

θβλιζε 2023/2024

Koło Naukowe Matematyków UAM

Wydawca: Koło Naukowe Matematyków UAM

Kontakt: konferencja@oblicze.edu.pl

Skład tekstu: Zuzanna Rygiewicz

Korekta: Zuzanna Rygiewicz

Projekt okładki: Adrianna Smolińska

Druk: Drukarnia cyfrowa Poznań - Axlo

Odpowiedzialność za treść tekstów ponoszą ich autorzy.

ISBN: 978-83-946301-1-9

<https://oblicze.edu.pl/>

Poznań, kwiecień 2025

Spis treści

Wstęp	5
1 Marcin Ból <i>Zabawy z iksami i igrekami, czyli o tym, że pierścienie spełniające tożsamość $x^3 = x$ są przemienne</i>	17
2 Krzysztof Caban <i>Atrakcyjność w zwartości, czyli jak dużo jest atraktorów IFS-ów</i>	25
3 Jakub Chmiel <i>Permanent - krótko o złym bracie-bliźniaku wyznacznika</i>	33
4 Aleksandra Choina <i>Matematyka w codziennym życiu. Propozycja lekcji i zadań.</i>	43
5 Patryk Doniec <i>Logarytmy dyskretne: Od podstaw do zastosowań</i>	51
6 Paweł Drzyzga <i>Maszyna uczenia ekstremalnego i pseudoodwrotności Moore'a-Penrose'a</i>	61
7 Łukasz Gorczyca <i>Wyznaczanie obrazu numerycznego macierzy</i>	73
8 Paulina Ewa Hennig <i>Rzut oka na klasyfikację szeregów</i>	83

9	Bartosz Kamiński <i>Drogi Banachu, a można tak ogólniej?</i>	93
10	Damian Kayzer <i>Wiązka główna z powiązaniem głównym, na przykładzie sfery zanurzonej w \mathbb{R}^3</i>	101
11	Paweł Przybyła <i>Topologia grup Liego i rozwłóknienie Hopfa</i>	109
12	Zuzanna Rygiewicz <i>RK relevance logic : lattice of extensions</i>	119
13	Adrianna Smolińska <i>Aerodynamika lotu samolotu</i>	129
14	Tomasz Sobczak <i>k-Kontaktowe układy Liego</i>	141
15	Julia Ścisłowska <i>Topologiczne czary w n-wymiarowym świecie</i>	151

Podsumowanie

W dniach 5 – 7 maja 2023 oraz 10 – 12 maja 2024 roku na Wydziale Matematyki i Informatyki UAM odbyły się X i XI edycja Ogólnopolskiej Konferencji Studentów Matematyki $\theta\beta licZ\epsilon$, której głównymi organizatorami byli Studenci należący do Koła Naukowego Matematyków UAM. $\theta\beta licZ\epsilon$ jest jedną z największych studenckich konferencji matematycznych w Polsce i jedyną taką poznańską inicjatywą matematyczną. W każdej edycji udział wzięło ponad 120 uczestników, w sumie wygłoszono ponad 100 referatów i przedstawiono ponad 40 posterów naukowych.



Nagrodzeni

W roku 2023 w gronie laureatów konkursu za najlepszy referat, znaleźli się:

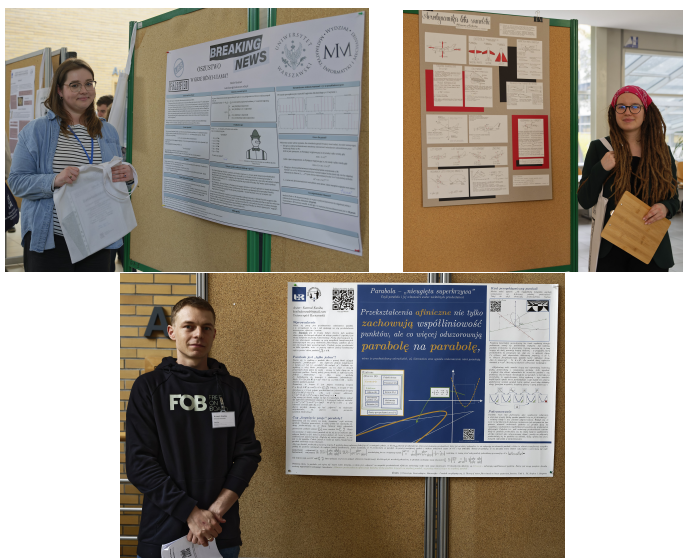
- Miejsce *I* – Marek Jendernalik – „Fraktale Łaciate”,
- Miejsce *II* – Jakub Szmelter – „Krótkie Wprowadzenie w temat grup automorfizmów zwartych powierzchni Riemana”,
- Miejsce *III* – Alan Żeromski – „Niemożliwy remis – o grze w Hex i co na to Twierdzenie Brouwera?”.



Dodatkowe wyróżnienia otrzymali: Bartosz Szachniewicz, Damian Kayzer, Krzysztof Caban, Jakub Kamiński, Mikołaj Roman.

Natomiast nagrody w konkursie posterów trafiły do:

- Miejsce *I* – Nicole Meisner – „Oszustwo przy grze w 20 pytań [ZOBACZ DOWODY]”,
- Miejsce *II* – Adrianna Smolińska – „Aerodynamika lotu samolotu (wstęp)”,
- Miejsce *III* – Konrad Kosiba – „Parabola – „nieugięta krzywa”, czyli o własnościach tej stożkowej wobec pewnych transformacji”.



Dodatkowo wyróżnienie otrzymał Krzysztof Andruch za poster „Najważniejsze odkrycia Dirichleta”.

Podczas *XI* konferencji wprowadzono nowe zasady wyróżniania w konkursie referatów, dodając kategorie. Laureatami zostali:

- Miejsce *I* – Bartosz Kamiński „Drogi Banachu, a można tak ogólniej? Czyli topologiczne kontrakcje i uogólnione twierdzenie Banacha”,
- Miejsce *II* – Krzysztof Caban „Atrakcyjność w zwartości, czyli jak dużo jest atraktorów IFS-ów”,
- Miejsce *III* – Mateusz Zdunek „Kombinatoryczne ciągi Lefschetza i ich związek z punktami periodycznymi odwzorowań”.

Wyróżniono Patryka Topora za „O naturze zbioru $\text{Fix}(f)$ w klasie homotopii” oraz Igora Hołowacza z „Modele agentowe, czyli co wspólnego ma socjologia z fizyką?”.



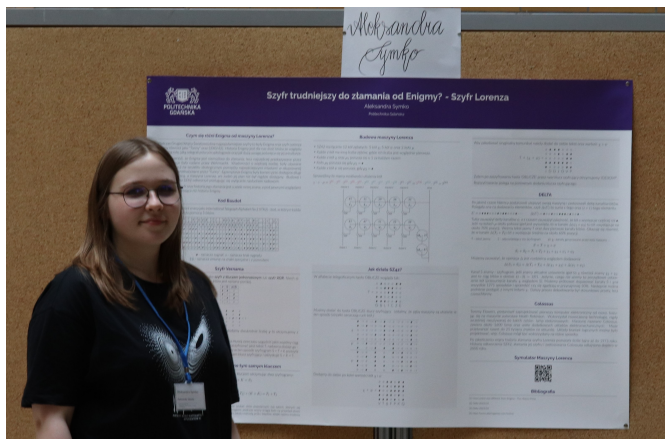
Natomiast w poszczególnych kategoriach wyróżnienia otrzymali:

- **BOGACTWO PRZEKAZANEJ WIEDZY** – Piotr Rysiński „Symetrie twojej ulubionej różności”,
- **PŁYNNA I WCIĄGAJĄCA NARRACJA** – Damian Kayzer „Łańcuchy czworościanów – zabawny problem z Nowej Szkockiej Księgi”,
- **ZROZUMIAŁOŚĆ PRZEDSTAWIONYCH KONCEPTÓW** – Paulina Ewa Henning „Rzut oka na klasyfikację szeregów”,
- **DOBRY KONTAKT Z WIDOWNIĄ** – Leonard Sikorski „Wszystkie fizyczne realizowalne operacje mam w czterech literach”,
- **TEMPO DOSTOSOWANE DO CZASU TRWANIA PRELEKCJI** – Jakub Chmiel „Permanent - krótko o złym bracie bliźniaku wyznacznika”.



Wśród laureatów konkursu na najlepszy poster znaleźli się:

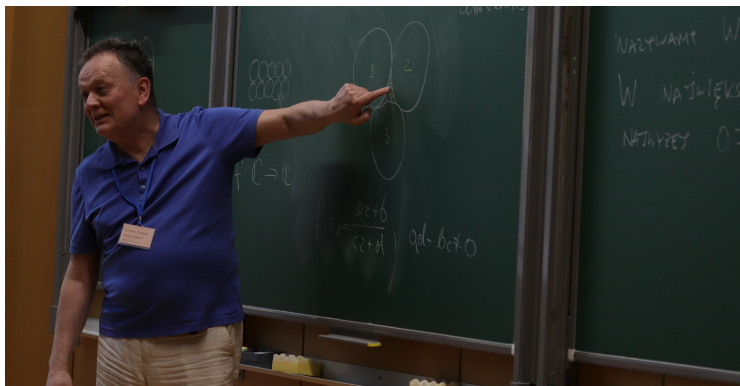
- Miejsce *I* – Aleksandra Symko „Szyfr trudniejszy do złamania od Enigmy? - Szyfr Lorenza”,
- Miejsce *II* – Paweł Grott „Paradoksy i fenomeny w statystyce”,
- Miejsce *III* – Maria Małasiewicz „Odkrywając Matematykę Origami: Rozwiązywanie równań sześciennych poprzez składanie papieru”.



Wyróżnienie trafiło do Oliwii Jarosz i Konrada Wójcika za „Rozwiązując tajemnice Diofantosa: Przegląd i zastosowanie równań diofantycznych”.

Wykłady otwierające

Edycję X konferencji rozpoczął wykład „Teoria gier – poletko doświadczalne matematyków i informatyków” prof. UAM dr hab. Małgorzaty Bednarskiej-Bzdegi, natomiast XI otworzył profesor Tomasz Łuczak prelekcją, pt. „Matematyczny bigos z informatycznymi przyprawami”.



Podczas XI edycji konferencji uczestnicy mogli podziwiać kolekcję maszyn liczących, którą udostępnił i szczegółowo o niej opowiedział dr Jan Kaczmarek.



Organizatorzy

W roku 2023 w organizację zaangażowani byli głównie: Jędrzej Garnek, Kamil Przespolewski, Martyna Stawna, Zuzanna Rygiewicz, Adrianna Smolińska, Anna Szymczyk, Michał Jastrzębski oraz Filip Jankowski. W 2024 roku konferencja nie odbyłaby się bez zaangażowania: Adrianny Smolińskiej, Zuzanny Rachuby, Zuzanny Rygiewicz, Jędrzeja Garnka, Filipa Jankowskiego, Roberta Benduna, Dawida Andrysa, Klaudii Piwowarczyk, Piotra Marczykowskiego, Kacpra Tabaki, Stefana Kaczmarka, Anny Izodorczyk oraz Jakuba Plucińskiego. W przygotowaniach pomagali również: Anastasiya Bandarchuk, Bartosz Wawrzyniak, Adrian Antkowiak, Zuzanna Maciejewska, Karol Wapniarski, Albianna Lapchevska, Cezary Dudkiewicz, Liwia Luch, Asia Kończal, Katarzyna Karkowska, Tymon Tomczak, Aleksander Kiryk.



Sponsorzy i partnerzy

Naszą konferencję wsparli następujący sponsorzy:

- AstraZeneca Pharma Poland Sp. z o.o.,
- wydawnictwo Znak Literanova,
- MuMa - Muzeum Matematyki w Kórniku,
- Oddział Poznański Polskiego Towarzystwa Matematycznego,
- firma Wolfram Research.



AstraZeneca to innowacyjna firma biofarmaceutyczna, znajdująca się w czołówce największych firm tego sektora na świecie. Z myślą o pacjentach opracowujemy i wytwarzamy nowoczesne leki pomagające zwalczać choroby, które stanowią największe wyzwania współczesnej medycyny.



Znak Literanova to zespół ludzi z pasją do literatury - wydawnictwo serwujące prawdziwą ucztę czytelniczą. To książki idące pod prąd – eksperymentujące z formą i treścią, odważne, komentujące wydarzenia i trendy XXI wieku. Wśród nich znajdziemy literaturę piękną z najwyższej półki, interesujące debiuty, bestsellery, biografie czy literaturę non-fiction.



**Muzeum
Matematyki**

MuMa to projekt, którego celem jest przedstawianie matematyki w przystępny i interesujący sposób. Jednym z kolejnych etapów jego rozwoju będzie powstanie Muzeum Matematyki w Kórniku. W ramach przygotowań realizowane są wydarzenia w różny sposób odnoszące się do zagadnień matematycznych poprzez konkursy, warsztaty czy doroczny Festiwal Matematyki w Kórniku.



Polskie Towarzystwo Matematyczne to istniejące od 1919 roku stowarzyszenie zrzeszające osoby związane z polską matematyką. Do jego celów należą między innymi wspieranie badań matematycznych i zastosowań matematyki, krzewienie kultury matematycznej - w tym wspieranie edukacji matematycznej i popularyzacja matematyki, oraz integracja polskiego środowiska matematycznego.



Wolfram Research to amerykańska międzynarodowa firma zajmująca się tworzeniem technologii obliczeniowej. Jej czołowym produktem jest Mathematica - system matematyczny umożliwiający obliczanie wyrażeń numerycznych, symbolicznych i algebraicznych wraz z wyświetlaniem wizualizacji czy danych statystycznych. Inne to m.in. znany i lubiany wśród studentów WolframAlpha, Wolfram SystemModeler, Wolfram Finance Platform czy Wolfram Programming Lab.

Partnerami medialnymi konferencji byli Czasopismo Delta oraz portal unikonferencje.pl. Dziękujemy!

Zabawy z iksami i igrekami, czyli o tym, że pierścienie spełniające tożsamość $x^3 = x$ są przemienne

Marcin Ból

Politechnika Krakowska im. Tadeusza Kościuszki
Wydział Informatyki i Telekomunikacji

1.1 Wstęp

Podobno (źródło: [1]) I. N. Herstein powiedział kiedyś, że otrzymał więcej listów od czytelników dotyczących jednego zadania ze swojej książki *Topics in Algebra* [4], niż listów dotyczących wszystkich innych zadań z tej książki razem wziętych. Zadanie to brzmiało:

Niech R będzie pierścieniem, w którym $x^3 = x$ dla każdego $x \in R$. Udowodnij, że pierścień R jest przemienny.

Stephen Buckley i Desmond MacHale w pracy [1] podają siedem różnych dowodów tego twierdzenia. Po co zwracać sobie głowę wieloma różnymi dowodami pewnego twierdzenia, skoro wystarczy tylko jeden aby mieć pewność, że jest ono prawdziwe? Jest tak dlatego, że zrozumienie dowodu twierdzenia często pozwala dowiedzieć się więcej o obiektach matematycznych, których dane twierdzenie dotyczy, rozwija intuicję i pogłębia rozumienie poruszanego tematu. Wiele różnych dowodów rzuca światło z różnych stron na pewne zagadnienie i umożliwia wyrobienie

sobie opinii, który z ciągów rozumowań jest najciekawszy, najbardziej elegancki i dający największy wgląd w poruszany temat.

Dlaczego przytoczone wyżej zadanie okazało się tak popularne? Może wynika to z braku natychmiastowego związku między warunkami $x^3 = x$ i $xy = yx$? Może z prostoty, elegancji i elementarności warunku $x^3 = x$ i braku dodatkowych, komplikujących zadanie warunków? A może to zadanie daje okazję do tytułowej zabawy z iksami i igrekami oraz czerpania z niej frajdy? W niniejszym artykule przytoczymy dwa z siedmiu wspomnianych dowodów i omówimy kilka uogólnień tego twierdzenia.

1.2 Twierdzenia o przemienności pierścieni

Zacniemy od podania i udowodnienia trzech krótkich twierdzeń, które będą nam później potrzebne. Pierwsze z nich dotyczy pierścieni Boole'a.

Definicja 1.1. Pierścień R nazywamy pierścieniem Boole'a, jeżeli dla każdego $x \in R$ zachodzi warunek $x^2 = x$.

Okazuje się, że pierścienie Boole'a są przemienne, a dowód tego faktu jest bardzo prosty.

Twierdzenie 1.2. *Każdy pierścień Boole'a jest przemienny.*

Dowód. Dla dowolnego $x \in R$ mamy $-x = (-x)^2 = x^2 = x$, a zatem $x + x = 0$. Następnie

$$x^2 + y^2 = x + y = (x + y)^2 = x^2 + xy + yx + y^2$$

i używając prawa skracania

$$xy + yx = 0 = xy + xy.$$

Korzystając znowu z prawa skracania otrzymujemy, że $xy = yx$.
Q.E.D.

Warunek $x^2 = x$ z Twierdzenia 1.2 można osłabić, żądając tylko aby dla dowolnego $x \in R$ wyrażenie $x^2 - x$ należało do centrum pierścienia R , niekoniecznie się zerując. Od tego momentu centrum pierścienia R będziemy oznaczać symbolem $Z(R)$.

Twierdzenie 1.3. *Jeśli $x^2 - x \in Z(R)$ dla dowolnego $x \in R$, to pierścień R jest przemienny.*

Dowód. Z tego, że

$$(x + y)^2 - (x + y) = (x^2 - x) + (y^2 - y) + xy + yx \in Z(R),$$

dostajemy $xy + yx \in Z(R)$. W takim razie $x(xy + yx) = (xy + yx)x$, czyli $x^2y + xyx = xyx + yx^2$ i dlatego $x^2y = yx^2$. Otrzymaliśmy, że $x^2 \in Z(R)$, a stąd już

$$x^2 - (x^2 - x) = x \in Z(R)$$

dla każdego $x \in R$, czyli pierścień R jest przemienny. Q.E.D.

Zmodyfikujmy nieco powyższe twierdzenie.

Twierdzenie 1.4. *Jeśli $x^2 + x \in Z(R)$ dla dowolnego $x \in R$, to pierścień R jest przemienny.*

Dowód. W miejsce x wstawmy $-x$. Wtedy $(-x)^2 - x = x^2 - x \in Z(R)$ i pierścień R jest przemienny z Twierdzenia 1.3. Q.E.D.

Przechodzimy teraz do zasadniczej części artykułu. Podamy twierdzenie z dowodem, o który jesteśmy proszeni w zadaniu Hersteina.

Twierdzenie 1.5. *Niech R będzie pierścieniem w którym $x^3 = x$ dla każdego $x \in R$. Wtedy pierścień R jest przemienny.*

Dowód pierwszy. Niech $x, y \in R$. Rozpisując lewą stronę równości $(x + y)^3 = x + y$ otrzymujemy, że

$$x^2y + xyx + yx^2 + y^2x + yxy + xy^2 = 0.$$

Kładąc $-y$ w miejsce y mamy, że

$$-x^2y - xyx - yx^2 + y^2x + yxy + xy^2 = 0.$$

Dodając powyższe równości stronami otrzymujemy

$$2y^2x + 2yxy + 2xy^2 = 0 \in Z(R).$$

W takim razie

$$(2y^2x + 2yxy + 2xy^2)y = y(2y^2x + 2yxy + 2xy^2)$$

$$2y^2xy + 2yxy^2 + 2xy^3 = 2y^3x + 2y^2xy + 2yxy^2$$

co daje $2xy^3 = 2y^3x$, a zatem $(2x)y = y(2x)$. Stąd $2x \in Z(R)$ dla każdego $x \in R$. Dla dowolnego $x \in R$ mamy następnie

$$\begin{aligned} x^2 + x &= (x^2 + x)^3 = x^6 + 3x^5 + 3x^4 + x^3 \\ &= (x^3)^2 + 3x^3x^2 + 3x^3x + x^3 \\ &= x^2 + 3xx^2 + 3xx + x = x^2 + 3x^3 + 3x^2 + x \\ &= x^2 + 3x + 3x^2 + x = 4(x^2 + x) \in Z(R). \end{aligned}$$

Z Twierdzenia 1.4 wynika, że pierścień R jest przemienny. Q.E.D.

Do drugiego dowodu Twierdzenia 1.5 będziemy potrzebować jeszcze jednej, prostej do udowodnienia własności.

Twierdzenie 1.6. *Niech R będzie pierścieniem, w którym $x^3 = x$ dla każdego $x \in R$. Wtedy $6x = 0$ dla każdego $x \in R$.*

Dowód. Mamy

$$2x = (2x)^3 = 8x^3 = 8x,$$

a zatem $6x = 0$.

Q.E.D.

Drugi dowód Twierdzenia 1.5. Tak jak w dowodzie pierwszym mamy $2y^2x + 2yxy + 2xy^2 = 0$. Mnożąc przez y z lewej strony mamy

$$2(y^3x + y^2xy + yxy^2) = 0,$$

a mnożąc przez y z prawej otrzymujemy

$$2(y^2xy + yxy^2 + xy^3) = 0.$$

Odejmując powyższe równości dostajemy $2xy = 2yx$, czyli $2(xy - yx) = 0$. Udowodniliśmy, że $2(xy - yx) = 0$ dla $x, y \in R$.

Tak jak w dowodzie pierwszym mamy $3(x^2 + x) = 0$, a z tego wynika, że

$$0 = 3((x + y)^2 + (x + y)) = 3((x^2 + x) + (y^2 + y) + (xy + yx)).$$

W takim razie $3(xy + yx) = 0$. Z Twierdzenia 1.6 wiemy, że $6yx = 0$, i dlatego otrzymujemy, że $3(xy - yx) = 0$. Łącząc ten fakt z informacją, że $2(xy - yx) = 0$, dostajemy równość $xy - yx = 0$, czyli pierścień R jest przemienny. Q.E.D.

1.3 Uogólnienia i kontrprzykłady

Przejdźmy teraz do kilku uogólnień Twierdzenia 1.5, które omówimy już bez podawania ich dowodów. Okazuje się, że warunek $x^3 = x$ można osłabić do postaci $(xy)^3 = xy$.

Twierdzenie 1.7. *Niech R będzie pierścieniem, w którym $(xy)^3 = xy$ dla dowolnych $x, y \in R$. Wtedy pierścień R jest przemienny.*

Podobnie jak wcześniej warunek $x^2 - x = 0$ udało się osłabić do postaci $x^2 - x \in Z(R)$, tak i teraz warunek $x^3 - x = 0$ udaje się osłabić do postaci $x^3 - x \in Z(R)$. Co ciekawe, w przypadku warunku z trzecią potęgą otrzymujemy twierdzenie mówiące o jego równoważności z przemiennością pierścienia, a nie tylko o implikowaniu przemienności jak w przypadku drugiej potęgi.

Twierdzenie 1.8. *Pierścień R jest przemienny wtedy i tylko wtedy, gdy $x^3 - x \in Z(R)$ dla każdego $x \in R$.*

Podobną równoważność otrzymuje się, zastępując x w warunku $x^3 = x$ komutatorem elementów x, y pierścienia R , czyli wyrażeniem $xy - yx$.

Twierdzenie 1.9. *Pierścień R jest przemienny wtedy i tylko wtedy, gdy $(xy - yx)^3 = xy - yx$ dla dowolnych $x, y \in R$.*

Istnienie takich uogólnień rodzi naturalne pytania: skoro udało się osłabić warunek $x^3 = x$ do $(xy)^3 = xy$ i otrzymać przemienność pierścienia R , to czy można dalej osłabić ten warunek do $(xyz)^3 = xyz$? Okazuje się, że nie! Nawet mocniejszy warunek $(xyz)^2 = xyz$ nie implikuje przemienności pierścienia R .

Stwierdzenie 1.10. *Istnieją pierścienie nieprzemienne spełniające tożsamość $(xyz)^2 = xyz$.*

Dowód. Przykładem pierścienia nieprzemiennego spełniającego warunek $(xyz)^2 = xyz$ dla wszystkich $x, y, z \in R$ jest pierścień macierzy ściśle górnotrójkątnych wymiaru 3×3 o elementach rzeczywistych. Iloczyn trzech dowolnych macierzy ściśle górnotrójkątnych wymiaru 3×3 jest macierzą zerową, więc warunek $(xyz)^2 = xyz$ jest w tym pierścieniu spełniony w sposób oczywisty. Q.E.D.

Rozważmy jeszcze jeden warunek podobny do tych, które rozważaliśmy wcześniej, ale nie pociągający za sobą przemienności pierścienia R .

Stwierdzenie 1.11. *Istnieją pierścienie nieprzemienne R takie, że $xy \in Z(R)$ dla dowolnych $x, y \in R$.*

Dowód. Weźmy pierścień z poprzedniego Stwierdzenia. Każdy iloczyn xy w tym pierścieniu jest postaci $\begin{bmatrix} 0 & 0 & d \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ dla pewnego $d \in \mathbb{R}$. Takie macierze leżą w centrum pierścienia R . Q.E.D.

Rozważane do tej pory twierdzenia były o tyle przyjemne, że można było dowodzić je bez dogłębnej wiedzy z teorii pierścieni nieprzemiennych w kilku(nastu) liniijkach. Istnieją jednak mocniejsze uogólnienia rozważanych twierdzeń, których dowody wymagają już takiej wiedzy. Takie właśnie są twierdzenie Jacobona z pracy [5] oraz twierdzenia Hersteina z prac [2] i [3].

Twierdzenie 1.12 (Jacobson). *Niech R będzie pierścieniem, w którym dla każdego $x \in R$ istnieje liczba naturalna $n(x) > 1$ taka, że $x^{n(x)} = x$. Wtedy pierścień R jest przemienny.*

Przypadkiem szczególnym powyższego twierdzenia jest sytuacja, w której $n(x)$ jest wspólne dla wszystkich $x \in R$, czyli $x^n = x$ dla wszystkich $x \in R$ i pewnej liczby naturalnej $n > 1$. I. N. Herstein uogólnił to twierdzenie dla $n = 2$ i $n = 3$.

Twierdzenie 1.13 (Herstein). *Niech R będzie pierścieniem, w którym dla każdego $x \in R$ istnieje liczba naturalna $n(x) > 1$ taka, że $x^{n(x)} - x \in Z(R)$. Wtedy pierścień R jest przemienny.*

Co więcej, okazuje się, że podobne uogólnienie zachodzi również dla wspomnianego wcześniej Twierdzenia 1.9, gdzie warunek $x^3 = x$ zastąpiliśmy przez $(xy - yx)^3 = xy - yx$.

Twierdzenie 1.14 (Herstein). *Niech R będzie pierścieniem, w którym dla wszystkich $x, y \in R$ istnieje liczba naturalna $n(x, y) > 1$ taka, że $(xy - yx)^{n(x, y)} = xy - yx$. Wtedy pierścień R jest przemienny.*

Istnieje wiele innych warunków wystarczających przemienności pierścieni, niektóre z nich można znaleźć w pracy przeglądowej [6]. Część z nich jest podobna do warunków opisywanych wyżej, niektóre związane są z pojęciem różniczkowań w pierścieniach, a jeszcze inne dotyczą pewnych szczególnych klas pierścieni.

Poszukiwanie warunków wystarczających przemienności pierścieni wydaje się być atrakcyjną i wciąż aktywną dziedziną algebry, a pewnie matematycy, podobnie jak czytelnicy książki Hersteina, czerpią z tych poszukiwań wiele radości.

Bibliografia

- [1] Buckley S., MacHale D., *Variations on a Theme: Rings Satisfying $x^3 = x$ Are Commutative*, Amer. Math. Monthly 120(5) (2013).
- [2] Herstein I.N., *A generalization of a theorem of Jacobson III*, Amer. J. Math. 75 (1953), 105–111.

- [3] Herstein I.N., *A condition for the commutativity of rings*, Canad. J. Math. 9 (1957), 583–586.
- [4] Herstein I.N., *Topics in Algebra*, Blaisdell Pub. Co., Waltham, 1964.
- [5] Jacobson N., *Structure theory for algebraic algebras of bounded degree*, Ann. Math. 46 (1945), 695–707.
- [6] Pinter-Lucke J., *Commutativity conditions for rings: 1950–2005*, Expo. Math. 25 (2007) 165 – 174.

Atrakcyjność w zwartości, czyli jak dużo jest atraktorów IFS-ów

Krzysztof Caban

Politechnika Łódzka

Wydział Fizyki Technicznej, Informatyki i Matematyki
Stosowanej

2.1 Wstęp

Fraktale to zbiory, które posiadają trzy proste cechy. Okazuje się jednak, że oprócz niewątpliwego piękna tych zbiorów, wiele obiektów czy zjawisk z naszej rzeczywistości ma strukturę fraktalną (przynajmniej do pewnego stopnia). Czym jednak jest fraktal?

Definicja 2.1. Fraktalem nazywamy zbiór, który posiada następujące cechy

- jest samopodobny - jego część jest podobna do całości;
- ma nietrywialną strukturę;
- ma rekurencyjną definicję.

Jak opisać powyższe własności za pomocą matematyki? Z pomocą przychodzi nam iterowane układy odwzorowań, które jak się okazuje, w prosty sposób mogą generować fraktale.

2.2 Teoria Hutchinsona-Barnsleya

Cała matematyka dotycząca iterowanych układów odwzorowań oraz fraktali będzie działała się w *hiperprzestrzeni zbiorów zwartych*.

Definicja 2.2. Niech X będzie przestrzenią metryczną. Zbiór

$$\mathcal{K}(X) := \{K \subset X : K \text{ jest zwarty i niepusty}\}$$

nazywamy **hiperprzestrzenią zbiorów zwartych**.

Oczywiście skoro mówimy o *przestrzeni*, to wypadaloby wyposażyć $\mathcal{K}(X)$ w pewną strukturę. Możemy na przykład zadać na niej metrykę:

$$d_H(K, S) := \max\{d(K, S), d(S, K)\},$$

gdzie $d(K, S) := \sup\{d(x, S) : x \in K\}$ oraz $K, S \in \mathcal{K}(X)$. Powyższa funkcja nosi nazwę **metryki Hausdorffa**.

Lemat 2.3. *Zachodzą poniższe implikacje.*

1. *Jeżeli (X, d) jest zupełna, to $(\mathcal{K}(X), d_H)$ jest zupełna.*
2. *Jeżeli (X, d) jest zwarta, to $(\mathcal{K}(X), d_H)$ jest zwarta.*
3. *Jeżeli (X, d) jest ośrodkowa, to $(\mathcal{K}(X), d_H)$ jest ośrodkowa.*

Teraz jesteśmy gotowi do wprowadzenia najważniejszej definicji. Połączymy tym samym świat fraktali z matematyką.

Definicja 2.4. Rodzinę $\mathcal{F} = \{f_1, \dots, f_k\}$ ciągłych przekształceń przestrzeni metrycznej X w siebie nazywamy **iterowanym układem odwzorowań**, w skrócie **IFS-em**. Funkcję

$$\mathcal{F} : \mathcal{K}(X) \longrightarrow \mathcal{K}(X)$$

zdefiniowaną wzorem

$$\forall_{K \in \mathcal{K}(X)} \mathcal{F}(K) := \bigcup_{n=1}^k f_n(K)$$

nazywamy **operatorem Hutchinsona** indukowanym przez IFS \mathcal{F} .

Łatwo zauważyć, że definicja operatora Hutchinsona jest poprawna. Wynika to z tego, iż obraz zbioru zwartej przez funkcję ciągłą jest zwarty.

Poniższe twierdzenie zostało udowodnione przez Johna E. Hutchinsona w 1981 roku, lecz nie zyskało wielkiego rozgłosu, dopóki Michael F. Barnsley w 1993 nie opublikował książki „Fractals Everywhere”.

Twierdzenie 2.5 (Twierdzenie Hutchinsona-Barnsleya). *Niech X będzie przestrzenią metryczną zupełną. Jeżeli IFS \mathcal{F} złożony jest z kontrakcji, to operator Hutchinsona \mathcal{F} ma kontrakcyjny punkt stały, tj. istnieje dokładnie jeden taki zbiór $A_{\mathcal{F}} \in \mathcal{K}(X)$, że*

$$1. A_{\mathcal{F}} = \mathcal{F}(A_{\mathcal{F}}) = \bigcup_{n=1}^k f_n(A_{\mathcal{F}});$$

2. dla każdego $K \in \mathcal{K}(X)$ ciąg iteracji $(\mathcal{F}^n(K))$ jest zbieżny do $A_{\mathcal{F}}$.

Dowód twierdzenia Hutchinsona-Barnsleya bazuje na Twierdzeniu Banacha o punkcie stałym oraz fakcie, że operator Hutchinsona IFS-u złożonego z kontrakcji będzie kontrakcją.

Ale w końcu, jak związane są IFS-y oraz Twierdzenie 2.5 z pojęciem fraktali?

Przykład 2.6. *Niech $f_1, f_2 : \mathbb{R} \rightarrow \mathbb{R}$ będą dane wzorami*

$$f_1(x) := \frac{1}{3}x, \quad f_2(x) := \frac{1}{3}x + \frac{2}{3}.$$

Oczywiście widać, że są to kontrakcje o stałej Lipschitza równej $\frac{1}{3}$. Natomiast atraktorem IFS-u $\mathcal{F} = \{f_1, f_2\}$ jest zbiór Cantora.

Powyższy przykład oraz inne mu podobne (trójkąt Sierpińskiego, krzywa Kocha itp.) prowadzą nas do następującej definicji.

Definicja 2.7. Zbiór $A_{\mathcal{F}}$ spełniający tezę Twierdzenia 2.5 nazywać będziemy **fraktalem** bądź **atraktorem IFS-u \mathcal{F}** .

Okazuje się jednak, że nie każdy atraktor IFS-u jest fraktalem (w sensie definicji ze Wstępu). Warunek bycia zbiorem skomplikowanym nie zawsze będzie spełniony. Dodatkowo nie każdy fraktal jest atraktorem IFS-u. Za przykład może posłużyć zbiór Mandelbrota.

2.3 Postawienie problemu

Zastanowimy się teraz czy typowe zbiory, którymi się zajmujemy, to fraktale. Będziemy poszukiwali odpowiedzi na pytanie:

Jak duża jest rodzina wszystkich atraktorów IFS-u?

Albo trochę bardziej matematycznie.

Problem 2.8. *Jak duża w sensie kategorii Baire'a jest rodzina*

$$A := \{K \in \mathcal{K}(X) : K \text{ jest atraktorem pewnego IFS-u } \mathcal{G}\}?$$

Zanim przejdziemy do konkretnych wyników, musimy omówić pojęcie porowatości oraz to, jak wiąże się z kategorią Baire'a.

Definicja 2.9. Niech X będzie przestrzenią metryczną. Dla zbioru $A \subset X$ oraz $x \in X$ niech

$$K_R(A, x) := \sup\{r > 0 : B(y, r) \subseteq B(x, R) \setminus A \text{ dla pewnego } y \in X\},$$

wtedy liczbę

$$p(A, x) := \liminf_{R \rightarrow 0^+} \frac{K_R(A, x)}{R}$$

nazywamy **porowatością zbioru A w punkcie x** . Jeżeli dla każdego $x \in X$, $p(A, x) > 0$, to mówimy, że A jest **porowaty**. Dodatkowo powiemy, że zbiór jest **σ -porowaty** jeżeli jest przeliczalną sumą zbiorów porowatych.

Lemat 2.10. *Zachodzą następujące własności:*

1. $p(A, x) = 1 \iff x \notin \bar{A}$.
2. $0 \leq p(A, x) \leq \frac{1}{2} \iff x \in \bar{A}$.

3. *Zbiory porowate są nigdziegęste.*

Okazuje się więc, że być σ -porowatym, to znaczy być jeszcze mniejszym niż pierwszej kategorii. Dla lepszego zrozumienia pojęcia porowatości i różnych jej zastosowań warto zajrzeć do książki [5].

Jesteśmy już gotowi do odpowiedzi (choć mało zadowolającej) na postawione pytanie. Jeśli mamy tylko do dyspozycji IFS-y złożone z kontrakcji oraz $X = [0, 1]^n$ dla $n \in \mathbb{N}$, to wówczas:

Twierdzenie 2.11. [2] *Rodzina \mathcal{A} jest zbiorem σ -porowatym.*

Widzimy zatem, że rodzina atraktorów IFS-ów złożonych z kontrakcji jest *mała*. Co gdyby stworzyć IFS-y z innego rodzaju odwzorowań? Jak zmieni się rozmiar rodziny \mathcal{A} ?

2.4 Słabe kontrakcje na ratunek?

W tym rozdziale odpowiemy na pytanie, kiedy IFS posiada jednoznaczny atraktor. Z wcześniejszych rozważań wiemy, że jeśli funkcje, z których powstał, są kontrakcjami, to zachodzi Twierdzenie 2.5. Jak osłabić warunki kontraktywności, by zachodziło analogiczne Twierdzenie?

Definicja 2.12. Niech X będzie przestrzenią metryczną. Powiemy, że funkcja $\varphi : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ jest φ -**kontrakcją**, jeżeli

$$\forall_{x,y \in X} d(f(x), f(y)) \leq \varphi(d(x, y)).$$

Nietrudno znaleźć związek powyższej definicji z definicją kontrakcji.

Definicja 2.13. Niech X będzie przestrzenią metryczną. Mówimy, że $f : X \rightarrow X$ jest

1. **kontrakcją Rakotchą**, jeśli f jest φ -kontrakcją dla pewnego $\varphi(t) := \lambda(t)t$, gdzie $\lambda : \mathbb{R}_+ \rightarrow [0, 1]$ jest nierosnąca i $\lambda(t) < 1$ dla $t > 0$;

2. **kontrakcją Browdera**, jeśli f jest φ -kontrakcją, gdzie φ jest nierosnąca, prawostronnie ciągła i $\varphi(t) < t$ dla $t > 0$;
3. **kontrakcją Edelsteina**, jeśli f spełnia

$$d(f(x), f(y)) < (d(x, y))$$

dla każdego $x, y \in X$, $x \neq y$.

Oczywiście każda kontrakcja jest też kontrakcją Rakotcha. Natomiast każda kontrakcja Browdera jest Edelsteina. Co ważne, implikacje nie odwracają się w dowolnych przestrzeniach.

W roku 1962 E. Rakotch [4] pokazał, że w przestrzeniach zupełnych każda kontrakcja Rakotcha ma jednoznaczny kontrakcyjny punkt stały. Później w 1968 F. Browder [1] uogólnił wynik Rakotcha dla kontrakcji Browdera. Dodatkowo w 1962 M. Edelstein pokazał, że w zupełnych przestrzeniach kontrakcje Edelsteina mają punkty stałe. Wszystkie te twierdzenia to pewne odpowiedniki Twierdzenia Banacha. Dlatego w połączeniu z poniższym faktem dają istotne wzmocnienie Twierdzenia Hutchinsona-Barnsleya.

Twierdzenie 2.14. [3] *Niech \mathcal{F} będzie IFS-em na przestrzeni metrycznej X złożonym z φ -kontrakcji dla pewnej nierosnącej funkcji φ . Wówczas operator Hutchinsona $\mathcal{F} : \mathcal{K}(X) \rightarrow \mathcal{K}(X)$ jest φ -kontrakcją.*

Twierdzenie 2.15. [3] *Jeżeli \mathcal{F} jest IFS-em na zupełnej przestrzeni metrycznej X złożonym z kontrakcji Rakotcha (odpowiednio Browdera), to wtedy operator Hutchinsona \mathcal{F} ma kontrakcyjny punkt stały, tj. \mathcal{F} generuje jednoznaczny atraktor.*

2.5 Ile w końcu tych atraktorów?

Wracamy teraz do Problemu 2.8. Jesteśmy wyposażeni w inne rodzaje kontrakcji i wiemy, że zwiększyliśmy rodzinę \mathcal{A} dokładając inne atraktory. Czy rozwiązanie problemu się zmieni?

Twierdzenie 2.16. [3] *Niech X będzie zupełną i ośrodkową przestrzenią metryczną bez punktów izolowanych. Wówczas rodzina*

$\mathcal{A} := \{K \in \mathcal{K}(X) : K \text{ jest atraktorem słabo kontraktywnego IFS-u } \mathcal{G}\}$
jest pierwszej kategorii.

Szkic dowodu. Krok 1:

Dla każdego zbioru otwartego $D \subset X$ definiujemy

$$C_D := \{K \in \mathcal{K}(X) : \emptyset \neq K \cap D \subseteq f(K \setminus D) \\ \text{dla pewnej } f : K \rightarrow X \text{ z } Lip(f) \leq 1\}.$$

Każdy z tych zbiorów jest nigdziegęsty w $\mathcal{K}(X)$.

Krok 2:

Ustalmy przeliczalną bazę \mathcal{B} topologii przestrzeni X i zdefiniujmy:

$$\mathcal{NA} := Perf(X) \setminus \bigcup_{D \in \mathcal{B}} C_D.$$

Gdzie $Perf(X)$ to rodzina niepustych zwartych podzbiorów X , które nie mają punktów izolowanych. Korzystając z poniższego lematu:

Lemat 2.17. [3] *Rodzina*

$\mathcal{C}(X) := \{K \in \mathcal{K}(X) : K \text{ jest homeomorficzny ze zbiorem Cantora}\}$
jest rezydualna w $\mathcal{K}(X)$,

otrzymujemy, że \mathcal{NA} jest zbiorem rezydualnym w $\mathcal{K}(X)$.

Krok 3:

Wykazujemy, że każdy zbiór $K \in \mathcal{NA}$ nie jest atraktorem słabo kontraktywnego IFS-u. By to uzyskać, należy pokazać, że dla każdej słabej kontrakcji $f : K \rightarrow K$, obraz $f(K)$ jest nigdziegęsty w K . Tak naprawdę pokazujemy, że $f(K)$ ma puste wnętrze, bo jest domknięty. Ponieważ atraktor jest zwarty, to jest on przestrzenią zupełną, więc nie może być drugiej kategorii. W szczególności nie jest sumą skończoną zbiorów nigdziegęstych. Q.E.D.

Widzimy zatem, że nie uzyskaliśmy istotnie różnego wyniku od Twierdzenia 2.11. Jednak Lemat 2.17 prowadzi nas do następującego wniosku.

Wniosek 2.18. *Rodzina zbiorów homeomorficznych do atraktorów IFS-u jest rezydualna w $\mathcal{K}(X)$.*

Ostatecznie pokazaliśmy, że typowy zbiór nie jest atraktorem żadnego IFS-u. Jednocześnie z powyższego Wniosku wynika, że jest on homeomorficzny z pewnym atraktorem.

Bibliografia

- [1] Browder F., *On the convergence of successive approximations for nonlinear functional equations*. Nederl. Akad. Wetensch. Proc. Ser. A 71 = Indag. Math (1968). 30, 27–35.
- [2] Klinga P., Kwela A., Staniszewski M., *Size of the set of attractors for iterated function systems*. Chaos, Solitons and Fractals 128 (2019) 104-107
- [3] Leśniak K., Snigrieva N., Strobin F., *Weakly contractive iterated function systems and beyond: a manual*. Journal of Difference Equations and Applications (2020), 26:8, 1114-1173, DOI: 10.1080/10236198.2020.1760258
- [4] Rakotch E., *A note on contractive mappings*. Proc. Amer. Math. Soc. 13 (1962), 459–465.
- [5] Zajicek L., *POROSITY AND σ -POROSITY*. Real analysis exchange 13 (1987), 314.

Permanent – krótko o złym bracie-bliźniaku wyznacznika

Jakub Chmiel

Politechnika Krakowska

Wydział Informatyki i Telekomunikacji

3.1 Permanent

Definicja permanentu jest bardzo podobna do definicji wyznacznika, dlatego na początku warto zdefiniować, czym jest wyznacznik.

Definicja 3.1. Wyznacznikiem nazywamy funkcję przyporządkowującą każdej macierzy kwadratowej A stopnia n , o elementach z dowolnego ciała o charakterystyce różnej od 2, skalar zgodnie ze wzorem:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)}.$$

Wyznacznik jest również jedyną funkcją, która jest:

- n -liniowa względem kolumn danej macierzy,
- antysymetryczna względem zamiany dowolnych dwóch kolumn,
- przyporządkowująca macierzy jednostkowej wartość 1.

Zakładając te własności wyznacznika, można wyprowadzić powyższy wzór na wyznacznik.

Po zdefiniowaniu wyznacznika, przejdźmy do definicji permanentu.

Definicja 3.2. Permanentem nazywamy funkcję przyporządkowującą każdej macierzy kwadratowej A stopnia n , o elementach z dowolnego ciała o charakterystyce różnej od 2, skalar zgodnie ze wzorem:

$$\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i\sigma(i)}.$$

Permanent jest sumą po wszystkich możliwych iloczynach wyrazów macierzy takich, że w każdym wierszu i każdej kolumnie wybierany jest dokładnie jeden element. Takie intuicyjne zrozumienie permanentu przyda się w dalszej części pracy.

Liczenie permanentu macierzy 2x2 jest proste, wystarczy zmienić znak minus podczas liczenia wyznacznika na plus.

$$\text{perm} \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = ad + bc$$

Podobnie przy liczeniu permanentu macierzy stopnia 3.

$$\text{perm} \left(\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \right) = aei + bfg + cdh + ceg + afh + bdi$$

Stosując rozwinięcie analogiczne do rozwinięcia Laplace'a (jedyną różnicą jest pomijanie znaku) możemy policzyć permanent dowolnej macierzy kwadratowej.

3.1.1 Permanent, a wyznacznik

Podobieństwa:

- podobieństwo wzoru (we wzorze na permanent macierzy względem wzoru na wyznacznik został usunięty znak permutacji),

- transpozycja nie powoduje zmiany permanentu $\text{perm}(A) = \text{perm}(A^T)$,
- zamiana wierszy lub kolumn nie zmienia permanentu macierzy (przy wyznaczniku zachowywana była wartość bezwzględna),
- przy liczeniu permanentu macierzy istnieje analogiczne rozwinięcie do rozwinięcia Laplace'a,
- pomnożenie dowolnego wiersza lub kolumny przez pewien skalar λ mnoży permanent przez ten skalar,
- permanent macierzy trójkątnej jest równy iloczynowi elementów na głównej przekątnej.

Różnice:

- dodanie do kolumny (lub wiersza) kombinacji liniowej innych kolumn nie zachowuje wartości permanentu, stąd brak odpowiednika metody Gaussa,
- macierz, w której wiersze lub kolumny są liniowo zależne na ogół nie ma permanentu równego 0,
- brak prostej interpretacji geometrycznej permanentu,
- brak niektórych własności algebraicznych takich jak:
 $\text{perm}(AB) = \text{perm}(A)\text{perm}(B)$, $\text{perm}(AB) = \text{perm}(BA)$.

3.1.2 Pólya permanent problem

Liczenie permanentu macierzy dowolnego stopnia wygląda analogicznie jak liczenie wyznacznika tej macierzy. Problem może się jednak pojawić, gdy uświadomimy sobie, że zazwyczaj dostając do policzenia wyznacznik większej macierzy upraszczaliśmy macierz dodając i odejmując wiersze i kolumny. Stosując operacje, które nie zmieniają wyznacznika. Używając metody eliminacji Gaussa. Można zauważyć, że takiego sposobu nie można zastosować do liczenia permanentu macierzy:

$$0 = \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} = 0$$

$$2 = \text{perm} \left(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right) \neq \text{perm} \left(\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right) = 0$$

Z tego powodu pojawia się problem, jak w krótszym czasie, który nie będzie rósł wykładniczo wraz ze wzrostem rozmiaru macierzy, policzyć permanenty macierzy wyższych stopni. Jak uprościć ich liczenie?

Można zauważyć, że dla macierzy kwadratowych stopnia 2 zachodzi następująca własność:

$$\text{perm} \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \det \left(\begin{bmatrix} a & b \\ -c & d \end{bmatrix} \right)$$

Nie jest to nic przełomowego, ale wraz z tą obserwacją zapisaną przez Pólyię powstało pytanie, czy można analogicznie liczyć permanent macierzy stopni wyższych jako wyznacznik z tej macierzy z dopisanymi znakami minus przy niektórych elementach macierzy, czyli zmieniając siatkę znaków.

Rok po obserwacji Pólyi, w 1914 roku inny węgierski matematyk Gábor Szegő pokazał, że nie ma analogicznych twierdzeń dla macierzy stopnia większego lub równego 3. Uzasadnił to w następujący sposób:

$$\text{perm} \left(\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right) = 6$$

$$\det \left(\begin{bmatrix} \pm 1 & \pm 1 & \pm 1 \\ \pm 1 & \pm 1 & \pm 1 \\ \pm 1 & \pm 1 & \pm 1 \end{bmatrix} \right) < 6$$

Ponieważ każda liczba występuje w dwóch sumach (w wyznaczniku są to sumy o przeciwnym znaku) nie jest możliwe, aby taki wyznacznik był równy 6. Czasem jednak taka zamiana permanentu na wyznacznik jest możliwa. W sytuacji gdy wyraz $a_{1,3} = 0$ wystarczy zmienić znak wyrazu $a_{2,1}$ oraz $a_{3,2}$.

To spostrzeżenie można uogólnić do dowolnej macierzy Hessenberga. Macierzą Hessenberga nazywamy macierz, która jest „prawie” trójkątna, czyli taka, w której elementy $a_{ij} = 0$ dla $j - i \geq 2$. Permanent z takiej macierzy jest równy wyznacznikowi z macierzy B takiej, że:

$$A \rightarrow B = (b_{ij}) : b_{ij} \begin{cases} -a_{ij}, & \text{dla } j - i = 1 \\ a_{ij}, & \text{dla } j - i \neq 1 \end{cases}$$

Kolejnym pytaniem postawionym, aby uprościć liczenie permanentu macierzy jest pytanie o odwzorowanie liniowe Φ takie, że:

$$\begin{aligned} \Phi : M_n(\mathbb{F}) &\longrightarrow M_n(\mathbb{F}) \\ \text{perm}(A) &= \det(\Phi(A)) \end{aligned}$$

W 1961 roku Marcus i Minc wykazali, że nie istnieje takie odwzorowanie Φ , jeżeli $\text{char}\mathbb{F} = 0$ oraz $n > 2$.

Poszerzmy nasze poszukiwania jeszcze bardziej, tym razem do odwzorowania afinicznego $\Phi : M_n(\mathbb{F}) \longrightarrow M_m(\mathbb{F})$. Zostało dowiedzione, że istnieje takie odwzorowanie Φ prowadzące z $M_3(\mathbb{F})$ w $M_7(\mathbb{F})$. Prezentuje się ono następująco:

$$\text{perm} \left(\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \right) = \det \left(\begin{bmatrix} 0 & a & d & g & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & i & f & 0 \\ 0 & 0 & 1 & 0 & 0 & c & i \\ 0 & 0 & 0 & 1 & c & 0 & f \\ e & 0 & 0 & 0 & 1 & 0 & 0 \\ h & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \right)$$

3.1.3 Wzór Rysera

Istnieją różne wzory pozwalające policzyć permanent. Najbardziej znanym i zarazem jednym z najefektywniejszych tego typu wzorów jest wzór Rysera.

$$\text{perm}(A) = (-1)^n \sum_{S \subset \{1, \dots, n\}} (-1)^{|S|} \prod_{i=1}^n \sum_{j \in S} a_{ij}$$

Wzór ten oparty jest na zasadzie włączania–wyłączania i może być opisany w jeszcze inny sposób. Niech A_k będzie macierzą powstałą przez usunięcie k kolumn w macierzy A oraz $P(A_k)$ będzie iloczynem sum wierszy macierzy A_k . Niech w końcu Σ_k będzie sumą $P(A_k)$ dla wszystkich możliwych A_k . Wtedy prawdziwy jest wzór:

$$\text{perm}(A) = \sum_{k=0}^{n-1} (-1)^k \Sigma_k.$$

3.2 Zastosowania

3.2.1 Transwersale

Ćwiczenie 3.3. *Na ile sposobów możemy wybrać różne elementy ze zbiorów: $\{3, 5, 6, 7\}$, $\{3, 7\}$, $\{1, 2, 4, 5, 7\}$, $\{3\}$, $\{1, 3, 6\}$, $\{1, 5, 7\}$, $\{1, 2, 3, 6\}$, wybierając dokładnie jeden element z każdego zbioru?*

Na początku zauważmy, że musimy wybrać liczbę 3 ze zbioru będącym singletonem trójki. Skoro trójkę mamy już wybraną, jedyną opcją wyboru elementu ze zbioru $\{3, 7\}$ jest wybranie liczby 7. Natomiast jedyną możliwością, aby wybrać 4 jest wzięcie jej z trzeciego zbioru. Tym samym liczba 2 może zostać zgarnięta tylko z ostatniego zbioru, a my po tych 4 ruchach zostajemy z możliwością wyboru 1, 5, 6 ze zbiorów $\{5, 6\}$, $\{1, 6\}$, $\{1, 5\}$, a takich możliwości mamy 2.

Zadanie to można rozwiązać w inny sposób. Niewymagający nieraz ślepego kombinowania i prostszy w sytuacji, gdy zbiorów lub ich elementów jest więcej. Zapiszmy zbiory i ich elementy jako macierz A , w której kolumny odpowiadają za kolejne zbiory, a wiersze odpowiadają za kolejne elementy zbioru wstawiając 0 tam, gdzie dany zbiór nie posiada wybranego elementu, i 1, gdy

go posiada. W tym przypadku wyglądałaby ona następująco:

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Zadanie sprowadza się do wybrania jedynek w taki sposób, by w każdym wierszu i każdej kolumnie została wybrana dokładnie jedna jedynka. Liczba możliwych takich wyborów w oczywisty sposób jest permanentem tej macierzy, a zatem rozwiązaniem zadania jest liczba: $\text{perm}(A) = 2$.

3.2.2 Skojarzenie doskonałe

Definicja 3.4. Skojarzeniem doskonałym nazywamy zbiór M krawędzi grafu G , taki że każdy wierzchołek grafu G jest końcem dokładnie jednej krawędzi należącej do M .

Pierwszym nietrywialnym ograniczeniem dolnym liczby skojarzeń doskonałych wśród 3-regularnych grafów dwudzielnych była wartość $\frac{n}{3}$ ustalona przez Sinkhorna, gdzie n jest liczbą wierzchołków jednego koloru. Następnie Minc przesunął tę granicę do $\frac{n}{3} + 2$, a Hartfiel do $\frac{n}{3} + 3$. Powstawały kolejne coraz to lepsze ograniczenia jak np. $6 \cdot (\frac{4}{3})^{\frac{n}{2}-3}$ (Voorhoeve, 1979), a Schrijver uogólnił to ograniczenie na wszystkie regularne grafy dwudzielne.

Okazuje się jednak, że jeśli zapiszemy zadany graf dwudzielny G w postaci macierzy sąsiedztwa A (między wierzchołkami jednego koloru a drugiego), to permanent tej macierzy będzie równy liczbie skojarzeń doskonałych:

$$\text{perm}(A) = pm(G).$$

3.2.3 Kombinatoryka

Ćwiczenie 3.5. *Na ile sposobów można ułożyć taniec dla n małżeństw tak, by żadna żona nie tańczyła ze swoim mężem?*

Skoro każda żona może zatańczyć z każdym mężem, ale nie ze swoim, to taką sytuację możemy zapisać w postaci grafu. Będzie to graf dwudzielny, który jest prawie pełny, ponieważ każdy z wierzchołków jednej grupy (symbolizującej w tym zadaniu żony) będzie połączony z każdym wierzchołkiem drugiej grupy (symbolizującej mężów) poza jednym (odpowiadającym mężowi danej kobiety). Wtedy rozwiązanie zadania będzie polegało na wybraniu skojarzenia doskonałego tego grafu (każdy musi zatańczyć dokładnie z jedną osobą). Zatem rozwiązaniem tego zadania jest liczba:

$$\text{perm}(J_n - I_n) = \text{perm} \left(\begin{bmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 0 \end{bmatrix} \right),$$

gdzie J_n jest macierzą stopnia n z samymi jedynkami, a I_n macierzą jednostkową stopnia n .

3.2.4 Bijekcje

Ćwiczenie 3.6. *Ile istnieje bijekcji zbioru n -elementowego, takich że żaden element nie jest swoim obrazem (czyli innymi słowy permutacji bez punktów stałych lub nieporządków)?*

Jest to zadanie analogiczne do poprzedniego, a zatem liczba takich permutacji jest równa permanentowi z macierzy kwadratowej stopnia n z jedynkami na każdej pozycji minus macierz jednostkowa. Możemy to również policzyć używając zasady włączania-wyłączania. Tym samym prawidłowy jest następujący

wzór:

$$\text{perm} \begin{pmatrix} [0 & 1 & \dots & 1] \\ [1 & 0 & \dots & 1] \\ [\vdots & \vdots & \ddots & \vdots] \\ [1 & 1 & \dots & 0] \end{pmatrix} = \sum_{k=0}^n (-1)^k \cdot \frac{n!}{k!}.$$

Warto przy okazji dodać, że istnieje bardziej ogólny wzór prezentujący się następująco ($\lambda \in \mathbb{Z}$):

$$\text{perm} \begin{pmatrix} [\lambda + 1 & 1 & \dots & 1] \\ [1 & \lambda + 1 & \dots & 1] \\ [\vdots & \vdots & \ddots & \vdots] \\ [1 & 1 & \dots & \lambda + 1] \end{pmatrix} = \sum_{k=0}^n \lambda^k \cdot \frac{n!}{k!}.$$

3.2.5 Ménage problem

Na ile sposobów można posadzić n małżeństw przy okrągłym stole tak, by żadna żona nie siedziała obok męża?

Okazuje się, że odpowiedź na to pytanie również można rozwiązać używając permanentu

$$2 \cdot n! \cdot \text{perm}(J_n - I_n - P_n) = 2 \cdot n! \cdot \text{perm} \begin{pmatrix} [0 & 0 & 1 & \dots & 1] \\ [1 & 0 & 0 & \dots & 1] \\ [1 & 1 & 0 & \dots & 1] \\ [\vdots & \vdots & \vdots & \ddots & \vdots] \\ [0 & 1 & 1 & \dots & 0] \end{pmatrix},$$

gdzie P_n jest macierzą permutacyjną, z jedynekami na pierwszej nadprzekątnej oraz z jedynką na miejscu $a_{n,1}$. Problem zaprezentowany powyżej nosi nazwę Ménage problem i został po raz pierwszy zaprezentowany na koniec XIX wieku, a rozwiązany kilkadziesiąt lat później. Ma on swoje konsekwencje w teorii grafów czy teorii węzłów. Dla liczby par równych 2, 3, 4 itd. liczba sposobów wynosi kolejno: 0, 12, 96, 3120, 115200, 5836320... W 1934 roku Touchard wyprowadził wzór rozwiązujący ten problem, któ-

ry dla n par wygląda następująco:

$$2 \cdot n! \sum_{k=0}^n (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k} (n-k)!$$

$$\text{perm}(J_n - I_n - P_n) = \sum_{k=0}^n (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k} (n-k)!$$

3.3 Zakończenie

Podsumowując, permanent wydaje się niepozorny, jeden drobny szczegół zmieniony we wzorze, a konsekwencje tego są ogromne. W przeciwieństwie do swojego brata wyznacznika, używa się go w zupełnie innych działach matematyki niż algebra liniowa, takich jak kombinatoryka czy teoria grafów. Są z nim również niemałe komplikacje podczas liczenia, a problem znalezienia szybkiej metody pozwalającej go wyliczyć nadal pozostaje nierozwiązany.

Bibliografia

- [1] Robin Wilson *Wprowadzenie do teorii grafów*, Wydawnictwo Naukowe PWN SA. Warszawa, wydanie II, 1998.
- [2] Marvin Marcus, Henryk Minc, *Permanents*, Uniweristy of Carolina, Santa Barbara.
- [3] Martin Loeb, *Grafy a počty*, (2009).
- [4] Marvin Marcus, F.C. May, *The Permanent Function*, Cambridge University Press, (2018).
- [5] Frank Ban, *Permanent vs. Determinant* (2014).

Matematyka w codziennym życiu. Propozycja lekcji i zadań.

Aleksandra Choina

Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Wydział Matematyki, Fizyki i Informatyki.

4.1 Wstęp

Matematyka odgrywa kluczową rolę nie tylko w świecie nauki i technologii, ale także w codziennym życiu. Jednakże, wielu uczniów często traci motywację do nauki matematyki, uznając ją za abstrakcyjną i trudną do zrozumienia. W związku z tym, przedstawiony artykuł ma na celu wykazanie korzyści płynących z przeprowadzenia lekcji matematyki w codziennym życiu. Głównym celem lekcji matematyki w codziennym życiu jest pokazanie uczniom praktycznych zastosowań matematyki w różnych sytuacjach życiowych, takich jak budżetowanie, planowanie podróży, zakupy, czy podejmowanie decyzji finansowych. Poprzez przykłady i ćwiczenia praktyczne, uczniowie mają szansę zrozumieć, jak matematyka jest powszechnie obecna w ich otoczeniu i jak może być użyteczna w rozwiązywaniu rzeczywistych problemów.

4.2 Wprowadzenie

Matematyka odgrywa niezaprzeczalną rolę w naszym życiu codziennym, choć często możemy nie zdawać sobie z tego sprawy. Od prostych codziennych czynności, takich jak zakupy w sklepie,

czy planowanie budżetu, po bardziej złożone wyzwania, takie jak planowanie podróży czy podejmowanie decyzji finansowych, matematyka jest wszechobecna. Jest fundamentem, na którym opiera się wiele aspektów naszego życia, a jej zrozumienie i umiejętności wykorzystania w praktyce mogą znacząco ułatwić codzienne funkcjonowanie. Przeprowadzenie takiej lekcji może sprawić, że uczniowie polubią matematykę i będą zauważać jej użyteczność w życiu.

Cele:

1. Zrozumienie znaczenia matematyki w życiu codziennym.
2. Eliminowanie lęku przed matematyką.
3. Motywacja do dalszej nauki.
4. Rozwijanie krytycznego myślenia.
5. Rozwijanie umiejętności życiowych.
6. Rozwijanie umiejętności rozwiązywania problemów (problem-solving).
7. Zrozumienie różnorodnych problemów.

4.3 Materiały i metody

Przy przeprowadzeniu takiej lekcji trzeba mieć na uwadze potrzeby naszych uczniów i ich ulubione metody pracy na lekcji, aby ta lekcja była dla nich przyjemna. Zatem metody pracy na tej lekcji powinniśmy dobrać indywidualnie do każdej klasy. Moją propozycją jest praca indywidualna lub w grupach nad zadaniami, a następnie zaprezentowanie owoców pracy przez uczniów. Nauczyciel powinien być w takiej sytuacji cały czas do dyspozycji uczniów, powinien sprawdzać postępy pracy i ich wyniki. Przykładowe zadania, które można wykorzystać podczas takiej lekcji są zawarte w dalszej części pracy.

4.4 Szkoła podstawowa

W szkole podstawowej możemy przeprowadzić taką lekcję odnośnie obniżek, przecen, wyprzedaży, lokat lub proporcji. Takie zadania pojawiają się między innymi na egzaminie ósmoklasisty.

Zadanie 1. (0–1)

Poniżej przedstawiono składniki potrzebne do przygotowania ciasta na 8 gofrów.

Gofry

Składniki na 8 gofrów:

- ✓ $1\frac{1}{2}$ szklanki mąki
- ✓ $1\frac{1}{3}$ szklanki mleka
- ✓ 2 jajka
- ✓ $1\frac{1}{2}$ łyżeczki proszku do pieczenia
- ✓ 2 łyżeczki cukru pudru
- ✓ $\frac{1}{2}$ szklanki oleju
- ✓ szczypta soli



Oceń prawdziwość podanych zdań. Wybierz P, jeśli zdanie jest prawdziwe, albo F – jeśli jest fałszywe.

Do przygotowania ciasta na 40 gofrów, przy zachowaniu właściwych proporcji odpowiednich składników, potrzeba 10 jajek.	P	F
Do przygotowania ciasta na 72 gofry, przy zachowaniu właściwych proporcji odpowiednich składników, potrzeba 12 szklanek mleka.	P	F

Rysunek 4.1: Zadanie 1 z egzaminu ósmoklasisty 2023. por.[1]

Powyższe zadanie można rozwiązać za pomocą proporcji (proporcjonalności prostej), która przydaje się nam przy obliczeniu ilości składników. W szkole podstawowej można przedstawić zadania związane z przecenami, obniżkami i podwyżkami.

Przykładowe zadania związane z obniżkami i podwyżkami:

Przykład 4.1. *Cena płyty kompaktowej po 30% obniżce wynosi 49zł. Jaka była cena tej płyty przed obniżką? (por. [2]).*

Przykładowe zadanie związane z lokatami:

Przykład 4.2. *Pan Jan wpłacił do banku na jeden rok 5000 zł przy oprocentowaniu 6% w skali roku, a pan Tomek 4000 zł też na rok przy oprocentowaniu 8% w skali roku. Który z nich zarobi więcej?*

W szkole podstawowej możemy również zacząć przedstawiać zadania związane z liczeniem składników odżywczych w naszej diecie, tak jak w poniższym zadaniu.

Przykład 4.3. Śniadanie Michała: *200g bułki paryskiej, 30g masła śmietankowego, 50g sera edamskiego tłustego, 40g szynki wieprzowej gotowanej. Ile gram białka zjadł Michał podczas śniadania?(por. [3])*

Nazwa produktu	Zawartość białka w 100 g produktu
Bułka paryska	6,9 g
Masło śmietankowe	0,6 g
Ser edamski tłusty	26,1 g
Szynka wieprzowa gotowana	16,4 g

Rysunek 4.2: Zadanie 27/28 z egzaminu gimnazjalnego 2009

Przedstawione zadania mogą pomóc uczniom zrozumieć matematykę w kontekście realnym i rozwijać umiejętności potrzebne do rozwiązywania problemów.

4.5 Szkoła średnia

W szkole średniej możemy przedstawić na lekcji odnośnie matematyki w codziennym życiu trudniejsze zadania. Zadania zwią-

zane z lokatami i obniżkami czy podwyżkami cen pojawiają się na egzaminie maturalnym, więc warto poćwiczyć rozwiązywanie ich z uczniami. Poniżej mamy przykładowe zadania z matur związanych z obniżkami i ratami.

Zadanie 3. (0–1)

Kwotę 1000 zł ulokowano w banku na roczną lokatę oprocentowaną w wysokości 4% w stosunku rocznym. Po zakończeniu lokaty od naliczonych odsetek odprowadzany jest podatek w wysokości 19%. Maksymalna kwota, jaką po upływie roku będzie można wypłacić z banku, jest równa

A. $1000 \cdot \left(1 - \frac{81}{100} \cdot \frac{4}{100}\right)$

B. $1000 \cdot \left(1 + \frac{19}{100} \cdot \frac{4}{100}\right)$

C. $1000 \cdot \left(1 + \frac{81}{100} \cdot \frac{4}{100}\right)$

D. $1000 \cdot \left(1 - \frac{19}{100} \cdot \frac{4}{100}\right)$

Rysunek 4.3: Zadanie 3 z egzaminu maturalnego 2015 (por. [6])

Zadanie 2. (1 pkt)

Spodnie po obniżce ceny o 30% kosztują 126 zł. Ile kosztowały spodnie przed obniżką?

A. 163,80 zł

B. 180 zł

C. 294 zł

D. 420 zł

Rysunek 4.4: Zadanie 2 z egzaminu maturalnego 2012 (por. [5])

Zadanie 2. (1 pkt)

Pierwsza rata, która stanowi 9% ceny roweru, jest równa 189 zł. Rower kosztuje

A. 1701 zł.

B. 2100 zł.

C. 1890 zł.

D. 2091 zł.

Rysunek 4.5: Zadanie 2 z egzaminu maturalnego 2011 (por. [4])

4.6 Zadania optymalizacyjne oraz zadania prowadzące do rozwiązywania równań kwadratowych.

Podczas tematu matematyki w codziennym życiu warto wspomnieć o zadaniach optymalizacyjnych.

Zadania optymalizacyjne to zadania na wyznaczenie przy użyciu metod matematycznych optymalnego ze względu na wybrane kryteria rozwiązania danego problemu.

Takie zadania związane są najczęściej z powierzchniami różnych obiektów. Do rozwiązywania tego typu problemów matematycznych używamy układu równań, a następnie rozwiązujemy równania kwadratowe.

Przykładowym zadaniem, które prowadzi do rozwiązania równania kwadratowego jest poniższe zadanie:

Zadanie 34. (5 pkt)

W dwóch hotelach wybudowano prostokątne baseny. Basen w pierwszym hotelu ma powierzchnię 240 m^2 . Basen w drugim hotelu ma powierzchnię 350 m^2 oraz jest o 5 m dłuższy i 2 m szerszy niż w pierwszym hotelu. Oblicz, jakie wymiary mogą mieć baseny w obu hotelach. Podaj wszystkie możliwe odpowiedzi.

Rysunek 4.6: Zadanie 34 z egzaminu maturalnego 2010 (por. [7])

Rozwiązując to zadanie, można zauważyć, że otrzymujemy poniższy układ równań.

$$\begin{cases} x \cdot y = 240 \\ (x + 5) \cdot (y + 2) = 350 \end{cases}$$

Z powyższego układu równań otrzymamy równanie kwadratowe, które powstanie w wyniku podstawienia $x = \frac{240}{y}$:

$$5 \cdot y^2 - 100 \cdot y + 480 = 0.$$

W tej sytuacji musimy obliczyć pierwiastki tego równania, następnie odrzucić ujemne wyniki. W przypadku tego zadania oba pierwiastki są dodatnie, więc mamy możliwe dwa wymiarów jednego basenu i dwa możliwe wymiary drugiego basenu.

4.7 Podsumowanie

Matematyka w codziennym życiu odgrywa kluczową rolę, ale często uczniowie tracą z nią kontakt, uznając ją za trudną i abstrakcyjną. Przedstawiony artykuł pokazuje, jak przeprowadzenie praktycznych zadań na lekcji matematyki może zmienić tę perspektywę. Poprzez praktyczne przykłady i zadania, uczniowie mają szansę zobaczyć, jak matematyka jest obecna w różnych aspektach życia, od zakupów po planowanie podróży. Cele lekcji matematyki w codziennym życiu obejmują nie tylko zrozumienie jej znaczenia, ale także eliminację lęku przed nią i rozwijanie umiejętności życiowych oraz krytycznego myślenia. Materiały prezentowane w tej pracy uwzględniają potrzeby uczniów na różnych etapach edukacji, od szkoły podstawowej po szkołę średnią. Zadania optymalizacyjne są także omawiane, aby pokazać uczniom, jak matematyka może być użyteczna w rozwiązywaniu realnych problemów. Przez to podejście, lekcje matematyki stają się bardziej atrakcyjne i motywujące, zachęcając uczniów do dalszego eksplorowania tej dziedziny nauki. Warto dodać, że można również wprowadzić zadania związane z zakupami w sklepie, lecz ze względu na ich łatwiejsze rozwiązywanie zostały one pominięte.

Bibliografia

- [1] Centralna Komisja Egzaminacyjna, *Egzamin ósmoklasisty. Matematyka*, maj 2023.
- [2] Centralna Komisja Egzaminacyjna, *Egzamin w klasie trzeciej gimnazjum. Część matematyczno-przyrodnicza. Matematyka*, kwiecień 2012.
- [3] Centralna Komisja Egzaminacyjna, *Egzamin w klasie trzeciej gimnazjum. Część matematyczno-przyrodnicza. Matematyka*, kwiecień 2009.

- [4] Centralna Komisja Egzaminacyjna, *Egzamin maturalny z matematyki. Poziom podstawowy*, maj 2011.
- [5] Centralna Komisja Egzaminacyjna, *Egzamin maturalny z matematyki. Poziom podstawowy*, maj 2012.
- [6] Centralna Komisja Egzaminacyjna, *Egzamin w klasie trzeciej gimnazjum. Część matematyczno-przyrodnicza. Matematyka*, kwiecień 2015.
- [7] Centralna Komisja Egzaminacyjna, *Egzamin maturalny z matematyki. Poziom podstawowy*, maj 2010.

Logarytmy dyskretne: Od podstaw do zastosowań

Patryk Doniec

Politechnika Krakowska

Wydział Informatyki i Telekomunikacji

5.1 Wprowadzenie

Artykuł ten poświęcony jest zagadnieniu logarytmu dyskretnego, jego zastosowaniom w kryptografii, oraz metodom rozwiązywania tego problemu.

Logarytmowanie w skończonych grupach multiplikatywnych napotyka na istotne problemy obliczeniowe, co odróżnia je od klasycznego logarytmowania. Obliczenie logarytmów dyskretnych w takich grupach jest powszechnie uważane za trudne, podczas gdy odwrotna operacja – potęgowanie – może być przeprowadzona wydajnie przy użyciu metod takich jak szybkie potęgowanie. Innymi słowy, potęgowanie w odpowiednich grupach jest funkcją jednokierunkową.

Ta właściwość jest kluczowa dla kryptografii, gdyż umożliwia tworzenie kryptosystemów opartych na trudności problemu logarytmu dyskretnego. W dalszej części artykułu zostaną omówione kryptosystemy, takie jak Protokół Wymiany Klucza Diffiego-Hellmana oraz System ElGamala, które wykorzystują tę jednokierunkowość do zapewnienia bezpieczeństwa komunikacji. Artykuł przedstawi także metody służące do obliczania logarytmów dyskretnych, przeanalizujemy Algorytm Pohliga-Hellmana, oraz pokażemy jak z jego pomocą obliczyć logarytm dyskretny.

W pierwszej kolejności, musimy jednak zapoznać się z kilkoma podstawowymi definicjami potrzebnymi do dalszego opisanie logarytmu dyskretnego.

Definicja 5.1. Niech $n \in \mathbb{N} : n > 1$. Zbiór \mathbb{Z}_n^* to zbiór wszystkich liczb naturalnych mniejszych niż n , które są względnie pierwsze z n . Innymi słowy:

$$\mathbb{Z}_n^* = \{a \in \mathbb{N} : 1 \leq a < n, (a, n) = 1\}.$$

Zbiór \mathbb{Z}_n^* jest **grupą multiplikatywną** modulo n , co oznacza, że dla dowolnych dwóch elementów a i b należących do \mathbb{Z}_n^* , ich iloczyn ab również należy do \mathbb{Z}_n^* , inaczej:

$$\forall a, b \in \mathbb{Z}_n^* : abn \in \mathbb{Z}_n^*,$$

oraz że istnieje element odwrotny dla każdego elementu w tym zbiorze, czyli:

$$\forall a \in \mathbb{Z}_n^* \exists a^{-1} \in \mathbb{Z}_n^* : aa^{-1} \equiv 1n.$$

Definicja 5.2. Jeśli a jest elementem \mathbb{Z}_n^* , to **rzędem** a nazywamy najmniejsze $k \in \mathbb{N} : k > 0$, takie że:

$$a^k \equiv 1n.$$

Rząd a modulo n jest zwykle oznaczany przez $\text{ord}_n(a)$.

Przykład 5.3. Weźmy $n = 5$, oraz $a = 2$. Obliczymy $\text{ord}_5(2)$. Ponieważ dla $k \in \{1, 2, 3\}$ mamy: $2^k \not\equiv 15$, natomiast dla $k = 4 : 2^k \equiv 15$, to $\text{ord}_5(2) = 4$.

Definicja 5.4. Niech $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ będzie funkcją przypisującą liczbie n liczbę $k \in \{1, \dots, n\}$ liczb względnie pierwszych z n :

$$\varphi(n) = \#\{k \in \{1, \dots, n\} : (k, n) = 1\}.$$

Funkcję φ nazywamy **funkcją Eulera**, lub inaczej **tocjentem**.

Twierdzenie 5.5 (Własności funkcji Eulera). Niech $p \in \mathbb{N}$ będzie liczbą pierwszą oraz niech $m, n \in \mathbb{N}$ będą liczbami względnie pierwszymi. Wtedy:

$$\begin{aligned} \varphi(p) &= p - 1, \\ \varphi(mn) &= \varphi(m)\varphi(n). \end{aligned}$$

Definicja 5.6. Jeśli $g \in \mathbb{Z}_n^*$ i jest spełniona równość:

$$\text{ord}_n(g) = \varphi(n),$$

to mówimy, że g jest **pierwiastkiem pierwotnym** modulo n , lub inaczej **generatorem** \mathbb{Z}_n^* .

Przykład 5.7. Weźmy $n = 5$ oraz $g = 2$. Sprawdźmy czy 2 jest pierwiastkiem pierwotnym modulo 5 . W przykładzie 5.3 obliczyliśmy iż $\text{ord}_5(2) = 4$. Korzystając z twierdzenia 5.5 mamy iż $\varphi(5) = 4$. Mamy spełnioną równość:

$$\text{ord}_5(2) = \varphi(5),$$

zatem 2 jest pierwiastkiem pierwotnym modulo 5 .

Twierdzenie 5.8 (Warunek konieczny i dostateczny istnienia). Niech $k \in \mathbb{N}$. Pierwiastek pierwotny modulo n istnieje wtedy i tylko wtedy, gdy n jest jedną z następujących liczb:

- potęgą liczb pierwszych nieparzystych: $n = p^k$,
- podwojoną potęgą liczb pierwszych nieparzystych: $n = 2p^k$,
- liczbą 2 i 4 .

Twierdzenie 5.9. Element g jest pierwiastkiem pierwotnym modulo n wtedy i tylko wtedy, gdy każdy element \mathbb{Z}_n^* jest odpowiednią potęgą elementu g .

5.2 Zagadnienie logarytmu dyskretnego

Definicja 5.10. Niech $a, b \in \mathbb{Z}_n^*$. Zagadnienie logarytmu dyskretnego polega na znalezieniu takiego $x \in \mathbb{N} : 0 \leq x < \varphi(n)$, które spełnia kongruencję:

$$b^x \equiv an.$$

Wykładnik x nazywa się **logarytmem dyskretnym** a przy podstawie b modulo n i oznacza:

$$x = \log_b(a)n.$$

Aby mieć pewność, że liczba a ma dobrze określony logarytm dyskretny zakłada się, że podstawa b jest pierwiastkiem pierwotnym modulo n .

Problem 5.11. Weźmy $n = 557, b = 2$, oraz $a = 7$. Będziemy szukać takiego $x \in \mathbb{N} : 0 \leq x < \varphi(n)$, że:

$$x = \log_2(7)557,$$

lub inaczej:

$$2^x \equiv 7557.$$

Najprostszym rozwiązaniem, jest metoda przeliczania, czyli sprawdzenie czy dla kolejnych liczb $x = 0, 1, 2, \dots$ zachodzi równość. Dla wybranych przez nas liczb, obliczylibyśmy w ten sposób że równość zachodzi dla $x = 458$:

$$2^{458} \equiv 7557.$$

Oznacza to, iż z punktu widzenia kryptografii, dla małej liczby n musielibyśmy wykonać dużo obliczeń, aby otrzymać wynik. Ogólnie w metodzie przeliczania należy wykonać $x - 1$ mnożeń modulo n , aby znaleźć logarytm dyskretny.

Dochodzimy tutaj do sedna wykorzystywania logarytmów dyskretnych w kryptografii. Cecha, o której powiedzieliśmy sprawia, że dla dużych liczb pierwszych metoda wyczerpująca jest po prostu nieprzydatna.

5.3 Protokół Diffiego-Hellmana

Pierwszym szandarowym zastosowaniem zagadnienia logarytmu dyskretnego jest Protokół Wymiany Klucza Diffiego-Hellmana. Jego siła oparta jest na trudności obliczenia logarytmów dyskretnych w skończonych grupach multiplikatywnych.

Uzgadnianie klucza Diffiego-Hellmana jest kryptosystemem klucza publicznego. Oznacza to, iż wykorzystuje niezabezpieczony kanał do bezpiecznego przekazywania informacji. Będziemy zakładać sytuację, gdy Alicja(**A**) i Bob(**B**) chcą uzgodnić wspólny, tajny klucz korzystając właśnie z takiego kanału. Spójrzmy zatem na protokół wymiany klucza.

1. Użytkownicy **A** i **B** uzgadniają dużą liczbę pierwszą p oraz liczbę g , która jest pierwiastkiem pierwotnym modulo p . Liczby p, g są znane publicznie.

2. **A** wybiera tajną liczbę $a \in \mathbb{N}$ oraz przesyła **B** wartość:

$$x \equiv g^a p.$$

3. **B** wybiera tajną liczbę $b \in \mathbb{N}$ oraz przesyła **A** wartość:

$$y \equiv g^b p.$$

4. Wspólnym tajnym kluczem jest teraz:

$$K \equiv g^{ab} p.$$

Jeżeli Cezary podsłuchiwał konwersację i zna p, g, x, y , będzie chciał obliczyć K . Aby to zrobić musi obliczyć jeden z wykładników: a lub b . Jest to równoważne z obliczeniem logarytmów dyskretnych:

$$a = \log_g(x)p, \quad b = \log_g(y)p.$$

Kryptosystem opiera się zatem na własności, iż w grupie \mathbb{Z}_p^* :

$$K \equiv g^{ab} \equiv (g^a)^b \equiv (g^b)^a \equiv x^b \equiv y^a p$$

oraz, że jeżeli Cezary słucha, to zna g^a, g^b, g^{a+b} , ale nie zna g^{ab} .

5.4 System ElGamala

System ElGamala jest kolejnym kryptosystemem opartym na trudności problemu logarytmu dyskretnego w skończonych grupach multiplikatywnych. Algorytm w połowie lat 80. XX wieku zaproponował Egipcjanin Taher ElGamal. Podobnie jak metoda Diffiego-Hellmana korzysta on z bezpiecznego przesyłania wiadomości niezabezpieczonym kanałem.

System wymaga aby użytkownik posiadał zarówno klucz prywatny jak i klucz publiczny. Zaszifrowane wiadomości są ogólnie dostępne, natomiast deszyfrowanie jest możliwe tylko poprzez powołane osoby, które posiadają klucz prywatny. Krótko mówiąc, system ElGamala jest kryptosystemem asymetrycznym. Posiadanie klucza publicznego danego użytkownika oraz znajomość metody szyfrowania nie są wystarczające do odkrycia jego klucza prywatnego.

Pokażemy teraz algorytm generowania klucza publicznego, algorytm szyfrowania oraz deszyfrowania w systemie ElGamala.

5.4.1 Algorytm generowania klucza w systemie ElGamala

1. Użytkownik **A** wybiera liczbę pierwszą p oraz liczbę g , która jest pierwiastkiem pierwotnym modulo p .
2. **A** wybiera również liczbę $k \in \mathbb{N} : 0 \leq k < p - 1$ służącą za klucz prywatny. Obliczana jest liczba:

$$x \equiv g^k p.$$

3. Trójka (p, g, x) jest kluczem publicznym użytkownika **A**. Jest on dostępny dla wszystkich innych użytkowników.

Odkrycie liczby k na podstawie znajomości jawnych liczb (p, g, x) wymaga rozwiązania zagadnienia logarytmu dyskretnego. Analogicznie jak w przypadku metody Diffiego-Hellmana:

$$k = \log_g(x)p.$$

Zobaczyliśmy jak Alicja generuje klucz publiczny. Teraz po jego publikacji Bob chce przesłać jej wiadomość. Pierwsze co Bob musi zrobić, to przekształcić ją na odpowiednik liczbowy oraz ewentualnie może podzielić wiadomość na bloki. Spójrzmy zatem co z tak przygotowaną wiadomością należy dalej zrobić.

5.4.2 Algorytm szyfrowania w systemie ElGamala

Użytkownik **B** chce przesłać użytkownikowi **A** wiadomość, którą przekształcił na odpowiednik liczbowy M .

1. Użytkownik **B** wybiera liczbę $j \in \mathbb{N} : 0 \leq j < p - 1$ oraz oblicza:

$$C_1 \equiv g^j p, \quad C_2 \equiv Mx^j p.$$

2. Szyfrogramem wiadomości M jest $C = (C_1, C_2)$.

Bob zaszyfrował wiadomość M oraz przesłał Alicji szyfrogram C . Zobaczmy teraz co należy zrobić, aby odzyskać oryginalną wiadomość.

5.4.3 Algorytm deszyfrowania w systemie ElGamala

Użytkownik **A** może odszyfrować otrzymaną wiadomość używając swojego klucza prywatnego k .

$$C_2 C_1^{-k} \equiv (Mx^j)(g^{-jk}) \equiv (Mg^{jk})(g^{-jk}) \equiv Mp.$$

Przykład 5.12. *Użytkownik **B** chce przesłać wiadomość SZYFR osobie z kluczem publicznym $(p, g, x) = (43, 3, 22)$ oraz kluczem prywatnym $k = 15$.*

1. *Odpowiednikiem SZYFR jest $M = [18, 25, 24, 5, 17]$.*
2. ***B** wybiera $j = 23$ i oblicza:*

$$C_1 = g^j = 3^{23} \equiv 3443,$$

$$C_2 = Mx^j = M \cdot 22^{23} \equiv [17, 26, 37, 31, 28]43.$$

3. Zaszzyfrowana wiadomość ma następującą postać

$$(C_1, C_2) = (34, [17, 26, 37, 31, 28]).$$

Teraz popatrzymy jak użytkownik **A** poradzi sobie z otrzymanym szyfrogramem (C_1, C_2) .

4. **A** używa klucza prywatnego $k = 15$ otrzymując

$$C_2 C_1^{-k} = C_2 \cdot 34^{-15} \equiv C_2 \cdot 39 \equiv [18, 25, 24, 5, 17]43.$$

Użytkownik **A** otrzymał oryginalną wiadomość M , której odpowiednikiem jest wiadomość *SZYFR*.

We wcześniejszej części artykułu rozważaliśmy problem 5.11, z którego wnioskowaliśmy, iż szukanie logarytmów dyskretnych metodą przeliczania jest nieefektywne dla dużych liczb pierwszych. Konsekwencją są protokoły kryptograficzne bazujące na tej własności. Istnieją jednak inne metody, które pozwalają przyspieszyć proces obliczania logarytmów dyskretnych.

Przedstawimy teraz algorytm Pohliga-Hellmana oraz pokażemy jak korzystając z niego możemy obliczyć przykładowy logarytm.

5.5 Algorytm Pohliga-Hellmana

Algorytm Pohliga-Hellmana polega na zredukowaniu zagadnienia logarytmu dyskretnego do analogicznego problemu w mniejszych grupach cyklicznych.

1. Zakładamy że szukamy $x : b^x \equiv ap$ w grupie \mathbb{Z}_p^* rzędu n oraz że liczba n ma rozkład postaci:

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

2. Dla każdej liczby p_i występującej w rozkładzie n obliczamy trzy liczby:

$$n_{p_i} = \frac{n}{p_i^{\alpha_i}}, \quad b_{p_i} \equiv b^{n_{p_i}} p, \quad a_{p_i} \equiv a^{n_{p_i}} p.$$

Twierdzenie 5.13. *Załóżmy, że dla każdego czynnika pierwszego p_i rozkładu liczby n , liczba $x(p_i)$ jest rozwiązaniem logarytmu dyskretnego:*

$$b_{p_i}^{x(p_i)} \equiv a_{p_i} p.$$

Niech x będzie rozwiązaniem układu kongruencji:

$$x \equiv x(p_i) p_i^{\alpha_i},$$

dla wszystkich liczb pierwszych p_i w rozkładzie n . Wówczas x jest również rozwiązaniem zagadnienia logarytmu dyskretnego:

$$b^x \equiv ap.$$

Przykład 5.14. *Spróbujmy znaleźć $x : 2^x \equiv 7181$.*

1. *Dla grupy \mathbb{Z}_{181}^* , której rząd wynosi 180, mamy rozkład:*

$$180 = 2^2 \cdot 3^2 \cdot 5^1.$$

2. *Obliczamy kolejno:*

$$\begin{aligned} p_1 = 2^2, \quad n_{p_1} = 45, \quad b_{p_1} = 162, \quad a_{p_1} = 19, \\ p_2 = 3^2, \quad n_{p_2} = 20, \quad b_{p_2} = 43, \quad a_{p_2} = 132, \\ p_3 = 5^1, \quad n_{p_3} = 36, \quad b_{p_3} = 59, \quad a_{p_3} = 1. \end{aligned}$$

3. *Wyznaczenie logarytmu dyskretnego $x : 2^x \equiv 7181$ możemy sprowadzić do rozwiązania trzech zagadnień:*

$$\begin{aligned} 162^{x(2)} &\equiv 19181, \\ 43^{x(3)} &\equiv 132181, \\ 59^{x(5)} &\equiv 1181. \end{aligned}$$

4. *Obliczając logarytmy związane z kolejnymi p_i , otrzymujemy:*

$$x(2) = 3, \quad x(3) = 6, \quad x(5) = 0.$$

5. Zgodnie z twierdzeniem 5.13, szukany logarytm dyskretny x jest rozwiązaniem układu kongruencji:

$$x \equiv 32^2,$$

$$x \equiv 63^2,$$

$$x \equiv 05^1.$$

6. Rozwiązując układ otrzymamy $x = 15$.

Algorytm Pohliga-Hellmana nie jest oczywiście jedyną metodą przyspieszającą obliczanie logarytmów dyskretnych. Innym algorytmem, który warto wymienić jest algorytm Małych i Wielkich Kroków. Metoda ta jest zdecydowanie szybsza niż przeliczanie, jednak mniej wydajna niż algorytm Pohliga-Hellmana. Oprócz kwestii czasu, wymaga ona dużo więcej pamięci niż pozostałe dwie metody. Dla dużych liczb pierwszych obliczenie logarytmu będzie wymagało przechowywania ogromnych tablic.

Kolejną interesującą metodą jest Algorytm ρ Pollarda. Pomimo tego, że jest on bardziej efektywny pod względem czasu obliczeń niż algorytm Małych i Wielkich Kroków, także wymaga przechowywania dużych ilości danych. Warto również wspomnieć, iż istnieją metody obliczania logarytmów dyskretnych na krzywych eliptycznych. Krzywe eliptyczne stanowią zaawansowaną dziedzinę kryptografii oferującą zwiększone bezpieczeństwo i wydajność w porównaniu do tradycyjnych metod.

Bibliografia

- [1] Stinson D.R., Paterson M.B., *Kryptografia. W teorii i praktyce*, PWN, Wydanie IV, 2021.
- [2] Dummit E., *Discrete Logarithms in Cryptography*, 2016.
- [3] Chrząszczczyk A., *Algorytmy teorii liczb i kryptografii w przykładach*, BTC, 2010.
- [4] Aumasson J.P., *Nowoczesna Kryptografia. Praktyczne wprowadzenie do szyfrowania*, PWN, 2018.

Maszyna uczenia ekstremalnego i pseudoodwrotności Moore'a–Penrose'a

Paweł Drzyzga

Politechnika Krakowska

Wydział Informatyki i Telekomunikacji

6.1 Wstęp

6.1.1 Sieć neuronowa z pojedynczą warstwą ukrytą (SLFN)

Maszyna Uczenia Ekstremalnego (ELM) jest jedną z najpopularniejszych sieci neuronowych ze względu na jej prostą strukturę i potężne zdolności aproksymacyjne. Została pierwszy raz zaproponowana w 2004 roku przez prof. Guang–Bin Huanga. Jest to metoda, która stanowi rodzaj jednowarstwowej sztucznej sieci neuronowej (SLFN), przez co jest dość prosta w budowie. Sieci SLFN pochodzą z rodziny sieci FNN, czyli jednokierunkowych sieci neuronowych. SLFN składa się z warstwy neuronów wejściowych, jednej warstwy ukrytej oraz warstwy wyjściowej.

Mamy N dowolnych, parami różnych próbek (x_i, y_i) , gdzie $x_i = [x_{i1}, x_{i2}, \dots, x_{in}]^T \in \mathbb{R}^m$ i $y_i = [y_{i1}, y_{i2}, \dots, y_{im}]^T \in \mathbb{R}^n$. Standardowa sieć SLFN z L ukrytymi neuronami i funkcją aktywacji $g(x)$, która jest nieskończenie różniczkowalna, może dokładnie przybliżyć te N próbek bez błędu. Możemy to zapisać jako:

$$\sum_{i=1}^L \beta_i g(w_i \cdot x_j + b_i) = \mathbf{y}_j \quad j = 1, \dots, N,$$

gdzie $w_i = [w_{i1}, w_{i2}, \dots, w_{in}]^T$ jest wektorem wag, łączącym i-ty neuron ukryty z neuronami wejściowymi, $\beta_i = [\beta_{i1}, \beta_{i2}, \dots, \beta_{im}]^T$ jest wektorem wag łączącym i-ty ukryty neuron z neuronami wyjściowymi, b_i jest biasem i-tego neuronu ukrytego, $w_i \cdot x_j$ opisuje iloczyn skalarny między w_i a x_j . Po dobraniu wag i biasu, sieci SLFN można po prostu traktować jako system liniowy.

6.1.2 Co to jest ELM?

Maszyna uczenia ekstremalnego jest to sieć neuronowa z pojedynczą warstwą neuronów ukrytych. W 1997 roku udowodniono, że sieć SLFN z N ukrytymi neuronami może nauczyć się N różnych obserwacji. Huang i Babri wykazali, że sieć SLFN z maksymalnie N neuronami ukrytymi oraz praktycznie dowolną nieliniową funkcją aktywacji może dokładnie nauczyć się N różnych obserwacji.

Pod względem wydajności, ELM ma istotną przewagę nad tradycyjnymi sieciami neuronowymi, które są oparte na metodach gradientowych. Nie wymaga iteracyjnej metody wstecznej propagacji błędów, lecz korzysta z uogólnionych macierzy Moore'a-Penrose'a. W przypadku metody wstecznej propagacji błędów proces wygląda następująco: najpierw wartości wejściowe są mnożone przez wagi, dodawany jest bias, stosowana jest funkcja aktywacji i kroki te są powtarzane dla każdej warstwy. Następnie obliczane są wartości wyjściowe, a proces ten jest powtarzany wielokrotnie poprzez wsteczną propagację.

ELM eliminuje konieczność powtarzania tych kroków przez liczbę warstw, ponieważ posiada tylko jedną warstwę. Wsteczną propagację zastępuje obliczaniem pseudoodwrotności, co znacząco redukuje ilość wymaganej pracy, a w praktyce oszczędza dużo czasu. Ponadto, ELM eliminuje problem minimów lokalnych, gdyż nie stosuje metod gradientowych.

Dodatkową zaletą ELM jest to, że nie ma potrzeby dostrajania biasu i wag, gdyż są one generowane losowo, co znacznie upraszcza proces uczenia. Wagi wyjściowe są następnie obliczane przy użyciu macierzy pseudoodwrotnej.

6.1.3 Do czego potrzebne nam są pseudoodwrotności?

Sieć SLFN jest modelowana jako układ równań liniowych, można by nawet powiedzieć, że macierzowych. Taki układ rozwiązuje się bardzo efektywnie przy użyciu macierzy, o ile można znaleźć macierz odwrotną. Problemem jest to, że w ELM otrzymywany układ liniowy jest nadokreślony. Oznacza to, że mamy więcej równań niż niewiadomych. Sprawia to, że takie równanie prawie na pewno nie ma rozwiązania. Remedium na ten problem są uogólnione macierze Moore'a–Penrose'a. Pseudoodwrotność Moore'a–Penrose'a jest ogólnym rozszerzeniem pojęcia odwrotności macierzy na macierze niekwadratowe. W kontekście ELM pseudoodwrotność jest używana do obliczania wag sieci. Istnieje wiele metod obliczania pseudoodwrotności, a wybór odpowiedniej zależy od rozmiaru macierzy oraz dostępnych zasobów obliczeniowych. Dzięki pseudoodwrotności jesteśmy w stanie obliczyć rozwiązanie w sensie najmniejszych kwadratów o najmniejszej normie.

Tutaj dochodzimy do istoty zagadnienia: najmniejszej normy wag. W odróżnieniu od tradycyjnych algorytmów, ELM dąży nie tylko do osiągnięcia jak najmniejszego błędu treningowego, ale także do jak najmniejszej normy wag. Bartlett udowodnił, że im mniejsza norma wag modelu, tym lepiej model generalizuje[1]. Aby model lepiej uogólniał, poszukujemy rozwiązania w sensie najmniejszych kwadratów o najmniejszej normie.

Jednakże ELM mogą ograniczać posiadane zasoby, gdy jest stosowana do dużych zbiorów danych. Głównym problemem jest duża ilość pamięci potrzebnej do przechowywania wag czy biasów. Może to prowadzić do spadku wydajności, a nawet do uniemożliwienia trenowania modelu.

6.1.4 Kontrowersje historyczne

Początki ELM sięgają 2004 roku, kiedy to prof. Guang-Bin Huang opublikował artykuł pt. „Extreme Learning Machine: A New Learning Scheme of Feedforward Neural Networks”. W artykule tym Huang przedstawił nową koncepcję, którą nazwał Extreme Learning Machine.

W 2006 roku Huang opublikował kolejny artykuł poświęcony ELM, pt. „Extreme Learning Machine: Theory and Applications”. Omówił w nim szerzej podstawy ELM oraz zaprezentował jego nowe zastosowania.

Publikacja artykułów Huanga o ELM wzbudziła pewne kontrowersje. Lipo P. Wang i Chunru R. Wan w komentarzu do artykułu Huanga z 2004 roku zarzucili mu, iż przedstawiona przez Huanga metoda ELM jest jedynie znaną już wcześniej metodą sieci neuronowych z radialną funkcją bazową (RBF). Huang odniósł się do tych zarzutów, twierdząc, że ELM jest oryginalną metodą, różniącą się od RBF pod wieloma względami.

Kontrowersja ta skłoniła badaczy do bardziej szczegółowej analizy różnic między ELM a RBF oraz do zastanowienia się nad kryteriami, które należy stosować przy ocenie oryginalności i wartości nowych metod.

6.1.5 Zastosowania ELM

1. Medycyna:

- Klasyfikacja guzków tarczycy na złośliwe i łagodne.
- W mammografii wykrywa się nieprawidłowości oraz klasyfikuje masy jako łagodne lub złośliwe.

2. Ekonomia:

- Prognozowanie wzrostu gospodarczego.
- Przewidywanie ryzyka kredytowego.

3. Żywność:

- Monitorowanie bezpieczeństwa żywności.

- Klasyfikacja różnych rodzajów win.

6.2 Co tutaj robi pseudoodwrotność?

6.2.1 Macierz neuronów ukrytych

Przypomnijmy sobie na początku, w jaki sposób powstaje nasz układ równań liniowych. Mamy N różnych równań liniowych. Możemy to bardzo łatwo zapisać w postaci macierzowej:

$$\mathbf{H}\beta = \mathbf{Y},$$

gdzie macierz \mathbf{H} to:

$$\mathbf{H}(w_1, \dots, w_L, b_1, \dots, b_L, x_1, \dots, x_N) =$$

$$\begin{bmatrix} g(w_1 \cdot x_1 + b_1) & \dots & g(w_L \cdot x_1 + b_L) \\ \dots & \dots & \dots \\ g(w_1 \cdot x_N + b_1) & \dots & g(w_L \cdot x_N + b_L) \end{bmatrix}_{N \times L}$$

$$\beta = [\beta_1, \dots, \beta_L]^T \in \mathbb{R}^{L \times m} \text{ i } \mathbf{Y} = [\mathbf{y}_1, \dots, \mathbf{y}_N]^T \in \mathbb{R}^{N \times m}.$$

Macierz \mathbf{H} jest nazywana macierzą warstwy ukrytej sieci neuronowej.

6.2.2 Kwestia nadokreślonego układu równań

Żeby pokazać, że nasza macierz neuronów ukrytych jest prostokątna, prof. Guang pokazał 2 twierdzenia. Pierwsze:

Twierdzenie 6.1. *Weźmy standardową sieć SLFN, z N ukrytymi neuronami. Dla N parami różnych próbek (x_i, y_i) , gdzie $x_i \in \mathbb{R}^n$ i $y_i \in \mathbb{R}^m$, dla dowolnych w_i oraz b_i wybranych losowo z \mathbb{R}^n i \mathbb{R} (odpowiednio), zgodnie z dowolnym ciągłym rozkładem prawdopodobieństwa, macierz \mathbf{H} warstwy ukrytej sieci SLFN jest prawie na pewno odwracalna, a z tego wynika, że $\|\mathbf{H}\beta - \mathbf{Y}\| = 0$.*

Twierdzenie mówi, że dla sieci SLFN z N ukrytymi neuronami, macierz H jest prawie na pewno odwracalna. Oznacza to, że dla każdej próbki danych (x_i, y_i) , istnieje zestaw wag β , który dokładnie przewiduje etykietę y_i dla x_i .

Wartość $\|H\beta - Y\| = 0$ oznacza, że błąd pomiędzy rzeczywistymi etykietami, a przewidywanymi etykietami jest zerowy, wskazując na idealne dopasowanie modelu do danych treningowych. W praktyce, ze względu na szum lub zakłócenia w danych, całkowite dopasowanie może być trudne do osiągnięcia, więc wartość ta będzie zwykle bardzo bliska zeru.

Twierdzenie 6.2. *Weźmy małą dodatnią liczbę ε . Wówczas istnieje $L \leq N$, takie że dla N parami różnych próbek (x_i, y_i) , gdzie $x_i \in \mathbb{R}^n$ oraz $y_i \in \mathbb{R}^m$, dla dowolnych w_i oraz b_i wybranych losowo z \mathbb{R}^n i \mathbb{R}^m odpowiednio, zgodnie z dowolnym ciągłym rozkładem prawdopodobieństwa, z prawdopodobieństwem równym 1 zachodzi nierówność: $\|H\beta - Y\| < \varepsilon$.*

Innymi słowy, oznacza to, że można znaleźć takie L (liczba neuronów w warstwie ukrytej), które zapewni, że błąd aproksymacji będzie mniejszy niż dowolnie mała zadana wartość ε , przy losowym wyborze wag i biasów.

6.2.3 Jak to z tą pseudoodwrotnością?

Twierdzenie 6.3. *Mamy macierz G , taką, że GY istnieje. Wtedy następujące warunki są równoważne:*

1. *Dla dowolnego Y iloczyn GY jest mającym najmniejszą normę, rozwiązaniem w sensie najmniejszych kwadratów układu $H\beta = Y$.*
2. *G jest uogólnioną macierzą odwrotną w sensie Moore'a-Penrose'a macierzy H .*

To twierdzenie mówi nam, że iloczyn GY jest najlepszym rozwiązaniem w sensie najmniejszych kwadratów dla każdego Y w kontekście układu liniowego $H\beta = Y$ wtedy i tylko wtedy, gdy G jest uogólnioną macierzą odwrotną macierzy H w sensie

Moore'a-Penrose'a.

Roger Penrose i Eliakim Hastings Moore zdefiniowali nową odwrotność macierzy, nazywaną macierzą pseudoodwrotną Moore'a-Penrose'a lub uogólnioną macierzą Moore'a-Penrose'a. Definicję równoważności macierzy odwrotnych Moore'a-Penrose'a podał Penrose. Wygląda ona następująco.

Definicja 6.4. Pseudoodwrotnością Moore'a-Penrose'a macierzy $\mathbf{H} \in \mathbb{R}^{N \times L}$ nazywa się macierz $\mathbf{G} \in \mathbb{R}^{L \times N}$, która spełnia następujące cztery warunki:

1. $\mathbf{HGH} = \mathbf{H}$,
2. $\mathbf{GHG} = \mathbf{G}$,
3. $(\mathbf{HG})^T = \mathbf{HG}$,
4. $(\mathbf{GH})^T = \mathbf{GH}$.

Piszemy: $\mathbf{G} = \mathbf{H}^+$.

Uwaga 6.5. Powyższe warunki nazywa się aksjomatami Moore'a-Penrose'a. Zasadniczo powinno mówić się „uogólnione macierze odwrotne w sensie Moore'a-Penrose'a”, jednak na potrzeby prezentacji pozostaniemy przy nazewnictwie „pseudoodwrotność”.

Twierdzenie 6.6. Każda macierz $\mathbf{H} \in \mathbb{R}^{N \times L}$ ma dokładnie jedną pseudoodwrotność w sensie Moore'a-Penrose'a.

Wniosek 6.7. Jeśli macierz $\mathbf{H} \in \mathbb{R}^{N \times L}$ jest odwracalna, to $\mathbf{H}^+ = \mathbf{H}^{-1}$

Własności pseudoodwrotności:

1. $(\mathbf{G}^+)^+ = \mathbf{G}$,
2. $(\lambda \mathbf{G}^+)^+ = \frac{1}{\lambda} \mathbf{G}^+$,
3. $(\mathbf{G}^*)^+ = (\mathbf{G}^+)^*$,
4. $(\mathbf{G}^+)^T = (\mathbf{G}^T)^+$.

Uwaga 6.8. *Nie zachodzi równość $(GH)^+ = H^+G^+$.*

Warto wspomnieć, że pojęcie to opracowali niezależnie od siebie E. H. Moore w 1920 i Roger Penrose w 1955 roku.

Dla układu liniowego $H\beta = Y$ specjalne rozwiązanie $\beta = H^+Y$ jest rozwiązaniem metody najmniejszych kwadratów. Spośród wszystkich możliwych rozwiązań ma ono najmniejszą normę.

Jeśli macierz H ma pełny rząd, rozwiązanie w sensie najmniejszych kwadratów jest jednoznaczne. W przeciwnym razie, gdy H nie ma pełnego rzędu, istnieje nieskończenie wiele rozwiązań metody najmniejszych kwadratów.

6.2.4 Metody znajdowania pseudoodwrotności

Istnieje wiele sposobów znajdowania pseudoodwrotności, jednak najpowszechniejszą metodą w wielu wariantach ELM jest SVD, czyli rozkład według wartości osobliwych. SVD generuje macierze pseudoodwrotne z dużą dokładnością, jednak problem polega na tym, że pochłania on dość sporą ilość zasobów, co może prowadzić do obniżenia wydajności. Dlatego możemy korzystać między innymi z takich metod jak:

- Rozkład QR.
- Rozkład Choleskyego.
- Rozkład na macierze pełnego rzędu.

6.3 Algorytmy ELM

Samych sposobów znajdowania macierzy pseudoodwrotnych jest sporo, jednak, algorytmów ELM jest jeszcze więcej, ponieważ pomijając już fakt, że do każdej metody znajdowania pseudoodwrotności, moglibyśmy dopasować jeden algorytm ELM, to dodatkowo ludzie cały czas próbują w jakiś sposób łączyć algorytmy ze sobą, aby uzyskać lepszą wydajność lub/i dokładność.

- SVD-ELM
- Geninv-ELM
- QRGinv-ELM
- CGS-ELM
- TPM-ELM

6.4 Algorytm SVD-ELM

6.4.1 Rozkład według wartości osobliwych

SVD zostało zdefiniowane dla rzeczywistych macierzy kwadratowych w latach 70. XIX wieku przez Beltramię i Jordana. Poniżej znajduje się twierdzenie przedstawiające SVD.

Twierdzenie 6.9. *Niech $\mathbf{H} \in \mathbb{R}^{N \times L}$ i $r = \text{rank}(\mathbf{H})$. Wtedy istnieją macierze ortogonalne $\mathbf{U} \in \mathbb{R}^{N \times N}$ oraz $\mathbf{V} \in \mathbb{R}^{L \times L}$ taka, że: $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T$, gdzie:*

$$\mathbf{\Sigma} = \begin{bmatrix} \mathbf{S} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$$

i $\mathbf{S} = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_r)$, gdzie $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > 0$.

Liczby $\sigma_1, \sigma_2, \dots, \sigma_r$ razem z $\sigma_{r+1} = 0, \dots, \sigma_L = 0$ są nazywane wartościami osobliwymi macierzy \mathbf{H} , są one nieujemnymi pierwiastkami kwadratowymi wartości własnych (które są nieujemne) $\mathbf{H}^T\mathbf{H}$. Kolumny macierzy \mathbf{U} nazywane są lewymi wektorami osobliwymi \mathbf{H} (są to ortonormalne wektory własne $\mathbf{H}\mathbf{H}^T$), a kolumny \mathbf{V} są nazywane prawymi wektorami osobliwymi \mathbf{H} (są to ortonormalne wektory własne $\mathbf{H}^T\mathbf{H}$)

Uwaga 6.10. *Pseudoodwrotność macierzy \mathbf{H} obliczamy z następującego równania:*

$$\mathbf{H}^+ = \mathbf{V}\mathbf{\Sigma}^+\mathbf{U}^T, \text{ gdzie } \mathbf{\Sigma}^+ = \begin{bmatrix} \mathbf{S}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

6.4.2 SVD-ELM

Rozważmy zatem zbiór treningowy $N = \{(x_i, y_i) | x_i \in \mathbb{R}^n, y_i \in \mathbb{R}^m, i = 1, \dots, N\}$, funkcje aktywacji $g(x)$ oraz L ukrytych neuronów. Możemy teraz rozłożyć algorytm na trzy kluczowe etapy.

Krok 1:

Zaczynamy od losowego przypisania wag wejściowych w_i oraz biasu $b_i (i = 1, \dots, L)$.

Krok 2:

Obliczamy macierz warstwy ukrytej opisanej jako $\mathbf{H} \in \mathbb{R}^{N \times L}$.

Krok 3:

Obliczamy wagę wyjściową $\beta \in \mathbb{R}^{L \times m}$:

$$\beta = \mathbf{H}^+ \mathbf{Y},$$

gdzie $\mathbf{Y} = [y_1, \dots, y_N]^T \in \mathbb{R}^{N \times m}$.

Bibliografia

- [1] P.L. Bartlett *The sample complexity of pattern classification with neural networks: the size of the weights is more important than the size of the network*, IEEE Transactions on Information Theory, March 1998
- [2] Lipo P. Wang, Chunru R. Wan, *Comments on "The Extreme Learning Machine"*, IEEE Transactions on Neural Networks, August 2008
- [3] Guang-Bin Huang, Qin-Yu Zhu, Chee-Kheong Siew *Extreme learning machine: Theory and applications*, Neurocomputing, December 2006
- [4] Shuxia Lu, Xizhao Wang, Guiqiang Zhang, Xu Zhou *Effective algorithms of the Moore-Penrose inverse matrices for extreme learning machine*, Intelligent Data Analysis, July 2015

- [5] Jian Wang, Siyuan Lu, Shui-Hua Wang, Yu-Dong Zhang, *A review on extreme learning machine*, IEEE Transactions on Neural Networks, May 2021

Wyznaczanie obrazu numerycznego macierzy

Łukasz Gorczyca

Uniwersytet Jagielloński

Wydział Matematyki i Informatyki

7.1 Definicje i podstawowe własności

7.1.1 Definicje obrazu numerycznego

Definicja 7.1. Obraz numeryczny operatora T w zespolonej przestrzeni Hilberta \mathcal{H} jest podzbiorem płaszczyzny zespolonej określonym wzorem:

$$W(T) = \{\langle Tx, x \rangle \mid x \in \mathcal{H}, \|x\| = 1\}$$

dla danego iloczynu skalarnego $\langle \cdot, - \rangle$ oraz normy indukowanej $\|x\| = \sqrt{\langle x, x \rangle}$.

Od tej pory przez A będziemy oznaczać dowolną macierz ze zbioru macierzy kwadratowych o wartościach zespolonych i n kolumnach (oznaczanego też przez $\mathcal{M}_n(\mathbb{C})$). Dla dowolnego wektora $x \in \mathbb{C}^n$, przez x^* oznaczamy sprzężenie hermitowskie wektora x . Dla $x = [x_1, \dots, x_n]^T$ mamy $x^* = [\bar{x}_1, \dots, \bar{x}_n]$, gdzie dla $y \in \mathbb{C}$, $\bar{y} = \text{Re}(y) - i \text{Im}(y)$ oznacza sprzężenie zespolone.

Uwaga 7.2. Dla x, x^* zdefiniowanych jak wyżej, wyrażenie $x^*x = \sum_{i=1}^n x_i \bar{x}_i$ jest liczbą zespoloną. Dodatkowo, dla macierzy

$A = [a_{ij}]$ zdefiniowanej jak wyżej, otrzymujemy

$$x^*Ax = \sum_{j=1}^n \sum_{i=1}^n a_{ji} \bar{x}_i x_j \in \mathbb{C}.$$

Przestrzeń liczb zespolonych (n wymiarowa) z iloczynem skalarnym oraz normą indukowaną jest przestrzenią Hilberta. Możemy więc przenieść pierwotną definicję obrazu numerycznego na język macierzy zespolonych. W tej pracy skupimy się tylko na obrazie numerycznym we wspomnianej przestrzeni.

Definicja 7.3. Obraz numeryczny macierzy A określamy przy pomocy normy $\|x\| = \sqrt{x^*x}$, wtedy:

$$W(A) = \{x^*Ax : x \in \mathbb{C}^n, x^*x = 1\} = \left\{ \frac{x^*Ax}{x^*x} : x \in \mathbb{C}^n, x \neq 0 \right\}.$$

Przydatne będzie również zdefiniowanie powiązanych z obrazem numerycznym pojęć. Promień numeryczny i wewnętrzny promień numeryczny wyznaczają wartości, które mówią o tym jak dana macierz jest rozpięta.

Definicja 7.4. Promień numeryczny macierzy A jest określony jako:

$$r(A) = \max\{|z| : z \in W(A)\}.$$

Definicja 7.5. Wewnętrzny promień numeryczny macierzy A jest określony jako:

$$\bar{r}(A) = \max\{|z| : z \in \partial W(A)\}.$$

Otoczka wypukła pewnego zbioru jest natomiast najmniejszym zbiorem wypukłym, który zawiera ten zbiór. W dalszej części pracy pokażemy, że obraz numeryczny macierzy jest wypukły, dlatego otoczka wypukła będzie nam bardzo przydatna.

Definicja 7.6. Otoczką wypukłą zbioru P nazywamy zbiór

$$CH\{A\} = \{tp_1 + (1-t)p_2 : t \in [0, 1], p_1, p_2 \in P\}.$$

7.1.2 Własności obrazu numerycznego

Jedną z podstawowych własności obrazu numerycznego macierzy jest jego zwartość. Obraz numeryczny zawiera swoje domknięcie, jak również zawsze jest ograniczony, co czyni go zwartym.

Obraz numeryczny macierzy A jest liniowy, w takim sensie, że dla dowolnego $a \in \mathbb{C}$ zachodzi $W(aA) = aW(A)$. Weźmy też $b \in \mathbb{C}$, a przez I_n oznaczmy macierz identycznościową o n niezerowych wartościach. Obraz numeryczny spełnia własność translacji, w tym sensie, że $W(aA + bI) = aW(A) + b$. Jeśli zarówno A jak i B są ze zbioru $\mathcal{M}_n(\mathbb{C})$, to zachodzi inkluzja $W(A + B) \subseteq W(A) + W(B)$.

Popularnym faktem z algebry liniowej jest możliwość przedstawienia macierzy kwadratowej jako sumę macierzy hermitowskiej (spełniającej $M = M^*$) i antyhermitowskiej (spełniającej $M = -M^*$). Dla naszej macierzy A ten rozkład wygląda następująco:

$$A = \frac{A + A^*}{2} + \frac{A - A^*}{2}.$$

Okazuje się, że taki rozkład można wykorzystać do podzielenia obrazu numerycznego macierzy na jego rzeczywistą i urojoną część, a mianowicie zachodzi

$$\operatorname{Re}W(A) = W\left(\frac{A + A^*}{2}\right), \quad \operatorname{Im}W(A) = W\left(\frac{A - A^*}{2}\right).$$

Obraz numeryczny macierzy jest rzeczywisty, to znaczy $\operatorname{Im}W(A) = 0$ (równoważnie $W(A) \subset \mathbb{R}$), tylko wtedy, gdy macierz A jest hermitowska, czyli $A = A^*$. W takim przypadku, punkty końcowe obrazu numerycznego wyznaczają najmniejszą i największą wartość własną tej macierzy.

Obraz numeryczny jest taki sam dla macierzy transponowanej. W przypadku sprzężenia hermitowskiego macierzy, jej obraz numeryczny jest sprzężeniem zespolonym obrazu numerycznego wyjściowej macierzy, to znaczy

$$W(A^T) = W(A), \quad W(A^*) = \overline{W(A)}.$$

Pojawia się pytanie, jaki jest związek pomiędzy obrazem numerycznym, a otoczką wypukłą? W celu odpowiedzenia na to pytanie wprowadzimy definicję spektrum i promienia spektralnego macierzy.

Definicja 7.7. Spektrum macierzy A to zbiór wszystkich wartości własnych tej macierzy,

$$\sigma(A) = \{\lambda : \lambda \text{ jest wartością własną macierzy } A\}.$$

Definicja 7.8. Promień spektralny macierzy A jest określony jako:

$$\rho(A) = \max\{|z| : z \in \sigma(A)\}.$$

Okazuje się, że zawsze mamy inkluzję $CH(\sigma(A)) \subseteq W(A)$, a równość $CH(\sigma(A)) = W(A)$ zachodzi tylko w przypadku, gdy A jest dodatkowo hermitowska.

7.2 Wypukłość

W celu udowodnienia wypukłości obrazu numerycznego pokażemy najpierw lemat mówiący o drogowej spójności zbiorów unormowanych wektorów, które tworzą obraz numeryczny o określonej wartości. Najpierw przypomnijmy pojęcie wspomnianego rodzaju spójności.

Definicja 7.9. Zbiór P nazywamy **drogowo spójnym**, gdy dowolnie wybrane punkty $p_1, p_2 \in P$ mogą być połączone ciągłą krzywą zawierającą się w całości w zbiorze P .

Lemat 7.10. *Niech A będzie macierzą hermitowską oraz niech $\mu \in W(A)$. Wtedy zbiór:*

$$\mathcal{L}_A(\mu) := \{x \in \mathbb{C}^n : x^*x = 1, x^*Ax = \mu\}$$

jest drogowo spójny.

Dowód. Bez straty ogólności zakładamy, że $\mu = 0$ oraz macierz A jest diagonalna o rzeczywistych wartościach, tj. $A = \text{diag}(d_1, \dots, d_n)$, wtedy:

$$W(A) = \left\{ \sum_{i=1}^n d_i |x_i|^2 : x_1, x_2, \dots, x_n \in \mathbb{C}, \sum_{i=1}^n |x_i|^2 = 1 \right\}.$$

Założmy, że $x = (x_i)$, $y = (y_i) \in \mathcal{L}_A(0)$, tzn. x oraz y są wektorami jednostkowymi takimi, że

$$\sum_{i=1}^n d_i |x_i|^2 = \sum_{i=1}^n d_i |y_i|^2 = 0.$$

Pokażemy, że możemy połączyć x i y za pomocą ciągłej krzywej zawierającej się w zbiorze $\mathcal{L}_A(0)$. Wektor $[r_1 e^{i\theta_1}, \dots, r_n e^{i\theta_n}]^T \in \mathcal{L}_H(0)$ dla nieujemnych r_j oraz $\theta_k \in [0, 2\pi)$ dla $k = 1, 2, \dots, n$ jest połączony z wektorem $[r_1, \dots, r_n]^T \in \mathcal{L}_H(0)$ ciągłą krzywą daną wzorem $[r_1 e^{i\theta_1(1-t)}, \dots, r_n e^{i\theta_n(1-t)}]^T$, $t \in [0, 1]$ zawiera się w $\mathcal{L}_H(0)$. Możemy więc założyć, że x i y są rzeczywiste i nieujemne ze względu na wszystkie współrzędne. W takim wypadku, rozwiązaniem spełniającym warunki $u(0) = x$, $u(1) = y$ jest krzywa $u(t) = \left(\sqrt{(1-t)x_i^2 + ty_i^2} \right)$.

Pokażemy teraz silniejszą własność obrazu numerycznego macierzy, a mianowicie wypukłość.

Twierdzenie 7.11 (Toeplitz-Hausdorff). *Dla dowolnej macierzy A jej obraz numeryczny $W(A)$ jest wypukły.*

Pokażemy, że odcinek łączący dwa dowolne różne punkty z $W(A)$ zawiera się w $W(A)$. Bez straty ogólności możemy przyjąć, że te punkty to $p = 0$ oraz $q = 1$ (korzystając z własności translacji obrazu numerycznego). Teraz wystarczy pokazać, że $[0, 1] \subseteq W(A)$. Weźmy $x, y \in \mathbb{C}^n$ takie, że $\|x\| = 1 = \|y\|$ oraz $p = x^* A x$, $q = y^* A y$. Oczywiście $A = H(A) + S(A)$, gdzie $H(A)$ oznacza część hermitowską, a $S(A)$ część antyhermitowską macierzy A . Korzystając z poprzedniego lematu mamy drogową

spójność zbioru $\mathcal{L}_{S(A)(0)}$. Zauważmy, że $x, y \in \mathcal{L}_{S(A)}(0)$.

Dla $t \in [0, 1]$ istnieje ciągle odwzorowanie

$z_t : [0, 1] \ni t \rightarrow z(t) \in \mathcal{L}_{S(A)}(0)$, wówczas $z_0 = x$, $z_1 = y$.

W takim razie $z_0^* A z_0 = 1$ oraz $z_1^* A z_1 = 0$. Mamy, że

$$z_t^* A z_t = z_t^* H(A) z_t$$

jest rzeczywistą i ciąglą funkcją, więc oznacza to, że odcinek pomiędzy p a q leży w $W(A)$, co dowodzi wypukłości obrazu numerycznego.

7.3 Dalsze własności obrazu numerycznego

Stwierdzenie 7.12. *Dla macierzy A zachodzą następujące własności:*

1. $W(A) = \{\mu\} \iff A = \mu I_n$.
2. $W(A) = \partial W(A) \iff \frac{1}{n} \operatorname{tr}(A) = \frac{1}{n} \sum_{i=1}^n a_{ii} \in \partial W(A)$.

Definicja 7.13. Punkt brzegowy μ zamkniętego obszaru $\Omega \subset \mathbb{C}$, czyli $\mu \in \partial\Omega$ nazywamy **narożnikiem zbioru Ω** , gdy istnieje

$\epsilon > 0$ taki, że zbiór $K(\mu, \epsilon) := \Omega \cap S(\mu, \epsilon)$

(dla $S(\mu, \epsilon) := \{z \in \mathbb{C} : |z - \mu| \leq \epsilon\}$) zawiera się w wycinku koła $S(\mu, \epsilon)$ o kącie mniejszym niż π .

Przykład 7.14. *Dla $A \in \mathcal{M}_n(\mathbb{C})$ zachodzi*

$$\mu \text{ - narożnik } W(A) \implies \mu \in \sigma(A).$$

Uwaga 7.15. *Wynikanie w drugą stronę nie zachodzi w ogólności, czyli nie każda wartość własna macierzy A na brzegu jej obrazu numerycznego musi być jego narożnikiem.*

Stwierdzenie 7.16. *Każda wartość własna μ macierzy A na brzegu jej obrazu numerycznego jest półprostą, to znaczy, że krotność algebraiczna jest równa jej krotności geometrycznej.*

Stwierdzenie 7.17. *Każdy wektor własny macierzy A odpowiadający μ jest ortogonalny do wektorów własnych A odpowiadających wartościom własnym ze zbioru $\sigma(A) \setminus \{\mu\}$.*

7.4 Wyznaczanie obrazu numerycznego

7.4.1 Wersja prymitywna

Metoda ta polega na losowym wybraniu wektorów unormowanych $\{x_i\}_i \in I$ i policzeniu wyrażeń $x_i^*Ax_i$ dla ustalonej wcześniej macierzy kwadratowej A oraz $i \in I$. Wadą tego sposobu jest bardzo duża liczba obliczeń potrzebnych do otrzymania sensownego rysunku. Dodatkowo, nie mamy dokładnej informacji na temat brzegu obrazu numerycznego.

7.4.2 Aproksymacja wielokątami - zastosowanie twierdzenia Toeplitza-Hausdorffa

Jeśli zauważymy, że dla macierzy A jej obraz numeryczny jest wypukły to możemy jego brzeg przybliżyć pewnymi wielokątami wypukłymi. Jak pokazywaliśmy m.in. w dowodzenie twierdzenia Toeplitza-Hausdorffa, $W(H(A)) = [\lambda_{\min}(H(A)), \lambda_{\max}(H(A))]$ jest zamkniętym przedziałem o wartościach rzeczywistych o końcach przedziału będącymi ekstremalnymi wartościami własnymi macierzy $H(A)$. Z własności obrazu numerycznego mamy, że $\text{Re}W(A) = W(H(A))$, skąd wynika, że dla dowolnego unormowanego $x \in \mathbb{C}^n$, punkt $\mu = x^*Ax$ spełnia równość $\text{Re}(\mu) = \max\{\text{Re}\lambda : \lambda \in W(A)\}$ wtedy i tylko wtedy, gdy

$$\text{Re}\mu = \text{Re}(x^*Ax) = x^*H(A)x = \lambda_{\max}(H(A)).$$

Z drugiej strony $x^*H(A)x = \lambda_{\max}(H(A))$ wtedy i tylko wtedy, gdy x jest unormowanym wektorem własnym $H(A)$ odpowiadającym największej wartości własnej tej macierzy. W tym przypadku, $\mu = x^*Ax$ odpowiada punktowi najbardziej wysuniętemu na prawą stronę płaszczyzny spośród elementów $W(A)$. W związku z tym, prosta $\{u + iv : u, v \in \mathbb{R}, u = \lambda_{\max}(H(A))\}$ jest linią podpierającą (supporting line) $W(A)$ w μ .

Dla dowolnego $\theta \in [0, 2\pi)$ rozważmy macierze $e^{i\theta}A = (\cos \theta + i \sin \theta)A$, $H(e^{i\theta}A) = \cos(\theta)H(A) + \sin \theta(iS(A))$,

wartość własną $\lambda_\theta = \lambda_{\max}(H(e^{i\theta}A))$ oraz odpowiadający jej unormowany wektor własny x_θ taki, że

$$H(e^{i\theta}A)x_\theta = \lambda_\theta x_\theta \text{ oraz } x_\theta^* x_\theta = 1.$$

Przez to, że $\{i + iv : u, v \in \mathbb{R}, u = \lambda_\theta\}$ jest linią podpierającą $W(e^{i\theta}A)$ w punkcie $x_\theta^*(e^{i\theta}A)x_\theta$, widać, że

$$e^{-i\theta} = \{u + iv : u, v \in \mathbb{R}, u = \lambda_\theta\},$$

równoważnie $\{u + iv : u, v \in \mathbb{R}, u \cos \theta - v \sin \theta = \lambda_\theta\}$ jest linią podpierającą $W(A)$ w $x_\theta^*Ax_\theta$. Wybierając ρ różnych wartości takich, że $0 = \theta_1 < \theta_2 < \dots < \theta_{\rho+1} = 2\pi$, możemy przybliżyć $W(A)$ jako wpisany wielokąt wypukły $\mathcal{Q}(\theta_1, \theta_2, \dots, \theta_\rho)$ o wierzchołkach

$$q_j = x_{\theta_j}^*Ax_{\theta_j} \text{ dla } j = 1, 2, \dots, \rho$$

oraz jako opisany wielokąt wypukły $\mathcal{P}(\theta_1, \theta_2, \dots, \theta_\rho)$ o wierzchołkach

$$p_j = e^{-i\theta_j} \left[\lambda_{\theta_j} + \frac{\lambda_{\theta_j} \cos(\theta_{j+1} - \theta_j) - \lambda_{\theta_{j+1}}}{\sin(\theta_{j+1} - \theta_j)} \right], \quad j = 1, 2, \dots, \rho.$$

Wprowadźmy pomocnicze oznaczenie na różnicę pól wielokątów,

$$\delta_V(\rho) := V(\mathcal{P}(\theta_1, \theta_2, \dots, \theta_\rho)) - V(\mathcal{Q}(\theta_1, \theta_2, \dots, \theta_\rho)).$$

Zauważmy, że wierzchołki wielokąta wpisanego $\mathcal{P}(\theta_1, \theta_2, \dots, \theta_\rho)$ są łatwo obliczane, gdyż są przecięciami punktów linii podpierających obraz numeryczny macierzy. Zwiększając liczbę podziałów ρ sprawiamy, że różnica powierzchni

$$\delta_V(\rho) = \frac{1}{2} \operatorname{Im} \left[\sum_{j=1}^{\rho-1} (\bar{p}_j p_{j+1} - \bar{q}_j q_{j+1}) - (\bar{p}_\rho) p_1 - \bar{q}_\rho q_1 \right]$$

jest wystarczająco mała.

7.4.3 Algorytm wyznaczający obraz numeryczny

1. Wybieramy $0 = \theta_1 < \theta_2 < \dots < \theta_\rho < \theta_{\rho+1} = 2\pi$.
2. Dla $j = 1, 2, \dots, \rho$:
 - (a) Obliczamy wartość własną $\lambda_j = \lambda_{\max}(H(e^{i\theta_j} A))$,
 - (b) Obliczamy wektor własny $x_j = x_{\theta_j}$ odpowiadający λ_j ,
 - (c) Obliczamy j -ty wierzchołek wielokąta $\mathcal{Q}(\theta_1, \theta_2, \dots, \theta_\rho)$, czyli $q_j = x_j^* A x_j$,
 - (d) Obliczamy j -ty wierzchołek wielokąta $\mathcal{P}(\theta_1, \theta_2, \dots, \theta_\rho)$, czyli

$$p_j = e^{i\theta_j} \left[\lambda_{\theta_j} + \frac{\lambda_{\theta_j} \cos(\theta_{j+1} - \theta_j) - \lambda_{\theta_{j+1}}}{\sin(\theta_{j+1} - \theta_j)} \right].$$

3. Aby "domknąć" wielokąty, zakładamy, że $p_{\rho+1} = p_1$ oraz $q_{\rho+1} = q_1$, a następnie wyznaczamy różnicę powierzchni między wielokątami, tj zdefiniowane wcześniej $\delta_V(\rho)$.
4. Jeśli różnica $\delta_V(\rho)$ jest dostatecznie mała, wykreślamy $\mathcal{P}(\theta_1, \theta_2, \dots, \theta_\rho)$. W przeciwnym razie wracamy do kroku pierwszego i wybieramy podział składający się z większej liczby wierzchołków.

Bibliografia

- [1] Psarrakos J.P., Tsatsomereos M.J., *Numerical range: (in) a matrix nutshell*, August 12, 2002.
- [2] Benzi M., *Some uses of the field of values in numerical analysis*, Bollettino dell'Unione Matematica Italiana (2021) 14:159-177.
- [3] <https://numericalshadow.org/>

Rzut oka na klasyfikację szeregów

Paulina Ewa Hennig

Uniwersytet Szczeciński
Instytut Matematyki

8.1 Wstęp

Podczas podróży przez tę pracę będziemy przemieszczać się po obszarze klasycznej analizy rzeczywistej. Na starcie zaczniemy od założeń, w tym przypadku od pewnego ograniczenia. To znaczy interesować nas będą szeregi rzeczywiste, a dokładniej te z nich, które spełniają warunek konieczny zbieżności. Są to oczywiście te, dla których wyraz ogólny dąży do 0. Jak wynika z tytułu artykułu, naszym celem jest podzielenie ich w pewien sposób, w szczególności tak, żeby ten podział dostarczył jakąś istotną informację. Powstaną nam trzy grupy, które po kolei omówię.

8.2 Szeregi mocno rozbieżne

Definicja 8.1. Szereg liczbowy o wyrazach rzeczywistych $\sum_{n=1}^{\infty} a_n$ określa się jako **mocno rozbieżny** (z ang. *strongly divergent*), jeśli dla dowolnej permutacji $\pi : \mathbb{N} \longleftrightarrow \mathbb{N}$ szereg $\sum_{n=1}^{\infty} a_{\pi(n)}$ jest rozbieżny.

Powyższa definicja oznacza, że w szeregu mocno rozbieżnym nieistotna okaże się kolejność ustawienia jego wyrazów, ponieważ za każdym razem otrzymujemy po prostu szereg rozbieżny.

Niestety warunek z Definicji 8.1 nie jest łatwy do sprawdzenia, przez co w praktyce chcielibyśmy mieć bardziej użyteczny opis. Okazuje się, że taki istnieje i idealnie rozgranicza między sobą wszystkie trzy typy szeregów. Do wprowadzenia go konieczne jest przypomnienie sobie definicji szeregów $\sum a_n^-$ oraz $\sum a_n^+$.

Rozważmy zatem dowolny (w tym miejscu nie potrzebujemy ograniczać się do tego, żeby wyraz ogólny dążył do 0) szereg

$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + a_3 + a_4 + a_5 + \dots$. Generując na jego podstawie szereg $\sum a_n^-$ zostawiamy bez zmian te a_i , które są mniejsze od 0, natomiast pozostałe zastępujemy zerami. Dla przypadku szeregu $\sum a_n^+$ jest podobnie. Tu jednak zachowujemy wszystkie a_i , które są większe od 0, a pozostałe zastępujemy zerami.

W skrócie: $\sum a_n^-$ lubi $a_i < 0$, toleruje $a_i = 0$ i nie dopuszcza $a_i > 0$. Szereg $\sum a_n^+$ odwrotnie.

Przykład 8.2.

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} \frac{(-2)^n}{n!} = -2 + 2 - \frac{8}{6} + \frac{16}{24} - \frac{32}{120} + \dots,$$

$$\sum_{n=1}^{\infty} a_n^- = -2 + 0 - \frac{8}{6} + 0 - \frac{32}{120} + \dots,$$

$$\sum_{n=1}^{\infty} a_n^+ = 0 + 2 + 0 + \frac{16}{24} + 0 + \dots$$

Wróćmy teraz do zagadnienia szeregów mocno rozbieżnych.

Twierdzenie 8.3. Szereg liczbowy rzeczywisty $\sum_{n=1}^{\infty} a_n$ jest mocno rozbieżny wtedy i tylko wtedy, gdy dokładnie jeden z szeregów: $\sum_{n=1}^{\infty} a_n^-$, $\sum_{n=1}^{\infty} a_n^+$ jest zbieżny, a drugi rozbieżny.

Zobaczymy na przykładzie, że warunek z tego twierdzenia jest szybki i wygodny w użyciu.

Przykład 8.4. *Rozważmy szereg postaci*

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} \frac{6n^2 + 8}{2n^3 - n} = \frac{14}{1} + \frac{32}{14} + \frac{62}{51} + \frac{104}{124} + \dots$$

(i zauważmy, że jego wyraz ogólny dąży do 0).

$\sum_{n=1}^{\infty} a_n^- = \sum_{n=1}^{\infty} 0 = 0$ - istnieje skończona suma, czyli $\sum_{n=1}^{\infty} a_n^-$ jest zbieżny.

$$\sum_{n=1}^{\infty} a_n^+ = \sum_{n=1}^{\infty} \frac{6n^2 + 8}{2n^3 - n} \quad \text{oraz mamy} \quad \frac{6n^2 + 8}{2n^3 - n} > \frac{6n^2}{2n^3} > \frac{1}{n}.$$

Pamiętamy, że szereg $\sum \frac{1}{n}$ jest rozbieżny oraz zachodzą powyższe nierówności, zatem na mocy kryterium porównawczego $\sum_{n=1}^{\infty} a_n^+$ jest też rozbieżny. Wobec tego w oparciu o Twierdzenie 8.3 szereg $\sum_{n=1}^{\infty} \frac{6n^2+8}{2n^3-n}$ jest mocno rozbieżny.

Mając scharakteryzowany jeden szereg jesteśmy w stanie bez wysiłku generować inne (podobne). Jest to cudowna rozrywka. Zatem popatrzymy na następne przykłady szeregów mocno rozbieżnych. Choć ich wygląd na może odstraszać, to zachowują się one tak samo, jak ten rozpisany wyżej.

$$\begin{aligned} & \sum_{n=1}^{\infty} \frac{18n^{18} + 5}{4n^{19} - 3}, \\ & \sum_{n=1}^{\infty} \frac{101 \cdot n^{100} + 101}{100 \cdot n^{101} - n}, \\ & \sum_{n=1}^{\infty} \frac{2^{10} \cdot n^{(2^{10}-1)}}{(2^{10} - 1) \cdot n^{(2^{10})} - 2^9}, \\ & \sum_{n=1}^{\infty} \frac{8! \cdot n^{7!} + 6!}{5! \cdot n^{7!+1} - 4!}. \end{aligned}$$

8.3 Szeregi mające długą nazwę, czyli potencjalnie względnie zbieżne

Definicja 8.5. Szereg liczbowy o wyrazach rzeczywistych $\sum_{n=1}^{\infty} b_n$ będziemy nazywać **potencjalnie względnie zbieżnym** (z ang. *potentially non-absolutely convergent*), jeśli istnieją permutacje jego wyrazów $\pi_1, \pi_2 : \mathbb{N} \longleftrightarrow \mathbb{N}$ takie, że zbieżny jest szereg $\sum_{n=1}^{\infty} b_{\pi_1(n)}$, natomiast $\sum_{n=1}^{\infty} b_{\pi_2(n)}$ jest rozbieżny.

Podobnie jak dla szeregów mocno rozbieżnych, tutaj także istnieje inny opis za pomocą $\sum b_n^-$ oraz $\sum b_n^+$.

Twierdzenie 8.6. Szereg rzeczywisty $\sum_{n=1}^{\infty} b_n$ jest potencjalnie względnie zbieżny wtedy i tylko wtedy, gdy oba szeregi: $\sum_{n=1}^{\infty} b_n^-$ oraz $\sum_{n=1}^{\infty} b_n^+$ są rozbieżne.

Przykład 8.7. Rozważmy następujący szereg

$$\begin{aligned} \sum_{n=1}^{\infty} b_n &= \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n_1 - 1} + \frac{1}{n_1} - 1 + \\ &+ \frac{1}{n_1 + 1} + \frac{1}{n_1 + 2} + \dots + \frac{1}{n_2} - \frac{1}{2} + \\ &+ \frac{1}{n_2 + 1} + \frac{1}{n_2 + 2} + \dots + \frac{1}{n_3} - \frac{1}{3} + \dots \quad , \end{aligned}$$

gdzie n_1 jest takie, że $\frac{1}{1} + \dots + \frac{1}{n_1} > 2$ (oczywiście istnieje takie n_1 , bo szereg $\sum \frac{1}{n}$ jest rozbieżny);

n_2 jest takie, że $\frac{1}{n_1+1} + \dots + \frac{1}{n_2} > 3$;

n_3 jest takie, że $\frac{1}{n_2+1} + \dots + \frac{1}{n_3} > 4$; itd.

Co więcej można zauważyć, że $b_n \rightarrow 0$.

Próbując użyć ostatniego twierdzenia, patrzymy teraz na szereg

$$\sum_{n=1}^{\infty} b_n^- = 0 + \dots + 0 - 1 + 0 + \dots + 0 - \frac{1}{2} + 0 + \dots + 0 - \frac{1}{3} + \dots \quad .$$

Pisząc w pełni formalnie, tych wszystkich zer nie możemy po prostu opuścić. Możemy za to utworzyć nowy szereg:

$$\sum_{n=1}^{\infty} B_n^- = -1 - \frac{1}{2} - \frac{1}{3} - \dots = \sum_{n=1}^{\infty} -\frac{1}{n}.$$

Zaobserwujemy, że szeregi $\sum_{n=1}^{\infty} b_n^-$ oraz $\sum_{n=1}^{\infty} B_n^-$ zachowują się tak samo. Dodatkowo wiemy, że szereg $\sum_{n=1}^{\infty} -\frac{1}{n}$ jest rozbieżny, zatem

$\sum_{n=1}^{\infty} b_n^-$ też musi być rozbieżny.

W przypadku szeregu $\sum_{n=1}^{\infty} b_n^+$ postąpimy tak samo, jak przy

$\sum_{n=1}^{\infty} b_n^-$, czyli utworzymy pomocniczy szereg.

$$\begin{aligned} \sum_{n=1}^{\infty} b_n^+ &= \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n_1 - 1} + \frac{1}{n_1} + 0 + \\ &+ \frac{1}{n_1 + 1} + \dots + \frac{1}{n_2} + 0 + \frac{1}{n_2 + 1} + \dots + \frac{1}{n_3} + 0 + \dots \end{aligned}$$

oraz

$$\begin{aligned} \sum_{n=1}^{\infty} B_n^+ &= \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n_1} + \frac{1}{n_1 + 1} + \dots + \frac{1}{n_2} + \\ &+ \frac{1}{n_2 + 1} + \dots + \frac{1}{n_3} + \dots = \sum_{n=1}^{\infty} \frac{1}{n}. \end{aligned}$$

Szeregi $\sum_{n=1}^{\infty} B_n^+$ i $\sum_{n=1}^{\infty} b_n^+$ zachowują się tak samo oraz szereg $\sum_{n=1}^{\infty} \frac{1}{n}$

jest rozbieżny, więc $\sum_{n=1}^{\infty} b_n^+$ też musi być rozbieżny.

Z uzyskanych informacji mamy, że oba pomocnicze szeregi $\sum_{n=1}^{\infty} b_n^-$ i $\sum_{n=1}^{\infty} b_n^+$ są rozbieżne, zatem po użyciu Twierdzenia 8.6 dostajemy, że szereg $\sum_{n=1}^{\infty} b_n$ jest potencjalnie względnie zbieżny.

Istotnie, wyjściowy szereg $\sum_{n=1}^{\infty} b_n$ ze swojej konstrukcji wydaje się być rozbieżny, jednak jesteśmy w stanie tak przestawić wszystkie jego wyrazy, że otrzymamy $1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \dots$, co daje zbieżność do sumy równej 0.

Szeregi potencjalnie względnie zbieżne mają z reguły bardziej rozbudowany opis, przez co trudno generować różne podobne do siebie przykłady. Ale między innymi odwołując się do szeregu $\sum_{n=1}^{\infty} b_n$ z Przykładu 8.7 i zmieniając w nim liczniki wszystkich ułamków (zastępując jedynki inną niezerową liczbą rzeczywistą), otrzymamy nowy szereg potencjalnie względnie zbieżny.

8.4 Szeregi bezwzględnie zbieżne

Ostatnią grupą szeregów, które idealnie dopełniają klasyfikację, są dobrze znane szeregi bezwzględnie zbieżne. Ich podstawowa definicja oznacza tyle, że szereg modułów jest zbieżny. Możemy jednak patrzeć inaczej.

Definicja 8.8. Szereg liczbowy rzeczywisty $\sum_{n=1}^{\infty} c_n$ nazwiemy **bezwzględnie zbieżnym** (z ang. *absolutely convergent*), jeśli biorąc dowolną permutację jego wyrazów $\pi : \mathbb{N} \leftarrow \mathbb{N}$, szereg $\sum_{n=1}^{\infty} c_{\pi(n)}$ będzie zbieżny.

Przy wyjściowym założeniu z początku artykułu ($c_n \rightarrow 0$) okazuje się, że Definicja 8.8 jest równoważna temu, że $\sum_{n=1}^{\infty} |c_n|$ jest zbieżny. Nie jest to jednak powód, dla którego to ograniczenie zostało wprowadzone.

Warunek z Definicji 8.8 jest niestety ponownie w większości przypadków ciężki do sprawdzenia, przez co znowu z pomocą przyjdą szeregi $\sum_{n=1}^{\infty} c_n^-$ oraz $\sum_{n=1}^{\infty} c_n^+$.

Twierdzenie 8.9. Szereg rzeczywisty $\sum_{n=1}^{\infty} c_n$ jest bezwzględnie zbieżny wtedy i tylko wtedy, gdy oba szeregi: $\sum_{n=1}^{\infty} c_n^-$, $\sum_{n=1}^{\infty} c_n^+$ są zbieżne.

Przykład 8.10. Rozważmy następujący szereg, w którym wyraz ogólny dąży do 0:

$$\sum_{n=1}^{\infty} c_n = \sum_{n=1}^{\infty} \frac{9 \cdot (-1)^n}{n^9} = -\frac{9}{1^9} + \frac{9}{2^9} - \frac{9}{3^9} + \frac{9}{4^9} - \frac{9}{5^9} + \dots$$

Ma on naprzemienny znak. Możemy zobaczyć, że

$$\sum_{n=1}^{\infty} c_n^- = -\frac{9}{1^9} + 0 - \frac{9}{3^9} + 0 - \frac{9}{5^9} + \dots$$

Z jednej strony $\sum_{n=1}^{\infty} c_n^- = \sum_{n=1}^{\infty} -9 \cdot \frac{(-1)^{n+1} + 1}{2 \cdot n^9}$. My jednak zbieżność $\sum_{n=1}^{\infty} c_n^-$ wykażemy szybciej poprzez porównanie z zachowującym się tak samo szeregiem

$$\sum_{n=1}^{\infty} C_n^- = -\frac{9}{1^9} - \frac{9}{3^9} - \frac{9}{5^9} - \dots = -9 \cdot \sum_{n=1}^{\infty} \frac{1}{(2n-1)^9}$$

Szereg $\sum_{n=1}^{\infty} \frac{1}{n^9}$ jest zbieżny oraz $\frac{1}{(2n-1)^9} \leq \frac{1}{n^9}$, więc na mocy kryterium porównawczego i własności szeregów otrzymujemy, że $\sum_{n=1}^{\infty} C_n^-$ jest zbieżny (a co za tym idzie $\sum_{n=1}^{\infty} c_n^-$ także).

Z $\sum_{n=1}^{\infty} c_n^+ = 0 + \frac{9}{2^9} + 0 + \frac{9}{4^9} + \dots$ postępujemy analogicznie.

Definiujemy $\sum_{n=1}^{\infty} C_n^+ = \frac{9}{2^9} + \frac{9}{4^9} + \dots = 9 \cdot \sum_{n=1}^{\infty} \frac{1}{(2n)^9}$. Dodatkowo $\frac{1}{(2n)^9} < \frac{1}{n^9}$, więc (kryterium porównawcze i własności szeregów) $\sum_{n=1}^{\infty} C_n^+$, a także $\sum_{n=1}^{\infty} c_n^+$ są zbieżne. Zatem na mocy Twierdzenia 8.9 szereg $\sum_{n=1}^{\infty} \frac{9 \cdot (-1)^n}{n^9}$ jest bezwzględnie zbieżny.

Spójrzmy teraz na kilka podobnych szeregów bezwzględnie zbieżnych. Wbrew pierwszemu wrażeniu możemy rozpatrywać je dokładnie tak samo, jak szereg w Przykładzie 8.10.

$$\sum_{n=1}^{\infty} \frac{\sqrt{2} \cdot (-1)^{n+1}}{n^{99}},$$

$$\sum_{n=1}^{\infty} \frac{(-1)^{123n}}{123n^{123}},$$

$$\sum_{n=1}^{\infty} \frac{(\pi + 1) \cdot (-1)^{n^2}}{\pi n^2}.$$

8.5 Zastosowanie

Informacja do jakiej klasy zakwalifikujemy dany szereg powie nam o wyglądzie zbioru osiągalnego dla tego szeregu.

Formalnie:

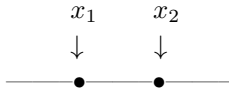
Definicja 8.11. Niech dany będzie szereg liczbowy o wyrazach rzeczywistych $\sum_{n=1}^{\infty} a_n$. Możemy zdefiniować **zbiór osiągalny** dla tego szeregu jako $\left\{ x \in \mathbb{R} : \exists A \subseteq \mathbb{N} \ x = \sum_{i \in A} a_i \right\}$. Będziemy go oznaczać jako $E\left(\sum_{n=1}^{\infty} a_n\right)$ lub w skrócie $E(\sum a_n)$.

Uwaga 8.12. W ogólności przyjmuje się, że do zbioru $E(\sum a_n)$ mogą należeć także $-\infty, +\infty$. Natomiast w zbiorach osiągalnych

dla szeregów opisanych w tej pracy te dwa skrajne punkty nie występują, więc dla uproszczenia rozumowania pominiemy je.

Nieformalnie:

Popatrzmy na dowolny szereg o wyrazach rzeczywistych postaci $\sum_{n=1}^{\infty} a_n = a_1 + a_2 + a_3 + a_4 + \dots$. Weźmy jakiś fragment (w skrajnym przypadku całość) z tej rozpisanej sumy. Na przykład $x_1 = a_3$ lub $x_2 = a_1 + a_4$ (są to jakieś liczby z \mathbb{R}). Przenieśmy je na oś rzeczywistą.



Chcielibyśmy w ten sposób przenieść wszystkie możliwe sumy (skończone i nieskończone) utworzone z $a_1 + a_2 + a_3 + a_4 + \dots$. Dodatkowo zawsze przyjmujemy $\sum_{i \in \emptyset} a_i = 0$.

Podzbiór \mathbb{R} , który ostatecznie otrzymamy, to będzie interesujący nas zbiór osiągalny dla szeregu $\sum_{n=1}^{\infty} a_n$.

Po zakończeniu "nieformalnej" części dochodzimy do głównego twierdzenia. To ze względu na jego poprawność wprowadziliśmy na samym początku ograniczenie dotyczące szeregów.

Twierdzenie 8.13. Niech dany będzie szereg rzeczywisty $\sum_{n=1}^{\infty} a_n$.

Szereg ten jest:

- a) mocno rozbieżny wtedy i tylko wtedy, gdy jego zbiór osiągalny $E(\sum a_n)$ jest półprostą domkniętą,
- b) potencjalnie względnie zbieżny wtedy i tylko wtedy, gdy $E(\sum a_n) = \mathbb{R}$,
- c) bezwzględnie zbieżny wtedy i tylko wtedy, gdy $E(\sum a_n)$ jest zbiorem ograniczonym w \mathbb{R} .

Bibliografia

- [1] Bartoszewicz A., Filipczak M., Prus-Wiśniowski F.,
Topological and algebraic aspects of subsums of series,
Traditional and present-day topics in real analysis, Faculty
of Mathematics and Computer Science. University of Łódź,
Łódź, (2013), 345-366

Drogi Banachu, a można tak ogólniej? Czyli topologiczne kontrakcje i uogólnione twierdzenie Banacha

Bartosz Kamiński

Politechnika Łódzka

Wydział Fizyki Technicznej, Informatyki i Matematyki
Stosowanej

9.1 Wstęp

Celem tej pracy jest zapoznanie czytelnika z uogólnioną wersją twierdzenia Banacha o punkcie stałym na przestrzeni T_1 , *zwarte*, za pomocą topologicznych kontrakcji - klasy funkcji rozszerzającej pojęcie kontrakcji na przestrzenie topologiczne.

9.2 Pojęcia wprowadzające

Definicja 9.1. Niech (X, d) będzie przestrzenią metryczną. Funkcję $f: X \rightarrow X$ nazywamy **kontrakcją**, jeśli

$$\exists C < 1 \forall x, y \in X \quad d(f(x), f(y)) \leq C \cdot d(x, y).$$

Twierdzenie 9.2 (Banacha o punkcie stałym). *Niech (X, d) będzie przestrzenią metryczną zupełną, natomiast $f: X \rightarrow X$*

kontrakcją. Wówczas f posiada jednoznaczny punkt stały tj.

$$\exists x_* \in X \quad f(x_*) = x_*.$$

Dowód twierdzenia silnie polega na fakcie, iż przestrzeń jest metryczna, a w szczególności zupełna. Da się jednak uzyskać podobny rezultat bez tak *silnych* założeń.

9.3 Topologiczne kontrakcje

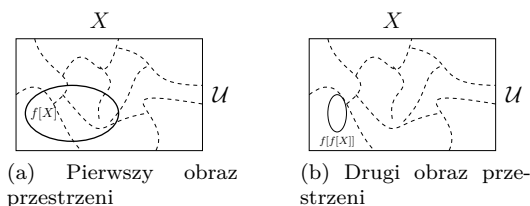
Ten podrozdział poświęcony jest dwóm równoważnym definicjom topologicznych kontrakcji, intuicji związanej z nazwaniem ich *kontrakcjami*, oraz relacji z kontrakcjami lipschitzowskimi.

9.3.1 Pierwsza definicja, oraz intuicja

Definicja 9.3. Niech X będzie przestrzenią topologiczną. Funkcję $f: X \rightarrow X$ nazwiemy **topologiczną kontrakcją**, jeśli jest *domknięta* oraz dla dowolnego pokrycia $\mathcal{U} = \{U_\alpha : \alpha \in \Lambda\}$

$$\exists n \in \mathbb{N} \quad \exists \lambda \in \Lambda \quad f^n[X] \subset U_\lambda.$$

Aby zobaczyć *kontraktywność* powyższej definicji warto posłużyć się rysunkami.



9.3.2 Związek z kontrakcjami lipschitzowskimi

Żeby zrozumieć relację między zwykłymi kontrakcjami w przestrzeniach metrycznych, a topologicznymi kontrakcjami w prze-

strzeniach topologicznych, potrzebujemy bardzo użytecznego lematu.

Lemat 9.4 (Liczba Lebesque'a). *Niech (X, d) będzie zwartą przestrzenią metryczną. Jeśli $\mathcal{U} = \{U_1, \dots, U_n\}$ jest pokryciem X , to istnieje taka liczba $\delta > 0$, że*

$$\forall_{A \subset X} (\text{diam}(A) < \delta \implies \exists_{i \in \mathbb{N}} A \subset U_i).$$

Pozwoli nam on na udowodnienie poniższego twierdzenia. Mówi ono o tym, że w przestrzeniach metrycznych zwartych każda kontrakcja w klasycznym sensie jest również topologiczną kontrakcją.

Twierdzenie 9.5. *Niech (X, d) będzie zwartą przestrzenią metryczną. Wówczas, jeśli $f: X \rightarrow X$ jest kontrakcją, to jest topologiczną kontrakcją.*

Dowód. Niech $f: X \rightarrow X$ będzie kontrakcją, \mathcal{U} pokryciem X , natomiast $\delta > 0$ taka jak w treści lematu (9.4).

Skoro X jest zwarta, to jest ograniczona, zatem $\text{diam}(X) = \varepsilon > 0$. Wiedząc, że f jest kontrakcją, $\text{diam}(f^n[X]) < C^n \cdot \varepsilon$. Weźmy zatem takie $n_0 \in \mathbb{N}$, że $\text{diam}(f^{n_0}[X]) < \delta$. Z lematu wiemy, że istnieje takie $i \in \mathbb{N}$, że $f^{n_0}[X] \subset U_i$.

Z dowolności pokrycia, f jest topologiczną kontrakcją. Q.E.D.

9.3.3 Równoważna definicja oraz przykład

Uogólnienie twierdzenia Banacha (9.2) będzie wymagało równoważnej definicji topologicznej kontrakcji, która mimo mniejszej intuicji jest bardziej użyteczna w zastosowaniu.

Twierdzenie 9.6. *Niech X będzie T_1 , zwarta. Wówczas $f: X \rightarrow X$ jest topologiczną kontrakcją wtw. gdy jest domknięta oraz dla dowolnych dwóch $x, y \in X$, $x \neq y$*

$$\exists_{n \in \mathbb{N}} (f^n[X] \subset X \setminus \{x\}) \vee (f^n[X] \subset X \setminus \{y\}).$$

Dowód tego twierdzenia zostanie pokazany później. Teraz zostanie przedstawiony przykład.

Przykład 9.7. Niech $X := \{\frac{1}{n} : n \in \mathbb{N}\} \cup \{0, 2, 3\}$ z metryką euklidesową, oraz $f: X \rightarrow X$ będzie następująca:

$$f(x) := \begin{cases} 2, & x \in \{\frac{1}{n} : n \in \mathbb{N}\} \\ 3, & x \in \{0, 2, 3\} \end{cases}.$$

W oczywisty sposób jest to topologiczna kontrakcja, ponieważ $f^2[X] = \{3\}$ i jest domknięta, gdyż $f[X] = \{2, 3\}$.

Co najważniejsze nie jest ciągła. Istotnie

$$f\left(\lim_{n \rightarrow \infty} \frac{1}{n}\right) = f(0) = 3 \neq 2 = \lim_{n \rightarrow \infty} f\left(\frac{1}{n}\right).$$

9.4 Topologiczne twierdzenie Banacha o punkcie stałym

Mając już przygotowane odpowiednie narzędzia, możemy udowodnić następujące twierdzenie.

Twierdzenie 9.8. Niech X będzie T_1 , zwarta, natomiast $f: X \rightarrow X$ będzie topologiczną kontrakcją. Wówczas f posiada dokładnie jeden punkt stały.

Do dowodu użyjemy równoważnej definicji (9.6) topologicznej kontrakcji.

Dowód. Zauważmy, że ciąg $(f^n[X])_{n \in \mathbb{N}}$ jest zstępującym ciągiem zbiorów domkniętych. Weźmy zatem

$$K := \bigcap_{n \in \mathbb{N}} f^n[X].$$

Z faktu, że rodzina $\{f^n[X] : n \in \mathbb{N}\}$ ma własność skończonych przekrojów, $K \neq \emptyset$.

Pokażemy, że K ma tylko jeden element x_* .

Istotnie gdyby istniały takie dwa punkty x_* oraz y_* , że $x_* \neq y_*$, oraz $x_*, y_* \in K$, to z definicji K

$$\forall_{n \in \mathbb{N}} x_*, y_* \in f^n[X].$$

Jednak to jest sprzeczność z definicją (9.6) topologicznej kontrakcji, gdy weźmiemy za nasze punkty x_* oraz y_* .

Oczywistym jest, że x_* jest punktem stałym, gdyż $f(x_*) \in K$, zatem

$$f(x_*) = x_*.$$

Zostaje nam pokazać jednoznaczność punktu stałego. Niech $z_* \in X$ będzie taki, że $f(z_*) = z_*$. Wówczas $z_* \in K$, więc $z_* = x_*$. Q.E.D.

Mając udowodnione to twierdzenie możemy w końcu wrócić do dowodu twierdzenia (9.6)

Dowód. Pokażemy implikację w dwie strony.

(\implies) Z założenia, że X jest T_1 , dla dowolnych dwóch punktów $x, y \in X$ stworzymy pokrycie \mathcal{U} , którego elementami są zbiory otwarte U takie, że $x \notin U$, albo $y \notin U$.

(\impliedby) Niech $\mathcal{U} = \{U_n : n \in \mathbb{N}\}$ będzie pokryciem X . Skorzystamy z tego, że dla funkcji spełniającej te założenia, zachodzi treść topologicznego twierdzenia Banacha (9.8) tj. f posiada dokładnie jeden punkt stały.

Niech zatem x_* będzie tym punktem. Wiemy, że $x_* \in U_{n_0}$ dla pewnego $n_0 \in \mathbb{N}$. Naszym celem będzie pokazanie, że

$$\exists_{k \in \mathbb{N}} f^k[X] \subset U_{n_0}.$$

Załóżmy, ku sprzeczności, że takie $k \in \mathbb{N}$ nie istnieje. Wówczas

$$\bigcap_{n \in \mathbb{N}} f^n[X] \cap U_{n_0}^c \neq \emptyset.$$

W takim razie istnieje $y \in \bigcap_{n \in \mathbb{N}} f^n[X] \cap U_{n_0}^c$, który daje sprzeczność z założeniami, jeśli weźmiemy za nasze punkty y oraz x_* . Q.E.D.

9.5 Kontraktywne IFS-y

Ta sekcja jest całkiem naturalną drogą, w którą można się zagłębić wiedząc, że twierdzenie Banacha ma swój topologiczny odpowiednik. Otóż teoria IFS-ów bardzo polega na twierdzeniu Hutchinsona-Barnsleya, który natomiast opiera się właśnie na twierdzeniu Banacha o punkcie stałym.

Tym samym w tej części powiemy o *kontraktywnych IFS-ach* oraz o warunkach potrzebnych do posiadania jednoznacznego atraktora.

9.5.1 IFS, hiperprzestrzeń X , operator Hutchinsona

Definicja 9.9 (IFS). Niech X będzie przestrzenią topologiczną, natomiast $f_i: X \rightarrow X$ dla $i \leq n$ funkcjami domkniętymi. Wówczas zbiór $\mathcal{F} := \{f_1, f_2, \dots, f_n\}$ nazywamy *IFS-em* (Iterated Function System).

Funkcje, które będą wchodziły w skład IFS-a będą takie jak w definicji, chyba, że będzie powiedziane inaczej. W ogólności IFS jest po prostu skończonym zbiorem funkcji, u których wymagamy konkretnych własności (np. ciągłości).

Definicja 9.10 (Hiperprzestrzeń). Niech X będzie przestrzenią topologiczną. Przestrzeń

$$\mathcal{K}(X) := \{K \subset X : K \neq \emptyset \text{ oraz } K \text{ jest zwarty}\}$$

z topologią Vietorisa generowaną przez zbiory bazowe postaci

$$\begin{aligned} &\{K \in \mathcal{K}(X) : K \cap U \neq \emptyset\}, \\ &\{K \in \mathcal{K}(X) : K \subset U\} \end{aligned}$$

dla U otwartego, nazywamy **hiperprzestrzenią X** .

Sama definicja nie jest aż tak ważna, większą wartość ma dla nas to, że hiperprzestrzeń $\mathcal{K}(X)$ *przejmuje* wiele własności przestrzeni X .

Stwierdzenie 9.11. *Niech X będzie T_1 zwarta. Wówczas $\mathcal{K}(X)$ jest T_1 zwarta.*

Definicja 9.12. Niech X będzie przestrzenią zwartą T_1 oraz $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ będzie IFS-em. **Operatorem Hutchinsona generowanym przez \mathcal{F}** nazywamy funkcję $F: \mathcal{K}(X) \rightarrow \mathcal{K}(X)$ zdefiniowaną wzorem

$$F(K) := \bigcup_{i=1}^n f_i[K].$$

Definicje te są podstawowymi zagadnieniami teorii IFS-ów, których przedstawienie i zrozumienie jest konieczne, aby zrozumieć wykorzystanie wcześniej udowodnionego topologicznego twierdzenia Banacha o punkcie stałym.

9.5.2 Użyteczne fakty teorii IFS-ów

W tym podrozdziale umieszczona została część faktów owej teorii, w celu poszerzenia wiedzy czytelnika w tym zakresie.

Stwierdzenie 9.13. *Niech X będzie polska. Wówczas $\mathcal{K}(X)$ jest polska.*

Metryką zupełną, którą można zadać hiperprzestrzeni jest między innymi *metryka Hausdorffa*.

Stwierdzenie 9.14.

Niech X będzie T_1 zwarta oraz $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ będzie IFS-em. Wówczas operator Hutchinsona generowany przez \mathcal{F} ma punkt stały.

Punkt stały operatora Hutchinsona generowanego przez \mathcal{F} nazywamy *atraktorem*.

Stwierdzenie 9.15. *Niech X będzie przestrzenią metryczną oraz $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ będzie IFS-em składającym się z kontrakcji lipschitzowskich. Wówczas operator Hutchinsona F generowany przez \mathcal{F} jest kontrakcją.*

Powyższe fakty można podsumować w jednym zdaniu. Jeśli X ma jakąś strukturę, to \mathcal{K} również ją będzie miał, oraz jeśli IFS będzie się składał z funkcji danego typu, to operator Hutchinsona również będzie funkcją takiego samego typu.

9.5.3 Kontraktywność w IFS-ach

Definicja 9.16.

Niech X będzie T_1 zwarta. IFS $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ nazwiemy **kontraktywnym**, jeśli dla dowolnego pokrycia $\mathcal{U} = \{U_\alpha : \alpha \in \Lambda\}$ istnieje takie $m \in \mathbb{N}$, że dla dowolnego układ indeksów (i_1, \dots, i_m) , $1 \leq i_j \leq n$ zbiór $f_{i_1} \circ \dots \circ f_{i_m}[X] \subset U_\lambda$, dla pewnego $U_\lambda \in \mathcal{U}$.

Mając tą definicję, dostajemy ważną własność operatora Hutchinsona.

Twierdzenie 9.17 (Jednoznaczność atraktora). *Niech X będzie T_1 zwarta, oraz \mathcal{F} będzie kontraktywnym IFS-em. Jeśli operator Hutchinsona F generowany przez \mathcal{F} jest domknięty, to F jest topologiczną kontrakcją na \mathcal{K} .*

Powstaje nam naturalne pytanie, czy nie wystarczy, żeby IFS składał się z topologicznych kontrakcji, żeby samo F również nią było.

Okazuje się, że mimo tego, iż wiele własność przestrzeni oraz funkcji wchodzących w skład IFS-u, przechodzą na odpowiednio hiperprzestrzeń i F , bycie topologiczną kontrakcją jest jednym z *wyjątków od tej reguły*.

Bibliografia

- [1] Michał Morayne, Robert Rałowski, The Baire theorem, an analogue of the Banach fixed point theorem and attractors in T_1 , compact spaces.

Wiązka główna z powiązaniem głównym, na przykładzie sfery zanurzonej w \mathbb{R}^3

Damian Kayzer

Uniwersytet Warszawski
Wydział Fizyki

10.1 Wstęp

Definicja wiązki głównej jest dość zawiła, lecz można ją zwięźle - choć nieformalnie - podsumować słowami: wiązka główna to rozmaitość z grupą przyklejoną do każdego jej punktu. Wiązkę główną można wyposażyć w dodatkową strukturę - powiązanie główne, będącą pewnym rozkładem przestrzeni stycznej do wiązki głównej na sumę prostą. Pojęcia te naturalnie pojawiają się w geometrii różniczkowej, a także - co być może zaskakujące - w fizyce. Okazuje się, że struktura wiązki głównej z powiązaniem głównym idealnie nadaje się do modelowania takich zagadnień fizycznych jak m.in. teorie pola z cechowaniem, czy faza geometryczna. W niniejszym artykule przyjrzymy się tym pojęciom przez pryzmat przykładu wiązki baz ortonormalnych na sferze.

10.2 Definicja wiązki

Zacznijmy od ogólniejszej definicji wiązki włóknistej, a następnie podamy definicję wiązki głównej jako wiązki włóknistej szczególnego typu.

Wiązka główna z powiązaniem głównym, na przykładzie sfery
zanurzonej w \mathbb{R}^3

Definicja 10.1. Czwórkę (P, B, G, π) nazwiemy **wiązką włóknistą** jeśli spełnione są warunki:

1. P, B, G są gładkimi rozmaitościami,
2. $\pi: P \rightarrow B$ jest gładką surjektywną submersją,
3. istnieje pokrycie $\{\mathcal{O}_i\}$ rozmaitości B i dyfeomorfizmy

$$\tau_i: \pi^{-1}(\mathcal{O}_i) \rightarrow \mathcal{O}_i \times G,$$

4. przemienny jest diagram

$$\begin{array}{ccc} \pi^{-1}(\mathcal{O}_i) & \xrightarrow{\tau_i} & \mathcal{O}_i \times G \\ & \searrow \pi & \swarrow \text{pr}_1 \\ & & \mathcal{O}_i \end{array},$$

gdzie pr_1 jest projekcją na pierwszy składnik.

Rozmaitości P, B, G nazywamy kolejno: **przestrzenią totalną**, **bazą** i **włóknem typowym wiązki**, a π **rzutem na bazę**. Niech $b \in B$. **Włóknem nad b** nazywamy zbiór $\pi^{-1}(b)$. Zwróćmy uwagę, że włókno nad b jest dyfeomorficzne z G . Z tego powodu interpretujemy przestrzeń totalną jako sumę włókien typowych poprzyklejanych do każdego punktu bazy. Podstawowym przykładem wiązki głównej jest **wiązka trywialna** $(B \times G, B, G, \text{pr}_1)$. Warunek 3. wyraża, że wiązka włóknista lokalnie wygląda jak wiązka trywialna, dlatego τ_i nazywać będziemy **lokalnymi trywializacjami**.

Definicja 10.2. Wiazkę włóknistą nazwiemy **wiązką główną** ilekroć

1. G jest grupą Liego,
2. określone jest działanie $r: P \times G \rightarrow P$ - gładkie, wolne i przechodnie w obcięciu do włókna,

3. działanie nie wyprowadza poza włókno, tj.

$$\begin{array}{ccc} P \times G & \xrightarrow{r} & P \\ \text{pr}_1 \downarrow & & \downarrow \pi, \\ P & \xrightarrow{\pi} & B \end{array}$$

4. lokalne trywializacje są G - ekwiwariatne, tj.

$$\begin{array}{ccc} \pi^{-1}(\mathcal{O}_i) \times G & \xrightarrow{r} & \pi^{-1}(\mathcal{O}_i) \\ \tau_i \times \text{id}_G \downarrow & & \downarrow \tau_i, \\ \mathcal{O}_i \times G \times G & \xrightarrow{\text{id}_{\mathcal{O}_i} \times R} & B \end{array}$$

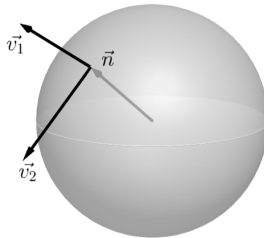
gdzie $R(g, h) = gh$.

10.3 Przykład wiązki nad sferą

Rozważmy sferę S^2 jako rozmaitość zanurzoną w \mathbb{R}^3 . Niech $(\cdot | \cdot)$ oznacza standardowy iloczyn skalarny, a \times iloczyn wektorowy. Przestrzeń styczną możemy zapisać jako

$$T_n S^2 = \text{Span}(n)^\perp \equiv \{v \in \mathbb{R}^3 : (v|n) = 0\},$$

Powiemy, że baza (v_1, v_2) jest zorientowana na zewnątrz, jeśli $v_1 \times v_2 = n$.



Rysunek 10.1

Wiązka główna z powiązaniem głównym, na przykładzie sfery
zanurzonej w \mathbb{R}^3

Włóknem nad n będzie zbiór P_n zorientowanych na zewnątrz baz ortonormalnych przestrzeni $T_n S^2$, a przestrzenią totalną wiązki

$$P = \bigsqcup_{n \in S^2} P_n.$$

Elementami P są trójki wektorów (v_1, v_2, n) . Taką trójkę możemy traktować jak macierz 3×3 . Ponieważ wektory te są ortogonalne, to $(v_1, v_2, n) \in SO(3)$. Łatwo się przekonać, że $P = SO(3)$. Rzutem na bazę będzie $\pi(v_1, v_2, n) = n$.

Na $SO(3)$ działa grupa $SO(2)$ obracając bazę wokół punktu zaczepienia, co można zapisać wzorem jako:

$$r_{A_\varphi}(v_1, v_2, n) = (v_1, v_2, n)R_z(\varphi),$$

gdzie

$$A_\varphi := \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}, R_z(\varphi) := \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Niech (\mathcal{O}, x^i) będzie układem współrzędnych na S^2 , indukując on bazę (∂_{x^i}) . Bazę tę możemy - stosując algorytm Grama-Schmidta - zortonormalizować, oznaczmy wynik tej procedury przez (e_i) . Rozkładając w ostatniej bazie wektory v_1, v_2 dostajemy lokalną trywializację:

$$\begin{aligned} \tau(v_1, v_2, n) &= \tau(\alpha e_1 + \beta e_2, \gamma e_1 + \delta e_2, n) = \\ &= \left(n, \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \right) \in \mathcal{O} \times SO(2). \end{aligned}$$

Łatwo można sprawdzić, że $(SO(3), S^2, \pi, SO(2))$ spełnia definicję wiązki głównej.

10.4 Definicja powiązania

Pojęcie powiązania można zdefiniować na wiele równoważnych sposobów, my zrobimy to w duchu tzw. powiązania Ehresmanna. Ponownie podamy ogólną definicję powiązania na wiązce włóknistej, a dalej wyspecjalizujemy się do wiązki głównej.

Definicja 10.3. Niech (P, B, G, π) będzie wiązką włóknistą. **Podwiązką pionową** nazywamy zbiór

$$\forall P = \ker \tau \pi.$$

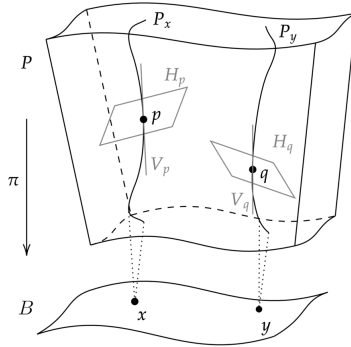
Powiązaniem Ehresmanna lub **podwiązką horyzontalną** H nazywamy dowolne dopełnienie podwiązki pionowej do całej wiązki stycznej:

$$\tau P = \forall P \oplus_B H. \quad (10.1)$$

Niech (P, B, G, π) będzie wiązką główną. Powiązanie Ehresmanna nazwiemy **głównym** ilekroć jest niezmiennicze na działanie grupy. tj.:

$$\forall (p, g) \in P \times G: \tau_p r_g(H_p) = H_{r_g(p)}$$

Kilka słów wyjaśnienia: podwiązkę pionową można rozumieć jako zbiór tych wektorów, które są styczne do włókien. Występujące w równaniu 10.1 wyrazy są wiązkami wektorowymi, czyli wiązkami włóknistymi których włókna są przestrzeniami wektorowymi. Sumą prostą takich wiązek nazywamy wiązkę, której włókna są sumami prostymi włókien składników.



Rysunek 10.2: zaczerpnięto z [3]. Krzywe P_x i P_y przedstawiają włókna nad x i y , V_p i V_q - przestrzenie pionowe zaczepione w punktach $p \in P_x, q \in P_y$, a H_p i H_q - dopełniające je przestrzenie horyzontalne.

Wiązka główna z powiązaniem głównym, na przykładzie sfery
zanurzonej w \mathbb{R}^3

Opiszemy teraz kilka pojęć pochodnych od powiązania głównego. Niech $p \in P$ i $n := \pi(p)$. Odwzorowanie styczne

$$\mathbb{T}_p\pi: \mathbb{T}_pP \rightarrow \mathbb{T}_nB$$

jest surjekcją, więc istnieje izomorfizm

$$(\cdot)_p^h: \mathbb{T}_nB \rightarrow H_p,$$

określony wzorem $\mathbb{T}_p\pi \circ (\cdot)_p^h = \text{id}_{\mathbb{T}_nB}$. Będziemy nazywać go **podniesieniem horyzontalnym**.

Z teorii grup Liego wiemy, że wiązka styczna do grupy Liego jest trywialna: $\mathbb{T}G \simeq G \times \mathfrak{g}$, gdzie \mathfrak{g} jest algebrą Liego grupy Liego. Fakt ten można uogólnić do stwierdzenia: podwiązka pionowa wiązki głównej jest trywialna - $\mathbb{V}P \simeq P \times \mathfrak{g}$. Wobec tego rzut na $\mathbb{V}P$ wzdłuż H indukują 1-formę θ o wartościach w \mathfrak{g} , nazywać ją będziemy **1-formą powiązania**. Niech $X, Y \in \mathbb{T}_pP$. Rozłóżmy je na część pionową i część poziomą:

$$X = X^H + X^V, \quad Y = Y^H + Y^V.$$

Definiujemy **krzywiznę powiązania** jako

$$\Omega(X, Y) = d\theta(X^H, Y^H).$$

10.5 Przykład powiązania

Przestrzeń styczna do przestrzeni totalnej naszej wiązki to

$$\mathbb{T}P \simeq P \times \mathfrak{so}(3).$$

Algebra Liego ($\mathfrak{so}(3)$, $[\cdot, \cdot]$) jest izomorficzna z algebrą Liego (\mathbb{R}^3 , \times):

$$X = \begin{bmatrix} 0 & -z & y \\ z & 0 & x \\ -y & x & 0 \end{bmatrix} \mapsto \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \vec{X}$$

Wektor $X \in \mathbb{T}_pP$ jest styczny do krzywej $t \mapsto \exp(tX)p$ oraz mamy

$$\pi(\exp(tX)p) = \pi(\exp(tX)v_1, \exp(tX)v_2, \exp(tX)n) = \exp(tX)n.$$

Zatem

$$\mathbb{T}\pi(X) = Xn = \vec{X} \times n.$$

Stąd podwiązka pionowa ma postać

$$\mathbb{V}_p P = \left\{ \vec{X} \in \mathbb{R}^3 : \vec{X} \times n = 0 \right\} = \text{Span}(n).$$

Powiązanie Ehresmanna wybieramy następująco

$$H_p := \text{Span}(n)^\perp.$$

Sprawdźmy, że wybrane powiązanie jest główne.

$$\begin{aligned} \mathbb{T}_p r_{A_\varphi}(p, X) &= \left. \frac{d}{dt} \right|_{t=0} r_{A_\varphi}(\exp(tX)p) = \\ &= \left. \frac{d}{dt} \right|_{t=0} \exp(tX)p R_z(\varphi) = \\ &= \left. \frac{d}{dt} \right|_{t=0} \exp(tX)r_{A_\varphi}(p) = (r_{A_\varphi}(p), X), \end{aligned}$$

zatem $\mathbb{T}r_{A_\varphi}$ nie zmienia X , a ponieważ $\pi(r_{A_\varphi}(p)) = \pi(p) = n$, to

$$\mathbb{T}_p r_{A_\varphi}(H_p) = \text{Span}(n)^\perp = H_{r_{A_\varphi}(p)}.$$

Podniesienie horzontalne ma postać

$$(v)_p^h = n \times v$$

dla $v \in \mathbb{T}_n S^2$, ponieważ

$$\mathbb{T}_p \pi((v)_p^h) = (n \times v) \times n = v(n|n) - n(n|v) = v.$$

Forma koneksji $\theta: \mathbb{T}P \simeq P \times \mathfrak{so}(3) \rightarrow \mathfrak{so}(2) \simeq \mathbb{R}$ to rzutowanie wektora na prostą $\text{Span}(n)$:

$$\theta(p, X) = (\vec{X}|n).$$

Z kolei krzywizna koneksji to

$$\begin{aligned} \Omega(X, Y) &= d\theta(X^H, Y^H) \\ &= X^H(\theta(Y^H)) - Y^H(\theta(X^H)) - \theta([X^H, Y^H]) \\ &= 0 - 0 - \theta(\vec{X}^H \times \vec{Y}^H) = -\left(\vec{X}^H \times \vec{Y}^H \Big| n\right). \end{aligned}$$

Wiązka główna z powiązaniem głównym, na przykładzie sfery
zanurzonej w \mathbb{R}^3

Podniesienie horyzontalne jest izomorfizmem $\mathbb{T}_n S^2 \simeq H_p$, więc Ω zstępuje do 2-formy na przestrzeni bazowej S^2 : dla $v, w \in \mathbb{T}_n S^2$ mamy

$$\Omega(v_p^h, w_p^h) = -((n \times v) \times (n \times w)|n) = -(v \times w|n).$$

Bibliografia

- [1] J.J. Duistermaat, *Principal Fiber Bundles*, Spring School, June 17-22, 2004, Utrecht
- [2] J.M. Lee: *Introduction to Smooth Manifolds*, Graduate Texts in Mathematics, wyd. 2, Springer, New York, (2012)
- [3] [https://en.wikipedia.org/wiki/Connection_\(principal_bundle\)](https://en.wikipedia.org/wiki/Connection_(principal_bundle))

Topologia grup Liego i rozwłóknienie Hopfa

Paweł Przybyła

Uniwersytet Warszawski
Wydział Fizyki

11.1 Motywacja i cel

Celem tego artykułu jest wprowadzenie czytelnika w podstawy teorii grup Liego poprzez zobrazowanie ich użyteczności w wielu różnych działach nauki. Grupy Liego znalazły swoje zastosowanie w następujących obszarach:

- mechanika kwantowa – teoria reprezentacji rozważanych symetrii modelowanych przez grupy Liego [1],
- fizyka wysokich energii – klasyfikacja multipletów cząstek za pomocą reprezentacji odpowiednich grup [2],
- oddziaływania fundamentalne – opis przez teorie z cechowaniem, zawierające wiązki główne grup Liego na czasoprzestrzenią (chromodynamika kwantowa, teoria elektrosłaba, grawitacja) [3]
- mechanika klasyczna – redukcja symplektyczna układów, wpływ topologii przestrzeni konfiguracyjnej na dynamikę układu (np. bryły sztywnej, podwójnego wahadła) [4] [5]
- hydrodynamika [6] [7], robotyka (teoria sterowania [8]), ...

Nie będzie to jednak wprowadzenie o ściśle określonej logicznej strukturze. To co chciałbym zrobić to dać czytelnikowi motywację do zgłębienia tego tematu samemu zapewniając mu wiele ciekawych przykładów oraz bogatą bibliografię na temat poruszonych zagadnień. Godnym zauważenia jest fakt, że często sama nietrywialna topologia rozważanej grupy ma nietrywialne konsekwencje. Przykładem może być istnienie fermionów oraz stabilność atomów wielopowłokowych jaką to pociąga za sobą. W dalszej części zostanie omówiona konstrukcja wiązki Hopfa, która występuje w ogromnej liczbie zastosowań, a także jest dość prosta do zrozumienia oraz posiada niesłychane geometryczne piękno.

11.2 Definicja i przykłady

Definicja 11.1. Grupa Liego to grupa będąca rozmaitością gładką, w której działanie i branie odwrotności jest gładkie (por. [10]).

Poprzez powyższe stwierdzenie rozumiemy, że grupa Liego to zbiór z dwoma zgodnymi strukturami. Od teraz znakiem \simeq będziemy oznaczać relację homeomorficzności. Poniżej przykłady **macierzowych grup Liego**:

Przykład 11.2. Grupa trywialna $\{e\}$ z topologią dyskretną spełnia powyższą definicję

Przykład 11.3. Okrąg jednostkowy na płaszczyźnie:

$$U(1) := \{e^{i\theta} : \theta \in [0, 2\pi[\} \simeq S^1. \quad (11.1)$$

Przykład 11.4. Pełna grupa liniowa:

$$GL(N, \mathbb{R}) := \{A \in \text{Mat}_{N \times N, \mathbb{R}} : \det A \neq 0\}. \quad (11.2)$$

Przykład 11.5. Specjalna grupa liniowa:

$$SL(N, \mathbb{R}) = \{A \in GL(N, \mathbb{R}) : \det A = 1\}. \quad (11.3)$$

Ciekawostka 11.6. Grupa $SL(2, \mathbb{R})$ jest homeomorficzna z pełnym torusem $S^1 \times D^2$.

Przykład 11.7. Specjalna grupa ortogonalna:

$$SO(N) := \{A \in SL(N, \mathbb{R}) : A^T = A^{-1}\}. \quad (11.4)$$

Widzimy, że $SO(2) \simeq U(1)$. Pierwszy nietrywialny fakt, jaki będziemy chcieli omówić to:

Stwierdzenie 11.8. Zachodzi homeomorfizm: $SO(3) \simeq \mathbb{RP}^3$ [kids].

Grupa $SO(3)$ to grupa obrotów w trzech wymiarach. Do opisu każdego takiego obrotu wystarczy podać jego oś oraz kąt. Niech $(\theta, \phi) \in S^2$ parametryzują oś obrotu (wraz z orientacją), zaś niech $\alpha \in [0, \pi]$ będzie kątem obrotu zgodnie z naturalną orientacją wyznaczaną przez zwrot osi. Niech

$$\mathbf{n} = \sin \theta \cos \phi \mathbf{e}_x + \sin \theta \sin \phi \mathbf{e}_y + \cos \theta \mathbf{e}_z \quad (11.5)$$

będzie wektorem jednostkowym w kierunku punktu $(\theta, \phi) \in S^2$. Widzimy, że zbiór o elementach postaci $\mathbf{x} = \alpha \mathbf{n} \in \mathbb{R}^3$ jest kulą o promieniu π . Jednakże nie jest to jeszcze zbiór wszystkich obrotów. Obrót o kąt $\alpha = \pi$ w jednym kierunku jest równoważny obrotowi o ten sam kąt w kierunku przeciwnym. Aby uzyskany zbiór był homeomorficzny z $SO(N)$ należy zatem utożsamić ze sobą punkty antypodalne na sferze S^2 będącej jego brzegiem. Kula z utożsamionymi antypodami to jedno z przedstawień przestrzeni rzutowej \mathbb{RP}^3 Q.E.D..

Przykład 11.9. Specjalna grupa unitarna:

$$SU(N) = \{U \in \text{Mat}_{N \times N, \mathbb{C}} : \det U = 1, U^\dagger = U^{-1}\}. \quad (11.6)$$

Grupy te są bardzo istotne w mechanice kwantowej, bowiem zazwyczaj gdy chcemy opisać układ posiadający N stanów zachowujących się tak samo ze względu na jakieś oddziaływanie, system ma symetrię $SU(N)$. Przykładami tego są chromodynamika kwantowa z grupą symetrii $SU(3)$ stowarzyszona z istnieniem 3

kolorów kwarków czy symetria $SU(2)$ oddziaływania protonów i neutronów [2]. W szczególności grupa $SU(2)$ ma ogromne znaczenie w zastosowaniach.

Stwierdzenie 11.10. *Zachodzi homeomorfizm $SU(2) \simeq S^3$. Ze względu na fakt, że S^3 jest uniwersalnym nakryciem $\mathbb{R}P^3$ zachodzi także izomorfizm [10]:*

$$\frac{SU(2)}{\{I, -I\}} \approx SO(3). \quad (11.7)$$

Dowolna macierz unitarna jest macierzą przejścia między dwoma bazami ortonormalnymi. Zatem jej kolumny stanowią wektory ortonormalne ze względu na standardowy iloczyn skalarny na \mathbb{C}^N dany wzorem $(u, v) = \sum_{i=1}^N u_i^* v_i$. Dowolną macierz $SU(2)$ można sparametryzować przez $\alpha, \beta \in \mathbb{C}$ jako:

$$U = \begin{bmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{bmatrix}, \quad (11.8)$$

gdzie parametry spełniają równanie:

$$\det U = |\alpha|^2 + |\beta|^2 = 1. \quad (11.9)$$

Jest ono równaniem definiującym sferę $S^3 \subset \mathbb{R}^4 \simeq \mathbb{C}^2$, co chcieliśmy pokazać. Dla czytelników zaznajomionych z teorią kwaternionów może okazać się znajoma

Uwaga 11.11. *Odwzorowanie $\Phi : \mathbb{H} \rightarrow SU(2)$ liniowe, takie, że $\Phi(1) = I$, $\Phi(\mathbf{i}) = i\sigma_z$, $\Phi(\mathbf{j}) = i\sigma_y$, $\Phi(\mathbf{k}) = i\sigma_x$ indukuje izomorfizm grupy jednostkowych kwaternionów (z mnożeniem jako działaniem) z $SU(2)$.*

Fakt 11.12. *Kwaterniony jednostkowe reprezentują obroty w \mathbb{R}^3 w następujący sposób. Zapiszmy wektor $v \in \mathbb{R}^3$ w bazie $(\mathbf{i}, \mathbf{j}, \mathbf{k})$ i oznaczmy go przez $\mathbf{v} \in \mathbb{H}$. Wtedy każde $\mathbf{q} \in \mathbb{H}$, $\|\mathbf{q}\| = 1$ reprezentuje pewien obrót $R_{\mathbf{q}} : \mathbf{v} \mapsto \mathbf{q}\mathbf{v}\mathbf{q}^{-1}$. Ponadto, każdy obrót $R \in SO(3)$ da się otrzymać w ten sposób na dokładnie dwa sposoby za pomocą dokładnie dwóch kwaternionów jednostkowych, pewnego \mathbf{q} oraz $-\mathbf{q}$.*

W ten sposób ustanowiliśmy izomorfizm 11.7.

11.3 Rozwłóknienie Hopfa

Powyższe odwzorowanie pozwala przyporządkować każdemu elementowi $SU(2)$ oś obrotu oraz kąt obrotu. Odwzorowanie to jest 2:1. Okazuje się, że jeżeli każdemu elementowi $SU(2)$ przypiszemy kąt obrotu nie z przedziału $[0, \pi]$ a $[0, 2\pi]$ to wtedy przyporządkowanie to jest jednoznaczne. Można to przyporządkowanie rozumieć jako konstrukcję pewnej nietrywialnej wiązki włóknistej $S^1 \hookrightarrow S^3 \xrightarrow{\pi} S^2$. Konstrukcję tę można przeprowadzić następująco [11]:

- Rozważmy $S^3 \subset \mathbb{R}^4 \simeq \mathbb{C}^2$.
- Ustalmy pewną płaszczyznę przechodzącą przez środek układu współrzędnych tzn. prostą zespoloną $X = \{(z, w) \in \mathbb{C}^2 : Az + Bw = 0\}$, gdzie $A, B \in \mathbb{C}$.
- Przecięciami tych prostych zespolonych ze sferą są jej okręgi wielkie.
- Zbiór wszystkich prostych zespolonych przechodzących przez $(0, 0)$ parametryzowany jest współrzędnymi jednorodnymi $[A : B]$ a zatem jest zespoloną prostą rzutową $\mathbb{C}P^1 \simeq S^2$.
- Zatem możemy zdefiniować rzutowanie π takie, że każdemu punktowi z S^3 przyporządkowuje odpowiednią prostą z $\mathbb{C}P^1$, na której leży. Z powyższych rozważań wynika, że $\pi^{-1}(\{(z, w)\}) \simeq S^1$.

Powyższa wiązka pojawia się w wielu zastosowaniach od informacji kwantowej przez opis pól spinorowych, ogólną teorię względności [12], modelowanie braionów [13], mechanikę bąków [5] po (magneto)hydrodynamikę [6].

Fakt 11.13. *Powyższa konstrukcja daje się zastosować do wszystkich skończenie wymiarowych algebr z dzieleniem nad \mathbb{R} (czyli $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$). Daje to wiązki postaci:*

$$S^{n-1} \hookrightarrow S^{2n-1} \twoheadrightarrow S^n \quad (11.10)$$

dla $n = 1, 2, 4, 8$.

Ciekawostka 11.14. *Podobne wiązki istnieją dla innych grup $SU(N)$:*

$$SU(N - 1) \hookrightarrow SU(N) \xrightarrow{\pi} S^{2N-1}. \quad (11.11)$$

Rozważmy rzutowanie $\pi : SU(N) \rightarrow S^{2N-1}$, które każdej macierzy przyporządkowuje jej pierwszą kolumnę, którą interpretujemy potem jako element \mathbb{R}^{2N} , który spełnia warunek unormowania do jedności. Rozważmy włókno $\pi^{-1}(\{(1, 0, \dots, 0)\})$. Łatwo zauważyć, że z warunku ortogonalności kolumn macierzy $SU(N)$ wynika, że to włókno jest homeomorficzne z $SU(N - 1)$. Z symetrii można pokazać, że tak wygląda każde włókno, więc mamy wiązkę opisaną powyżej.

11.4 Algebry Liego

Grupy Liego są obiektami geometrycznymi, jednak ze względu na strukturę grupową wykazują własności, które pozwalają się bardzo dużo o nich dowiedzieć za pomocą badania ich w otoczeniu elementu neutralnego. Dlatego umotywowana jest następująca definicja.

Definicja 11.15. Algebra Liego \mathfrak{g} macierzowej grupy Liego G to przestrzeń styczna do grupy w elemencie neutralnym $\mathfrak{g} = T_e G$ wyposażona w działanie zwane **nawiasem Liego** zdefiniowane następująco:

$$[X, Y] := XY - YX, \quad (11.12)$$

gdzie $X, Y \in \mathfrak{g}$, zaś iloczyn jest iloczynem macierzy.

Aby uogólnić tę definicję na przypadek grup Liego, które niekoniecznie są macierzowe a jednocześnie nadać nawiasowi Liego sens geometryczny, będziemy musieli posłużyć się pojęciami geometrii różniczkowej.

Definicja 11.16. Polem wektorowym lewonieźmienniczym na grupie Liego G nazywamy pole wektorowe X , takie że jeżeli dla pewnej krzywej $\gamma : \mathbb{R} \rightarrow G$ przechodzącej przez początek układu współrzędnych $X(e) = \gamma'(0) \in \mathfrak{g}$, to $X(g) = (g \cdot \gamma)'(0)$ [kir].

Innymi słowy $X(g) = (L_g)_*X(e)$ jest pchnięciem wektora $X(0)$ względem lewego działania grupy na sobie.

Definicja 11.17. Potokiem pola wektorowego X na rozma-
itości M nazywamy odwzorowanie $\Phi_X : \mathbb{R} \rightarrow M$, takie że:

$$\frac{d}{dt} \Big|_{t=s} \Phi_t^X = X(\Phi_s^X). \quad (11.13)$$

Co prowadzi nas do geometrycznej definicji nawiasu Liego dla pól wektorowych na dowolnej rozmaitości.

Definicja 11.18. Nawias Liego pól wektorowych X oraz Y w punkcie p to $[X, Y](p) := \frac{d}{ds} \Big|_{s=0^+} \alpha_p(s)$, gdzie:

$$\alpha_p(t^2) := \Phi_{-t}^Y \circ \Phi_{-t}^X \circ \Phi_t^Y \circ \Phi_t^X \quad (11.14)$$

oraz zachodzi warunek początkowych $\Phi_0^X = \Phi_0^Y = p$.

Czyli nawias Liego to komutator nieskończenie małych przepływów pól wektorowych [7] [13]. Stosując powyższą definicję do pól wektorowych lewniezmienicznych uzyskanych przez pchnięcia wektorów $X_0, Y_0 \in \mathfrak{g}$ uzyskamy pole wektorowe, które w punkcie $p = e$ da nam działanie dwuargumentowe na algebrze Liego. Można pokazać, że ta uogólniona definicja zgadza się z definicją 11.15 dla grup macierzowych.

Warto zauważyć, że do zdefiniowania nawiasu Liego jako działania w algebrze Liego jest nam potrzebna znajomość pól wektorowych w pewnym otoczeniu elementu neutralnego a tę uzyskujemy poprzez warunek lewniezmienności pól.

Algebrę Liego można także zdefiniować abstrakcyjnie (w oderwaniu od konkretnej grupy) jako przestrzeń wektorową z dwuliniowym działaniem antysymetrycznym spełniającym tożsamość Jacobiego.

Możemy klasyfikować grupy Liego za pomocą klasyfikacji ich algebr, dzięki następującemu twierdzeniu.

Twierdzenie 11.19. *Dla dowolnej algebry Liego \mathfrak{g} występuje, z dokładnością do izomorfizmu, dokładnie jedna, jednospójna grupa Liego \tilde{G} , taka że $\mathfrak{g} = T_e \tilde{G}$. [1]*

Przykład 11.20. Grupa $SO(3)$ ma algebrę Liego izomorficzną do algebry Liego grupy $SU(2)$ daną przez $\mathfrak{su}(2) := \text{span}\{\sigma_x, \sigma_y, \sigma_z\}$. Wiemy, że $SU(2) \simeq S^3$ jest jednospójna i pokrywa $SO(3)$, co ob-
razuje powyższe twierdzenie.

11.5 Podsumowanie i podziękowania

W powyższej dyskusji omówiliśmy grupy oraz algebry Liego wraz z ich zastosowaniami. Zainteresowanemu czytelnikowi polecamy zgłębienie podanej literatury w szczególności [1].

Bardzo dziękuję Mateuszowi Kulejewskiemu oraz Bartoszowi Prechowi za pomoc w korekcie, jak również Tymonowi Frelikowi za liczne i pomocne uwagi merytoryczne.

Bibliografia

- [1] Hall, Brian C. *Quantum Theory for Mathematicians*, Springer New York, Graduate Texts in Mathematics, 2013.
- [2] Weinberg, S. *The Quantum Theory of Fields*. Cambridge: Cambridge University Press, 1996.
- [3] Mayer, M.E., Trautman, A. *A Brief Introduction to the Geometry of Gauge Fields*. In: Mitter, H., Pittner, L. (eds) *New Developments in Mathematical Physics*. Acta Physica Austriaca, vol 23/1981. Springer, Vienna, 1981.
- [4] Arnol'd, V. I. *Mathematical methods of classical mechanics*. Springer Science & Business Media, 2013.
- [5] Marsden, J. E., Ratiu, T. S. *Introduction to mechanics and symmetry: a basic exposition of classical mechanical systems* (Vol. 17). Springer Science & Business Media, 2013.
- [6] Edixhoven, S. J., & Dalhuisen, J. W. . *The Hopf Map in Magnetohydrodynamics*, Mathematical Institute, Leiden Institute of Physics, Leiden University, praca licencjacka.

- [7] Arnol'd, V.I. *The asymptotic Hopf invariant and its applications*. In: Givental, A., Khesin, B., Varchenko, A., Vassiliev, V., Viro, O. (eds) Vladimir I. Arnold - Collected Works. Vladimir I. Arnold - Collected Works, vol 2. Springer, Berlin, Heidelberg, 1974.
- [8] Montgomery, R. *Nonholonomic Control and Gauge Theory*. In: Li, Z., Canny, J.F. (eds) Nonholonomic Motion Planning. The Springer International Series in Engineering and Computer Science, vol 192. Springer, Boston, MA, 1993.
- [9] Stoytchev, O. *Topology of $SO(3)$ For Kids*. arXiv preprint arXiv:2310.19665 2023.
- [10] Kirillov, Jr, A. *An Introduction to Lie Groups and Lie Algebras*. Cambridge: Cambridge University Press (Cambridge Studies in Advanced Mathematics), 2008.
- [11] Penrose, R. *The Road to Reality: A Complete Guide to the Laws of the Universe*. Jonathan Cape, London, 2004.
- [12] Urbantke, H. K., *The Hopf fibration—seven times in physics*, Journal of Geometry and Physics, Volume 46, Issue 2, 2003.
- [13] Skyrme, T. (1962). "A unified field theory of mesons and baryons". Nuclear Physics. 31: 556–569.
- [14] Kijowski, J. *Geometria różniczkowa jako narzędzie nauk przyrodniczych*. Centrum Studiów Zaawansowanych Politechniki Warszawskiej, Warszawa, 2015.

RK relevance logic : lattice of extensions

Zuzanna Rygiewicz

Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Introduction : logic R

Logic is the science of correct entailment. It is considered that entailment is correct when the conclusion follows from the premises, so entailment is the most important concept in logic. It is assumed that the succedent B follows from the antecedent A if there is a relationship between the antecedent and the succedent, i.e. When A is a substitution in the antecedent of a logical law in the form of an implication, and B is a substitution in its succedent. However, there are logical laws in classical logic, i.e. $p \wedge \neg p \rightarrow q$, $p \rightarrow (q \rightarrow p)$, $p \rightarrow (q \rightarrow q)$ which are non-intuitive, so it is questioned whether they should be the basis of the result. Hence attempts to find a formal logic that does not contain such controversial implications.

An example of such logic is relevance logic.

Relevance logic is an attempt to reconstruct colloquial language. Classical logic seems to be too strong in colloquial inference, as it has various logical laws or rules of inference that provide us with paradoxical sentences.

Relevant logic R (from relevant – significant, important) appeared in 1975; it was described by A.R. Anderson and N. Belnap. A weaker version of this logic was the logic E (from entailment

logic), and the strengthening of R was the logic RM. The logics R and E particularly satisfied the principle of relevance.

Relevance logic is intended to be an attempt to formally define the concept of entailment.

The intuition: between the antecedent of an implication and the succedent we must have some content relationship. This connection cannot be just that the underneath we have just an implication.

Counterexample is Duns Scotus' law. Numerous critics have recognized that classical logic does not describe the entailment correctly.

There have been attempts to find a logic that would omit certain laws that are considered paradoxical, i.e. Duns Scotus' law, the contrapositive law, etc. One of these attempts, which is widely regarded as successful, is the logic of R.

The concept of proof is as usual by means of the concept of consequences.

The theorems of this logic are all that we get from these axioms by means of the notion of proof and rules.

Axioms for R:

- A1. $\phi \rightarrow ((\phi \rightarrow \psi) \rightarrow \psi)$,
- A2. $\phi \rightarrow \phi$,
- A3. $(\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi))$,
- A4. $(\phi \rightarrow (\phi \rightarrow \psi)) \rightarrow (\phi \rightarrow \psi)$,
- A5. $\phi \wedge \psi \rightarrow \phi$,
- A6. $\phi \wedge \psi \rightarrow \psi$,
- A7. $(\phi \rightarrow \psi) \wedge (\phi \rightarrow \chi) \rightarrow (\phi \rightarrow \psi \wedge \chi)$,
- A8. $\phi \rightarrow \phi \vee \psi$,
- A9. $\psi \rightarrow \phi \vee \psi$,
- A10. $(\phi \rightarrow \chi) \wedge (\psi \rightarrow \chi) \rightarrow (\phi \vee \psi \rightarrow \chi)$,

A11. $(\phi \wedge (\psi \vee \chi)) \rightarrow ((\phi \wedge \psi) \vee \chi)$,

A12. $(\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\phi)$,

A13. $\neg\neg\phi \rightarrow \phi$.

Rules:

(MP) Modus Ponens

$$\frac{\phi \rightarrow \psi, \phi}{\psi} \quad (MP)$$

(DK) The conjunction rule

$$\frac{\phi, \psi}{\phi \wedge \psi} \quad (DK)$$

\rightarrow is a connective in the first four axioms. With this set of axioms, we will not be able to prove the contrapositive law, Duns Scotus' law and others considered paradoxical.

The basic property that can be proved in R logic is that the implications that occur there have the same variable in antecedent and succedent. Which means that Duns Scotus' law is false.

If we take implicational version of Duns Scotus' law ($\neg a \rightarrow (a \rightarrow b)$), then we will get classical logic. But conjunctio-
 nal one ($a \wedge \neg a \rightarrow b$) is the best choice.

The undecidability of the R system was proven by A. Urquhart in 1984, but this does not mean that we cannot prove theorems in this calculus. In my bachelor's thesis from 2021, I described F. Fitch's method, which was elaborated in detail by M. Tokarz. This method is similar to classical natural deduction.

Now we will move on to the semantics of logic R.

Matrix semantics

There are two semantics (relational and algebraical) that give the completeness theorem. In the case of R logic, this will be the matrix semantics.

Matrices are theorems that, for any valuation, are included in the set of distinguished elements.

An extreme example is classical logic, where everything is in 1. One of the prominent representatives of this discipline, Robert Meyer, asked the question what would happen if Duns Scotus' law was added to R and if we add Duns Scotus we would get classical logic.

Despite people's surprise, we don't get classical logic.

Relational semantics $\langle U, P, R, g \rangle$, where U is universe, P- set of distinguished elements, relation R, function of negation g. The relation R has additional properties, which we will now omit.

Theorem 1 (The (weak) completeness theorem of R).

The (weak) completeness theorem of R logic has the following form

$\vdash_R \phi \iff$ for any C_R -matrix $\langle \mathbf{A}, \nabla_A \rangle$ and for any valuation h , $h(\phi) \in \nabla_A$.

Theorem 2 (The completeness theorem of R logic).

$\vdash_R \phi \iff$ for any R-structure $\mathcal{A} = \langle U, R, g, \{0\} \rangle$, for any valuation V over this structure, $0 \models \phi$.

RK logic

The algebraic semantics are the same as for R logic.

We define the implication as follows: $(x \rightarrow y) \in \nabla_{\mathbf{A}} \iff x \leq y$, where $\nabla_{\mathbf{A}}$ is set of distinguished elements.

RK logic is logic R + axiom Duns Scotus.

RK logic is superlogic of R logic. Formulas which are not theorems can be added to RK logic so as not to get classical logic.

The aim is to find the maximum extension of RK logic that is not classical logic.

In logic R , we have a structure $\langle U, R, g, P, \leq \rangle$, where U is the universe ($U \neq 0$), R is three-argument relation ($R \subseteq U \times U \times U$), P is set of distinguished elements ($P \subseteq U$). Function g is identity function, so it can be omitted from the structure notation, \leq is reflexive and transitive.

This RK logic is complete when taking only one distinguished element.

Finally, *RK logic* has a structure of the form $\langle U, R, 0 \rangle$, omitting the relation \leq and function g from the notation.

A consequence of the fact that the function g is an identity is that the relation R is "totally symmetric". If $P = \{0\}$, then \leq is diagonal.

Definition 1 (RK-space).

$\mathcal{K} = \langle U, R, 0 \rangle$ is called **RK-space**, if 0 is distinguished element and R is three-argument relation R of set U , which satisfies the four axioms:

1. $R(0, a, b) \iff a = b$,
2. $R(a, a, a)$,
3. $R(a, b, c) \Rightarrow R(b, a, c) \wedge R(a, c, b)$ (totally symmetric),
4. $R(a, b, c) \wedge R(c, d, e) \Rightarrow \exists f(R(a, d, f) \wedge R(f, b, e))$ (**pseudo-Pasch axiom**).

RK relevance logic : lattice of extensions

Logic is located between classical logic and R logic. The question is how many extensions does each such considered logic have? We will address the answer to the question for RK logic. What are the largest extensions of RK logic that are not classical logic?

Conclusion 1. *Each extension of the logic R uniquely corresponds to a certain variety of R -algebras.*

Based on this, one can observe that "the more algebras, the fewer theorems." And we are looking for the smallest algebras.

Thus, the greatest logics correspond to the smallest varieties. Therefore, to find the largest extensions of the logic RK , one must find the smallest subvarieties of the RK -variety.

R and RK logics are determined by a certain variety. The superlogics of R logic are subvariety of R -variety.

Our R -algebra is $\langle \mathbf{A}, \nabla_A \rangle$, where $\nabla_A \subseteq A$ is the set of distinguished values, i.e., the elements that determine tautology.

In the R -variety, there are exactly three minimal R -algebras.

To find the upper part of the lattice of extensions, we will use subdirectly irreducible algebras.

Conclusion 2. *The models of the relevant logic RK are Boolean algebras, that is, distributive lattices with 1 and 0 along with complement. Thus, $x \rightarrow y \neq \neg x \cup y$.*

The largest nontrivial extension of the logic RK is classical logic. We will call R -logics that are directly below the logic $L(2)$ premaximal.

Since RK is an extension of the logic R , the lattice of extensions of RK is a sublattice of the extensions of R . Among the premaximal extensions of the logic R , only the third one is also an extension of RK because its lattice is a Boolean algebra.

Notation:

Instead of listing all triples that are variations of a given triple (x, y, z) we write $(x, y, z)^\circ$. So $(a, 1, 1)^\circ$ to $\{(a, 1, 1), (1, a, 1), (1, 1, a)\}$.

The only premaximal extension of the logic RK is the logic $L(4)$. Now, with the author's permission, we will reference the unpublished results of K. Świrydowicz concerning the classification of infinite countable RK -spaces with one distinguished element.

We will assume that each of the relations R considered below in the space $\langle U, R, 0 \rangle$ contains all triples (x, x, x) and $(0, x, x)$ for all $x \in U$.

1. Totally space, TOT. Relation R in $\langle U, R, 0 \rangle$ is total, i.e. every element $z \neq 0$ is connected with all pair (x, y) , or:

$$R = (U' \times U' \times U') = \{(x, y, z) : x, y, z \in U'\}.$$

2. Completeness binary space \mathbf{B}^{xxy} . Completeness binary

relation is relation $R \subseteq (U' \times U' \times U')$; our R is the smallest relation containing every triple (x, y, y) . Completeness binary space fulfills the condition:

if $x \neq y$, then $(x, x, y) \in R$ and $(y, y, x) \in R$.

3. First weak binary space \mathbf{B}_{up}^{xxy} We will show that there are spaces satisfying the condition

if $x \neq y$, then $(x, x, y) \in R$ or $(y, y, x) \in R$.

Word "or" means that only one of the triples $(x, x, y), (y, y, x)$ belong to R .

Relation R_1 will be defined as the smallest relation consisting of triples

$(n, n + k, n + k), k \geq 0$.

Relation R in first weak binary space we will define as the smallest relation containing the relation R_1 and every triples $(0, n, n)$ for all $n \in U$, where 0 is distinguished element.

4. Second weak binary space \mathbf{B}_{dn}^{xxy} . Second weak binary space forms every triples of the forms $(n + k, n + k, n), k \geq 0$. These are the triples lying at the bottom under the diagonal composed of triples (n, n, n) .

Lemma 1. *Infinite spaces \mathbf{B}_{up}^{xxy} and \mathbf{B}_{dn}^{xxy} are not isomorphic. But finite spaces \mathbf{B}_{up}^{xxy} and \mathbf{B}_{dn}^{xxy} are isomorphic.*

5. Unitary space \mathbf{S}^{1xy} , i.e. **1** Let $R_1 = (U' \times U' \times \{1\}) = \{(1, x, y) : x, y \in U'\}$; in unitary space $R = R_1 \cup \{(x, x, x) : x \in U\} \cup \{(a, x, x) : x \in U\}$.

Fact 1. *Unitary space $\langle U, R, 0 \rangle$ is RK -space.*

An important property of the unitary space is informed by the following lemma; R_1 denotes here the relation defining the unitary space.

Lemma 2. *Let $S \subseteq U' \times U' \times U'$ will be an arbitrary set of triples. If $R = R_1 \cup S$, then structure $\langle U, R, a \rangle$ is RK -space.*

Therefore: Adding to the R_1 relation defining the unitary space of any set of triples gives us RK -space. So, for example, pretabular RK -spaces will be spaces that we will briefly denote by $\mathbf{1} + \mathbf{B}^{(xxy)}$, $\mathbf{1} + \mathbf{B}_{up}^{xxy}$ and $\mathbf{1} + \mathbf{B}_{dn}^{xxy}$.

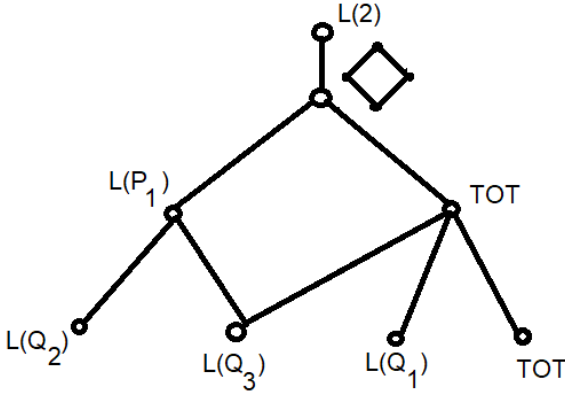
We do not have t, which fulfilled pseudoPasch axiom.

So $\mathbf{B}_{up+(3,3,1)}^4$ is not *RK*-structure .

Fact 2. So, we have 10 *RK*-spaces:

$$\mathbf{B}_{xy}^4, \mathbf{B}_{TOT}^4, \mathbf{B}_{up}^4, \mathbf{B}_{up+1}^4, \mathbf{B}_{up+(2,2,1)}^4, \mathbf{B}_{up+(3,3,2)}^4, \mathbf{1}_{1xy}^4, \\ \mathbf{1}_{1xy+(2,2,3)}^4, \mathbf{1}_{1xy+(3,3,2)}^4, \mathbf{1}_{1xy+(3,3,2)+(2,2,3)}^4.$$

We will see *RK*-spaces in the diagram.



REFERENCES:

- 1 A. R. A. Anderson and N. D. Belnap, Jr. [1975], Entailment, vol. 1, Princeton, p. 558-570.
- 2 L. Maksimowa [1973], Struktury z implikacjami, Algebra i logika, vol. 12, no. 4, pp. 445-467.
- 3 K. Swirydowicz [1995], A remark on the maximal extensions of the relevant logic R, Reports on Mathematical Logic, vol. 29, pp. 19-33.
- 4 A. Urquhart [1996], Duality for algebras of relevant logics, Studia Logica, vol. 56, pp. 277-290.
- 5 Alasdair Urquhart, The Geometry of Relevant Implication, IFCoLog Journal of Logics and their Applications, 4:3:591-604, 2017

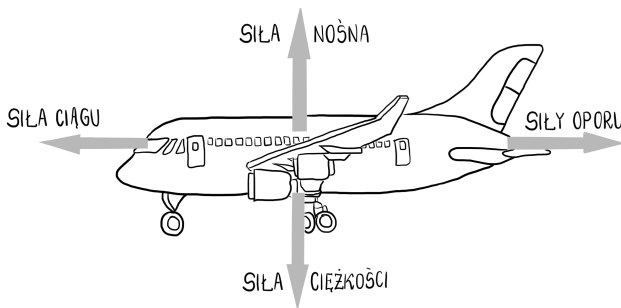
Aerodynamika lotu samolotu

Adrianna Smolińska

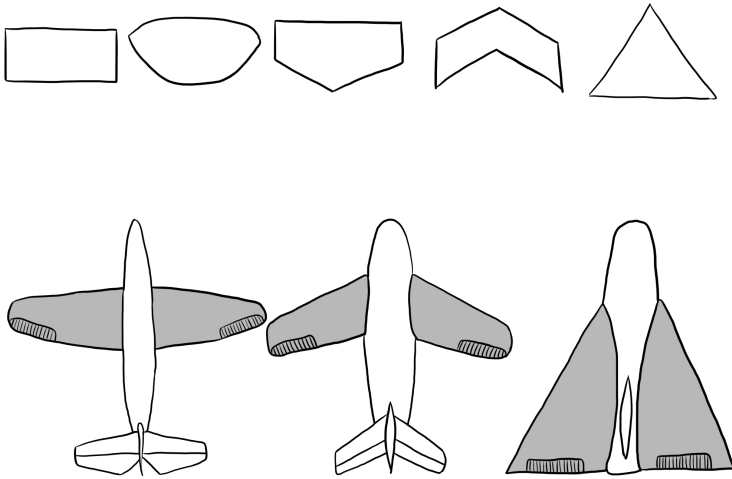
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki
Wydział Fizyki i Astronomii

13.1 Obrys i geometria skrzydła

Samolotem nazwiemy cięższy od powietrza statek powietrzny, napędzany silnikiem lub silnikami, uzyskujący siłę nośną w locie na skutek zjawisk aerodynamicznych występujących głównie na jego powierzchniach pozostających w ustalonym od kadłuba położeniu. *Statek powietrzny* jest dowolnym urządzeniem przeznaczonym do przenoszenia osób lub rzeczy w przestrzeni powietrznej, zdolnym do unoszenia się na skutek wzajemnego oddziaływania konstrukcji oraz powietrza bez równoczesnego oddziaływania tego powietrza na powierzchnię ziemi lub wody.



Istnieje wiele kryteriów pozwalających na klasyfikację samolotów. Dzielimy je np. pod względem przeznaczenia, konstrukcji i napędu, wielkości, liczby silników, liczby miejsc, technologii i funkcji specjalnych, warunków operacyjnych czy techniki lotu. Jednakże my skupimy się na podziale względem obrysu skrzydeł, czyli kształtu widzianego od góry. Najczęściej napotkać możemy obrysy prostokątne, eliptyczne, trapezowe, skośne oraz delty.

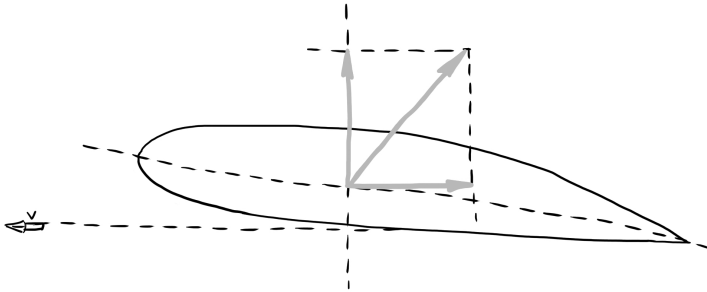


Skrzydła prostokątne rozpoznamy w samolotach raczej prostych konstrukcyjnie, samolotach pasażerskich czy transportowych. Ten rodzaj obrysu pozwala na rozwój względnie małych prędkości, ponieważ nie jest wydajny aerodynamicznie. Skrzydła eliptyczne spotykamy w płatowcach. Jest to doskonały aerodynamicznie obrys, zapewniający znakomitą manewrowość oraz minimalizujący opór powietrza. Skrzydła trapezowe cechują samoloty sportowe czy szybowce. Poprawiają one stabilność i umożliwiają dobrą manewrowość. Skrzydła skośne niekiedy zaliczane są do grupy skrzydeł trapezowych. Jednak te odchylone są od osi samolotu pod pewnym kątem. Stosowane są w samolotach przydźwiękowych oraz naddźwiękowych. Jest to ważna kategoria w

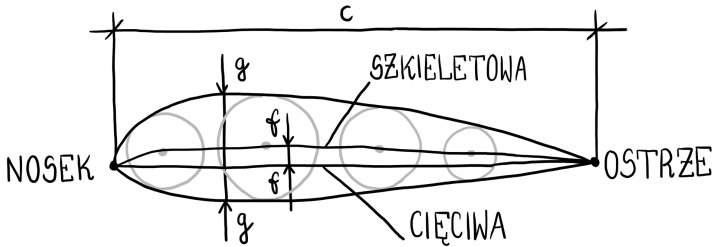
kontekście nowoczesnego lotnictwa wojskowego. Ostatnim z wymienionych obrysów skrzydeł jest delta. Mają one kształt trójkąta, a ich powierzchnia przypomina literę Δ . Stosuje się je w samolotach naddźwiękowych.

W powyższym podziale odwołujemy się do *aerodynamiczności*. W mowie potocznej termin ten wiąże się z kształtem opływowym, przypominającym kroplę, z obiektem, który w czasie ruchu napotyka na mały opór powietrza. Zauważmy, że określenie to nacechowane jest nadto pozytywnie, jakby wiązało się z przekonaniem, że *zawsze* pożądane jest, aby na ciało poruszające się w powietrzu działała minimalna siła aerodynamiczna. Takie rozumienie nie w pełni pokrywa się z rzeczywistością, np. w przypadku pławca preferowana jest jak największa siła aerodynamiczna, jednak *korzystnie* skierowana!

Im mniej wypadkowa siła aerodynamiczna jest odchylna od prostopadłej do kierunku lotu, tym większa jest siła nośna, a mniejszy opór skrzydła. Ta własność wskazuje nam na doskonałość aerodynamiczną skrzydła.



Pojęcie doskonałości aerodynamicznej d skrzydła możemy zdefiniować jako stosunek siły nośnej do oporu skrzydła. Wprowadzenie tej wielkości pozwala na porównywanie własności skrzydeł ze sobą. Zwróćmy jednak uwagę, że wielkość ta nie jest stała i zależy nie tylko od obrysu skrzydła, lecz także od kształtu profilu skrzydła czy ustawienia profilu względem kierunku lotu.



Poprzeczny przekrój skrzydła nazywamy *profilem lotniczym*, krótko *profilem*. Cięciwa to (umowna) prosta, na której „zbudowany” jest profil, najczęściej łączy ona nosek i ostrze. Szkieletowa jest linią łączącą środki kół wpisanych w obrys profilu, a strzałka f to największa odległość między cięciwą a szkieletową. Grubość g profilu jest największą odległością pomiędzy punktami leżącymi na górnym i dolnym obrysie profilu. Odpowiednio dobrane parametry geometrii skrzydła pozwalają na skonstruowanie ich zgodnie z przeznaczeniem samolotu.

Zauważmy, że obrys skrzydeł nie określa jego kształtu, ponieważ sam obrys może mieć różne proporcje rozpiętości skrzydeł b do długości cięciwy c . Tzw. *wydłużenie skrzydła*, czyli proporcję, obliczamy na dwa sposoby. Dla skrzydła prostokątnego jest to $\lambda = \frac{b}{c}$, natomiast dla pozostałych obrysów:

$$\lambda = \frac{b^2}{S},$$

gdzie S jest powierzchnią skrzydła.

13.2 Siła nośna i prawo Bernoulliego

Siła aerodynamiczna R zależy nie tylko od kształtu ciała i jego ustawienia względem kierunku ruchu, lecz także od powierzchni ciała S , gęstości powietrza ρ czy prędkości ruchu v . Zależność tę

przedstawia równanie Bernoulliego:

$$R = c \cdot S \cdot \frac{\rho \cdot v^2}{2},$$

gdzie przez c rozumiemy bezwymiarowy współczynnik siły aerodynamicznej, którego wartość jest warunkowana przez kształt oraz ustawienie ciała względem kierunku opływu. Kluczowym do zrozumienia powstawania sił aerodynamicznych jest, sformułowane przez Daniela Bernoulliego, jedno z podstawowych praw rządzących ruchem powietrza. Wskazuje ono na wzajemne powiązanie między ciśnieniem i prędkością cieczy lub gazu (w zakresie małych prędkości).

Wzdłuż strugi powietrza suma ciśnienia statycznego oraz dynamicznego jest wielkością stałą. Co zapiszemy jako:

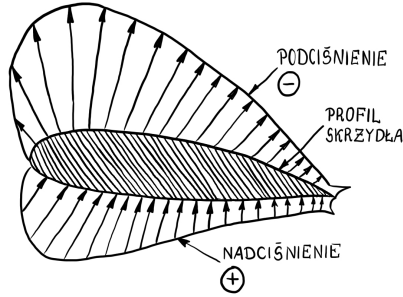
$$p + \frac{\rho \cdot v^2}{2} = \text{constans},$$

gdzie poprzez p rozumiemy ciśnienie statyczne, natomiast $\frac{\rho \cdot v^2}{2}$ jest ciśnieniem dynamicznym. Zwróćmy uwagę na bezpośredni wniosek płynący w powyższego prawa: jeżeli w jednym z punktów strugi powietrza rośnie prędkość, to w tym punkcie musi maleć ciśnienie – i odwrotnie.

Siła nośna powstaje głównie na skrzydle samolotu. Wysoce zależy od kształtu profilu skrzydła, kąta natarcia α , pod którym skrzydło ustawione jest do napływających strug powietrza, ciśnienia dynamicznego przepływu (a stąd gęstości powietrza ρ oraz prędkości przepływającego powietrza v) oraz od powierzchni skrzydła. Zależność tę przedstawia wzór:

$$L = c_L \cdot \frac{\rho \cdot v^2}{2} \cdot S,$$

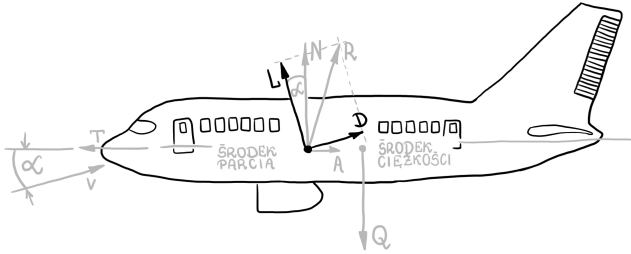
gdzie L jest siłą nośną (prostopadłą do wektora prędkości \vec{v}), c_L to współczynnik siły nośnej, a S jest powierzchnią skrzydła.



To właśnie korzystny rozkład ciśnień, tzn. nadciśnienie na dolnej powierzchni skrzydła, a podciśnienie na górnej, wywołuje siłę nośną. Z prawa Bernoulliego wnioskujemy, że strugi powietrzne szybciej poruszają się wzdłuż górnej niżeli dolnej powierzchni! Aby znaleźć przyczynę tego zjawiska, należy przeanalizować ruch cząstek powietrza. Gdy skrzydło zaczyna się przesuwac, cząstki powietrza rozdzielają się na dwa strumienie, początkowo poruszające się z tą samą prędkością. Górny strumień napotyka na dłuższą do przebycia drogę, przez co strumienie nie mogą spotkać się na krawędzi splywu. Dolny strumień, próbując opłynąć ostrą krawędź, tworzy *wir rozruchowy*. Zgodnie z prawami aerodynamiki, powstałemu wirowi towarzyszy drugi, nazywany *cyrkulacją*. Prędkość cyrkulacji dodaje się do strug powietrza na górnej powierzchni, natomiast odejmuje na dolnej. Teraz strumienie mogą spotkać się na krawędzi splywu! Znika próba omińnięcia ostrej krawędzi, nie ma potrzeby istnienia wiru rozruchowego – ten zostaje uniesiony przez powietrze. Cyrkulacja pozostaje.



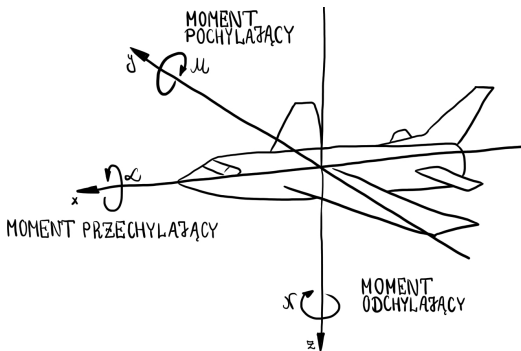
13.3 Podstawy mechaniki lotu



Podczas rozważania lotu samolotu, wypadkową siłę aerodynamiczną R zapisujemy przy użyciu dwóch składowych – siły nośnej L , prostopadłej do wektora prędkości powietrza \vec{v} oraz siły oporu D , równoległej do owego wektora prędkości. Siły te możemy zapisać w lokalnym układzie odniesienia, jako:

$$\begin{cases} L = N \cos \alpha - A \sin \alpha \\ D = N \sin \alpha + A \cos \alpha \end{cases},$$

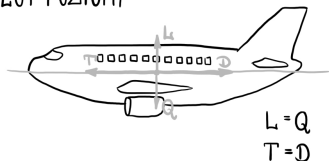
gdzie A jest oporem powietrza. W przypadku lotu ustalonego, tzn. bez przyspieszenia, wartość siły nośnej jest równa sile ciężkości, natomiast siła ciągu równoważy opór.



W przypadku ogólnym środek parcia nie pokrywa się ze środkiem ciężkości. W związku z tym należy zwrócić szczególną uwagę na trzy momenty: *moment pochylający*, który jest wynikiem oddziaływania siły nośnej oraz siły oporu, *moment przechylający*, powstający wskutek różnicy siły nośnej na skrzydłach, oraz *moment odchylający*, powodujący zmianę kąta nachylenia samolotu względem poziomu.

Ruch poziomy samolotu odbywa się, gdy siła nośna równoważy jego ciężar, a ciąg silników jest skierowany poziomo, co pozwala na utrzymanie stałej prędkości i wysokości. W ruchu ślizgowym, przy minimalnej prędkości, siła nośna nie wystarcza do równoważenia ciężaru, co prowadzi do opadania samolotu. Wznoszenie wymaga dodatkowej siły nośnej, co jest związane z odpowiednim kątem natarcia skrzydła oraz wystarczającą prędkością, by generować większą siłę nośną niż ciężar samolotu, natomiast zniżanie jest efektem zmniejszenia tej siły lub obniżenia prędkości, co prowadzi do spadku wysokości.

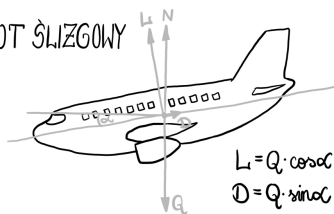
LOT POZIOMY



$$L = Q$$

$$T = D$$

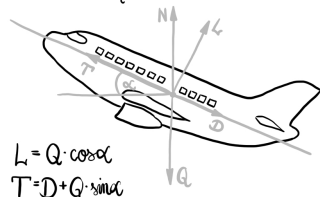
LOT ŚLIZGOWY



$$L = Q \cdot \cos \alpha$$

$$D = Q \cdot \sin \alpha$$

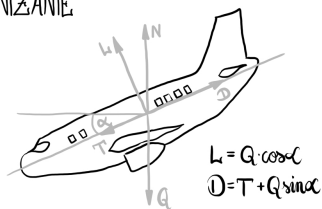
LOT WZNOŚZĄCY



$$L = Q \cdot \cos \alpha$$

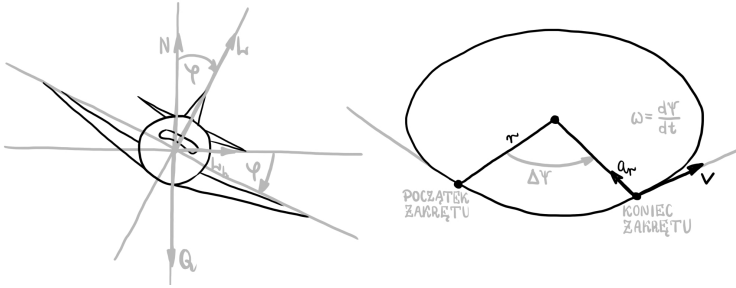
$$T = D + Q \cdot \sin \alpha$$

ZNIŻANIE



$$L = Q \cdot \cos \alpha$$

$$D = T + Q \cdot \sin \alpha$$



W przypadku zakrętu samolotu, musi znajdować się on pod pewnym kątem przechylenia φ tak, by odpowiednie składowe siły nośnej równoważyły siłę ciężkości oraz odśrodkową. Zachodzi:

$$L_v = L \cos \varphi = Q \quad \text{oraz} \quad L_h = \sqrt{L^2 + Q^2}.$$

Po wprowadzeniu współczynnika przeciążenia $n = \frac{L}{Q}$, mamy:

$$n = \frac{1}{\cos \varphi} \quad \text{oraz} \quad L_h = Q \sqrt{n^2 - 1}.$$

Znając przyspieszenie dośrodkowe $a_r = \frac{v^2}{r}$, którego doświadcza samolot w ustalonym zakręcie o promieniu r , możemy explicite zapisać siłę odśrodkową działającą na samolot w kierunku poziomym, skąd mamy:

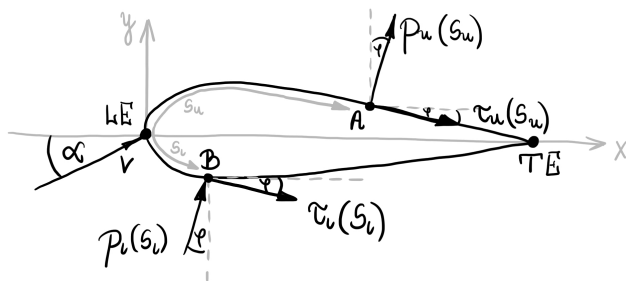
$$L_h = \frac{Qv^2}{gr}.$$

Ostatecznie zapiszemy zależności:

$$r = \frac{v^2}{g\sqrt{n^2 - 1}} = \frac{v^2}{g \operatorname{tg} \varphi} \quad \text{oraz} \quad \omega = \frac{d\psi}{dt} = \frac{g\sqrt{n^2 - 1}}{v} = \frac{g \operatorname{tg} \varphi}{v}.$$

Zwróćmy uwagę, że powyższe równania potwierdzają znane fakty o manewrowości samolotów. Aby wykonać ostry zakręt, tzn. taki o małym promieniu r , należy zmniejszyć prędkość lub dopuścić większe przeciążenia! Dopuszczalne maksymalne przeciążenia są determinowane przez ograniczenia konstrukcyjne oraz ludzkie, natomiast minimalna prędkość lotu jest bezpośrednią konsekwencją ograniczeń aerodynamicznych.

13.4 Siły i momenty



Rozważamy profil aerodynamiczny ustawiony pod kątem α w jednorodnym przepływie z prędkością v . Na powierzchni płata generowana jest całkowita siła aerodynamiczna R oraz moment aerodynamiczny M dla ogólnego przypadku. Analizując stronę ssącą, tzn. górną, składowe siły aerodynamicznej możemy wyrazić następująco:

$$\begin{aligned} dN_u &= -p_u ds_u \cos \varphi - \tau_u ds_u \sin \varphi, \\ dA_u &= -p ds_u \sin \varphi + \tau_u ds_u \cos \varphi. \end{aligned}$$

W przypadku strony ciśnieniowej, czyli dolnej, otrzymujemy:

$$\begin{aligned} dN_l &= p_l ds_l \cos \varphi - \tau ds_l \sin \varphi, \\ dA_l &= p_l ds_l \sin \varphi + \tau ds_l \cos \varphi. \end{aligned}$$

Całkując powyższe zależności, uzyskujemy wartości składowych normalnych i stycznych siły aerodynamicznej, w lokalnym dla rozpatrywanego płata układzie odniesienia:

$$N = - \int_{LE}^{TE} (p_u \cos \varphi + \tau \sin \varphi) ds_u + \int_{LE}^{TE} (p_l \cos \varphi - \tau_l \sin \varphi) ds_l$$

oraz

$$A = \int_{LE}^{TE} (-p_u \sin \varphi + \tau \cos \varphi) ds_u + \int_{LE}^{TE} (p_l \sin \varphi + \tau_l \cos \varphi) ds_l.$$

Nieskończenie mały moment aerodynamiczny od ssającej i ciśnieniowej części płata, mamy dany jako:

$$\begin{aligned}dM_u &= (p_u \cos \varphi + \tau \sin \varphi) ds_u x + (-p_u \sin \varphi + \tau_u \cos \varphi) ds_u y, \\dM_l &= (-p_l \cos \varphi + \tau_l \sin \varphi) ds_l x + (p_l \sin \varphi + \tau_l \cos \varphi) ds_l y.\end{aligned}$$

Całkując powyższe równania, otrzymujemy całkowity moment względem krawędzi natarcia:

$$\begin{aligned}M_{LE} &= \int_{LE}^{TE} [(p_u \cos \varphi + \tau_u \sin \varphi)x + (-p_u \sin \varphi + \tau_u \cos \varphi)y] ds_u \\ &+ \int_{LE}^{TE} [(-p_l \cos \varphi + \tau_l \sin \varphi)x + (p_l \sin \varphi + \tau_l \cos \varphi)y] ds_l.\end{aligned}$$

Bibliografia

- [1] L., Szutkowski *Budowa i pilotaż samolotów lekkich. Przewodnik pilota i instruktora.*, Avia-Test, Poznań, 2007,
- [2] A. Abłamowicz, W. Nowakowski, *Podstawy aerodynamiki i mechaniki lotu*, Wydawnictwa Komunikacji i Łączności, Warszawa, 1980r.,
- [3] Dr inż. Zbigniew Rarata, *Aerodynamika 2, wykład 1: Wprowadzenie, podstawowe informacje z zakresu mechaniki lotu* [Wykład], Politechnika Warszawska, 2021r.

k -Kontatkowe układy Liego

Tomasz Sobczak

Uniwersytet Warszawski
Wydział Fizyki

14.1 Wstęp

Zanim wprowadzimy główne zagadnienia tego referatu, rozważmy kilka standardowych systemów równań różniczkowych.

Dla każdego układu jednorodnych, liniowych równań różniczkowych zwyczajnych pierwszego stopnia na \mathbb{R}^n postaci

$$\frac{dy^i}{dt} = \sum_{j=1}^n A_j^i(t)y^j, \quad i = 1, \dots, n, \quad (14.1)$$

gdzie funkcje $A_j^i(t)$, dla $i, j = 1, \dots, n$, zależą od parametru $t \in \mathbb{R}$, ogólne rozwiązanie (14.1) można wyrazić jako kombinację n liniowo niezależnych rozwiązań $y_{(1)}(t), \dots, y_{(n)}(t)$ równania (14.1) w postaci

$$y(t) = \sum_{j=1}^n k_j y_{(j)}(t), \quad (14.2)$$

gdzie k_1, \dots, k_n są dowolnymi stałymi. To wyrażenie nazywane jest **liniową regułą superpozycji** dla (14.1).

W ogólnym przypadku, poprzez wprowadzenie dyfeomorfizmu $\varphi : \mathbb{R}^n \ni y \mapsto \varphi(y) = x \in \mathbb{R}^n$, równania postaci (14.1) stają się nieliniowym układem zapisanym w sposób następujący

$$\frac{dx^i}{dt} = X^i(t, x), \quad i = 1, \dots, n. \quad (14.3)$$

Ze względu na (14.1), układ ten dopuszcza regułę superpozycji, którą można zapisać jako

$$x(t) = \varphi \left(\sum_{j=1}^n k_j \varphi^{-1}(x_{(j)}(t)) \right) \quad (14.4)$$

dla dowolnej rodziny $x_{(1)}(t), \dots, x_{(n)}(t)$ szczególnych rozwiązań układu (14.3). Powyższy wzór pokazuje, że istnieje wiele układów równań różniczkowych zwyczajnych pierwszego stopnia, których ogólne rozwiązania można wyrazić nieliniowo za pomocą dowolnej rodziny szczególnych rozwiązań i stałych. Przykładem takiego układu jest dowolne równanie Riccatiego postaci

$$\frac{dx}{dt} = b_1(t) + b_2(t)x + b_3(t)x^2, \quad (14.5)$$

gdzie $x \in \mathbb{R}, t \in \mathbb{R}$ oraz $b_1(t), b_2(t), b_3(t)$ są dowolnymi funkcjami zależnymi od t . Ogólne rozwiązanie równania (14.5) ma postać

$$x(t) = \frac{x_{(1)}(t)(x_{(3)}(t) - x_{(2)}(t)) - kx_{(2)}(t)(x_{(3)}(t) - x_{(1)}(t))}{x_{(3)}(t) - x_{(2)}(t) - k(x_{(3)}(t) - x_{(1)}(t))}, \quad (14.6)$$

gdzie $k \in \mathbb{R}$ oraz $x_{(1)}(t), x_{(2)}(t), x_{(3)}(t)$ są trzema różnymi szczególnymi rozwiązaniami równania (14.5).

Definicja 14.1. Układ jednorodnych równań różniczkowych zwyczajnych na M postaci

$$\frac{dx}{dt} = X(t, x), \quad (14.7)$$

dla t -zależnego pola wektorowego na M posiada **zasadę superpozycji**, jeśli istnieje t -niezależna funkcja $\Phi : M^m \times M \rightarrow M$ postaci

$$x = \Phi(x_{(1)}, \dots, x_{(m)}; k), \quad (14.8)$$

taka, że ogólne rozwiązanie równania (14.7) można zapisać jako

$$x(t) = \Phi(x_{(1)}(t), \dots, x_{(m)}(t); k), \quad (14.9)$$

gdzie $x_{(1)}(t), \dots, x_{(m)}(t)$ jest uogólnioną rodziną szczególnych rozwiązań układu (14.7), a k jest elementem M .

Istnieją pewne subtelne problemy związane z powyższą definicją i znaczeniem "uogólnionej" rodziny. Są one głównie techniczne i opisane w [4], dlatego pominiemy ich szczegółowy komentarz. Powiemy tylko, że dziedzina Φ jest w rzeczywistości pewnym otwartym podzbiorem $M^m \times M$.

14.2 Twierdzenie Liego i układy Liego

Po wprowadzeniu definicji zasady superpozycji, rodzi się naturalne pytanie: które układy równań różniczkowych pierwszego rzędu w formie normalnej przyjmują zasadę superpozycji? Warunki konieczne i wystarczające zostały dostarczone przez Sophusa Liego, a jego wynik jest znany jako *Twierdzenie Liego* [5].

Twierdzenie 14.2 (Twierdzenie Liego). *Układ równań różniczkowych pierwszego rzędu (14.7) na rozmałości M przyjmuje zasadę superpozycji (14.8) wtedy i tylko wtedy, gdy odpowiadające mu t -zależne pole wektorowe X można przedstawić w postaci*

$$X(t, x) = \sum_{\alpha=1}^r b_{\alpha}(t)X_{\alpha}(x), \quad (14.10)$$

gdzie X_1, \dots, X_r to rodzina pól wektorowych na M , tworząca r -wymiarową rzeczywistą algebrę Liego pól wektorowych V na M .

Dla przykładu, równanie Riccatiego opisuje krzywe całkowite t -zależnego pola wektorowego na \mathbb{R} postaci

$$X(t, x) = (b_1(t) + b_2(t)x + b_3(t)x^2) \frac{\partial}{\partial x}.$$

X można przedstawić jako liniową kombinację trzech pól wektorowych na \mathbb{R}

$$X_1 = \frac{\partial}{\partial x}, \quad X_2 = x \frac{\partial}{\partial x}, \quad X_3 = x^2 \frac{\partial}{\partial x},$$

które spełniają relacje komutacyjne:

$$[X_1, X_2] = X_1, \quad [X_1, X_3] = 2X_2, \quad [X_2, X_3] = X_3.$$

Z tego wynika, że równania Riccatiego posiadają regułę superpozycji. Jak wcześniej, istnienie reguły superpozycji (14.6) implikuje, że (14.2) przyjmuje wartości w pewnej algebrze Liego o wymiarze 3 lub mniejszym. Można pokazać, że pola wektorowe (14.2) rozpinają algebrę Liego izomorficzną z $\mathfrak{sl}(2, \mathbb{R})$ [6], która jest trójwymiarowa. Ponieważ reguła superpozycji (14.6) zależy od trzech szczególnych rozwiązań, równania Riccatiego spełniają warunek Liego.

14.3 Geometria kontaktowa

Nowatorskim podejściem do analizy układów Liego i związanych z nimi pól wektorowych rozpinających skończenie wymiarową algebrę Liego jest potraktowanie ich jako k -Hamiltonowskie pola wektorowe związane ze strukturą k -kontaktową. Dla lepszego zrozumienia tego podejścia, warto przytoczyć podstawowe definicje i własności struktur kontaktowych oraz pojęć z nimi związanych [3].

Definicja 14.3. Niech M będzie gładką rozmaitością wymiaru m .

- **Dystrybucja uogólniona** na M to podzbiór $D \subset \mathcal{T}M$ taki, że $D_x = D \cap \mathcal{T}_x M$ jest podprzestrzenią wektorową $\mathcal{T}_x M$ dla każdego $x \in M$. Wartość $\dim D_x$ nazywamy **rzędem** dystrybucji D w punkcie $x \in M$.
- Dystrybucja D jest **gładka**, jeśli można ją lokalnie przedstawić w bazie złożonej z rodziny pól wektorowych, tzn. istnieje dla każdego $x \in M$ rodzina pól wektorowych X_1, \dots, X_r określonych w sąsiedztwie U punktu x , taka że $D_{x'} = \langle X_1(x'), \dots, X_r(x') \rangle$ dla każdego $x' \in U$.
- Dystrybucja D jest **regularna**, jeśli jest gładka i ma lokalnie stały rząd.

Definicja 14.4. Rozważmy gładką rozmaitość M nieparzystego wymiaru $2n + 1$. Forma różniczkowa $\eta \in \Omega^1(M)$ taka, że

$\eta \wedge (d\eta)^n$ jest formą objętościową na M , nazywana jest **formą kontaktową**. W takim przypadku (M, η) nazywa się **rozmaitością kontaktową**.

Warto zauważyć, że warunek $\eta \wedge (d\eta)^n \neq 0$ implikuje, że forma kontaktowa η indukuje dekompozycję wiązki stycznej TM w postaci $TM = \ker \eta \oplus \ker d\eta \equiv \mathcal{D}_C \oplus \mathcal{D}_R$.

Stwierdzenie 14.5. *Dla danej rozmaitości kontaktowej (M, η) , istnieje jedyne pole wektorowe $R \in \mathfrak{X}(M)$, zwane **połem wektorowym Reeba**, takie że*

$$\begin{cases} \iota_R d\eta = 0, \\ \iota_R \eta = 1. \end{cases} \quad (14.11)$$

*Pole wektorowe Reeba R generuje dystrybucję \mathcal{D}_R , zwaną **dystrybucją Reeba**.*

Użytecznym faktem związanym ze strukturą kontaktową jest istnienie lokalnych współrzędnych kanonicznych, zwanych **współrzędnymi Darboux**

Twierdzenie 14.6 (Twierdzenie Darboux dla rozmaitości kontaktowych). *Rozważmy rozmaitość kontaktową (M, η) o wymiarze $2n + 1$. Wówczas, w otoczeniu każdego punktu $p \in M$ istnieje lokalny układ współrzędnych $\{q_i, p_i, s\}$, gdzie $i = 1, \dots, n$, taki, że*

$$\eta|_U = ds - p_i dq^i.$$

*Te współrzędne nazywane są **współrzędnymi Darboux** rozmaitości kontaktowej (M, η) .*

Ważną własnością formy kontaktowej jest fakt, że można ją opisywać Hamiltonowskie układy dynamiczne.

Twierdzenie 14.7. *Dla rozmaitości kontaktowej (M, η) , dla każdego $H \in C^\infty(M)$, istnieje jedyne pole wektorowe $X_H \in \mathfrak{X}(M)$, nazywane **Hamiltonowskim polem wektorowym**, takie, że*

$$\begin{aligned} i(X_H)d\eta &= dH - (\mathcal{L}_R H)\eta, \\ i(X_H)\eta &= -H. \end{aligned} \quad (14.12)$$

Rozważając współrzędne Darboux (q^i, p_i, s) na rozmaiłości kontaktowej (M, η) , Hamiltonowskie pole wektorowe lokalne przyjmuje postać

$$X_H = \frac{\partial H}{\partial p_i} \frac{\partial}{\partial q^i} - \left(\frac{\partial H}{\partial q^i} + p_i \frac{\partial H}{\partial s} \right) \frac{\partial}{\partial p_i} + \left(p_i \frac{\partial H}{\partial p_i} - H \right) \frac{\partial}{\partial s}.$$

Równania na krzywą całkową tego pola, $\gamma(t) = (q^i(t), p_i(t), s(t))$, we współrzędnych Darboux mają postać

$$\begin{cases} \dot{q}^i = \frac{\partial H}{\partial p_i}, \\ \dot{p}_i = - \left(\frac{\partial H}{\partial q^i} + p_i \frac{\partial H}{\partial s} \right), \\ \dot{s} = p_i \frac{\partial H}{\partial p_i} - H. \end{cases}$$

14.4 Geometria k -kontaktowa

Geometria k -kontaktowa pojawiła się niedawno jako rozszerzenie geometrii kontaktowej do opisu teorii pól niezachowawczych [2, 7]. Wiele jej właściwości rozszerza te związane zarówno z rozmaiłościami kontaktowymi, jak i rozmaiłościami k -symplektycznymi.

Definicja 14.8. Forma k -kontaktowa na rozmaiłości M jest jednoformą o wartościach w \mathbb{R}^k , postaci $\eta = \sum_{\alpha=1}^k \eta^\alpha \otimes e_\alpha$, spełniającą:

- (i) $\mathcal{D}^C := \ker \eta = \bigcap_{\alpha=1}^k \ker \eta^\alpha$ jest regularną dystrybucją rzędu k ,
- (ii) $\mathcal{D}^R := \ker d\eta = \bigcap_{\alpha=1}^k \ker d\eta^\alpha$ jest regularną dystrybucją rzędu k ,
- (iii) $\mathcal{D}^C \cap \mathcal{D}^R = \{0\}$.

Para (M, η) , gdzie η jest formą k -kontaktową, nazywana jest **rozmaiłością k -kontaktową**. Dystrybucje \mathcal{D}^C nazywamy **dystrybucją kontaktową**, a \mathcal{D}^R nazywamy **dystrybucją Reeba** rozmaiłości (M, η) .

Jeśli $\dim M = n + nk + k$ dla pewnego $n \in \mathbb{N}$ oraz M zawiera dystrybucję całkowaną \mathcal{V} zawartą w \mathcal{D}^C z rank $\mathcal{V} = nk$, mówimy, że $(M, \boldsymbol{\eta}, \mathcal{V})$ jest **rozmaitością k -kontaktową z polaryzacją**. Dystrybucja \mathcal{V} nazywana jest **polaryzacją** $(M, \boldsymbol{\eta})$.

Stwierdzenie 14.9. *Dla rozmaitości k -kontaktowej $(M, \boldsymbol{\eta})$, istnieje jedyne k -pole wektorowe $\mathbf{R} = \sum_{\alpha=1}^k R_\alpha \otimes e_\alpha$ na M takie, że*

$$\iota_{R_\alpha} \eta^\beta = \delta_\alpha^\beta, \quad \iota_{R_\alpha} d\eta^\beta = 0, \quad \forall \alpha, \beta = 1, \dots, k,$$

gdzie ι_{R_α} oznacza iloczyn wewnętrzny z R_α .

Definicja 14.10. Dla rozmaitości k -kontaktowej $(M, \boldsymbol{\eta})$, k -**połem wektorowym Reeba** $\mathbf{R} (M, \boldsymbol{\eta})$ jest k -pole wektorowe opisane w Stwierdzeniu 14.9. Pola wektorowe $R_1, \dots, R_k \in \mathfrak{X}(M)$ nazywamy **polami wektorowymi Reeba** rozmaitości k -kontaktowej $(M, \boldsymbol{\eta})$.

Twierdzenie 14.11 (Twierdzenie Darboux dla rozmaitości k -kontaktowych z polaryzacją). *Niech $(M, \boldsymbol{\eta}, \mathcal{V})$ będzie rozmaitością k -kontaktową z polaryzacją. Wówczas wokół każdego punktu $x \in M$ istnieją lokalne współrzędne $\{q^i, p_i^\alpha, s^\alpha\}$ na otwartym sąsiedztwie punktu x , gdzie $1 \leq \alpha \leq k$ i $1 \leq i \leq n$, takie że*

$$\boldsymbol{\eta} = \sum_{\alpha=1}^k \left(ds^\alpha - \sum_{i=1}^n p_i^\alpha dq^i \right) \otimes e_\alpha.$$

W tych współrzędnych,

$$\mathcal{D}^R = \langle R_\alpha = \frac{\partial}{\partial s^\alpha} \rangle, \quad \mathcal{V} = \langle \frac{\partial}{\partial p_i^\alpha} \rangle.$$

Lokalne współrzędne $\{q^i, p_i^\alpha, s^\alpha\}$ nazywane są **współrzędnymi Darboux**.

W ogólności, współrzędne Darboux dla rozmaitości k -kontaktowych bez polaryzacji nie istnieją.

Definicja 14.12. Niech (M, η) będzie rozmaiłością k -kontaktową z polami wektorowymi Reeba R_1, \dots, R_k . Pole wektorowe $X \in \mathfrak{X}(M)$ jest **η -Hamiltonowskie**, jeśli

$$\begin{cases} \iota_X d\eta^\alpha = dh^\alpha - (R_\alpha h^\alpha)\eta^\alpha, \\ \iota_X \eta^\alpha = -h^\alpha, \end{cases} \quad \alpha = 1, \dots, k,$$

dla pewnej funkcji $\mathbf{h} = \sum_{\alpha=1}^k h^\alpha \otimes e_\alpha \in \mathcal{C}^\infty(M, \mathbb{R}^k)$. Przez $\mathfrak{X}_\eta(M)$ oznaczamy przestrzeń pól wektorowych η -Hamiltonowskich. Ponadto, funkcja $\mathbf{h} \in \mathcal{C}^\infty(M, \mathbb{R}^k)$ jest nazywana **η -Hamiltonowską**. Przez $\mathcal{C}_\eta^\infty(M)$ oznaczamy przestrzeń funkcji η -Hamiltonowskich.

14.5 k -Kontaktowe układy Liego

Przypomnijmy standardową teorię systemów Liego w kontekście rozmaiłości kontaktowych. Szczegółowe omówienie można znaleźć w [1].

Definicja 14.13. Kontaktowym układem Liego nazywamy trójkę (M, η, X) , gdzie η jest formą kontaktową na M , a X jest systemem Liego na M , którego najmniejsza algebra Liego, V^X , jest rzeczywistą algebrą Liego skończonego wymiaru pól wektorowych hamiltonowskich względem η . Kontaktowy układ Liego nazywamy **zachowawczym**, jeśli funkcje hamiltonowskie wektorów pola w V^X są całkami pierwszymi wektora Reeba rozmaiłości (M, η) .

Okazuje się, że nie wszystkie układy Liego są kontaktowymi układami Liego. Wprowadzenie pojęcia k -kontaktowych układów Liego pozwala na analizę znacznie większej liczby przykładów.

Definicja 14.14. k -Kontaktowym układem Liego nazywamy trójkę (M, η, X) , gdzie η jest formą k -kontaktową na M , a X jest systemem Liego na M , którego najmniejsza algebra Liego, V^X , składa się z η -Hamiltonowskich pól wektorowych.

k -Kontaktowy układ Liego nazywamy *zachowawczym*, jeśli funkcje η -Hamiltonowskie związane z polami wektorowymi w V^X są pierwszymi całkami pól Reeba rozmaitości (M, η) . Taką algebrę Liego nazywamy **algebrą Liego–Hamiltona**.

Przykład 14.15. *Rozważmy rozmaitość \mathbb{R}^5 wyposażoną w standardowe współrzędne $\{q, p_1, p_2, z_1, z_2\}$. Rozmaitość \mathbb{R}^5 posiada naturalną dwu-kontaktową formę daną przez jednoformę*

$$\eta = (dz_1 - p_1 dq) \otimes e_1 + (dz_2 - p_2 dq) \otimes e_2.$$

Powiązane z nią pola Reeba to $R_1 = \frac{\partial}{\partial z_1}$ i $R_2 = \frac{\partial}{\partial z_2}$. Rozważmy następujące pola wektorowe na M :

$$X_0 = \frac{\partial}{\partial z_1}, \quad X_1 = \frac{\partial}{\partial z_2}, \quad X_2 = \frac{\partial}{\partial q}, \quad X_3 = q \frac{\partial}{\partial q} - p_1 \frac{\partial}{\partial p_1} - p_2 \frac{\partial}{\partial p_2},$$

$$X_4 = z_1 \frac{\partial}{\partial z_1} + z_2 \frac{\partial}{\partial z_2} + q \frac{\partial}{\partial q}.$$

Te pola wektorowe są hamiltonowskie względem (\mathbb{R}^5, η) z funkcjami hamiltonowskimi:

$$h_0 = (-1, 0), \quad h_1 = (0, -1), \quad h_2 = (p_1, p_2), \quad h_3 = (p_1 q, p_2 q),$$

$$h_4 = (-z_1 + q p_1, -z_2 + q p_2).$$

Pola te tworzą pięciowymiarową algebrę Liego VG z relacjami komutacyjnymi:

$$[X_0, X_1] = 0, \quad [X_0, X_2] = 0, \quad [X_0, X_3] = 0, \quad [X_0, X_4] = X_0,$$

$$[X_1, X_2] = 0, \quad [X_1, X_3] = 0, \quad [X_1, X_4] = X_1,$$

$$[X_2, X_3] = X_2, \quad [X_2, X_4] = X_2,$$

$$[X_3, X_4] = 0.$$

To pozwala zdefiniować dwu-kontaktowy system Liego na \mathbb{R}^5 względem η , dany przez (\mathbb{R}^5, η, X) , gdzie

$$X = \sum_{\alpha=0}^4 b_\alpha(t) X_\alpha, \tag{14.13}$$

gdzie $b_0(t), \dots, b_4(t)$ są funkcjami zależnymi od czasu takimi, że $V^X = \langle X_0, X_1, X_2, X_3, X_4 \rangle$.

Powyższe rozważanie jest przykładem niezachowawczego układu Liego, którego nie da się opisać za pomocą standardowych technik wykorzystywanych w geometrii kontaktowej. Istnieje wiele innych przykładów, gdzie podejście k -kontaktowe ułatwia klasyfikację oraz analizę układów Liego występujących w matematyce czy fizyce. Z tego względu nie tylko interesującym, ale i użytecznym wydaje się rozwijanie tej teorii i aplikowanie jej do bardziej skomplikowanych systemów.

Bibliografia

- [1] J. de Lucas and X. Rivas. *Contact Lie systems: theory and applications*. J. Phys. A: Math. Theor., 56(33):335203, 2023
- [2] J. Gaset, X. Gracia, M. C. Munoz-Lecanda, X. Rivas, and N. Roman-Roy. *A contact geometry framework for field theories with dissipation*. Ann. Phys., 414:168092, 2020.
- [3] X. Rivas. *Geometrical aspects of contact mechanical systems and field theories*. PhD thesis, Universitat Politècnica de Catalunya (UPC), 2021.
- [4] J. F. Carinena and J. de Lucas. *Lie systems: theory, generalisations, and applications*. Dissertationes Math., 479:1–162, 2011
- [5] S. Lie. *On differential equations possessing fundamental integrals*. Leipziger Berichte, 1893.
- [6] J. F. Carinena and A. Ramos. *A new geometric approach to Lie systems and physical applications*, 2001
- [7] J. Gaset, X. Gracia, M. C. Munoz-Lecanda, X. Rivas, and N. Roman-Roy. *A k -contact Lagrangian formulation for non-conservative field theories*. Rep. Math. Phys., 87(3):347–368, 2021.

Topologiczne czary w n -wymiarowym świecie

Julia Ścisłowska

Uniwersytet Warszawski

Wydział Matematyki, Informatyki i Mechaniki

15.1 Prolog

15.1.1 Topolożek w Jaskini Teoriowymiarowców

Pewnego razu młody Topolożek (młody obywatel Puszczy Topologów; jeszcze nie topolog, już nie topuś) zawędrował do Jaskini Teoriowymiarowców, w której były przeróżne magiczne matematyczności związane z teorią wymiaru. Były tam np. eliksiry, dzięki którym można było mieć wymiar fraktalny równy r , gdzie r - dowolna liczba z \mathbb{R}_+ , a także bryły posklejane dziwacznie z kryształowych kul (czasem kryształowych sfer), które po policzeniu „odpowiednich wymiarów” pokazywały dowolnie wybrany zakątek matematycznego świata.

Topolożek znalazł w Jaskini Teoriowymiarowców sekretną księgę, zwaną Księgą Zakłęb. Nasz bohater otworzył ją - ale z nim zaczął czytać, coś przykuło jego uwagę - w Księdze znajdowała się czysta kartka. Topolożek położył ją na stole i zaczął czytać Księgę Zakłęb na głos.

15.1.2 Co napisano w Księdze Zakłęb?

„*Additivum nullen closerum!*” - zawołał Topolożek. Ku jego zdumieniu, na dotychczas pustej kartce ukazał się napis:

Twierdzenie 15.1 (*Additivum nullen closerum*).

Jeśli $X = \bigcup_{i \in \mathbb{N}} F_i$, gdzie $\forall_i F_i$ - domknięty, zerowymiarowy, to X - zerowymiarowa.

Podkscytowanie Topolożka osiągało wszelkie suprema. Ciąg emocji biegał po całym jego ciele i choć biegał i biegał, to nie był rozbieżny - miał dość sporo punktów skupienia w okolicach topologicznego, otwartego serca naszego bohatera, który, cały rozemocjonowany, wyczytał drugie zakłęb: „*Produktivum nullen!*”. Na niezwyklej kartce pojawiła się wówczas treść:

Twierdzenie 15.2 (*Produktivum nullen*).

Jeśli X jest produktem przeliczalnie wielu przestrzeni zerowymiarowych, to X - zerowymiarowa.

„A zatem sprawa będzie toczyć się wokół zerowymiarowości”, pomyślał Topolożek, gładząc swoją clopeniastą bazę. Sam czuł się dość mocno zerowymiarowo wobec dziwacznej Księgi Zakłęb (no i przy okazji był niezłe niespójny). Mimo to zerowymiarowość zaczęła na niego działać niczym narkotyk, więc dalej czytał treści zakłęb: „*Decompositionus nulldimgraden*” - gdy tylko wypowiedział kolejne zakłęb, na kartce znów pojawiły się jakieś nowe słowa.

Twierdzenie 15.3 (*Decompositionus nulldimgraden*).

Przestrzeń metryczna ośrodkowa X spełnia: $\dim(X) \leq n \iff X = Z_0 \cup Z_1 \cup \dots \cup Z_n$, gdzie $\forall_i \dim(Z_i) \leq 0$.

Topolożek myślał: „Czy to jawa, czy sen? Zabierzcie mnie do realnego świata... ewentualnie do zespolonego, choć realny byłby najlepszy”. Czuł się coraz dziwniej i dziwniej - narkotyczne działanie zerowymiarowości robiło swoje. Podniecenie Topolożka zaczęło zamieniać się w furję, która za wszelką cenę pragnęła przeciwstawić się narastającej zerowymiarowości. To wszystko było takie nierzeczywiste. Topolożek pragnął wrócić do swojej

ulubionej podprzestrzeni Puszczy Topologów, czyli do swojego bezpiecznego, metryzowalnego domku.

Topolożek ucieszył się, gdy ujrzał dość realnie brzmiące zakłęcie. Przeczytał: „*Realitum interraccio*” - na kartce ukazało się wówczas:

Twierdzenie 15.4 (Realitum interraccio).

Jeśli $X \subseteq \mathbb{R}$, to $\dim(X) = 0 \iff X$ - brzegowy.

Topolożek rozejrzał się wokół. „No i gdzie ta rzeczywistość” - myślał sobie - „znów zerowymiarowość?!” Topolożek poczuł, że zaraz sięgnie swoich asymptot i wybuchnie. Dziedzina jego życia nie była raczej zbyt zwarta, a jego funkcja życiowa była ciągła - więc chyba mógłby sobie pozwolić na wybuchanie od czasu do czasu? Topolożek ujrzał w Księdze Zakłęt adekwatny tekst: „*Homeodimensoro bum bum*”. Przeczytał go, akcentując szczególnie mocno dwa ostatnie bumbumowe słowa. Wówczas na kartce ukazał się napis:

Twierdzenie 15.5 (Homeodimensoro bum bum).

Jeśli $X \stackrel{\text{homeo}}{\simeq} Y$, to $\dim(X) = \dim(Y)$.

Topolożek już - już liczył na słodkie nieistnienie w zbiorze pustym. Ale jak widać, bumbumowanie wcale nie skończyło jego męki z tą dziwną magią.

Topolożek zadał w myślach funkcję nieciągłą na niewinnym zwierzaczku topologicznym (to bardzo niekulturalne, proszę tak nie robić!) i poszedł spać, nie wiedząc, co sądzić o tej dziwnej przygodzie.

A w międzyczasie, zamiast gapić się na pochrapującego Topolożka, przenieśmy się do Krainy Wielu Wymiarów i opowiedzmy coś niecoś matematycznego bardziej.

15.2 To i owo z podstawowego teoriiwymiarowego definicjoznawstwa

Najpierw poczynimy istotne założenia ontologiczne: wszystko, co żyje w eksplorowanym przez nas zakątku Puszczy Topolo-

gów, jest metryzowalne i ośrodkowe (tzn. zakładamy, że każda przestrzeń, którą będziemy rozważać, posiada te cechy).

Wprowadzimy teraz definicję wymiaru pokryciowego dim .

Niech $\mathcal{U} = \{U_0, U_1, U_2, \dots\}$ będzie pokryciem przestrzeni X . **Rząd pokrycia** \mathcal{U} , ozn. $ord(\mathcal{U})$, to najmniejsze takie $n \in \mathbb{N} \cup \{-1\}$, dla którego każde $n + 2$ elementy \mathcal{U} mają puste przecięcie (oraz ∞ , gdy nie ma takiego n). Przykładowo:

- $ord(\mathcal{U}) = -1 \iff \mathcal{U} = \{\emptyset\}$.
- $ord(\mathcal{U}) = 0 \iff \mathcal{U}$ zawiera zbiór niepusty i ma elementy parami rozłączne.

Mówimy, że pokrycie \mathcal{A} jest **wpisane** w pokrycie \mathcal{B} , ozn. $\mathcal{A} \prec \mathcal{B}$, jeśli $\forall A \in \mathcal{A} \exists B \in \mathcal{B} : A \subseteq B$.

Każdej przestrzeni regularnej X (tzn. $X \in T_3$) przypisujemy **wymiar pokryciowy** $dim(X)$, będący liczbą $n \in \mathbb{N} \cup \{-1\}$ lub ∞ , spełniający następujące warunki:

1. $dim(X) = -1 \iff X = \emptyset$,
2. $dim(X) \leq n \iff$ w każde skończone pokrycie otwarte X można wpisać skończone pokrycie otwarte X rzędu $\leq n$,
3. $dim(X) = n \iff dim(X) \leq n \wedge \neg(dim(X) \leq n - 1)$,
4. $dim(X) = \infty \iff \forall n \in \mathbb{N} \neg(dim(X) \leq n)$.

Dobrze wiedzieć, że topologiczni mędrcy rozważają również inne definicje wymiaru przestrzeni topologicznej, np. mały/duży wymiar indukcyjny ind/Ind . Ale dla X - metryzowalnej ośrodkowej zachodzi: $ind = Ind = dim$.

15.3 Sen Topolożka

Topolożek ujrzał w swoim śnie Króla Aniołów, który przemówił do niego złocistym głosem:

Twierdzenie 15.6 (Twierdzenie Zasadnicze Wszelkich Wymiarów Wszelkich Światów).

Przestrzeń euklidesowa \mathbb{R}^n ma wymiar n .

Topolożek wyśnił cały dowód Twierdzenia Zasadniczego Wszelkich Wymiarów Wszelkich Światów, ale była to bardzo prywatna część jego snu (więc ją zachowamy w tajemnicy). Ale za to opowiemy o czymś, co śniło mu się od razu potem.

Niech \mathbb{Q}_k^n będzie zbiorem punktów w \mathbb{R}^n , które mają dokładnie k współrzędnych wymiernych. Niech \mathbb{N}_n^k będzie zbiorem punktów w \mathbb{R}^n , które mają co najwyżej k współrzędnych wymiernych, czyli:

$$\mathbb{N}_n^k = \mathbb{Q}_0^n \cup \mathbb{Q}_1^n \cup \dots \cup \mathbb{Q}_k^n.$$

Niech \mathbb{L}_n^k będzie zbiorem punktów w \mathbb{R}^n , które mają co najmniej k współrzędnych wymiernych, czyli:

$$\mathbb{L}_n^k = \mathbb{Q}_k^n \cup \mathbb{Q}_{k+1}^n \cup \dots \cup \mathbb{Q}_n^n.$$

Przestrzeń \mathbb{N}_n^{2n+1} nazywamy **przestrzenią Nöbelinga** lub **kostką Nöbelinga**.

Lemat 15.7. $\dim(\mathbb{Q}_k^n) = 0$.

Dowód. Wybieramy ciąg k indeksów: $i_1 < i_2 < \dots < i_k \leq n$ oraz k liczb wymiernych $q_1, q_2, \dots, q_k \in \mathbb{Q}$. Rozważamy produkt:

$$\prod_{i=1}^n r_i, \text{ gdzie: } r_i = \begin{cases} \mathbb{R}, & \text{gdy } i \notin \{q_1, q_2, \dots, q_k\}, \\ \{q_i\}, & \text{gdy } i \in \{q_1, q_2, \dots, q_k\}. \end{cases}$$

Rozpatrzmy przestrzeń $\mathbb{Q}_n^k \cap \prod_{i=1}^n r_i \subseteq \mathbb{R}^n$. Na k współrzędnych w $\mathbb{Q}_n^k \cap \prod_{i=1}^n r_i$ wybraliśmy singleton liczby wymiernej, na pozostałych $n - k$ współrzędnych w \mathbb{Q}_n^k wybraliśmy liczby niewymierne. Dlatego zachodzi:

$$\mathbb{Q}_n^k \cap \prod_{i=1}^n r_i \stackrel{\text{homeo}}{\simeq} (\mathbb{R} \setminus \mathbb{Q})^{n-k}.$$

Homeomorfizm zachowuje wymiary, więc skoro $\dim(\mathbb{R} \setminus \mathbb{Q}) = \dim(\mathbb{R} \setminus \mathbb{Q})^{n-k} = 0$, to $\dim(\mathbb{Q}_n^k \cap \prod_{i=1}^n r_i) = 0$. Ale suma po

wyborach i_j oraz q_i wynosi \mathbb{Q}_n^k , czyli $\bigcup(\mathbb{Q}_n^k \cap \prod_{i=1}^n r_i) = \mathbb{Q}_n^k$. Ponadto $(\mathbb{Q}_n^k \cap \prod_{i=1}^n r_i)$ są domkniętymi podzbiorami \mathbb{Q}_n^k (więc mogliśmy skorzystać z twierdzenia Additivum nullen closerum).
Q.E.D.

Lemat 15.8. $ind(\mathbb{N}_k^n) = k$.

Dowód. Wiemy, że:

$$\mathbb{N}_n^k = \mathbb{Q}_0^n \cup \mathbb{Q}_1^n \cup \dots \cup \mathbb{Q}_k^n.$$

$$\mathbb{L}_n^k = \mathbb{Q}_k^n \cup \mathbb{Q}_{k+1}^n \cup \dots \cup \mathbb{Q}_n^n.$$

Na mocy tw. o rozkładzie (Decompositionus nullidimgraden) mamy: $dim(\mathbb{N}_n^k) \leq k$ oraz $dim(\mathbb{L}_n^k) \leq n - k$. Mamy też rozkład całej przestrzeni \mathbb{R}^n postaci: $\mathbb{R}^n = \mathbb{N}_n^k \cup \mathbb{L}_n^k$. Stąd wynika: $dim(\mathbb{N}_n^k) = k$, $dim(\mathbb{L}_n^k) = n - k$.
Q.E.D.

15.4 Topolożek obudził się...

...i zobaczył wiedźmę!

*Myślałeś - mówi wiedźma - że **Księga Zaklęć** wraz z tymi wszystkimi twierdzeniami to coś, co należy Ci się za darmo? Otóż nie! Równoważna wymiana tak działa - coś dostalesz, coś musisz dać od siebie. Ale ja Cię poszantażuję ciutkę, he, he, bo mogę. To ja Ci podsunęłam tę książeczkę... właśnie, oddawaj! - wiedźma wyrwała smutnemu Topolożkowi Księgę Zaklęć z rąk i tak zaczęły się Cierpienia Młodego Topolożka. Wiedźma dalej przemawiała i pograżała Topolożkowi: *Albo wymyślisz mi zaklęcie na zanurzenie dowolnej przestrzeni n - wymiarowej w przestrzeń Nöbelinga, albo zostaniesz rozatomiony i pogromiony! To znaczy, he, he, he, że każdy punkcik Twojego ciała zrobi się izolowany, a Ty, roztopologizowany, zginiesz dyskretną śmiercią. Co wybierasz? - spytała wiedźma.**

15.5 Topolożek uczy się, aby pokonać wiedzmę

Szkolenie matematyczne wypada zacząć od definicji...

Definicja 15.9. Ustalmy $\varepsilon > 0$. Niech $f : X \rightarrow Y$ będzie ciągłą. Mówimy, że f jest ε -**przekształceniem**, jeśli

$$\forall_{y \in Y} \text{diam}(f^{-1}(\{y\})) < \varepsilon.$$

...ale jedna definicja to za mało, by uczciwie zgłębiać tajniki topologicznego świata! Topolożek wytrwale podowodził co nieco ważnych lematów, które mogły odmienić jego los w batalii ze złowrogą wiedzmą. A oto i one:

Lemat 15.10. *Załóżmy, że $\varepsilon > 0$, X – zwarta, Y – metryczna, ośrodkowa. Niech G_ε będzie zbiorem ε -przekształceń z X w Y . Wtedy G_ε jest otwarty w przestrzeni funkcyjnej $(C(X, Y), d_{sup})$.*

Dowód. Niech $g \in G_\varepsilon$. Znajdziemy kulę wokół g zawartą w G_ε . Niech

$$r = \inf\{\text{dist}(g(x_1), g(x_2)) : x_1, x_2 \in X, \text{dist}(x_1, x_2) \geq \varepsilon\}.$$

Ze zwartości X istnieją $x_1, x_2 \in X$ takie, że $r = \text{dist}(g(x_1), g(x_2))$ (bo kresy funkcji ciągłych na zb. zwartym są przyjmowane). Oczywiście $g(x_1) \neq g(x_2)$ - wynika to stąd, że gdyby $g(x_1) = g(x_2) = y$, to przeciwobraz $g^{-1}(\{y\})$ nie byłby zawarty w kuli o promieniu ε , czyli otrzymalibyśmy sprzeczność z tym, że g jest ε -przekształceniem. Zatem $r > 0$. Wtedy $B(g, \frac{r}{2}) \subseteq G_\varepsilon$. Q.E.D.

Lemat 15.11. *Załóżmy, że X – zwarta, Y – zupełna. Wtedy $(C(X, Y), d_{sup})$ jest zupełna.*

Dowód. Niech $(f_n)_{n \in \mathbb{N}}$ będzie ciągiem Cauchy'ego w $(C(X, Y), d_{sup})$. Pokażemy, że jest on zbieżny. Wiemy (z zupełności Y), że dla dowolnego $x \in X$ zachodzi: $f_n(x) \rightarrow f(x)$ przy $n \rightarrow \infty$. Ustalmy $\varepsilon > 0$. Ponieważ $(f_n)_{n \in \mathbb{N}}$ jest ciągiem Cauchy'ego, to istnieje takie n_0 , że $\forall_{n, m \geq n_0} \forall_{x \in X}$ zachodzi: $\text{dist}(f_n(x), f_m(x)) < \varepsilon$.

Przy ustalonym n , przechodząc z m do nieskończoności, dostajemy: $\text{dist}(f_n(x), f(x)) < \varepsilon$ dla $n \geq n_0, x \in X$. Z dowolności ε wiemy, że ciąg $(\{\sup(\text{dist}(f_n(x), f(x)) : x \in X)\}_{n \in \mathbb{N}})$ zbiega do 0 przy $n \rightarrow \infty$. Pokazaliśmy więc, że $d_{\text{sup}}(f, f_n)$ zbiega do 0 przy $n \rightarrow \infty$. Q.E.D.

Lemat 15.12. *Załóżmy, że X – zwarta, $f : X \rightarrow Y$ – ciągła surjekcja. Wtedy żeby f było zanurzeniem potrzeba i wystarcza, żeby f było $\frac{1}{n}$ -przekształceniem dla każdego $n \in \mathbb{N}$.*

Dowód. Jeśli f nie jest $\frac{1}{k}$ -przekształceniem dla pewnego k , to niech x_1, x_2 będą oddalone o więcej niż $\frac{1}{k}$ takie, że $f(x_1) = f(x_2)$ – czyli f nie jest 1-1, czyli nie może być homeomorfizmem. W drugą stronę: skoro $\forall_n f$ jest $\frac{1}{n}$ - przekształceniem, to jest ona różnowartościowa. Korzystamy z faktu, że ciągła bijekcja z przestrzeni zwartej na przestrzeń Hausdorffa jest homeomorfizmem. Q.E.D.

Lemat 15.13. $\mathbb{R}^{2n+1} \setminus \mathbb{N}_n^{2n+1} = \bigcup_{k \in \mathbb{N}} H_k$, gdzie $\forall_k H_k$ – pewna podprzestrzeń afiniczna w \mathbb{R}^{2n+1} wymiaru n .

Dowód. Wiemy, że:

$$\mathbb{R}^{2n+1} \setminus \mathbb{N}_n^{2n+1} = \{\mathbf{x} : \mathbf{x} \text{ ma co najmniej } n + 1 \text{ współrzędnych wymiernych}\}$$

Zauważmy więc, że:

$$\mathbb{R}^{2n+1} \setminus \mathbb{N}_n^{2n+1} = \bigcup_{\substack{i_0, i_1, \dots, i_n \\ \in \{1, 2, \dots, 2n+1\}}} \bigcup_{\substack{(q_0, \dots, q_n) \\ \in \mathbb{Q}^{n+1}}} \{\mathbf{x} \in \mathbb{R}^{2n+1} : x_{i_0} = q_0, \dots, x_{i_n} = q_n\}.$$

Wiemy też, że zbiór:

$$H = \{\mathbf{x} \in \mathbb{R}^{2n+1} : x_{i_0} = q_0, \dots, x_{i_n} = q_n\}$$

to hiperpłaszczyzna wymiaru n . Wszystkie hiperpłaszczyzny postaci

$$\{\mathbf{x} \in \mathbb{R}^{2n+1} : x_{i_0} = q_0, \dots, x_{i_n} = q_n\}$$

dla pewnych $i_0, i_1, \dots, i_n \in \{1, 2, \dots, 2n + 1\}$ i $(q_0, \dots, q_n) \in \mathbb{Q}^{n+1}$ ustawiamy w ciąg H_0, H_1, H_2, \dots numerowany \mathbb{N} . Q.E.D.

Lemat 15.14. *Niech G_k będzie zbiorem $\frac{1}{\varepsilon}$ -przekształceń z X w przestrzeń $\mathbb{R}^{2n+1} \setminus H_k$. Wówczas G_k jest otwarty i gęsty w $C(X, \mathbb{R}^{2n+1})$.*

Dowód. Z lematu 15.10 zbiór $\frac{1}{k}$ -przekształceń jest otwarty w $C(X, \mathbb{R}^{2n+1})$. Zbiór przekształceń o obrazie rozłącznym z H_k też jest otwarty w $C(X, \mathbb{R}^{2n+1})$. Zatem G_k jest otwarty w $C(X, \mathbb{R}^{2n+1})$.
Q.E.D.

Udowodnienie gęstości zbioru G_k w $C(X, \mathbb{R}^{2n+1})$ wykracza poza ramy tego artykułu - dociekliwego Czytelnika spragnionego szczegółów zachęcamy do zajrzenia do paragrafów 1.11 i 1.12 w monografii [ksiązka].

15.6 Topolożek i wiedźma - ostateczne starcie

Wreszcie Topolożek stanął oko w oko ze swoim matematycznym przeznaczeniem. Dane mu było topologizować heroicznie i niezłomnie, jak na prawdziwego teoriowymiarowca przystało.

Twierdzenie 15.15 (Twierdzenie Mengersa–Nöbelinga). *Załóżmy, że X jest przestrzenią zwartą, metryzowalną i ośrodkową oraz $\dim X \leq n$. Wówczas X można homeomorficznie zanurzyć w przestrzeń Nöbelinga, tzn. istnieje homeomorfizm*

$$h : X \rightarrow h[X] \text{ taki, że } h[X] \subseteq \mathbb{N}_n^{2n+1} \subseteq \mathbb{R}^{2n+1}.$$

Uwaga 15.16. (zob. [1]) *Twierdzenie Mengersa–Nöbelinga jest prawdziwe dla dowolnych przestrzeni metryzowalnych ośrodkowych wymiaru $\leq n$ na mocy twierdzenia o uzwarcaniu (które mówi, że dowolna przestrzeń wymiaru n ma uzwarcanie wymiaru n).*

Dowód twierdzenia Mengersa–Nöbelinga. Dla $k \in \mathbb{N}$ niech G_k będzie zbiorem $\frac{1}{k}$ -przekształceń z X w przestrzeń $\mathbb{R}^{2n+1} \setminus H_k$. Z lematu 15.14 wiemy, że dla każdego k zbiór G_k jest otwarty i

gęsty w $C(X, \mathbb{R}^{2n+1})$. Ponieważ przestrzeń $C(X, \mathbb{R}^{2n+1})$ jest zupełna (na mocy lematu 15.11), to możemy użyć twierdzenia Baire'a, które mówi, że w przestrzeni zupełnej przecięcie przeliczalnie wielu zbiorów otwartych i gęstych jest zbiorem gęstym (więc w szczególności $\bigcap_{k=1}^{\infty} G_k$ jest niepuste). Weźmy $h \in \bigcap_{k=1}^{\infty} G_k$. Wiemy, że wtedy $\forall_k h$ jest $\frac{1}{k}$ -przekształceniem. Z lematu 15.12 h jest zanurzeniem homeomorficznym. Wiemy, że \forall_k obraz $h[X]$ jest rozłączny z H_k , czyli na mocy lematu 15.13 $h[X]$ jest zawarty w \mathbb{N}_n^{2n+1} . To kończy dowód twierdzenia Mengera–Nöbelinga. Q.E.D.

15.7 Zło topologią zwyciężaj!

Topolożek po udowodnieniu twierdzenia Mengera–Nöbelinga uzyskał magiczne moce, o jakich nie śniło się nawet samemu Królowi Aniołów. Więc namierzył wiedźmę, policzył jej wymiar topologiczny (wyszedł on równy k , dla pewnego $k \in \mathbb{N}$), a następnie uwięził nietopolubną czarną charakterkę w przestrzeni Nöbelinga \mathbb{N}_k^{2k+1} .

Przedtem jednak Topolożek odebrał wiedźmie **Księgę Zaklęć**, stał się jej panem i władcą, i po dziś dzień szkoli się na topologa - teoriowymiarowca natchnionego. Oczywiście dalej ma słodkie, topologiczne sny, kto ciekaw, niech sam zdobędzie **Księgę Zaklęć** i się przekona na własnej skórze, jak to jest...

Wszystko dobre, co się topologicznie kończy!

Bibliografia

- [1] Engelking R., *Teoria wymiaru*, Państwowe Wydawnictwo Naukowe, Warszawa 1977 (znana również jako **Księga Zaklęć**).