(Полу)групе, алгоритми, језици и облици: један век бескрајне игре речима

Игор Долинка

Департман за математику и информатику, ПМФ, Универзитет у Новом Саду

Приступно предавање

(уз клавирски рецитал Доротеје Ћирић)

Огранак САНУ у Новом Саду, 16. март 2022.

I. (Полу)групе: математичка разгледница

Полугрупе, инверзне полугрупе, групе

Полугрупа – $(S, \bullet)$, операција $\bullet$ је асоцијативна:

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

Моноид – Полугрупа са јединицом: $1 \bullet x = x \bullet 1 = x$.

☞ типичан пример: $\mathbb{T}_X$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 5 & 2 & 1 \end{pmatrix}$$

Полугрупе, инверзне полугрупе, групе

Група – Моноид у којем сваки елемент има инверз:

$$x \bullet x^{-1} = x^{-1} \bullet x = 1.$$

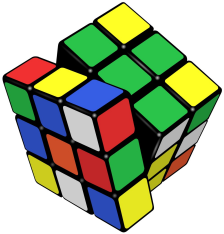
- ☞ типичан пример: симетрична група $\mathbb{S}_X$

Инверзна полугрупа – Полугрупа у којој сваки елемент има јединствен "слаб" инверз:

$$x \bullet x^{-1} \bullet x = x^{-1} \bullet x \bullet x^{-1} = x.$$

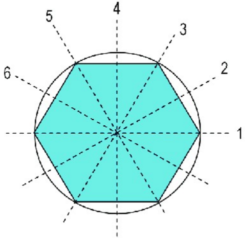
- групе моделирају реверзибилне процесе и појаве у природи, друштву,...
- полугрупе моделирају иреверзибилне процесе

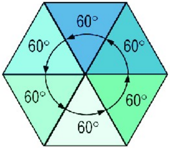
Група Рубикове коцке (наравно...!)



- састоји се од свих коначних низова потеза [...]
- садржана у $\mathbb{S}_{48}$
- има 43,252,003,274,489,856,000 елемената
- свака "легална" позиција се може решити у ≤ 26 потеза

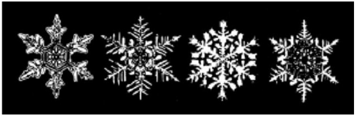
Групе су мера симетрије



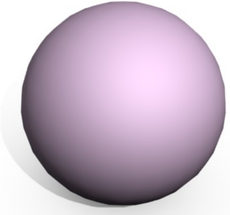


Група симетрија правилног n-тоугла – диједарска група D_n:

- n ротација,
- n осних симетрија.



Групе су мера симетрије



Група симетрија сфере – ортогонална група $O(3)$

- ☞ Садржи групу 3D ротација $SO(3)$, од огромног значаја у физици елементарних честица

Групе и геометрија: Феликс Клајн

Феликс Клајн (1849-1925),
немачки математичар

Клајново виђење геометријских система:
класификација по групама симетрија

Ерлангенски програм (1872):

геометрија = изучавање својстава простора инваријантних у односу на групе трансформација

Смрт у двобоју: групе и једначине

Једначина

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

је решива радикалима (lat. *radix* = корен) ако се њена решења могу изразити преко елемената поља коефицијената и симбола $+, -, \cdot, \div, \sqrt[n]{}$.

Главни пример:

$$ax^2 + bx + c = 0 \quad \Rightarrow \quad x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Смрт у двобоју: групе и једначине

Да ли свака једначина има решење радикалима?

- $n = 3$ ✓ (1545 – Кардано, Тартаља, инквизиција,...)
- $n = 4$ ✓ (Ферари (Карданов зет))
- $n = 5$ ✗ (1824 – Н.Х.Абел (1802-1829))

Због чега је то тако? Наравно, због групa.

Еварист Галоа (25. окт. 1811 - 31. мај 1832), француски математичар и револуционар

Први употребио термин група.

Савремена теорија једначина води порекло из писма које је написао пријатељу током ноћи пред фатални двобој.

Пример: Једначина $x^5 - 6x + 3 = 0$ није решива радикалима.

Групе и топологија: фундаменталне групе

Хомотопија кривих:

Групе и топологија: фундаменталне групе

Хомотопија кривих:

Групе и топологија: фундаменталне групе

Хомотопија кривих:

Групе и топологија: фундаменталне групе

Хомотопија кривих:

Групе и топологија: фундаменталне групе

Нехомотопне криве:

Групе и топологија: фундаменталне групе

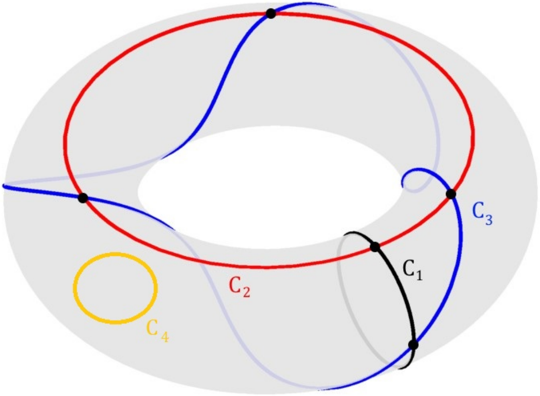
Нехомотопне криве:

Групе и топологија: фундаменталне групе

Нехомотопне криве:

Групе и топологија: фундаменталне групе

А сад, озбиљно:



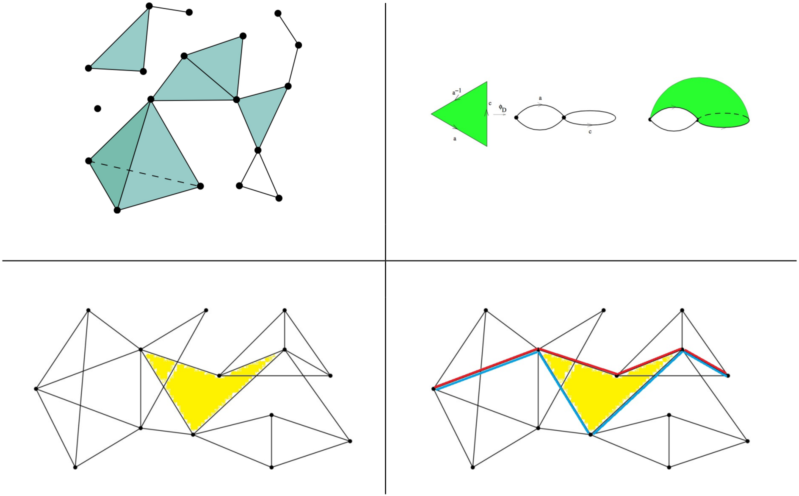
Групе и топологија: фундаменталне групе

Фундаментална група (Анри Поенкаре, 1895):

☞ група коју чине класе хомотопних затворених кривих (у датој тачки) у односу на операцију "лепљења"

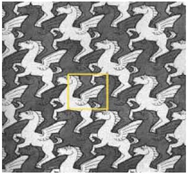
Описује "облик", "конфигурацију терена" тополошког простора.

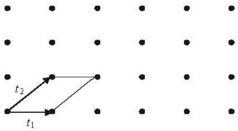
Комплекси

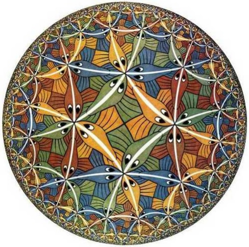


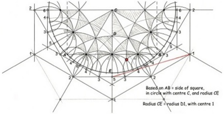
Морис Ешер

Морис К. Ешер (1898-1972) – холандски графички уметник чија су дела била инспирисана математиком









Морис Ешер

М. К. Ешер: Ослобођење (1955)

II. Речи, језици, презентације

Речи, формални језици, слободни моноиди

Реч (над алфабетом X) $=$ коначан низ слова из X

X^* $=$ све речи над X (укључујући и λ)

Језик: $L \subseteq X^*$

Слободни моноид X^*:

$$\text{игор} \cdot \text{долинка} = \text{игордолинка}$$

Слободна полугрупа $X^+ = X^* \setminus \{\lambda\}$:

Редуковане речи и слободне групе

Сада посматрајмо речи из $(X \cup X^{-1})^*$.

У "амбијенту" група желимо:

$$abcc^{-1}b^{-1}da^{-1}ab^{-1} = adb^{-1} = abb^{-1}db^{-1}$$

Редукција речи: $\mathrm{red}(abcc^{-1}b^{-1}da^{-1}ab^{-1}) = adb^{-1}$

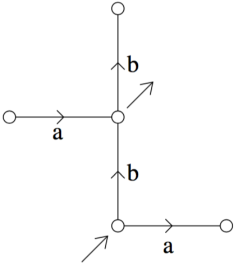
Редукована реч: $\mathrm{red}(w) = w$

Слободна група $FG(X)$: $u \cdot v = \mathrm{red}(uv)$

Пример: $\mathrm{red}(acb^{-1} \cdot bc^{-1}d^{-1}) = ad^{-1}$

Слободне инверзни моноиди/полугрупе

$FIM(X)$ = Мунова дрвета над X



Горње дрво показује да је:

$$aa^{-1}bb^{-1}ba^{-1}abb^{-1} = bbb^{-1}a^{-1}ab^{-1}aa^{-1}b.$$

Групне и полугрупне презентације

$$G = \mathrm{Gp}\langle X \mid w_1 = 1, w_2 = 1, \ldots \rangle$$

значи да је $G \cong FG(X)/N$,

$N =$ нормална подгрупа $FG(X)$ генерисана са $w_1, w_2, \ldots$

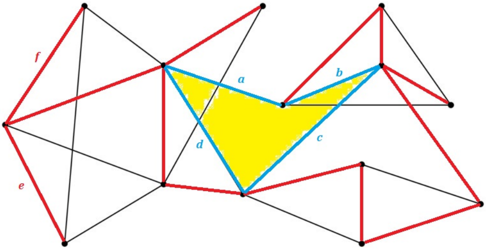
Пример: $\mathbb{Z}_8 = \mathrm{Gp}\langle x \mid x^8 = 1 \rangle$

$$S = \mathrm{Sgp}\langle X \mid u_1 = v_1, u_2 = v_2, \ldots \rangle$$

значи да је $G \cong X^+/\rho$,

$\rho =$ конгруенција X^+ генерисана са $(u_1, v_1), (u_2, v_2), \ldots$

Презентација фундаменталне групе



X = гране графа ("костур", 1-дим. ћелије)

Релације:

- $e = 1, f = 1, \ldots$
- $abcd = 1, \ldots$

III. Алгоритми и неодлучивост

Појам алгоритма

Сродни појмови:

- поступак
- процедура
- рутина
- рецепт

5 основних својстава алгоритама (Доналд Кнут):

- улаз
- излаз
- коначност
- одређеност
- ефективност

Ћитап о рачуну

Мудамед ибн-Муса ал-Хорезми (780-850)

арапски научник персијског порекла

- први употребио термин алгебра (ал-џабр)
- "Китаб ал-хисаб ал-хинди": описује вештину рачунања индијским (данас: арапским) цифрама = алгоритам

"Ми морамо сазнати, ми ћемо сазнати"

Давид Хилберт (1862-1943)

немачки математичар

- 23 проблема за XX век (1900)
- формалистички програм
- "доказивач теорема"

Курт Гедел

Курт Гедел (1906-1978)

чешко-аустријско-амерички логичар, математичар и филозоф

- ☞ свака "иоле сложенија" математичка формална теорија је некомплетна
- ☞ постоје алгоритамски нерешиви (неодлучиви) проблеми

"Ово тврђење није теорема теорије природних бројева."

Алан Тјуринг и његове машине

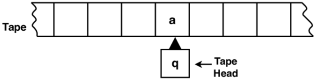
Алан Тјуринг (1912-1954)

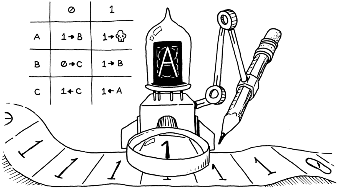
британски математичар, логичар и биолог

☞ први информатичар/програмер у историји

☞ научник најзаслужнији за пораз нациста

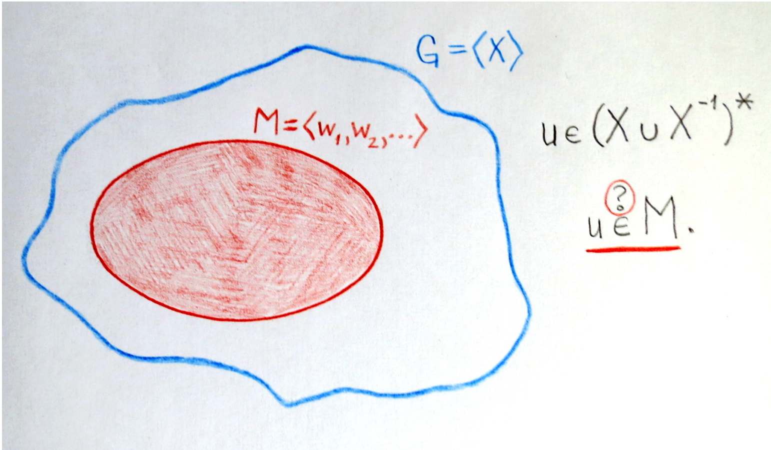
☞ формализовао појам алгоритма
(уз Гедела и Черча)





	⊘	1
A	1→B	1→
B	⊘→C	1→B
C	1←C	1←A

(Не)одлучивост



Проблем речи

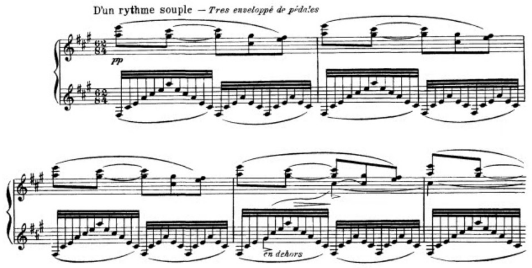
$G = \mathrm{Gp}\langle X \mid w_1 = 1, w_2 = 1, \ldots \rangle$

УЛАЗ: $w \in (X \cup X^{-1})^*$
ИЗЛАЗ: Да ли у G важи $w = 1$?

$S = \mathrm{Sgp}\langle X \mid u_1 = v_1, u_2 = v_2, \ldots \rangle$

УЛАЗ: $u, v \in X^*$
ИЗЛАЗ: Да ли у S важи $u = v$?

IV. 1-релаторске структуре



1-релаторске групе

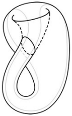
Примери:

- $\mathbb{Z} \times \mathbb{Z} = \mathrm{Gp}\langle a, b \mid ab = ba \rangle = \mathrm{Gp}\langle a, b \mid a^{-1}b^{-1}ab = 1 \rangle$
- фундаменталне групе оријентабилних површи

$$\mathrm{Gp}\langle a_1, b_1, a_2, b_2, \ldots, a_n, b_n \mid [a_1, b_1][a_2, b_2] \ldots [a_n, b_n] = 1 \rangle$$

- фундаменталне групе неоријентабилних површи

$$\mathrm{Gp}\langle a_1, \ldots, a_n \mid a_1^2 \ldots a_n^2 = 1 \rangle$$



- групе Баумслаг-Солитара $B(m, n) = \mathrm{Gp}\langle a, b \mid b^{-1}a^m ba^{-n} = 1 \rangle$

Проблем речи

Теорема (В.Магнус, 1932): Све 1-релаторске групе имају алгоритамски решив проблем речи.

“Da sind Sie also blind gegangen!”

Макс Ден (Магнусов ментор)

Отворен проблем (још увек! – 16.3.2022.):
Да ли сви 1-релаторски моноиди имају алгоритамски решив проблем речи?

С.И.Адјан (1966): да, у неким случајевима –

- специјални моноиди $w = 1$
- $u = v$, где u, v имају различита почетна и завршна слова
- са Оганесјаном (1987): све се своди на $aub = avc$

Улога инверзних моноида

Иванов, Марголис, Микин (2001):

Сви $\mathrm{Inv}\langle X \mid w = 1\rangle$ имају одлучив ПР

$$\Longrightarrow$$

позитивно решење Адјановог проблема

Разлог: $\mathrm{Mon}\langle X \mid aub = avc\rangle \hookrightarrow \mathrm{Inv}\langle X \mid aubc^{-1}v^{-1}a^{-1} = 1\rangle$

	$\mathrm{Gp}\langle X \mid w = 1\rangle$	$\mathrm{Mon}\langle X \mid w = 1\rangle$	$\mathrm{Inv}\langle X \mid w = 1\rangle$
одлучив ПР	✓	✓	? ✗
	(Магнус, 1932)	(Адјан, 1966)	(Греј, 2020)


Проблем префиксног моноида

Иванов, Марголис, Микин (2001), клапа 2:

$\mathrm{Inv}\langle X \mid w = 1\rangle$ E-унитаран (= "пристојан") онда је његов ПР

$$=$$

проблем префиксног моноида за групу $\mathrm{Gp}\langle X \mid w = 1\rangle$

Задатак:

Изучавати проблем префиксног моноида за 1-релаторске групе.

I.Dolinka, R.D.Gray, New results on the prefix membership problem for one-relator groups, *Transactions of the American Mathematical Society* **374** (2021), 4309-4358.

Презентације 1-релаторских група са одлучивим ППМ

- $\mathrm{Gp}\langle a, b, x, y \mid (axb)(ayb)(ayb)(axb)(ayb)(axb) = 1\rangle$
- $\mathrm{Gp}\langle a, b, c, d \mid (abcd)(acd)(ad)(abbcd)(acd) = 1\rangle$
  (О'Хер група – Марголис, Микин, чикашки аеродром, 1987)
- $\mathrm{Gp}\langle a, b, c, d \mid (abab)(cdcd)(abab)(cdcd)(cdcd)(abab) = 1\rangle$
- $\mathrm{Gp}\langle a_1, \ldots, a_n, b_1, \ldots, b_n \mid [a_1, b_1] \ldots [a_n, b_n] = 1\rangle$
  (фунд. групе оријентабилних површи)
- $\mathrm{Gp}\langle a_1, \ldots, a_n \mid a_1^2 \ldots a_n^2 = 1\rangle$
  (фунд. групе неоријентабилних површи)
- $\mathrm{Gp}\langle a, b, c, t \mid t^{-1}bcbt^{-8}bbct^6ct^3at^{-3}bt^3at^{-3}ct^2cta = 1\rangle$
- $B(m, n) = \mathrm{Gp}\langle a, b \mid b^{-1}a^mba^{-n} = 1\rangle$
- ...

V. $\mathsf{IG}(\mathcal{E})$: скривена геометрија полугрупа

Идемпотенти

Идемпотенти полугрупе S: $e^2 = e$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 1 & 3 \end{pmatrix}$$

$$\begin{bmatrix} 3 & -6 \\ 1 & -2 \end{bmatrix}^2 = \begin{bmatrix} 3 & -6 \\ 1 & -2 \end{bmatrix}$$

Биуређен скуп: парцијална алгебра $\mathcal{E}_S = (E(S), \cdot)$ где је $\cdot$ ограничено на основне парове,

$$\{ef, fe\} \cap \{e, f\} \neq \varnothing.$$

$\mathsf{IG}(\mathcal{E})$

Слободна идемпотентно генерисана полугрупа над $\mathcal{E}$:

$$\mathsf{IG}(\mathcal{E}) = \mathsf{Sgp}\langle X_E \mid x_e x_f = x_{ef} \text{ где је } \{e, f\} \text{ основни пар у } \mathcal{E}\rangle$$

(К.С.С.Намбурипад, 80-тих)

Главни проблеми:

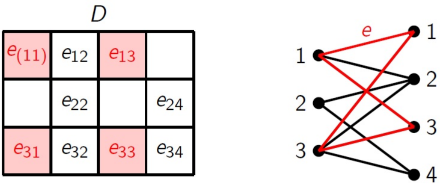
- одређивање максималних подгрупа
- одлучивост проблема речи

Хипотеза (из 1980-тих):
Максималне подгрупе су увек слободне групе.

Максималне подгрупе (1)

Бритенхам, Марголис, Микин (2009): Хипотеза није тачна!

Максималне подгрупе = фундаменталне групе Грејем-Хоутоновог 2-комплекса $GH(\mathcal{E})$



Греј, Рушкуц (2012): Заправо, за сваку групу G посотји полугрупа S тако да се G јавља као максимална подгрупа у $\mathrm{IG}(\mathcal{E}_S)$

ИгД, Рушкуц (2013): Довољно је узети траке (идемпотентне полугрупе) S

Максималне подгрупе (2)

Израчунате максималне подгрупе у $\mathrm{IG}(\mathcal{E}_S)$:

S	макс. подгр.	ко и кад
$\mathbb{T}_n$	$\mathbb{S}_r$ за $r \leq n-2$	Греј, Рушкуц (2012, PLMS)
$\mathbb{PT}_n$	$\mathbb{S}_r$ за $r \leq n-2$	ИгД (2013, Comm.Alg.)
$\mathcal{M}_n(\mathbb{F})$	$\mathrm{GL}_r(\mathbb{F})$ за $r < n/3$	ИгД, Греј (2014, TrAMS)
$\mathrm{End}(F_n(G))$	$G \wr \mathbb{S}_r$ за $r \leq n-2$	ИгД, Гулд, Јанг (2015, J.Alg.)

Проблем речи за $\mathsf{IG}(\mathcal{E})$

Општа теорија у вези са проблемом речи за $\mathsf{IG}(\mathcal{E})$ развијена је у радовима:

- I.Dolinka (2021, *Israel Journal of Mathematics*)
- I.Dolinka, V.Gould, D.Yang (2019, *Advances in Mathematics*)
- I.Dolinka, R.D.Gray, N.Ruškuc (2017, *Proceedings of the London Mathematical Society*)

Проблем речи за $\mathsf{IG}(\mathcal{E})$

=

алгоритамски проблем CSP типа над подгрупама производа максималних подгрупа (које такође настају на геометријско-тополошки начин)

- ☞ постоји коначна полугрупа S тако да је ПР у $\mathsf{IG}(\mathcal{E}_S)$ неодлучив, иако је ПР одлучив у свим подгрупама
- ☞ ПР у $\mathsf{IG}(\mathcal{E}_{\mathbb{T}_n})$ је одлучив – експлицитни алгоритам: ИгД (2022)

Voici mon secret. Il est très simple: on ne voit bien qu'avec le cœur. L'essentiel est invisible pour les yeux. [...] C'est le temps que tu as perdu pour ta rose qui fait ta rose si importante.

— A. de Saint-Exupéry, *Le petit prince*

Хвала на пажњи!