УНИВЕРЗИТЕТ У БЕОГРАДУ

МАТЕМАТИЧКИ ФАКУЛТЕТ

Мастер рад

Тема: **Тарскијева средњошколска алгебра**

Професор **Студент**

Небојша Икодиновић **Стеван Брдар 1070/2018**

Београд, 2020.

Садржај

Увод

Тарски је 60-их година прошлог века издвојио само 11 основних идентитета о природним бројевима N који се уче у средњој школи:

$$HSI\begin{cases}\overline{HSI}\begin{cases}(1)x+y\approx y+x\\(2)x+(y+z)\approx(x+y)+z\\(3)x\cdot 1\approx x\\(4)x\cdot y\approx y\cdot x\\(5)x\cdot(y\cdot z)\approx(x\cdot y)\cdot z\\(6)x\cdot(y+z)\approx x\cdot y+x\cdot z\end{cases}\\(7)1^x\approx 1\\(8)x^1\approx x\\(9)x^{y+z}\approx x^y\cdot x^z\\(10)(x\cdot y)^z\approx x^z\cdot y^z\\(11)(x^y)^z\approx x^{y\cdot z}.\end{cases}$$

Све ове идентитете заједно означавамо *HSI* (High School Identities), а идентитете који се односе само на операције $+,\cdot,1$ означавамо $\overline{HSI}$. Идентитети *HSI* истакнути су и у чувеном делу Дедекинда из 1888. године „Was sind und was sollen die Zahlen“. Дедекинд је доказао да ови идентитети следе из познатих Пеанових аксиома. За многе математичаре, изучавање основних идентитета за природне бројеве завршава се у средњој школи. Ипак, постоји доста проблема за истраживање, који излазе из оквира средњошколске наставе математике. На пример,

1. постоји пуно такозваних малих модела за идентитете *HSI*, и
2. постоје идентитети који важе у $\mathbf{N}$, а који се не могу извести из *HSI*.

Покушај класификације коначних модела доводи до занимљивих проблема у теорији бројева. Поводом 2, сам Тарски се питао да ли је *HSI* основа за све идентитете из $\mathbf{N}$. На ово питање, познато као Тарскијев средњошколски проблем, негативно је одговорио Вилки 1980. године. Вилкијев резултат доказујемо користећи један мали модел *HSI*, методом коју је увео Гуревич 1985. године.

1. Основе

Дефиниција 1.1. Нека је λ језик $\{+, \cdot, \uparrow, 1\}$ који се састоји од три симбола за бинарне операције и једног симбола константе. λ -алгебра која задовољава (1)-(11) назива се *HSI-алгебра*.

Дефиниција 1.2. **N** је *HSI*-алгебра $\langle N, +, \cdot, \uparrow, 1\rangle$, где је N скуп позитивних целих бројева, и $+, \cdot, \uparrow$ су редом операције сабирања, множења и степеновања природних бројева.

Дефиниција 1.3. Нека је $\bar{\lambda}$ језик $\{+, \cdot, 1\}$ који се састоји од два бинарна операцијска симбола и једног симбола константе. $\bar{\lambda}$-алгебра **A** која задовољава $\overline{HSI}$ назива се $\overline{HSI}$*-алгебра*.

Дефиниција 1.4. Ако је $\mathbf{A} = \langle A, +, \cdot, \uparrow, 1\rangle$ λ -алгебра, онда се њена *редукција* на језик $\bar{\lambda}$ означава $\bar{\mathbf{A}}$, тј., $\bar{\mathbf{A}} = \langle A, +, \cdot, 1\rangle$, где су $+, \cdot$ и 1 из **A.**

Очигледно је да ако је **A** *HSI*-алгебра онда је $\bar{\mathbf{A}}$ $\overline{HSI}$-алгебра. Специјално, $\bar{\mathbf{N}}$ је позната $\overline{HSI}$-алгебра $\langle N, +, \cdot, 1\rangle$. Наравно, постоји могућност да се нека $\overline{HSI}$-алгебра **B** не може проширити до *HSI*-алгебре, тј. да не постоји *HSI*-алгебра **A** тако да важи $\bar{\mathbf{N}} = \mathbf{B}$. Заиста, ускоро ћемо видети мноштво примера који потврђују то.

Дефиниција 1.5. Нека је **A** $\overline{HSI}$- или *HSI*-алгебра. Елементи универзума алгебре генерисане константом 1 називају се *цели бројеви* из **A**.

Лема 1.6. *Ако је* **A** $\overline{HSI}$*- или HSI-алгебра онда је скуп целих бројева из* **A**

$$\{\underbrace{1 + 1 + \cdots + 1}_{n} : n \in N\},$$

скуп коначних сума јединица.

Доказ. Јасно, свака коначна сума јединица мора бити цео број из **A.** Користећи $\overline{HSI}$, респективно *HSI*, видимо да је ова колекција елемената затворена за операције из **A** укључујући и елемент 1. □

У $\overline{HSI}$ или *HSI*-алгебри **A** једноставно пишемо n уместо $\underbrace{1 + 1 + \cdots + n}_{n}$.

Није тешко уочити да се као модели теорије $\overline{HSI}$, осим алгебре $\bar{\mathbf{N}}$ над скупом природним бројева, појављују и друге познате алгебре бројева, над скупом целих, рационалних, реалних и комплексних бројева; као и одговарајуће подалгебре над позитивним бројевима. Међутим, многе од ових алгебри не могу бити раширене до модела за *HSI*. На пример, позитивни рационални бројеви нису затворени за уобичајено степеновање реалних бројева. Важно је приметити да $\overline{HSI}$-алгебра над позитивним реалним бројевима допушта природно проширење до *HSI*-алгебре $\mathbf{R}^+ = \langle R^+, +, \cdot, \exp, 1\rangle$.

Један природан извор примера пронашао је Биркхоф (1942). Он је показао да идентитети *HSI* важе за алгебру посета, са следећим операцијама: $+$ је дисјунктна унија два посета, $\times$ је Декартов производ посета, $\uparrow$ је скуп функција које чувају уређења. Самим тим, алгебра кардиналних бројева такође задовољава *HSI* идентитете. У наредној

леми издвојене су особине које се односе на степеновање кардиналних бројева. Ако су A и B скупови, онда је B^A скуп свих функција из A у B. При овој интерпретацији, нпр. идентитети (10) и (11) постају $|(A \times B)^C| = |A^C \times B^C|$ и $|(A^B)^C| = |A^{B\times C}|$.

Веома важне методе за проучавање идентитета алгебре **N** потичу из Хардијеве монографије

(1921) о парцијалним функцијама дефинисаним термима парцијалне алгебре над реалним бројевима коју означавамо $\mathbf{R}_H$:

$$\mathbf{R}_H = \langle R, +, -, \cdot, /, \left(\sqrt[n]{\ }\right)_{n\in N}, \exp, \log, (r)_{r\in R}\rangle .$$

Нека је $\mathcal{H}$ скуп свих парцијалних функција дефинисаних у $\mathbf{R}_H$ термима $t(x)$, и нека је $\mathcal{H}_\infty$ скуп функција $f \in \mathcal{H}$ које су дефинисане за довољно велике реалне бројеве (тј. почев од неког реалног броја). Харди је на скупу $\mathcal{H}_\infty$, тзв. логаритамско-експоненцијалних функција дефинисао уређење $\prec$,

$f \prec g$ ако су вредности функције f мање од вредности функције g, за довољно велике реалне бројеве,

и следећу релацију

$f \approx g$ ако су вредности функција f и g једнаке, за довољно велике реалне бројеве.

Доказао је и следећи фундаментални резултат.

Теорема 1.7. За све $f, g \in \mathcal{H}$ важи $f \prec g$, $g \prec f$ или $f \approx g$.

Посебно је важна следећа последица.

Последица 1.8. Ако су $f, g \in \mathcal{H}$ две функције дефинисане на $(a, +\infty)$, али нису једнаке на овом интервалу, онда је или $f \prec g$ или $g \prec f$.

Хардијево истраживање се на природан начин преводи на алгебру $\mathbf{R}^+$: за сваки λ-терм $t(x)$ нека је $t^*(x)$ терм добијен тако што се подтерми од t облика u^v замењују са $\exp(v \log u)$. Тада за сваки λ-терм $t(x)$, превод $t^*(x)$ дефинише једну парцијалну функцију која је дефинисана за све позитивне реалне бројеве, и за те вредности функција је једнака функцији над R^+ коју дефинише терм t. Овако дефинисано превођење израза нам омогућава да претходну последицу пренесемо на алгебре $\mathbf{R}^+$ и **N**.

Теорема 1.9. Ако терми s и t одређују две различите функције над $\mathbf{R}^+$, односно **N**, онда је или $s \prec t$ или $t \prec s$.

Теорема 1.10. Алгебре $\mathbf{R}^+$ и **N** задовољавају исте λ-идентитете.

Доказ. Како је **N** подалгебра од $\mathbf{R}^+$, треба доказати да сваки идентитет тачан у **N** такође важи и у $\mathbf{R}^+$.

Најпре разматрамо идентитет са једном променљивом, $s(x) = t(x)$. Ако овај идентитет није тачан у $\mathbf{R}^+$, онда су вредности $s(x)$ и $t(x)$ различите за довољно велике реалне бројеве x, а самим тим и за довољно велике природне бројеве. Дакле, $s(x) = t(x)$ не важи у **N**. Индукцијом по броју променљивих се доказује да сваки идентитет тачан у **N** такође важи и у $\mathbf{R}^+$. □

Хардијева истраживања асимптотског понашања $\mathcal{H}_\infty$-функција била су полазна тачка за истраживања одлучивости једнакосне теорије структуре **N**. Ричардсон је 1969. године, ослањајући се на Хардијев рад, показао да је једнакосна теорија од **N** над једном променљивом одлучива, тј. да постоји процедура да се одлучи да ли је једнакост $s(x) = t(x)$ тачна у **N**. Ричардсонов метод се састојао у испитивању важења једнакости у једној модификацији структуре $\mathbf{R}_H$. Наиме, да би се уопште дискутовало о одлучивости, неопходно је да језик буде пребројив, што значи да треба избећи непребројиво много реалних константи које се појављују у Хардијевом приступу. Ако од константи $(r)_{r\in R}$ у $\mathbf{R}_H$ оставимо само 0 и 1, језик постаје пребројив, а свака парцијална функција из $\mathcal{H}$ је дефинисана неким термом овог редукованог језика, али са реалним параметарима, тј. изразом $t(x,\vec{r})$, где је $t(x,\vec{y})$ терм у коме се евентуално појављују само константе 0 и 1, и $\vec{r}$ је неки низ реалних бројева. Ричардсон је из Хардијевог језика избацио и кореновање $\left(\sqrt[n]{\ }\right)_{n\in N}$, а функцију log заменио са $\log|\quad|$:

$$\overline{\mathbf{R}_H} = \langle R, +, -, \cdot, \exp, \log|\quad|, 0, 1\rangle.$$

Нека је $\overline{\mathcal{H}}$ скуп парцијалних функција дефинисаних термима $t(x,\vec{r})$ над језиком алгебре $\overline{\mathbf{R}_H}$ са реалним параметрима $\vec{r}$, а $\overline{\mathcal{H}}_\infty$ скуп функција $f \in \overline{\mathcal{H}}$ које су дефинисане за довољно велике реалне бројеве. Очигледно је $\overline{\mathcal{H}} \subseteq \mathcal{H}$, па Хардијева теорема важи и за $\overline{\mathcal{H}}_\infty$. Приметимо и да су све терм-функције над $\mathbf{R}^+$ рестрикције на $(0,+\infty)$ функција из $\overline{\mathcal{H}}_\infty$.

Приметимо да сваки терм $t(x,\vec{y})$ над језиком алгебре $\overline{\mathbf{R}_H}$ и све $\vec{b} \in R$ такве да је $t(x,\vec{b})$ дефинисано над неким интервалом I, $t(x,\vec{b})$ дефинише функцију из $C^\infty(I)$. Основна идеја Ричардсоновог приступа је да сваком терму t над језиком алгебре $\overline{\mathbf{R}_H}$ придружи низ термова истог језика $t_0, t_1, \dots, t_k$, који даје важне информације о броју различитих нула функције $t(x,\vec{b})$ у на интервалу на коме је дефинисан.

Кажемо да терм $t(x,\vec{y})$ има особину $\mathcal{R}(x,k)$ ако постоји низ термова над језиком алгебре $\overline{\mathbf{R}_H}$:

$$t_0(x,\vec{y}), t_1(x,\vec{y}), \dots, t_k(x,\vec{y}),$$

такав да

- $t_0(x,\vec{y}) = t(x,\vec{y})$ и $\frac{\partial}{\partial x} t_k(x,\vec{y}) = 0$,
- за сваки интервал $I \subseteq R$ и све $\vec{b} \in R$, ако је $t(x,\vec{b})$ дефинисано на I, онда за свако $a \in R$ и свеи $< k$, $t_{i+1}(a,\vec{b})$ је дефинисано и

$$t_{i+1}(a,\vec{b}) = 0 \iff \frac{\partial}{\partial x} t_k(a,\vec{b}) = 0.$$

Сваки полином $t(x)$ је најједноставнији пример терма који има особину $\mathcal{R}(x,k)$.

Пример. Ако је $p(x)$ полином степена k и $q(x)$ полином степена ℓ, нека је $t(x) = \exp\big(p(x)/q(x)\big) - 1$ и $r(x) = p(x)q'(x) - q(x)p'(x)$. Низ

$$\exp\big(p(x)/q(x)\big) - 1, r(x), r'(x), \dots, r^{(k+\ell-1)}(x)$$

показује да терм $t(x)$ има особину $\mathcal{R}(x, k+\ell-1)$.

Ако терм $t(x,\vec{y})$ има особину $\mathcal{R}(x,k)$, једноставно се показује да за сваки интервал $I \subseteq R$ и све $\vec{b} \in R$, ако је $t(x,\vec{b})$ дефинисано на I, тада је или $t(x,\vec{b}) = 0$ на I, или $t(x,\vec{b})$ има највише k различитих корена у I. Ричардсонов основни резултат јесте да за сваки терм $t(\vec{x})$ и сваку променљиву x_i постоји ефективна процедура да се пронађе ненегативан број k такав да $t(\vec{x})$ има особину $\mathcal{R}(x_i,k)$. Занимљиво је да се ефективно

може одредити горња граница броја корена од $t(x, \vec{b})$ на било ком интервалу I, на коме је терм дефинисан и није идентички једнак нули, али није познато да ли се ефективно може одредити горње ограничење самих корена у интервалу I. Из Ричардсоновог резултата следи следећа теорема.

Теорема 1.11. Једнакосна теорија од **N** над једном променљивом је одлучива.

Касније, 1981. године, Мекинтајер је додатно усавршио Хардијеве технике и добио следећи општији резултат.

Теорема 1.12. Једнакосна теорија од **N** је одлучива.

Скорашњи модел-теоретски резултати који се односе на структуру $\mathbf{R}_{\exp} = \langle R, +, -, \cdot, \exp, 0, 1, < \rangle$ значајно доприносе разумевању алгебре **N**, али их у овом раду нећемо наводити.

2. Напомене о једнакосним теоријама за $\overline{\mathbf{N}}$ и $\mathbf{N}$

Рад са једнакосном теоријом за $\overline{\mathbf{N}}$ значајно поједностављује чињеница да сваки $\bar{\lambda}$-терм t има једноставну *нормалну форму* $v(t)$ *– полином*. У ствари, једнакост $\bar{\lambda}$-терма и одговарајуће нормалне форме јесте последица $\overline{HSI}$.

Теорема 2.1.

(а) *једнакосна теорија* $\mathbf{Id}(\overline{\mathbf{N}})$ *за природне бројеве са сабирањем и множењем је одлучива.*

(б) *једнакосна теорија за* $\overline{\mathbf{N}}$ *је аксиоматизована идентитетима* $\overline{HSI}$.

Доказ. (а) Једнакост $t_1 \approx t_2$ важи у $\mathbf{N}$ ако и само ако важи $v(t_1) = v(t_2)$. Будући да можемо ефективно да одредимо нормалну форму сваког $\bar{\lambda}$-терма, јасно је да имамо и процедуру одлучивања.

(б) Нека је $\sum$ скуп $\bar{\lambda}$-једнакости које могу да се изведу из $\overline{HSI}$. Како $\overline{HSI}$ важе у $\overline{\mathbf{N}}$ следи да $\sum \subseteq \mathbf{Id}(\overline{\mathbf{N}})$. Ако $t_1 \approx t_2$ важи у $\overline{\mathbf{N}}$, користећи $\overline{HSI}$ можемо наћи нормалне форме за t_1, t_2, и самим тим добити доказ за $t_1 \approx t_2$ из $\overline{HSI}$. □

Не постоје лепе нормалне форме за $\bar{\lambda}$-терме по модулу $\mathbf{Id}(\overline{\mathbf{N}})$ па се уводе разне софистициране технике. Методе из анализе (које потичу од Г.Х.Хардија) користио је Ричардсон [12] да покаже одлучивост једнакосне теорије са једном променљивом за $\mathbf{N}$.

Вилкијев доказ [16] да HSI не аксиоматизује $\mathbf{Id}(\mathbf{N})$ заснован је на неким суптилним методама теорије доказа. Вилки је пронашао идентитет $W(x, y)$ који важи у $\mathbf{N}$ и из $HSI \vdash W(x, y)$ следи (1)-(10) $\vdash W(x, y)$. Елиминација потребе за Аксиомом (11) је најтежи део његовог доказа. Након овога, он дефинише једно необично степеновање над $\overline{\mathbf{N}}[x]$, полиномима са природним коефицијентима, да би добио модел за (1)-(10) који не задовољава $W(x, y)$. Касније, Гуревич [4] је пронашао 59-елементни модел HSI који не задовољава $W(x, y)$.

3. **Целобројне Алгебре и Прости Бројеви**

Дефиниција 3.1. $\overline{HSI}$-алгебра генерисана константом 1 назива се *целобројна* $\overline{HSI}$*-алгебра*. Исто тако, *HSI*-алгебра генерисана константом 1 назива се *целобројна HSI-алгебра*.

Лема 3.2. *Ако је* **A** *целобројна* $\overline{HSI}$*- или HSI-алгебра онда*

$$A = \{\underbrace{1 + 1 + \cdots + 1}_{n} : n \in N\}.$$

Доказ. Директно из 1.6. □

Лема 3.3. *У целобројној* $\overline{HSI}$*- или HSI-алгебри* **A** *можемо користити индуктивне доказе, тј. ако је* Φ *својство тако да важи* $\Phi(1)$*, и важи* $\Phi(x) \rightarrow \Phi(x+1)$*, онда за свако* x $\Phi(x)$ *важи.*

Доказ. Директно из 3.2. □

Лема 3.4. *Слободна алгебра генерисана празним скупом у класи* $\overline{HSI}$*-алгебри је* $\overline{\mathbf{N}}$*; и у класи HSI-алгебри је* **N**. *Последично, целобројне* $\overline{HSI}$*-алгебре су (до на изоморфизам) тачно количници од* $\overline{\mathbf{N}}$*; и целобројне HSI-алгебре су количници од* **N**.

Доказ. Ово је евидентно из чињенице да постоји само бесконачна $\overline{HSI}$-алгебра, респективно *HSI*-алгебра, генерисана празним скупом. □

Дефиниција 3.01. *Бинарна релација* ***конгруенције****, у ознаци "≡" дефинише се на скупу целих бројева на следећи начин:*

$$a \equiv b \bmod m \text{ ако и само ако } m|a-b.$$

Теорема 3.02. *За све* $a, b, c, d \in Z$ *и* $m > 0$ *важи:*

1) $a \equiv a \bmod m$.
2) $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$.
3) $a \equiv b \bmod m,\ b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$.
4) $a \equiv b \bmod m,\ c \equiv d \bmod m \Rightarrow a + c \equiv b + d \bmod m,\ a - c \equiv b - d \bmod m$.
5) $a \equiv b \bmod m,\ c \equiv d \bmod m \Rightarrow ac \equiv bd \bmod m$.

Доказ. Илустрације ради, показаћемо само 5. По датим условима имамо да $m|a-b$ и $m|c-d$. Због тога, $m|c(a-b) + b(c-d) = ac - bd$, тј. $ac \equiv bd \bmod m$. □

Дефиниција 3.03. *Нека је* $\sim$ *релација еквиваленције на скупу A.* ***Косет*** *(класа) елемента* $a \in A$ *је скуп*

$$a/_{\sim} = \{b \in A | b \sim a\}.$$

Количнички (фактор) скуп *скупа A по релацији* $\sim$ *је скуп*

$$A/_{\sim} = \{a/_{\sim} | a \in A\}.$$

Дефиниција 3.5. Нека је $\triangle_N$ релација једнакости на N, и за $a, k \in N$ нека је

$$\theta_{a,k} = \{\langle m, n\rangle \in N \times N : m = n; \text{или } a \leq m, n \text{ и } m \equiv n \; mod \; k\}.$$

Пропозиција 3.6. *Конгруенције од* $\overline{\mathbf{N}}$ *су тачно релације* $\triangle_N$ *и* $\theta_{a,k}$ *, где* $a, k \in N$.

Доказ. Прво ћемо доказати да је релација $\theta_{a,k}$ релација еквиваленције и да је сагласна са операцијама сабирања и множења.

(Р): Нека $\langle m, m\rangle \in N \times N. \; m = m$, тривијално. Такође, $a \leq m$ и $m \equiv m \; mod \; k$. Према дефиницији релације конгруенције имамо да је $m \equiv m \; mod \; k$ што је еквивалентно са $k|0$. Сваки број који је већи од нуле дели нулу.

(С): Претпоставимо да $\langle m, n\rangle$ припада релацији $\theta_{a,k}$. Треба показати да $\langle n, m\rangle$ такође припада $\theta_{a,k}$. Из $\langle m, n\rangle \in N \times N$ следи да $\langle n, m\rangle \in N \times N$. Ако је $m = n$ онда је $n = m$. Из $a \leq m, n$ следи $a \leq n, m$ и ако је $m \equiv n \; mod \; k$ онда је $n \equiv m \; mod \; k$ (особина релације конгруенције).

(Т): Претпоставимо да $\langle \ell, m\rangle$ и $\langle m, n\rangle$ припадају релацији $\theta_{a,k}$. Треба показати да $\langle \ell, n\rangle$ такође припада $\theta_{a,k}$.

Из $\langle \ell, m\rangle \in \theta_{a,k}$ следи да је $l = m$ или $a \leq l, m, \; l \equiv m \; mod \; k$. Из $\langle m, n\rangle \in \theta_{a,k}$ следи да је $m = n$ или $a \leq m, n, \; m \equiv n \; mod \; k$. Разликујемо четири случаја.

1. случај: $l = m, m = n$. Тада је $\ell = n$, па $\langle \ell, n\rangle \in \theta_{a,k}$.
2. случај: $l = m, \; a \leq m, n, \; m \equiv n \; mod \; k$. Тада је $a \leq \ell, n, \; \ell \equiv n \bmod k$, па $\langle \ell, n\rangle \in \theta_{a,k}$.
3. случај: $a \leq l, m, \; l \equiv m \; mod \; k, \; m = n$. Слично као у 2. случају закључујемо да $\langle \ell, n\rangle \in \theta_{a,k}$.
4. случај: $a \leq l, m, \; l \equiv m \; mod \; k, a \leq m, n, \; m \equiv n \; mod \; k$. Конгруенција по задатом модулу је транзитивна релација, па је $\ell \equiv n \bmod k$, а како је и $a \leq \ell, n$, закључујемо $\langle \ell, n\rangle \in \theta_{a,k}$.

Дакле, показали смо да је релација $\theta_{a,k}$ РСТ релација.

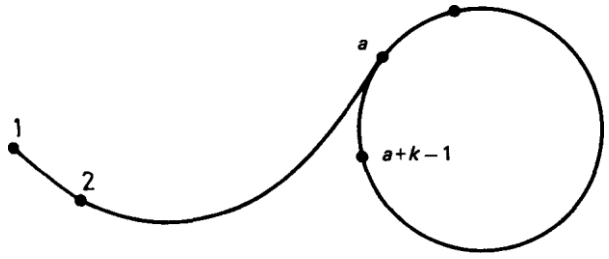
Сагласност са сабирањем: Нека $\langle e, f\rangle$ и $\langle g, h\rangle$ припадају релацији $\theta_{a,k}$. Из $\langle e, f\rangle \in N \times N$ и $\langle g, h\rangle \in N \times N$ следи да $\langle e + g, f + h\rangle \in N \times N$. Ако је $e = f$ и $g = h$ онда је $e + g = f + h$. Из $a \leq e, f$ и $a \leq g, h$ следи да је $a \leq e + g, f + h$ и ако је $e \equiv f \; mod \; k$ и $g \equiv h \; mod \; k$ следи да је $e + g \equiv f + h \; mod \; k$ (особина релације конгруенције).

Сагласност са множењем: Нека $\langle e, f\rangle$ и $\langle g, h\rangle$ припадају релацији $\theta_{a,k}$. Из $\langle e, f\rangle \in N \times N$ и $\langle g, h\rangle \in N \times N$ следи да $\langle e \cdot g, f \cdot h\rangle \in N \times N$. Ако је $e = f$ и $g = h$ онда је $e \cdot g = f \cdot h$. Из $a \leq e, f$ и $a \leq g, h$ следи да је $a \leq e \cdot g, f \cdot h$ и ако је $e \equiv f \; mod \; k$ и $g \equiv h \; mod \; k$ следи да је $e \cdot g \equiv f \cdot h \; mod \; k$ (особина релације конгруенције).

Дакле, $\triangle_N$ *и* $\theta_{a,k}$ су конгруенције од $\overline{\mathbf{N}}$, па једино што треба да покажемо јесте да је било која конгруенција од $\overline{\mathbf{N}}$ у жељеној форми. Нека је θ конгруенција од $\overline{\mathbf{N}}$. Бирамо најмањи елемент $a \in N$ тако да a/θ, класа еквиваленције по модулу θ, има бар два елемента, а затим онда бирамо најмање $k \in N$ тако да $a + k \in a/\theta$. Тада је $\theta = \theta_{a,k}$. □

Дефиниција 3.7. За $a, k \in N$ нека је $\overline{\mathbf{N}}_{a,k}$ количничка алгебра $\overline{N}/\theta_{a,k}$.

Није тешко описати (до на изоморфизам) све целобројне $\overline{HSI}$-алгебре. То су $\overline{\mathbf{N}}$ и $\overline{\mathbf{N}}_{a,k}$ за $a, k \in N$. Коначне целобројне $\overline{HSI}$-алгебре $\overline{\mathbf{N}}_{a,k}$ можемо визуализовати као петље са репом:



Слика 1. $\overline{N}_{a,k}$

Лема 3.8. *Било која конгруенција од* **N** *која није релација идентитета мора бити једна од* $\theta_{a,k}$.

Доказ. Свака конгруенција од **N** је такође и конгруенција од $\overline{\mathbf{N}}$. □

Дефиниција 3.9. Ако је $\theta_{a,k}$ конгруенција од **N** нека $\mathbf{N}_{a,k}$ означава $N/\theta_{a,k}$.

Лема 3.10. $\theta_{a,k}$ *је конгруенција од* **N** *ако и само ако*

$$x^a \equiv x^{a+k} \; mod \; k$$

важи за све $x \in N$.

Доказ. $\theta_{a,k}$ је конгруенција од **N** ако и само ако се слаже са операцијом степеновања, тј. ако $\langle m, n\rangle \in \theta_{a,k}$ онда за $s \in N$ треба да важи следеће:

$$\langle m^s, n^s\rangle \in \theta_{a,k} \qquad (12)$$

$$\langle s^m, s^n\rangle \in \theta_{a,k} \qquad (13)$$

Релација (12) следи из чињенице да се $\theta_{a,k}$ слаже са множењем. Остаје нам још услов (13) који се своди на следећи специјални случај:

$$\langle s^a, s^{a+k}\rangle \in \theta_{a,k} \qquad (14)$$

који може бити формулисан и као захтев:

$$x^a \equiv x^{a+k} \, mod \, k \tag{15}$$

који важи за све $x \in N$. □

Лема 3.11. *За било које* $a, k \in N$

$$x^a \equiv x^{a+k} \, mod \, k \, , \tag{16}$$

важи за све $x \in N$ *ако и само ако за све просте бројеве* p *имамо,*

$$p^e | k \Rightarrow e \leq a, \quad и \tag{17}$$

$$p | k \Rightarrow (p-1) | k. \tag{18}$$

Доказ. (⇒) Претпоставимо да су прост број p и $e \in N$ такви да важи $p^e | k$. Тада

$$\begin{aligned} p^a \equiv p^{a+k} \, mod \, k &\Rightarrow k | p^{a+k} - p^a \\ &\Rightarrow k | p^a (p^k - 1) \\ &\Rightarrow p^e | p^a (p^k - 1) \\ &\Rightarrow e \leq a. \end{aligned}$$

Овим смо установили (17).

Сада претпоставимо да $p | k$. Бирамо $b \in N$ тако да ред од $[b]$ у мултипликативној групи $\mathbf{Z}_p^*$ прстена $\mathbf{Z}_p$ буде $p-1$ (то је могуће јер је поменута група циклична). Из $p | k$ и (16), тј. $k | b^a (b^k - 1)$, следи да $p | b^a (b^k - 1)$; а пошто p не дели b закључујемо да $p | b^k - 1$. Дакле, $[b]^k = 1$ у $\mathbf{Z}_p^*$, па користећи познату теорему теорије група добијамо $(p-1) | k$, тј. (18).

(⇐) Ако је $k = 1$, импликација је тривијална. Нека је $k > 1$, и

$$k = p_1^{e_1} \cdots p_r^{e_r}$$

где су p_i различити прости бројеви, и e_i позитивни цели бројеви. Тада из наших претпоставки имамо, за $1 \leq i \leq r$,

$$e_i \leq a \quad \text{и} \quad (p_i - 1) | k.$$

Фокусирајмо се на један од p_i и нека је дат $b \in N$.

Случај 1. Претпоставимо да $p_i|b$. Тада користимо

$$\begin{aligned} p_i|b &\Rightarrow p_i^{e_i}|b^{e_i}|b^a \\ &\Rightarrow p_i^{e_i}|b^a(b^k-1) \\ &\Rightarrow b^a \equiv b^{a+k}\, mod p_i^{e_i}. \end{aligned}$$

Случај 2. Претпоставимо да $p_i \nmid b$. Приметимо прво да $\varphi(p_i^{e_i})|k$, где је φ Ојлерова функција, јер је $\varphi\left(p_i^{e_i}\right) = p_i^{e_i-1}(p_i-1)$, и $p_i^{e_i-1}|k$ и $p_i-1|k$. Користећи ово имамо

$$\begin{aligned} p_i \nmid b &\Rightarrow b^{\varphi(p_i^{e_i})} \equiv 1\, mod\, p_i^{e_i} \\ &\Rightarrow b^k \equiv 1\, mod\, p_i^{e_i} \\ &\Rightarrow b^{a+k} \equiv b^a\, mod\, p_i^{e_i}. \end{aligned}$$

Тако, у сваком случају, имамо $b^a \equiv b^{a+k}\, mod\, p_i^{e_i}$; и пошто ово важи за свако $p_i^{e_i}$ следи да је $b^a \equiv b^{a+k}\, mod\, k$. Овим је лема доказана. □

Комбиновањем ове две леме дошли смо до наше главне карактеризације конгруенција од **N**.

Теорема 3.12. *За $a, k \in N$ релација $\theta_{a,k}$ је конгруенција од* **N** *ако и само ако за све просте бројеве p важи*

$$p^e|k \Rightarrow e \leq a \qquad (19)$$

$$p|k \Rightarrow (p-1)|k. \qquad (20)$$

Из (20) видимо да за непаран број k добијамо коначну целобројну HSI-алгебру $\mathbf{N}_{a,k}$ само у случају да је $k = 1$. Ако је $k = 1$ онда за свако $a \in N$ имамо по једну коначну целобројну HSI-алгебру $\mathbf{N}_{a,1}$, која садржи природне бројеве мање или једнаке од a. Такође, лако се види да за $k = 2$ и било које $a \in N$ имамо коначну целобројну HSI-алгебру $\mathbf{N}_{a,2}$.

Последица 3.13. *Нека је* $\mathbf{N}_{a,k}$ *коначна целобројна HSI-алгебра за* $k > 1$, *и нека је* $k = {p_1}^{e_1} \cdots {p_r}^{e_r}$ *за* $p_1 < \cdots < p_r$. *Тада*

$$e_i \leq a \quad за \quad 1 \leq i \leq r \tag{21}$$

$$p_1 = 2 \tag{22}$$

$$(p_i - 1) | {p_1}^{e_1} \cdots {p_{i-1}}^{e_{i-1}} \quad за \quad 2 \leq i \leq r. \tag{23}$$

Доказ. (21) следи из (19); (22) и (23) следе из (20). □

Из (23) видимо да је p_2 увек облика $2^m + 1$, и стога је Фермаов прост број. Следећа последица нам даје комплетну листу 5 „цикличних“ целобројних *HSI*-алгебри, тј. алгебри „без репа“ за које је $a = 1$.

Последица 3.14. (Д. Хигс) *Постоји коначна целобројна HSI-алгебра* $\mathbf{N}_{1,\mathrm{k}}$ *ако и само ако* $k \in \{1, 2, 6, 42, 1806\}$.

Доказ. Претпоставимо да је $\mathbf{N}_{1,\mathrm{k}}$ целобројна *HSI*-алгебра. Тада према Последици 3.13. имамо

- $k = p_1 \cdots p_r$ где $p_1 < \cdots < p_r$
- $p_1 = 2$
- $(p_i - 1) | p_1 \cdots p_{i-1}$ за $2 \leq i \leq r$.

Онда како је сваки од p_2 до p_4 јединствено одређен, наиме

$$(p_2 - 1) | 2 \Rightarrow p_2 = 3$$

$$(p_3 - 1) | 2 \cdot 3 \Rightarrow p_3 = 7$$

$$(p_4 - 1) | 2 \cdot 3 \cdot 7 \Rightarrow p_4 = 43;$$

и не постоји прост број $p_5 > 43$ тако да је $(p_5 - 1) | 2 \cdot 3 \cdot 7 \cdot 43 = 1806$. □

Дефиниција 3.15. За дато $a \in N$ нека је $\sum_a = (p_1, p_2, \dots)$ низ простих бројева:

- $p_1 = 2$
- за дате $p_1, \dots, p_i$ нека p_{i+1} буде најмањи прост број p који је већи од p_i тако да

$(p - 1) | (p_1 \cdots p_i)^a$, претпостављајући да p постоји. Ако p не постоји онда се $\sum_a$ завршава са p_i.

Пропозиција 3.16. *За дат позитиван цео број* a*, постоји бесконачно много целобројних HSI-алгебри* $\mathbf{N}_{a,k}$ *(са репом дужине* $a-1$ *) ако и само ако је низ простих бројева* $\sum_a$ *бесконачан.*

Доказ. Нека је $\sum_a = (p_1, \dots)$, и дефинишимо да $\prod_a = (q_1, \dots)$ буде списак простих бројева q, у растућем поретку, за које постоји $k \in N$ тако да $q|k$ и $\theta_{a,k}$ је конгруенција од **N**.

Ако је $\prod_a$ бесконачан онда мора постојати произвољно велико k тако да је $\theta_{a,k}$ конгруенција од **N**, дакле постоје произвољно велике целобројне HSI-алгебре $\mathbf{N}_{a,k}$.

Са друге стране, за дат коначан скуп простих бројева S, по Теореми 3.12., за само коначно много k за које је $\theta_{a,k}$ конгруенција од **N** и просте бројеве који деле k су у S. Тако ако имамо бесконачно много целобројних HSI-алгебри $\mathbf{N}_{a,k}$ низ $\prod_a$ мора бити бесконачан. Последично постоји бесконачно много $\mathbf{N}_{a,k}$ ако и само ако је $\prod_a$ бесконачан.

Сада желимо да покажемо да је $\sum_a = \prod_a$. Нека $p \in \sum_a$, $p = p_i$. Тада стављајући $k = (p_1 \cdots p_i)^a$ имамо да је $\theta_{a,k}$ конгруенција од **N** по Теореми 3.12., па се p_i појављује у $\prod_a$.

Да покажемо да се сваки сваки прост број из $\prod_a$ јавља у $\sum_a$ користимо једноставан индуктивни аргумент. Прво приметимо да је $p_1 = q_1 = 2$. Сада претпоставимо да је $p_j = q_j$ за $1 \leq j \leq i$. Ако постоји q_{i+1} онда бирамо $k \in N$ тако да $q_{i+1}|k$ и $\theta_{a,k}$ је конгруенција од **N**. Прости бројеви који деле k а који су мањи од q_{i+1} морају бити између $q_1, \dots, q_i$ (по дефиницији $\prod_a$), па тако и између $p_1, \dots, p_i$. Из Последице 3.13. видимо да $(q_{i+1} - 1)|(p_1 \cdots p_i)^a$, па се q_{i+1} јавља у $\sum_a$.

Тако је $\sum_a = \prod_a$ па је пропозиција доказана. □

Као што смо видели у Хигсовом резултату, $\sum_1 = (2, 3, 7, 43)$ је коначан низ.

Проблем 1. Да ли је $\sum_a$ коначан за $a > 1$?

Проверено је да око 20% простих бројева мањих од 1000000 припада скупу $\sum_1 = (2, 3, 5, 7, 11, 13, 19, 23, \dots, 999667, 999727, \dots)$. Ова чињеница обесхрабрује покушаје да се и помоћу рачунара одреди скуп $\sum_2$, уколико је он коначан.

4. Пет 2-елементних HSI-Алгебри

У овом одељку одредићемо пет 2-елементних HSI-алгебри, и искористити их да покажемо како се може направити велик број коначних HSI-алгебри из већ познатих алгебри (на пример дистрибутивне мреже).

Теорема 4.1. *Постоји тачно 5 2-елементних HSI-алгебри, до на изоморфизам, и оне су:*

1.

$+$	1	a
1	1	1
a	1	a

$\cdot$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	1

2.

$+$	1	a
1	1	1
a	1	a

$\cdot$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	a

3.

$+$	1	a
1	1	a
a	a	a

$\cdot$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	a

4.

$+$	1	2
1	2	2
2	2	2

$\cdot$	1	2
1	1	2
2	2	2

$\uparrow$	1	2
1	1	1
2	2	2

5.

$+$	1	2
1	2	1
2	1	2

$\cdot$	1	2
1	1	2
2	2	2

$\uparrow$	1	2
1	1	1
2	2	2

Доказ. Прво крећемо налазити по могућству 2-елементне HSI-алгебре. Таква алгебра садржи један цео број или два цела броја, па су могући случајеви:

Случај 1. $\boxed{2 = 1}$ Из (6) и (9) имамо

$$x + x \approx x \quad x \cdot x \approx x.$$

Кејлијеве таблице за такву једну HSI-алгебру би изгледале овако

$+$	1	a
1	1	b
a	b	a

$\cdot$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	c

Постоји највише 4 могућности: алгебре 1, 2, 3 на претходној страни, и

$+$	1	a
1	1	a
a	a	a

$\cdot$	1	a
1	1	a
a	a	a

$\uparrow$	1	a
1	1	1
a	a	1

Међутим, последња алгебра не задовољава (9) јер $a^{1+a} = a^a = 1$, али $a^1 \cdot a^a = a \cdot 1 = a$.

Случај 2. $\boxed{2 \neq 1}$ Тада су сви елементи алгебре цели бројеви, па се бавимо целобројним HSI-алгебрама. Постоје тачно две 2-елементне целобројне HSI-алгебре: $\mathbf{N}_{2,1}$, која је 4., и $\mathbf{N}_{1,2}$, која је 5. на претходној страни.

На овај начин, број могућих 2-елементних HSI-алгебри је 5. Лако је проверити за сваку од њих да заиста задовољава HSI, и да нису сваке две изоморфне. □

Проблем 2. Да ли свака 2-елементна HSI-алгебра задовољава све идентитете из $\mathbf{N}$?

Наравно, алгебре $\mathbf{N}_{2,1}$ и $\mathbf{N}_{1,2}$ задовољавају $(\mathbf{N})$, јер су количници од $\mathbf{N}$. Проблем су преостале три алгебре из 4.1. Са тачке гледишта универзалне алгебре одговор је потврдан ако и само ако је свака од наведене три алгебре хомоморфна слика подалгебре F од $\mathbf{N}^N$ генерисане елементом $\langle 1, 2, 3, \dots \rangle$. Ако постоји идентитет $p \approx q$ који важи у $\mathbf{N}$ а не важи у некој од ових 2-елементних алгебри, онда добијамо доказ да $p \approx q$ не следи из HSI.

5. Пет Класа HSI-Алгебри

Прво неколико примера $\overline{HSI}$-алгебри.

Дефиниција 5.01. *Мрежа* $(D,\vee,\wedge)$ *је* ***дистрибутивна*** *ако следећи идентитети важе за све* x, y и z *из* D: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ и $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Дефиниција 5.02. *Полумрежа* $(S,\wedge)$ *је алгебарска структура која се састоји од скупа* S *и бинарне операције* $\wedge$, *тако да за све* x, y и z *из* S *важе следећи идентитети:* $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, $x \wedge y = y \wedge x$ *и* $x \wedge x = x$.

Лема 5.1.

(а) *Нека је* $\mathbf{D} = \langle D,\vee,\wedge, 1\rangle$ *дистрибутивна мрежа са највећим елементом* 1. *Тада је* $\mathbf{D}$ $\overline{HSI}$*-алгебра*.

(б) *Нека је* $\mathbf{S} = \langle S,\wedge, 1\rangle$ $\wedge$*-полумрежа са највећим елементом* 1. *Тада је* $\langle S,\wedge,\wedge, 1\rangle$ $\overline{HSI}$*-алгебра.*

Доказ. Директно из основних закона дистрибутивних мрежа и полумрежа. □

Лема 5.2. *Нека је* $\mathbf{A} = \langle A, +,\cdot, 1\rangle$ $\overline{HSI}$*-алгебра. Тада је проширење* $\mathbf{A}_\pi = \langle A, +,\cdot, \pi, 1\rangle$ *алгебре* $\mathbf{A}$, *где је* π *прва пројекција на* $A \times A$, *једна HSI-алгебра ако и само ако је операција множења идемпотентна, тј.,* $x \cdot x \approx x$ *важи у* $\mathbf{A}$.

Доказ. Ако имамо λ-алгебру са степеновањем где је $a^b = a$ онда је тривијално проверити да идентитети (7), (8), (10) и (11) важе. И (9) важи ако и само ако је множење идемпотентно. □

Приметимо да је у свим алгебрама из Теореме 4.1, осим у првој алгебри, степеновање заправо прва пројекција. У наставку описујемо својеврсна уопштења сваке од 2-елементних HSI-алгебри.

Дефиниција 5.03. *Хејтингова алгебра је ограничена мрежа дефинисана са бинарном операцијом* $a \to b$, *тако да је* $(c \wedge a) \leq b$ *еквивалентно са* $c \leq (a \to b)$.

Пропозиција 5.3. *Нека је* $\mathbf{H} = \langle H,\vee,\wedge,\to, 0, 1\rangle$ *Хејтингова алгебра. Тада је* $\mathbf{H^*} = \langle H,\vee,\wedge,\leftarrow, 1\rangle$ *HSI-алгебра, где је* $a \leftarrow b$ *дефинисано са* $b \to a$.

Доказ. Присетимо се да је Хејтингова операција $\to$ дефинисана на следећи начин: $a \to b = c$ ако и само ако је c највећи елемент тако да су $(c \wedge a) \leq b$. Будући да је $\langle H,\vee,\wedge, 1\rangle$ дистрибутивна мрежа са јединицом, то је и $\overline{HSI}$*-алгебра* по Леми 5.1. Идентитети (6)-(11), записани са операцијама из $\mathbf{H^*}$, добијају следећи облик:

$$1 \leftarrow x \approx 1$$

$$x \leftarrow 1 \approx x$$

$$x \leftarrow (y \vee z) \approx (x \leftarrow y) \wedge (x \leftarrow z)$$

$$(x \wedge y) \leftarrow z \approx (x \leftarrow z) \wedge (y \leftarrow z)$$

$$(x \leftarrow y) \leftarrow z \approx x \leftarrow (y \wedge z),$$

и позната су својства Хејтингових алгебри. □

Пропозиција 5.4. *Нека је* $\mathbf{D} = \langle D, \vee, \wedge, 1 \rangle$ *дистрибутивна мрежа са јединицом. Тада је* $\mathbf{D}_\pi = \langle D, \vee, \wedge, \pi, 1 \rangle$ *HSI-алгебра.*

Доказ. Применити Леме 5.1 и 5.2. □

$\mathbf{D}_\pi$ је изоморфна подалгебри неког степена друге алгебре у Теореми 4.1.

Пропозиција 5.5. *Нека је* $\mathbf{S} = \langle S, \wedge, 1 \rangle$ *полумрежа са јединицом. Тада је* $\langle S, \wedge, \wedge, \pi, 1 \rangle$ *HSI-алгебра.*

Доказ. Применити Леме 5.1 и 5.2. □

$\langle S, \wedge, \wedge, \pi, 1 \rangle$ је изоморфна подалгебри неког степена треће алгебре у Теореми 4.1.

Пропозиција 5.6. *Нека је* $\mathbf{S} = \langle S, \wedge, 0, 1 \rangle$ *полумрежа са* $0, 1$. *Тада је* $\langle S, f, \wedge, \pi, 1 \rangle$ *HSI-алгебра, где је* f *бинарна константна функција чија је вредност увек* 0.

Доказ. Применити Лему 5.2. □

$\langle S, f, \wedge, \pi, 1 \rangle$ је изоморфна подалгебри неког степена четврте алгебре у Теореми 4.1.

Пропозиција 5.7. *Нека је* $\mathbf{R} = \langle R, +, \cdot, 0, 1 \rangle$ *Булов прстен. Тада је* $\langle R, +, \cdot, \pi, 1 \rangle$ *HSI-алгебра.*

Доказ. Применити Лему 5.2. □

$\langle R, +, \cdot, \pi, 1 \rangle$ је изоморфна подалгебри неког степена пете алгебре у Теореми 4.1.

6. Напомене о могућностима примене рачунара

Ако је A коначан непразан скуп од n елемената онда постоји n^{n^2} могућих бинарних операција на A; па постоји $n \cdot n^{3n^2}$ могућих λ-алгебри из A, и $n \cdot n^{2n^2}$ могућих $\overline{\lambda}$-алгебри из A. Да бисмо пронашли 3-елементне HSI-алгебре чини се мудро да употребимо рачунар, након што претходно на неки начин смањимо број могућности. Применом идентитета (1), (3), (4), (7) и (8) уочавамо да су 3-елементне HSI-алгебре следећег облика:

$+$	1	a	b
1	c	d	e
a	d	f	g
b	e	g	h

$\cdot$	1	a	b
1	1	a	b
a	a	i	j
b	b	j	k

$\uparrow$	1	a	b
1	1	1	1
a	a	l	m
b	b	n	o

Укупан број алгебри за тестирање је сада 3^{13}, приближно 1600000. Компјутеру би требало дуго времена да спроведе сва тестирања. Да бисмо додатно убрзали потрагу, настављамо као у одељку 4 и да разликујемо случајеве у зависности од тога како изгледају целобројне HSI-алгебре. Разматрамо сваку од пет могућности $\mathbf{N}_{1,1}, \mathbf{N}_{1,2}, \mathbf{N}_{2,1}, \mathbf{N}_{2,2}, \mathbf{N}_{3,1}$.

Случај 1. $\boxed{\mathbf{N}_{1,1}}$ У овом случају важи $x + x \approx x$ и $x \cdot x \approx x$, и ово смањује могућности за Кејлијеве таблице до следећих:

$+$	1	a	b
1	1	d	e
a	d	a	g
b	e	g	b

$\cdot$	1	a	b
1	1	a	b
a	a	a	j
b	b	j	b

$\uparrow$	1	a	b
1	1	1	1
a	a	l	m
b	b	n	o

Коначан број случајева за проверу је сада $3^8 = 6581$. Ако се ограничимо само на прве две Кејлијеве таблице, треба испитати $3^4 = 81$ $\bar{\lambda}$-алгебри, и испоставиће се да су $\overline{HSI}$-алгебре само њих 10. За сваку од ових 10 $\overline{HSI}$-алгебри имамо 81 могућих проширења до λ-алгебре засноване на трећој Кејлијевој таблици изнад, па укупно имамо 810 λ-алгебри за проверу у овом случају.

Случај 2. $\boxed{\mathbf{N}_{2,1}}$ У овом случају (а и у преосталим случајевима) имамо $x + x \approx 2 \cdot x$ и $x \cdot x \approx x^2$, што нас доводи до следећих случајева:

$+$	1	2	b
1	1	2	e
2	2	2	g
b	e	g	h

$\cdot$	1	2	b
1	1	2	b
2	2	2	h
b	b	h	k

$\uparrow$	1	2	b
1	1	1	1
2	2	2	m
b	b	k	o

Коначан број λ-алгебри за проверу у овом случају је $3^6 = 729$.

Случај 3. $\boxed{\mathbf{N}_{1,2}}$ Имамо

$+$	1	2	b
1	2	1	e
2	1	2	g
b	e	g	h

$\cdot$	1	2	b
1	1	2	b
2	2	2	h
b	b	h	k

$\uparrow$	1	2	b
1	1	1	1
2	2	2	m
b	b	k	o

Коначан број λ-алгебри за проверу у овом случају је такође $3^6 = 729$.

Случај 4. $\boxed{\mathbf{N}_{2,2}}$ Једина HSI-алгебра је $\mathbf{N}_{2,2}$.

Случај 5. $\boxed{\mathbf{N}_{3,1}}$ Једина HSI-алгебра је $\mathbf{N}_{3,1}$.

Није тешко написати програм који ће пронаћи 3-елементне HSI-алгебре. Испоставља се да постоје тачно 44 3-елементне HSI-алгебре.

Могли бисмо такође наћи све 4- и 5-елементне HSI-алгебре у разумном времену. Потрага за 6-елементним HSI-алгебрама трајала би месецима, док је рачунарска потрага за 7-елементним HSI-алгебрама за сада безнадежна.

7. Вилкијев Идентитет

Дефиниција 7.1. Нека су

$$P(x) = 1 + x$$
$$Q(x) = 1 + x + x^2$$
$$R(x) = 1 + x^3$$
$$S(x) = 1 + x^2 + x^4.$$

1980. године Вилки је показао да следећи идентитет, који зовемо $W(x, y)$, важи у $\mathbf{N}$ али не може да се изведе из HSI (где је $P = P(x)$, итд):

$$(P^x + Q^x)^y \cdot (R^y + S^y)^x \approx (P^y + Q^y)^x \cdot (R^x + S^x)^y.$$

Пропозиција 7.2. $\mathbf{N}$ *задовољава* $W(x, y)$.

Доказ. Дефинишимо операцију □ на N са

$$m \square n = \begin{cases} m - n \text{ ако } m > n \\ 1 \text{ иначе,} \end{cases}$$

и нека је $\mathbf{N}_\square$ проширење $\langle N, +, \cdot, \uparrow, \square, 1\rangle$ од $\mathbf{N}$. Тада, ако је $F(x) = (1 + x^2) \square x$ имамо да у $\mathbf{N}_\square$ важи:

$$R \approx P \cdot F$$
$$S \approx Q \cdot F$$

Тако $\mathbf{N}_\square$ задовољава

$$\begin{aligned}(P^x + Q^x)^y \cdot (R^y + S^y)^x &\approx F^{x \cdot y}(P^x + Q^x)^y \cdot (P^y + Q^y)^x \\ &\approx (R^x + S^x)^y \cdot (P^y + Q^y)^x \\ &\approx (P^y + Q^y)^x \cdot (R^x + S^x)^y.\end{aligned}$$

Како $\mathbf{N}_\square$ задовољава $W(x, y)$, тако и $\mathbf{N}$. □

$W(x, y)$ је најједноставнији познат идентитет који важи у $\mathbf{N}$, али се не може извести из HSI. Као што је споменуто на почетку, Вилки је користио синтаксну анализу доказа; касније, 1985. године, Гуревич [4] је објавио нови доказ конструисањем 59-елементне алгебре која задовољава HSI али не и $W(x, y)$.

Дефиниција 7.3. *Гуревич-алгебра* (или G-алгебра) је модел HSI који не задовољава Вилкијев идентитет $W(x, y)$.

Гуревич у раду [6] на стр. 30 напомиње:

К. В. Хенсон се једном запитао да ли постоје контрамодели за Тарскијево питање (да ли су сви тачни идентитети $(+, \cdot, \uparrow)$ изводљиви) веома мале величине, рецимо, 5. Тренутно,

не знам, мој сопствени рекорд је 33 елемента, али сам чуо гласине да је неко оборио рекорд на 28 елемената.

Показаћемо да најмања G-алгебра има барем 7 елемената (видети одељак 8). 28-елементну G-алгебру је пронашао 1988. године Бурис, а 16-елементну Ли 1990. Недавно, Ли је пронашао најмању познату такву алгебру, са 15 елемената, која је приказана у одељку 9.

8. Доња граница

Показаћемо да било која HSI-алгебра која не задовољава $W(x,y)$ има барем 7 елемената. Да бисмо постигли ово, наводимо неколико својстава елемената a,b неке HSI-алгебре $\mathbf{A}$ која гарантују да $W(a,b)$ важи у $\mathbf{A}$. Избегавање ових својстава показаће да величина алгебре мора да буде барем седам.

Када пишемо P, Q, R, S без аргумента, мислимо на $P(x), Q(x), R(x), S(x)$.

Лема 8.1.

$$HSI \vdash \forall x W(x,x).$$

Доказ. То је очигледно јер су обе стране једнакости $W(x,x)$ исте. □

Лема 8.2. *За цео број* n, *тј.* $n = \underbrace{1+\cdots+1}_{n}$, *имамо*

$$HSI \vdash \forall y W(n,y).$$

Доказ. Нека је $m = 1 - n + n^2$, цео број. Тада

$$HSI \vdash P(n)\cdot m \approx R(n)$$
$$HSI \vdash Q(n)\cdot m \approx S(n)$$

Из HSI могу се извести следеће једнакости:

$$\begin{aligned}(P(n)^n + P(n)^n)^y \cdot (R(n)^y + S(n)^y)^n &\approx m^{n\cdot y}(P(n)^n + Q(n)^n)^y \cdot (P(n)^y + Q(n)^y)^n \\ &\approx (R(n)^n + S(n)^n)^y \cdot (P(n)^y + Q(n)^y)^n \\ &\approx (P(n)^y + Q(n)^y)^n \cdot (R(n)^n + S(n)^n)^y.\end{aligned}$$

Дакле,

$$HSI \vdash W(n,y). \square$$

Лема 8.3.

$$HSI \vdash P\cdot S \approx Q\cdot R.$$

Доказ. Ово заправо следи из $\overline{HSI}$; обе стране су једнаке $1 + x + x^2 + x^3 + x^4 + x^5$. □

Лема 8.4. *За цео број n имамо*

$$HSI \vdash \forall x W(x, n).$$

Доказ. Користећи HSI могу се извести једнакости:

$$(P^x + Q^x)^n \cdot (R^n + S^n)^x \approx \left(\sum_{i=0}^{n} \binom{n}{i} \cdot (P^x)^i \cdot (Q^x)^{n-i}\right) \cdot (R^n + S^n)^x$$
$$\approx \sum_{i=0}^{n} \binom{n}{i} \cdot (P^i \cdot Q^{n-i} \cdot R^n + P^i \cdot Q^{n-i} \cdot S^n)^x;$$

и

$$(P^n + Q^n)^x \cdot (R^x + S^x)^n \approx (P^n + Q^n)^x \cdot \left(\sum_{i=0}^{n} \binom{n}{i} \cdot (R^x)^i \cdot (S^x)^{n-i}\right)$$
$$\approx \sum_{i=0}^{n} \binom{n}{i} \cdot (P^n \cdot R^i \cdot S^{n-i} + Q^n \cdot R^i \cdot S^{n-i})^x.$$

Сада, користећи Лему 8.3, можемо извести из HSI, за $0 \leq i \leq n$,

$$P^i \cdot Q^{n-i} \cdot R^n \approx P^n \cdot R^i \cdot S^{n-i};$$
$$P^i \cdot Q^{n-i} \cdot S^n \approx Q^n \cdot R^i \cdot S^{n-i}.$$

Тако имамо извођење из HSI

$$(P^x + Q^x)^n \cdot (R^n + S^n)^x \approx (P^n + Q^n)^x \cdot (R^x + S^x)^n,$$

које је $W(x, n)$. □

Последица 8.5. *Ако је* **A** *G-алгебра и $a, b \in A$ такви да $W(a, b)$ не важи онда су a, b различити елементи из A који нису цели.*

Доказ. Комбиновањем Лема 8.1, 8.2 и 8.4. □

Дефиниција 8.6. Нека је $u|v$ скраћење за формулу $\exists w(v \approx u \cdot w)$.

Тврђење $HSI \vdash \sum \to W(x, y)$ заправо значи $HSI \vdash \forall x \forall y[\sum \to W(x, y)]$.

Лема 8.7. (Ли)

$$HSI \vdash x|y \to W(x, y).$$

Доказ. Нека је $y \approx u \cdot x$. Приметимо да је пети корак следећег извођења из HSI, последица Леме 8.3:

$$(P^x + Q^x)^y \cdot (R^y + S^y)^x \approx (P^x + Q^x)^{u \cdot x} \cdot (R^{u \cdot x} + S^{u \cdot x})^x$$
$$\approx [(P^x + Q^x)^u \cdot (R^{u \cdot x} + S^{u \cdot x})]^x$$
$$\approx [((P \cdot R)^x + (Q \cdot R)^x)^u + ((P \cdot S)^x + (Q \cdot S)^x)^u]^x$$
$$\approx [((P \cdot R)^x + (P \cdot S)^x)^u + ((Q \cdot R)^x + (Q \cdot S)^x)^u]^x$$
$$\approx [P^{ux}(R^x + S^x)^u + Q^{ux}(R^x + S^x)^u]^x$$
$$\approx [(P^{ux} + Q^{ux}) \cdot (R^x + S^x)^u]$$

$$\approx (P^y + Q^y) \cdot (R^x + S^x)^{ux}$$
$$\approx (P^y + Q^y) \cdot (R^x + S^x)^y. \square$$

У наставку описујемо једну од основних техника за успостављање услова под којима $W(a, b)$ важи.

Дефиниција 8.8. *Правила „Гурај-Вуци“*

Нека је Σ неки скуп λ-идентитета. Формулишемо правила преписивања петорки $\overline{HSI}$-термова као што следи (прва два су *вуци правила*, друга два *гурај правила*),

$$(t, \overline{t} \cdot p, \overline{t} \cdot q, r, s) \to_\Sigma (t \cdot \overline{t}, p, q, r, s) \quad (24)$$
$$(t, p, q, \overline{t} \cdot r, \overline{t} \cdot s) \to_\Sigma (t \cdot \overline{t}, p, q, r, s) \quad (25)$$
$$(t \cdot \overline{t}, p, q, r, s) \to_\Sigma (t, \overline{t} \cdot p, \overline{t} \cdot q, r, s) \quad (26)$$
$$(t \cdot \overline{t}, p, q, r, s) \to_\Sigma (t, p, q, \overline{t} \cdot r, \overline{t} \cdot s) \quad (27)$$

и ако је $\sum \to t \approx t' \wedge p \approx p' \wedge \cdots \wedge s \approx s'$ последица $\overline{HSI}$ онда

$$(t, p, q, r, s) \to_\Sigma (t', p', q', r', s') \quad (28)$$

Дефиниција 8.9. Нека је $\to_\Sigma^*$ рефлексивно и транзитивно затварање за $\to_\Sigma$.

Лема 8.10. *Претпоставимо* $(t, p, q, r, s) \to_\Sigma^* (t', p', q', r', s')$. *Тада*

$$(t, q, p, r, s) \to_\Sigma^* (t', q', p', r', s') \quad (29)$$
$$(t, p, q, s, r) \to_\Sigma^* (t', p', q', s', r') \quad (30)$$
$$(t, r, s, p, q) \to_\Sigma^* (t', r', s', p', q') \quad (31)$$

Доказ. Последица дефиниције 8.8. □

Сада да погледамо разлоге за увођење гурај-вуци правила.

Лема 8.11. *Ако*

$$(1, P, Q, R, S) \to_\Sigma^* (t, p, q, r, s)$$

онда

$$HSI \vdash \sum \to t \cdot p \cdot s \approx t \cdot q \cdot r; \quad (32)$$

и

$$HSI \vdash \sum \to (P^x + Q^x)^y \cdot (R^y + S^y)^x \approx t^{x \cdot y} (p^x + q^x)^y \cdot (r^y + s^y)^x \quad (33)$$

Доказ. Тврђење се једноставно доказује индукцијом по дужини $\to_\Sigma^*$ извођења за (t, p, q, r, s). За базу индукције користи се Лема 8.3. □

Лема 8.12. *Ако*

$$(1, P, Q, R, S) \to_{\Sigma}^{*} (t, p, q, r, s)$$

и важи једна од следећих једнакости:

$$\{p, q\} = \{r, s\} \tag{34}$$

$$p = q \tag{35}$$

$$r = s \tag{36}$$

онда

$$HSI \vdash \sum \to W(x, y).$$

Доказ.

Случај 1. $\boxed{\{p, q\} = \{r, s\}}$ Из (31) имамо

$$(1, R, S, P, Q) \to_{\Sigma}^{*} (t, r, s, p, q)$$

и затим из (33) и

$$HSI \vdash \sum \to W(x, y).$$

будући да $\{p, q\} = \{r, s\}$ обезбеђује

$$HSI \vdash t^{x \cdot y}(p^x + q^x)^y \cdot (r^y + s^y)^x \approx t^{x \cdot y}(p^y + q^y)^x \cdot (r^x + s^x)^y.$$

Случај 2. $\boxed{p \approx q}$ У овом случају користимо гурај-вуци правила и Лему 8.3:

$$\begin{aligned}(t, p, q, r, s) &\to_{\Sigma}^{*} (t, p, p, r, s)\\ &\to_{\Sigma}^{*} (t \cdot p, 1, 1, r, s)\\ &\to_{\Sigma}^{*} (1, 1, 1, t \cdot p \cdot r, t \cdot p \cdot s)\\ &\to_{\Sigma}^{*} (1, 1, 1, t \cdot q \cdot r, t \cdot p \cdot s)\\ &\to_{\Sigma}^{*} (1, 1, 1, t \cdot q \cdot r, t \cdot q \cdot r)\\ &\to_{\Sigma}^{*} (t \cdot q \cdot r, 1, 1, 1, 1).\end{aligned}$$

Добијамо

$$(1, P, Q, R, S) \to_{\Sigma}^{*} (t \cdot q \cdot r, 1, 1, 1, 1)$$

па можемо применити резутате из случаја 1.

Случај 3. $\boxed{r \approx s}$ Као случај 2. Овим је доказ завршен. □

Лема 8.13. (Ли) *Ако је* $\sum$ *један од следећих услова*

$$P|Q \qquad (37)$$

$$Q|P \qquad (38)$$

$$R|S \qquad (39)$$

$$S|R \qquad (40)$$

$$t \cdot P \approx R \;\; и \;\; t \cdot Q \approx S \qquad (41)$$

$$P \approx t \cdot R \;\; и \;\; Q \approx t \cdot S \qquad (42)$$

онда важи

$$HSI \vdash \sum \to W(x, y).$$

Доказ. Претпоставимо да важи (37). Нека је $\sum$ једнако $u \cdot P \approx Q$. Тада из гурај-вуци правила и Леме 8.3 имамо

$$\begin{aligned}(1, P, Q, R, S) &\to_{\Sigma}^{*} (1, P, u \cdot P, R, S) \\ &\to_{\Sigma}^{*} (P, 1, u, R, S) \\ &\to_{\Sigma}^{*} (1, 1, u, P \cdot R, P \cdot S) \\ &\to_{\Sigma}^{*} (1, 1, u, P \cdot R, Q \cdot R) \\ &\to_{\Sigma}^{*} (R, 1, u, P, Q) \\ &\to_{\Sigma}^{*} (R, 1, u, P, P \cdot u) \\ &\to_{\Sigma}^{*} (R \cdot P, 1, u, 1, u)\end{aligned}$$

па, по (34) из Леме 8.12, $W(x, y)$ је последица $\sum$, за дату HSI. Докази следећа три случаја су слична.

За пети случај нека је $\sum$ скуп $\{u \cdot P \approx R, u \cdot Q \approx S\}$. Тада

$$\begin{aligned}(1, P, Q, R, S) &\to_{\Sigma}^{*} (1, P, Q, u \cdot P, u \cdot Q) \\ &\to_{\Sigma}^{*} (u, P, Q, P, Q),\end{aligned}$$

па, опет из (34) у Леми 8.12, $W(x, y)$ је последица $\sum$ и осталих идентитета из HSI.

Шести случај је сличан петом случају. □

Сада смо спремни да почнемо успостављати доње границе за величину G-алгебре.

Пропозиција 8.14. *Нека је* **A** *HSI-алгебра. Ако постоји само један цео број (mj.*$2 \approx 1$ *важи у* **A***) онда* **A** *задовољава* $W(x, y)$.

Доказ. Нека је $\sum$ услов $1 \approx 2$. Претпостављајући HSI и $\sum$ имамо $Q(x) \approx 1 + x + x^2 \approx 1 + x + x \approx 1 + 2x \approx 1 + x \approx P(x)$, па из (37) у Леми 8.3 видимо да $HSI \vdash \sum \rightarrow W(x, y)$. Дакле, **A** задовољава $W(x, y)$. □

Пропозиција 8.15. (Дејвидсон) *Нека је* **A** *HSI-алгебра. Ако постоје тачно два цела броја у* **A** *онда* **A** *задовољава* $W(x, y)$.

Доказ. Поделићемо ово на случајеве када је $\sum$ једнакост $3 \approx 1$, и када је $3 \approx 2$.

Случај 1. $\boxed{3 \approx 1}$ Тада је $1 + x \approx (1 + x)^3 \approx 1 + 3x + 3x^2 + x^3 \approx 1 + 2x + x^2$, и одавде имамо $P(x) \cdot Q(x) \approx (1 + x)(1 + x + x^2) \approx 1 + 2x + 2x^2 + x^3 \approx 1 + 3x + 2x^2 \approx (1 + 2x + x^2) + (x + x^2) \approx (1 + x) + (x + x^2) \approx 1 + 2x + x^2 \approx 1 + x \approx P(x)$. Из (38) у Леми 8.13 видимо да **A** задовољава $W(x, y)$.

Случај 2. $\boxed{3 \approx 2}$ Тада је: $R(x)^2 \approx (1 + x^3)^2 \approx (1 + x^2)^2 \approx 1 + 2x^2 + x^4 \approx 1 + 2x^2 + x^2 \approx 1 + 2x^2 \approx 1 + x^2 + x^2 \approx 1 + x^2 + x^4 \approx S(x)$. Из (39) у Леми 8.13 видимо да **A** задовољава $W(x, y)$. □

Последица 8.16. *Ако је* **A** G*-алгебра и* a, b *такви да* $W(a, b)$ *не важи онда су елементи* $1, 2, 3, a, b$ *различити.*

Доказ. Из последња два резултата видимо да морају постојати барем 3 цела броја из **A**, и тиме смо доказали да у Последици 8.5 a, b морају да буду цели бројеви. □

Лема 8.17.

$$HSI \vdash x \approx k + x \rightarrow W(x, y) \text{ за } k \geq 1; \qquad (43)$$

$$HSI \vdash 1 \approx k + x \rightarrow W(x, y) \text{ за } k \geq 0. \qquad (44)$$

Доказ. (43) За $n \in N$, $x^n \approx (k + x)x^{n-1} \approx kx^{n-1} + x^n$; $kx^n \approx x^n + (k - 1)x^n \approx (kx^{n-1} + x^n) + (k - 1)x^n \approx kx^{n-1} + kx^n$. Тако $R(x) \approx 1 + x^3 \approx 1 + (kx^2 + x^3) \approx 1 + (kx + x^2) + x^3 \approx (1 + x)(1 + (k - 1)x + x^2) \approx P(x) \cdot (1 + (k - 1)x + x^2)$; $S(x) \approx 1 + x^2 + x^4 \approx 1 + (kx + x^2) + (kx^3 + x^4) \approx 1 + kx + x^2 + (kx^2 + x^3) + x^4 \approx 1 + kx + (1 + k)x^2 + kx^3 + x^4 \approx (1 + x + x^2)(1 + (k - 1)x + x^2) \approx Q(x) \cdot (1 + (k - 1)x + x^2)$. $W(x, y)$ следи из (41) у Леми 8.13.

(44) $R(x) \approx 1 + x^3 \approx (k + x) + x^3 \approx k + (k + x)x + x^3 \approx k + kx + x^2 + x^3 \approx (1 + x)(k + x^2) \approx P(x) \cdot (k + x^2)$; $S(x) \approx 1 + x^2 + x^4 \approx (k + x) + (k + x)x^2 + x^4 \approx k + x + kx^2 + x^3 + x^4 \approx k + (k + x)x + kx^2 + x^3 + x^4 \approx k + kx + (k + 1)x^2 + x^3 + x^4 \approx (1 + x + x^2)(k + x^2) \approx Q(x) \cdot (k + x^2)$. Дакле, $W(x, y)$ следи из (41) у Леми 8.13. □

Лема 8.18.

$$HSI \vdash x^2 \approx k + x \to W(x,y) \text{ за } k \geq 0; \qquad (45)$$

$$HSI \vdash x \approx k + x^2 \to W(x,y) \text{ за } k \geq 0. \qquad (46)$$

Доказ. (45) $Q(x) \approx 1 + x + x^2 \approx (1 + k) + 2x$; $R(x) \approx 1 + x^3 \approx 1 + x \cdot (k + x) \approx 1 + kx + x^2 \approx 1 + kx + (k + x) \approx (1 + k) + (1 + k)x \approx (1 + k) \cdot (1 + x) \approx (1 + k) \cdot P(x)$; $S(x) \approx 1 + x^2 + x^4 \approx 1 + x^2 + x^2 \cdot (k + x) \approx 1 + (1 + k) \cdot x^2 + x^3 \approx 1 + (1 + k) \cdot x^2 + x \cdot (k + x) \approx 1 + kx + (2 + k)x^2 \approx 1 + kx + (2 + k) \cdot (k + x) \approx (1 + 2k + k^2) + (2 + 2k)x \approx (1 + k) \cdot [(1 + k) + 2x] \approx (1 + k) \cdot Q(x)$. $W(x,y)$ следи из (41) у Леми 8.13.

(46) Случај $k = 0$ покривен је са (45). Претпоставимо $k \geq 1$. $R(x) \approx 1 + x^3 \approx 1 + x^2 \cdot (k + x^2) \approx 1 + kx^2 + x^4 \approx 1 + x^2 + (k - 1) \cdot x^2 + x^4 \approx 1 + (k + x^2) \cdot x + (k - 1) \cdot x^2 + x^4 \approx 1 + kx + (k - 1) \cdot x^2 + x^3 + x^4 \approx (1 + (k - 1)x + x^3) \cdot (1 + x) \approx (1 + (k - 1)x + x^3) \cdot P(x)$; $S(x) \approx 1 + x^2 + x^4 \approx 1 + x \cdot (k + x^2) + x^4 \approx 1 + kx + x^3 + x^4 \approx 1 + kx + x^2 \cdot (k + x^2) + x^4 \approx 1 + kx + kx^2 + 2x^4 \approx 1 + kx + kx^2 + x^4 + x^4 \approx 1 + kx + kx^2 + x^3(k + x^2) + x^4 \approx 1 + kx + kx^2 + kx^3 + x^4 + x^5 \approx (1 + (k - 1)x + x^3) \cdot (1 + x + x^2) \approx (1 + (k - 1)x + x^3) \cdot Q(x)$. $W(x,y)$ следи из (41) у Леми 8.13. □

Лема 8.19.

$$HSI \vdash x^2 \approx k \cdot x \to W(x,y) \text{ за } \quad k \geq 1 \qquad (47)$$

Доказ. $R(x) \approx 1 + x^3 \approx 1 + kx^2 \approx 1 + kx + (k - 1) \cdot x^2 \approx (1 + (k - 1)x) \cdot (1 + x) \approx (1 + (k - 1)x) \cdot P(x)$; $S(x) \approx 1 + x^2 + x^4 \approx 1 + kx + kx^3 \approx 1 + kx + kx^2 + (k - 1)x^3 \approx (1 + (k - 1)x) \cdot (1 + x + x^2) \approx (1 + (k - 1)x) \cdot Q(x)$. $W(x,y)$ следи из (41) у Леми 8.13. □

Лема 8.20. *Ако је* $\sum$ *било који од услова* $p \approx q$, *где* p *означава ред,* q *означава колону, у следећој табели, и појављује се „* $\bullet$ *“ у пољу* (p,q), *онда* $HSI \vdash \Sigma \to W(x,y)$. *Ако стоји „*□*“ у пољу* (p,q) *онда* $HSI \nvdash \Sigma \to W(x,y)$. (Знак „?“ означава да не изводимо никакву последицу.)

	1	2	3	x	$1+x$	$2+x$	$2x$	x^2	$1+x^2$	x^3
1	□	•	•	•	•	•	•	•	•	•
2	•	□	•	•	□	?	?	?	?	?
3	•	•	□	•	?	?	?	?	?	?
x	•	•	•	□	•	•	•	•	•	?
$1+x$	•	□	?	•	□	•	?	•	?	•
$2+x$	•	?	?	•	•	□	?	•	?	?
$2x$	•	?	?	•	?	?	□	•	?	?
x^2	•	?	?	•	•	•	•	□	•	□
$1+x^2$	•	?	?	•	?	?	?	•	□	?
x^3	•	?	?	?	•	?	?	□	?	□

Доказ. Резултате који повезују 1, 2, 3, и x знамо из Последице 8.16. За преостале случајеве показаћемо извођење $W(x,y)$.

Случај $\boxed{1 \approx 1+x}$ $W(x,y)$ следи из (44) у Леми 8.17.

Случај $\boxed{1 \approx 2+x}$ $W(x,y)$ следи из (44) у Леми 8.17.

Случај $\boxed{1 \approx 2x}$ Тада $x|1$. $W(x,y)$ следи из Леме 8.7.

Случај $\boxed{1 \approx x^2}$ Тада $x|1$. $W(x,y)$ следи из Леме 8.7.

Случај $\boxed{1 \approx 1+x^2}$ $P(x) \approx 1+x \approx 1+x^2+x \approx Q(x)$. $W(x,y)$ следи из (37) у Леми 8.13.

Случај $\boxed{1 \approx x^3}$ Тада $x|1$. $W(x,y)$ следи из Леме 8.7.

Случај $\boxed{x \approx 1+x}$ $W(x,y)$ следи из (43) у Леми 8.17.

Случај $\boxed{x \approx 2+x}$ $W(x,y)$ следи из (43) у Леми 8.17.

Случај $\boxed{x \approx 2x}$ $Q(x) \approx 1+x+x^2Q(x) \approx 1+2x+x^2 \approx (1+x)^2 \approx P(x)^2$. $W(x,y)$ следи из (37) у Леми 8.13.

Случај $\boxed{x \approx x^2}$ $W(x,y)$ следи из Леме 8.18.

Случај $\boxed{x \approx 1+x^2}$ $W(x,y)$ следи из (46) у Леми 8.18.

Случај $\boxed{1+x \approx 2+x}$ $Q(x) \approx 1+x+x^2 \approx 1+x(1+x) \approx 1+x(2+x) \approx 1+2x+x^2 \approx (1+x)^2 \approx P(x)^2$. $W(x,y)$ следи из (37) у Леми 8.13.

Случај $\boxed{1+x \approx x^2}$ $W(x,y)$ следи из (45) у Леми 8.18.

Случај $\boxed{2+x\approx x^2}$ $W(x,y)$ следи из (45) у Леми 8.18.

Случај $\boxed{1+x\approx x^3}$ $Q(x)\approx 1+x+x^2\approx x^3+x^2\approx x^2\cdot(1+x)\approx x^2\cdot P(x)$. $W(x,y)$ следи из (37) у Леми 8.13.

Случај $\boxed{2x\approx x^2}$ $W(x,y)$ следи из (47) у Леми 8.19.

Случај $\boxed{x^2\approx 1+x^2}$ $Q(x)\approx 1+x+x^2\approx x+x^2\approx x\cdot(1+x)\approx x\cdot P(x)$. $W(x,y)$ следи из (37) у Леми 8.13. □

Да бисмо успоставили 7 као доњу границу за величину G-алгебри *довољно је узети у обзир алгебре са 3 или 4 цела броја* (јер мањи број целих бројева гарантује да $W(x,y)$ важи; и јер било која G-алгебра има барем два елемента који нису цели бројеви). Прво се враћамо на случај када имамо тачно 3 цела броја, у том случају имамо 4=3 или 4=2.

8.1. Три цела броја, са 4=3

Кроз овај пододељак претпостављамо да је **A** G-алгебра са тачно 3 цела броја, 4=3, и **A**$\not\models W(a,b)$.

Лема 8.21. *Елементи* $1,2,3,a,1+a,a^2$ *су различити. Тако A има величину барем 6.*

Доказ. Показујемо да ако идентификујемо два од наведених шест елемената, онда $W(a,b)$ важи. Четири случаја су презентована испод, а сви остали су последице Леме 8.20.

Случај $\boxed{1+a=2}$ $Q(a)=1+a+a^2=1+a(1+a)=1+a\cdot 2=1+a+a=2+a=1+1+a=1+2=3=4=2\cdot 2=2\cdot(1+a)=2\cdot P(a)$. $W(a,b)$ следи из (37) у Леми 8.13.

Случај $\boxed{1+a=3}$ $Q(a)=1+a+a^2=1+a(1+a)=1+a\cdot 3=1+a+a+a=3+a+a=2+1+a+a=2+3+a=4+a=3+1+a=3+3=4=3=1+a=P(a)$. $W(a,b)$ следи из (37) у Леми 8.13.

Случај $\boxed{a^2=2}$ $S(a)=1+a^2+a^4=1+2+4=1+4=1+a^4=1+a^3=R(a)$. $W(a,b)$ следи из (39) у Леми 8.13.

Случај $\boxed{a^2=3}$ $S(a)=1+a^2+a^4=1+3+9=1+9=1+a^4=1+a^3=R(a)$. $W(a,b)$ следи из (39) у Леми 8.13. □

Лема 8.22. *Скуп* $U=\{1,2,3,a,1+a,a^2\}$ *није потпростор* $\overline{\mathbf{A}}$. *Тако A има барем 7 елемената у себи.*

Доказ. Размотримо елемент a^3. Знамо да a^3није 1 или $1+a$ по Леми 8.20. Следећи аргументи показују да U није затворен за $+,\cdot$.

Случај $\boxed{a^3 = 2}$ $2 = a^3 = a^6 = (a^3)^2 = 2^2 = 4 = 3$. Контрадикција са претпоставком да имамо три цела броја.

Случај $\boxed{a^3 = 3}$ $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^3 = 4 + a^2 = 7 + a^2 = 1 + a^2 + 2a^3 = 1 + a^2 + a^3 + a^3 = 1 + a^2 + a^3 + a^5 = (1 + a^3)(1 + a^2) = R(a) \cdot (1 + a^2)$. $W(a, b)$ следи из (39) у Леми 8.13.

Случај $\boxed{a^3 = a}$ $P(a) = 1 + a = 1 + a^3 = R(a)$. $W(a, b)$ следи из (41) у Леми 8.13.

Дакле, ако је a^3у U онда он мора бити елемент a^2.

Случај $\boxed{a^3 = a^2}$ Показаћемо да ово имплицира да $1 + a^2$ није у U. Прво видимо да је $1 + a^2$ различито од $1, a, a^2$ по Леми 8.20.

Подслучај $\boxed{1 + a^2 = 2}$ $R(a) = 1 + a^3 = 1 + a^2 = 2$; $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^3 = 1 + 2a^2 = 1 + a^2 + a^2 = 2 + a^2 = 1 + (1 + a^2) = 3 = 4 = 2^2 = R(a)^2$. $W(a, b)$ следи из (39) у Леми 8.13.

Подслучај $\boxed{1 + a^2 = 3}$ $R(a) = 1 + a^3 = 1 + a^2 = 3$; $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^3 = 1 + 2a^2 = 1 + a^2 + a^2 = 3 + a^2 = 5 = 3 = R(a)$. $W(a, b)$ следи из (39) у Леми 8.13.

Подслучај $\boxed{1 + a^2 = 1 + a}$ $P(a) = 1 + a = 1 + a^2 = 1 + a^3 = R(a)$; $Q(a) = 1 + a + a^2 = 1 + a^2 + a^2 = 1 + a^2 + a^3 = 1 + a^2 + a^4 = S(a)$. $W(a, b)$ следи из (41) у Леми 8.13. □

8.2. Три цела броја, са 4=2

У овом случају не знамо да ли постоји G-алгебра.

Кроз овај пододељак претпостављамо да је $\mathbf{A}$ G-алгебра са тачно 3 цела броја, 4=2, и $\mathbf{A} \not\models W(a, b)$.

Лема 8.23. *Елементи* $1, 2, 3, a, 1 + a$ *су различити.*

Доказ. С обзиром на Лему 8.20 потребно је да проверимо само да ли је $1 + a$ различито од 2 и 3.

Случај $\boxed{2 = 1 + a}$ $Q(a) = 1 + a + a^2 = 1 + a \cdot (1 + a) = 1 + 2 \cdot a = 1 + a + a = 2 + a = 3$; $P(a) = 1 + a = 2 = 2 \cdot 3 = 2 \cdot Q(a)$. $W(a, b)$ следи из (38) у Леми 8.13.

Случај $\boxed{3 = 1 + a}$ $Q(a) = 1 + a + a^2 = 1 + a \cdot (1 + a) = 1 + 3 \cdot a = 3 + 2 \cdot a = 7 = 3$; $P(a) = 1 + a = 3 = Q(a)$. $W(a, b)$ следи из (38) у Леми 8.13. □

Лема 8.24. $a^2 \neq 2 + a$, *и* a^2 *или* $2 + a$ *не припадају* $\{1, 2, 3, a, 1 + a\}$.

Доказ. $a^2 \neq 2 + a$ по Леми 8.20. Ако $\{a^2, 2 + a\} \subseteq \{1, 2, 3, a, 1 + a\}$ онда из Леме 8.20. a^2 је или 2 или 3; исто тако $2 + a$ је или 2 или 3. Али онда користимо (45) из Пропозиције 8.18 да покажемо да $W(a, b)$ важи. □

Дакле, потребно је показати да додавање елемента a^2 или елемента $2 + a$ у $\{1, 2, 3, a, 1 + a\}$ не даје подалгебру од $\overline{\mathbf{A}}$, одакле се закључује да A има барем 7 елемената.

Лема 8.25. *Скуп* $U = \{1, 2, 3, a, 1 + a, 2 + a\}$ *није подалгебра од* $\overline{\mathbf{A}}$.

Доказ. Претпоставимо да је U подалгебра од **A**. Као што смо приметили изнад, a^2 би могло бити 2 или 3. Под било којом од ових претпоставки показаћемо да $3 + a \notin U$. Прво приметимо да $3 + a \notin \{1, a\}$, по Леми 8.17. Такође $3 + a \notin \{2,3\}$ по (45) из Леме 8.18 (јер $a^2 \in \{2,3\}$). Преостаје да покажемо да $3 + a \notin \{1 + a, 2 + a\}$.

Случај $\boxed{2 = a^2}$

Подслучај $\boxed{3 + a = 1 + a}$ $Q(a) = 1 + a + a^2 = 1 + a + 2 = 3 + a = 1 + a = P(a)$. $W(a, b)$ следи из (37) у Леми 8.13.

Подслучај $\boxed{3 + a = 2 + a}$ $Q(a) = 1 + a + a^2 = 1 + a + 2 = 3 + a = 2 + a = a^2 + a = a(1 + a) = a \cdot P(a)$. $W(a, b)$ следи из (37) у Леми 8.13.

Случај $\boxed{3 = a^2}$

Подслучај $\boxed{3 + a = 1 + a}$ $Q(a) = 1 + a + a^2 = 4 + a = 2 + a$; $P(a) = 1 + a = 3 + a = 7 + a = 4 + a + a^2 = 4 + a(1 + a) = 4 + a(3 + a) = 4 + 3a + a^2 = 2 + 3a + a^2 = (2 + a) \cdot (1 + a) = Q(a) \cdot (1 + a)$. $W(a, b)$ следи из (38) у Леми 8.13.

Подслучај $\boxed{3 + a = 2 + a}$ $Q(a) = 1 + a + a^2 = 1 + a + 3 = 4 + a = 2 + a = 3 + a = a^2 + a = a(1 + a) = a \cdot P(a)$. $W(a, b)$ следи из (37) у Леми 8.13.

Дакле, претпоставка да је U подалгебра од $\overline{\mathbf{A}}$ доводи, кроз све могуће случајеве, до контрадикције. □

Лема 8.26. *Скуп* $U = \{1, 2, 3, a, 1 + a, a^2\}$ *није подалгебра од* **A**.

Доказ. Претпоставимо да је U подалгебра од **A**. У наставку ћемо показати да $W(a, b)$ важи, што даје контрадикцију.

Прво посматрамо елемент $2a$. Из Леме 8.20. знамо да $2a \notin \{1, a, a^2\}$. У следећа два случаја показаћемо да $2a \in \{3,1 + a\}$ доводи до $W(a, b)$.

Случај $\boxed{2a = 3}$ $3 = 2a = 4a = 2 \cdot 2a = 2 \cdot 3 = 2$ Ово је у контрадикцији са претпоставком да имамо три цела броја.

Случај $\boxed{2a = 1 + a}$ $P(a) = 1 + a = 2a;\ Q(a) = 1 + a + a^2 = 2a + a^2 = a + a(1 + a) = a + a(2a) = a(1 + a) + a^2 = a(2a) + a^2 = 3a^2;\ S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + a \cdot 2a = 1 + a \cdot (1 + a) = 1 + a + a^2 = 2a + a^2 = a + a(1 + a) = a + a(2a) = a(1 + a) + a^2 = a(2a) + a^2 = 3a^2.$

Са овим подацима о $P(a)$, $Q(a)$ и $S(a)$ можемо да спроведемо гурај-вуци аргумент да покажемо да $W(a, b)$ важи:

$$(1, P(a), Q(a), R(a), S(a) \to (1, 2a, 3a^2, 1 + a^3, 3a^2)$$
$$\to (a, 2, 3a, 1 + a^3, 3a^2)$$
$$\to (1, 2, 3a, a + a^4, 3a^3)$$
$$\to (1, 2, 3a, a + a^2, 3a^3)$$
$$\to (1, 2, 3a, 2a^2, 3a^3)$$
$$\to (a, 2, 3a, 2a, 3a^2)$$
$$\to (1, 2a, 3a^2, 2a, 3a^2).$$

$W(a, b)$ следи из (34) у Леми 8.12.

Дакле, ако је U подалгебра од $\overline{\mathbf{A}}$, онда је $\boxed{2a = 2}$.

Даље одредићемо могуће вредности за $2 + a$. Видимо из Леме 8.17 да $2 + a \notin \{1, a, 1 + a\}$, и $2 + a \neq a^2$ по Леми 8.18. Следећи случај показује да $2 + a \neq 2$.

Случај $\boxed{2 + a = 2}$ $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + 2a^2 = 1 + (2 + a)a^2 = 1 + 2a^2 + a^3 = 1 + (2 + a)a^2 + a^3 = 1 + 2a^2 + 2a^3 = (1 + a^2 + a^3) \cdot (1 + a^3) = (1 + a^2 + a^3) \cdot R(a)$. $W(a, b)$ следи из (39) у Леми 8.13.

Последично наша претпоставка да је U подалгебра од $\overline{\mathbf{A}}$ форсира $\boxed{2 + a = 3}$.

Коначно погледајмо могуће вредности за $1 + a^2$ и a^3 у U. Из Леме 8.20. видимо да $1 + a^2 \notin \{1, a, a^2\}$.

Случај $\boxed{1 + a^2 = 3}$ $2 = 4 = 1 + (1 + a^2) = 2 + a^2 = 2a + a^2 = a(2 + a) = a \cdot 3 = 2a + a = 2 + a = 3$. Ово је у контрадикцији са претпоставком да имамо три цела броја.

Тако $\boxed{1 + a^2 \in \{2, 1 + a\}}$.

Из Леме 8.20. такође имамо да $a^3 \notin \{1, 1 + a\}$. Следећа два случаја показују да $a^3 \notin \{2, 3\}$.

Случај $\boxed{a^3 = 2}$ $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + 2a^2 = 1 + a^3 \cdot a^2 = 1 + a^5 = 1 + a^3 = R(a)$. $W(a, b)$ следи из (39) у Леми 8.13.

Случај $\boxed{a^3 = 3}$ $S(a) = 1 + a^2 + a^4 = 1 + a^2 + a^2 = 1 + 2a^2 = 1 + 6a^2 = \quad 1 + 6a^6 = 1 + 2 \cdot 3a^3 \cdot a^3 = 1 + 2 \cdot 3 \cdot 3 \cdot 3 = 1 + 2 = 3;$ $R(a) = 1 + a^3 = 1 + 3 = 2 = 2 \cdot 3 = 2 \cdot S(a).$ $W(a, b)$ следи из (40) у Леми 8.13.

Последично наша претпоставка да је U подалгебра од $\overline{\mathbf{A}}$ форсира $\boxed{a^3 \in \{a, a^2\}}$.

Комбиновањем могућности за $1 + a^2$ и a^3 имамо четири случаја за анализу.

Случај $\boxed{1 + a^2 = 2 \text{ и } a^3 = a}$ $R(a) = 1 + a^3 = 1 + a = P(a);$ $S(a) = 1 + a^2 + a^4 = 1 + 2a^2 = 2 + a^2 = 3 = 2 + a = 1 + a^2 + a = Q(a).$ $W(a, b)$ следи из (41) у Леми 8.13.

Случај $\boxed{1 + a^2 = 2 \text{ и } a^3 = a^2}$ $S(a) = 1 + a^2 + a^4 = 2 + a^2 = 3;$ $R(a) = 1 + a^3 = 1 + a^2 = 2 = 2 \cdot 3 = 2 \cdot S(a).$ $W(a, b)$ следи из (40) у Леми 8.13.

Случај $\boxed{1 + a^2 = 1 + a \text{ и } a^3 = a}$ $R(a) = 1 + a^3 = 1 + a = P(a);$ $S(a) = 1 + a^2 + a^4 = 1 + 2a^2 = 1 + a^2 + a = Q(a).$ $W(a, b)$ следи из (41) у Леми 8.13.

Случај $\boxed{1 + a^2 = 1 + a \text{ и } a^3 = a^2}$ $R(a) = 1 + a^3 = 1 + a^2 = 1 + a = P(a);$ $S(a) = 1 + a^2 + a^4 = 1 + 2a^2 = 1 + a + a^2 = Q(a).$ $W(a, b)$ следи из (41) у Леми 8.13.

Дакле, претпоставка да је U подалгебра од $\overline{\mathbf{A}}$ доводи, кроз неколико случајева, до контрадикције. □

Пропозиција 8.27. *G-алгебра* **A** *има барем седам елемената ако* **A** *има тачно три цела броја.*

8.3. Четири цела броја

Кроз овај пододељак претпоставићемо да је **A** G-алгебра са тачно 4 цела броја, и

$\mathbf{A} \nvDash W(a, b)$. Постоје две могућности: или је 3=5 или је 4=5.

Даћемо 15-елементни пример за такву алгебру у последњем одељку, са 4=5. (Пример за 3=5 није познат.)

Лема 8.28. *Пет елемената* $1, 2, 3, 4, a$ *су различити и не формирају подалгебру од* $\overline{\mathbf{A}}$.

Доказ. Ови елементи су различити по Леми 8.2. Претпоставимо да они формирају подалгебру од $\overline{\mathbf{A}}$, и посматрајмо коју вредност $1 + a$ може да има. Из Леме 8.20 следи $1 + a \notin \{1, a\}$.

Случај $\boxed{1 + a = 3}$ $P(a) = 1 + a = 3;$ $Q(a) = 1 + a + a^2 = 1 + a(1 + a) = 1 + 3a = 7.$ $W(a, b)$ следи из (37) у Леми 8.13 (јер $3|7$).

Случај $\boxed{1+a=4}$ $P(a)=1+a=4;\ Q(a)=1+a+a^2=1+a(1+a)=1+4a=13=3$. Опет $W(a,b)$ следи из (38) у Леми 8.13.

Тако остаје једино могућност $\boxed{1+a=2}$. Даље посматрајмо могућности за вредност a^2. Из Леме 8.20 имамо $a^2 \notin \{1,a\}$. Тако $\boxed{a^2 \in \{2,3,4\}}$. Али онда постоји $k \geq 1$ тако да је $k+a=a^2$. Сада применом (45) из Леме 8.18 видимо да $W(a,b)$ важи, што је контрадикција. □

Дефниција 8.29. Нека је U_a подалгебра од $\overline{\mathbf{A}}$ генерисана са a.

Лема 8.30. *Ако* U_a *има шест елемената онда* **A** *има барем 7 елемената.*

Доказ. Претпоставимо да U_a има тачно шест елемената. Како $U=\{1,2,3,4,a\}$ није подалгебра од $\overline{\mathbf{A}}$ следи да бар један од $1+a, 2a, a^2$ није у U; и самим тим је шести елемент у U_a. Ако је шести елемент $2a$ или a^2 онда b не би могао бити у U_a , јер b не може бити цео број или дељив са a по Последици 8.5 и Леми 8.7.

Коначно претпоставимо $U_a=\{1,2,3,4,a,1+a\}$. Из Леме 8.20 знамо $a^2 \notin \{1,a,1+a\}$, и тако $a^2 \in \{2,3,4\}$. Такође из Леме 8.17, $2+a \notin \{a,1+a\}$, па $2+a \in \{1,2,3,4\}$. Такође $a^2 \neq k+a$ за било које ненегативно k из (45) у Леми 8.18, па $\boxed{2+a \in \{3,4\}}$ и $\boxed{a^2 \in \{2,3\}}$. Разликујемо следећа два случаја за четири цела броја.

Случај $\boxed{5=3}$ Тада је $a^2=2$ и $2+a \in \{3,4\}$ из (45) у Леми 8.18, па је $S(a)=1+a^2+a^4=1+2+4=3;\ R(a)=1+a^3=1+2a$. Ако је $2a$ цео број онда $S(a)|R(a)$ па применом (40) из 8.13 добијамо $W(a,b)$. Како $2a$ није цео број, из Леме 8.20 следи $2a=1+a$. Тада је $R(a)=1+a^3=1+2a=2+a \in \{3,4\}$. Па опет $S(a)|R(a)$ одакле следи $W(a,b)$ из (40) у Леми 8.13.

Случај $\boxed{5=4}$ Нека је $a^2=m \in \{2,3,4\}$. Тада је $R(a)=1+a^3=1+ma;\ S(a)=1+a^2+a^4=4=4+4=4a^4+4ma^5=4a^4(1+ma)=4a^4 \cdot R(a)$. Применом (39) из Леме 8.13 добијамо $W(a,b)$. □

Пропозиција 8.31. *Ако постоје тачно четири цела броја у* G*-алгебри* **A** *онда* **A** *садржи најмање седам елемената.*

Доказ. Знамо да постоји бар шест елемената у U_a по Леми 8.28; и ако постоји U_a са тачно шест елемената онда **A** има бар седам елемената по Леми 8.30. □

Теорема 8.32. G*-алгебра мора имати барем седам елемената.*

Доказ. Тврђење следи из Последице 8.5, Последице 8.16, Пропозиције 8.27 и Пропозиције 8.31. □

Проблем 3. Да ли постоји коначна G-алгебра **A** са целим бројевима из **A** која је изоморфна са $N_{a,k}$ за неко $k>1$?

9. Сајмон Лијев 15-елементни пример

Нека је C следећа алгебра.

$+$	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
1	2	3	4	4	2	3	e	3	4	4	4	4	4	4	4
2	3	4	4	4	3	4	3	4	4	4	4	4	4	4	4
3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	2	3	4	4	c	3	c	3	4	4	4	4	4	4	4
c	3	4	4	4	3	4	3	4	4	4	4	4	4	4	4
d	e	3	4	4	c	3	c	3	4	4	4	4	4	4	4
e	3	4	4	4	3	4	3	4	4	4	4	4	4	4	4
f	4	4	4	4	4	4	4	4	4	h	4	4	4	4	4
g	4	4	4	4	4	4	4	4	h	4	4	j	4	4	4
h	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
i	4	4	4	4	4	4	4	4	4	j	4	4	4	4	4
j	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
k	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
b	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

$\cdot$	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
1	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
2	2	4	4	4	c	4	c	4	4	4	4	4	4	4	4
3	3	4	4	4	3	4	3	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	c	3	4	d	c	d	c	4	g	4	4	4	4	4
c	c	4	4	4	c	4	c	4	4	4	4	4	4	4	4
d	d	c	3	4	d	c	d	c	4	g	4	4	4	4	4
e	e	4	4	4	c	4	c	4	4	4	4	4	4	4	4
f	f	4	4	4	4	4	4	4	4	4	4	k	4	4	4
g	g	4	4	4	g	4	g	4	4	4	4	4	4	4	4
h	h	4	4	4	4	4	4	4	4	4	4	4	4	4	4
i	i	4	4	4	4	4	4	4	k	4	4	4	4	4	4
j	j	4	4	4	4	4	4	4	4	4	4	4	4	4	4
k	k	4	4	4	4	4	4	4	4	4	4	4	4	4	4
b	b	4	4	4	4	4	4	4	4	4	4	4	4	4	4

$\uparrow$	1	2	3	4	a	c	d	e	f	g	h	i	j	k	b
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	4	4	f	4	4	4	4	4	4	4	4	4	4
3	3	4	4	4	g	4	4	4	4	4	4	4	4	4	g
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	d	d	d	d	d	d	d	d	d	d	d	d	d	d
c	c	4	4	4	4	4	4	4	4	4	4	4	4	4	4
d	d	d	d	d	d	d	d	d	d	d	d	d	d	d	d
e	e	4	4	4	4	4	4	4	4	4	4	4	4	4	i
f	f	4	4	4	4	4	4	4	4	4	4	4	4	4	4
g	g	4	4	4	4	4	4	4	4	4	4	4	4	4	4
h	h	4	4	4	4	4	4	4	4	4	4	4	4	4	i
i	i	4	4	4	4	4	4	4	4	4	4	4	4	4	4
j	j	4	4	4	f	4	4	4	4	4	4	4	4	4	4
k	k	4	4	4	4	4	4	4	4	4	4	4	4	4	4
b	b	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Биће показано да је **C G**-алгебра, и ова алгебра ће нас довести до доказа Вилкијеве теореме. Ово је најмања позната **G**-алгебра; штавише она је таква да $W(x,y)$ не важи само за пар $(x,y)=(a,b)$.

Нека је $S_1=\{1,a,d\}, S_2=\{2,c,e\}, S=\{2,3,4,c,e,h,j\}, R=C\backslash S_1$. У наставку користимо ознаку $A+B$ за $\{\alpha+\beta: \alpha\in A, \beta\in B\}$, где су $A,B\subseteq C$; и слично за друге две операције.

Лема 9.1. *Нека $\alpha,\beta\in C$ Тада важи*

1. $\alpha+\beta\in S_2$ *акко* $\alpha,\beta\in S_1$.
2. $\alpha+\beta=3$ *акко је један из* S_1 *и други је из* S_2.
3. $\alpha\beta=3$ *акко је један једнак* 3 *и други је из* S_1.
4. $\alpha\beta=g$ *акко је један једнак* g *и други је из* S_1.
5. $RS=\{4\}, R\uparrow S=\{4\}, RC=R, R+R=\{4,h,j\}$.
6. $C+C=S$.

Доказ. Ови искази су очигледни из таблица. □

Дефинишимо $T_1=\{a,d\}$ и $M=\{3,4,c,d,g,k\}$. Приметимо да је $T_1\subset S_1$.

Лема 9.2. *Нека* $\alpha, \beta \in C\backslash\{1\}$ *и* $\gamma \in T_1$. *Тада важи*

1. $\alpha + \beta = c$ *акко* $\alpha, \beta \in T_1$.
2. $\alpha\beta = c$ *акко је један из* T_1 *и други је из* S_2.
3. $\alpha\beta = d$ *акко су оба из* T_1.
4. $\alpha\beta \in T_1$ *акко су оба из* T_1.
5. $(C\backslash\{1\}) \cdot (C\backslash\{1\}) = M$.
6. $\delta \in S_1$ *акко* $\gamma\delta \in T_1 \subset S_1$.
7. $\delta \in S_2$ *акко* $\gamma\delta \in S_2$.

Доказ. Опет, ови искази су очигледни из таблица. □

Теорема 9.3. $\mathbf{C}$ *је HSI-алгебра.*

Доказ. Идентитети (1), (3), (4), (7) и (8) из HSI јасно важе у $\mathbf{C}$. Остали идентитети такође важе. У наставку нека $\alpha, \beta, \gamma \in C$.

Провера за (2). Из Леме 9.1, $\beta + \gamma \in S$. Посматрањем таблице сабирања, видимо да $\alpha + (\beta + \gamma) \in \{3, 4\}$ (заправо, збир било која три елемента мора бити или 3 или 4). Будући да збир два елемента не може бити никад у S_1, на основу Леме 9.1 имамо:

$$\begin{aligned} \alpha + (\beta + \gamma) = 3 \ &\text{ акко } \alpha \in S_1 \text{ и } \beta + \gamma \in S_2 \\ &\text{акко } \alpha, \beta, \gamma \in S_1 \\ &\text{акко } \alpha + \beta \in S_2 \text{ и } \gamma \in S_1 \\ &\text{акко } \alpha + (\beta + \gamma) = 3. \end{aligned}$$

Провера за (5). Приметимо да ако $1 \in \{\alpha, \beta, \gamma\}$ онда је провера готова. Зато претпоставимо да $\alpha, \beta, \gamma \neq 1$. Производ било која два елемента $(\neq 1)$ мора бити у M па је производ три елемента $(\neq 1)$ у $\{3, 4, c, d, g\}$.

$$\begin{aligned} \alpha(\beta\gamma) = 3 \ &\text{ акко } \alpha \in T_1, \beta\gamma = 3 \text{ или } \alpha = 3, \beta\gamma \in T_1 \\ &\text{акко је тачно један од } \alpha, \beta, \gamma \text{ једнак 3, и други су у } T_1 \\ &\text{акко } \alpha(\beta\gamma) = 3 \text{ (по симетрији).} \end{aligned}$$

$\alpha(\beta\gamma) = c$ акко $\alpha \in T_1, \beta\gamma \in S_2$ или $\alpha \in S_2, \beta\gamma \in T_1$

акко је тачно један од α, β, γ у S_2, и други су у T_1

акко $\alpha(\beta\gamma) = c$ (по симетрији).

$\alpha(\beta\gamma) = d$ акко $\alpha, \beta\gamma \in T_1$

акко $\alpha, \beta, \gamma \in T_1$

акко $\alpha(\beta\gamma) = d$ (по симетрији).

$\alpha(\beta\gamma) = g$ акко $\alpha \in T_1, \beta\gamma = g$ или $\alpha = g, \beta\gamma \in T_1$

акко је тачно један α, β, γ једнак g, и други су у T_1

акко $\alpha(\beta\gamma) = g$ (по симетрији).

Провера за (6). Ако је $\alpha = 1$, готови смо. Претпоставимо да је $\alpha \neq 1$.

Ако $\alpha \in R$ онда $\alpha(\beta + \gamma) \in RS = \{4\}$. Сада $(\alpha\beta) + (\alpha\gamma) \in RC + RC = R + R = \{4, h, j\}$. Међутим, само $f + g = g + f = h$ и $g + i = i + g = j$ и не постоји α такво да $\{f, g\} \subseteq \alpha C$ или $\{i, g\} \subseteq \alpha C$ па $(\alpha\beta) + (\alpha\gamma) = 4 = \alpha(\beta + \gamma)$.

Претпоставимо $\alpha \in T_1$. Тада $\alpha(\beta + \gamma) \in T_1 S = \{3, 4, c\}$ и $(\alpha\beta) + (\alpha\gamma) \in T_1 C + T_1 C$. Како је $T_1 C = \{3, 4, a, c, d, g\}$, $T_1 C + T_1 C = \{3, 4, c\}$.

$\alpha(\beta + \gamma) = 3$ акко $\beta + \gamma = 3$

акко тачно један од $\beta, \gamma \in S_1$, и други је у S_2

акко тачно један од $\alpha\beta, \alpha\gamma \in S_1$, и други је у S_2

акко $(\alpha\beta) + (\alpha\gamma) = 3$.

$\alpha(\beta + \gamma) = c$ акко $\beta + \gamma \in S_2$

акко $\beta, \gamma \in S_1$

акко $\alpha\beta, \alpha\gamma \in T_1$

акко $(\alpha\beta) + (\alpha\gamma) = c$.

Провера за (9). Ако је $\alpha = 1$, готови смо. Претпоставимо да је $\alpha \neq 1$.

За $\alpha \in R$, $\alpha \uparrow S = \{4\}$ па $\alpha^{\beta+\gamma} = 4$. Такође $\left(\alpha^{\beta}\right)(\alpha^{\gamma}) = 4$.

За $\alpha \in T_1$, $\alpha^{\beta+\gamma} \in \alpha \uparrow S = \{d\}$. Такође $\alpha^{\beta}, \alpha^{\gamma} \in \alpha \uparrow C = T_1$ па $\left(\alpha^{\beta}\right)(\alpha^{\gamma}) \in T_1 T_1 = \{d\}$; па (9) важи.

Провера за (10). Ако $1 \in \{\alpha, \beta, \gamma\}$, готови смо. Претпоставимо да $\alpha, \beta, \gamma \neq 1$.

Тада $(\alpha\beta)^{\gamma} \in M \uparrow (C\backslash\{1\}) = \{4, d, g\}$. И $(\alpha^{\gamma})(\beta^{\gamma}) \in \{4, d, f, g, i\}\{4, d, f, g, i\} = \{4, d, g, k\}$; међутим, k није достижно јер не постоји γ такво да $\{\alpha^{\gamma}, \beta^{\gamma}\} = \{f, i\}$, па $(\alpha^{\gamma})(\beta^{\gamma}) \in \{4, d, g\}$.

$(\alpha\beta)^{\gamma} = d$ акко $\alpha\beta \in T_1$

акко $\alpha, \beta \in T_1$

акко $\alpha^{\gamma}, \beta^{\gamma} = d$

акко $(\alpha^{\gamma})(\beta^{\gamma}) = d$.

$(\alpha\beta)^{\gamma} = g$ акко $\alpha\beta = 3$ и $\gamma \in \{\alpha, \beta\}$

акко је један од $\alpha, \beta = 3$, други је у T_1, и $\gamma \in a, b$

акко један од $\alpha^{\gamma}, \beta^{\gamma} = d$ и други је једнак g

акко $(\alpha^{\gamma})(\beta^{\gamma}) = g$.

Провера за (11). Ако $1 \in \{\alpha, \beta, \gamma\}$, готови смо. Претпоставимо да $\alpha, \beta, \gamma \neq 1$.

Тада $(\alpha^{\beta})^{\gamma} \in \{4, d\}$; и $\alpha^{\beta\gamma} \in \{4, d\}$.

$(\alpha^{\beta})^{\gamma} = d$ акко $\alpha^{\beta} \in T_1$

акко $\alpha \in T_1$

акко $\alpha^{\beta\gamma} = d$.

Теорема 9.4. **C** *је* G*-алгебра.*

Доказ. Посматрајмо $W(a,b)$. $P(a) = 1 + a = 2$, $Q(a) = 1 + a + a^2 = 3$, $R(a) = 1 + a^3 = e$, и $S(a) = 1 + a^2 + a^4 = 3$. Лева страна једнакости, LHS за $W(a,b)$ је тада:

$$\begin{aligned}\text{LHS} &= (2^a + 3^a)^b \cdot (e^b + 3^b)^a \\ &= (f + g)^b \cdot (i + g)^a \\ &= h^b \cdot j^a \\ &= i \cdot f \\ &= k.\end{aligned}$$

Десна страна једнакости је:

$$\begin{aligned}R\text{HS} &= (2^b + 3^b)^a \cdot (e^a + 3^a)^b \\ &= (4 + g)^a \cdot (4 + g)^b \\ &= 4^a \cdot 4^b \\ &= 4 \cdot 4 \\ &= 4.\end{aligned}$$

Дакле, $W(x,y)$ не важи у HSI-алгебри **C**, па је **C** заиста G-алгебра. □

Наредна табела показује прогрес у трагању за малим G-алгебрама.

Gurevič	59 елемената		1985
Gurevič	33 елемената		≤ 1990
Buriss	28 елемената		1988
Buriss	16 елемената		1990
Lee	15 елемената		1991
Buriss Lee	15 елемената	≥ 7	1992
Jackson	14 елемената	≥ 8	1996
Buriss Yeats	13 елемената		2001
Buriss Lee	12 елемената		2001

10. Закључак

У називу теме овог мастер рада се, између осталог, налази реч "средњошколска", и многи би помислили да ћемо се бавити средњошколском математиком и да ту нема шта претерано да се каже. Међутим, на Тарскијево питање да ли је HSI основа за све идентитете из **N** дат је, као што је већ речено, негативан одговор од стране Вилкија 1980. године. Због тога су Тарскијев проблем и Вилкијево решење покренули разне, још увек актуелне правце у истраживању HSI-алгебри.

У раду су презентовани најважнији резултати о HSI-алгебрама, уз истицање занимљивих веза ових алгебарских структура са теоријом бројева, теоријом полинома, неким логичким системима и теоријом доказа. Посебно је била посвећена пажња конструкцији тзв. малих (коначних) HSI-алгебри. Наведено је и неколико проблема који су и даље отворени. За веровати је, због све бржег напредовања на пољу информационих технологија, да ће се у блиској будућности ти проблеми решити.

11. Литература

1. S. Burris and S.Lee, *Tarski's high school identities,* to appear in the Amer. Math. Monthly.
2. S.Burris and H. P. Sankappanavar, *A Course in Universal Algebra,* Grad. Texts in Math.**78**, Springer-Verlag, 1981.
3. J. L. Davidson and J. O. Shallit, *Continued fractions for some alternating series*, Monatshefte Math. **111**, 1991.
4. R. Gurevič, *Equational theory of positive numbers with exponentiation*, Proc. Amer. Math. Soc. **94**, 1985.
5. R. Gurevič, *Transcendental numbers and eventual dominance of exponential functions*, Bull. London Math. Soc. **18**, 1986.
6. R. Gurevič, *Equational theory of positive numbers with exponentiation is not finitely axiomatizable,* Ann. Pure and Applied Logic **49**, 1990
7. G. H. Hardy, *Orders of Infinity, the 'Infinitar' Calcul of Paul Du Bois-Reymond.* Cambridge University Press. [first ed. 1921] 2nd ed. 1954.
8. C. W. Henson and L. A. Rubel, *Some applications of Nevanlinna theory to mathematical logic*: *identities of exponential functions*, Trans. Amer. Math. Soc. **282**, 1984
9. A. Macintyre, *The laws of Exponentiation*, Springer Lecture Notes in Math. **890**, 1981.
10. C. Martin, *Equational theories of natural numbers and transfinite ordinals*, Ph.D. Thesis, U. Cal. Berkeley, 1973.
11. G. McNulty, *An equational logic sampler*, Rewriting Techniques and Applications, RTA-89 Proceedings, ed N. Dershowitz, Springer Lecture Notes in Computer Science **335**, 1989.
12. D. Richardson, *Solution of the identity problem for integral exponential function*, Zeitschr. f. Math. Logik u. Grund. d. Math. **15**, 1969.
13. D. Richardson, *The simple exponential constant problem*, Zeitschr. f. math. Logik u. Grund. d. Math. **17**, 1971.
14. J. J. Sylvester, *On a point in the theory of vulgar fractions*, Amer. J. Math. **3**, 1880.
15. J. J. Sylvester, *Postscript to a note on a point in vulgar fractions*, Amer. J. Math. **3**, 1880.
16. A. J. Wilkie, *On exponentiation – a solution to Tarski's high school algebra problem*, preprint, Oxford University, 1980.
17. B. Šešelja i A. Tepavčević, *Bulove algebre i funkcije*, Prirodno-matematički fakultet, Departman za matematiku i informatiku u Novom Sadu, 2014.
18. R. Tošić, V. Vukoslavčević, *Elementi teorije brojeva*, Alef, Novi Sad, 1995.
19. G. Vojvodić, *Predavanja iz matematičke logike*, Prirodno-matematički fakultet u Novom Sadu, 2007.
20. G. Vojvodić, *Predavanja iz algebre*, Prirodno-matematički fakultet u Novom Sadu, 2007.