постои

$w_1 \in \mathcal{G}_B, z_1 \to^* w_1, R(x_1) \to^* w_1$. Овде повторно разгледуваме две можности

и. $d(R(x_1)R(x_2)) < d(x)$:

Тогаш од $R(x_1)R(x_2) = (tR(x_1))R(x_2) \to w_1R(x_2), R(x_1)R(x_2) = (tR(x_1))R(x_2) \to t$ следува постои $w \in \mathcal{G}_B, w_1R(x_2) \to^* w, t \to^* w$. Затоа, $z = z_1x_2 \to^* w_1x_2 \to w_1R(x_2) \to^* w$ и $y = t \to^* w$.

ии. $d(R(x_1)R(x_2)) = d(x)$:

Ова настапува кога $x_1 = R(x_1), x_2 = R(x_2)$ или редукцијата се сведува на разрешување комутативност, но тоа не влијае на препишувањата. Без губење на општост може да сметаме дека $x_1 = R(x_1), x_2 = R(x_2), x_1 = tx_2$, и притоа $x_1 \to z_1$, т.е. $tx_2 \to z_1$. Сега, ако $z_1 = tx_2'$ $(x_2 \to x_2')$, тогаш $z = z_1x_2 = (tx_2')x_2 \to (tx_2')x_2' \to t = y$. Ако пак $z_1 = t'x_2(t \to t')$, тогаш $z = z_1x_2 = (t'x_2)x_2 \to t'$ и $y = t \to t'$.

3. $y = R(x_1)R(x_2), z = z_1x_2$.

Повторно имаме $d(x_1) < d(x), x_1 \to z_1, x_1 \to R(x_1)$, па постои $w_1 \in \mathcal{G}_B, z_1 \to^* w_1, R(x_1) \to^* w_1$ и важи $y \to^* w_1R(x_2), z \to^* w_1x_2 \to w_1R(x_2)$.

$\square$

Да напоменеме дека всушност изведувањето на доказот на претходното својство се сведува на проверка на условот од *Теорема 31* но вака наведениот доказ со разгледани подслучаи претставува скица на доказот на истата теорема, во овој конкретен случај.

Сега од *Теорема 29* и *Последица 5* ги добиваме следните две последици.

Последица 6 Релацијата $\rightarrow$ е конфлуентна или Church-Rosser, т.е. $(\forall x, y, z \in \mathcal{G}_B)(\exists w \in \mathcal{G}_B)(x \rightarrow^* y \wedge x \rightarrow^* z \implies y \rightarrow^* w \wedge z \rightarrow^* w)$. $\square$

Последица 7 $(\forall x \in \mathcal{G}_B)(\exists! x^* \in \mathcal{G})(\forall y \in \mathcal{G}_B)(x \rightarrow^* x^* \wedge x^* \rightarrow^* y \implies x^* = y)$. $\square$

Односно препишувачкиот систем ја има особината на единствена нормална форма на секој терм. Во понатамошниот текст секаде нормалната форма на $w \in \mathcal{G}_B$ ќе ја означуваме со w^*.

Својство 30 (i) $(\forall x \in Term_B)\ x^* = R(x)^*$;

(ii) $(\forall x, y, z \in Term_B)(x^* = y^* \implies (zx)^* = (zy)^* \wedge (xz)^* = (yz)^*)$;

(iii) $(\forall x, y \in Term_B)\ (xy)^* = 1 \Leftrightarrow x^* = y^*$.

Доказ Тврдењата (i) и (ii) се јасни.

За (iii), нека $x^* = y^*$. Тогаш од (ii), $1 = (xx)^* = (xy)^*$. Обратно, нека $(xy)^* = 1$. Тогаш $y^* = (x(xy))^* = (x1)^* = x^*$ $\square$

Дефинираме релација β на $\mathcal{G}_{b(X)}$ со

$$x\beta y \Leftrightarrow x^* = y^*.$$

Секако, имајќи ги предвид претходните својства всушност $x\beta y \Leftrightarrow (R(xy))^* = 1 \Leftrightarrow (xy)^* = 1 \Leftrightarrow x^* = y^*$.

Од последното својство и дефиницијата на релацијата β веднаш се добива

Последица 8 $(\forall x \in \mathcal{G}_{b(X)})\ x\ \beta\ R(x)$. $\square$

Последица 9 $\beta \in Con\mathcal{G}_{b(X)}$. $\square$

Теорема 37 $(\forall x, y \in \mathcal{G}_X) x\ \alpha\ y \Leftrightarrow \bar{x}\ \beta\ \bar{y}$.

Доказ

Нека $(t_i, s_i) \in E$. Тогаш имаме $\bar{t_i} \to^* b(t_i)^*, \bar{s_i} \to^* b(s_i)^*$, и $b(t_i)^* = b(s_i)^* \in B \cup \{1\}$, бидејќи или $b(t_i)b(s_i) \in V$ или $b(s_i)b(t_i) \in V$ или постои $b_j \in B, b(t_i)b_j \in V, b(s_i)b_j \in V$ или $b(s_i), b(t_i) \in V$. Следи, $(\bar{t_i}, \bar{s_i}) \in \beta$.

Потоа, ако $(x, y) \in A_X$, тогаш $\bar{x}\ \beta\ \bar{R(x)} = \bar{R(y)}\ \beta\ \bar{y}$.

Понатаму, од тоа што и α и β се конгруенции и од претходното имаме $x\ \alpha\ y \implies \bar{x}\ \beta\ \bar{y}$.

Обратната инклузија е последица од *Својство 27*. Имено, од споменатото својство и од дефиницијата на релацијата $\to$ и пресликувањето e имаме $x \to y \implies e(x)\ \alpha\ e(y)$, за сите $x, y \in \mathcal{G}_B$. Значи, од транзитивноста на α, $x \to^* y \implies e(x)\ \alpha\ e(y)$, за сите $x, y \in \mathcal{G}_B$ и конечно $\bar{x}\ \beta\ \bar{y} \implies \bar{x} = e(\bar{x})\ \alpha\ e(x^*) = e(y^*)\ \alpha\ e(\bar{y}) = \bar{y}$. $\square$

Пример 14 Нека S е слупа зададена со множество генератори $X = \{a, b, c, d, e\}$ и множество дефинирачки релации $E = \{((ab)c, ad), ((ab)d, c)\}$. Тогаш имаме

$$X' = \{a, b, c, d, e, ab, (ab)c, ad, (ab)d\},$$

и нека $B = \{b_1, \ldots b_9\}$, при што $b_1 = b(a), b_2 = b(b), b_3 = b(c), b_4 = b(d), b_5 = b(e), b_6 = b(ab), b_7 = b((ab)c), b_8 = b(ad), b_9 = b((ab)d)$. Тогаш

$$D_0 = \{b_8b_7,\ b_9b_3,\ (b_2b_1)b_6,\ (b_6b_2)b_1,\ (b_6b_1)b_2,\ (b_6b_3)b_7,\ (b_7b_6)b_3,\ (b_7b_3)b_6,$$
$$(b_4b_1)b_8,\ (b_8b_1)b_4,\ (b_8b_4)b_1,\ (b_6b_4)b_9,\ (b_9b_6)b_4,\ (b_9b_4)b_6\},$$

$$V_1 = \{b_8b_7,\ b_9b_3\}$$

$$D_1 = \{b_7b_4,\ (b_2b_1)b_6,\ (b_6b_2)b_1,\ (b_6b_1)b_2,\ (b_6b_3)b_7,\ (b_7b_6)b_3,\ (b_7b_3)b_6,$$
$$(b_4b_1)b_7,\ (b_7b_1)b_4,\ (b_7b_4)b_1,\ (b_6b_3)b_4,\ (b_6b_4)b_3,\ (b_4b_3)b_6\}$$

$$V_2 = \{b_8b_4,\ b_7b_4,\ b_9b_3\}$$

$$D_2 = \{b_1,\ (b_2b_1)b_6,\ (b_6b_2)b_1,\ (b_6b_1)b_2,\ (b_6b_3)b_4,\ (b_6b_4)b_3,\ (b_4b_3)b_6\}$$

$$V_3 = \{b_1,\ b_6b_2,\ b_8b_4,\ b_7b_4,\ b_9b_3\}$$

$D_3 = \{(b_3b_2)b_4,\ (b_4b_2)b_3,\ (b_4b_3)b_2\}$ и конечно

$$V = \{b_1,\ b_6b_2,\ b_8b_4,\ b_7b_4,\ b_9b_3\}$$

$$D = \{(b_3b_2)b_4,\ (b_4b_2)b_3,\ (b_4b_3)b_2\}$$

Сега, директно со помош на препишувањата се утврдува на пример за $u,\ v,\ w \in \mathcal{G}_X,\ u = ab,\ v = c(ad),\ w = ad$ дека $u \,\alpha\, v,\ u \not\alpha\, w$.

Имаме, $\bar{u} = b_1b_2,\ \bar{v} = b_3(b_1b_4),\ \bar{w} = b_1b_4$ и $\bar{u} \to b_2$, т.е. $\bar{u}^* = b_2$, потоа $\bar{v} \to b_3 \cdot (1 \cdot b_4) \to b_3b_4 \to b_4b_3 \to b_2$, значи $\bar{u}^* = \bar{v}^*$, додека $\bar{w}^* = b_4$.

Би можеле приказната на формирањето на множествата D и V да ја раскажеме и поинаку, можеби интуитивно појасно, со постапно формирање на еден конечен делумен групоид со носител $B \cup \{1\}$ и една конечна листа од парови од облик (b_i, b_k) и $(b_i, 1)$. Имено, во наполно празна шема на делумен групоид со носител $B \cup \{1\}$ ако $t = t_1t_2 \in X', b(t) = b_l, b(t_1) = b_k, b(t_2) = b_i$, пополнуваме $b_lb_k = b_i,\ b_lb_i = b_k,\ b_kb_i = b_l,\ b_ib_k = b_l,\ b_ib_l = b_k,\ b_kb_l = b_i$, и секако $1 \cdot b_i = b_i,\ b_i \cdot 1 = b_i$, потоа за секоја дефиниречка релација од E, додаваме во листата пар $(b(t_i), b(s_i))$ или $(b(s_i), b(t_i))$ така што првата компонента од додадениот пар има поголем индекс од втората.

Понатаму постапката е следната,земаме елемент од листата (повторно со подредување на елементите таму) и ако е тоа елемент $(b_i, 1)$ ја споредуваме редицата на b_i со редицата на 1, секако и колоните (од комутативноста шемата е симетрична во однос на главната дијагонала). Притоа ако сме имале $b_i b_k = b_s$, тогаш на листата додаваме (b_k, b_s), и ја отстрануваме комплетно редицата (колоната) на b_i, додека во листата и во шемата вршиме сегде замена на b_i со 1. Ако пак од листата сме земале елемент (b_i, b_j), вршиме споредба (преклопување) на редицата на b_i и на b_j, преклопување бидејќи ако негде немало дефинирана вредност $b_j b_s$ а имало $b_i b_s$, тогаш ова станува вредност на $b_j b_s$ (и на $b_s b_j$, и уште 4 вредности се пополнуваат како и претходно, ако не биле пополнети), ако пак имале различни вредности $b_i b_s = b_m, b_j b_s = b_n,\ n > m$, на листата воведуваме пар (b_n, b_m) и се врши во целата шема и во листата замена на b_i со b_j. Последниот добиен делумен групоид одговара на множеството D, а последната останата листа на множеството V.

Литература

[1] R. U. Bruck, *A survey of Binary Systems*, Berlin - Götingen - Heidelberg, 1958

[2] H. Comon, J. P. Jouannaud, *Term Rewriting*, French Spring school of theoretical computer science, 1993, Springer-Verlag, Berlin Heidelberg NewYork, 1995

[3] N. Dershowitz, J.P. Jouannaud, *Rewrite Systems*, Handbook of Theoretical Computer Science, Volume B, Formal Models and Semantics, The MIT Press, 1990

[4] N. Dershowitz, *33 Examples of Termination*, French Spring school of theoretical computer science, 1993, Springer-Verlag, Berlin Heidelberg NewYork, 1995

[5] T. Evans, *The Word Problem for Abstract Algebras*, Journal of London Math. Soc., 26, 1951

[6] T. Evans, *Embeddability and the Word Problem*, Journal of London Math. Soc., 1952

[7] T. Evans, *Some connections between residual finiteness, finite embeddability and the word problem*, Journal of London Math. Soc.(2), 1, 1969

[8] T. Evans, *Some solvable word problems*, Word problems II, North-Holland Publishing Company, 1980

[9] J. W. Klop, *Term Rewriting Systems*, Handbook of Logic in Computer Science, Volume 2, Carendon Press - Oxford, 1992

[10] H. R. Lewis, C. H. Papadimitriou, *Elements of the Theory of Computation*, Prentice Hall, 1981

[11] G. Lallement, *Semigroups and combinatorial applications*, Wiley - Interscience Publication, 1979

[12] G. Lallement, *The Word Problem for Thue Rewriting Systems*, French Spring school of theoretical computer science, 1993, Springer-Verlag, Berlin Heidelberg NewYork, 1995

[13] R. Madarasz, S. Crvenkovic, *Relacione algebre*, Beograd, 1992

[14] S. Markovski, A. Sokolova: *Free Steiner Loops*, подготвен за печатење

[15] S. Markovski, A. Sokolova: *Term rewriting system for solving the word problem for sloops*, подготвен за печатење

[16] Y. Matiacevitch, *Word Problem for Thue Systems with a Few Relations*, French Spring school of theoretical computer science, 1993, Springer-Verlag, Berlin Heidelberg NewYork, 1995

[17] R. N. McKenzie, W. F. Taylor, G. F. McNulty: *Algebras, Lattices, Varieties*, Wadsworth & Brooks, Monterey, California, 1987

[18] D. M. Smirnov: *Mnogoobraziya Algebr*, Nauka, Novosibirsk, 1992

[19] W. Wechler, *Universal Algebra for Computer Scientists*, Springer-Verlag, Berlin Heidelberg NewYork, 1992