MathUp

Konferencja Zastosowań Matematyki

Edycja VI

Jak matematyka pomaga w lepszym zrozumieniu rzeczywistości - MathUp 2024

Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki
Centrum Nauczania Matematyki i Fizyki
Politechnika Łódzka

Politechnika Łódzka

SPIS TREŚCI

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

KOD ENIGMY, KLOTOIDY, PORTFEL INWESTYCYJNY I INNE ZASTOSOWANIA MATEMATYKI – MATHUP 2024

Gertruda GWÓŹDŹ-ŁUKAWSKA[1], Monika POTYRAŁA[1]

[1] Politechnika Łódzka, Centrum Nauczania Matematyki i Fizyki

Matematyka ma szereg zastosowań. Wiedzą to: inżynier, doktor matematyki, profesor nauk matematycznych. Chcemy, aby także kandydaci na inżynierów, uczniowie szkół średnich oraz Ty, Czytelniku, mieli szansę przekonać się, że to nie tylko słowa.

Od zarania dziejów matematyka ułatwiała ludziom życie. Jej znajomość (choć szczegółów wciąż nie znamy) pozwalała budować piramidy, pierwsze konstrukcje, a także maszyny bojowe. O współczesnych zastosowaniach nie mówi się jednak ani na lekcjach w szkole, ani tym bardziej w telewizji.

Publikacja ta pokazuje mały wycinek prac, którymi zajmują się młodzi ludzie, niekoniecznie będący matematykami, ale które bezpośrednio łączą się z królową nauk.

Prawdopodobnie świat byłby zupełnie inny, gdyby nie rozwój matematyki związany np. z szyfrowaniem i deszyfrowaniem. To dzięki pracy polskich matematyków w czasach drugiej wojny światowej, złamany został kod Enigmy, co prawdopodobnie ocaliło miliony istnień ludzkich i zmieniło bieg historii. Jak udało się tego dokonać? Jakie kluczowe informacje pomogły odkryć sposób szyfrowania?

Równie ważne z historycznego punktu widzenia są klotoidy. Te piękne krzywe to obiekty matematyczne mające wpływ na nasze bezpieczeństwo. Tym razem chodzi o czasy bardziej współczesne, bo o koniec dziewiętnastego wieku, gdy do kolejek górskich (projektowanych od dwóch wieków) dodano pętle, W naturalny sposób kształt pętli oparty był na okręgu, co okazało się powodować ogromne przeciążenia. Dopiero w 1976 roku w projektach pętli budowanych w Ameryce wykorzystano fragmenty klotoid, co zmniejszyło przeciążenia i sprawiło, że jazda kolejką górską przestała być niebezpieczna. Jaką tajemnicę kryją klotoidy?

XXI wiek to rozwój teleinformatyczny. Nie bez znaczenia jest dokładność i szybkość wykonywanych obliczeń. W analizie sygnałów, przetwarzaniu obrazów jak i w kodowaniu intensywnie wykorzystywana jest analiza Fouriera. Tym samym optymalizacja obliczeń numerycznych podczas obliczania współczynników szeregu Fouriera jest nie do przecenienia. Czy są na to metody?

Trudno jest wyobrazić sobie funkcjonowanie rynku instrumentów finansowych bez matematyki, czy to w przypadku lokat, obligacji, bonów skarbowych, akcji czy funduszy inwestycyjnych. Jak wyznaczyć efektywny portfel? Z odpowiedzią przychodzi teoria optymalizacji z twierdzeniem Karusha-Kuhna-Tuckera. I już mamy narzędzia by rozważać opłacalność planowanej inwestycji.

A jak dokonać analizy finansowej dotyczącej danego papieru wartościowego? Czy możliwe jest, aby techniczne podejście wykorzystywało ciąg Fibonacciego? Jak najbardziej. Fibonacci Time Zones, Fibonacci Retracement, Fibonacci Extension to narzędzia pozwalające wypracować strategie takie jak Harmonic patterns, Crab Pattern, Butterfly Pattern, Bat Pattern. Istnieje też teoria oparta na złotej proporcji – Elliott Wave Theory.

Dokonując jakiejkolwiek inwestycji, trzeba brać pod uwagę czynnik ludzki. Czy można przewidzieć ludzkie zachowanie? Co zrobi w danej sytuacji gracz? Jaką przyjmie strategię? Czym jest równowaga Nasha? Tym razem warto zagłębić się w teorię gier.

A altruizm? Skąd się wziął i co ma wspólnego z matematyką? Otóż to właśnie jedna ze strategii rozważanych w teorii gier. W iterowanym dylemacie więźnia zwycięskie postawy to WetZaWet oraz Obrażalski. Ale co się stanie w kolejnym pokoleniu graczy? Zgodnie z symulacją komputerową, bycie człowiekiem miłym, uczciwym, wybaczalskim, ale takim który nie daje się wykorzystywać i nie jest zazdrosny jest strategią, która najbardziej popłaca. To altruizm popłaca.

Wyjeżdżasz? To już wiesz jak się zachować. Ale jak się spakować? Zapewne znasz Problem plecakowy. Czy znasz również szyfr plecakowy? Łatwy, trudny, jak zaszyfrować, jak deszyfrować – sprawdź się, to nie Enigma – dasz radę.

A może jednak kusi Cię, żeby wspomóc się ChatemGPT? Czy ChatGPT jest dobry na wszystko? Jeśli wiesz już że nie, to jak wytrenować własną sztuczną inteligencję? Najpopularniejsze algorytmy sztucznej inteligencji opierają się na sieciach neuronowych. Aby taką sieć wykorzystać w rozwiązywaniu problemów, musi ona najpierw zostać… wytrenowana. Już dziś zostań nauczycielem sztucznej inteligencji!

Monografia zawiera prace napisane w języku polskim i angielskim. Tworzyli ją studenci entuzjaści, pasjonaci określonych zagadnień matemaycznych. To zaangażowanie autorów sprawia, że złożona tematyka staje się przystępna i wciągająca.

Zachęcamy Cię Czytelniku, byś po zapoznaniu się ze szczegółowymi opisami tych kilku niesamowitych zastosowań wiedzy matematycznej poszperał we własnych pracach, w bibliotece lub choćby w Internecie w celu znalezienia najbardziej zdumiewających przypadków, w których matematyka pomogła człowiekowi.

Podejmij **Challenge**: znajdź zastosowanie, które innym się nawet nie śniło i napisz do nas: mathup@info.p.lodz.pl.
Najciekawsze opisy zostaną umieszczone na stronie mathup.p.lodz.pl, a ich autorów zaprosimy do wygłoszenia referatu na Konferencji Zastosowań Matematyki MathUp.

MATEMATYCZNE SPOSOBY ZŁAMANIA SZYFRU ENIGMY – JAK POLACY DOKONALI NIEMOŻLIWEGO

Daniel ZIELONKA[1]

[1] Uniwersytet Ekonomiczny w Poznaniu

Wstęp

Artykuł ma na celu przybliżenie tematyki początkowej fazy rozszyfrowywania szyfru Enigmy przez Polaków. W przystępny sposób przedstawione zostały zarówno aspekty matematyczne, jak i historyczne. Artykuł nie zawiera wyników autorskich badań, a jedynie jest zbiorem zgromadzonej już wiedzy.

Geneza

Początek Enigmy można datować na wiosnę roku 1918, kiedy to dowództwo niemieckie miało w planach wprowadzenie do służby szyfrowania maszynowego. Jednak ze względu na zbliżającą się klęskę Państw Centralnych i wyczerpujące się środki, pomysł ten został zarzucony. Zrealizowano go dopiero w latach dwudziestych. W roku 1926 wprowadzono Enigmę do Reichsmarine (marynarki), a w roku 1928 do Reichswehry (wojsk lądowych). Były to zmienione wersje Enigmy występującej na rynku cywilnym[1]. Model ten, nazywany Enigmą A[2], służył do ochrony korespondencji i tajemnic handlowych firm.

Polski radiowywiad w roku 1928 rozpoznał, że przechwytuje depesze zaszyfrowane maszynowo. Cechą charakterystyczną szyfru była bardzo zbliżona do siebie częstotliwość występowania wszystkich liter. Podjęto wówczas próby złamania tego szyfru przez językoznawców, jednak żadne z nich nie odniosły zamierzonego efektu. W związku z tym polski radiowywiad postanowił wykorzystać matematykę. W tym celu zorganizowano kurs kryptografii dla najwybitniejszych studentów matematyki Uniwersytetu Poznańskiego, znających biegle język niemiecki. Wśród około dwudziestu studentów wybranych przez prof. Zdzisława Krygowskiego[3], największym talentem odznaczali się Marian Rejewski, Henryk Zygalski i Jerzy Różycki. W późniejszym okresie zostali oni zatrudnieni w referacie Niemieckim Biura Szyfrów Oddziału II Sztabu Głównego.

Enigma zasadniczo składała się z połączeń wtyczkowych, klawiatury, panelu z lampkami oraz wirników szyfrujących, inaczej zwanego mieszadłem. Używała ona szyfru polialfabetycznego, wariacji podstawieniowego, czyli takiego, w którym każda litera zamieniana jest według innego klucza. Działo się tak ze względu na obrót prawego bębenka szyfrującego przy każdym wciśnięciu klawisza klawiatury. Obroty środkowego i lewego wirnika były zależne od nacięć na odpowiednio prawym i środkowym bębnie. Nacięcia te, dla wystąpienia danej litery, były nazywane pozycjami obrotowymi. Dodatkowo, środkowy wirnik przesuwany był przez obrót lewego. Tak więc, by taka sama kombinacja ustawienia wirników powtórzyła się, należało wcisnąć klawisz 16 900 razy[4]. Enigma była maszyną szyfrującą jak i deszyfrującą.

Wpisanie liter zaszyfrowanego tekstu, przy identycznym ustawieniu wirników i wtyczek jak podczas szyfrowania, ujawniało na panelu lampowym litery pierwotnie szyfrowanego tekstu.

Niemcy zdawali sobie sprawę, że maszyna może zostać przechwycona podczas działań wojennych. Postanowili zatem, aby jej tajemnica leżała w czymś łatwo zmienianym, na przykład w kluczach dziennych, czyli początkowym ustawieniu wirników, które było następnie dwukrotnie szyfrowane na początku każdej depeszy.

Początkowo Polacy podchodzili do złamania szyfru Enigmy mało optymistycznie. Dowódca Biura Szyfrów numer 4, major Maksymilian Ciężki, zlecił, by Marian Rejewski w pojedynkę przyjrzał się posiadanym szyfrogramom i ewentualnie spróbował znaleźć zależności umożliwiające złamanie Enigmy. Analiza początków szyfrogramów ujawniła pewne schematy. Jeśli depesze zaczynały się od określonej litery, to litera z czwartej pozycji również się powtarzała. Przykładowo, dla każdej depeszy zaczynającej się od litery **m**, literą na czwartej pozycji była **d**. Takie zależności występowały również między drugą i piątą literą, oraz trzecią i szóstą. Nie było żadnych odstępstw od tej reguły, więc Rejewski wywnioskował, że jest to efektem dwukrotnego zaszyfrowania pewnej trójki liter. Wciskając na klawiaturze na przykład abc abc, zapisywano je w postaci permutacji A B C D E F (dokładniejsze wyjaśnienie permutacji znajduje się poniżej, w części “Słownik” pojęć matematycznych). Określały one przekształcenia liter wybieranych na klawiaturze, na zaszyfrowane przez maszynę. Można to zobrazować w następujący sposób: abc abc -> **m**kj **d**lw (A: a na m, B: b na k, C: c na j, D: a na d, E: b na l, F: c na w). Na podstawie tych danych, próbował on złamać szyfr, poprzez rozwiązanie układu równań, w którym rolę niewiadomych odgrywały permutacje. Niestety, niewiadomych było zbyt wiele, aby jednoznaczne rozwiązanie było możliwe do znalezienia.

Z nieoczekiwaną pomocą polskiemu wywiadowi, w grudniu 1932 roku, przybył wywiad francuski. Dowódca wywiadu radiowego Gustave Bertrand przekazał Polakom opis i rysunek Enigmy Eins, tabele kluczy z września i października 1932. Ważne było to, że pochodziły one z różnych kwartałów tego samego roku, przez co różniły się kolejnością bębenków szyfrujących. Dodatkowo, przekazano przykład szyfrowania, czyli tekst depeszy i odpowiadający mu szyfr. Umożliwiło to obliczenie połączeń wirników między bębnami szyfrującymi.

"Słownik” pojęć matematycznych

Podane tu zostaną podstawowe pojęcia niezbędne dla zrozumienia dalszych wywodów:

- Klucz to informacja umożliwiająca odczytanie danego szyfru, na przykład początkowe ustawienie wirników

- Permutacja A zbioru Ω to różnowartościowe odtworzenie zbioru Ω w siebie. Oznacza to przyporządkowanie każdej literze zbioru innej litery z tego zbioru.

- Stopień permutacji to liczba elementów zbioru Ω. Dla rozważań dotyczących Enigmy zawsze będzie wynosić 26, ze względu na liczbę liter na klawiaturze maszyny. Charakterystyczne niemieckie litery takie jak ä, ö, ü, ß zostały zamienione na ich zwykłe odpowiedniki, a wszystkie znaki interpunkcyjne, w tym spacje, zostały zastąpione literą X.

- Cyklem jest permutacja zbioru Ω, spełniająca warunek: w zbiorze Ω istnieje podzbiór Y taki, że $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, ... , $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$ oraz dla każdego a_i takiego, że a_i nie należy do podzbioru Y zachodzi $\pi(a_i) = a_i$. W praktyce przekłada się to na fakt, że permutacja: A = (a,b,c,d,e) przekształca literę a na b, b na c, ... oraz e z powrotem na a.

- Permutacja tożsamościowa oznaczana najczęściej literą "I", to permutacja, w której każda liczba, bądź litera, zamieniana jest na samą siebie.

- Transpozycją nazywamy cykl dwuwyrazowy, o przykładowej postaci B = (a,b).

- Superpozycja, inaczej zwana jest składaniem (iloczynem) permutacji. Definiujemy ją następująco:

A = [1, A(1)] [2, A(2)] ... [n, A(n)] **B = [1, B (1)] [2, B(2)] ... [n, B(n)]**

AB = [1, B(A(1))] [2, B(A(2))] ... [n, B(A(n))]

Jest ona działaniem nieprzemiennym. Ponadto, jeśli permutacje A i D składają się z samych cykli transpozycji oraz permutacja A zamienia α na c, a permutacja D zamienia α na r, to w superpozycji AD literze c przyporządkowywana jest litera r. Niewiadoma litera α jest jednak różna od r oraz c[4].

- Cykle rozłączne to takie cykle, które nie posiadają ze sobą elementów wspólnych. Czyli, na przykład (a, b, c) i (d, e, f).

- Każda permutacja jest cyklem lub może być przedstawiona w postaci iloczynu cykli rozłącznych, na przykład: A = (a, d, f, e, c, h, g, b); B = (a, d, e, f) (b, c) (g) (h).

- Permutacja odwrotna do permutacji A, zapisywana A^{-1}, to permutacja spełniająca równania:

$$\mathbf{A^{-1}A = AA^{-1} = I.}$$

- Twierdzenie o iloczynie transpozycji: jeśli A i B składają się z samych transpozycji rozłącznych i są tego samego (parzystego) stopnia, to w ich iloczynie występują pary cykli rozłącznych charakteryzujące się tym, że cykle należące do tej samej pary mają tę samą długość:

A = (a, c) (b, g) (h, f) (d, e) **B = (c, b) (g, h) (f, a) (d, e)**

AB = (b, h, a) (f, g, c) (d) (e)

Na podstawie tego twierdzenia można wyciągnąć następujące wnioski:

1) Litery wchodzące w skład tej samej transpozycji permutacji A lub B wchodzą zawsze do 2 różnych cykli tej samej długości permutacji AB:

A = (a, c) (b, g) (h, f) (d, e) **B = (c, b) (g, h) (f, a) (d, e)**

AB = (b, h, a) (f, g, c) (d) (e)

2) Jeżeli 2 litery znajdujące się w 2 różnych cyklach permutacji AB należą do tej samej transpozycji permutacji A albo B, to litery sąsiadujące z nimi w cyklach jedna z prawej strony od pierwszej litery, druga z lewej strony od drugiej litery, też należą do jednej transpozycji permutacji A albo B:

A = (a, c) (b, g) (h, f) (d, e) **B = (c, b) (g, h) (f, a) (d, e)**

AB = (b, h, a) (f, g, c) (d) (e) **AB = (b, h, a) (f, g, c) (d) (e)**

Wywód matematyczny

Rejewski wysnuł twierdzenie, że charakterystyka dnia (pierwsze sześć niezaszyfrowanych liter w nagłówku depeszy) była ustawiana indywidualnie przez szyfrantów, więc mogłaby być podatna na ludzkie błędy. Stwierdził, że szyfranci z lenistwa ustawiali trójki złożone z tych samych trzech liter, czyli np.: aaa, bbb, ccc itd. Okazało się, że trójki zaszyfrowane w ten sposób stanowiły znaczną część wszystkich wiadomości, co umożliwiło dekryptaż. Metodę tę zaczynało się od założenia, że wszystkie permutacje przekształcają taką samą niewiadomą literę, na te z obu trójek depeszy. Tak więc dla pierwszej depeszy występują następujące przekształcenia dla permutacji:

A: α na x B: α na r C: α na w D: α na r E: α na g F: α na s

Numer porządkowy depeszy	Sześć pierwszych liter depeszy
1	xrw rgs
2	chm grt
3	owo qkk
4	ppq cjl
5	fkr xoa
6	ouv qay
7	crx ggg
8	vvb zse
9	uuz yau
10	nnk mld

Tabela numer 1 (pierwotnie zawierała ona 76 pozycji)

Następnie z “dodatkowej własności superpozycji dla permutacji składających się z cykli transpozycji” oraz trójek depesz wyznaczamy iloczyny AD, BE, CF, przyjmujące następujące postacie:

AD = (a, u, y, v, z, i, w) (b, f, x, r, h, j, t) (c, g, n, m, k, p) (d, e, l, s, o, q)
BE = (a, w, k, o, y, m, x, p, j, i, e, t, u) (b, d, f, q, z, n, l, h, r, g, v, s, c)
CF = (a, i, h, m, t, x, g, c, f, q, l, j, r) (b, e, z, u, w, s, o, k, d, p, n, v, y)

Z wniosku 1), z twierdzenia o iloczynie transpozycji, można ustalić, że szukana litera α znajduje się w cyklu tworzącym parę (liczba elementów obu cykli jest taka sama) z cyklem, w którym znajduje się litera, na którą jest zamieniana przez permutacje A, B, C. Dla danych iloczynów są to pogrubione cykle:

AD = ***(a, u, y, v, z, i, w)*** (b, f, x, r, h, j, t) (c, g, n, m, k, p) (d, e, l, s, o, q)
BE = ***(a, w, k, o, y, m, x, p, j, i, e, t, u)*** (b, d, f, q, z, n, l, h, r, g, v, s, c)
CF = ***(a, i, h, m, t, x, g, c, f, q, l, j, r)*** (b, e, z, u, w, s, o, k, d, p, n, v, y)

Litera α nie może się znajdować w cyklach, z którymi ten cykl nie tworzy pary oraz α nie jest literą znajdującą się w cyklu z tą, na którą jest przekształcana. Tak więc, po dalszej eliminacji, α może pierwotnie być literą a lub i. Następnym krokiem jest wyznaczenie permutacji za pomocą wniosku 2) twierdzenia o iloczynie transpozycji. Zakładając, że α to a, transpozycje przyjmują następujące postacie:

A = (x, a) (r, w) (h, i) (j, z) (t, v) (b, y) (f, u) A’
B = (r, a) (g, u) (v, t) (s, e) (c, i) (b, j) (d, p) (f, x) (q, m) (z, y) (n, o) (l, k) (h, w)
C = (w, a) (s, r) (o, j) (k, l) (d, q) (p, f) (n, c) (v, g) (y, x) (b, t) (e, m) (z, h) (u, i)

Część permutacji A jest nam nieznana. Mimo to zestawiamy pierwszą trójkę (po lewej stronie tabeli) z pierwotnie wpisanymi przez niemieckich szyfrantów literami (po prawej stronie tabeli). Następnie patrzymy, czy w tych drugich mogą wystąpić trzykrotne powtórzenia.

c h m	? w e
o w o	? h j
p p q	? d d
f k r	u l s
o u v	? g g
c r x	? a y
v v b	t t t
u u z	f g h
n n k	? o l

Jeśli nie, dana trójka nie jest szyfrogramem jednej litery α. (Jeżeli uznamy, że niewiadoma litera α to i, wówczas żadna z trójek nie może być szyfrogramem jednej litery.) Przyjmując, że szyfrowano trójki o tych samych literach, przekształcenia (p, d) i (o, g) są konieczne, by litera a była szukaną α. Sprawdzamy, czy nie występuje sprzeczność z twierdzeniem o iloczynie transpozycji. Nie powoduje to sprzeczności, a pozwala na jednoznaczne wyznaczenie postaci permutacji A:

A = (x, a) (r, w) (h, i) (j, z) (t, v) (b, y) (f, u) (p, d) (c, q) (g, o) (n, s) (m, l) (k, e)

oraz na całkowite uzupełnienie charakterystyk dnia:

c h m	q w e
o w o	g h j
p p q	d d d
f k r	u l s
o u v	g g g
c r x	q a y
v v b	t t t
u u z	f g h
n n k	s o l

Na nieszczęście Polaków, na początku 1933 roku, niemieckim szyfrantom zakazano używać trójek złożonych z tych samych liter. Wówczas uwidoczniła się tendencja do wybierania trójek z sąsiadujących ze sobą na klawiaturze liter, na przykład q w e, a s d, e r t. Niedługo później te kombinacje zostały zabronione, więc trzeba było opracować inne metody łamania Enigmy.

Pierwszą była metoda statystyczna, badająca upodobania szyfrantów. Okazało się, że pierwszymi literami występującymi najczęściej były q oraz a, drugimi samogłoski, a trzecimi l oraz o. Najrzadszymi literami były y oraz j. Co ciekawe, wprawione osoby zajmujące się nasłuchem radiowym były w stanie rozpoznać po tempie i charakterystyce osobę, a tym samym jednostkę, nadającą wiadomość. Jednak metoda ta była mało praktyczna, bardzo zróżnicowana i trzeba było ją często zmieniać[5].

O wiele bardziej skuteczna była metoda niejednakowych liter. Polegała ona na tym, że po zakazie używania kluczy złożonych z tych samych liter, szyfranci unikali powtarzania jakiejkolwiek. Pierwszym krokiem było wyznaczenie iloczynów AD, BE i CF. Ich przykładowa postać to:

AD = (a, l, d, f, g, v, t, r, b, i, k, q, z) (j, h, e, n, u, s, y, m, c, x, o, w, p)
BE = (a, v, x, b, e, z, u, y, t, c, m, i, p) (d, o, n, w, g, r, k, q, l, j, f, s, h)
CF = (a, b, r, l, w, k, y, j, z, t, f, e, g) (d, x, u, m, i, v, c, q, p, s, o, n, h)

Następnie tworzymy tabelę, w której rzymskimi liczbami I, II, III oznaczone są kolejno cykle iloczynów AD, BE, CF. Za to w kolumny/wiersze oznaczone arabskimi liczbami wpisane są wszystkie możliwe przyporządkowania drugiego cyklu danych iloczynów.

I	1	2	3	4	5	6	7	8	9	10	11	12	13
a	p	w	o	x	c	m	y	s	u	n	e	h	j
l	w	o	x	c	m	y	s	u	n	e	h	j	p
d	o	x	c	m	y	s	u	n	e	h	j	p	w
f	x	c	m	y	s	u	n	e	h	j	p	w	o
g	c	m	y	s	u	n	e	h	j	p	w	o	x
v	m	y	s	u	n	e	h	j	p	w	o	x	c
t	y	s	u	n	e	h	j	p	w	o	x	c	m
r	s	u	n	e	h	j	p	w	o	x	c	m	y
b	u	n	e	h	j	p	w	o	x	c	m	y	s
i	n	e	h	j	p	w	o	x	c	m	y	s	u
k	e	h	j	p	w	o	x	c	m	y	s	u	n
q	h	j	p	w	o	x	c	m	y	s	u	n	e
z	j	p	w	o	x	c	m	y	s	u	n	e	h

II	a	v	x	b	e	z	u	y	t	c	m	i	p
1	h	s	f	j	l	q	k	r	g	w	n	o	d
2	s	f	j	l	q	k	r	g	w	n	o	d	h
3	f	j	l	q	k	r	g	w	n	o	d	h	s
4	j	l	q	k	r	g	w	n	o	d	h	s	f
5	l	q	k	r	g	w	n	o	d	h	s	f	j
6	q	k	r	g	w	n	o	d	h	s	f	j	l
7	k	r	g	w	n	o	d	h	s	f	j	l	q
8	r	g	w	n	o	d	h	s	f	j	l	q	k
9	g	w	n	o	d	h	s	f	j	l	q	k	r
10	w	n	o	d	h	s	f	j	l	q	k	r	g
11	n	o	d	h	s	f	j	l	q	k	r	g	w
12	o	d	h	s	f	j	l	q	k	r	g	w	n
13	d	h	s	f	j	l	q	k	r	g	w	n	o

Tabela numer 2

Kolejnym krokiem jest wstawienie znaku X w kwadraty, znajdujące się na przecięciu kolumn i wierszy, w których powtarzały się litery. Drugą opcją było uzupełnienie kwadratów numerami porządkowymi depesz zamiast X, dla ewentualnego, łatwiejszego sprawdzenia. Jeśli dana komórka jest wykluczana przez dwa lub więcej numerów depeszy, pierwszeństwo ma numer niższy. Całkowicie zapełnione wiersze bądź kolumny są eliminowane z dalszego rozważania.

I	1	2	3	4	5	6	7	8	9	10	11	12	13
a	p	w	o	x	c	m	y	s	u	n	e	h	j
l	w	o	x	c	m	y	s	u	n	e	h	j	p
d	o	x	c	m	y	s	u	n	e	h	j	p	w
f	x	c	m	y	s	u	n	e	h	j	p	w	o
g	c	m	y	s	u	n	e	h	j	p	w	o	x
v	m	y	s	u	n	e	h	j	p	w	o	x	c
t	y	s	u	n	e	h	j	p	w	o	x	c	m
r	s	u	n	e	h	j	p	w	o	x	c	m	y
b	u	n	e	h	j	p	w	o	x	c	m	y	s
i	n	e	h	j	p	w	o	x	c	m	y	s	u
k	e	h	j	p	w	o	x	c	m	y	s	u	n
q	h	j	p	w	o	x	c	m	y	s	u	n	e
z	j	p	w	o	x	c	m	y	s	u	n	e	h

II	a	v	x	b	e	z	u	y	t	c	m	i	p												
1	h	s	f	j	l	q	k	r	g	w	n	o	d	24	18	8	6	19	76	3	58	48	7	21	63	7
2	s	f	j	l	q	k	r	g	w	n	o	d	h	11	5	48	2	63	56	48	44	21	46	57	44	1
3	f	j	l	q	k	r	g	w	n	o	d	h	s	48	48	38	57	54		55	23	41	46	32	10	37
4	j	l	q	k	r	g	w	n	o	d	h	s	f	24	36	19	12	41		40	23	19	4	51		34
5	l	q	k	r	g	w	n	o	d	h	s	f	j	52	55		24	21	52	26		7	13	20	6	46
6	q	k	r	g	w	n	o	d	h	s	f	j	l	47	55	21	37	2	59	37	22	40	13	1	43	56
7	k	r	g	w	n	o	d	h	s	f	j	l	q	24	59		52	52	26	24	51	29	49	43	39	59
8	r	g	w	n	o	d	h	s	f	j	l	q	k	8		12	10		30	35	49	9	6	5	10	36
9	g	w	n	o	d	h	s	f	j	l	q	k	r	40	24	2	16	38	41	35	11	19	26	23	47	53
10	w	n	o	d	h	s	f	j	l	q	k	r	g	18	35	29	16	43	45	34	16	12	23	57	10	60
11	n	o	d	h	s	f	j	l	q	k	r	g	w	59	57	19	42	47	35	36	9	28	11	30	40	21
12	o	d	h	s	f	j	l	q	k	r	g	w	n	28	47	53	11	1	33	41	53	57	37	49	19	
13	d	h	s	f	j	l	q	k	r	g	w	n	o	27	38	9	16	25	18	25	49	2	27	6	1	39

Tabela numer 3

Następnym krokiem jest wykonanie podobnej tabeli, dla superpozycji BE (II) i CF (III).

II	3	4	5	7	***8***	12
a	f	j	l	k	***r***	o
v	j	l	q	r	***g***	d
x	l	q	k	g	***w***	h
b	q	k	r	w	***n***	s
e	k	r	g	n	***o***	f
z	r	g	w	o	***d***	j
u	g	w	n	d	***h***	l
y	w	n	o	h	***s***	q
t	n	o	d	s	***f***	k
c	o	d	h	f	***j***	r
m	d	h	s	j	***l***	g
i	h	s	f	l	***q***	w
p	s	f	j	q	***k***	n

III	a	b	r	l	w	k	y	j	z	t	f	e	g						
1	h	n	o	s	p	q	c	v	i	m	u	x	d	12	29	33	21	7	55
2	n	o	s	p	q	c	v	i	m	u	x	d	h	3	33	55	10	53	27
3	o	s	p	q	c	v	i	m	u	x	d	h	n	30	31	27	11	6	36
4	s	p	q	c	v	i	m	u	x	d	h	n	o	30	36	33	33	15	26
5	***p***	***q***	***c***	***v***	***i***	***m***	***u***	***x***	***d***	***h***	***n***	***o***	***s***	50	14	58	4		10
6	q	c	v	i	m	u	x	d	h	n	o	s	p	55	37	11	48	29	2
7	***c***	***v***	***i***	***m***	***u***	***x***	***d***	***h***	***n***	***o***	***s***	***p***	***q***	44	35	38	15		21
8	v	i	m	u	x	d	h	n	o	s	p	q	c	43	17	5	24	25	34
9	i	m	u	x	d	h	n	o	s	p	q	c	v	20	24	20	43	27	55
10	m	u	x	d	h	n	o	s	p	q	c	v	i	40	53	10	50	11	19
11	u	x	d	h	n	o	s	p	q	c	v	i	m	18	40	60	15	28	33
12	x	d	h	n	o	s	p	q	c	v	i	m	u	14	43	46	35	16	9
13	d	h	n	o	s	p	q	c	v	i	m	u	x	32	33	2	53	1	23

Tabela numer 4

Można zauważyć, że wszystkie kolumny, z wyjątkiem tej oznaczonej "8" zostały wyeliminowane. Oznacza to, że jesteśmy w stanie wyznaczyć jednoznaczną postać permutacji B:

B = (a, ***r***) (v, ***g***) (x, ***w***) (b, ***n***) (e, ***o***) (z, ***d***) (u, ***h***) (y, ***s***) (t, ***f***) (c, ***j***) (m, ***l***) (i, ***q***) (p, ***k***).

Eliminacja kolumn 3, 4, 5, 7, 12 dla superpozycji BE (II) (w *Tabeli numer 4*), powoduje wykluczenie kolumn 3, 6, 8, 12, 13 dla superpozycji AD (I) (w *Tabeli numer 3*). Permutacja C może przybrać dwie formy. Pierwsza z transpozycją (a, p) dla kolumny piątej oraz druga z (a,

c) dla kolumny numer 7. By ostatecznie wyznaczyć jedną, przyrównujemy iloczyny AD (I) i CF (III) w kolejnej tabeli.

													I	2	***5***
													a	w	***c***
													l	o	***m***
													d	x	***y***
													f	c	***s***
													g	m	***u***
													v	y	***n***
													t	s	***e***
													r	u	***h***
													b	n	***j***
													i	e	***p***
													k	h	***w***
													q	j	***o***
													z	p	***x***
III	a	b	r	l	w	k	y	j	z	t	f	e	g		
5	p	q	c	v	i	m	u	x	d	h	n	o	s	60	21
7	***c***	***v***	***i***	***m***	***u***	***x***	***d***	***h***	***n***	***o***	***s***	***p***	***q***	4	

Tabela numer 5

W taki sposób otrzymujemy jednoznaczne postaci permutacji:

A = (a, ***c***) (l, ***m***) (d, ***y***) (f, ***s***) (g, ***u***) (v, ***n***) (t, ***e***) (r, ***h***) (b, ***j***) (i, ***p***) (k, ***w***) (q, ***o***) (z, ***x***)

C= (a, ***c***) (b, ***v***) (r, ***i***) (l, ***m***) (w, ***u***) (k, ***x***) (y, ***d***) (j, ***h***) (z, **n**) (t, **o**) (f, **s**) (e, **p**) (g, **q**)[6]

Przedstawiony proces był jednak bardzo czasochłonny, gdyż zajmował 3-4 godzin z 8-10 potrzebnych na złamanie dziennego szyfru. By przyśpieszyć ten proces polscy kryptolodzy, za pomocą cyklometru, stworzyli katalog cykli, zawierający 80 000 różnych kombinacji. Zajęło im to prawie rok, jednak skrócili ten fragment dekryptażu do około 15 minut. Niestety zmiana w Enigmie dokonana 2 listopada 1937 roku sprawiła, że katalog trzeba było wykonać od nowa. Większość osób dziś myśli, że Enigma została złamana i można było otwierać przysłowiowego szampana. Jednak tak na prawdę była to ciągła walka z czasem oraz o to, kto kogo de facto przeliczy. Warto zaznaczyć, że sukcesy takie jak odczytanie depeszy o pojmaniu żywego lub martwego Ernsta Röhma, rozpoczynające noc długich noży, były dokonane mimo braków finansowych (spowodowanych zarządzeniami oszczędnościowymi lokującymi środki finansowe na funduszu na wypadek wojny). W praktyce “oszczędzone” pieniądze zamiast zostać wydane na ulepszenie stacji radiowych, czy wyprodukowanie większej ilości bomb, cyklometrów bądź Enigm AVA, wydane zostały na budowę zbędnych gmachów[7].

Po klęsce w kampanii wrześniowej

Dnia 5 września zarządzono ewakuację Sztabu Głównego, przy czym 6 września objęła ona Biuro Szyfrów. Pociąg Eszelon F zabrał polskich kryptologów do Bukaresztu. Tam skontaktowali się z francuskim attaché, powołując się na znajomość z "Bolkiem" (Pseudonim Gustavea Bertranda w kontaktach z Polakami), uzyskali pomoc w ucieczce do Francji, kolejno przez Jugosławię i północne Włochy[8]. Polscy kryptolodzy, po dotarciu do Paryża, wznowili swoją pracę w ośrodku "Bruno", na zamku Vignolles. Jednak nawet "Żółte Kartki" (Feuillets Janues) z informacjami o działaniach wojsk niemieckich, rozchwytywane przez dowódców francuskich, nie były w stanie zatrzymać niemieckiego Blitzkriegu. Rozkaz ewakuacji został wydany 10 czerwca 1940 roku. Nową bazą miała być miejscowość La Ferte Saint Aubin. Jednak podpisanie rozejmu przez Pétaina, zmusiło Polaków do dalszej ucieczki do Afryki północnej. Ukrywali się oni tam do przełomu września i października 1940 roku, kiedy to stopniowo zaczęli wracać na południe Francji. Gustave Bertrand, pod pseudonimem "Barsac" zakupił willę w miejscowości Uzès, gdzie zorganizowano ośrodek o kryptonimie "P. C. Cadix". Ze względu na mniejszy zasięg nasłuchu niż w ośrodku "Bruno", odczytywano tam głównie depesze policji i oddziałów okupacyjnych[9]. Do odczytu depesz z działań wojennych powrócono na początku 1941 roku, kiedy to otwarto filię "Cadix", o kryptonimie "Kouba", w Algierze. Między tymi placówkami dochodziło do rotacji personelu, w okresach liczących 3-4 miesiące. Podczas jednej z takich wymian, 9 stycznia 1942 roku, doszło do katastrofy statku Lamoricière, w rejonie Wysp Balearskich. Zginęli w niej Jerzy Różycki, Jan Graliński, Piotr Smoleński oraz François Lane[10].

Dnia 8 listopada 1942 roku, Niemcy, sprowokowani desantem aliantów w Afryce oraz groźbą desantu na południe Francji, przeprowadzili operację o kryptonimie "Attila". Polegała ona na zajęciu Francji Vichy i de facto jej likwidacji. Jako, że ruch oporu posiadał informacje o planach niemieckich sukcesywnie przeprowadził 9 listopada całkowitą ewakuację z terenów Vichy. Zaprowadziła ona polskich kryptologów przez śnieżne szczyty Pirenejów do hiszpańskiego więzienia w Belver, nie daleko Puicerda. Rejewskiemu i Zygalskiemu udało się przedostać do Portugalii dopiero pod koniec sierpnia 1943 roku. Stamtąd przepłynęli na Gibraltar, a następnie przelecieli do Anglii. Na wyspach nie zostali jednak dopuszczeni do prac związanych z Enigmą, ze względu na tak zwaną "ochronę tajemnicy". Dlatego polscy kryptolodzy zajęli się łamaniem szyfrów SS i SD. Oczywiście na efekty nie trzeba było długo czekać. Szyfry te zostały szybko złamane.

Można stwierdzić, że wkład Polaków w rozszyfrowanie Enigmy nie został doceniony. Niemal cała baza teoretyczno-praktyczna została stworzona przez polskich kryptologów. Poczynając od teorii permutacji, na Enigmie AVA, cyklometrze czy bombie kryptologicznej kończąc. Następnie wiedza ta została przekazana wywiadowi brytyjskiemu i francuskiemu na konferencji w podwarszawskich Pyrach 25 lipca 1939 roku. Dokładniej przekazano dokumentację i polskie kopie Enigmy wraz z częściami zamiennymi[11]. Jedna z najważniejszych publikacji dotycząca Enigmy, czyli "The Ultra Secret" Fredericka Williama Winterbothama, ogranicza role Polaków jedynie do wykradnięcia, a następnie przekazania Enigmy Brytyjczykom. Złamanie jej szyfru jest według autora zasługą jedynie pracowników Bletchley park[12]. Pierwsza wzmianka na zachodzie, o rzeczywistej roli Polaków w złamaniu szyfru Enigmy pojawia się w publikacji Gustava Bertranda "Enigma ou la plus grande énigme de la guerre 1939–1945", wydanej w 1973 roku.

Jednak nie znajdują się w niej nazwiska “ojców” sukcesu, czyli Rejewskiego, Zygalskiego i Różyckiego. Dodatkowo podaje on błędną datę złamania Enigmy. Zamiast przełomu 1932/1933 pada 1939 rok. Jest to zrozumiałe, gdyż kooperacja polsko-francuska nie była aż tak rozwinięta, a strona polska ukrywała fakt złamania szyfru Enigmy aż do 1939 roku. Dzisiejsza popkultura, na przykład film “Gra Tajemnic” z 2014 roku, odzwierciedla brytyjskie, błędne postrzeganie udziału Polaków w rozszyfrowaniu Enigmy. Można jedynie mieć nadzieję, że z czasem postrzeganie to zostanie zmienione.

Literatura

[1] Gaj, K., Szyfr Enigmy Metody Złamania. Wydawnictwa Komunikacji i Łączności, pp. 9, 1989
[2] *Louis Kruh, Cipher Deavours. The Commercial Enigma: Beginnings of Machine Cryptography. „Cryptologia”.*
[3] Gaj, K., Szyfr Enigmy Metody Złamania. Wydawnictwa Komunikacji i Łączności, pp. 10, 1989
[4] Gaj, K., Szyfr Enigmy Metody Złamania. Wydawnictwa Komunikacji i Łączności, pp. 54, 1989
[5] Gaj, K., Szyfr Enigmy Metody Złamania. Wydawnictwa Komunikacji i Łączności, pp. 113, 1989
[6] Gaj, K., Szyfr Enigmy Metody Złamania. Wydawnictwa Komunikacji i Łączności, pp. 113-120, 1989
[7] Kozaczuk, W., Bitwa o tajemnice: Służby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939 (wyd4). Wydawnictwo Książka i Wiedza, pp. 200-205, 1977
[8] Kozaczuk, W., Złamany Szyfr. Wydawnictwo Ministerstwa Obrony Narodowej, pp. 76 1976
[9] Kozaczuk, W., Złamany Szyfr. Wydawnictwo Ministerstwa Obrony Narodowej, pp. 114-121 1976
[10] Gaj, K., Szyfr Enigmy Metody Złamania. Wydawnictwa Komunikacji i Łączności, pp. 27, 1989
[11] Mazur, Sz, Zbiory Centrum Szyfrów Enigma; https://csenigma.pl/enigma/spotkanie-w-pyrach/. Wydawnictwo Miejskie Posnania
[12] Kozaczuk, W., Złamany Szyfr. Wydawnictwo Ministerstwa Obrony Narodowej, pp. 86-89 1976

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

BEZPIECZEŃSTWO W DRODZE I NIESAMOWITE PRZEŻYCIA W PARKU ROZRYWKI, CZYLI O KLOTOIDACH SŁÓW KILKA

Jerzy DUDEK[1]

[1] Politechnika Łódzka, Łódź

Wstęp

Niniejszy artykuł opisuje matematyczne właściwości krzywych zwanych klotoidami, jak również historyczny kontekst ich odkrycia. Przedstawia on także przykłady praktycznego zastosowania tych obiektów w różnych dziedzinach życia codziennego.

Definicja klotoidy

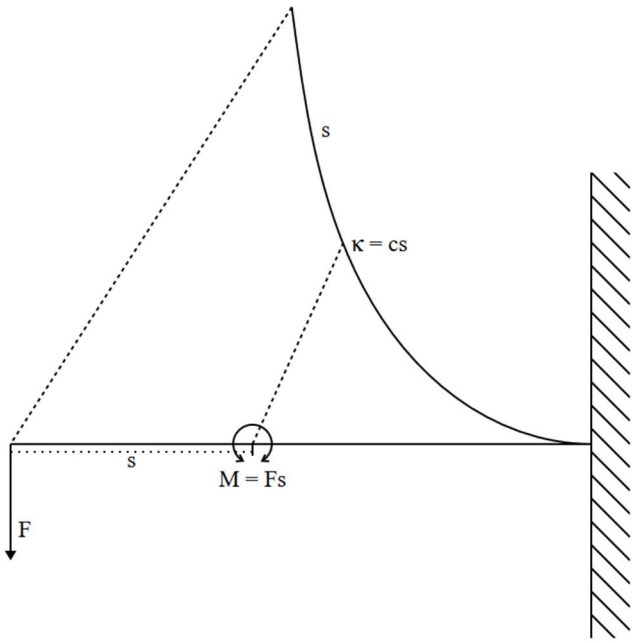
Klotoida – zwana inaczej *spiralą Eulera* bądź *spiralą Cornu*, to krzywa spiralna opisana dwoma równaniami:

$$S(t) = \int_0^t \sin(x^2)\,dx$$
$$C(t) = \int_0^t \cos(x^2)\,dx$$

Powstaje ona jako wykres parametryczny funkcji $S(t)$ względem $C(t)$. Powyższe równania znane są pod nazwą *całek Fresnela* (odpowiednio *sinus Fresnela* i *cosinus Fresnela*).
Cechą szczególną klotoidy jest liniowa zależność promienia jej krzywizny od długości jej łuku, i to ta własność zadecydowała o praktycznym wykorzystaniu tej krzywej.

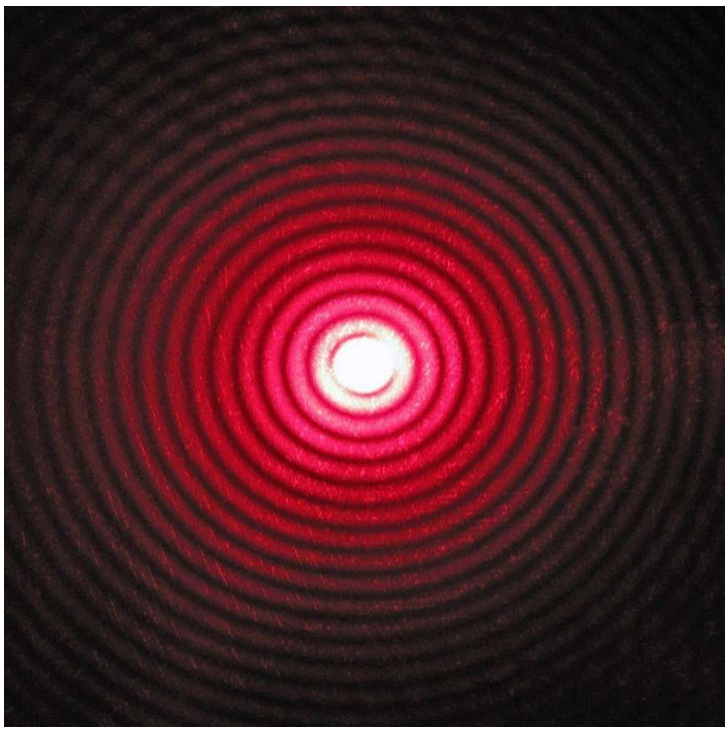
Historia

Krzywa, którą obecnie znamy jako klotoidę, została po raz pierwszy skonstruowana przez Leonharda Eulera w 1744 roku jako rozwiązanie zagadnienia dotyczącego zginania belek, które opublikował James Bernoulli w jednej ze swoich prac pod koniec XVII wieku. Badacz ten poszukiwał bowiem takiego kształtu belki z jednej strony utwierdzonej, która po zgięciu poprzez przyłożenie pionowo skierowanej punktowej siły do jej swobodnego końca uległaby wyprostowaniu. Do uzyskania takiego efektu konieczna była liniowa zależność momentu gnącego od długości belki.



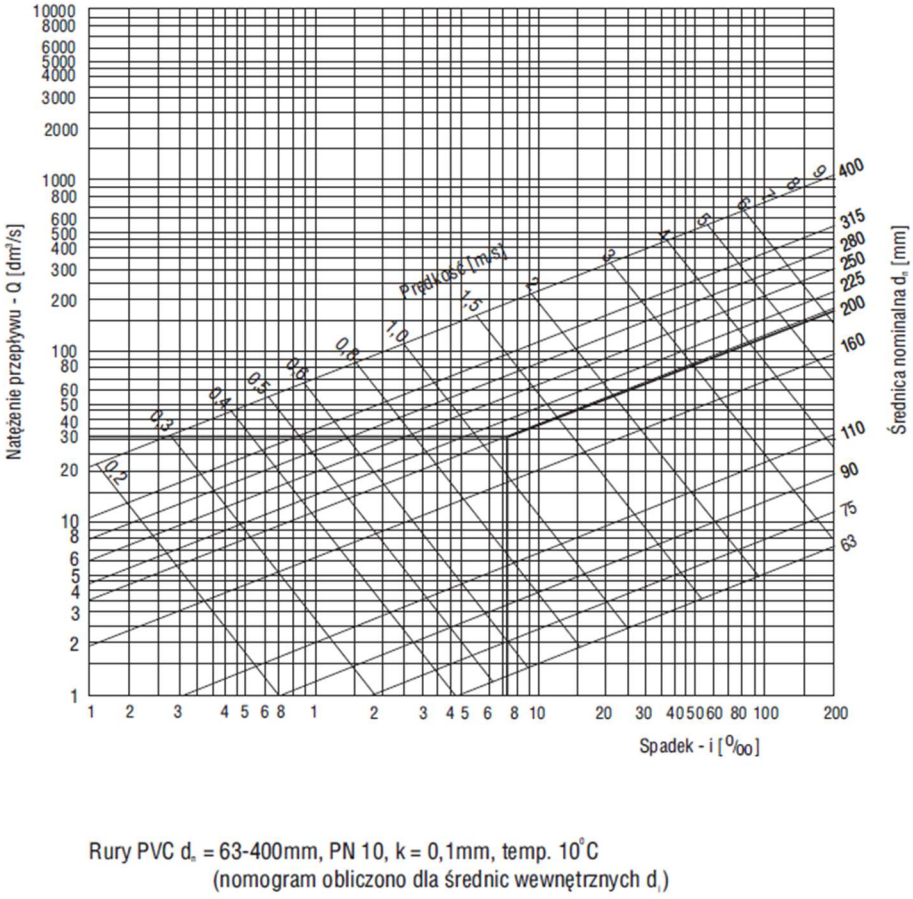
Rys. 1. Ilustracja zagadnienia Bernoulliego dotyczącego zginania belek. Oznaczenia na rysunku: F – siła, M – moment siły, s – długość odcinka belki, κ – krzywizna (odwrotność promienia krzywizny), c – stała. Źródło: [1]

Równania opisujące klotoidę zostały z kolei wyprowadzone przez francuskiego fizyka i inżyniera Augustina-Jeana Fresnela i były wynikiem jego badań nad dyfrakcją światła [2]. Od jego nazwiska nazywamy je właśnie całkami Fresnela. Nazwa *klotoida* została zaproponowana przez włoskiego matematyka Ernesto Cesàro i wywodziła się z greckiego *klothos*, które oznacza włóczkę.



Fot. 1. Przykład efektu zjawiska dyfrakcji na małej okrągłej szczelinie – widoczne są liczne prążki interferencyjne. Źródło: [3]

Pełny wykres klotoidy opracował inny francuski fizyk, Marie Alfred Cornu, jako nomogram dla obliczeń dyfrakcyjnych. Nomogram to wykres, który umożliwia szybkie wyznaczenie wartości dowolnej zmiennej z równania $f(x, y, \ldots) = 0$ (bez jej obliczania), gdy znane są wartości pozostałych zmiennych [4].
Na poniższej grafice zamieszczony został przykład nomogramu, który obrazuje dobór parametrów hydraulicznych przepływu cieczy w rurach wykonanych z tworzywa PVC. Pogrubioną linią zaznaczony jest przykładowy odczyt z nomogramu.



Rys. 2. Przykład nomogramu dotyczącego hydrauliki. Źródło: [5]

Trochę matematyki wyższej, czyli rozwinięcie w szeregi potęgowe

Całki Fresnela nie są możliwe do obliczenia na drodze analitycznej, aby zrobić to możliwie najdokładniej, trzeba korzystać z metod numerycznych. Jednak ich stosowanie nie jest konieczne, gdy zastosujemy tzw. twierdzenie Taylora i rozwiniemy wspomniane całki w szeregi potęgowe. Twierdzenie Taylora mówi nam, że dowolną funkcję n-krotnie różniczkowalną możemy przedstawić za pomocą wielomianu n-tego stopnia, w którym kolejne potęgi zmiennej x o wykładniku całkowitym (zaczynając od 0, czyli kolejno 0, 1, 2 itd.) mnożone są przez wartości kolejnych pochodnych funkcji w tzw. środku zbieżności szeregu i dzielone przez silnie kolejnych liczb całkowitych nieujemnych. Zerowa pochodna funkcji w punkcie to nic innego, jak wartość tej funkcji w punkcie.

Środek zbieżności to z kolei punkt, w którym wartość powstałego wielomianu jest identyczna jak wartość rozwijanej funkcji (standardowo przyjmujemy za taki środek punkt 0 i wówczas powstały szereg nazywamy szeregiem Maclaurina). Poniżej przedstawione są wyprowadzenia rozwinięć całek Fresnela w szeregi potęgowe. Cała procedura wygląda tak, że na początku rozwijamy w szereg funkcję podcałkową, a następnie całkujemy otrzymany szereg.

Najpierw pokażemy rozwinięcie w szereg potęgowy cosinusa Fresnela. Dla uproszczenia obliczeń argument funkcji podcałkowej zastąpimy podstawieniem s.
Policzmy kolejne pochodne funkcji $cosinus$:

$$cos'(s) = -\sin(s)$$
$$cos''(s) = -\cos(s)$$
$$cos'''(s) = \sin(s)$$
$$cos^{IV}(s) = \cos(s)$$

Widzimy, że co czwarta pochodna tej funkcji jest taka sama. Jej rozwinięcie w szereg będzie zatem miało postać:

$$C(s) = \frac{\cos(0)}{0!}s^0 + \frac{-\sin(0)}{1!}s^1 + \frac{-\cos(0)}{2!}s^2 + \frac{\sin(0)}{3!}s^3 + \frac{\cos(0)}{4!}s^4 + \frac{-\sin(0)}{5!}s^5 + \frac{-\cos(0)}{6!}s^6 + \frac{\sin(0)}{7!}s^7 + \cdots = 1 + 0 - \frac{1}{2}s^2 + 0 + \frac{1}{24}s^4 + 0 - \frac{1}{720}s^6 + 0 + \cdots = \sum_{n=0}^{\infty}(-1)^n\frac{s^{2n}}{(2n)!}$$

Po scałkowaniu otrzymamy wzór jak poniżej – w międzyczasie cofamy podstawienie i umieszczamy jako argument funkcji x^2 (korzystamy też z faktu, że całka sumy jest sumą całek oraz że wszelkie stałe możemy wyciągnąć przed całkę):

$$C(t) = \int_0^t \sum_{n=0}^{\infty}(-1)^n\frac{s^{2n}}{(2n)!}dx = \int_0^t \sum_{n=0}^{\infty}(-1)^n\frac{(x^2)^{2n}}{(2n)!}dx = \int_0^t \sum_{n=0}^{\infty}(-1)^n\frac{x^{4n}}{(2n)!}dx = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\int_0^t x^{4n}\,dx = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\left[\frac{x^{4n+1}}{4n+1}\right]_0^t = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\cdot\frac{t^{4n+1}}{4n+1} = \sum_{n=0}^{\infty}(-1)^n\frac{t^{4n+1}}{(2n)!\,(4n+1)}$$

Do takiego wzoru można podstawić wartość parametru t i w stosunkowo prosty sposób obliczyć wartość odciętej danego punktu klotoidy.

Dla sinusa Fresnela procedura rozwinięcia w szereg potęgowy jest analogiczna:

$$sin'(s) = \cos(s)$$
$$sin''(s) = -\sin(s)$$
$$sin'''(s) = -\cos(s)$$
$$sin^{IV}(s) = \sin(s)$$

Podobnie jak dla funkcji $cosinus$, również co czwarta pochodna funkcji $sinus$ jest identyczna.

$$S(s) = \frac{\sin(0)}{0!}s^0 + \frac{\cos(0)}{1!}s^1 + \frac{-\sin(0)}{2!}s^2 + \frac{-\cos(0)}{3!}s^3 + \frac{\sin(0)}{4!}s^4 + \frac{\cos(0)}{5!}s^5 + \frac{-\sin(0)}{6!}s^6 + \frac{-\cos(0)}{7!}s^7 + \cdots = 0 + s - 0 - \frac{1}{6}s^3 + 0 + \frac{1}{120}s^5 - 0 - \frac{1}{5040}s^7 + \cdots = \sum_{n=0}^{\infty}(-1)^n \frac{s^{2n+1}}{(2n+1)!}$$

$$S(t) = \int_0^t \sum_{n=0}^{\infty}(-1)^n \frac{s^{2n+1}}{(2n+1)!}dx = \int_0^t \sum_{n=0}^{\infty}(-1)^n \frac{(x^2)^{2n+1}}{(2n+1)!}dx = \int_0^t \sum_{n=0}^{\infty}(-1)^n \frac{x^{4n+2}}{(2n+1)!}dx = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\int_0^t x^{4n+2}\,dx = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\left[\frac{x^{4n+3}}{4n+3}\right]_0^t = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\cdot\frac{t^{4n+3}}{4n+3} = \sum_{n=0}^{\infty}(-1)^n \frac{t^{4n+3}}{(2n+1)!\,(4n+3)}$$

Finalnie otrzymujemy podobny wzór jak dla funkcji $C(t)$, przy podstawieniu do $S(t)$ konkretnej wartości parametru t możemy z łatwością obliczyć wartość rzędnej danego punktu klotoidy.

Rysowanie klotoidy

Równania klotoidy możemy także wyprowadzić z założenia o liniowej zależności pomiędzy promieniem krzywizny w każdym punkcie a długością krzywej liczoną od początku układu współrzędnych:

$$RL = R_i L_i = A^2$$

A jest w tym równaniu współczynnikiem skali klotoidy, który określa współrzędne środka okręgu o minimalnym (końcowym) promieniu. Współczynnik skali decyduje, jak duża będzie klotoida. R_i oraz L_i to odpowiednio promień krzywizny klotoidy w określonym punkcie oraz elementarna długość odcinka krzywej, której środkiem jest ten punkt, natomiast R i L to odpowiednio końcowy promień krzywizny oraz całkowita długość krzywej.

Parametry R i L definiują tzw. kąt załamania (ang. *deflection angle*), czyli różnicę kątów nachylenia stycznej do wykresu w danym punkcie i w początku układu współrzędnych.

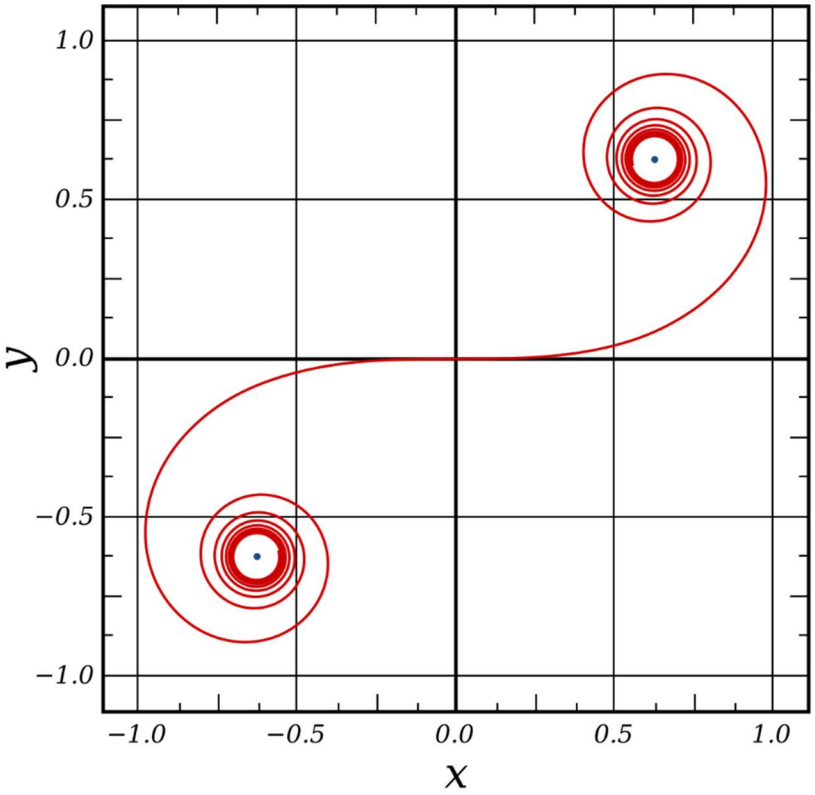
Jeśli obierzemy kąt załamania za parametr $t = \frac{L_i}{2R_i}$ i podstawimy do wcześniej wyprowadzonych szeregów, to otrzymamy następujące równania, które pozwalają na wyznaczenie współrzędnych kolejnych punktów klotoidy [6]:

$$x = l - \frac{l^5}{40(RL)^2} + \frac{l^9}{3456(RL)^4} - \frac{l^{13}}{599040(RL)^6} + \cdots$$

$$y = \frac{l^3}{6RL} - \frac{l^7}{336(RL)^3} + \frac{l^{11}}{42240(RL)^5} - \frac{l^{15}}{9676800(RL)^7} + \cdots$$

Z definicji są one nieskończone, ale w praktyce wystarczającą precyzję zapewnia użycie tylko 4 pierwszych wyrazów, zapisanych powyżej.

Punkty o współrzędnych o wartości bezwzględnej $\frac{A\sqrt{\pi}}{2}$ (jeden punkt ma obie współrzędne dodatnie, a drugi ujemne) to tzw. punkty asymptotyczne klotoidy – punkty, które krzywa okrąża nieskończenie wiele razy, jednocześnie nigdy ich nie osiągając.

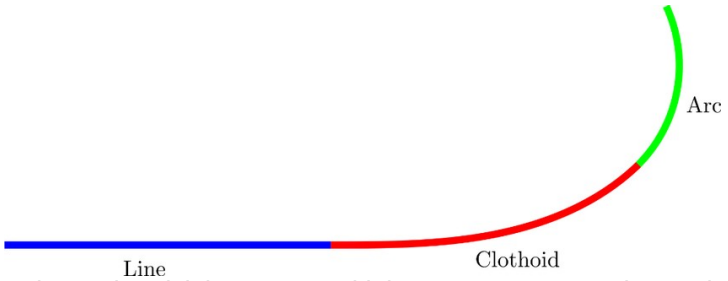


Rys. 3. Przykładowy wykres klotoidy w prostokątnym układzie współrzędnych. Źródło: [7]

Zastosowanie na drogach i liniach kolejowych

Okazuje się, że od dłuższego czasu klotoidy znajdują zastosowanie jako krzywe przejściowe przy projektowaniu zakrętów na drogach oraz na liniach kolejowych.

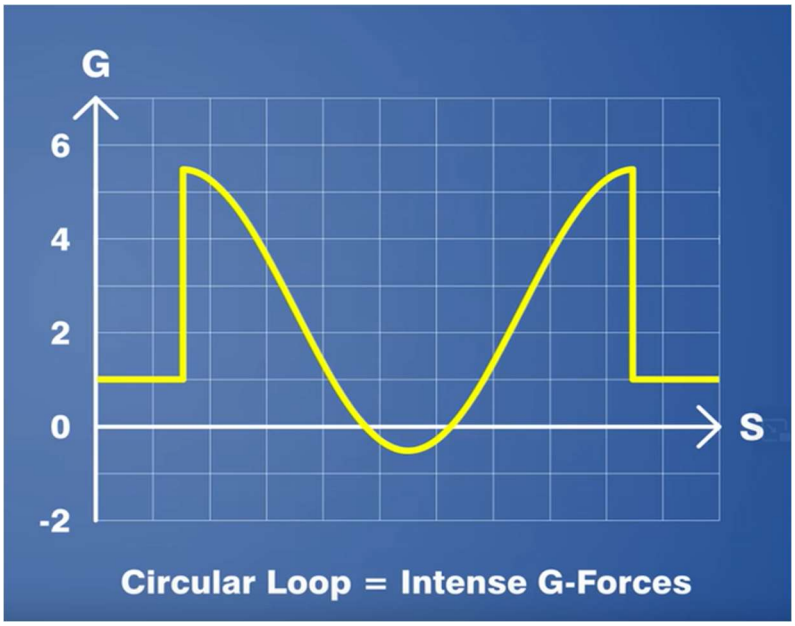
W przypadku projektowania zakrętu na drodze bądź linii kolejowej, chcemy jak najbardziej wyeliminować wpływ siły odśrodkowej – tak, by podczas pokonywania zakrętu móc stopniowo skręcać kierownicę. Z fizyki wiemy, iż ta siła jest wprost proporcjonalna do kwadratu prędkości i odwrotnie proporcjonalna do promienia krzywizny, po której porusza się pojazd. Wyobraźmy sobie, że najpierw poruszamy się po linii prostej – wtedy krzywizna drogi wynosi zero, a w pewnym momencie wjeżdżamy w zakręt będący fragmentem łuku okręgu o określonym promieniu. Krzywizna naszej trasy wzrasta zatem nagle do wartości istotnie większej od zera – to samo dzieje się z wartością siły odśrodkowej. Musimy zatem albo bardzo gwałtownie w maksymalnym stopniu skręcać kierownicę, albo jechać bardzo wolno. Połączenie prostych odcinków drogi z łukami poprzez fragmenty klotoid pozwala nam na komfortowe i bezpieczne pokonanie zakrętu z większą prędkością, bo zmiana krzywizny jest ciągła i stopniowa [8].



Rys. 4. Rzut z góry na połączenie odcinka prostego i łukowego za pomocą krzywej przejściowej (klotoidy). Źródło: [9]

Zastosowanie w roller coasterach

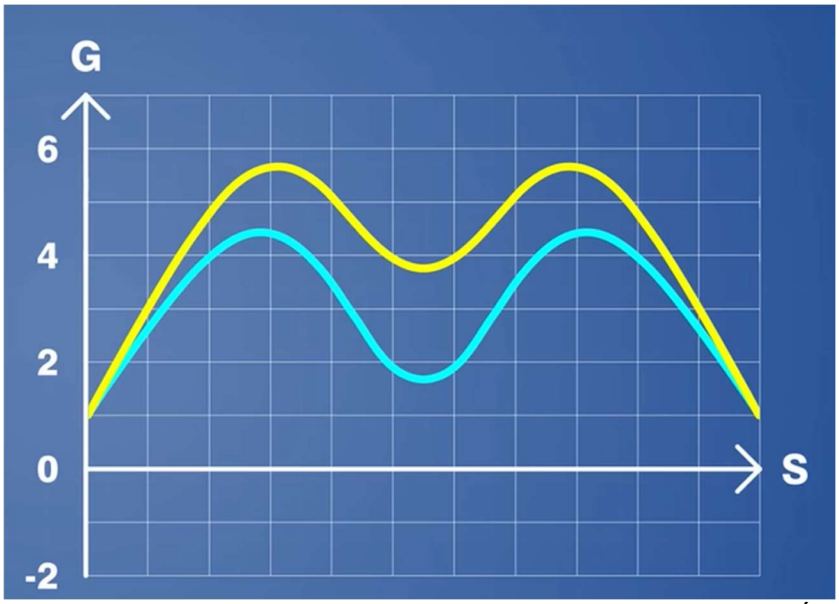
Klotoidy używane są także przy projektowaniu kolejek górskich, które posiadają pionowe pętle. Po raz pierwszy pętle zastosowano w konstrukcjach roller coasterów zbudowanych w Stanach Zjednoczonych u schyłku XIX wieku. Zastosowano pętle o kształcie okręgu – co wydawało się być naturalne, jednak pętle takie miały poważną wadę – ze względu na ich stosunkowo niewielki promień, w momencie wchodzenia i wychodzenia wagonu kolejki z pętli, następowała gwałtowna zmiana krzywizny toru jazdy – z linii prostej na łuk okręgu – co wiązało się z chwilowym występowaniem ogromnych przeciążeń rzędu nawet kilkunastu g. Przeciążenia te stanowiły duży dyskomfort dla pasażerów, a w skrajnych przypadkach prowadziły do omdleń i urazów szyi, dlatego do 1910 roku pętle takie zlikwidowano.



Rys. 5. Przebieg przeciążeń wzdłuż kołowego toru pętli kolejki górskiej. Oznaczenia na rysunku: S – względna odległość punktu na torze pętli od jej początku, G – wartość przeciążenia. Źródło: [10]

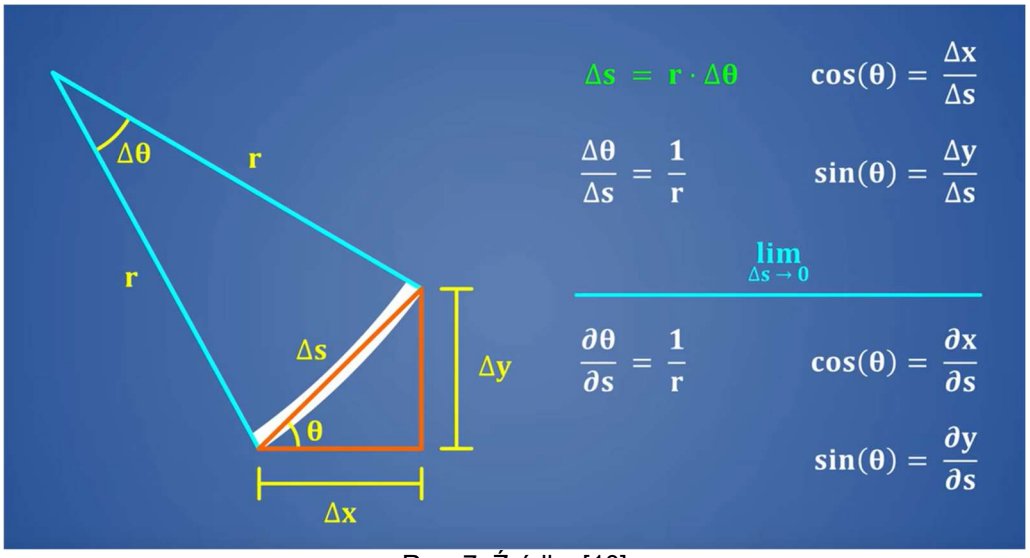
Fot. 2. Kolejka *Flip Flap Railway* w Coney Island w Nowym Jorku. Wartości przeciążeń na jej pętli sięgały 12 g. Źródło: [11]

Pętle w roller coasterach wróciły jednak do łask w 1976 roku, wraz z otwarciem kolejki *The Great American Revolution* w Kalifornii. W zaprojektowaniu jej pętli inżynierowie zastosowali dwa fragmenty klotoidy, będące swoimi lustrzanymi odbiciami. Dzięki temu udało się wyeliminować skokową zmianę przeciążenia przy wchodzeniu w i opuszczaniu pętli, a także zmniejszyć maksymalną jego wartość (tą można dostosować poprzez zmianę rozmiaru całej pętli). Ponadto kolejka mogła obsłużyć więcej pasażerów na raz. Wykres o kolorze żółtym na poniższej grafice dotyczy mniejszej pętli.



Rys. 6. Przebieg przeciążeń wzdłuż klotoidalnego toru pętli kolejki górskiej. Źródło: [10]

Klotoidę można zastosować także w połączeniu z innymi krzywymi, by otrzymać kształt pętli pozwalający na uzyskanie stałej wartości przyspieszenia dośrodkowego lub przeciążenia w jednostkach g na całej jej długości (można te krzywe zdefiniować, rozwiązując układ równań różniczkowych podany na grafice poniżej (rys. 7) – równania te są wyprowadzone z zależności geometrycznych dla krótkiego odcinka łuku okręgu). Użycie klotoidy w każdym z tych przypadków zapewnia możliwość płynnego połączenia prostych odcinków toru kolejki z pętlą.



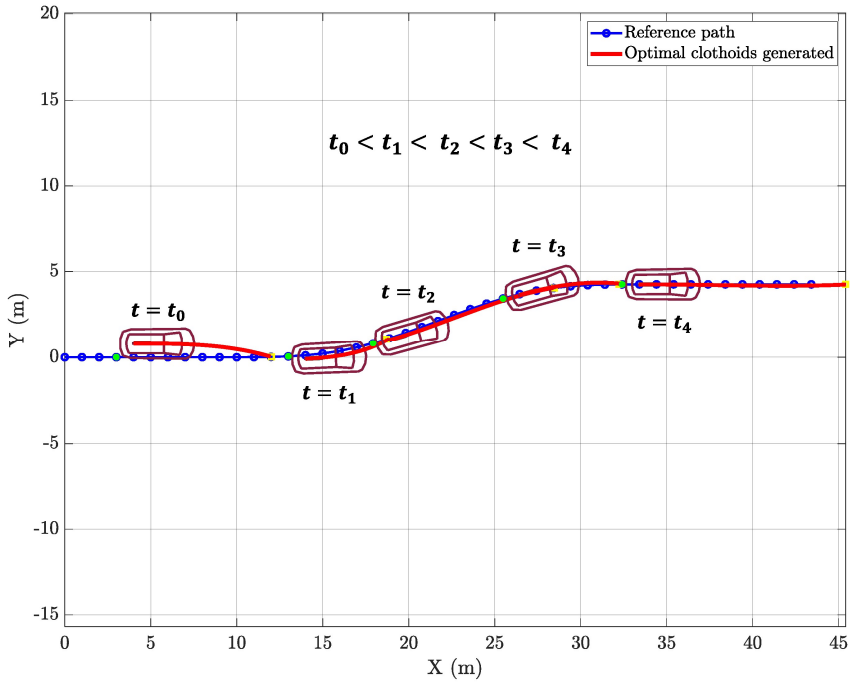
Rys. 7. Źródło: [10]

Przykładem pętli w kolejce górskiej zbudowanej z połączenia odcinków klotoidy i okręgu (czyli naturalnego kształtu, którego próby zastosowania były czynione na początku) jest *Blue Fire*, otwarta w parku rozrywki Europa-Park w Niemczech w 2009 roku.

Rys. 8. Pętla kolejki górskiej *Blue Fire*. Źródło: [10]

Zastosowanie w pojazdach autonomicznych

Ostatnim zastosowaniem klotoid, jakie zostanie opisane w niniejszym artykule, są pojazdy autonomiczne. Otóż krzywe te są stosowane do optymalizacji nawigacji trasy przez pojazdy – systemy tzw. lokalnego planowania ścieżki (ang. *local path planning*) na bieżąco generują odcinki klotoidalne, które minimalizują efekty dynamiczne podczas przejazdu po drodze i zapewniają płynność oraz bezpieczeństwo wykonywanych manewrów. Łącznie z obliczaniem tzw. odległości Frécheta określającej wzajemną zbieżność krzywych, klotoidy są możliwie jak najlepiej dopasowywane do rzeczywistego przebiegu trasy.



Rys. 9. Przykład przebiegu trasy wygenerowanej przez system lokalnego planowania ścieżki w pojeździe autonomicznym – kolorem czerwonym jest oznaczony zbiór tworzonych w kolejnych odstępach czasowych klotoid, a niebieskim – przebieg trasy odniesienia. Źródło: [12]

Podsumowanie

Jak zostało to opisane, pomimo iż szerszej publice klotoidy być może nie są zbyt znane, to jednak odpowiadają one za realizację niektórych fundamentalnych rozwiązań inżynierskich, bez których nie wyobrażamy sobie dzisiaj bezpieczeństwa w sieci drogowej i parkach rozrywki. Wciąż prowadzone są badania nad znalezieniem innych krzywych o specjalnych właściwościach łączących ich krzywiznę i długość [8], które w przyszłości prawdopodobnie wprowadzą przydatne usprawnienia w innych gałęziach gospodarki.

Literatura

[1] R. Levien: The Euler spiral: A mathematical history, Electrical Engineering and Computer Sciences – University of California at Berkeley, 2008
[2] Artykuł *Augustin-Jean Fresnel*, sekcja: *Contributions to physical optics – Prize memoir (1818) and sequel*, anglojęzyczna Wikipedia en.wikipedia.org [dostęp 24.06.2024]
[3] Artykuł *Dyfrakcja*, autor: Wisky, polskojęzyczna Wikipedia pl.wikipedia.org [dostęp 24.06.2024]
[4] Artykuł *Nomogram*, polskojęzyczna Wikipedia pl.wikipedia.org [dostęp 24.06.2024]
[5] Pipelife Polska S.A.: Obliczenia rurociągów. Obliczenia hydrauliczne przewodów z tworzyw sztucznych.

[6] Artykuł *The Clothoid*, www.pwayblog.com [dostęp 24.06.2024]
[7] Artykuł *Klotoida*, domena publiczna, polskojęzyczna Wikipedia pl.wikipedia.org [dostęp 24.06.2024]
[8] W. Koc: Smoothed transition curve for railways, Politechnika Gdańska, Katedra Transportu Szynowego i Mostów, 2019
[9] T. F. Brustad: Preliminary Studies on Transition Curve Geometry: Reality and Virtual Reality, „Emerging Science Journal", 2020
[10] Film *The Real Physics of Roller Coaster Loops* przesłany przez Art of Engineering, www.youtube.com [dostęp 24.06.2024]
[11] Artykuł *Flip Flap Railway*, domena publiczna, anglojęzyczna Wikipedia en.wikipedia.org [dostęp 24.06.2024]
[12] A. Shaju i in.: Enhancing Autonomous Vehicle Navigation with a Clothoid-Based Lateral Controller, Department of Mechanical Engineering, Virginia Tech, Blacksburg, 2024

SZEREGI FOURIERA - METODA OPTYMALIZACYJNA OBLICZEŃ NUMERYCZNYCH PRZY OBLICZANIU WSPÓŁCZYNNIKÓW SZEREGU FOURIERA

Marek KRZEMIŃSKI[1]

[1] Politechnika Łódzka, Łódź

Wstęp

Postęp technologiczny jest nieodłącznym elementem rozwoju każdej cywilizacji. To on pozwala na szybsze i łatwiejsze wykonywanie naszych codziennych czynności. W XXI wieku jednym z głównych kierunków rozwoju jest rozwój teleinformatyczny. Wraz z nim powstała dziedzina zajmująca się obliczeniami numerycznymi specjalizująca się w jak najdokładniejszych i najszybszych obliczeniach. Analiza Fouriera jest obecnie intensywnie wykorzystywana w postaci analizy sygnałów, przetwarzania obrazów jak i kodowaniu wraz z kompresją danych.
Przygotowany materiał porusza kwestie optymalizacji obliczeń numerycznych, podczas obliczania współczynników a_n oraz b_n szeregu Fouriera, przy założeniu korzystania z funkcji wielomianowych o stopniach nieujemnych.

Wyznaczenie algorytmu optymalizującego obliczenia współczynników szeregu

Szeregi Fouriera to potężne narzędzie, które jednak jest złożone obliczeniowo. Przy obliczaniu takich współczynników dla różnych funkcji, wymagane jest całkowanie przez części, które w przypadku niektórych funkcji (na przykład wykładniczych), może nigdy nie dać skończonego wyniku, ponieważ każde całkowanie przez części będzie generowało kolejne. Przy przybliżaniu numerycznym powstaje błąd przybliżenia, ponieważ procesory nie posiadają wbudowanej funkcji całkowania, a każde takie obliczenie jest czasochłonne.

Poniżej przedstawione są wzory (1, 2) potrzebne do wyznaczenia szeregu Fouriera:

$$S(x) = \frac{a_0}{2} + \sum_{n=1}^{N} \left(a_n \cos\left(\frac{2n\pi}{T}x\right) + b_n \sin\left(\frac{2n\pi}{T}x\right) \right) , \tag{1}$$

$$a_n = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} f(x)\cos\left(\frac{2n\pi}{T}x\right)dx \ , \qquad b_n = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} f(x)\sin\left(\frac{2n\pi}{T}x\right)dx \ , \tag{2}$$

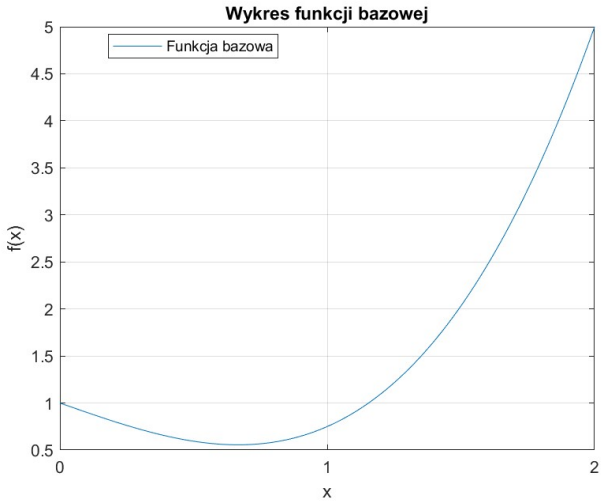
gdzie:
T – okres funkcji,
N – maksymalny stopień przybliżenia szeregu, dla $1 \leq n \leq \infty$,
$f(x)$ – funkcja bazowa.

Funkcja bazowa może być dowolną funkcją, jednak najczęściej używa się funkcji wielomianowych, ze względu na ich uniwersalność. Są one również stosunkowo proste w aproksymowaniu. Z tego powodu rozważane będą funkcje wielomianowe o stopniu nieujemnym (tj. $x^0, x^1, x^2, \ldots, x^k$ – gdzie k oznacza stopień wielomianu). Podana funkcja jest określona na danym przedziale.

Pierwotnie jest to odcinek zaczynający się połowę okresu funkcji na lewo od początku układu i trwający przez ten okres, czyli $[-\frac{T}{2},\frac{T}{2}]$. W ogólnym przypadku może być funkcją określoną na dowolnym przedziale, na przykład: $[c,d]$, w takim przypadku okres funkcji będzie wynosił: $T = |d-c|$.

W poniższym przykładzie została wykorzystana funkcja ciągła, określona na przedziale $< 0{,}2 >$ oraz została zapisana wzorem (3).

$$f(x) = \frac{4}{3}x^3 - x + 1 \tag{3}$$



Wyk. 1

W tym przypadku okres funkcji wynosi $T = 2$. Obliczenia zostały rozpoczęte od wyznaczenia współczynnika a_n:

$$a_n = \frac{2}{T}\int_c^{\mathrm{d}} f(x)\cos\left(\frac{2n\pi}{T}x\right)dx = \int_0^2 \left(\frac{4}{3}x^3 - x + 1\right)\cos(n\pi x)\,dx = \\ = \frac{4}{3}\int_0^2 x^3\cos(n\pi x)\,dx - \int_0^2 x\cos(n\pi x)\,dx + \int_0^2 \cos(n\pi x)\,dx \tag{4}$$

W celu lepszej prezentacji, zostały wprowadzone oznaczenia: $w_{k_{an}}$, $w_{k_{bn}}$ bazujące na zredukowanej postaci współczynników a_n i b_n (czyli tylko części podcałkowej danych współczynników szeregu, a dokładnie bez iloczynu z $\frac{2}{T}$ we współczynniku):

$$[w_{k_{an}}]_c^d = \int_c^d x^k \cos\left(\frac{2n\pi}{T}x\right)dx, \\ [w_{k_{bn}}]_c^d = \int_c^d x^k \sin\left(\frac{2n\pi}{T}x\right)dx, \tag{5}$$

gdzie:
k – stopień wielomianu,
a – odpowiednik fragmentu współczynnika a_n,

b – odpowiednik fragmentu współczynnika b_n,
c – dolna granica przedziału funkcji bazowej,
d – górna granica przedziału funkcji bazowej,
T – okres funkcji,
n – wskaźnik sumowania szeregu.

Przy takim oznaczeniu, można przejść do obliczania współczynników dla funkcji wielomianowych o dowolnym stopniu, zaczynając od zerowego.

$$[w_{0_{an}}]_c^d = \int_c^d x^0 \cos\left(\frac{2n\pi}{T}x\right)dx = \int_c^d \cos\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{T}{2n\pi} sin\left(\frac{2n\pi}{T}\ x\right)\right]_c^d$$
$$= \frac{T}{2n\pi}\left[sin\left(\frac{2n\pi}{T}\ x\right)\right]_c^d \tag{6}$$

$$[w_{0_{bn}}]_c^d = \int_c^d x^0 \sin\left(\frac{2n\pi}{T}x\right)dx = \int_c^d \sin\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{-T}{2n\pi} cos\left(\frac{2n\pi}{T}\ x\right)\right]_c^d$$
$$= \frac{T}{2n\pi}\left[-cos\left(\frac{2n\pi}{T}x\right)\right]_c^d \tag{7}$$

Obliczenie współczynnika dla pierwszego stopnia wielomianu.

$$[w_{1_{an}}]_c^d = \int_c^d x^1 \cos\left(\frac{2n\pi}{T}x\right)dx = \int_c^d x \cos\left(\frac{2n\pi}{T}x\right)dx\ =$$
$$= \left[\frac{T}{2n\pi}x\ sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - \frac{T}{2n\pi}\int_c^d \sin\left(\frac{2n\pi}{T}x\right)dx \tag{8}$$

$$[w_{1_{bn}}]_c^d = \int_c^d x^1 \sin\left(\frac{2n\pi}{T}x\right)dx = \int_c^d x \sin\left(\frac{2n\pi}{T}x\right)dx\ =$$
$$= \left[\frac{-T}{2n\pi}x\ cos\left(\frac{2n\pi}{T}\ x\right)\right]_c^d + \frac{T}{2n\pi}\int_c^d \cos\left(\frac{2n\pi}{T}x\right)dx \tag{9}$$

Można zauważyć, że całka, która powstała w wyniku całkowania przez części, została już obliczona wcześniej, przy obliczaniu współczynnika dla stopnia zerowego. W takim razie, zostanie ona zastąpiona wprowadzonym wcześniej oznaczeniem:

$$[w_{1_{an}}]_c^d = \int_c^d x \cos\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{T}{2n\pi}x\ sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - \frac{T}{2n\pi}\int_c^d \sin\left(\frac{2n\pi}{T}x\right)dx$$
$$= \frac{T}{2n\pi}\left(\left[x\ sin\left(\frac{2n\pi}{T}\ x\right)\right]_c^d - [w_{0_{bn}}]_c^d\right. \tag{10}$$

$$[w_{1_{bn}}]_c^d = \int_c^d x \sin\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{-T}{2n\pi}x\cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + \frac{T}{2n\pi}\int_c^d \cos\left(\frac{2n\pi}{T}x\right)dx = \\ = \frac{T}{2n\pi}\left(\left[-x\cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + [w_{0_{an}}]_c^d\right) \tag{11}$$

W następnym kroku zostały obliczone współczynniki dla drugiego i trzeciego stopnia wielomianu przy zastosowaniu tych samych metod obliczeń i oznaczeń:

$$[w_{2_{an}}]_c^d = \int_c^d x^2\cos\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{T}{2n\pi}x^2\sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - 2\frac{T}{2n\pi}\int_c^d x\sin\left(\frac{2n\pi}{T}x\right)dx \\ = \frac{T}{2n\pi}\left(\left[x^2\sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - 2[w_{1_{bn}}]_c^d\right) \tag{12}$$

$$[w_{2_{bn}}]_c^d = \int_c^d x^2\sin\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{-T}{2n\pi}x^2\cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + 2\frac{T}{2n\pi}\int_c^d x\cos\left(\frac{2n\pi}{T}x\right)dx \\ = \frac{T}{2n\pi}\left(\left[-x^2\cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + 2[w_{1_{an}}]_c^d\right) \tag{13}$$

$$[w_{3_{an}}]_c^d = \int_c^d x^3\cos\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{T}{2n\pi}x^3\sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - 3\frac{T}{2n\pi}\int_c^d x^2\sin\left(\frac{2n\pi}{T}x\right)dx \\ = \frac{T}{2n\pi}\left(\left[x^3\sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - 3[w_{2_{bn}}]_c^d\right) \tag{14}$$

$$[w_{3_{bn}}]_c^d = \int_c^d x^3\sin\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{-T}{2n\pi}x^3\cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + 3\frac{T}{2n\pi}\int_c^d x^2\cos\left(\frac{2n\pi}{T}x\right)dx \\ = \frac{T}{2n\pi}\left(\left[-x^3\cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + 3[w_{2_{an}}]_c^d\right) \tag{15}$$

Jak można zauważyć, zależność ta jest rekurencyjna i można ją określić wzorem:

$$[w_{k_{an}}]_c^d = \frac{T}{2n\pi}\left(\left[x^k\sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - k\cdot[w_{(k-1)_{bn}}]_c^d\right) \\ [w_{k_{bn}}]_c^d = \frac{T}{2n\pi}\left(\left[x^k\cos\left(\frac{2n\pi}{T}x\right)\right]_d^c + k\cdot[w_{(k-1)_{an}}]_c^d\right) \tag{16}$$

Dowód:

$$[w_{k_{an}}]_c^d = \int_c^d x^k \cos\left(\frac{2n\pi}{T}x\right)dx = \left[\frac{T}{2n\pi}x^k \sin\left(\frac{2n\pi}{T}\ x\right)\right]_c^d - k\frac{T}{2n\pi}\int_c^d x^{k-1}\sin\left(\frac{2n\pi}{T}x\right)dx$$
$$= \frac{T}{2n\pi}\left(\left[x^k \sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - k\cdot[w_{(k-1)_{bn}}]_c^d\right) \quad (17)$$

$$[w_{k_{bn}}]_c^d = \int_c^d x^k \sin\left(\frac{2n\pi}{T}x\right)dx\ =$$
$$= \left[\frac{-T}{2n\pi}x^k \cos\left(\frac{2n\pi}{T}x\right)\right]_c^d + k\frac{T}{2n\pi}\int_c^d x^{k-1}\cos\left(\frac{2n\pi}{T}x\right)dx\ = \quad (18)$$
$$= \frac{T}{2n\pi}\left(\left[x^k \cos\left(\frac{2n\pi}{T}x\right)\right]_d^c + k\cdot[w_{(k-1)_{an}}]_c^d\right)$$

Jednak wzór działa tylko dla $n > 0$, a ponieważ współczynnik a_n jest liczony również dla $n = 0$, należy podać oddzielny wzór dla tego właśnie przypadku:

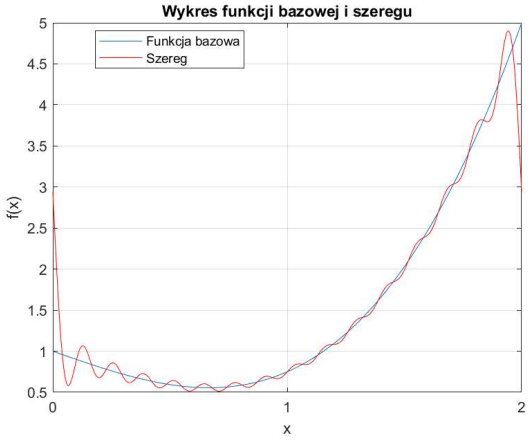
$$[w_{k_{a0}}]_c^d = \int_c^d x^k\,dx\ = \left[\frac{1}{k+1}x^{k+1}\right]_c^d \quad (19)$$

Wracając do przykładu, współczynnik a_n można teraz zapisać jako:

$$a_n = \frac{2}{T}\int_c^{\mathrm{d}} f(x)\cos\left(\frac{2n\pi}{T}x\right)dx\ = \int_0^2\left(\frac{4}{3}x^3 - x + 1\right)\cos(n\pi x)\,dx\ =$$
$$= \frac{4}{3}\int_0^2 x^3\cos(n\pi x)\,dx\ - \int_0^2 x\cos(n\pi x)\,dx\ + \int_0^2\cos(n\pi x)\,dx\ = \quad (20)$$
$$= \frac{4}{3}[w_{3_{an}}]_0^2 - [w_{1_{an}}]_0^2 + [w_{0_{an}}]_0^2$$

Współczynniki $a_0\ i\ b_n$ oblicza się analogicznie.

Znaleziony w ten sposób szereg został nałożony na wykres funkcji bazowej i przedstawiony na wykresie 2:



Wykres 2

Przyjmując powyżej wprowadzone oznaczenie, szereg możemy zapisać następująco:

$$S(x) = \frac{a_0}{2} + \sum_{n=1}^{N}\left(a_n \cos\left(\frac{2n\pi}{T}x\right) + b_n \sin\left(\frac{2n\pi}{T}x\right)\right) \tag{21}$$

gdzie:

$$a_0 = \frac{2}{T}\sum_{k=0}^{\mathrm{p}}[w_{k_{a0}}]_c^d \qquad a_n = \frac{2}{T}\sum_{k=0}^{\mathrm{p}}[w_{k_{an}}]_c^d \qquad b_n = \frac{2}{T}\sum_{k=0}^{\mathrm{p}}[w_{k_{bn}}]_c^d \tag{22}$$

$$\begin{aligned}
[w_{k_{a0}}]_c^d &= \left[\frac{1}{k+1}x^{k+1}\right]_c^d \\
[w_{k_{an}}]_c^d &= \frac{T}{2n\pi}\left(\left[x^k \sin\left(\frac{2n\pi}{T}x\right)\right]_c^d - k\cdot w_{(k-1)b}\right) \\
[w_{k_{bn}}]_c^d &= \frac{T}{2n\pi}\left(\left[x^k \cos\left(\frac{2n\pi}{T}x\right)\right]_d^c + k\cdot w_{(k-1)a}\right)
\end{aligned} \tag{23}$$

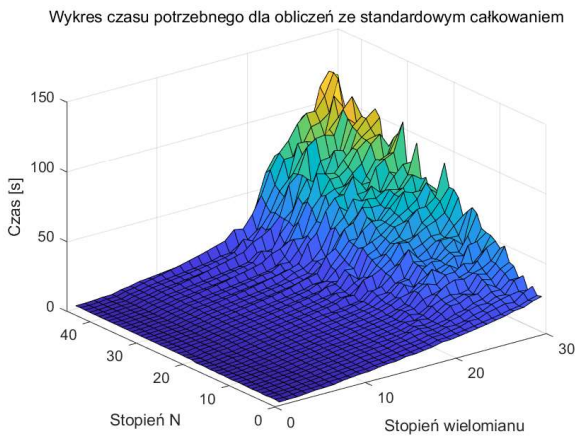
gdzie:
T – okres funkcji,
N – maksymalny stopień przybliżenia szeregu,
p – maksymalny stopień wielomianu funkcji bazowej,
k – stopień wielomianu,
a – odpowiednik fragmentu współczynnika a_n,
b – odpowiednik fragmentu współczynnika b_n,
c – dolna granica przedziału funkcji bazowej,
d – górna granica przedziału funkcji bazowej.

Implementacja algorytmu w środowisku *Matlab*

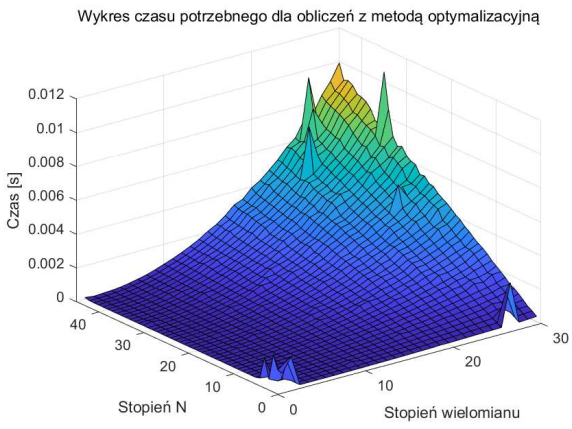
Jak można zauważyć, we wzorze nie występuje całkowanie, co sprowadza obliczenia związane z wyznaczeniem współczynników do korzystania z podstawowych funkcji jednostek arytmetyczno-logicznych procesora. Pod względem numerycznym jest to przyśpieszenie obliczeń oraz (dla wyższych stopni wielomianu i szeregu) zwiększenie dokładności obliczeń.

W celu sprawdzenia efektywności algorytmu, zostało wykonane porównanie wcześniej zaproponowanego algorytmu z wbudowaną funkcją *int()* służącą do symbolicznego obliczenia całek oznaczonych danej funkcji określonej na przedziale. Sprawdzany był czas potrzebny na obliczenie współczynników a_n i b_n. Czas był mierzony tylko w chwili obliczania współczynników obiema metodami oddzielnie.

Algorytm w pierwszej kolejności losował współczynnik do pierwszego elementu wielomianu (stanowiącego funkcję bazową) x^0, w zakresie od -1 do 1. W kolejnym kroku rozpoczynał pomiar czasu, który sprawdzał czas potrzebny na obliczenie współczynników szeregu dla: $n = 1$ metodą zoptymalizowaną. Po zakończonym pomiarze rozpoczynał następny, który mierzył czas przy metodzie wykorzystującej całkowanie. Po zakończonym pomiarze zapisywał dane w tablicy, a następnie zwiększał stopień szeregu o jeden i powtarzał proces. Gdy algorytm obliczył współczynniki szeregu do ustalonej wartości n (w tym przypadku 45), następowało zwiększenie stopnia wielomianu, poprzez kolejne losowanie wartości współczynnika wielomianu, tym razem dla x^1 i proces się powtarzał aż do uzyskania odpowiedniego stopnia wielomianu, w tym przypadku 30.



Wykres 3

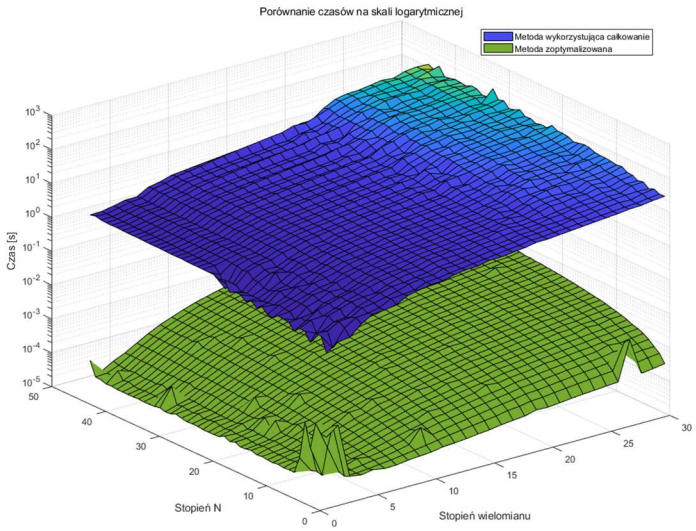


Wykres 4

Wykres 3 przedstawia czas potrzebny na wyznaczenie współczynników szeregu o odpowiednim stopniu N oraz szeregu, dla metody wykorzystującej całkowanie symboliczne. Wykres 4 przedstawia w sposób analogiczny, czas potrzebny dla metody zoptymalizowanej. Obliczenia wykorzystujące metodę zoptymalizowaną, zostały wykonane około 10 000 razy szybciej od standardowej metody wykorzystującej całkowanie. Do wyznaczenia wielomianu trzydziestego stopnia potrzebne było 116 sekund podczas, gdy metoda zoptymalizowana skróciła ten czas do 0.0099 sekundy. Mimo, że czas jest zależny od jednostki liczącej dane współczynniki, to jednak jest widoczny wzrost optymalizacji czasowej względem standardowej metody.

Dla obu sposobów tempo wzrostu czasu obliczeń względem stopnia przybliżenia szeregu jest liniowe. Wynika to z faktu sumowania kolejnych elementów obliczonych współczynników szeregu, o stałych stopniach wielomianu. Dla obu wykresów widać tempo wzrostu kwadratowe w stosunku do stopnia wielomianu. Wynika to z całkowania przez części lub, jak w przypadku metody zoptymalizowanej, odwoływania się rekurencyjnego kolejnych stopni wielomianu.

Aby lepiej zobrazować różnice w czasach potrzebnych na obliczenie współczynników, można przedstawić oba zestawy danych w skali logarytmicznej na wykresie 5:



Wykres 5

Podsumowanie

Zastosowanie przedstawionej metody optymalizacyjnej może znacząco wpłynąć na szybkość wykonywanych obliczeń. Przede wszystkim, wspomniana metoda będzie miała wpływ w jednostkach o mniejszych zasobach sprzętowych, takich jak systemy wbudowane lub mikrokontrolery. Metoda ta znajdzie zastosowanie również w przypadkach, gdzie liczy się czas potrzebny na obliczenia, ze względu na działanie w czasie rzeczywistym. Należy zaznaczyć, że obliczenia zostały przeprowadzone na funkcjach ciągłych, co daje dokładne wartości obliczonych całek. Obie metody zwracały dokładne wartości, jednak metoda zoptymalizowana wykonuje obliczenia znacząco szybciej, z tą samą dokładnością.

Literatura

[1] D. S. Stoffer and P. Bloomfield, ‘Fourier Analysis of Time Series: An Introduction’, *J Am Stat Assoc*, vol. 95, no. 452, 2000, doi: 10.2307/2669794.

[2] D. H. Bailey and P. N. Swarztrauber, ‘Fractional Fourier transform and applications’, *SIAM Review*, vol. 33, no. 3, 1991, doi: 10.1137/1033097.

[3] S. C. Hillmer and W. W. S. Wei, ‘Time Series Analysis: Univariate and Multivariate Methods.’, *J Am Stat Assoc*, vol. 86, no. 413, 1991, doi: 10.2307/2289741.

MATEMATYCZNIE OPTYMALNY PORTFEL INWESTYCYJNY

Jakub ŁOMPIEŚ

Politechnika Łódzka, Łódź

Wprowadzenie

Z pewnością każdy student, który zmierzył się z kursem Analizy Matematycznej, spotkał się z następującym zadaniem:

(P) *Znaleźć minimum pewnej różniczkowalnej funkcji rzeczywistej* f *na przedziale* $[a, b]$.

Dla funkcji rzeczywistych jednej zmiennej potrafimy wyznaczyć pewien schemat, który pozwala na rozwiązanie problemu (P), m. in.

- wyznaczamy punkty krytyczne f i sprawdzamy, czy należą do (a, b);
- jeśli tak, to wyznaczamy wartości funkcji f w tych punktach;
- obliczamy $f(a)$ i $f(b)$;
- porównujemy wartości funkcji f w punktach krytycznych z $f(a)$ oraz $f(b)$ i wybieramy najmniejszą.

Czy optymalizacja wielowymiarowa z ograniczeniami również da się opisać podobnym schematem? Przejdźmy zatem z prostej na płaszczyznę i rozważmy następujące zagadnienie:

(P') *Znaleźć minimum pewnej różniczkowalnej funkcji rzeczywistej* f *na domkniętym kole o środku w punkcie* $(0, 0)$ *i promieniu* 1.

Wykorzystując znaną nam nierówność koła zagadnienie (P') możemy zapisać w postaci:

$$\begin{cases} f(x, y) \to \min \\ \text{przy ograniczeniu} \\ x^2 + y^2 \leq 1, \\ (x, y) \in \mathbb{R}^2. \end{cases}$$

Sugerując się metodą dla przypadku jednowymiarowego, rozwiązanie problemu (P') możemy rozpocząć od wyznaczenia punktów krytycznych wewnątrz koła. Pozostaje pytanie, **czy potrafimy wyznaczyć wartości ekstremalne funkcji f na brzegu naszego zbioru ograniczającego, tj. na okręgu jednostkowym?** Jest to wyzwanie nietrywialne, a więc potrzebujemy innego sposobu, który umożliwi nam rozwiązywanie tego typu zagadnień.

W tym celu, w sekcji 2 omówimy twierdzenie Karusha-Kuhna-Tuckera, które umożliwia rozwiązanie problemu (P'). W rozdziale 3, pokażemy zastosowanie wspomnianych powyżej rozwiązań w modelu Markowitza z instrumentem wolnym od ryzyka. W sekcji 4, postawimy się w roli brokera i będziemy inwestować na giełdzie z pomocą poznanej wcześniej teorii.

Optymalizacja z ograniczeniami

Niniejszy rozdział został opracowany na podstawie [1] i [6]. W teorii portfelowej, dotyczącej modeli Markowitza, mierzymy się z problemami optymalizacji z ograniczeniami mieszanymi w postaci:

$$\begin{cases} f(\boldsymbol{x}) \to \min \\ \text{przy ograniczeniach} \\ g_j(\boldsymbol{x}) \leq 0 \text{ dla } j \in \{1, ..., k\}, \\ g_j(\boldsymbol{x}) = 0 \text{ dla } j \in \{k+1, ..., m\}, \\ \boldsymbol{x} \in \mathbb{R}^n. \end{cases} \tag{1}$$

Do ułatwienia obliczeń związanych z poszukiwaniem rozwiązania zagadnienia (1) wprowadzamy funkcję pomocniczą.

Definicja 1. Funkcję $L : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ postaci

$$L(\boldsymbol{x}, \boldsymbol{\lambda}) := f(\boldsymbol{x}) + \sum_{j=1}^{m} \lambda_j g_j(\boldsymbol{x}),$$

gdzie $\boldsymbol{\lambda} = [\lambda_1, ..., \lambda_m]^T \in \mathbb{R}^m$, nazywamy funkcją Lagrange'a stowarzyszoną z problemem (1).

W poszukiwaniach minimum dla problemu (1) przychodzi nam z pomocą

Twierdzenie 2 (Karush-Kuhn-Tucker)**.** Załóżmy, że $f\colon \mathbb{R}^n \to \mathbb{R}$ jest wypukła, $g_j\colon \mathbb{R}^n \to \mathbb{R}$ są wypukłe dla $j \in \{1, \ldots, k\}$ i $g_j\colon \mathbb{R}^n \to \mathbb{R}$ są liniowe dla $j \in \{k+1, \ldots, m\}$ oraz istnieje taki $\boldsymbol{x} \in \mathbb{R}^n$, że $g_j(\boldsymbol{x}) < 0$ dla $j = 1, \ldots, k$, oraz $g_j(\boldsymbol{x}) = 0$ dla $j = k+1, \ldots, m$. Jeżeli funkcje $f, g_1, \ldots, g_m$ są różniczkowalne w $\boldsymbol{x_0} \in \mathbb{R}^n$, to $\boldsymbol{x_0}$ jest rozwiązaniem (1) wtedy i tylko wtedy, gdy istnieje taka $\boldsymbol{\lambda} = [\lambda_1, \ldots, \lambda_m]^T$, że:

(1) $\lambda_i \geq 0$ dla $i = 1, \ldots, k$;

(2) $\sum_{i=1}^{k} \lambda_i g_i(\boldsymbol{x_0}) = 0$;

(3) $\boldsymbol{x_0}$ spełnia ograniczenia problemu (1);

(4) $\nabla_{\boldsymbol{x}} L(\boldsymbol{x_0}, \boldsymbol{\lambda}) = \nabla f(\boldsymbol{x_0}) + \sum_{i=1}^{m} \lambda_i \nabla g_i(\boldsymbol{x_0}) = \Theta_{\mathbb{R}^n}$,

gdzie $\Theta_{\mathbb{R}^n}$ jest wektorem zerowym w przestrzeni $\mathbb{R}^n$.

Twierdzenie 2 zapewnia warunek konieczny i wystarczający istnienia rozwiązania problemu (1). Zatem stanowi ono narzędzie do rozwiązywania zagadnień optymalizacyjnych z ograniczeniami. W celu lepszego zapoznania się z twierdzeniem 2, rozważmy następujący przykład:

Przykład 3. Minimalizujemy funkcję celu $f(x,y) := x+y$ na domkniętym kole o środku w punkcie $(0,0)$ i promieniu 1, tj.

$$\begin{cases} x+y \to \min \\ \text{przy ograniczeniu} \\ x^2+y^2 \leq 1, \\ (x,y) \in \mathbb{R}^2. \end{cases} \tag{2}$$

Funkcja Lagrange'a stowarzyszona z problemem (2) ma postać

$$L(x,y,\lambda) = x+y+\lambda(x^2+y^2-1).$$

Zauważmy, że

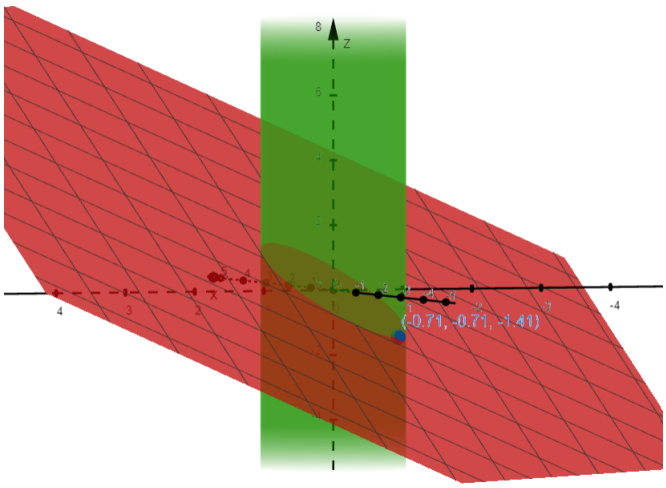
$$\nabla_{\boldsymbol{x}} L(x,y,\lambda) = [1+2\lambda x, 1+2\lambda y]^T.$$

Zatem wykorzystując warunki (1)-(4) z twierdzenia 2 otrzymujemy układ równań

$$\begin{cases} 1+2\lambda x = 0 \\ 1+2\lambda y = 0 \\ x^2+y^2 = 1 \\ \lambda > 0, \end{cases}$$

którego rozwiązaniem jest

$$\begin{cases} x = (-\frac{\sqrt{2}}{2}) \\ y = (-\frac{\sqrt{2}}{2}) \\ \lambda = \frac{\sqrt{2}}{2}. \end{cases}$$



Rysunek 1: Graficzna interpretacja funkcji celu, ograniczenia oraz rozwiązania problemu (2).

Model Markowitza z instrumentem wolnym od ryzyka

Treść tego rozdziału została napisana na podstawie [2], [3], [4] oraz [5]. Rozważmy rynek instrumentów finansowych złożony z instrumentu bezpiecznego, np. lokaty, obligacji lub bonu skarbowego, o stałej stopie zwrotu R_0 oraz z n instrumentów ryzykownych, np. akcje lub fundusze inwestycyjne, o stopach zwrotu

$$R_j = \frac{P_j^1 - P_j^0 + CV_j(0,1)}{P_j^0} \quad \text{dla } j \in \{1, ..., n\}, \tag{3}$$

gdzie P_j^0 i P_j^1 oznaczają ceny j-tego instrumentu odpowiednio na początku i na końcu okresu inwestycyjnego, a $CV_j(0,1)$ opisuje wartość przepływu gotówkowego netto na koniec okresu inwestycyjnego j-tego instrumentu finansowego. Uwzględnianie składowej $CV_j(0,1)$ jest istotne dla takich instrumentów jak np. akcje z dywidendą. Inwestor posiadający kapitał W_0 chce zbudować portfel $\bar{\boldsymbol{x}} = [x_0, x_1, ..., x_n]^T \in \mathbb{R}^{n+1}$, który umożliwi mu możliwie najlepszy sposób ulokowania swoich środków pomiędzy wszystkie dostępne instrumenty. Naturalnym jest, że $\sum_{j=0}^{n} x_j = 1$. Ponadto niech m_j, dla $j \in \{1, ..., n\}$, opisuje ilość j-tego instrumentu finansowego w portfelu inwestycyjnym. Wówczas

$$x_j = \frac{m_j P_j^0}{W_0} \quad \text{oraz} \quad x_0 = 1 - \sum_{j=1}^{n} x_j. \tag{4}$$

Zwróćmy uwagę, że wektor $\bar{\boldsymbol{R}} = [R_0, R_1, ..., R_n]^T$ jest wektorem losowym określonym na pewnej przestrzeni probabilistycznej $(\Omega, \mathcal{F}, \mathbb{P})$. Dodatkowo, będziemy zakładać, że momenty drugiego rzędu zmiennych losowych R_j istnieją i są skończone, tj. $\mathbb{E}(R_j)^2 < \infty$, dla $j \in \{1, ..., n\}$. Wówczas możemy rozważać takie wielkości jak wektor wartości oczekiwanych $\bar{\boldsymbol{\mu}} = [\mathbb{E}(R_j)]_{0 \le j \le n}^T$ i macierz kowariancji $\bar{\boldsymbol{\Sigma}} = [\mathrm{Cov}(R_i, R_j)]_{0 \le i,j \le n}$ dla wektora $\bar{\boldsymbol{R}}$ oraz macierz kowariancji $\bar{\boldsymbol{\Sigma}}_{\mathbf{1,1}}$, która powstaje poprzez skreślenie z macierzy $\bar{\boldsymbol{\Sigma}}$ pierwszego wiersza i pierwszej kolumny. W teorii Markowitza wskaźnikami optymalności porfela są jego wartość oczekiwana oraz wariancja. W tym celu określamy stopę zwrotu całego portfela

$$R_{\bar{\boldsymbol{x}}} = \sum_{j=0}^{n} x_j R_j$$

oraz jej parametry, tj. oczekiwany zwrot portfela

$$\mu_{\bar{\boldsymbol{x}}} = \mathbb{E}\left(R_{\bar{\boldsymbol{x}}}\right) = \mathbb{E}\left(\sum_{j=0}^{n} x_j R_j\right) = \sum_{j=0}^{n} x_j \mathbb{E}\left(R_j\right) = \bar{\boldsymbol{x}}^T \bar{\boldsymbol{\mu}} \tag{5}$$

jak i jego ryzyko

$$\sigma_{\bar{\boldsymbol{x}}}^2 = \mathrm{Var}\left(R_{\bar{\boldsymbol{x}}}\right) = \mathrm{Var}\left(\sum_{j=0}^{n} x_j R_j\right) = \sum_{i=0}^{n} \sum_{j=0}^{n} x_i x_j \,\mathrm{Cov}(R_i, R_j) = \bar{\boldsymbol{x}}^T \bar{\boldsymbol{\Sigma}} \bar{\boldsymbol{x}}. \tag{6}$$

Zatem jesteśmy już gotowi, aby podać definicję efektywnego portfela (w sensie Markowitza).

Definicja 4. Portfel $\bar{x}$ nazywamy efektywnym, gdy nie istnieje taki portfel $\boldsymbol{x}^*$, że

$$\mu_{\boldsymbol{x}^*} \geq \mu_{\bar{\boldsymbol{x}}} \quad \text{i} \quad \sigma^2_{\boldsymbol{x}^*} < \sigma^2_{\bar{\boldsymbol{x}}}.$$

Chcąc wyznaczyć portfel efektywny w modelu Markowitza z instrumentem bezpiecznym musimy rozwiązać zagadnienie optymalizacyjne

$$\begin{cases} \sigma^2_{\bar{\boldsymbol{x}}} - 2\tau\mu_{\bar{\boldsymbol{x}}} \to \min \\ \text{przy ograniczeniu} \\ \sum_{j=0}^{n} x_j = 1, \end{cases} \tag{7}$$

gdzie parametr $\tau \geq 0$ jest nazywany współczynnikiem tolerancji ryzyka inwestora. Zauważmy, że skoro R_0 jest stałą zmienną losową, to $\text{Cov}(R_j, R_0) = 0$ dla każdego $j \in \{0, ..., n\}$. Stąd i z symetryczności kowariancji otrzymujemy

$$\sigma^2_{\bar{\boldsymbol{x}}} = \sum_{i=0}^{n}\sum_{j=0}^{n} x_i x_j \,\text{Cov}(R_i, R_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j \,\text{Cov}(R_i, R_j) = \boldsymbol{x}^T \bar{\boldsymbol{\Sigma}}_{\mathbf{1,1}} \boldsymbol{x}, \tag{8}$$

gdzie $\boldsymbol{x} = [x_1, ..., x_n]^T \in \mathbb{R}^n$ jest portfelem bez instrumentu bezpiecznego. Wobec (5), (6) i (8) problem (7) możemy zapisać w postaci macierzowej

$$\begin{cases} \boldsymbol{x}^T \bar{\boldsymbol{\Sigma}}_{\mathbf{1,1}} \boldsymbol{x} - 2\tau \boldsymbol{x}^T \boldsymbol{\mu} - 2\tau x_0 R_0 \to \min \\ \text{przy ograniczeniu} \\ \boldsymbol{e}^T \boldsymbol{x} + x_0 = 1, \end{cases} \tag{9}$$

gdzie $\boldsymbol{\mu} = [\mathbb{E}(R_j)]^T_{1 \leq j \leq n}$ i $\boldsymbol{e} = [1, ..., 1]^T \in \mathbb{R}^n$.

Twierdzenie 5. Jeżeli macierz $\boldsymbol{\Sigma}_{\mathbf{1,1}}$ jest dodatnio określona, wektory $\boldsymbol{\mu}$ i $\boldsymbol{e}$ są liniowo niezależne oraz istnieje instrument finansowy, którego oczekiwana stopa zwrotu jest większa od R_0, to dla ustalonego $\tau \geq 0$ rozwiązanie problemu (9) ma postać

$$\bar{\boldsymbol{x}} = \boldsymbol{x_0} + \tau \bar{\boldsymbol{z}}, \tag{10}$$

gdzie $\boldsymbol{x_0} = [1, 0, ..., 0]^T \in \mathbb{R}^{n+1}$ oraz $\bar{\boldsymbol{z}} = [-\boldsymbol{e}^T \boldsymbol{u}, \boldsymbol{u}^T]^T$, przy czym $\boldsymbol{u} = (\boldsymbol{\Sigma}_{\mathbf{1,1}})^{-1}\boldsymbol{\mu} - R_0(\boldsymbol{\Sigma}_{\mathbf{1,1}})^{-1}\boldsymbol{e}$.

Z dodatniej określoności macierzy $\boldsymbol{\Sigma}_{\mathbf{1,1}}$ wynika jej odwracalność oraz wypukłość funkcji celu w zagadnieniu (9), a ponieważ ograniczenie równościowe jest liniowe, więc w dowodzie twierdzenia 5 wykorzystujemy twierdzenie Karusha-Kuhna-Tuckera. Dodatkowo, gdybyśmy pominęli założenie o dodatniej określoności macierzy $\boldsymbol{\Sigma}_{\mathbf{1,1}}$, to wówczas istniałby taki portfel $\boldsymbol{x} \neq \Theta_{\mathbb{R}^n}$, dla którego $\text{Var}(R_{\boldsymbol{x}}) = 0$, czyli w skład portfela $\boldsymbol{x}$ wchodziłaby stopa zwrotu zależna w sposób liniowy od pozostałych, a więc moglibyśmy pominąć ją w naszych rozważaniach. Natomiast liniowa zależność wektorów $\boldsymbol{\mu}$ i $\boldsymbol{e}$ spowodowałaby, że oczekiwane stopy zwrotu wszystkich instrumentów byłyby takie same. Wtedy nasze rozważania uprościłyby się do modelu rynku jednookresowego dwustanowego.

Przykładowa inwestycja

Wyobraźmy sobie sytuację, w której jesteśmy brokerami w firmie ”Markowitz&Company”. W naszej działalności posługujemy się następującymi zasadami:

- Zakładamy możliwość krótkiej sprzedaży, tj. współrzędne wyznaczanych przez nas portfeli mogą przyjmować wartości ujemne;
- Dokonujemy kupna i sprzedaży instrumentów w momencie otwarcia GPW (Giełdy Papierów Wartościowych);
- Zakładamy doskonałą podzielność akcji, tj. możemy kupować rzeczywiste ilości akcji;
- W obliczeniach pomijamy podatki oraz prowizje.

Pewnego dnia przychodzi do nas klient, który chce zainwestować swój kapitał w wysokości **15 000 PLN**. Oznajmia nam również, że przez ostatni tydzień obserwował otwarcia GPW i wybrał już akcje spółek, w które chce zainwestować.

Dzień pracujący GPW	Ceny akcji spółki α	Ceny akcji spółki β
18.03	2510	65.6
19.03	2550	63.4
20.03	2630	62.2
21.03	2700	63
22.03	2660	63.6

Tabela 1: Ceny akcji spółek wybranych przez naszego klienta.

Żeby zamortyzować ewentualne straty proponujemy klientowi konto oszczędnościowe oprocentowane **7%** w skali roku (na którym fundusze akumulują się dziennie oraz można je wybrać w każdej chwili) lub identycznie oprocentowany kredyt (który możemy spłacić w każdej chwili). Na zakończenie wywiadu z klientem dowiadujemy się, że toleruje on ryzyko na poziomie **5%**. Z klientem kontaktujemy się w momencie wykonania korzystnej transakcji, żeby ustalić dalszy przebieg inwestycji. Zabieramy się do pracy. Korzystając z wzoru (3) wyznaczamy dzienne stopy zwrotu akcji spółek α i β, a ponieważ nie generują one żadnych dodatkowych przychodów, więc przyjmujemy $CV_{\alpha}(0,1) = CV_{\beta}(0,1) = 0$.

Dzienne stopy zwrotu akcji α (R_k^{α})	Dzienne stopy zwrotu akcji β $\left(R_k^{\beta}\right)$
0.0159	−0.0335
0.0313	−0.0189
0.0266	0.0128
−0.0148	0.0095

Tabela 2: Dzienne stopy zwrotu z akcji spółek wybranych przez naszego klienta.

Natomiast dzienna stopa zwrotu naszego instrumentu bezpiecznego wynosi $R_0 = \frac{0.07}{364.25} = 1.921 \cdot 10^{-4}$.
Do wyznaczenia $\boldsymbol{\mu}$ i $\bar{\boldsymbol{\Sigma}}_{\mathbf{1,1}}$ z danych wykorzystamy następujące estymatory wartości oczekiwanej i kowariancji, odpowiednio:

$$\hat{\mu}_{R^j} = \frac{1}{4}\sum_{k=1}^{4} R_k^j \quad \text{oraz} \quad \hat{\gamma}_{R^j R^i} = \frac{1}{3}\sum_{k=1}^{4}(R_k^j - \hat{\mu}_{R^j})(R_k^i - \hat{\mu}_{R^i}),$$

dla $j \in \{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$. Wówczas

$$\boldsymbol{\mu} = \begin{bmatrix} 9.851 \\ -5.013 \end{bmatrix} \cdot 10^{-3} \quad \text{oraz} \quad \bar{\boldsymbol{\Sigma}}_{\mathbf{1,1}} = \begin{bmatrix} 2.779 & -1.063 \\ -1.063 & 3.076 \end{bmatrix} \cdot 10^{-4}.$$

Następnie odwracamy macierz $\bar{\boldsymbol{\Sigma}}_{\mathbf{1,1}}$ i wykorzystujemy wzór (10) z twierdzenia 5. W ten sposób otrzymujemy portfel w postaci

$$\bar{\boldsymbol{x}} = [-0.344, 1.61, -0.266]^T.$$

W dniu 22.03 ceny akcji spółek $\boldsymbol{\alpha}$ i $\boldsymbol{\beta}$ wynoszą odpowiednio **2 660 PLN** i **63.6 PLN**. Wyznaczając m_j, dla $j \in \{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$, z wzoru (4) otrzymamy ilości akcji, którymi będziemy operować podczas inwestycji. Rozpoczynamy transakcję zgodnie z portfelem $\bar{\boldsymbol{x}}$:

- bierzemy kredyt w wysokości $0.344 \cdot 15000 =$ **5 160 PLN**;
- pożyczamy $m_{\boldsymbol{\beta}} = \frac{0.266 \cdot 15000}{63.6} =$ **62.74** jednostki akcji spółki $\boldsymbol{\beta}$;
- kupujemy $m_{\boldsymbol{\alpha}} = \frac{1.61 \cdot 15000}{2660} =$ **9.08** jednostek akcji spółki $\boldsymbol{\alpha}$.

Kolejnego dnia pracy GPW, tzn. 25.03, w momencie otwarcia akcja spółki $\boldsymbol{\alpha}$ kosztuje **2 690 PLN**, a akcja spółki $\boldsymbol{\beta}$ kosztuje **63 PLN**. Przechodzimy do rozliczenia naszego portfela:

- sprzedajemy **9.08** jednostek akcji spółki $\boldsymbol{\alpha}$, dzięki temu jesteśmy w posiadaniu $9.08 \cdot 2690 =$ **24 425.2 PLN**;
- oddajemy kredyt wraz z odsetkami w wysokości $5160 \cdot \left(1 + \frac{0.07}{364.25}\right)^3 =$ **5 162.97 PLN**;
- zwracamy pożyczone **62.74** jednostki akcji spółki $\boldsymbol{\beta}$, a więc $62.74 \cdot 63 =$ **3 952.62 PLN**.

Ostatecznie zostajemy z kwotą **15 309.61 PLN**, czyli przez weekend zarobiliśmy **309.61 PLN**. Kontaktujemy się z naszym klientem i uzgadniamy dalszy plan działania ...

Literatura

[1] Drwalewska A., Lipińska V.; Wstęp do optymalizacji: zastosowania w logistyce i biznesie; Wydawnictwo Politechniki Łódzkiej; Łódź 2013.

[2] Drwalewska A., Lipińska V.; Optymalny portfel inwestycyjny; Wydawnictwo Politechniki Łódzkiej; Łódź 2012.

[3] Elton E.J., Gruber M.J.; Nowoczesna teoria portfelowa i analiza papierów wartościowych; WIG-Press; Warszawa 1998.

[4] Gajek L., Ostaszewski K.; Plany emerytalne. Zarządzanie aktywami i zobowiązaniami; Wydawnictwo Naukowo Techniczne; Warszawa 2002.

[5] Markowitz H.; Portfolio Selection; The Journal of Finance 7 (1952); 77-91.

[6] Panjer H.H.; Financial economics with application to investments, insurance and pension; Actuarial Foundation; 1998.

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

APPLICATIONS OF THE FIBONACCI SEQUENCE IN FINANCIAL MARKETS

Mateusz SZYDŁOWSKI[1], Tohid ZEINALI[1]

[1] Faculty of Organization and Management, Lodz University of Technology, Lodz

Abstract

This paper demonstrates how mathematics can be used to forecast financial market behaviour. The authors aim to share their knowledge and experience with a set of tools used in technical analysis. The given techniques are based on the Fibonacci sequence and are shown as applicable to market strategies. The authors present their analyses from real-life examples. A study of large financial markets, such as the S&P 500 Index and Bitcoin, revealed the following characteristics of those equities.

Keywords: Fibonacci sequence, financial market, technical analysis, Fibonacci retracement, financial market strategy

Introduction

Interest in investing in financial markets increased significantly during a time of constant changes and search for new ways of earning money. The main idea of all business models remains the same: buy cheap, sell high. However, this principle is as difficult to implement in “typical” businesses as it is in financial markets. It is not possible to make decisions on which shares to buy or sell and at which time solely by guessing and achieve satisfactory results. Good luck may eventually run out, and unfavourable consequences may become real. Traders aim to base their investments not only on their hunches but also on the study of actual and historical data and created plenty of tools, patterns, and strategies.

The first thought about financial markets is often associated with the stock market. Although such a connection is correct, it does not fully explain this term. On the stock market, also called a stock exchange or equities market, companies list their shares, whose price is later regulated by the pricing of buyers and sellers as well as economic circumstances [1]. The financial market is a more general term. According to [2] *“Financial Markets include any place or system that provides buyers and sellers the means to trade financial instruments, including bonds, equities, the various international currencies, and derivatives.”* There are two types of analyses which give traders higher level of confidence – fundamental and technical. Fundamental analysis is based on the financial statements, micro- and macro-economic factors that can provide insights into the instrument's condition. This type of analysis helps assess the intrinsic value and make it easier to indicate whether the actual price is under- or overvalued [3]. Technical analysis focuses on a security’s price fluctuations and behaviour based on historical data. This type of analysis uses statistics, mathematical models, and patterns. This is why the focus of this paper is on technical analysis, with special emphasis on Fibonacci tools. It should be remembered that a single technical analysis tool cannot be used as the only indicator. Conducting such analyses requires experience and understanding of the market in which one plans to invest.

Fibonacci was an Italian mathematician, Leonardo of Pisa, who lived in the 12th and 13th centuries. Although he provided many works, his name is mostly known for defining a number sequence. The sequence originated from a prediction of idealized rabbit population growth. The next sequence element is calculated as the sum of two former numbers. A formula describing this sequence, stated later by Albert Girard, is presented in (1) and is applicable to natural numbers [4].

$$F_{n+2} = F_{n+1} + F_n \quad (1)$$

The common ratios in financial market analysis are 0.236, 0.382, 0.618 and 1.618. Their derivation comes from dividing specific numbers in order. 0.236 is calculated by dividing an element by a number that is 3 places ahead, 0.382 by dividing an element by a number that is 2 places ahead, and, following the pattern, 0.618 is a division of an element by its follower. 1.618 is the inverse of 0.618, as is its calculation method. These ratios are not derivable at the lower order elements. Robert Simson showed in 1753 that as the numbers increase in value, the ratios between the following numbers are closer to the golden ratio – 1.618 [5].

Fibonacci tools in financial markets

Fibonacci tools are pivotal in technical analysis. These tools utilize Fibonacci sequence numbers and derived ratios to identify significant support and resistance levels in financial markets. Traders apply Fibonacci retracement levels to predict potential price pullbacks that follow specific movements. Fibonacci extensions offer insights into future price targets beyond the initial trend, enhancing traders' ability to forecast market dynamics. The additional use of Fibonacci time zones enriches analysis by presenting the potential timing of market reversals and trend continuations. Employing these tools helps traders make strategic decisions about entry and exit points.

Fibonacci Time Zones

Fibonacci time zones focus on when the trend turning points may occur, but they do not indicate whether the turn will be an increase in value or a correction. This tool's methodology is based on selecting a minimum and maximum price within a chosen period. The time between these two points is set as a reference time length, which is then extended to the future. The time zones are created in accordance with the consecutive numbers of the Fibonacci sequence, with the reference time length being the interval between the 0^{th} and 1^{st} elements of the sequence [5]. An exemplary use of this tool can be seen on the historical graph of the S&P 500 Index, where the reference time length was approximately two years (Figure 1).

Figure 1 Reference time step selection

The first forecast turn was expected to occur at the beginning of 2020. According to Figure 2 such a situation occurred. The S&P 500 Index experienced some minor shifts within the Fibonacci time zones and the next turn is predicted to happen in 2026.

Figure 2 Forecast throughout the years and in the future

Fibonacci Retracement

With the help of Fibonacci retracement, traders can identify trends or retracements in financial markets. The methodology, similar to that of time zones, focuses on selection of a minimum and maximum within a chosen period. It is important to examine a stock that: a) has either a downtrend or up-trend, and b) has recently started a retracement [6]. This distance is referred to as a unit and is divided into several regions. Popular ratios for Fibonacci retracement are 0.236, 0.382, 0.5, 0.618 and 0.786. 0.5 does not originally come from the Fibonacci sequence, it was utilized by Charles Dow and William D. Gann [7]. The choice of which level corresponds to the support and resistance is based on knowledge of the market, experience, and the duration of a change – known as the "swing". For example, if the swing is relatively long, a ratio of 0.236 is sometimes used [8].

An example of a stock following the Fibonacci retracement can be Microsoft Corporation (MSFT) in years 2020 – 2024. As minimum point was chosen a value of stock after a significant correction in 2020, as a maximum – price in 2022. The reference value range is divided into only 3 regions by lines corresponding to 38.2% and 61.8%, to obtain a clear picture. It was decided that the aimed retracement ratio is when the price reaches the level of 61.8%. Then the stock would go uptrend and it would be a good time to buy [9]. The examined stock proved this hypothesis. Price of a single MSFT share almost doubled its value in less than two years (Figure 3).

Figure 3 Fibonacci retracement application and result

Fibonacci Extension

This tool is based on the idea that markets might retrace a predictable portion of a move, after which they will continue to move in the original direction. Fibonacci extensions are particularly useful in trending markets for setting profit targets. In this tool, the most important ratio is 161.8%. To draw it, one needs to specify three points on the chart. The first point is the end of a correction and marks the beginning of a new trend. The second point is the end of that trend. The third point is the beginning of the wave that we want to find the end of [4]. The example of the application of this tool is shown in the Tesla chart in Figure 4.

Figure 4 Fibonacci extension application

Strategies Based on Fibonacci tools

To gain a more comprehensive view of the financial markets and maximize profits while minimizing losses, financial market analysts have developed several strategies. These strategies, shaped by various technical analysts, combine recurring patterns, Fibonacci tools, and insights into investor psychology to provide more accurate entry and exit points. Three of the most widely used strategies are Harmonic Patterns, Elliott Wave Theory, and NeoWave.

Harmonic patterns

Harmonic patterns are in a group of specific chart formations that traders use to identify potential reversal points based on Fibonacci ratios. They are characterized by unique geometric structures and specific sequences of price movements, referred to as legs [10]. Schematic structures of four patterns and simplified breakdown of each one are shown in Figure 5.

Crab Pattern

This pattern often signals significant price reversals, potentially providing high rewards. It involves four legs: XA, AB, BC, and CD. The CD leg extends up to 161.8% of the XA leg. AB retraces 38.2% to 61.8% of XA, BC extends 38.2% to 88.6% of AB, and CD extends beyond 161.8% of XA.

Butterfly Pattern

This pattern includes four legs: XA, AB, BC, and CD. CD extends 127.2% to 161.8% of the XA leg. AB retraces 78.6% of XA, while BC extends 38.2% to 88.6% of AB.

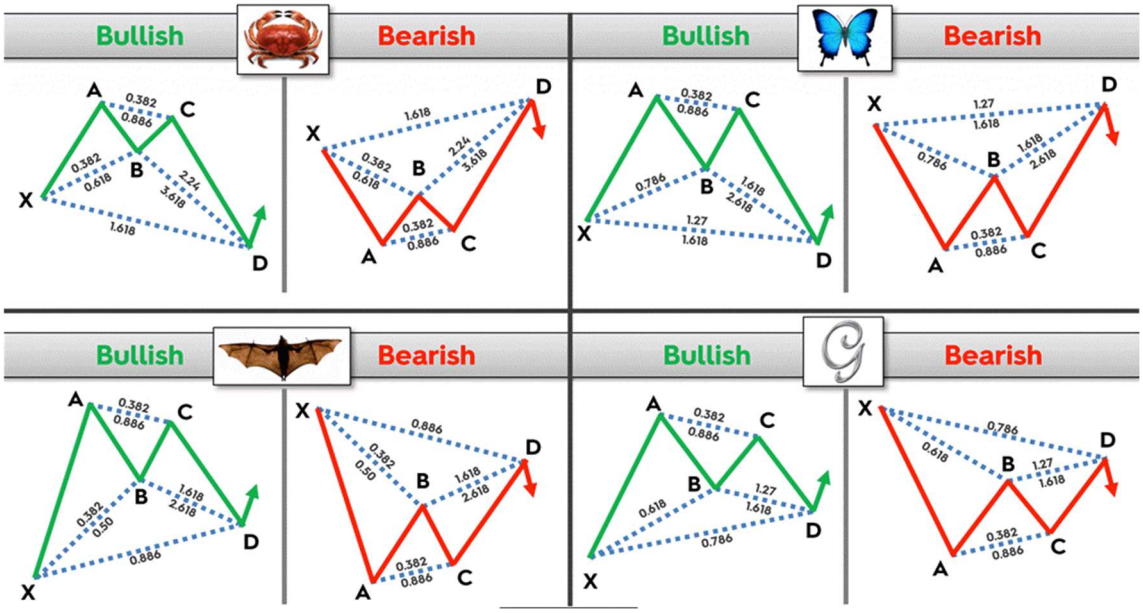


Figure 5 Schematic structure of patterns [11]

A classic harmonic pattern known as the "222 pattern" after its origin in H.M. Gartley's book. It has four legs: XA, AB, BC, and CD, with the CD leg retracing about 78.6% of the XA leg. AB retraces 61.8% of XA, BC extends 38.2% to 88.6% of AB, and CD retraces around 78.6% of XA.

Bat Pattern

This pattern offers a different risk-reward setup than the Gartley pattern. It includes four legs: XA, AB, BC and CD. The CD leg extends to around 88.6% of the XA leg. AB retraces 38.2% to 50% of XA, BC extends 38.2% to 88.6% of AB, and CD retraces roughly 88.6% of XA [10]. The studied cryptocurrency (Bitcoin) shows a bat pattern (Figure 6).

Figure 6 Bat pattern application and result

Elliott Wave Theory

Elliott Wave Theory is a technical analysis method established in the 1930s by Ralph Nelson Elliott. It seeks to identify patterns in financial market movements that reflect collective investor psychology, forming identifiable wave patterns. This theory is strongly associated with Fibonacci ratios, which help predict wave lengths and retracement levels. These patterns consist of impulse waves, corrective waves.

Impulse Waves

Five waves that move in the same direction as the main market trend. In the five-wave impulse structure, the third wave often extends to 1.618 times the length of the first.

Corrective Waves

Three waves that go against the main trend. In the three-wave corrective structure, the B wave typically retraces 38.2% to 61.8% of the A wave. The C wave often matches the length of wave A or extends to 1.618 times its length [12]. Schematic structures of this theory are shown in Figure 7.

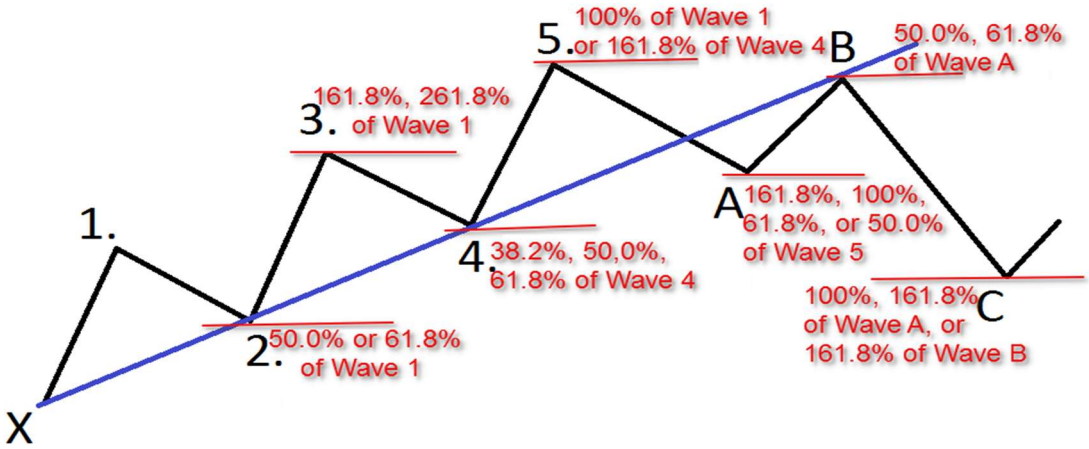


Figure 7 Schematic structure of Elite wave [13]

NeoWave

NeoWave is an advanced version of Elliott Wave Theory, developed by Glenn Neely. This approach builds upon the original concepts of Elliott Wave Theory by adding new rules and guidelines to address the complexities and ambiguities often encountered in traditional wave analysis. NeoWave introduces additional patterns, refines wave classification, and offers more specific rules to improve the accuracy of wave identification and trading predictions. NeoWave continues to use Fibonacci ratios to predict potential extensions and retracements of waves, providing more precise guidelines for these measurements. It ensures that retracements and extensions fall within specific ranges that align with market conditions.

NeoWave recognizes more complex patterns that involve Fibonacci ratios, such as expanded flats, triangles, and other corrective structures, which need careful interpretation. The relationships between different waves are refined to incorporate Fibonacci ratios, not only within the context of impulse and corrective waves but also considering more complex structures and sub-waves. In 1990, Neely published a forecast about the Dow Jones Index. After examining 200 years of data, he concluded that this index would reach 100,000 per unit by 2060. At the time this analysis was published the price per unit was 1000 [14]. The analysis of his forecast is shown in Figure 8.

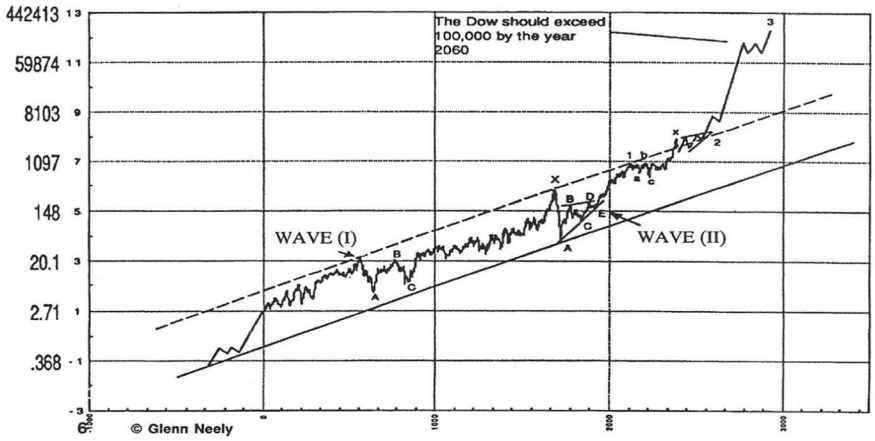


Figure 8 Graph of Neely forecast [14]

Conclusion

The Fibonacci sequence has demonstrated remarkable applications in technical analysis for forecasting financial markets. By leveraging Fibonacci retracements, extensions and time zones, traders can better anticipate potential market movements. Harmonic patterns and Elliott Wave Theory, supported by Fibonacci ratios, further enhance traders' ability to predict price movements. While these techniques are valuable, they require a solid understanding of market behavior and should be used alongside other analytical methods. Achieving proficiency in these strategies can greatly enhance market prediction accuracy, giving traders a strategic edge in the constantly shifting financial world.

Bibliography

[1] Y. Mishura, 'Introduction', in *Finance Mathematics*, Y. Mishura, Ed., Elsevier, 2016, pp. xi–xiv. doi: 10.1016/B978-1-78548-046-1.50006-5.
[2] 'Financial Markets', OCC.gov. Accessed: May 05, 2024. [Online]. Available: https://www.occ.gov/topics/supervision-and-examination/capital-markets/financial-markets/index-financial-markets.html
[3] R. Patel, J. W. Goodell, M. E. Oriani, A. Paltrinieri, and L. Yarovaya, 'A bibliometric review of financial market integration literature', *Int. Rev. Financ. Anal.*, vol. 80, p. 102035, Mar. 2022, doi: 10.1016/j.irfa.2022.102035.
[4] C. Brown, *Fibonacci analysis*, vol. 42. John Wiley & Sons, 2008.
[5] G. MacLean, *Fibonacci and Gann Applications in Financial Markets: Practical Applications of Natural and Synthetic Ratios in Technical Analysis*. John Wiley & Sons, 2005.
[6] N. Sethi, N. Bhateja, J. Singh, and P. Mor, 'Fibonacci Retracement in Stock Market', Mar. 2020, doi: 10.2139/ssrn.3701439.
[7] R. A. Batchelor and R. Ramyar, 'Magic numbers in the Dow', Sep. 2006.
[8] D. S. Hobbs, *Fibonacci for the Active Trader*. TradingMarkets, 2003.
[9] L. Lusindah and E. Sumirat, 'Implementation of Fibonacci Retracements and Exponential Moving Average (EMA) Trading Strategy in Indonesia Stock Exchange', *Eur. J. Bus. Manag. Res.*, vol. 6, no. 4, Art. no. 4, Aug. 2021, doi: 10.24018/ejbmr.2021.6.4.1033.
[10] S. M. Carney, *Turning Patterns into Profits with Harmonic Trading (Collection)*. FT Press, 2012.
[11] InvestarIndia, 'Harmonic Patterns – An Introduction to Harmonic Trading', Investar Blog. Accessed: May 05, 2024. [Online]. Available: https://investarindia.com/blog/harmonic-trading/
[12] Alfred John Frost and Robert Rougelot Prechter, *Elliott wave principle: key to market behavior.* New Classics Library, 1995.
[13] V. Patel, 'Using Elliott Wave Theory To Trade Forex', Forex Training Group. Accessed: May 05, 2024. [Online]. Available: https://forextraininggroup.com/understanding-the-basics-of-trading-with-the-elliott-wave-theory/
[14] G. Neely and E. Hall, *Mastering Elliott Wave: Version 2.0*. Windsor Books, 1990.

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

GAME THEORY: THE ACCURACY OF MATHEMATICAL MODELS IN PREDICTING HUMAN BEHAVIOR.

Adrianna CZECHOWSKA[1]

[1] Politechnika Łódzka, Łódź

Introduction

This article explores the disparity between the accuracy of mathematical models in predicting human behaviour within game theory. At the beginning a brief history and general applications of game theory will be introduced, explaining its foundational concepts such as zero-sum games, Nash equilibrium, and the prisoner's dilemma. Bridging the gap between rational predictions and actual human actions will be discussed at the end. Theoretical questions will be addressed as follows: How do normative models rationally explain optimal strategies? Why do these models fail to predict human behaviour accurately? How do descriptive models from psychology account for emotional and cognitive factors influencing decisions?

Game theory

Game theory is a branch of mathematics addressing situations involving conflicting interests. It was first mathematically formulated in 1944 by John von Neumann and Oskar Morgenstern who took notice of the fact that mathematics used in physical sciences was of a disinterested nature [1][2]. It did not take into consideration the strategic interactions and it assumed the behaviour of the objective natural phenomena, hence it was not a good fit for economics involving a complex interplay between individuals, businesses, and governments, each responding to different incentives. Consequently, Neumann and Morgenstern developed game theory to model these situations as "games," where individuals are depicted as rational players (usually referred to as agents) with specific goals to maximise their gain. Agents rely on logic and rationality, rather than chance or luck. The strategic process of decision-making is usually modelled using directed graphs called game trees or matrices[1]. This article will use matrices as they effectively display the outcomes, represented by players' utility functions, for all possible strategy combinations.

Zero-sum games

A zero-sum game is a situation in game theory where one player's gain is exactly balanced by another player's loss, resulting in a net sum of zero [2]. Some examples include poker, chess or election campaigns. A depiction of such a situation in a two-person arrangement can be observed in Figure 1. Each cell in the matrix shows the payoff for both players based on their chosen strategies. The first number in each cell is Player 1's payoff and the second number is Player 2's payoff. It can be observed that regardless of the strategy chosen, one player will always lose, indicating there is no equilibrium in this game. There is no stable solution where the outcome can be optimised for both players.

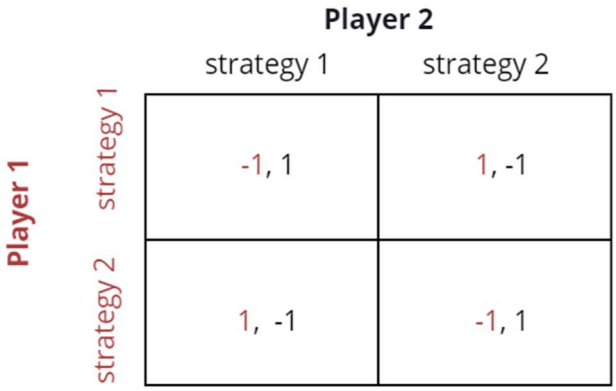


Figure 1: An Example of a Matrix for a Two-Person Zero-Sum Game

Nash equilibrium

Nash equilibrium is a stable state in game theory where each player's strategy is optimal given the strategies chosen by the other players, with no incentive for any player to unilaterally deviate [3]. A portrayal of such a situation in a two-person scenario can be observed in Figure 2. The numbers in each cell represent the payoffs for Player 1 and Player 2 for each combination of strategies. Here, the Nash equilibrium occurs twice. First, when Player 1 chooses Strategy 1, and Player 2 chooses Strategy 1. The payoffs are (5, 9). Second, when Player 1 chooses Strategy 2, and Player 2 chooses Strategy 2. The payoffs are (4, 7). In both cases, each player's strategy is optimal given the strategy of the other player, and neither has an incentive to unilaterally change their strategy. Rational thinking leads to the maximisation of gain.

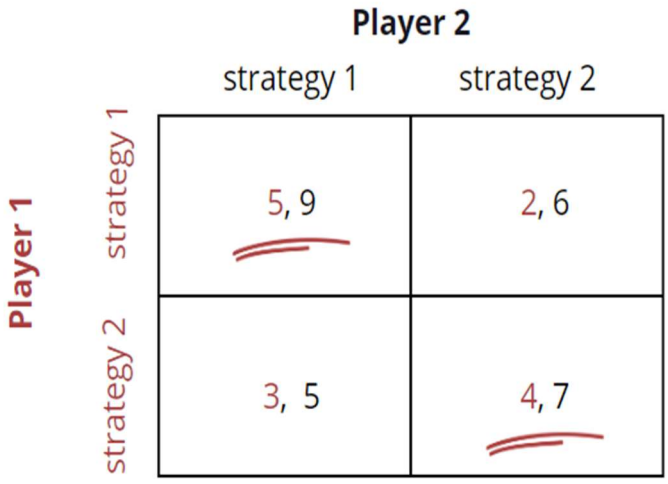


Figure 2: An Example of a Matrix for a Two-Person Nash Equilibrium.

Prisoner's dilemma

A prisoner's dilemma is a situation in which two individuals, acting in their own self-interest, result in a collectively worse outcome by not cooperating, even though cooperation would yield the best outcome for both [3]. An illustration of this situation in a two-person scenario is shown in Figure 3. If both prisoners confess, they each receive 5 years in prison. If Prisoner A confesses while Prisoner B remains silent, A goes free (0 years) and B receives 20 years.

If Prisoner A remains silent while Prisoner B confesses, A receives 20 years and B goes free (0 years). If both prisoners remain silent, they each receive 1 year in prison. The optimal collective outcome is achieved when both prisoners remain silent, resulting in 1 year of imprisonment for each. It is the best choice assuming both prisoners are led by pure reason and want to minimise their sentence. Unfortunately, due to fear and self-interest, it is more probable that each prisoner confesses, anticipating that the other might confess to minimise their own sentence. This results in a worse collective outcome of 5 years each, but it minimises the risk. The pressing question is how we can more accurately predict the prisoners' choices if the rational choice that maximises collective gain is often not the strategy they actually follow? Descriptive models and psychology prove to be useful.

Figure 3: An Example of a Matrix for a Prisoner's Dilemma.

Descriptive and normative models

Normative models assume that the decision-maker is strictly rational. They provide standards for how decisions should be made to achieve the most optimal outcomes. They are based on mathematical principles and logical analysis. On the other hand, descriptive models take into consideration that the decision-maker might be influenced by some other factors such as emotions or heuristics [4].

An example of a descriptive model from the field of psychology which helps to fill the gap between rational predictions of game theory and actual human actions is the adaptive decision-maker framework developed by Payne, Bettman and Johnson in 1933 [5]. It showcases that the strategy one uses is based on one of the 4 meta-goals proposed in the framework:

- maximising decision accuracy
- minimising the cognitive effort
- minimising the experience of negative emotion
- maximising the ease of justification of a decision

These goals demonstrate why in many cases, just like in Prisoner's dilemma, normative models are not enough to accurately predict one's actions. Based on the previously given example from Figure 3. it can be interpreted that prisoners chose to confess because it is easier to do it and reduce the sentence rather than analyse the most collectively optimal choice and take the risk that the other person might also disclose some information. This decision can also be relatively easy to justify as individuals are acting in their self-interest and it can be less stressful (which minimises the experience of negative emotion) because it lowers the chance of the extended sentence.

Discussion and conclusions

In summary, normative models from game theory provide the idealised decision-making strategy based on which we can predict one's behaviour assuming that they are led purely by logic. What they lack is the consideration of the complexity of the human psyche. Nevertheless, they are a good tool to speculate what might be the choice of our opponent in a situation of conflicting interests.

The accuracy of game theory in predicting human behaviour can be increased by taking into account descriptive models as well as the fact that humans have limited cognitive ability and often will take mental shortcuts while making decisions. What seems to be crucial is the comprehensive analysis of different phenomena from the perspective of different fields of science as this betters our understanding of human behaviour.

Bibliography:

[1] Ross D.: Game Theory, In The Stanford Encyclopedia of Philosophy, edited by Edward N. Zalta and Uri Nodelman, Spring 2024 edition, Metaphysics Research Lab, Stanford University, 2024. https://plato.stanford.edu/archives/spr2024/entries/game-theory/.

[2] Davis M. D., Brams S. J.: Game Theory, Encyclopedia Britannica, May 10, 2024. https://www.britannica.com/science/game-theory.

[3] Chen J.: Nash Equilibrium: How It Works in Game Theory, Examples, Plus Prisoner's Dilemma, Trading Strategies, Investopedia, Updated February 28, 2024, reviewed by Gordon Scott, fact-checked by Kirsten Rohrs Schmitt. https://www.investopedia.com/terms/n/nash-equilibrium.asp

[4] Ronen, Joshua, and George H. Sorter. "Descriptive and the Normative." In Objectives of Financial Statements, Volume 2: Selected Papers, edited by University of Mississippi. eGrove, Touche Ross Publications, Deloitte Collection, 1974.

[5] Payne, J. W., Bettman, J. R., and Johnson, E. J. The Adaptive Decision Maker. Cambridge University Press, 1993. https://doi.org/10.1017/CBO9781139173933.

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

MATEMATYCZNA DROGA DO ALTRUIZMU

Jakub CHMIEL
Politechnika Krakowska im. Tadeusza Kościuszki, Kraków

Wprowadzenie

Skąd wziął się altruizm? I czy prawdziwy altruizm istnieje? Zaskakujące jest, że odpowiedzi na te pytania może nam przynieść matematyka, a konkretnie teoria gier i iterowany dylemat więźnia. W tej pracy chciałbym pokazać jak Robert Axelrod badał problem altruizmu oraz przedstawić wyniki napisanego przeze mnie programu. Padną istotne pytania o pochodzenie altruizmu oraz o to czy prawdziwy altruizm istnieje. Ciekawym wnioskiem jest to, że matematyka pokazuje nam dlaczego opłaca się być dobrym człowiekiem.

Dylemat więźnia

W pewnym teleturnieju dwaj przypadkowi gracze dostają do podziału nagrodę pieniężną. Każdy z nic musi podjąć decyzję niezależnie, nie wiedząc, co wybierze druga osoba. Każdy uczestnik ma dwie możliwości: współpracować albo zdradzić. Współpraca oznacza, że obaj uczestnicy decydują się podzielić nagrodę w sposób sprawiedliwy. Zdrada oznacza, że jeden z uczestników próbuje zdobyć większą część nagrody kosztem drugiego.
Jeśli obaj zdecydują się współpracować, obaj dostaną po 3 tysiące złotych. Jeśli obaj zdecydują się zdradzić, obaj dostaną po 1 tysiącu złotych. Jeśli jedna osoba zdecyduje się współpracować, a druga zdradzić, osoba współpracująca dostanie 0 złotych, a osoba zdradzająca 5 tysięcy złotych. Podział nagrody w zależności od wybranej strategii prezentuje poniższa macierz wypłat.

	Gracz B		
Gracz A		Współpraca	Zdrada
	Współpraca	(3, 3)	(0, 5)
	Zdrada	(5, 0)	(1, 1)

Para (a, b) znajdująca się na przecięciu strategii wybranych przez graczy to suma ich wypłat, gdzie a oznacza wypłatę gracza A, natomiast b - wypłatę gracza B (w tysiącach złotych).

Gra tego typu znana jest jako dylemat więźnia i jest jedną z ciekawszych gier o sumie niezerowej. Gra o sumie niezerowej to taka gra, w której suma wygranych wszystkich graczy nie jest równa zero. Inną definicją używaną w teorii gier to gracz racjonalny, czyli taki gracz, który podejmuje możliwie najlepsze dla siebie decyzje. W tym przypadku zdrada jest zawsze lepsza od współpracy.

Jeśli przeciwnik chce współpracować, to możemy wybrać współpracę i otrzymać 3 tysiące nagrody lub zdradę i otrzymać 5 tysięcy. Podobnie w przypadku, gdy przeciwnik zdradzi: mamy wtedy wybór między brakiem wygranej (przy wyborze współpracy) lub wygraniu tysiąca (przy zdradzie).

W obu przypadkach wybór zdrady daje nam większą wygraną. Jednak jeśli obaj gracze są racjonalni to obaj wybiorą zdradę (1, 1) i dostaną po tysiącu złotych mimo, że istnieje wybór zdecydowanie lepszy jednocześnie dla każdego z nich (3, 3). Punkt (1, 1) jest tak zwaną równowagą Nash'a, gdyż przy takich wyborach nie opłaca się żadnemu graczowi zmienić swojej decyzji, jeśli drugi gracz swojego zdania nie zmienia.

Z dylematem więźnia mamy do czynienia w wielu sytuacjach np. gdy dwa państwa toczą ze sobą wyścig zbrojeń i zastanawiają się, czy się zbroić czy rozbrajać. Gra ta spotykana jest w takich naukach jak ekonomia, polityka czy socjologia.

Rys historyczny

W 1859 roku Charles Darwin opublikował dzieło „O powstaniu gatunków", które wstrząsnęło światem. Darwin napisał tam, że dobroć wśród zwierząt jest „najpoważniejszym problemem mojej teorii".
Kto korzysta na tej dobroci? Wspólnota? Czy dobór działa na poziomie grupy szkodząc jednostce? W jaki sposób w doborze naturalnym mogą być preferowane cechy zmniejszające przystosowanie jednostki? Cechy takie jak np. altruizm.

Altruizm możemy zdefiniować jako:
- Kierowanie się w swym postępowaniu dobrem innych, gotowość do poświęceń. (Słownik PWN)
- Działanie na korzyść innych; dobrowolne ponoszenie pewnych kosztów przez jednostkę na rzecz innej jednostki lub grupy; zachowanie przeciwstawne egoizmowi. (Wikipedia)

Turniej

Nad problemem altruizmu zastanawiało się wiele osób. Warto przy tej okazji wymienić Piotra Kropotkina, który jako jeden z pierwszych uczonych spojrzał na altruizm jak na sumę zysków i strat, które podświadomie są analizowane przez ludzi lub zwierzęta. Swój wkład miał także William Hamilton, który badał temat doboru krewniaczego. Należy również wspomnieć o Georgu Price'ie, chemiku, twórcy równania kowariacyjnego. Równanie to opisuje proces zmiany częstości alleli w populacji.
W ciekawy sposób zagadkę altruizmu badał Robert Axelrod. Wpadł on na pomysł, że to zagadnienie można badać poprzez iterowany dylemat więźnia. Polega on na graniu w dylemat więźnia raz za razem. Gra ta jest dużo bardziej skomplikowana niż jej klasyczna wersja, ponieważ gracze są świadomi tego, jak ich przeciwnik zagrał w poprzedniej rundzie.
Jaka jest najlepsza strategia w iterowanym dylemacie więźnia? Poniżej prezentuję przykładowe strategie (fenotypy):

- Zdrajca (zawsze zdradza),
- Frajer (zawsze współpracuje),
- Losowy (podejmuje losowe decyzje),
- Obrażalski (współpracuje do momentu, aż przeciwnik po raz pierwszy go zdradzi. Wtedy się obraża raz na zawsze),
- WetZaWet (zaczyna od współpracy, a następnie kopiuje poprzedni ruch przeciwnika).

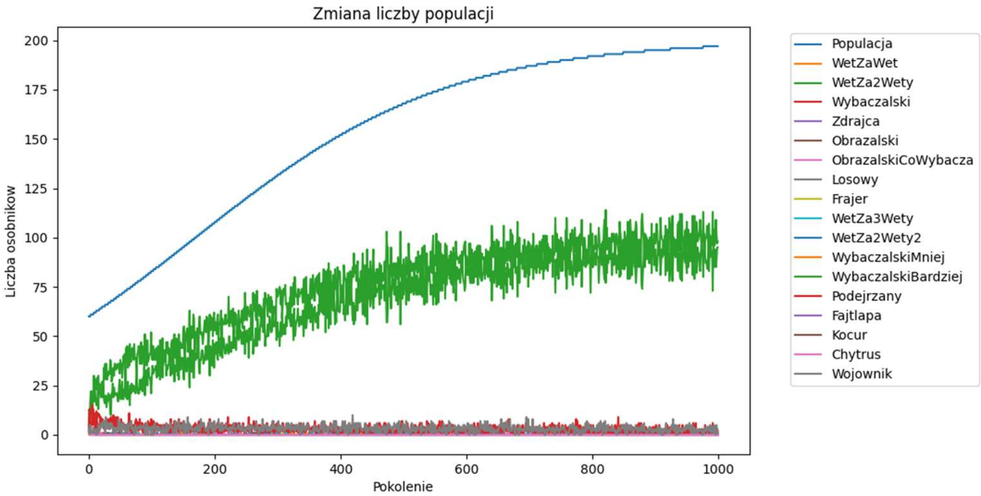
Właśnie to zagadnienie badał Robert Axelrod. Wymyślił on turniej, w którym osobniki o różnych fenotypach grały, w systemie każdy z każdym, w iterowany dylemat więźnia. Przeanalizujemy program, który bada to zagadnienie. W populacji znajduje się 17 osobników grających różnymi strategiami. Program przeprowadza dylemat więźnia pomiędzy każdymi dwoma osobnikami 200 razy, a następnie porządkuje ich malejąco w zależności od liczby zdobytych punktów. Po przeprowadzeniu wielu gier można zauważyć, że najlepszymi strategiami są WetZaWet oraz Obrażalski.

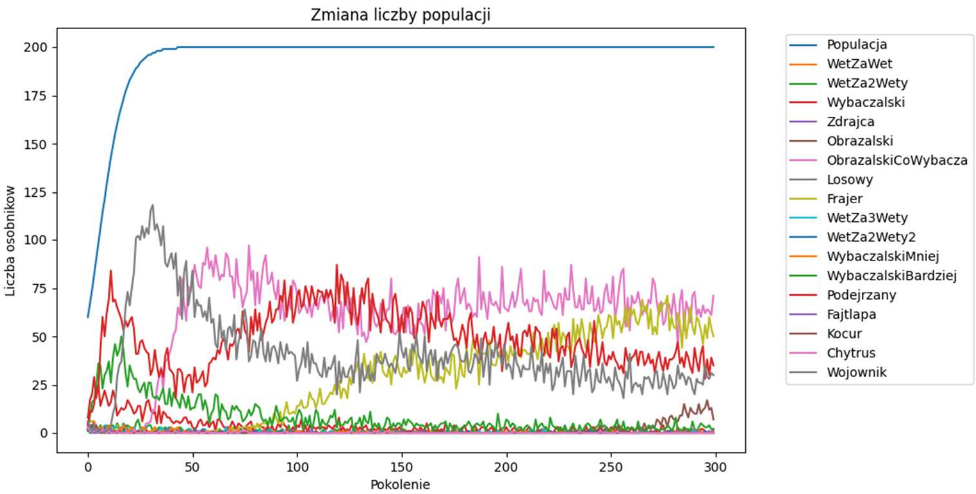
Jeśli jednak program ten ma w jakiś sposób symulować otaczającą nas rzeczywistość pojawia się pewien problem. Gdy w tej symulacji spotkają się dwa osobniki o fenotypie WetZaWet będą one współpracowały ze sobą cały czas, jednak w rzeczywistości czasami dobre intencje są źle odbierane, innymi słowy dochodzi do pomyłek, które trzeba wziąć pod uwagę. W takim przypadku, gdy czasem jednostki będą się mylić, dwa osobniki będą współpracowały z sobą do momentu pierwszej pomyłki, wtedy zaczną się nawzajem zdradzać, a gdy dojdzie do drugiej pomyłki obrażą się na siebie na zawsze. Ponadto w otaczającym nas świecie iterowany dylemat więźnia objawia się w różnych grupach, czasem w grupie w której jest więcej osób naiwnych, a czasem zdradliwych.

Dlatego, ponownie przeanalizujmy drugą wersję programu. Program ten:

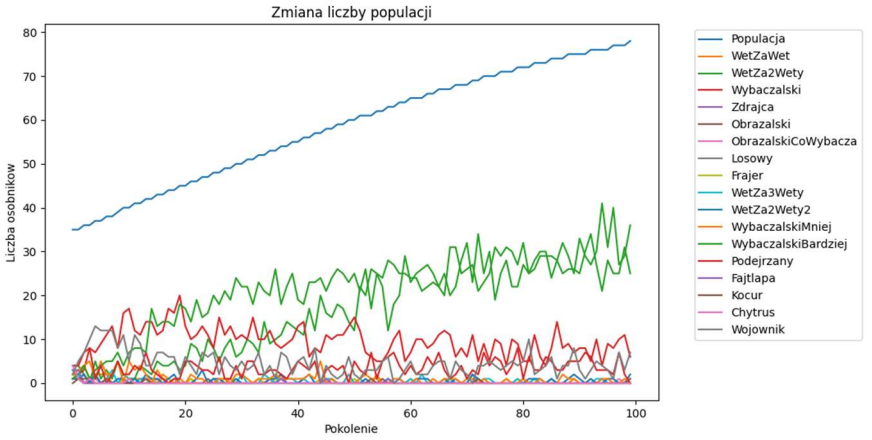
- losuje początkową populację złożoną z osobników o różnych fenotypach,
- przeprowadza iterowany dylemat więźnia między każdymi dwoma osobnikami,
- preferuje w następnym pokoleniu geny osób, które sobie najlepiej poradziły (dobór naturalny),
- sprawdza co się stanie po wielu pokoleniach.

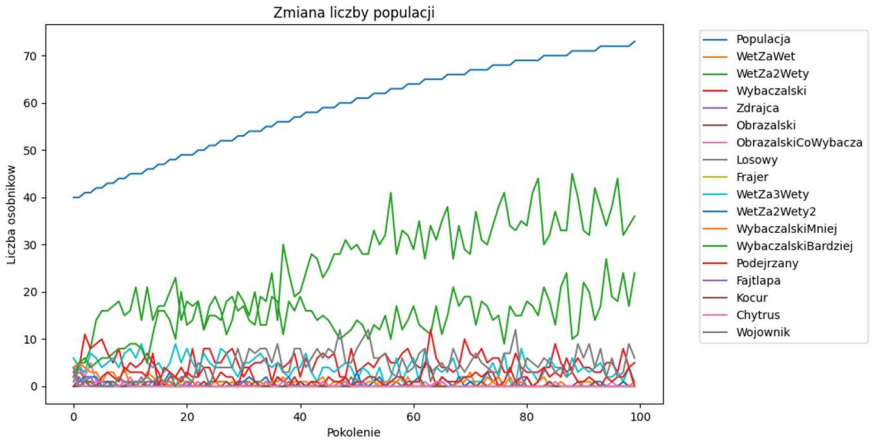
Przykładowe wykresy liczby osobników danej populacji w kolejnych pokoleniach prezentują się następująco:


Zmiana liczby populacji
Liczba osobnikow
Pokolenie
Populacja
WetZaWet
WetZa2Wety
Wybaczalski
Zdrajca
Obrazalski
ObrazalskiCoWybacza
Losowy
Frajer
WetZa3Wety
WetZa2Wety2
WybaczalskiMniej
WybaczalskiBardziej
Podejrzany
Fajtlapa
Kocur
Chytrus
Wojownik


Zmiana liczby populacji
Liczba osobnikow
Pokolenie
Populacja
WetZaWet
WetZa2Wety
Wybaczalski
Zdrajca
Obrazalski
ObrazalskiCoWybacza
Losowy
Frajer
WetZa3Wety
WetZa2Wety2
WybaczalskiMniej
WybaczalskiBardziej
Podejrzany
Fajtlapa
Kocur
Chytrus
Wojownik


Zmiana liczby populacji
Liczba osobnikow
Pokolenie
Populacja
WetZaWet
WetZa2Wety
Wybaczalski
Zdrajca
Obrazalski
ObrazalskiCoWybacza
Losowy
Frajer
WetZa3Wety
WetZa2Wety2
WybaczalskiMniej
WybaczalskiBardziej
Podejrzany
Fajtlapa
Kocur
Chytrus
Wojownik





W przeważającej liczbie przypadków zwyciężają osobniki oznaczeni kolorem zielonym. Jaka strategia była zwycięska? Był to WybaczalskiBardziej, który:

- jest miły (zaczyna od współpracy),
- nie daje się wykorzystywać (reaguje na zdradę przeciwnika),
- jest uczciwy (nie zdradza pierwszy),
- nie jest zazdrosny (nie dąży do wygrania, przeciwnik zyskuje więcej niż on sam),
- jest wybaczalski (czasem po prostu wybacza).

Matematyka pokazuje nam więc, że aby zyskać najwięcej z otaczającego nas świata, trzeba zachowywać się jak zwycięski genotyp. Trzeba być miłym, nie być zazdrosnym, być uczciwym ale nie dać się wykorzystywać i czasem powinno się wybaczać. Trzeba być po prostu dobrym człowiekiem.

Jak to się odnosi do świata?

Można zadać pytanie: czy matematyka rzeczywiście odpowiada na pytanie skąd wziął się altruizm w świecie zwierząt? Wydaje się, że tak. Skoro jest to najbardziej opłacalna strategia to nic dziwnego, że dobór naturalny sprawił, że strategia ta została przyjęta przez większość gatunków. W celu lepszego zilustrowania, posłużę się następującym argumentem.

Wielu ludzi zachwyca się wszechobecną złotą proporcją. Odpowiedź na pytanie, dlaczego złota proporcja występuje tak często w przyrodzie, może być prosta. Załóżmy, że mamy rośliny, które wypuszczają jeden liść dokładnie nad drugim. Następny liść zawsze będzie zasłaniał poprzedni, co powoduje, że proces fotosyntezy jest małoj wydajny. Jeśli w takiej grupie dojdzie do mutacji, która sprawi, że następny liść będzie obrócony o 90 stopni względem poprzedniego, proces fotosyntezy dla tej rośliny stanie się bardziej wydajny, co spowoduje przewagę nad innymi roślinami, które tej mutacji nie posiadają. Łatwo można zauważyć, że najlepszym rozwiązaniem będzie tu kąt niewymierny (nigdy idealnie nie zasłoni żadnego z poprzednich liści). Biorąc pod uwagę, że roślina, która najszybciej zakryje liśćmi największy procent przestrzeni, będzie jeszcze wydajniej pobierać energię ze słońca, okazuje się, że najlepszym rozwiązaniem w tej sytuacji jest, aby roślina obracała swoje liście o złoty kąt. Przez wiele lat powstawały liczne mutacje, a rośliny których rozkład liści coraz dokładniej przybliżał złotą proporcję, miały przewagę nad innymi, dzięki czemu złoty podział może być obecnie zaobserwowany w tak wielu sytuacjach.
Wydaje się, że analogicznie można uzasadnić fakt obserwacji zachowań altruistycznych w przyrodzie. Załóżmy, że w dalekich czasach istniała pewna populacja osobników w dużej mierze zdradliwych. Mutacje spowodowały pojawienie się kilku osobników o cechach podobnych do strategii Wybaczalski. W pojedynkę taki osobnik mógł zdziałać nie zbyt wiele, ale kilku takich osobników mogło łączyć się w grupy i produkować więcej dóbr, niż grupy konkurencyjne, które się wzajemnie zwalczały, a wewnętrznie nie mogły dogadać. W momencie, gdy reprezentacja osób wybaczalskich w populacji osiągnęła pewien poziom, społeczeństwo mogło rozwijać się tak, jak pokazują wyniki z wcześniejszej części artykułu. Po prostu dobór naturalny preferował geny tych osób. Po wielu latach interpretujemy wyniki ewolucji jako zachowania altruistyczne.
Przedstawione przemyślenia mogą być błędne, jednak wydaje się, że stanowią pewną podstawę by uważać, że iterowany dylemat więźnia jak najbardziej odnosi się do otaczającego nas świata i rzeczywiście odpowiada na pytanie, skąd się wziął altruizm w przyrodzie.

Przemyślenia

Jeśli zachowania altruistyczne są wynikiem tego, co dyktują nam geny, można zadać pytanie: czy człowiek jest zdolny do czegoś, co nazwalibyśmy prawdziwym altruizmem, do czegoś więcej niż tylko to, co każą nam czynić nasze geny?

Literatura

[1] Oren Harman, The Price of Altruism. George Price and the Search for the Origins of Kindness, Copernicus Center Press, 2017
[2] Robert Axelrod, The Evolution of Cooperation, Basic Books, Inc., Publishers, 1984

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

JAK DOBRZE ZAPAKOWAĆ PLECAK?

Patryk NITKOWSKI

Uniwersytet Jagielloński w Krakowie

Wstęp

Kryptografia jest dziedziną matematyki zajmującą się zabezpieczaniem informacji oraz komunikacji za pomocą kodowania, tak aby tylko uprawnione osoby mogły odczytać zakodowaną wiadomość.

Po odkryciu jednego z najpopularniejszych i obecnie najczęściej wykorzystywanych kryptosystemów asymetrycznych RSA, Ralph Merkle wraz z Martinem Hellmanem zaproponowali szyfr plecakowy. Został on zbudowany na bazie tzw. problemu plecakowego. W artykule zostanie sformułowany problem plecakowy oraz przedstawione łatwy i trudny szyfr plecakowy. Ponadto, zostanie sformułowana hipoteza $P = NP$.

Zdefiniowanie problemu

Problem plecakowy. *Rozważmy 'plecak' o objętości S oraz n 'przedmiotów', których objętości wynoszą $a_1, ..., a_n$. Czy istnieją liczby $x_i \in \{0, 1\},\ i = 1, ..., n$ takie, że zachodzi równość*

$$\sum_{i=1}^{n} x_i a_i = S?$$

Łatwo zauważyć, że są trzy możliwości.

1. Problem posiada dokładnie 1 rozwiązanie
   np. dla $n = 3,\ S = 6,\ a_1 = 1,\ a_2 = 2,\ a_3 = 3$, bo $a_1 + a_2 + a_3 = S$.
2. Problem posiada więcej niż jedno rozwiązanie
   np. dla $n = 4,\ S = 7,\ a_1 = 1,\ a_2 = 2,\ a_3 = 5,\ a_4 = 6$, bo $a_1 + a_4 = S = a_2 + a_3$.
3. Problem nie posiada rozwiązania
   np. dla $n = 2,\ S = 10,\ a_1 = 3,\ a_2 = 8$, bo $a_1 \neq S \neq a_2$ i $a_1 + a_2 \neq S$.

Szyfr plecakowy

Wykorzystując teraz problem plecakowy, zostanie zbudowany szyfr plecakowy.

Definicja 1 (Ciąg superrosnący)**.** *Ciąg liczbowy* $(a_i)_{i\leq n}$ *nazywamy superrosnącym, gdy*

$$\forall j \in \{2, ..., n\} \quad \sum_{i=1}^{j-1} a_i < a_j.$$

Szyfr łatwy

Szyfrowanie

Na początku zostanie zbudowany łatwy szyfr plecakowy. Do szyfrowania potrzebne są:

1. wiadomość $x = (x_1, ..., x_r),\ r \in \mathbb{N}$ składająca się z ciągu zer i jedynek (mogą one na przykład oznaczać litery utożsamione z liczbami zapisanymi w systemie binarnym),
2. ciąg superrosnący $(a_i)_{i\leq n}$ o wyrazach naturalnych.

Szyfrowanie wiadomości $x = (x_1, ..., x_r)$ odbywa się poprzez podzielenie jej na k bloków $x_j,\ j \in \{1, ..., k\}$ długości n (jeżeli n nie jest dzielnikiem r uzupełnia się ostatni blok odpowiednią liczbą jedynek na końcu). Wykorzystując ciąg (a_i) przekształcony zostaje każdy z bloków x_j, otrzymując układ sum

$$S_j = \sum_{i=1}^{n} x_{j,i} a_i.$$

Otrzymany układ sum jest zaszyfrowaną wiadomością.
Poniższy przykład ilustruje działanie opisanego szyfru.

Przykład 2. *Ustalmy ciąg superrosnący* $(a_1, a_2, a_3, a_4) = (5, 7, 29, 49)$. *Celem jest zaszyfrowanie wiadomości* $x = (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$. *Na początku dzielimy wiadomość na bloki długości cztery, otrzymując:* $x_1 = (1, 0, 0, 1),\ x_2 = (1, 1, 0, 0),\ x_3 = (0, 1, 0, 0)$. *Budujemy teraz układ sum*

$$S_1 = \sum_{i=1}^{n} x_{1,i} a_i = 1 \cdot 5 + 7 \cdot 0 + 29 \cdot 0 + 49 \cdot 1 = 54,$$

$$S_2 = 5 + 7 = 12,$$

$$S_3 = 7.$$

Układ sum $(S_1, S_2, S_3) = (54, 12, 7)$ *jest zaszyfrowaną wiadomością.*

Deszyfracja

Dysponując ciągami $(a_i)_{i\leq n}$ oraz $(S_j)_{j\leq k}$, odszyfrowana zostanie wiadomość x. Celem będzie przedstawienie każdego z elementów ciągu (S_j) za pomocą sumy wyrazów ciągu (a_i).

Aby to zrobić trzeba porównać $S_j,\ j \in \{1, ..., k\}$ z ostatnim elementem ciągu (a_i) i odszyfrować wiadomość 'od końca', postępując następująco

$$x_n = \begin{cases} 1 & \text{gdy } S \geq a_n, \\ 0 & \text{gdy } S < a_n. \end{cases}$$

Jeżeli na ostatnim miejscu pojawi się jeden, wyznaczana jest różnica $S_j - a_n$ i dalej tak samo, jak wyżej. Jeżeli pojawi się zero, wyznaczany zostaje wyraz x_{n-1} tak samo, jak x_n. Zatem

$$x_j = \begin{cases} 1 & \text{gdy } S_j - \sum_{i=j+1}^{n} a_i x_i \geq a_j, \\ 0 & \text{w p. p.} \end{cases}$$

Ciąg x będący ciągiem zer i jedynek jest odszyfrowaną wiadomością.
Odszyfrowana zostanie wiadomość z przykładu 2, aby lepiej zrozumieć działanie algorytmu.

Przykład 3. *Mamy dany ciąg* $(a_1, a_2, a_3, a_4) = (5, 7, 29, 49)$ *oraz układ sum* $(S_1, S_2, S_3) = (54, 12, 7)$.
Odszyfrujmy na początku $S_1 = 54$.
Widzimy, że $54 > 49$, *więc na ostatnim miejscu będzie cyfra jeden. Wyznaczamy* $54 - 49 = 5$ *i widzimy, że na dwóch kolejnych miejscach od końca będą zera.* $a_1 = 5$, *więc mamy* $x_1 = (1, 0, 0, 1)$.
Skoro $S_2 = 12$, *to łatwo widać, że* $x_2 = (1, 1, 0, 0)$ *oraz* $S_3 = 7$, *więc* $x_3 = (0, 1, 0, 0)$.
Naszą odszyfrowaną wiadomością jest $x = (x_1, x_2, x_3) = (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$.

Ten rodzaj szyfru jest szyfrem łatwym, gdyż znając ciągi (a_i) i (S_j), bez problemu można odszyfrować zakodowaną wiadomość.

Szyfr trudny

Teraz przedstawiona zostanie trudna wersja szyfru.

Szyfrowanie

Do szyfrowania potrzeba:

1. wiadomości $x = (x_1, ...x_i)\ i \in \mathbb{N}$ składającej się z ciągu zer i jedynek,
2. ciągu superrosnącego $(a_i)_{i \leq n}$ o wyrazach naturalnych,
3. liczby $m > \sum_{i=1}^{n} a_i$ oraz $w \in \mathbb{N}$ takie, że $(w, m) = 1$ (poprzez (m, w) oznaczamy największy wspólny dzielnik liczb naturalnych m i w),
4. ciągu $(b_i)_{i \leq n}$, gdzie $b_i \equiv wa_i (\text{mod } m),\ i \in \{1, ..., n\}$.

Szyfrowanie przebiega podobnie, jak w szyfrze łatwym. Mając ciąg (a_i), wybiera się $m > \sum_{i=1}^{n} a_i$ oraz w takie, że $(w, m) = 1$. Wyznacza się ciąg (b_i) tak, jak został zdefiniowany w punkcie 4.

Wiadomość zostaje podzielona na bloki długości n oraz wyznacza się układ sum

$$S_j = \sum_{i=1}^{n} x_{j,i} b_i.$$

Przykład 4. *Weźmy ciąg superrosnący* $(a_i) = (17, 19, 44, 85, 172, 359)$ *i ustalmy* $m = 728$. *Oczywiście,* $728 = m > \sum_{i=1}^{n} a_i = 696$. *Dobieramy* $w = 17$. *Łatwo widać, że* $(m, w) = (2^3 \cdot 7 \cdot 13, 17) = 1$.
Będziemy chcieli zakodować wiadomość $x = (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$.
Wyznaczamy ciąg $(b_i) = 17(17, 19, 44, 85, 172, 359) (\text{mod } 728)$.
Otrzymujemy $(b_i) = (289, 323, 20, 717, 12, 279)$. *Dzielimy wiadomość na bloki długości* 6 *i otrzymujemy* $x_1 = (0, 0, 1, 1, 0, 1)$ *i* $x_2 = (0, 1, 0, 1, 0, 0)$.
Wyznaczamy teraz S_1 *i* S_2

$$S_1 = 20 + 717 + 279 = 1016,$$

$$S_2 = 323 + 717 = 1040.$$

Otrzymany ciąg $(S_1, S_2) = (1016, 1040)$ *jest zaszyfrowaną wiadomością.*

Deszyfracja

Aby odszyfrować wiadomość x zaszyfrowaną trudną wersją szyfru, mając ciągi (b_i), (S_j) oraz liczby m i w, trzeba znaleźć rozwiązanie kongruencji $wx \equiv 1 (\text{mod } m)$ (istnieje dokładnie jedno rozwiązanie, bo $(m, w) = 1$). Dalej mnoży się $S_j \cdot w^{-1} (\text{mod } m)$ i dostaje

$$w^{-1} S_j \equiv \sum_{i=1}^{n} (w^{-1} b_i) x_i \equiv \sum_{i=1}^{n} a_i x_i (\text{mod } m).$$

Skoro $m > \sum_{i=1}^{n} a_i$ i (a_i) jest superrosnący, to

$$w^{-1} (\text{mod } m) S_j = \sum_{i=1}^{n} a_i x_i.$$

Dalej postępowanie jest takie, jak w łatwej wersji szyfru.

Odszyfrowana zostanie teraz wiadomość zakodowana w przykładzie 4.

Przykład 5. *Dane są: ciąg* $(S_1, S_2) = (1016, 1040)$, *liczby* $m = 728$ *i* $w = 17$ *oraz ciąg* $(b_i) = (289, 323, 20, 717, 12, 279)$. *Najpierw wyznaczymy ciąg* (a_i).
Wyznaczamy $17^{-1} (\text{mod } 728) = 257$. *Wykonujemy mnożenie*

$$257(289, 323, 20, 717, 12, 279) (\text{mod } 728) = (17, 19, 44, 85, 172, 359) = (a_i).$$

Wyznaczamy teraz

$$257 \cdot S_1 (\text{mod } 728) = 257 \cdot 1016 (\text{mod } 728) = 488$$

oraz

$$257 \cdot S_2 (\text{mod } 728) = 257 \cdot 1040 (\text{mod } 728) = 104.$$

Łatwo widać, że

$$488 = 359 + 85 + 44 \text{ i } 104 = 85 + 19.$$

Zatem mamy $x_1 = (0, 0, 1, 1, 0, 1)$ *oraz* $x_2 = (0, 1, 0, 1, 0, 0)$. *Naszą odszyfrowaną wiadomością jest więc ciąg* $x = (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$.

P=NP

Na początku sformułowanych zostanie kilka definicji.

Definicja 6 (Notacja **O**)**.** *Niech* $f, g : \mathbb{R} \to \mathbb{R}$*. Jeżeli*

$$\exists x_0 > 0, c > 0 \; \forall x \geq x_0 \; f(x) \leq cg(x),$$

to zapisujemy $f(x) = \mathbf{O}(g(x))$.

Definicja 7. *Mówimy, że problem da się rozwiązać w czasie wielomianowym, jeżeli jego rozwiązanie ma złożoność* $\mathbf{O}(n^k),\ k \in \mathbb{N}$.

Definicja 8 (Problem klasy P)**.** *Mówimy, że problem jest klasy* P*, jeżeli da się go rozwiązać w czasie wielomianowym.*

Definicja 9 (Problem klasy NP)**.** *Mówimy, że problem jest klasy* NP*, jeżeli jego rozwiązanie da się zweryfikować w czasie wielomianowym.*

Definicja 10. *Problem, który można rozwiązać w czasie wielomianowym nazywamy łatwym (wydajnym). W przeciwnym przypadku mówimy, że problem jest trudny.*

Definicja 11. *Mówimy, że problem* S_1 *nie jest trudniejszy od problemu* S_2*, jeżeli istnieje algorytm rozwiązujący problem* S_2*, którego rozszerzenie o algorytm wydajny rozwiązuje problem* S_1.

Definicja 12 (Problem NP-zupełny)**.** *Problem* $S \in NP$ *nazywamy* NP*-zupełnym, jeżeli wszystkie problemy* $T \in NP$ *nie są trudniejsze, niż* S.

Łatwo da się udowodnić, że problem plecakowy należy do problemów klasy NP, a nawet:

Twierdzenie 13. *Problem plecakowy jest problemem* NP*-zupełnym.*

Dowód powyższego twierdzenia można znaleźć w [1].

Wiadomo, że jest związek pomiędzy problemami klasy P oraz NP.

Lemat 14. *Zachodzi związek*

$$P \subset NP.$$

Stephen Cook w 1971 roku zadał naturalne pytanie dotyczące tych klas, a mianowicie: Czy klasa problemów P to to samo co klasa problemów NP?

Do dzisiaj, niestety, nie znamy na nie odpowiedzi, ale wiele osób przypuszcza, że nie jest to prawda.

Co więcej, jest to jeden z siedmiu problemów milenijnych ogłoszonych przez Instytut Matematyczny Claya w 2000 roku, za których rozwiązanie przysługuje nagroda w wysokości $1\ 000\ 000\$$.

Hipoteza 15. *Zachodzi związek*

$$NP \subset P \text{ (równoważnie } P = NP).$$

Można również łatwo zauważyć, że jest związek pomiędzy problemem plecakowym, a hipotezą 15 i można ją sformułować alternatywnie wykorzystując problem plecakowy.

Hipoteza 16. *Problem plecakowy należy do klasy problemów* P.

Reasumując, rozwiązanie problemu plecakowego da się zweryfikować w czasie wielomianowym, a nawet jest on problemem NP-zupełnym. Pytanie, czy da się go rozwiązać w czasie wielomianowym, wciąż pozostaje otwarte, a jego rozwiązanie miałoby ogromne znaczenie w dalszym rozwoju obecnej matematyki i informatyki.

Bibliografia

[1] Hans Kellerer, Ulrich Pferschy i David Pisinger. *Knapsack Problem*. Berlin Heidelberg New York: Springer-Verlag, 2004.

Konferencja Zastosowań
Matematyki MathUp
edycja 6.

JAK WYTRENOWAĆ WŁASNĄ SZTUCZNĄ INTELIGENCJĘ

Wiktor BARAŃCZYK[1]

[1] Politechnika Łódzka, Łódź

Wstęp

Sztuczna inteligencja (SI) jest jednym z najgorętszych tematów dyskutowanych w społeczeństwie. Opracowanie ChataGPT, a dokładniej darmowe udostępnienie jego trzeciej wersji, lawinowo przyspieszyło rozmowy na temat zagrożeń i szans związanych ze sztuczną inteligencją. Dla wielu uczenie maszynowe jest nowym tematem, jednak już w 1950 Turing zaproponował, jak budować inteligentne maszyny i testować ich inteligencję [1]. Oczywiście, opracowywane wtedy algorytmy sztucznej inteligencji znacząco się różniły od tych, które znamy dzisiaj. Wiele sformułowanych teorii okazało się błędnych lub niedokładnych, jednak niektóre z algorytmów, które zostały opracowane w tamtych czasach, dopiero teraz możemy wykorzystać z pełną skutecznością.
Dzisiaj najpopularniejsze algorytmy sztucznej inteligencji opierają się na sieciach neuronowych, które były rewolucją w temacie SI, ponieważ to one pozwoliły między innymi na generowanie obrazów, rozpoznawanie obiektów czy opracowanie modeli językowych. Mimo że sieci neuronowe różnią się wielkością, trudnością operacji w nich zawartych czy problemami, które rozwiązują, to mają one jedną wspólną cechę – każda z nich musiała zostać wyuczona.

Perceptron

Perceptron jest matematyczną reprezentacją biologicznego neuronu. Główną częścią perceptronu są wagi, które pozwalają obliczyć ważoną sumę wartości wejściowych. Dzięki temu jest on w stanie rozwiązać zadanie klasyfikacji do jednej z dwóch klas oraz proste problemy regresyjne. Schemat perceptronu został przedstawiony na Rys. 1.

Rys. 1. Schemat perceptronu z jedną wagą.

Sposób działania perceptronu jest bardzo prosty. Wejścia, które na danej pozycji zawsze oznaczają to samo, są mnożone przez odpowiadające im wagi. Następnie wyniki mnożeń są sumowane i tym samym zostaje obliczone wyjście. Perceptron można przedstawić jako operację macierzową opisaną równaniem:

$$(1)\ [\boldsymbol{waga_1} \quad \boldsymbol{waga_2} \quad \dots \quad \boldsymbol{waga_i}] * \begin{bmatrix} \boldsymbol{wejście_1} \\ \boldsymbol{wejście_2} \\ \dots \\ \boldsymbol{wejście_i} \end{bmatrix} = \boldsymbol{wyjście}$$

W celu lepszego wyjaśnienia konceptu perceptronu, zostanie przedstawiony praktyczny przykład jego użycia.

Wyobraźmy sobie, że jesteśmy studentami. Od kolegi dostaliśmy perceptron, który ma obliczyć na bazie czasu spędzonego na nauce w godzinach, oceny z laboratorium oraz frekwencji na laboratorium, jaką ocenę otrzymamy. Zakładamy, że:

- wejście 1 to czas spędzony na nauce w godzinach,
- wejście 2 to ocena z laboratorium,
- wejście 3 to frekwencja studenta na laboratorium,
- wyjście to szansa na zdanie egzaminu,
- waga 1 wynosi 0.1,
- waga 2 wynosi 0.02,
- waga 3 wynosi 0.01.

W planach mamy uczyć się 8 godzin, z laboratorium otrzymaliśmy ocenę 4.5, a nasza frekwencja wynosiła 90%.

$$(2)\ [0.1 \quad 0.02 \quad 0.01] * \begin{bmatrix} 8 \\ 4.5 \\ 0.9 \end{bmatrix} = 0.899$$

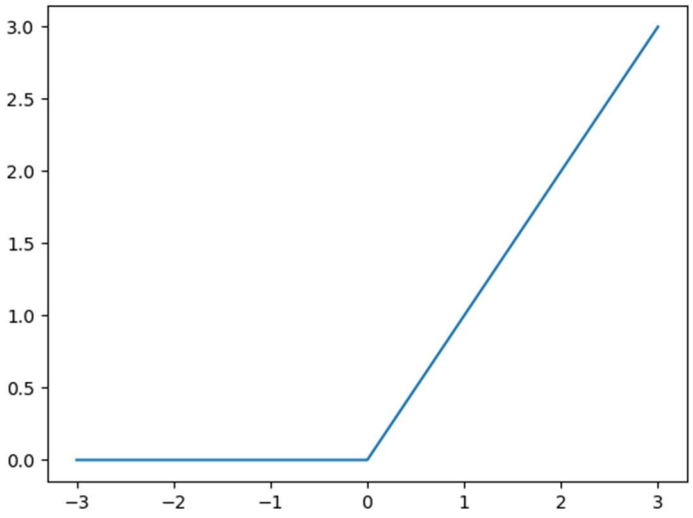
Zgodnie z wyliczeniami przedstawionymi powyżej, szansa na zdanie wynosi 0.899.
Perceptrony mają jednak bardzo duże ograniczenie. Są w stanie rozwiązać jedynie problemy liniowe. Liczba użytych warstw nie ma na to żadnego wpływu, ponieważ wiele warstw perceptronowych i tak może zostać zaprezentowana przez tylko jedną warstwę. Spowodowane jest to łącznością mnożenia macierzy, dlatego najpierw przemnożyć wagi wszystkich warstw ze sobą, zostawiając tylko jedną skumulowaną warstwę. Ogranicza to mocno pulę zadań, które można rozwiązać przy pomocy takiej sieci ze względu na to, że problemy w rzeczywistym świecie są zwykle nieliniowe [2].

Funkcja aktywacji

W celu wyeliminowania ograniczenia sieci co do problemów, które może rozwiązać, zaczęto wykorzystywać funkcje aktywacji. Przekształcają one wyjścia perceptronu zgodnie z wybraną funkcją. Głównym celem funkcji jest wprowadzenie nieliniowości do sieci neuronowych. Dzięki temu perceptrony są w stanie rozwiązywać problemy nieliniowe, a wiele warstw już nie może być skumulowana do tylko jednej warstwy [3]. Najpopularniejszą funkcją aktywacji jest rektyfikowana liniowa funkcja aktywacji (ReLU). Przekształca ona wartości zgodnie ze wzorem (3):

$$(3)\ wartość = \max(0, wartość)$$

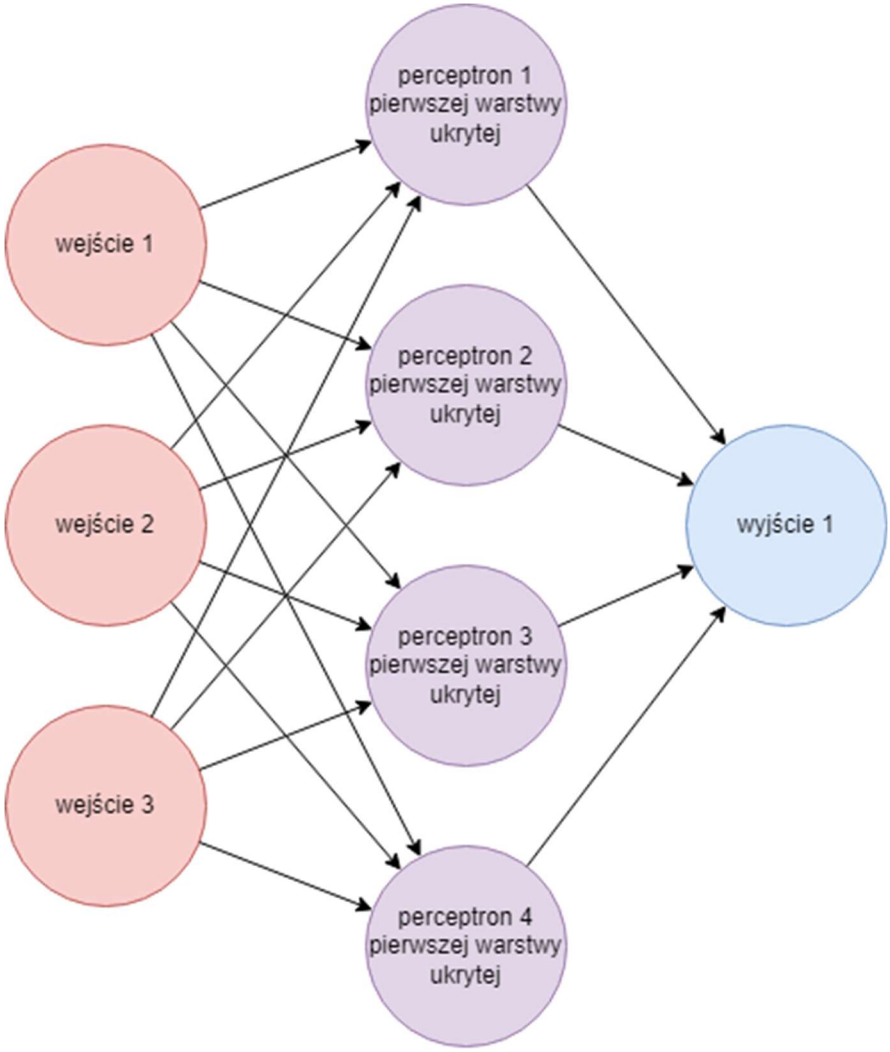
Na Rys. 2 przedstawiono, jak zmienia się przebieg wartości wyjściowych. Aktualnie coraz częściej inne funkcje aktywacji wypierają ReLU, jednak zwykle są one przekształceniem tej funkcji [4, 5].



Rys. 2. Przebieg wartości dla funkcji ReLU.

Wielowarstwowe sieci perceptronowe

Wraz z pojawieniem się funkcji aktywacji zaczęły być opracowywane wielowarstwowe sieci perceptronowe, które są w stanie rozwiązywać bardziej skomplikowane problemy. Składają się one z warstwy wejściowej, minimum jednej warstwy ukrytej oraz warstwy wyjściowej. Po każdej warstwie wartości są przekształcane zgodnie z funkcją aktywacji. Schemat wielowarstwowej sieci perceptronowej został przedstawiony na Rys. 3.



Rys. 3. Schemat wielowarstwowej sieci perceptronowej.

Działanie wielowarstwowej sieci perceptronowej nie różni się znacząco od perceptronów, gdyż każda warstwa posiada wartości wejściowe, wagi i wartości wyjściowe. Największą różnicą jest to, że może istnieć więcej niż jedno wyjście i to nie tylko w warstwie wejściowej czy ukrytej, ale również w warstwie wyjściowej.
Warstwy dalej mogą być prezentowane przez macierze, jednak w odróżnieniu od równania (1), czasami macierz wag ma więcej niż jedną kolumnę, ponieważ może być więcej niż jedno wyjście [6].

$$(4)\quad \begin{bmatrix} waga_{11} & waga_{12} & \dots & waga_{1i} \\ waga_{21} & waga_{22} & \dots & waga_{2i} \\ \dots & \dots & \dots & \dots \\ waga_{j1} & waga_{j2} & \dots & waga_{ji} \end{bmatrix} * \begin{bmatrix} wejście_1 \\ wejście_2 \\ \dots \\ wejście_i \end{bmatrix} = \begin{bmatrix} wyjście_1 \\ wyjście_2 \\ \dots \\ wyjście_j \end{bmatrix}$$

W celu lepszego zrozumienia działania wielowarstwowej sieci perceptronowej zostanie przedstawiony praktyczny przykład.

Zakładamy, że:
- wejście 1 to czas spędzony na nauce,
- wejście 2 to ocena z laboratorium,
- wejście 3 to frekwencja studenta na laboratorium,
- wyjście to szansa na zdanie egzaminu,
- wielowarstwowa sieć perceptronowa posiada dwie warstwy.

Macierze reprezentujące kolejne warstwy są następujące:

$$(5)\ warstwa_1 = \begin{bmatrix} 0.01 & 0.02 & 0.002 \\ -0.2 & 0.03 & 0.001 \\ 0.001 & 0.01 & 0.01 \\ 0.004 & 0.001 & 0.001 \end{bmatrix}$$

$$(6)\ warstwa_2 = [0.8 \quad -0.5 \quad 0.6 \quad 0.2]$$

Szansa na zdanie egzaminu zostanie obliczona dla studenta, który uczył się 8 godzin, miał ocenę 4.5 z laboratorium, a jego frekwencja wynosiła 90%.
Na początku wartości wejściowe zostają przemnożone przez *warstwę*$_1$.

$$(7)\begin{bmatrix} 0.01 & 0.02 & 0.002 \\ -0.2 & 0.03 & 0.001 \\ 0.001 & 0.01 & 0.01 \\ 0.004 & 0.001 & 0.001 \end{bmatrix} * \begin{bmatrix} 8 \\ 4.5 \\ 0.9 \end{bmatrix} = \begin{bmatrix} 0.1718 \\ -1.4641 \\ 0.062 \\ 0.0374 \end{bmatrix}$$

Wynik działania (7) wykorzystywany jest w kolejnej warstwie. W tym przypadku, obliczana jest wartość wyjściowa.

$$(8)[0.8 \quad -0.5 \quad 0.6 \quad 0.2] * \begin{bmatrix} 0.1718 \\ -1.4641 \\ 0.062 \\ 0.0374 \end{bmatrix} = 0.9142$$

Wynik dla tych samych parametrów wejściowych jest różni się w znacznym stopniu. Jest to spowodowane arbitralnym wybraniem wag, a nie ich prawidłowym wyznaczeniem przy pomocy algorytmów uczenia.
Wraz z pojawieniem się wielowarstwowych sieci perceptronowych powstał problem z interpretacją wag. W przypadku pojedynczej warstwy było widoczne, który parametr ma największy wpływ na wynik, ponieważ czym wyższa była waga dla danego wejścia, tym większe było znaczenie wejścia. Wraz ze wzrostem liczby warstw, interpretacja kolejnych wag jest coraz trudniejsza, dlatego też nazywamy te warstwy ukrytymi. Aktualnie istnieją algorytmy do interpretacji znaczenia wag w sieciach neuronowych, takie jak GradCAM, jednak działają one tylko dla stosunkowo prostych algorytmów [7].
Ustalenie wag perceptronów jest najtrudniejszym zadaniem związanym ze sztuczną inteligencją, gdyż od tego zależy skuteczność algorytmu. W celu dostosowania wag do tego, żeby były w stanie rozwiązywać wybrany problem, zostały opracowane odpowiednie algorytmy. Sam proces poszukiwania odpowiednich parametrów nazywany jest treningiem lub uczeniem sieci neutronowej. W dalszej części zostanie przedstawiony przykładowy proces uczenia.

Przygotowanie danych

Zanim dane zostaną wykorzystane do treningu, muszą one zostać odpowiednio przygotowane. Dane wejściowe często mogą mieć bardzo różne zakresy wartości. Za przykład weźmy dane do przewidywania oceny. Czas nauki może wynosić od zera do nawet kilkudziesięciu godzin, ocena z laboratorium to wartość między 2 a 5, a frekwencja na laboratorium będzie wartością z zakresu między 0 a 1 lub inaczej 0% a 100%. Takie różnice powodują, że cecha, która będzie miała wysokie wartości, może mieć duży wpływ na wynik, nawet jeśli tak naprawdę nie jest znacząca. Dodatkowo, w treningu powoduje to dużą niestabilność wag, co utrudnia wytrenowanie algorytmu.
Rozwiązaniem tego problemu jest skalowanie wszystkich wartości wejściowych do tego samego zakresu. Najczęściej jest to między -1 a 1 lub między 0 a 1. Dzięki temu różnice między wartościami tej samej cechy zostają zachowane, a jednocześnie każda cecha ma wpływ na model zgodnie z jej realną przydatnością w rozwiązaniu problemu. Przykładem skalowania wartości jest normalizacja min-max, która skaluje wartości zgodnie ze wzorem:

$$(9)\quad \frac{wartość\ skalowana\ -\ wartość\ minmalna\ cechy}{wartość\ maksymalna\ cechy\ -\ wartość\ minimalna\ cechy} = wartość\ przeskalowana$$

W takiej formie normalizacja zapewnia, że wartości każdej cechy będą z zakresu między 0 a 1 [8].

Sposoby polepszenia procesu nauki

W procesie nauki wykorzystywane są różne hiperparametry oraz techniki zapewniające lepszy i stabilniejszy trening. Jednym z nich jest współczynnik uczenia. Wpływa on na szybkość aktualizowania wag, zwykle ją zmniejszając. Współczynnik nie może być ani zbyt duży, ani zbyt mały. W przypadku zbyt dużej wartości, wagi aktualizowane są zbyt szybko, przez co z łatwością mogą ominąć wartości, które zapewniają najlepsze rozwiązania. Zbyt mała wartość sprawi, że proces treningu znacznie się przedłuży lub nawet nie będzie przynosić żadnego efektu. Nie ma zasady, która zapewni dobry wynik dla trenowanej sieci. Zwykle wartość współczynnika jest między 0 a 1. W celu znalezienia optymalnej wartości testowane jest wiele różnych wartości i sprawdzane, która daje najlepszy wynik [9].
Inną techniką jest wykorzystywanie serii danych. Zamiast uczyć sieć na jednym przykładzie, wagi są aktualizowane na bazie uśrednionego błędu dla całego zestawu. W tym przypadku również testowane są różne rozmiary serii, jednak często maksymalna liczba przykładów w serii jest uzależniona od możliwości sprzętu, na którym uczona jest sieć. Głównym powodem wykorzystania serii danych jest zmniejszenie szansy na to, że sieć podczas treningu pomyli minimum lokalne z optymalnym rozwiązaniem [10].

Trening sieci neuronowych

Każda sieć neuronowa opiera swoje działania na wagach. To od ich odpowiednich wartości uzależniona jest skuteczność działania algorytmu. Proces ustalania odpowiednich wartości wag nazywamy treningiem. Trzema głównymi rodzajami treningu są:

- trening nadzorowany,
- trening nienadzorowany,
- uczenie ze wzmocnieniem.

Trening nadzorowany polega na tym, że zapewniamy sieci wartości wejściowe oraz oczekiwane dla nich kategorie (w przypadku klasyfikacji) czy (wartość w przypadku regresji). Algorytm sztucznej inteligencji szuka wzorców w przygotowanych danych, które pozwolą odpowiednio sklasyfikować czy przypisać wartość nowym, wcześniej nie spotkanym, przykładom. Nazywamy to generalizacją problemu.
W treningu nienadzorowanym zapewniamy tylko dane wejściowe, bez żadnych oczekiwanych odpowiedzi. Podczas treningu algorytm stara się znaleźć wzorce. Przykładem problemu, który rozwiązywany jest podczas takiego treningu jest klasteryzacja.
W uczeniu ze wzmocnieniem algorytm uczy się poprzez nagrody, które otrzymuje na podstawie interakcji ze środowiskiem. Przykładem tego są algorytmy, które uczą się grać w różne gry [11].
W dalszej części opisywany będzie trening nadzorowany sieci wielowarstwowej.

Przykład kroku w treningu sieci neuronowych

Załóżmy, że seria danych składa się z czterech próbek:

$$(10)\begin{bmatrix} 8 & 10 & 3 & 6 \\ 4.5 & 5 & 3 & 4 \\ 0.9 & 0.8 & 0.8 & 0.7 \end{bmatrix}$$

Wartości oczekiwane przykładów to:

$$(11)\ [1 \quad 1 \quad 0.2 \quad 0.5]$$

Sieć w tym przykładzie składa się z wag przedstawionych we wzorach (5) oraz (6). Po pierwszej warstwie zostanie wykorzystana funkcja aktywacji ReLU; po drugiej nie zostanie wykorzystana żadna funkcja aktywacji. Współczynnik uczenia będzie wynosić 0.1.
Najpierw wartości zostaną przeskalowane zgodnie z równaniem (9). Przykład dla pierwszej próbki z serii danych:

$$(12)\ \frac{8-3}{10-3} = \frac{5}{7} \approx 0.714;\ \frac{4.5-3}{5-3} = \frac{1.5}{2} = 0.75;\ \frac{0.9-0.7}{0.9-0.7} = \frac{0.2}{0.2} = 1$$

Seria danych po przeskalowaniu wszystkich wartości:

$$(13)\begin{bmatrix} 0.714 & 1 & 0 & 0.429 \\ 0.75 & 1 & 0 & 0.5 \\ 1 & 0.5 & 0.5 & 0.0 \end{bmatrix}$$

W tym przypadku wartości oczekiwane nie muszą być skalowane, ponieważ są to wartości między 0 a 1.
W przypadku treningu nadzorowanego, kolejne kroki treningu można podzielić na:

1. obliczenie wyjścia,
2. porównanie wyjścia z wartością oczekiwaną,
3. aktualizacja wag przy pomocy propagacji wstecznej.

Na początku zostaje obliczona wartość wyjściowa. Wartości zostaną zaokrąglone do czwartego miejsca po przecinku:

$$(14)\begin{bmatrix} 0.01 & 0.02 & 0.002 \\ -0.2 & 0.03 & 0.001 \\ 0.001 & 0.01 & 0.01 \\ 0.004 & 0.001 & 0.001 \end{bmatrix} * \begin{bmatrix} 0.714 & 1 & 0 & 0.429 \\ 0.75 & 1 & 0 & 0.5 \\ 1 & 0.5 & 0.5 & 0.0 \end{bmatrix} = \begin{bmatrix} 0.0241 & 0.031 & 0.001 & 0.0143 \\ -0.1193 & -0.1695 & 0.0005 & -0.0708 \\ 0.0182 & 0.016 & 0.005 & 0.0054 \\ 0.0046 & 0.0055 & 0.0005 & 0.0022 \end{bmatrix}$$

$$(15)\ ReLU\left(\begin{bmatrix} 0.0241 & 0.031 & 0.001 & 0.0143 \\ -0.1193 & -0.1695 & 0.0005 & -0.0708 \\ 0.0182 & 0.016 & 0.005 & 0.0054 \\ 0.0046 & 0.0055 & 0.0005 & 0.0022 \end{bmatrix}\right) = \begin{bmatrix} 0.0241 & 0.031 & 0.001 & 0.0143 \\ 0 & 0 & 0.0005 & 0 \\ 0.0182 & 0.016 & 0.005 & 0.0054 \\ 0.0046 & 0.0055 & 0.0005 & 0.0022 \end{bmatrix}$$

$$(16)\ [0.8 \quad -0.5 \quad 0.6 \quad 0.2] * \begin{bmatrix} 0.0241 & 0.031 & 0.001 & 0.0143 \\ 0 & 0 & 0.0005 & 0 \\ 0.0182 & 0.016 & 0.005 & 0.0054 \\ 0.0046 & 0.0055 & 0.0005 & 0.0022 \end{bmatrix}$$

$$= [0.0311 \quad 0.0355 \quad 0.0036 \quad 0.0151]$$

W celu zrozumienia, na ile odpowiedzi są bliskie oczekiwanym, obliczany jest błąd zgodnie ze wzorem:

$$(17)\ błąd = średnia\big(wartość\_bezwzględna(wynik\ przewidywany\ -\ wynik\ oczekiwany)\big)$$

Błąd dla aktualnych wag wynosi:

$$(18)\ avg(abs([0.0311 \quad 0.0355 \quad 0.0036 \quad 0.0151] - [1 \quad 1 \quad 0.2 \quad 0.5])) = 0.6537$$

Błąd jednak nie daje informacji, w którą stronę zaktualizować wagi. W ramach tego trzeba obliczyć pochodną błędu, która obliczana jest zgodnie ze wzorem:

$$(19)\ delta = (wynik\ przewidywany\ -\ wynik\ oczekiwany)$$

Takie określenie błędu wskazuje nam kierunek, w którym mają zostać zaktualizowane wagi. Jednak przez wzgląd na to, że wykorzystywana jest seria danych, delta musi zostać podzielona przez jej liczność serii. Brak podzielenia sprawiłby, że proces uczenia kończyłby się takim samym wynikiem, jakby próbki byłyby przedstawiane sieci pojedynczo. Wzór ostatecznie ma postać:

$$(20)\ delta = \frac{wynik\ przewidywany\ -\ wynik\ oczekiwany}{rozmiar\ serii}$$

Tym samym równanie (20) zapewnia większą generalizację delty.
Delta dla tego przypadku wyniesie:

$$(21)\ \frac{[0.0311 \quad 0.0355 \quad 0.0036 \quad 0.0151] - [1 \quad 1 \quad 0.2 \quad 0.5]}{4}$$

$$= [-0.2422 \quad -0.2411 \quad -0.0491 \quad -0.1212]$$

Następnie można obliczyć deltę dla warstwy ukrytej. Nie istnieje sposób, żeby zrobić to bezpośrednio, ponieważ nie ma sposobu na zapewnienie oczekiwanych odpowiedzi dla warstwy ukrytej. Z tego powodu robi się to poprzez przemnożenie wag ostatniej warstwy przez deltę, zgodnie ze wzorem:

$$(22)\ delta\ warstwy\ ukrytej = warstwa_2^T * delta$$

Zgodnie ze wzorem delta będzie wynosić:

$$(23)\begin{bmatrix}0.8\\-0.5\\0.6\\0.2\end{bmatrix} * [-0.2422 \quad -0.2411 \quad -0.0491 \quad -0.1212]$$

$$= \begin{bmatrix}-0.1938 & -0.1929 & -0.0393 & -0.097\\ 0.1211 & 0.1206 & 0.0246 & 0.0606\\ -0.1453 & -0.1447 & -0.0295 & -0.0727\\ -0.0484 & -0.0482 & -0.0098 & -0.0242\end{bmatrix}$$

Część wartości została wyzerowana przez wzgląd na funkcję aktywacji ReLU. Dla odpowiadających wartości delty muszą również zostać wyzerowane, korzystając z pochodnej funkcji aktywacji.

Pochodna ma wartość 0 dla wartości nie większych niż 0 i 1 dla większych od zera. Delta warstwy ukrytej ma postać:

$$(24)\ delta\_warstwy\_ukrytej =$$

$$\begin{bmatrix}-0.1938 & -0.1929 & -0.0393 & -0.097\\ 0.1211 & 0.1206 & 0.0246 & 0.0606\\ -0.1453 & -0.1447 & -0.0295 & -0.0727\\ -0.0484 & -0.0482 & -0.0098 & -0.0242\end{bmatrix} \circ ReLU\left(\begin{bmatrix}0.0241 & 0.031 & 0.001 & 0.0143\\ -0.1193 & -0.1695 & 0.0005 & -0.0708\\ 0.0182 & 0.016 & 0.005 & 0.0054\\ 0.0046 & 0.0055 & 0.0005 & 0.0022\end{bmatrix}\right)' =$$

$$\begin{bmatrix}-0.1938 & -0.1929 & -0.0393 & -0.097\\ 0.1211 & 0.1206 & 0.0246 & 0.0606\\ -0.1453 & -0.1447 & -0.0295 & -0.0727\\ -0.0484 & -0.0482 & -0.0098 & -0.0242\end{bmatrix} \circ \begin{bmatrix}1 & 1 & 1 & 1\\ 0 & 0 & 1 & 0\\ 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\end{bmatrix} =$$

$$\begin{bmatrix}-0.1938 & -0.1929 & -0.0393 & -0.097\\ 0 & 0 & 0.0246 & 0\\ -0.1453 & -0.1447 & -0.0295 & -0.0727\\ -0.0484 & -0.0482 & -0.0098 & -0.0242\end{bmatrix}$$

Następnie musi zostać obliczona delta ważona, ponieważ wartości wejściowe również mają wpływ na błąd. Deltę ważoną oblicza się zgodnie ze wzorem:

$$(25)\ delta\ ważona = \ delta\ *\ wartości\ wejściowe\ do\ warstwy^T$$

Wagi ważone dla warstw w tym przykładzie wynoszą odpowiednio:

- dla pierwszej warstwy,

$$(26)\ [-0.2422 \quad -0.2411 \quad -0.0491 \quad -0.1212] * \begin{bmatrix}0.0241 & 0.0 & 0.0182 & 0.0046\\ 0.031 & 0.0 & 0.016 & 0.0055\\ 0.001 & 0.0005 & 0.005 & 0.0005\\ 0.0143 & 0.0 & 0.0054 & 0.0022\end{bmatrix}$$

$$= [-0.0151 \quad 0.0 \quad -0.0092 \quad -0.0027]$$

- dla warstwy ukrytej.

$$(27)\ \begin{bmatrix} -0.1938 & -0.1929 & -0.0393 & -0.097 \\ 0 & 0 & 0.0246 & 0 \\ -0.1453 & -0.1447 & -0.0295 & -0.0727 \\ -0.0484 & -0.0482 & -0.0098 & -0.0242 \end{bmatrix} * \begin{bmatrix} 0.714 & 0.75 & 1.0 \\ 1.0 & 1.0 & 0.5 \\ 0.0 & 0.0 & 0.5 \\ 0.429 & 0.5 & 0.0 \end{bmatrix}$$

$$= \begin{bmatrix} -0.3729 & -0.3868 & -0.3099 \\ 0 & 0 & 0.0123 \\ -0.2796 & -0.29 & -0.2324 \\ -0.0931 & -0.0966 & -0.0774 \end{bmatrix}$$

Znając wartości delt ważonych, można zaktualizować wagi zgodnie ze wzorem:

$$(28)\ zaktualizowane\ wagi = wagi - współczynnik\ uczenia * delta\ ważona$$

Zaktualizowane wagi będą miały następujące wartości:

- dla pierwszej warstwy,

$$(29)\ [0.8 \quad -0.5 \quad 0.6 \quad 0.2] - 0.1 * [-0.0151 \quad 0.0 \quad -0.0092 \quad -0.0027]$$

$$= [0.8015 \quad -0.5 \quad 0.6009 \quad 0.2003]$$

- dla warstwy ukrytej.

$$(30)\ \begin{bmatrix} 0.01 & 0.02 & 0.002 \\ -0.2 & 0.03 & 0.001 \\ 0.001 & 0.01 & 0.01 \\ 0.004 & 0.001 & 0.001 \end{bmatrix} - 0.1 * \begin{bmatrix} -0.3729 & -0.3868 & -0.3099 \\ 0 & 0 & 0.0123 \\ -0.2796 & -0.29 & -0.2324 \\ -0.0931 & -0.0966 & -0.0774 \end{bmatrix}$$

$$= \begin{bmatrix} 0.0473 & 0.0587 & 0.033 \\ -0.2 & 0.03 & -0.00023 \\ 0.029 & 0.039 & 0.0332 \\ 0.0133 & 0.0107 & 0.0087 \end{bmatrix}$$

Wyniki dla zaktualizowanych wag wynoszą 0.8015, -0.5, 0.6009, 0.2003, a błąd zmalał do 0.579, czyli o około 11%. W celu odpowiedniego wytrenowania modelu musiałoby się odbyć wiele aktualizacji wag, jednak są one analogiczne, jak przedstawiony powyżej proces [12].

Podsumowanie

W artykule została przedstawiona budowa wielowarstwowych sieci perceptronowych, która jest częścią wielu najnowocześniejszych architektur sieci neuronowych. Wyjaśniony został proces treningu prostej sieci, który nie różni się od aktualizacji wag w bardziej rozbudowanych i zaawansowanych sieciach neuronowych. Praktyczne przykłady służą ilustracji przedstawionych koncepcji i wzorów.

Literatura

[1] Rockwell, A. (2017, August 10). The History of Artificial Intelligence. Harvard, Science in the News. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

[2] Clabaugh, C., Myszewski, D. i Pang, J. (n.d.). The perceptron. Stanford, Neural Networks. https://cs.stanford.edu/people/eroberts/courses/soco/projects/neural-networks/Neuron/index.html

[3] Grosse, R. (2019). Lecture 3: Multilayer Perceptrons. Department of Computer Science, University of Toronto. https://www.cs.toronto.edu/~rgrosse/courses/csc421_2019/readings/L03%20Multilayer%20Perceptrons.pdf

[4] Olamendy, C J. (2023, December 4). Understanding ReLU, LeakyReLU, and PReLU: A Comprehensive Guide. Medium. https://medium.com/@juanc.olamendy/understanding-relu-leakyrelu-and-prelu-a-comprehensive-guide-20f2775d3d64

[5] Li, F., Karpathy, A. & Johnson, J. (2016). Lecture 5: Training Neural Networks, Part I. Stanford. https://cs231n.stanford.edu/slides/2016/winter1516_lecture5.pdf

[6] Hellwig, D. (2019, January 31). Mathematical Representation of a Perceptron Layer (with example in TensorFlow). Medium. https://medium.com/@daniel.hellwig.p/mathematical-representation-of-a-perceptron-layer-with-example-in-tensorflow-754a38833b44

[7] IBM (n.d.) What is explainable AI? https://www.ibm.com/topics/explainable-ai

[8] Brownlee, J. (2020, August 28). How to Use StandardScaler and MinMaxScaler Transforms in Python. Machine Learning Mastery. https://machinelearningmastery.com/standardscaler-and-minmaxscaler-transforms-in-python/

[9] Brownlee, J. (2020, September 12). Understand the Impact of Learning Rate on Neural Network Performance. Machine Learning Mastery. https://machinelearningmastery.com/understand-the-dynamics-of-learning-rate-on-deep-learning-neural-networks/

[10] Barreto, S. (2024, Mach 18). Why Mini-Batch Size Is Better Than One Single “Batch” With All Training Data. Baeldung. https://www.baeldung.com/cs/mini-batch-vs-single-batch-training-data

[11] Salian, I. (2018, August 2). SuperVize Me: What’s the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning? Nvidia. https://blogs.nvidia.com/blog/supervised-unsupervised-learning/

[12] Trask, A. W. (2019) grooking Deep Learning (1st ed.). Manning Publications Co.

MathUp

Konferencja Zastosowań Matematyki

Pod redakcją: dr inż. Gertruda Gwóźdź-Łukawska, dr Monika Potyrała
Recenzja naukowa: dr inż. Gertruda Gwóźdź-Łukawska, dr Monika Potyrała
Skład i edycja: dr hab. inż. Ewa Korzeniewska, prof. uczelni

Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki
Centrum Nauczania Matematyki i Fizyki
Politechnika Łódzka 2024

ISBN 978-83-938538-4-7