POLITECHNIKA LUBELSKA

MONOGRAFIE

KWATERNION 2

Prace studentów WPT kierunku matematyka

redakcja

Anna Kuczmaszewska

Lublin 2021

Kwaternion 2

Prace studentów WPT kierunku matematyka

Monografie – Politechnika Lubelska

Politechnika Lubelska
Wydział Podstaw Techniki
ul. Nadbystrzycka 38
20-618 LUBLIN

Kwaternion 2

Prace studentów WPT kierunku matematyka

redakcja:
Anna Kuczmaszewska

Wydawnictwo Politechniki Lubelskiej
Lublin 2021

Recenzenci:
prof. dr hab. Witold Rzymowski, Politechnika Lubelska
dr hab. Adam Stachura, Politechnika Lubelska

Publikacja wydana za zgodą Rektora Politechniki Lubelskiej

ISBN: 978-83-7947-457-8

Wydawca: Wydawnictwo Politechniki Lubelskiej
www.biblioteka.pollub.pl/wydawnictwa
ul. Nadbystrzycka 36C, 20-618 Lublin
tel. (81) 538-46-59

Druk: DjaF – 30-092 Kraków, ul. Kmietowicza 1/1
www.djaf.pl

Nakład: 75 egz.

Spis treści

Przedmowa 7

Magdalena Blacha. Wybrane modele grafów losowych 9

Paulina Dębicka. Sposoby obliczania NWD i NWW 31

Dagmara Dudek. Hipergrafy w modelowaniu 47

Marcin Dziadosz, Matylda Jankowska. Liczby przestępne 63

Alicja Hołowiecka. Enigma (nie) do złamania 73

Magdalena Majewska. Co wpływa na wysokość składki netto
w ubezpieczeniach komunikacyjnych? 101

Aleksandra Pawłowska, Izabela Szady. Złota liczba 122

Emilia Popławska, Monika Sowa. Niezwykłe zero i jeden 135

Przedmowa

KWATERNION – tak studenci kierunku matematyka na Wydziale Podstaw Techniki Politechniki Lubelskiej nazwali swoje koło naukowe.

Kwaternion to najprościej mówiąc taka „czterowymiarowa liczba". Kwaterniony zostały wprowadzone przez Williama Hamiltona w 1843 roku jako narzędzie do opisu ruchów sztywnych w przestrzeni trójwymiarowej. Współczesna matematyka traktuje kwaterniony jako czterowymiarową, unormowaną algebrę z dzieleniem nad liczbami rzeczywistymi

W działalności koła KWATERNION też zaobserwujemy cztery obszary, możemy więc powiedzieć, że opisuje ją czterowymiarowy wektor, którego pierwsza składowa to działalność popularyzatorska, druga to zainteresowania naukowe, trzecia to zastosowania matematyki w życiu codziennym a czwarta to działalność edukacyjna oraz pogłębianie własnej wiedzy i umiejętności, z myślą o zawodowej przyszłości. Monografia dokładnie odzwierciedla tę czteroobszarową strukturę.

Monografia „*KWATERNION 2. Prace studentów WPT kierunku matematyka*" składa się z ośmiu różnorodnych tematycznie prac. Są tu prace o charakterze popularyzującym wiedzę matematyczną, prace popularnonaukowe i prace z obszaru zastosowań matematyki. Wszystkie spełniają warunek przynależności do czwartego obszaru działalności Koła, stanowią przyczynek do własnego rozwoju zwiększającego szanse na dostosowanie do zmieniającego się rynku pracy.

Różne też były inspiracje do powstania tych prac. Część z nich, dotycząca liczb, powstała w ramach przygotowań do święta liczby π pod hasłem „*Odczarować matematykę*", które niestety trzeba było odwołać, z powodu ogłoszonej pandemii. W ten sposób powstały prace o liczbach jeden i zero, o liczbach przestępnych i złotej liczbie.

Wydaje się, że o jedynce i zerze wiemy wszystko, bo są naszą codziennością. Jednak krótkie historyczne opisy powstawania tych pojęć, przykłady współczesnej ich użyteczności oraz takie ciekawe fakty jak brak umiejętności posługiwania się liczebnikami innymi niż jeden i dwa, które zawarte są w pracy „*Niezwykłe zero i jeden*", na pewno wydadzą się interesujące.

Liczba przestępna to nie jest pojęcie znane powszechnie, wymaga znajomości kilku faktów z algebry i teorii liczb. Praca „*Liczby przestępne*" prezentuje zbiór zagadnień związanych z liczbami przestępnymi, wybranych nie pod kątem systematycznego wykładu, ale zbioru podstawowych pojęć i historycznego rozwoju tego pojęcia wraz z przykładami różnych liczb przestępnych.

W pracy „*Złota liczba*" znajdziemy jej definicję i związki z ciągiem Fibonacciego oraz liczne przykłady obecności tej liczby w różnych dziedzinach naszego życia, w architekturze, w przyrodzie i innych.

Ciekawą jest też praca o Enigmie. Prezentuje ona historię działań podejmowanych w latach poprzedzających wybuch II Wojny Światowej i w jej trakcie, a zmierzających do złamania kodu używanych przez Niemców wojskowych maszyn szyfrujących „Enigma". Z pracy „*Enigma (nie) do złamania*" dowiadujemy się wiele o losach Enigmy, metodach szyfrowania i rozszyfrowywania tekstów z jej użyciem, oraz matematycznych metodach wykorzystywanych do tego celu. Za rekomendację niech posłuży fakt, że praca otrzymała trzecią nagrodę w Konkursie Polskiego Towarzystwa Matematycznego im. Witolda Wilkosza na najlepszą studencką pracę popularyzującą matematykę.

Najmniejsza wspólna wielokrotność, największy wspólny dzielnik liczb to pojęcia, które znamy ze szkoły i wydaje się, że nic więcej nie można już tutaj wymyślić. Praca „*Sposoby obliczania NWD i NWW*" dowodzi, że tak nie jest. Powstała w wyniku własnych spostrzeżeń autorki po zajęciach z teorii liczb.

Inspiracją do napisania prac o grafach i wysokości składki ubezpieczeniowej były prace dyplomowe na studiach pierwszego stopnia.

Hipergrafy są stosunkowo nowym narzędziem w modelowaniu, mimo to znajdują szerokie zastosowanie w wielu dziedzinach nauki, zarówno w naukach ścisłych, jak i humanistycznych. W pracy „*Hipergrafy w modelowaniu*" przedstawione zostały dwa zagadnienia – modelowanie wybranych cząsteczek chemicznych oraz tzw. sieci Petriego.

Druga praca z teorii grafów dotyczy wybranych aspektów teorii grafów losowych. Zaprezentowano w niej pewne idee związane z zastosowaniem tych grafów jako narzędzi do modelowania sieci złożonych, oraz przedstawiono dwa modele takich sieci. Praca „*Wybrane modele grafów losowych*" może być potraktowana jako krótkie wprowadzenie do teorii grafów losowych.

Wysokość składki ubezpieczeniowej, czynniki, które mają wpływ na jej wzrost to temat, który interesuje wszystkich zmotoryzowanych. Po lekturze pracy „*Co wpływa na wysokość składki netto w ubezpieczeniach komunikacyjnych?*" będziemy wiedzieli dużo więcej na ten temat.

Monografia „*KWATERNION 2. Prace studentów WPT kierunku matematyka*" jest drugą monografią zawierającą prace studentów kierunku matematyka. Pierwsza, wydana w roku 2018, roku jubileuszu 10-lecia Wydziału Podstaw Techniki, była wydzieloną częścią wspólnej prezentacji prac studentów zrzeszonych w kołach naukowych Wydziału Podstaw Techniki, reprezentujących wszystkie kierunki studiów prowadzone na Wydziale. Obecna, jest wyłącznie zbiorem prac studentów kierunku matematyka. Monografia powstała z inspiracji Studenckiego Koła Naukowego KWATERNION, ale do współpracy zaproszeni zostali też inni studenci kierunku matematyka.

Anna Kuczmaszewska

Magdalena Blacha[1]

Wybrane modele grafów losowych

Streszczenie

W pracy tej zaprezentowano ideę grafu losowego jako narzędzia do modelowania sieci złożonych oraz przedstawiono dwa modele takich grafów: Erdősa-Rényi'ego oraz Barabási'ego-Albert. Zaprezentowany został teoretyczny opis konstrukcji obu modeli oraz przykładowe ich realizacje otrzymane w środowisku R. Wyznaczone zostały wybrane parametry symulowanych sieci, a następnie dokonano porównania rezultatów otrzymanych podczas symulacji z wynikami teoretycznymi wynikającymi z odpowiednich twierdzeń. Dane wykorzystane podczas symulacji zostały wybrane w taki sposób, żeby przedstawić działanie modeli w różnych warunkach. Na tej podstawie sformułowane zostały wnioski pozwalające stwierdzić, kiedy symulacje dobrze odzwierciedlają sytuacje rzeczywiste.

Słowa kluczowe: grafy losowe, sieci złożone, Model Erdősa-Rényi'ego, Model Barabási'ego-Albert

Wstęp

Rozwój technologiczny ostatnich dwóch dekad dostarczył ogromnej ilości danych o sieciach zawierających setki i tysiące wierzchołków. Te tak zwane sieci złożone są wykorzystywane w wielu dziedzinach. Zaczynając od sieci technologicznych, poprzez portale społecznościowe, do sieci biologicznych. Badanie sieci złożonych stało się podstawą prowadzenia badań w wielu dziedzinach takich jak matematyka, statystyka, informatyka, fizyka i biologia. Modele sieci złożonych można zaklasyfikować do grafów losowych.

Sieci złożone przez długi czas były dziedziną, w której teoria składała się jedynie z kilku reguł i wzorów. Niejednokrotnie jedyną metodą służącą do analizy grafów losowych pozostają symulacje komputerowe. Metoda analizy, którą zaproponowali Erdős i Rényi przetarła szlaki badaniom nad rozpowszechnieniem informacji w sieci. Pozwoliło to między innymi zrozumieć w jaki sposób rozprzestrzenia się infekcja, plotka lub panika. Teoria tych dwóch Węgrów wiodła prym w dziedzinie grafów losowych przez ponad trzydzieści lat. Co ciekawe, najwyższej pozycji pozbawiła jej inna sieć, a mianowicie Internet. Pod koniec XX wieku intensywny wzrost mocy obliczeniowej komputerów dał możliwość gromadzenia, analizowania i wymiany danych na temat sieci na niespotykaną dotąd skalę.

[1] Magdalena Blacha, studentka matematyki, Wydział Podstaw Techniki, Politechnika Lubelska, magdalena.blacha@pollub.edu.pl

1. Pojęcia wstępne

1.1. Najważniejsze definicje i twierdzenia klasycznej teorii grafów

Definicja 1.1. [9] *Grafem G* nazywa się parę $G = (V(G), E(G))$, gdzie $V(G)$ jest niepustym zbiorem, a $E(G)$ dowolnym podzbiorem zbioru $\{\{u,v\} : u,v \in V(G)\}$.
$V(G)$ nazywamy zbiorem wierzchołków (węzłów) grafu G, zaś element $n \in V(G)$ nazywamy wierzchołkiem grafu G.
$E(G)$ nazywamy zbiorem krawędzi grafu G, a element $k = \{u,v\} = uv$ krawędzią grafu G. Wierzchołki u i v nazywamy wtedy sąsiednimi.
Należy zwrócić uwagę, że zgodnie z definicją, w rozważanych przez nas grafach nie występują krawędzie wielokrotne i pętle.

Definicja 1.2. [9] Niech $G = (V(G), E(G))$ będzie grafem. Stopniem wierzchołka $u \in V(G)$ w grafie G, nazywamy liczbę $d_G(u)$ wszystkich wierzchołków sąsiednich z wierzchołkiem u. Jeżeli wiadomo o jaki graf chodzi, to używamy krótszego zapisu $d(u)$
Średnim stopniem wszystkich wierzchołków w grafie $G = (V(G), E(G))$ nazywamy liczbę $\overline{\delta(G)}$ daną wzorem:

$$\overline{\delta(G)} = \frac{1}{|V(G)|} \sum_{u \in V(G)} d(u),$$

gdzie $|V(G)|$ oznacza liczbę jego wierzchołków.

Definicja 1.3. [9] Grafem *k-regularnym* nazywamy graf, w którym każdy wierzchołek ma stopień k.

Definicja 1.4. [9] *Marszrutą* o długości n w grafie G z wierzchołka u, do wierzchołka w nazywamy ciąg krawędzi: $uv_1, v_1v_2, ..., v_{n-1}w$.
Wierzchołek u nazywa się *początkowym*, a *w końcowym* wierzchołkiem marszruty $uv_1, v_1v_2, ..., v_{n-1}w$. Marszrutę $uv_1, v_1v_2, ..., v_{n-1}w$, oznaczamy też symbolem $u \to v_1 \to v_2 \to ... \to v_{n-1} \to w$.
Długością marszruty jest liczba jej krawędzi, więc w danym przypadku jest to liczba n.

Definicja 1.5. [9] *Ścieżką* nazywamy marszrutę, w której żaden wierzchołek się nie powtarza.

Definicja 1.6. [9] Graf, którego każde dwa wierzchołki połączone są ścieżką nazywamy *spójnym*.

Definicja 1.7. [9] *Odległością* $d(u,v)$ wierzchołka u od wierzchołka v w grafie spójnym nazywamy długość najkrótszej ścieżki prowadzącej z u do v.

Definicja 1.8. [9] *Średnicą* spójnego grafu G nazywamy liczbę:

$$\operatorname{diam}(G) = \max_{u,v \in G} d(u,v).$$

Lemat 1.1. [9] *W każdym grafie G suma stopni wszystkich wierzchołków jest liczbą parzystą i jest równa podwojonej liczbie krawędzi* $|E(G)|$.

$$\sum_{v \in V(G)} d(v) = 2|E(G)|.$$

1.2. Najważniejsze definicje i twierdzenia rachunku prawdopodobieństwa

W tym rozdziale zostały podane tylko te definicje i twierdzenia, które będą wykorzystane w dalszej części pracy.

Zdarzenie elementarne jest określane jako najprostszy nierozkładalny wynik doświadczenia losowego, możliwy do pojawienia się w tych samych warunkach.

Definicja 1.9. [6] Zbiór wszystkich możliwych wyników doświadczenia nazywamy *zbiorem zdarzeń elementarnych* i zazwyczaj oznaczamy Ω.

Definicja 1.10. [6] Niech $\mathscr{Z}$ będzie pewną rodziną podzbiorów zbioru Ω ($\mathscr{Z} \subset 2^{\Omega}$) spełniającą następujące aksjomaty;

1. $\Omega \in \mathscr{Z}$,
2. jeśli $A \in \mathscr{Z}$, to $A' \in \mathscr{Z}$,
3. jeśli $A_1, A_2, \ldots, A_n \cdots \in \mathscr{Z}$, to $\bigcup_{i=1}^{\infty} A_i \in \mathscr{Z}$.

Wtedy $\mathscr{Z}$ nazywamy σ-*ciałem* lub σ-*algebrą* zdarzeń losowych.

Definicja 1.11. [6] Niech Ω będzie zbiorem zdarzeń elementarnych, a $\mathscr{Z}$ $\sigma-$ciałem zdarzeń losowych tej przestrzeni. *Prawdopodobieństwem* nazywa się funkcję $\mathbb{P}$ określoną na zbiorze $\mathscr{Z}$ taką, że:

1. $\forall\, A \in \mathscr{Z} \quad \mathbb{P}(A) \geqslant 0$,
2. $\mathbb{P}(\Omega) = 1$,
3. jeśli $A_1, A_2, \ldots \in \mathscr{Z}$, i $\forall_{i \neq j}\, A_i \cap A_j = \emptyset \quad \mathbb{P}(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \mathbb{P}(A_i)$.

Definicja 1.12. [6] Niech dana będzie przestrzeń probabilistyczna $(\Omega, \mathscr{Z}, \mathbb{P})$. *Jednowymiarową zmienną losową* X o wartościach rzeczywistych nazywa się funkcję o wartościach rzeczywistych taką, że: $\forall\, r \in \mathbb{R}\ \{\omega \in \Omega : X(\omega) < r\} \in \mathscr{Z}$.

Definicja 1.13. [6] *Rozkładem prawdopodobieństwa* zmiennej losowej X nazywa się funkcję

$$\mathbb{P}_X(B) = \mathbb{P}(X^{-1}(B)), \quad \forall\, B \in \mathscr{B},$$

gdzie $\mathscr{B}$ jest σ-ciałem borelowskim przestrzeni $\mathbb{R}$, a $X^{-1}(B)$ jest przeciwobrazem zbioru B.

Definicja 1.14. [6] *Dystrybuantą* zmiennej losowej X nazywamy funkcję postaci:

$$F_X(x) = \mathbb{P}(X \leqslant x), \quad \forall\, x \in \mathbb{R}.$$

Definicja 1.15. [5] Mówimy, że zmienna losowa X jest typu *skokowego*, jeżeli przyjmuje skończoną lub przeliczalną liczbę wartości oraz

$$f(x_i) = \mathbb{P}(X = x_i) = p_i \geqslant 0 \tag{1}$$

i

$$\sum_i p_i = 1, \tag{2}$$

gdzie $x_i \in \mathscr{A} \subset \mathbb{R},\ i \in \mathscr{I},\ \mathscr{I}$ jest skończonym lub przeliczalnym zbiorem indeksów, $\mathscr{A}$ jest zbiorem wartości zmiennej losowej X. Funkcję $f(x_i) = p_i$ nazywa się *funkcją prawdopodobieństwa* zmiennej losowej X.

Definicja 1.16. [5] Mówimy, że zmienna losowa X jest typu *ciągłego*, jeżeli istnieje taka nieujemna funkcja f, że dystrybuanta F tej zmiennej losowej daje się wyrazić wzorem:

$$F(x) = \int_{-\infty}^{x} f(u)du \quad \text{dla} \quad x \in \mathbb{R},$$

Funkcję f nazywamy *gęstością* lub *funkcją gęstości* zmiennej losowej X.

Definicja 1.17. [5] Jeżeli X jest jednowymiarową zmienną losową ciągłą o gęstości f, to *wartość oczekiwana* tej zmiennej określona jest wzorem:

$$E(X) = \int_{-\infty}^{\infty} xf(x)dx,$$

pod warunkiem, że całka istnieje i jest skończona. Jeżeli jest to zmienna losowa skokowa o funkcji prawdopodobieństwa f postaci (1)–(2), to wartość oczekiwana tej zmiennej jest równa:

$$E(X) = \sum_i x_i \mathbb{P}(X = x_i),$$

pod warunkiem, że szereg jest zbieżny.

Definicja 1.18. [5] Jeżeli istnieje wartość oczekiwana zmiennej losowej X^t, to liczbę EX^t nazywamy *momentem rzędu t* zmiennej losowej X. Definiuje się ją

następująco:
$E(X^t) = \int_{-\infty}^{\infty} x^t f(x)dx$ – w przypadku zmiennej losowej typu ciągłego,
$E(X^t) = \sum_i x_i^t \mathbb{P}(X = x_i)$ – w przypadku zmiennej losowej typu skokowego,
pod warunkiem, że obie wartości istnieją.

Definicja 1.19. [5] *Wariancją* zmiennej losowej X nazywamy liczbę $D^2(X)$ lub $Var(X)$ określoną zdefiniowaną następująco:

$$Var(X) = D^2(X) = E(X - EX)^2 = E(X^2) - (EX)^2,$$

pod warunkiem, że taka wartość oczekiwana istnieje.

Definicja 1.20. [5] *Odchyleniem standardowym* zmiennej losowej X o wariancji $D^2(X)$ nazywamy liczbę $D(X)$ zdefiniowaną następująco:

$$D(X) = \sqrt{D^2(X)}.$$

Twierdzenie 1.1. ***Twierdzenie Poissona (Przybliżenie Poissona rozkładu dwumianowego)*** *Niech X_n oznacza liczbę sukcesów w n próbach Bernoulliego z prawdopodobieństwem sukcesu p_n. Jeżeli $p_n \xrightarrow[n\to\infty]{} 0$ tak, że $np_n \xrightarrow[n\to\infty]{} \lambda > 0$, to dla dowolnego ustalonego $k \in \mathbb{N}$*

$$\mathbb{P}(X_n = k) = \binom{n}{k} p_n^k (1 - p_n)^{n-k} \xrightarrow[n\to\infty]{} \frac{\lambda^k}{k!} e^{-\lambda} = \mathbb{P}(Y_\lambda = k),$$

gdzie Y_λ ma rozkład Poissona z parametrem λ.

2. Model Erdősa-Rényi'ego

W latach pięćdziesiątych XX wieku dwóch węgierskich matematyków Paul Erdős i Alfred Rényi opracowało definicję grafu losowego, która zrewolucjonizowała tradycyjną teorię grafów. Do tego momentu teoria ta była związana głównie z kombinatoryką. Nowym pomysłem było połączenie rozumowania probabilistycznego z kombinatoryką. Pomysł polegał na tym, aby wziąć pod uwagę nie pojedynczy graf, ale rodzinę wszystkich możliwych grafów z pewnymi stałymi własnościami (na przykład z n węzłami i m krawędziami), a następnie wykorzystać teorię prawdopodobieństwa, aby otrzymać właściwości rodziny.

Przedstawimy dwie wersje modelu Erdősa-Rényi'ego.

2.1. Jednostajny graf losowy

Definicja 2.1. [7] (Model Erdősa i Rényi'ego A: Jednostajny graf losowy)
Niech $0 \leqslant m \leqslant M$, gdzie $M = \dfrac{n(n-1)}{2}$. Model oznaczony jako $\mathbb{G}_{n,m}$ składa się z rodziny grafów o n wierzchołkach generowanych przez połączenie m losowo wybranych par wierzchołków, spośród M możliwych par. Każdy graf $G = (V(G), E(G))$, gdzie $|V(G)| = n$ i $|E(G)| = m$ ma przypisane takie samo prawdopodobieństwo

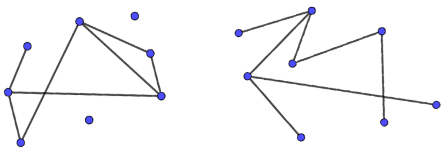
$$\mathbb{P}(G) = \binom{\binom{n}{2}}{m}^{-1}.$$

W praktyce, pomysłem było rozważanie nie pojedynczego grafu, ale całej rodziny grafów, co pozwala modelować bardziej złożone zjawiska. Procedura powstania takiej rodziny obejmuje dwa etapy:
— ustalenie zbioru wierzchołków $V(G)$, $|V(G)| = n$ należących do grafu;
— losowe wybranie m par wierzchołków, pomiędzy którymi zostaną utworzone krawędzie.

Najpierw losowo otrzymuje się pierwszą z M możliwych krawędzi, tak że wszystkie są tak samo prawdopodobne. Następnie losowo wybiera się drugą krawędź z jednakowym prawdopodobieństwem z pozostałych $M-1$ możliwych krawędzi i kontynuuje się ten proces do czasu otrzymania m krawędzi. Otrzymany graf jest jednym z wielu możliwych rezultatów.

Ile różnych grafów o n wierzchołkach i m krawędziach jest w takiej rodzinie? Liczba ta jest równa liczbie sposobów na ile można wybrać m obiektów spośród M możliwych. Będzie to $\dfrac{M!}{m!(M-m)!}$. Wielkość ta nazywana jest współczynnikiem dwumianowym. Oznacza się go jako: C_M^m lub $\binom{M}{m}$.

Na rysunku 1 przedstawiono przykładowe realizacje tego modelu.



Rysunek 1. Dwie różne realizacje modelu Erdősa i Rényi'ego A $\mathbb{G}_{8,7}$
Źródło: Opracowanie własne

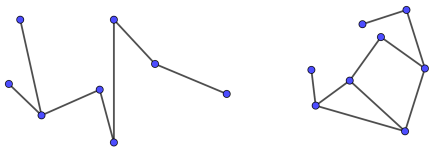
2.2. Dwumianowy graf losowy

Definicja 2.2. [7] (Model Erdősa i Rényi'ego *B*: Dwumianowy graf losowy)
Niech $0 \leqslant p \leqslant 1$. Model oznaczony jako $\mathbb{G}_{n,p}$ zawiera rodzinę grafów z n wierzchołkami uzyskanymi w wyniku połączenia każdej pary węzłów z prawdopodobieństwem p. Prawdopodobieństwo $P_{\mathbb{G}}$ powiązane z grafem $\mathbb{G} = (V(\mathbb{G}), E(\mathbb{G}))$, gdzie $|V(\mathbb{G})| = n$ i $|E(\mathbb{G})| = m$, to $P_{\mathbb{G}} = p^m(1-p)^{M-m}$, gdzie $M = \dfrac{n(n-1)}{2}$.

Model ten jest uogólnieniem modelu omawianego wcześniej. Liczba krawędzi w grafie, zostaje zastąpiona przez prawdopodobieństwo istnienia krawędzi między dowolnymi parami wierzchołków. Procedura konstrukcyjna tego modelu wygląda następująco:

— ustalenie zbioru wierzchołków $V(G)$, $|V(G)| = n$ należących do grafu;
— z ustalonym prawdopodobieństwem p łączy się krawędzią każdą z $\binom{n}{2}$ par wierzchołków.

Na rysunku 2 przedstawiono przykładowe realizacje tego modelu.



Rysunek 2. Dwie różne realizacje modelu Erdősa i Rényi'ego *B* $\mathbb{G}_{8,0.5}$
Źródło: Opracowanie własne

Rodzina grafów zdefiniowanych przez model *B* jest całkowicie różna od tej, którą otrzymano w modelu *A*. Różnice można zauważyć na rysunkach 1 i 2.

Wszystkie grafy na rysunku 1 mają taką samą liczbę wierzchołków i taką samą liczbę krawędzi. Na rysunku 2 wszystkie grafy mają taką samą liczbę wierzchołków, ale liczba krawędzi się zmienia. Każdy z grafów na rysunku 2, będąc reprezentacją modelu Erdősa i Rényi'ego *B*, jest jednocześnie jedną z wielu realizacji modelu Erdősa i Rényi'ego *A*, przy $m_1 = 7$, $m_2 = 9$.

W modelu *B*, można otrzymać graf pełny, albo graf pusty. Jednak ich uzyskanie jest mało prawdopodobne. Chyba, że $p \approx 1$ w przypadku grafu pełnego i $p \approx 0$ dla grafu pustego. Z modelu *B* można otrzymać wszystkie możliwe grafy o ustalonej liczbie wierzchołków, ale nie z takim samym prawdopodobieństwem.

2.3. Własności dwumianowego grafu losowego Erdősa i Rényi'ego

Z uwagi na to, że w pewnych warunkach model jednostajny i dwumianowy możemy uważać za równoważne, omawiać będziemy tylko dwumianowy model grafu losowego Erdősa-Rényi'ego.

Średnia liczba krawędzi

Z algorytmu konstrukcji grafów Erdősa i Rényi'ego wynika, że wartość oczekiwana Em liczby krawędzi w grafie $\mathbb{G}_{n,p}$ wynosi:

$$Em = p \cdot \binom{n}{2} = p \cdot \frac{n(n-1)}{2}$$

Średni stopień wierzchołka

Na podstawie lematu 1.1 otrzymujemy twierdzenie.

Twierdzenie 2.1. [3] *Średni stopień wierzchołka w grafie Erdősa-Rényi'ego* $\mathbb{G}_{n,p}$ *wynosi:*

$$Ek = \frac{2 \cdot Em}{n} = p(n-1) \approx pn,$$

gdzie Em oznacza oczekiwaną liczbę krawędzi.

Oznacza to, że średni stopień wierzchołka w grafie Erdősa-Rényi'ego jest iloczynem liczby wierzchołków i prawdopodobieństwa istnienia krawędzi między dowolnymi parami wierzchołków w tym grafie.

Rozkład stopni wierzchołków

Z algorytmu konstrukcji dwumianowych grafów losowych, można wywnioskować, że rozkład stopni węzłów w tych grafach jest rozkładem dwumianowym [3]. Prawdopodobieństwo posiadania przez dowolny wierzchołek stopnia k, przy największym możliwym $n-1$ jest równe prawdopodobieństwu osiągnięcia k sukcesów w $n-1$ próbach, przy prawdopodobieństwie sukcesu równym p i przy prawdopodobieństwie porażki $1-p$:

$$\mathbb{P}(d(v) = k) = \binom{n-1}{k} p^k (1-p)^{n-1-k}.$$

Gdy liczba krawędzi w grafie jest mała, czyli gdy $p \ll 1$, rozkład dwumianowy, zgodnie z twierdzeniem 1.1, można przybliżyć rozkładem Poissona:

$$\mathbb{P}(d(v) = k) = \frac{e^{-Ek}(Ek)^k}{k!}. \tag{3}$$

Ze względu na rozkład (3) dwumianowe grafy losowe Erdősa-Rényi'ego często określa się terminem „grafy poissonowskie". Zazwyczaj wyrażenie to pojawia się razem z wyrażeniem „sieci bezskalowe" lub „potęgowe" (które są opisane w rozdziale 3) i ma to na celu wyeksponowanie jednej z najpoważniejszych wad grafów Erdősa i Rényi'ego, która nie pozwala na użycie tych sieci do modelowania sieci rzeczywistych. Mankamentem tym jest rozkład stopni wierzchołków o niewielkiej wariancji. W rozkładzie Poissona wariancja σ_k^2 równa jest wartości średniej Ek [3].

$$\sigma_k^2 = E(k^2) - (Ek)^2 = Ek$$

Okazuje się, że odchylenie standardowe stopni wierzchołków od wartości średniej Ek, w porównaniu do tej wartości jest niewielkie.

$$\sigma_k = \sqrt{Ek}$$

Ta własność rozkładu Poissona ma wpływ na brak w grafach Erdősa i Rényi'ego wierzchołków o stopniach istotnie różniących się od średniej wartości Ek. Na skutek tego, na dwumianowe grafy losowe możemy patrzeć jak na grafy regularne, których wszystkie wierzchołki mają stopień równy Ek [3].

Średnia długość ścieżki

Twierdzenie 2.2. [2] *Niech $\overline{s}(\mathbb{G}_{n,p})$ oznacza średnią długość ścieżki w dwumianowym modelu Erdősa-Rényi'ego. Wówczas*

$$\mathbb{P}\left(\overline{s}(\mathbb{G}_{n,p}) = \frac{\ln(n) - \gamma}{\ln(np)} + 0.5\right) \xrightarrow[n\to\infty]{} 1,$$

gdzie γ jest stałą Eulera.

Średnica

Twierdzenie 2.3. [4] *Niech* $\mathrm{diam}(\mathbb{G}_{n,p})$ *oznacza średnicę w dwumianowym modelu Erdősa-Rényi'ego. Załóżmy, że* $p = \frac{\omega \ln(n)}{n}$, *gdzie* $\omega \to \infty$. *Wówczas*

$$\mathbb{P}\left(\mathrm{diam}(\mathbb{G}_{n,p}) = \frac{\ln(n)}{\ln(np)}\right) \xrightarrow[n\to\infty]{} 1.$$

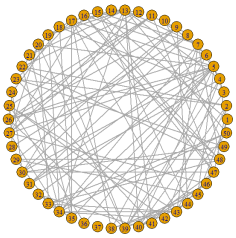
Powyższe twierdzenia zostaną wykorzystane w dalszej części pracy.

2.4. Symulacja modelu

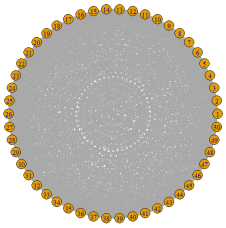
W tym podrozdziale przedstawione zostaną wyniki symulacji modelu Erdősa-Rényi'ego przeprowadzonych w środowisku R. W celu wykonania symulacji wykorzystano funkcję `erdos-renyi-game()` pakietu `igraph`. Realizację tego modelu przeprowadzono dla liczby wierzchołków n równej 50 i 1000 oraz dla prawdopodobieństwa p równego 0.1 i 0.8.

W celu wyznaczenia rozważanych parametrów oraz rozkładów stopni wierzchołków, wykorzystano funkcje pakietu `igraph` takie jak: `degree()`, `degree.distribution()`, `diameter()`, `average.path.length()`.

2.4.1. Realizacja modelu



Rysunek 3. Realizacja modelu Erdősa-Rényi'ego dla $n = 50$ **i** $p = 0.1$
Źródło: Opracowanie własne



Rysunek 4. Realizacja modelu Erdősa-Rényi'ego dla $n = 50$ **i** $p = 0.8$
Źródło: Opracowanie własne

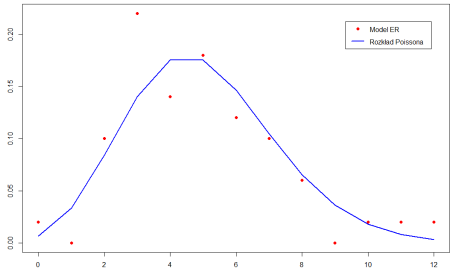
Na rysunkach 3 i 4 przedstawiono realizacje modelu Erdősa-Rényi'ego.

Dane wykorzystane podczas symulacji zostały dobrane w taki sposób, żeby zaprezentować działanie modelu w różnych warunkach. Jak można zauważyć, im wyższy poziom prawdopodobieństwa, tym graf jest gęstszy.

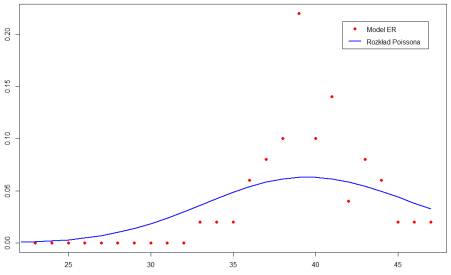
Jak można zauważyć, na rysunku 4 dla $n = 50$ i $p = 0.5$ graf jest nieczytelny. Dlatego nie przedstawimy realizacji dla $n = 1000$.

2.4.2. Rozkład stopni wierzchołków

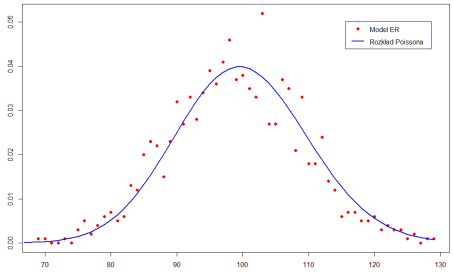
Na rysunkach 5–8 zostały zaprezentowane wykresy przedstawiające rozkład stopni wierzchołków w grafach losowych Erdősa-Rényi'ego. Dodatkowo niebieską linią narysowany został wykres gęstości rozkładu Poissona odpowiadający danej realizacji, czyli z $\lambda = Ek$.



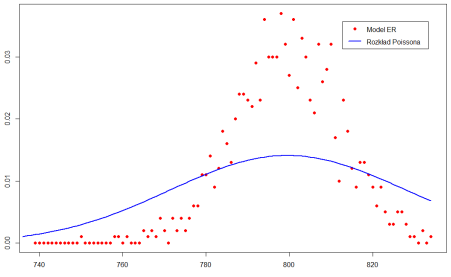
Rysunek 5. Rozkład stopni wierzchołków w grafie Erdősa-Rényi'ego dla $n = 50$ i $p = 0.1$
Źródło: Opracowanie własne



Rysunek 6. Rozkład stopni wierzchołków w grafie Erdősa-Rényi'ego dla $n = 50$ i $p = 0.8$
Źródło: Opracowanie własne



Rysunek 7. Rozkład stopni wierzchołków w grafie Erdősa-Rényi'ego dla $n = 1000$ i $p = 0.1$
Źródło: Opracowanie własne



Rysunek 8. Rozkład stopni wierzchołków w grafie Erdősa-Rényi'ego dla $n = 1000$ i $p = 0.8$
Źródło: Opracowanie własne

Analizując wykresy rozkładów stopni wierzchołków, możemy dostrzec, że im mniej krawędzi graf posiada, tym lepiej można taki rozkład przybliżyć rozkładem Poissona. Najłatwiej można to zauważyć na wykresie 7. Jest to zgodne z twierdzeniem 1.1. Na wykresach grafów o prawdopodobieństwie równym 0.8,

wartości stopni wierzchołków modelu Erdősa-Rényi'ego przewyższają wartości otrzymane z rozkładu Poissona.

2.4.3. Średni stopień wierzchołka

Tabela 1. Średnie stopnie wierzchołków obliczone z twierdzenia 2.1

Prawdopodobieństwo \ Liczba wierzchołków	50	1000
0.1	5	100
0.8	40	800

Tabela 2. Średnie stopnie wierzchołków uzyskane w symulacji

Prawdopodobieństwo \ Liczba wierzchołków	50	1000
0.1	4.88	99.04
0.8	39.8	799.32

Analizując wyniki zawarte w tabelach 1 i 2, możemy wnioskować, że wyniki otrzymane za pomocą funkcji w środowisku R odpowiadają wynikom otrzymanym na podstawie twierdzenia 2.1. Im więcej wierzchołków graf posiada, tym mniejsze różnice w wynikach otrzymujemy. Można zauważyć, że w prawie każdym przypadku różnice w otrzymanych wartościach średnich stopni wierzchołków są poniżej 1.

2.4.4. Średnica

Tabela 3. Teoretyczne wartości średnic z twierdzenia 2.3

Prawdopodobieństwo \ Liczba wierzchołków	50	1000
0.1	2.43	1.5
0.8	1.06	1.03

Tabela 4. Średnie wartości średnic otrzymane podczas 100 symulacji

Prawdopodobieństwo \ Liczba wierzchołków	50	1000
0.1	5.06	3
0.8	2	2

Porównując wyniki otrzymane za pomocą twierdzenia 2.3 z średnimi wynikami otrzymanymi podczas 100 symulacji, możemy zauważyć, że w pierwszym wierszu są one istotnie różne. Jest to spowodowane założeniami twierdzenia, które w tym przypadku nie zostały spełnione. Jednakże wartości w ostatnim wierszu nie różnią się już tak znacząco. Ponieważ średnica musi być liczbą całkowitą, to gdyby obliczyć wartości otrzymanych wyników zaokrąglonych do liczb całkowitych do góry, otrzymalibyśmy takie same rezultaty.

2.4.5. Średnia długość ścieżki

Tabela 5. Średnie długości ścieżek otrzymane za pomocą twierdzenia 2.2

Prawdopodobieństwo \ Liczba wierzchołków	50	1000
0.1	2.59	1.9
0.8	1.2	1.2

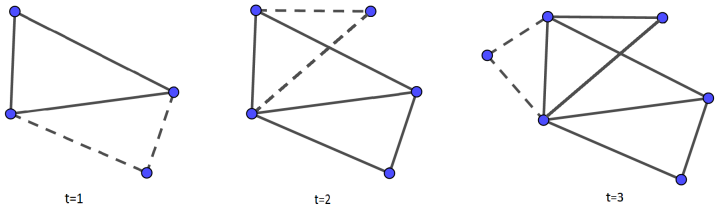
Tabela 6. Uśrednione średnie długości ścieżek otrzymane podczas 100 symulacji

Prawdopodobieństwo \ Liczba wierzchołków	50	1000
0.1	2.56	1.9
0.8	1.2	1.2

Porównując wyniki otrzymane za pomocą twierdzenia 2.2 z średnimi wynikami otrzymanymi podczas 100 symulacji możemy powiedzieć, że otrzymane wielkości są porównywalne. Twierdzenie, z którego skorzystano, zostało opublikowane w [2], a cytowane jest w niewielu publikacjach, między innymi w [8]. Jednak, jak widać działa ono prawie idealnie.

3. Model Barabási'ego-Albert

W odpowiedzi na pytanie, w jaki sposób modelować graf, aby uzyskać bezskalowy rozkład stopni wierzchołków, Albert László Barabási i Réka Albert, dwoje fizyków, zaproponowali pewien model. W szczególności zakłada się, że liczba krawędzi wzrasta proporcjonalnie do liczby węzłów, a istniejące węzły sieci łączą się z nowymi węzłami z prawdopodobieństwem liniowo proporcjonalnym do ich stopnia. Chociaż model zapewnia niezwykle uproszczony opis rozwijających się sieci, daje początek sieciom bezskalowym z potęgowymi rozkładami stopni z wykładnikiem $\alpha = 3$.



Rysunek 9. Ilustracja modelu Barabási'ego-Albert dla $n_0 = 3$ i $m = 2$.
Źródło: Opracowanie własne

3.1. Opis konstrukcji

Definicja 3.1. [7] (Model Barabási'ego-Albert) Weźmy trzy dodatnie liczby całkowite N, n_0 i m ($m \leqslant n_0 \ll N$), niech n_t i l_t oznaczają liczbę wierzchołków i krawędzi grafu wygenerowanych w czasie t. W czasie $t = 0$, zaczynamy z grafem pełnym o n_0 wierzchołkach, oznaczonych $1, 2, 3, ..., n_0$ i $l_0 = \binom{n_0}{2}$ krawędziach. Graf rośnie, jak na rysunku 9 poprzez iteracyjne powtarzanie w czasie $t = 1, 2, 3, ..., N - n_0$ poniższych dwóch kroków:

1. Nowy wierzchołek, oznaczony indeksem n, gdzie $n = n_0 + t$, zostaje dodany do grafu.
2. m krawędzi łączy nowy wierzchołek z m innymi wierzchołkami już obecnymi w grafie, zgodnie z regułą preferencyjnego dołączania węzłów, czyli zasadą, że częściej wybierane są wierzchołki, które mają wyższy stopień, niż te które mają stopień niższy. Formalny opis tej zasady znajduje się poniżej.

Otrzymany graf nazywany jest losowym grafem Barabási'ego-Albert i oznaczany jest $BA(N, n_0, m)$.

Niech $k_{i,t}$ oznacza stopień wierzchołka i w chwili t, a $\mathbb{P}(n \to i)$ niech oznacza prawdopodobieństwo tego, że nowa krawędź połączy nowy wierzchołek n z wierzchołkiem i, gdzie $i = 1,2,...,n-1$ w chwili t. Prawdopodobieństwo to wynosi:

$$\mathbb{P}(n \to i) = \frac{k_{i,t-1}}{\sum_{j=1}^{n-1} k_{j,t-1}} = \frac{k_{i,t-1}}{2l_{t-1}}. \tag{4}$$

W modelu *prawdopodobieństwo połączenia* $\mathbb{P}(n \to i)$ jest normalizowane, zatem

$$\sum_{i=1}^{n-1} \mathbb{P}(n \to i) = 1.$$

Warto zauważyć, że $\mathbb{P}(n \to i)$ w zależności (4) zależy nie tylko od stopnia k_i wierzchołka i, a także od całkowitej liczby krawędzi l_{t-1}, to znaczy:

$$\mathbb{P}(n \to i) = \mathbb{P}(k_{i,t-1}, l_{t-1}).$$

Dokładniej, jest to liniowo proporcjonalne do stopnia wierzchołka i. Naśladuje to liniowe preferencje połączeń obserwowane w rzeczywistych systemach, jak na przykład w naukowych sieciach cytowań. Od teraz uwzględniamy zależność od czasu i całkowitej liczby krawędzi, i piszemy $\mathbb{P}(n \to i) = \mathbb{P}(k_i)$, gdzie

$$\mathbb{P}(k_i) = \frac{k_i}{\sum_l k_l}. \tag{5}$$

Zauważmy, że odkąd prawdopodobieństwo $\mathbb{P}(n \to i)$ zależy tylko od k_i, normalizacja mianownika $\sum_l k_l$ może być zapisana jako $\sum_k kN_k$. Wyrażenie $\mathbb{P}(k)$ otrzymuje zatem postać:

$$\mathbb{P}(k) = \frac{k}{\sum_k kN_k},$$

gdzie N_k jest liczbą wierzchołków o stopniu k z oczywistą normalizacją:

$$\sum_k N_k \mathbb{P}(k) = 1.$$

W danej chwili t proces wzrostu modelu Barabási'ego-Albert tworzy graf o:

$$n_t = n_0 + t \text{ wierzchołkach}$$

i

$$l_t = \binom{n_0}{2} + mt \text{ krawędziach.}$$

Proces jest iterowany do chwili $N - n_0$, generując nieskierowany graf o N wierzchołkach i $K = m(N-n_0) + \frac{n_0(n_0-1)}{2}$ krawędziach. Dla dużych N, oznacza to, że wartość średnia stopnia wierzchołka wynosi: $Ek = 2m$.

3.2. Własności sieci Barabási'ego-Albert

Rozkład stopni wierzchołków

Jedną z najważniejszych cech sieci Barabási'ego-Albert jest potęgowy rozkład stopni wierzchołków. Oznacza to, że prawdopodobieństwo tego, że pewien wierzchołek ma stopień k jest proporcjonalne do $k^{-\alpha}$ dla pewnej liczby $\alpha > 1$ zwanej wykładnikiem skalującym. Można to zapisać jako:

$$\mathbb{P}(d(v) = k) \propto k^{-\alpha}.$$

Rozkład ten decyduje o tym, że większość węzłów ma niski stopień, ale niektóre z nich mają bardzo duży stopień. Wierzchołki takie to tak zwane huby.

Uśredniony rozkład stopni wierzchołków opisywany jest przez zależność:

$$\mathbb{P}(d(v) = k) = \frac{2m^2}{k^3}.$$

Twierdzenie 3.1. [8] *Dla dowolnego grafu G będącego grafem $BA(N, n_0, m)$, prawdopodobieństwo tego, że wierzchołek $v \in V(G)$ ma stopień $k \geqslant m$ dane jest jako:*

$$\mathbb{P}(k) = \frac{2m(m+1)}{k(k+1)(k+2)} \propto k^{-3}.$$

Średni stopień wierzchołka

Twierdzenie 3.2. [8] *Średni stopnień wierzchołka w sieci Barabási'ego-Albert wyraża się wzorem:*

$$Ek = \sum_{k=m}^{\infty} k \cdot P(k) = 2m(m+1) \sum_{k=m}^{\infty} \frac{k}{k(k+1)(k+2)} = 2m.$$

Średnia długość ścieżki

Twierdzenie 3.3. [2] *Średnią długość ścieżki w sieci Barabási'ego-Albert* $BA(N,n_0,m)$ *wyraża się wzorem:*

$$\overline{d}(BA(N,n_0,m)) = \frac{\ln(N) - \ln(\frac{m}{2}) - 1 - \gamma}{\ln(\ln(N)) + \ln(\frac{m}{2})} + 1.5,$$

gdzie γ *jest stałą Eulera.*

Średnica

Twierdzenie 3.4. [1] *Dla* $m > 1$ *i dostatecznie dużego N, średnicę sieci w modelu Barabási'ego-Albert wyraża się wzorem*

$$\operatorname{diam}(BA(N,n_0,m)) = \frac{\ln N}{\ln\ln N}.$$

Średnica rośnie wolniej niż $\ln N$, dzięki czemu odległości w modelu Barabási'eg-Albert są mniejsze niż odległości obserwowane na grafie losowym Erdősa-Rényi'ego o podobnej wielkości. Różnica jest szczególnie istotna w przypadku dużych N.

Powyższe twierdzenia zostaną wykorzystane w dalszej części pracy.

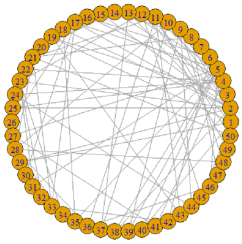
3.3. Symulacja modelu

W tym rozdziale przedstawimy wyniki symulacji modelu Barabási'ego-Albert przeprowadzonych w środowisku R. W celu wykonania symulacji wykorzystano funkcję `barabasi-game()` pochodzącą z pakietu `igraph`. Grafem startowym jest graf pełny o trzech wierzchołkach. Realizację tego modelu przeprowadzono dla liczby wierzchołków N równej 50 i 1000 oraz liczby dodawanych krawędzi m równej 2 i 4.

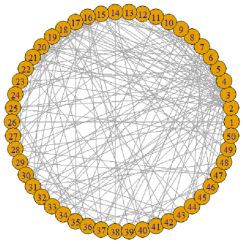
W celu wyznaczenia rozważanych parametrów oraz rozkładów stopni wierzchołków, wykorzystano funkcje pakietu `igraph` takie jak: `degree(), diameter(), degree.distribution(), average.path.length()`.

3.3.1. Realizacja modelu

Na rysunkach 10–11 zostały przedstawione wybrane realizacje grafów losowych Barabási'ego-Albert otrzymane w środowisku R.



Rysunek 10. Realizacja modelu Barabási'ego-Albert dla $N = 50$ i $m = 2$
Źródło: Opracowanie własne

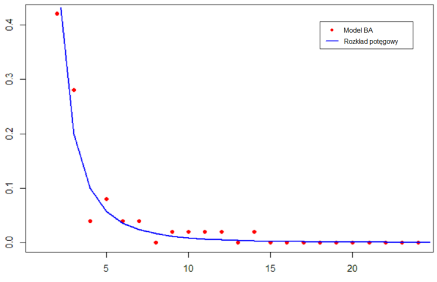


Rysunek 11. Realizacja modelu Barabási'ego-Albert dla $N = 50$ i $m = 4$
Źródło: Opracowanie własne

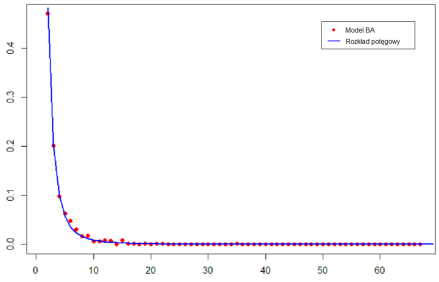
Realizacje dla $N = 1000$ są mało czytelne, dlatego nie zostaną przedstawione.

3.3.2. Rozkład stopni wierzchołków

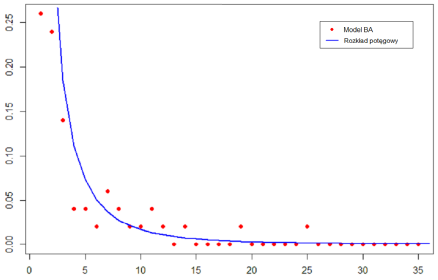
Na rysunkach 12–15 zostały zaprezentowane wykresy przedstawiające rozkład stopni wierzchołków w grafach losowych Barabási'ego-Albert. Dodatkowo niebieską linią narysowany został odpowiadający danej realizacji wykres gęstości rozkładu potęgowego z twierdzenia 3.1.



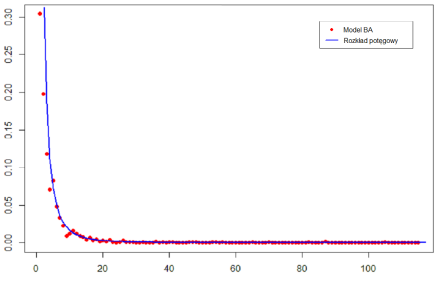
Rysunek 12. Rozkład stopni wierzchołków w grafie Barabási'ego-Albert dla $N = 50$ i $m = 2$
Źródło: Opracowanie własne



Rysunek 13. Rozkład stopni wierzchołków w grafie Barabási'ego-Albert dla $N = 1000$ i $m = 2$
Źródło: Opracowanie własne



Rysunek 14. Rozkład stopni wierzchołków w grafie Barabási'ego-Albert dla $N = 50$ i $m = 4$
Źródło: Opracowanie własne



Rysunek 15. Rozkład stopni wierzchołków w grafie Barabási'ego-Albert dla $N = 1000$ i $m = 4$
Źródło: Opracowanie własne

Analizując powyższe wykresy dochodzimy do wniosku, że im więcej wierzchołków ma graf, tym lepiej rozkład stopni wierzchołków można przybliżyć rozkładem potęgowym. Najłatwiej można to dostrzec na wykresach wykonanych dla 1000 wierzchołków. Wtedy czerwone punkty oznaczające poszczególne wierzchołki w grafie prawie idealnie pokrywają się z niebieską linią, oznaczającą teoretyczną funkcję gęstości rozkładu potęgowego.

3.3.3. Średni stopień wierzchołka

Tabela 7. Średnie stopnie wierzchołków obliczone z twierdzenia 3.2

Liczba wierzchołków / Liczba dodawanych krawędzi	50 i 1000
2	4
4	8

Tabela 8. Średnie stopnie wierzchołków uzyskane w symulacji

Liczba wierzchołków / Liczba dodawanych krawędzi	50	1000
2	3.88	3.99
4	7.60	7.98

Po przeanalizowaniu tabel 7 i 8 można zauważyć, że otrzymujemy podobne wartości. Różnice pomiędzy nimi nie przekraczają 1. Niezgodności te maleją wraz ze wzrostem liczby wierzchołków w grafie i rosną wraz ze wzrostem liczby dodanych krawędzi.

3.3.4. Średnica

Tabela 9. Średnice otrzymane za pomocą twierdzenia 3.4

Liczba dodawanych krawędzi \ Liczba wierzchołków	50	1000
2 i 4	2.87	3.57

Tabela 10. Uśrednione wartości średnic otrzymane podczas 100 symulacji

Liczba dodawanych krawędzi \ Liczba wierzchołków	50	1000
2	4.42	4.71
4	1.97	2.29

Analizując tabele 9 i 10 widzimy różne wyniki. Jest to spowodowane tym, że w założeniach twierdzenia znajduje się warunek, że liczba wierzchołków w grafie musi być wystarczająco duża. W książce [1] możemy przeczytać, że dopiero przy liczbie wierzchołków równej co najmniej 10000 obliczanie wartości średnicy, korzystając z twierdzenia 3.4 da poprawne wyniki.

3.3.5. Średnia długość ścieżki

Tabela 11. Średnie długości ścieżek otrzymane za pomocą twierdzenia 3.3

Liczba dodawanych krawędzi \ Liczba wierzchołków	50	1000
2	2.21	4.26
4	2.3	3.27

Tabela 12. Uśrednione średnie długości ścieżek otrzymane podczas 100 symulacji

Liczba dodawanych krawędzi \ Liczba wierzchołków	50	1000
2	2.23	2.03
4	2.21	1.99

Poddając analizie tabele 11 i 12 zauważamy, że w przypadku większej liczby dodawanych krawędzi wartości otrzymane na mocy twierdzenia 3.3 przewyższają wartości otrzymane w wyniku symulacji. Na ten temat możemy przeczytać w [2]. Zostało tam napisane, że w przypadku małej liczby dodawanych krawędzi, różnice otrzymanych wyników będą niewielkie dopiero w grafach składających się z prawie 10000 wierzchołków. Natomiast przy liczbie dodawanych krawędzi równej 10, różnice otrzymanych wyników są nieznaczne, nawet gdy graf składa się z 100 wierzchołków.

4. Podsumowanie i wnioski

Grafy losowe to stosunkowo nowy temat w dziedzinie matematyki. Pierwsza publikacja poruszająca tę problematykę ukazała się dość niedawno, bo miało to miejsce w latach pięćdziesiątych ubiegłego wieku. Był to artykuł, w którym zaprezentowano model Erdősa-Rényi'ego. Początkowo cała teoria składała się tylko z kilku wzorów i reguł. Pod koniec XX wieku intensywny wzrost mocy obliczeniowej komputerów pozwolił tej dziedzinie rozwinąć skrzydła. Wtedy to Albert-László Barabási wraz z Réką Albert zaproponował inny model, nazwany ich nazwiskami.

Celem pracy było omówienie idei grafu losowego oraz zaprezentowanie dwóch modeli grafów losowych, a mianowicie modelu Erdősa-Rényi'ego oraz modelu Barabási'ego-Albert. Przedstawiono tutaj przykładowe realizacje tychże modeli. Wyznaczono charakterystyczne dla nich parametry, a następnie dokonano porównania rezultatów otrzymanych podczas symulacji z wynikami odpowiednich twierdzeń. Porównano również efekty przeprowadzonych realizacji z teoretycznymi rozkładami stopni wierzchołków. Dane wykorzystane podczas symulacji zostały wybrane w taki sposób, żeby przedstawić działanie modeli w różnych warunkach.

Rozkłady stopni wierzchołków w modelu Erdősa-Rényi'ego pokazują silne związki z twierdzeniem o przybliżaniu rozkładu dwumianowego rozkładem Poissona. W przypadku dużego p rozkład symulacji wyraźnie odbiega od rozkładu teoretycznego. Natomiast w przypadku modelu Barabási'ego-Albert można zauwa-

żyć szybką zbieżność wartości teoretycznych z symulacyjnymi, wraz ze wzrostem liczby wierzchołków.

Ciekawie ma się sprawa porównywanych średnich długości ścieżek w obu modelach. Porównywano tam wartości teoretyczne z średnimi wartościami otrzymanymi podczas 100 realizacji. W przypadku modelu Erdősa-Rényi'ego wartości uzyskane w wyniku symulacji praktycznie nie różniły się od oszacowań podanych w jednym artykule. Natomiast w modelu Barabási'ego-Albert otrzymane wartości znacząco się różniły. Spowodowane było to tym, że w tym przypadku podane w artykule oszacowania są spełnione przy zbyt dużej, jak na możliwości sprzętowe autorki, wielkości grafu.

Podobnie było przy porównywaniu wartości średnic w tych modelach. Do otrzymania efektów zawartych w artykule, potrzebne są grafy mające co najmniej 10000 wierzchołków. Co ciekawe, przypadku modelu Erdősa-Rényi'ego do otrzymania wartości takich, jak w twierdzeniu wystarczyło już 1000 wierzchołków.

Na podstawie przeprowadzonych symulacji można powiedzieć, że jeśli wszystkie założenia twierdzeń są spełnione, to otrzymane wyniki można bez obaw zastąpić tymi, które otrzymano podczas symulacji w środowisku R.

Literatura

[1] A. L. Barabási, *Network Science*, książka hybrydowa http://networksciencebook.com, *dostęp w dniu 17.01.2020*.
[2] A. Fronczak, P. Fronczak, J. Hołyst, *Average Path Length in Random Networks*, Physical Review E 70, 056110, 2004.
[3] A. Fronczak, P. Fronczak, *Świat sieci złożonych od fizyki do internetu*, Wydawnictwo Naukowe PWN, 2009.
[4] A. Frieze, M. Karoński, *Introduction to random graphs*, Cambridge University Press, 2016.
[5] C. L. Grinstead, J. L. Snell, *Introduction to Probability*, American Mathematical Society, 1997.
[6] J. Jakubowski, R. Sztencel *Wstęp do teorii prawdopodobieństwa*, SCRIPT, 2001.
[7] V. Latora, V. Nicosia, G. Russo, *Complex networks: principles, methods and applications* Cambridge University Press, 2017.
[8] M. van Steen, *Graph Theory and Complex Networks, an introduction*, Maarten van Steen, 2010.
[9] R. J. Wilson, *Wprowadzenie do teorii grafów*, Wydawnictwo Naukowe PWN, 2012.

Paulina Dębicka [1]

Sposoby obliczania NWD i NWW

Streszczenie

Niniejsza praca poświęcona jest wybranym pojęciom z zakresu teorii liczb tj. pojęciu *największego wspólnego dzielnika* (NWD) i pojęciu *najmniejszej wspólnej wielokrotności* (NWW) oraz sposobom ich wyznaczania.

Zawarte są w niej dwa spojrzenia na definicję tych dwóch wielkości oraz trzy sposoby ich obliczania. Zamieszczone zostały także dwa nowe twierdzenia wprowadzające zależności między NWD i NWW co najmniej trzech liczb naturalnych.

Słowa kluczowe: największy wspólny dzielnik, najmniejsza wspólna wielokrotność

Wstęp

Pozornie nie spotykamy się w życiu codziennym z takimi pojęciami, jak najmniejsza wspólna wielokrotność i największy wspólny dzielnik. Jednak, mimo że często nie zdajemy sobie z tego sprawy, mamy z nimi do czynienia. Przykładowo mamy trzech gości (cztery osoby razem z nami) i chcemy zamówić pizzę (która jest dzielona na sześć równych kawałków) tak, by każdy dostał tyle samo kawałków. Nie mamy także zbyt dużego budżetu, więc staramy się wydać jak najmniej. Dlatego musimy znaleźć NWW dla liczb 6 i 4, co sprowadzi się do 12 kawałków. Należy więc zamówić dwie pizze.

Warto więc przypatrzeć się sposobom obliczenia tych wartości, gdyż nie zawsze rachunki te będą proste.

1. Podejście wczesnoszkolne

Z pojęciami największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności spotykamy się już w szkole podstawowej. Poznajemy w niej także sposoby ich wyznaczania [1, 2, 6].

Przyjmiemy następujące oznaczenia:
$\mathbb{N} = \{0,1,2,3,...\}$ – zbiór liczb naturalnych,
$\mathbb{N}_+ = \{1,2,3,...\}$ – zbiór liczb naturalnych dodatnich,
$\mathbb{Z} = \{...,-2,-1,0,1,2,...\}$ – zbiór liczb całkowitych,
$\mathbb{P} = \{2,3,5,7,11,...\}$ – zbiór wszystkich liczb pierwszych.

[1] inż. Paulina Dębicka, studentka studiów II stopnia na kierunku Matematyka, e-mail:paulina.debicka1@pollub.edu.pl, Wydział Podstaw Techniki, Politechnika Lubelska

Definicja 1. [6] Największym wspólnym dzielnikiem liczb a i b ($a,b \in \mathbb{N}_+$) nazywamy największą liczbę naturalną dodatnią dzielącą obie te liczby jednocześnie (ozn. $NWD(a,b)$).

Definicja 2. [5] Niech $x_1, x_2, ..., x_n$ będą dodatnimi liczbami naturalnymi. Największym wspólnym dzielnikiem tych liczb nazywamy największą, dodatnią liczbę naturalną dzielącą każdą z tych liczb. Oznaczamy ją przez $NWD(x_1, x_2, ..., x_n)$.

Algorytm 1. (*Algorytm wyznaczania NWD*) Niech $x_1, x_2, ..., x_n \in \mathbb{N}_+$.

1) Każdą liczbę naturalną x_i ($i \in 1, 2, ..., n$) rozkładamy na czynniki pierwsze.
2) Zaznaczamy wspólne dzielniki tych liczb.
3) Jeśli nie została zakreślona żadna liczba to NWD wynosi **1**.
4) Mnożymy zaznaczone czynniki przez siebie otrzymując szukaną wartość.

Przykład 1. Obliczmy największy wspólny dzielnik liczb 4 410, 24 255, 20 790 i 137 655.

Rozwiązanie:

Na wstępie dokonamy rozkładu podanych liczb na czynniki pierwsze.

4 410	2	24 255	3	20 790	2	137 655	3
2 205	3	8 085	3	10 395	3	45 885	3
735	3	2 695	5	3 465	3	15 295	5
245	5	539	7	1 155	3	3 059	7
49	7	77	7	385	5	437	19
7	7	11	11	77	7	23	23
1		1		11	11	1	
				1			

Następnie zaznaczamy wspólne czynniki.

4 410	2	24 255	3	20 790	2	137 655	3
2 205	3	8 085	3	10 395	3	45 885	3
735	3	2 695	5	3 465	3	15 295	5
245	5	539	7	1 155	3	3 059	7
49	7	77	7	385	5	437	19
7	7	11	11	77	7	23	23
1		1		11	11	1	
				1			

Na koniec mnożymy zaznaczone liczby przez siebie.

$$NWD(4410, 24255, 20790, 137655) = 3 \cdot 3 \cdot 5 \cdot 7 = 315$$

Definicja 3. [6] Najmniejszą wspólną wielokrotnością liczb a i b ($a,b \in \mathbb{N}_+$) nazywamy najmniejszą liczbę naturalną różną od 0 dzielącą się bez reszty zarówno przez a jak i b (ozn. $NWW(a,b)$).

Definicja 4. [5] Niech $x_1, x_2, ..., x_n$ będą dodatnimi liczbami naturalnymi. Najmniejszą wspólną wielokrotnością tych liczb nazywamy najmniejszą liczbę naturalną różną od 0 dzielącą się bez reszty przez każdą z liczb x_i, $i \in \{1, 2, ..., n\}$. Oznaczamy ją przez $NWW(x_1, x_2, ..., x_n)$.

Algorytm 2. (*Algorytm wyznaczania NWW*) Niech $x_1, x_2, ..., x_n \in \mathbb{N}_+$.

1) Każdą liczbę naturalną x_i ($i \in 1, 2, ..., n$) rozkładamy na czynniki pierwsze.
2) Jako tymczasową wartość NWW przyjmujemy x_1.
3) Z rozkładów pozostałych liczb wykreślamy te czynniki, które występują w rozkładzie pierwszej liczby.
4) Tymczasową wartość NWW mnożymy przez nieskreślone czynniki z rozkładu drugiej liczby i skreślamy je z rozkładów kolejnych liczb.
5) Punkt 4 powtarzamy dla pozostałych liczb, aż do ich wyczerpania. Otrzymujemy wtedy z wartości tymczasowej ostateczny wynik.

Algorytmy 1 i 2 zostały napisane na podstawie wiadomości zawartych w podręcznikach szkolnych [1, 2] oraz na stronie internetowej [6].

Przykład 2. Obliczmy najmniejszą wspólna wielokrotność liczb 4 410, 24 255, 20 790 i 137 655.

Rozwiązanie:

Wykorzystamy rozkład liczb z przykładu 1.

4 410	2	24 255	3	20 790	2	137 655	3
2 205	3	8 085	3	10 395	3	45 885	3
735	3	2 695	5	3 465	3	15 295	5
245	5	539	7	1 155	3	3 059	7
49	7	77	7	385	5	437	19
7	7	11	11	77	7	23	23
1		1		11	11	1	
				1			

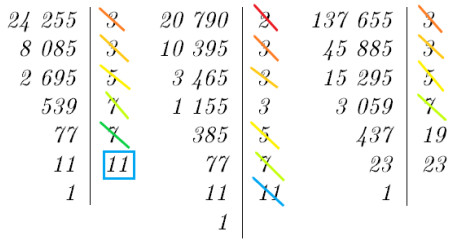
Tymczasowe NWW oznaczamy jako x. W pierwszym kroku mamy więc $x = 4410$.

Teraz czas na pierwsze wykreślanie.

4 410	2	24 255	3	20 790	2	137 655	3
2 205	3	8 085	3	10 395	3	45 885	3
735	3	2 695	5	3 465	3	15 295	5
245	5	539	7	1 155	3	3 059	7
49	7	77	7	385	5	437	19
7	7	11	11	77	7	23	23
1		1		11	11	1	
				1			

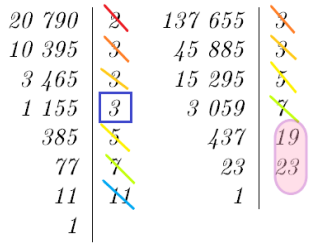
W rozkładzie drugiej liczby pozostała nam już tylko jeden czynnik, mnożymy więc x przez niego. Otrzymujemy teraz $x = 4410 \cdot 11 = 48510$.

Przechodzimy do kolejnego kroku.



Po dalszym wykreśleniu w rozkładzie trzeciej liczby została tylko jedna liczba 3. Stąd x wynosi teraz $48510 \cdot 3 = 145530$.

Zostało już tylko ostatnie wykreślanie.



Aby otrzymać ostateczną wartość NWW mnożymy dotychczasowy x przez wszystkie pozostałe czynniki z rozkładu ostatniej liczby. W wyniku końcowym otrzymujemy NWW równą $145530 \cdot 19 \cdot 23 = 63596610$.

2. Podejście akademickie

Z innym ujęciem tego tematu spotykamy się na studiach, kiedy definicje tych samych pojęć stają się bardziej sformalizowane.

Definicja 5. [3] Niech $a, b \in \mathbb{Z}$, przy czym $a \neq 0$ lub $b \neq 0$. Największym wspólnym dzielnikiem liczb a i b nazywamy liczbę całkowitą $d \geqslant 1$, która spełnia następujące warunki:

— $d|a$ i $d|b$,

— dla każdej liczby całkowitej c takiej, że $c|a$ i $c|b$ spełniony jest warunek $c|d$.

Największy wspólny dzielnik liczb a i b oznaczamy przez $NWD(a,b)$ lub (a,b).

Definicja 6. [3] Niech $a, b \in \mathbb{Z}$, przy czym $a \neq 0$ i $b \neq 0$. Najmniejszą wspólną wielokrotnością liczb a i b nazywamy liczbę całkowitą $m \geqslant 1$, która spełnia następujące warunki:

— $a|m$ i $b|m$

— dla każdej liczby całkowitej c takiej, że $a|c$ i $b|c$ spełniony jest warunek $m|c$.

Najmniejszą wspólną wielokrotność liczb a i b oznaczamy przez $NWW(a,b)$ lub $[a,b]$.

Możemy zauważyć, iż prawdziwe są następujące równości: $(|a|,|b|) = (a,b)$ oraz $[|a|,|b|] = [a,b]$. Dlatego w dalszych rozważaniach założymy, że $a, b \in \mathbb{N}$.

Rozpatrzmy teraz sytuację, gdy jedna z liczb jest zerem. W takim przypadku NWD równa się drugiej liczbie, a NWW zgodnie z definicją nie istnieje.

Zarówno największy wspólny dzielnik, jak i najmniejsza wspólna wielokrotność posiadają własność przemienności argumentów.

$$(a,b) = (b,a) \qquad \text{oraz} \qquad [a,b] = [b,a]$$

Załóżmy więc, że $a \geqslant b > 0$.

Wszystkie powyższe definicje i fakty w łatwy sposób można przenieść na większą liczbę argumentów.

Zanim przejdziemy do algorytmu obliczania NWD zaproponowanego przez Euklidesa, przytoczmy jeszcze pewien lemat.

Lemat 1. [3] *Niech $a, b, q, r \in \mathbb{N}$ oraz niech $a \neq 0$ lub $b \neq 0$.*
Jeśli $a = qb + r$, to $(a,b) = (b,r)$.

Algorytm 3. (Euklidesa) [3] W algorytmie zakładamy, że $a \geqslant b$.

1. Dzielimy a przez b:

$$a = bq_1 + r_1, \quad q_1, r_1 \in \mathbb{Z}, \quad 0 \leqslant r_1 < b.$$

2. Jeśli $r_1 = 0$, to $(a,b) = b$.
3. Jeśli $r_1 \neq 0$, to dzielimy b przez r_1:

$$b = r_1 q_2 + r_2, \quad q_2, r_2 \in \mathbb{Z}, \quad 0 \leqslant r_2 < r_1.$$

4. Jeśli $r_2 = 0$, to $(a,b) = (b,r_1) = r_1$.
5. Jeśli $r_2 \neq 0$, to dzielimy r_1 przez r_2:

$$r_1 = r_2 q_3 + r_3, \quad q_3, r_3 \in \mathbb{Z}, \quad 0 \leqslant r_3 < r_2.$$

6. Postępujemy analogicznie, aż do otrzymania zerowej reszty.
7. Na końcu otrzymujemy ciąg równości

$$(a,b) = (b,r_1) = (r_1,r_2) = ... = (r_{n-1},r_n) = r_n.$$

Powyższy algorytm musi się zakończyć, ponieważ mamy do czynienia z malejącym ciągiem liczb naturalnych, większych od zera: $r_1 > r_2 > ... > r_n \geqslant 0$.

Na koniec tej części przytoczymy jeszcze twierdzenie wykorzystywane do wyznaczania najmniejszej wspólnej wielokrotności, będące także wstępem do rozważań przedstawionych w następnym rozdziale. Zainteresowanych dowodem tego twierdzenia odsyłam do książki *Elementarna teoria liczb* W. Marzantowicz i P. Zarzycki.

Twierdzenie 1. [3] *Jeżeli* $a,b \in \mathbb{N}$, *to* $(a,b) \cdot [a,b] = a \cdot b$.

Przykład 3. Za pomocą algorytmu Euklidesa obliczamy NWD i NWW liczb 4 410, 24 255, 20 790 i 137 655.

Rozwiązanie:

Algorytm Euklidesa zdefiniowany jest jedynie dla dwóch liczb, dlatego nasze rozwiązanie trzeba podzielić na etapy.
Pamiętając, że prawdziwe są równości $(a,b,c,d) = ((a,b),(c,d))$ oraz $[a,b,c,d] = [[a,b],[c,d]]$ mamy:

$$(4410, 24255, 20790, 137655) = ((4410, 24255), (20790, 137655))$$

oraz

$$[4410, 24255, 20790, 137655] = [[4410, 24255], [20790, 137655]].$$

(i) Obliczymy $(4410, 24255)$. Pamiętając o warunku $a \geqslant b$ mamy $a = 24255$, $b = 4410$.
   a) Dzielimy a przez b.

$$24255 = 4410 \cdot 5 + 2205.$$

   b) Otrzymaliśmy $r_1 = 2205 \neq 0$, więc prowadzimy dalsze rachunki.
   c) Teraz dzielimy b przez r_1.

$$4410 = 2205 \cdot 2 + 0.$$

   d) $r_2 = 0$, dlatego kończymy algorytm otrzymując

$$(4410, 24255) = r_1 = 2205.$$

(ii) Korzystając z lematu 1, dostaniemy $[4410, 24255]$.

$$(4410, 24255) \cdot [4410, 24255] = 4410 \cdot 24255,$$

$$[4410, 24255] = \frac{4410 \cdot 24255}{(4410, 24255)},$$

$$[4410, 24255] = \frac{4410 \cdot 24255}{2205} = 48510.$$

(iii) Analogicznie jak w punkcie (i) wyznaczamy wartość NWD dla liczb 20 790 i 137 655.

$$137655 = 20790 \cdot 6 + 12915, \quad r_1 = 12915 \neq 0,$$

$$20790 = 12915 \cdot 1 + 7875, \quad r_2 = 7875 \neq 0,$$

$$12915 = 7875 \cdot 1 + 5040, \quad r_3 = 5040 \neq 0,$$

$$7875 = 5040 \cdot 1 + 2835, \quad r_4 = 2835 \neq 0,$$

$$5040 = 2835 \cdot 1 + 2205, \quad r_5 = 2205 \neq 0,$$

$$2835 = 2205 \cdot 1 + 630, \quad r_6 = 630 \neq 0,$$

$$2205 = 630 \cdot 3 + 315, \quad r_7 = 315 \neq 0,$$

$$630 = 315 \cdot 2 + 0, \quad r_8 = 0 \Rightarrow (20790, 137655) = r_7 = 315.$$

(iv) Następnie obliczymy $[20790, 137655]$.

$$[20790, 137655] = \frac{20790 \cdot 137655}{(20790, 137655)} = \frac{20790 \cdot 137655}{315} = 9085230.$$

(v) Przejdziemy do obliczenia największego wspólnego dzielnika wszystkich liczb.

$$(4410, 24255, 20790, 137655) = (2205, 315).$$

Ponownie wykorzystujemy algorytm Euklidesa.

$$2205 = 315 \cdot 7 + 0, \quad r_1 = 0 \Rightarrow (2205, 315) = 315,$$

$$(4410, 24255, 20790, 137655) = (2205, 315) = 315.$$

(vi) Pozostało jedynie znalezienie NWW wszystkich liczb.
Musimy więc obliczyć $([4410, 24255], [20790, 137655])$.
a) $([4410, 24255], [20790, 137655]) = (48510, 9085230) =?$

$$9085230 = 48510 \cdot 187 + 13860, \quad r_1 = 13860 \neq 0,$$

$$48510 = 13860 \cdot 3 + 6930, \quad r_2 = 6930 \neq 0,$$

$$13860 = 6930 \cdot 2 + 0, \quad r_3 = 0 \Rightarrow (48510, 9085230) = r_2 = 6930.$$

b) $[4410, 24255, 20790, 137655] = [[4410, 24255], [20790, 137655]]$
$= [48510, 9085230] =?$

$$[48510, 9085230] = \frac{48510 \cdot 9085230}{(48510, 9085230)} = \frac{48510 \cdot 9085230}{6930} = 63596610.$$

Odp. *Tak więc NWD(4 410, 24 255, 20 790, 137 655) wynosi 315, natomiast NWW(4 410, 24 255, 20 790, 137 655) wynosi 63 596 610.*

3. Nowe rezultaty

W tej części zostaną przedstawione twierdzenia będące wynikiem spostrzeżeń autorki dotyczących zależności występujących między $(n_1,\ldots,n_k)$ i $[n_1,\ldots,n_k]$, dla $k \geqslant 2$. Zanim jednak przejdziemy do wypowiedzi i dowodów tych twierdzeń, przytoczymy kilka potrzebnych faktów.

Twierdzenie 2. *(zasadnicze twierdzenie arytmetyki)* [4] *Każdą liczbę naturalną $n > 1$ można przedstawić jednoznacznie w postaci iloczynu liczb pierwszych*

$$n = p_1 \cdot \ldots \cdot p_k,$$

przy czym $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$, $p_i \in \mathbb{P}$.

Wniosek 1. [4] *Każdą liczbę całkowitą $n \neq 0$ można zapisać jednoznacznie w postaci*

$$n = \varepsilon \prod_{p \in \mathbb{P}} p^{\alpha_p(n)},$$

przy czym $\varepsilon \in \{-1,1\}$, $\alpha_p(n) \in \mathbb{N}$. Występujący we wzorze iloczyn zawiera jedynie skończenie wiele czynników różnych od jedności.

Dowód powyższego twierdzenia, jak i wniosku, można znaleźć w książce W. Narkiewicza [4].

Wniosek 1 został wykorzystany w dowodach twierdzeń 3 i 4.

Lemat 2. *Dla dowolnych liczb rzeczywistych $a,b,c \in \mathbb{R}$ zachodzi następująca równość:*

$$\min(a,b)+\min(a,c)+\min(b,c)-a-b-c = \min(a,b,c)-\max(a,b,c)$$

Dowód. Bez zmniejszenia ogólności możemy przyjąć, że między liczbami występuje następująca zależność:

$$a \leqslant b \leqslant c.$$

Otrzymujemy wtedy następujący ciąg równości:

$$\min(a,b)+\min(a,c)+\min(b,c)-a-b-c = a+a+b-a-b-c$$

$$= a-c = \min(a,b,c)-\max(a,b,c)$$

Tak więc z lewej strony wzoru z lematu 2 otrzymaliśmy jego prawą stronę co kończy dowód.

Dla innych uporządkowań liczb a,b,c dowód przebiega analogicznie. □

Twierdzenie 3. *Dla $a, b, c \in \mathbb{N}_+$ ma miejsce równość:*

$$\frac{(a,b,c)}{[a,b,c]} = \frac{(a,b)(a,c)(b,c)}{abc}. \tag{1}$$

Dowód. Bez zmniejszania ogólności rozważań możemy przyjąć, że $a \leqslant b \leqslant c$. Niech ściśle rosnący ciąg $p_1, p_2, p_3, ..., p_n$ będzie ciągiem wszystkich liczb pierwszych, nie większych niż c.

Liczby a, b i c przedstawiamy w postaci iloczynu liczb pierwszych:

$$a = \prod_{i=1}^{n} p_i^{a_i}, \qquad b = \prod_{i=1}^{n} p_i^{b_i}, \qquad c = \prod_{i=1}^{n} p_i^{c_i}, \qquad \text{gdzie } a_i, b_i, c_i \in \mathbb{N}. \tag{2}$$

Wykorzystując równości (2) otrzymujemy:

$$abc = \prod_{i=1}^{n} p_i^{a_i} \cdot \prod_{i=1}^{n} p_i^{b_i} \cdot \prod_{i=1}^{n} p_i^{c_i} = \prod_{i=1}^{n} p_i^{a_i+b_i+c_i} \tag{3}$$

$$(a,b,c) = \prod_{i=1}^{n} p_i^{\min(a_i,b_i,c_i)}, \tag{4}$$

$$(a,b) = \prod_{i=1}^{n} p_i^{\min(a_i,b_i)}, \tag{5}$$

$$(a,c) = \prod_{i=1}^{n} p_i^{\min(a_i,c_i)}, \tag{6}$$

$$(b,c) = \prod_{i=1}^{n} p_i^{\min(b_i,c_i)}, \tag{7}$$

$$[a,b,c] = \prod_{i=1}^{n} p_i^{\max(a_i,b_i,c_i)}. \tag{8}$$

Powołując się na prawdziwość lematu 2 otrzymujemy poniższe przekształcenie.

$$\begin{aligned}\frac{(a,b)(a,c)(b,c)}{abc} &= \frac{\prod_{i=1}^{n} p_i^{\min(a_i,b_i)} \cdot \prod_{i=1}^{n} p_i^{\min(a_i,c_i)} \cdot \prod_{i=1}^{n} p_i^{\min(b_i,c_i)}}{\prod_{i=1}^{n} p_i^{a_i+b_i+c_i}} \\ &= \prod_{i=1}^{n} p_i^{\min(a_i,b_i)+\min(a_i,c_i)+\min(b_i,c_i)-a_i-b_i-c_i} \\ &= \prod_{i=1}^{n} p_i^{\min(a_i,b_i,c_i)-\max(a_i,b_i,c_i)} = \frac{\prod_{i=1}^{n} p^{\min(a_i,b_i,c_i)}}{\prod_{i=1}^{n} p^{\max(a_i,b_i,c_i)}} \\ &= \frac{(a,b,c)}{[a,b,c]}.\end{aligned}$$

□

Niech $k,n \in \mathbb{N}_+$ oraz $k \leqslant n$. Niech $I_n = \{1,2,...,3\}$ będzie zbiorem indeksów, a $\{i_1,i_2,...,i_k\} \subset I_n$ jego dowolnym uporządkowanym ($i_1 < i_2 < ... < i_k$) k-elementowym podzbiorem .
Dla dowolnych liczb $x_1,x_2,...,x_n \in \mathbb{N}_+$ wprowadzimy oznaczenie

$$M_k(n) = \prod_{\{i_1,i_2,...,i_k\} \subset I_n} (x_{i_1},x_{i_2},...,x_{i_k}),$$

gdzie iloczyn jest po wszystkich możliwych k-elementowych podzbiorach zbioru I_n, a $(x_{i_1},x_{i_2},...,x_{i_k})$ oznacza największy wspólny dzielnik liczb $x_{i_1},x_{i_2},...,x_{i_k}$.

Przykładowo dla $k = 1$ otrzymujemy iloczyn wszystkich liczb:

$$M_1(n) = \prod_{i=1}^{n} x_i,$$

a gdy $k = n$ dostajemy ich największą wspólną wielokrotność:

$$M_n(n) = (x_1,x_2,...,x_n).$$

Twierdzenie 4. *Niech $n \in \mathbb{N} \setminus \{0,1\}$. Do obliczenia najmniejszej wspólnej wielokrotności n liczb można wykorzystać następujące wzory:*

1^o *dla parzystego n*

$$[x_1, x_2, ..., x_n] = \prod_{k=1}^{\frac{n}{2}} \frac{M_{2k-1}(n)}{M_{2k}(n)}, \tag{9}$$

2^o *dla nieparzystego n*

$$[x_1, x_2, ..., x_n] = M_n(n) \cdot \prod_{k=1}^{\frac{n-1}{2}} \frac{M_{2k-1}(n)}{M_{2k}(n)}. \tag{10}$$

Dowód. Przyjmijmy oznaczenie $x = \max\{x_1, x_2, ..., x_n\}$.
Niech rosnący ciąg $p_1, p_2, ..., p_m$ zawiera wszystkie liczby pierwsze nie większe niż x. Liczby x_i $(i = 1, 2, ..., n)$ przedstawimy w postaci iloczynu liczb pierwszych w następujący sposób:

$$x_i = \prod_{j=1}^{m} p_j^{x_{i,j}}, \qquad \text{gdzie} \qquad x_{i,j} \in \mathbb{N}. \tag{11}$$

Elementy każdego ciągu $x_{1,j}, x_{2,j}, ..., x_{n,j}$ przypisane liczbie pierwszej p_j (dla $j = 1, 2, ..., m$) ustawiamy w porządku niemalejącym i oznaczamy następująco:

$$z_{1,j} \leqslant z_{2,j} \leqslant ... \leqslant z_{n,j}. \tag{12}$$

Następnie przedstawiamy $[x_1, x_2, ..., x_n]$ i $M_k(n)$ w postaci iloczynu liczb pierwszych:

$$[x_1, x_2, ..., x_n] = \prod_{j=1}^{m} p_j^{\max(x_{1,j}, x_{2,j}, ..., x_{n,j})} = \prod_{j=1}^{m} p_j^{z_{n,j}}. \tag{13}$$

$$\begin{aligned} M_k(n) &= \prod_{\{i_1, i_2, ..., i_k\} \subset I_n} (x_{i_1}, x_{i_2}, ..., x_{i_k}) \\ &= \prod_{\{i_1, i_2, ..., i_k\} \subset I_n} \left(\prod_{j=1}^{m} p_j^{\min(x_{i_1,j}, x_{i_2,j}, ..., x_{i_k,j})} \right) \\ &= \prod_{j=1}^{m} \left(\prod_{\{i_1, i_2, ..., i_k\} \subset I_n} p_j^{\min(x_{i_1,j}, x_{i_2,j}, ..., x_{i_k,j})} \right). \end{aligned} \tag{14}$$

Korzystając z tego, iż zarówno $x_{i,j}$ jak i $z_{i,j}$ reprezentują ten sam zbiór, a my prowadzimy iloczyn po wszystkich k-elementowych podzbiorach tego zbioru, otrzymujemy równoważny wzór:

$$\begin{aligned} M_k(n) &= \prod_{j=1}^{m} \left(\prod_{\{i_1,i_2,\ldots,i_k\}\subset I_n} p_j^{\min(z_{i_1,j},z_{i_2,j},\ldots,z_{i_k,j})} \right) \\ &= \prod_{j=1}^{m} \left(\prod_{\{i_1,i_2,\ldots,i_k\}\subset I_n} p_j^{z_{i_1,j}} \right) \end{aligned} \tag{15}$$

Zauważamy teraz, że

$$\prod_{\{i_1,i_2,\ldots,i_k\}\subset I_n} p_j^{z_{i_1,j}} = \underbrace{p_j^{z_{1,j}} \cdot \ldots \cdot p_j^{z_{1,j}}}_{d_{1,j,k}} \cdot \underbrace{p_j^{z_{2,j}} \cdot \ldots \cdot p_j^{z_{2,j}}}_{d_{2,j,k}} \cdot \ldots \cdot \underbrace{p_j^{z_{n-k+,j}} \cdot \ldots \cdot p_j^{z_{n-k+1,j}}}_{d_{n-k+1,j,k}}$$

$$= p_j^{d_{1,j,k}\cdot z_{1,j}+d_{2,j,k}\cdot z_{2,j}+\cdots+d_{n-k+1,j,k}\cdot z_{n-k+1,j}},$$

gdzie $d_{l,j,k}$ oznacza liczbę wszystkich podzbiorów $(i_1,i_2,\ldots,i_k)\subset I_n$ spełniających warunek $i_1 = l$, $l = 1,2,\ldots,n-k+1$.

Zgodnie z wzorami kombinatorycznymi, wszystkich k-elementowych podzbiorów zbioru indeksów I_n spełniających warunek $i_1 = 1$, jest

$$\binom{n-1}{k-1},$$

natomiast spełniających warunek $i_1 = 2$ jest

$$\binom{n-2}{k-1}.$$

Kontynuując to rozumowanie otrzymamy współczynniki $d_{l,j,k}$, które będą stały przy liczbach $z_{l,j}$ w dalszym rozwinięciu wzoru (15). Wzór, który określa postać tych współczynników można zapisać następująco:

$$d_{l,j,k} = \binom{n-l}{k-1} \qquad \text{dla } l \leqslant n-k+1$$

Ze względu na to, że wartość tego współczynnika nie zależy od j możemy zamiast oznaczenia $d_{l,j,k}$ użyć zapisu $d_{l,k}$.
Ostatecznie $M_k(n)$ ma postać:

$$M_k(n) = \prod_{j=1}^{m} p_j^{d_{1,k}z_{1,j}+d_{2,k}z_{2,j}+\ldots+d_{n-k+1,k}z_{n-k+1,j}}. \tag{16}$$

Korzystając z wzoru (16) mamy:

1^o dla parzystego n

$$\prod_{k=1}^{\frac{n}{2}} \frac{M_{2k-1}(n)}{M_{2k}(n)} = \prod_{k=1}^{\frac{n}{2}} \frac{\prod_{j=1}^{m} p_j^{d_{1,2k-1}z_{1,j}+d_{2,2k-1}z_{2,j}+\ldots+d_{n-2k+2,2k-1}z_{n-2k+2,j}}}{\prod_{j=1}^{m} p_j^{d_{1,2k}z_{1,j}+d_{2,2k}z_{2,j}+\ldots+d_{n-2k+1,2k}z_{n-2k+1,j}}}$$

$$\prod_{j=1}^{m} p_j^{s_{1,j}z_{1,j}+s_{2,j}z_{2,j}+\ldots+s_{n,j}z_{n,j}}, \tag{17}$$

gdzie

$$s_{i,j} = \sum_{k=1}^{\frac{n}{2}} (d_{i,2k-1} - d_{i,2k}) = \sum_{k=1}^{\frac{n}{2}} \left(\binom{n-i}{2k-2} - \binom{n-i}{2k-1} \right)$$

$$= \sum_{k=0}^{n-i} (-1)^k \binom{n-i}{k}; \tag{18}$$

2^o dla nieparzystego n

$$M_n(n) \cdot \prod_{k=1}^{\frac{n-1}{2}} \frac{M_{2k-1}(n)}{M_{2k}(n)} = \prod_{j=1}^{m} p_j^{z_{1,j}} \cdot \prod_{k=1}^{\frac{n-1}{2}} \frac{\prod_{j=1}^{m} p_j^{d_{1,2k-1}z_{1,j}+d_{2,2k-1}z_{2,j}+\ldots+d_{n-2k+2,2k-1}z_{n-2k+2,j}}}{\prod_{j=1}^{m} p_j^{d_{1,2k}z_{1,j}+d_{2,2k}z_{2,j}+\ldots+d_{n-2k+1,2k}z_{n-2k+1,j}}}$$

$$= \prod_{j=1}^{m} p_j^{s_{1,j}z_{1,j}+s_{2,j}z_{2,j}+\ldots+s_{n,j}z_{n,j}}, \tag{19}$$

gdzie

$$s_{i,j} = d_{i,n} + \sum_{k=1}^{\frac{n-1}{2}} (d_{i,2k-1} - d_{i,2k}) = \binom{n-i}{n-1} + \sum_{k=1}^{\frac{n-1}{2}} \left(\binom{n-i}{2k-2} - \binom{n-i}{2k-1} \right)$$

$$= \sum_{k=0}^{n-i} (-1)^k \binom{n-i}{k}. \tag{20}$$

Zajmiemy się teraz wartościami zmiennych $s_{i,j}$. Najpierw rozważmy sytuację, gdy $i \neq n$. Z własności dwumianu Newtona mamy, że

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Jeśli w tym równaniu n zamienimy na $n-i$, to otrzymujemy, że

$$\sum_{k=0}^{n-i} (-1)^k \binom{n-i}{k} = 0.$$

Widzimy, że lewa strona równania to wzór na zmienne $s_{i,j}$. Stąd dla $i = 1,2,...,n-1$ zmienne $s_{i,j}$ się zerują.

Jeżeli $i = n$, to zmienne $s_{i,j}$ wyrażają się następującym wzorem:

$$s_{i,j} = s_{n,j} = \sum_{k=0}^{n-n} (-1)^k \binom{n-n}{k} = \sum_{k=0}^{0} (-1)^k \binom{0}{k} = (-1)^0 \binom{0}{0} = 1 \cdot 1 = 1.$$

Stąd mamy, że $s_{n,j} = 1$.

Podstawmy teraz wyznaczone wartości do równania (17).

$$\begin{aligned} \prod_{k=1}^{\frac{n}{2}} \frac{M_{2k-1}(n)}{M_{2k}(n)} &= \prod_{j=1}^{m} p_j^{s_{1,j}z_{1,j}+s_{2,j}z_{2,j}+...+s_{n,j}z_{n,j}} \\ &= \prod_{j=1}^{m} p_j^{0\cdot z_{1,j}+0\cdot\ z_{2,j}+...+0\cdot z_{n,j}+1\cdot z_{n,j}} \\ &= \prod_{j=1}^{m} p_j^{z_{n,j}} = [x_1, x_2, ..., x_n]. \end{aligned}$$

Analogicznie postępujemy z przypadkiem dla n nieparzystych, podstawiając te wartości do równania (19).

□

4. Podsumowanie

Praca pokazuje, że podejście uniwersyteckie do sposobu wyznaczania NWW za pomocą NWD można rozszerzyć na więcej argumentów. Dla dużych liczb ten sposób okazać się może znacznie prostszy, niż sposób wykorzystujący wyłącznie algorytm Euklidesa.

Dzięki rozkładowi liczb na czynniki pierwsze dostajemy łatwiejszy sposób znajdowania szukanych wartości. Można jednak korzystać także z wersji hybrydowych, łączących wykorzystanie algorytmu Euklidesa z rozkładem na liczby pierwsze i wykorzystaniem zależności między *największym wspólnym dzielnikiem* a *najmniejszą wspólną wielokrotnością* wielu liczb.

Literatura

[1] M. Braun, A. Mańkowska, M. Paszyńska, K. Wej, W. Babiański, E. Szytkiewicz, J. Janowicz, *Matematyka z kluczem. Klasa 7*, Wydawnictwo Nowa Era, Warszawa 2020

[2] Praca zbiorowa pod redakcją M. Dobrowolskiej, *Matematyka 8 z plusem*, Gdańskie Wydawnictwo Oświatowe, Gdańsk 2018

[3] W. Marzantowicz, P. Zarzycki, *Elementarna teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2012

[4] W. Narkiewicz, *Teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2003

[5] *Największy wspólny dzielnik, Największa wspólna wielokrotna* w: *Encyklopedia popularna*, wyd. 7, Wydawnictwo Naukowe PWN, Warszawa 1982, s. 501

[6] *Matematyka maksymalnie prosta*, https://www.matemaks.pl/, (stan w dniu 5.06.2020)

Dagmara Dudek[1]

Hipergrafy w modelowaniu

Streszczenie

Praca dotyczy problematyki matematycznego modelowania wybranych zagadnień z wykorzystaniem hipergrafów. Pierwsza część zawiera pojęcia wstępne z zakresu teorii hipergrafów. W części drugiej przedstawione zostały przykłady hipergrafów modelujących konkretne zagadnienia z zakresu chemii organicznej i sieci Petriego.

Słowa kluczowe: hipergraf, modelowanie cząsteczki chemicznej, sieć Petriego

Wstęp

Hipergrafy to struktury umożliwiające reprezentację złożonych systemów i relacji. Wykazują bardzo dużą siłę opisową, są uogólnieniem oraz rozszerzeniem tradycyjnych pojęć grafów i zbiorów skończonych. Teoria hipergrafów zaczęła się kształtować w ostatnich dziesięcioleciach. W 1973 roku francuski matematyk Claude Berge opracował monografię pt. „Grafy i hipergrafy" [2], w której sformalizował oraz ujednolicił podstawowe definicje związane z teorią hipergrafów.

Modelowanie z wykorzystaniem hipergrafów pozwala na analizę różnych zagadnień w wielu dziedzinach nauki i umożliwia znalezienie optymalnego rozwiązania związanych z nimi problemów. W modelu hipergrafu wierzchołki reprezentują elementy zbioru, a hiperkrawędzie odzwierciedlają właściwości różnych podzbiorów. Hipergrafy znajdują zastosowanie np. w matematyce, informatyce, telekomunikacji oraz socjologii [9].

W matematyce hipergrafy mogą służyć do opisu pewnych zbiorów. Na przykład wierzchołki hipergrafu opisują liczby naturalne od 1 do 100, a hiperkrawędzie reprezentują podzbiory liczb mających wspólny dzielnik większy niż 1. W informatyce wierzchołki hipergrafu odpowiadają zbiorowi cech, a hiperkrawędzie wyznaczają relacje pomiędzy danymi cechami. Hipergrafy w telekomunikacji mogą być wykorzystane do opisu sieci komórkowej w następujący sposób: wierzchołki hipergrafu odpowiadają telefonom komórkowym, a hiperkrawędzie wyznaczają komórki działające w tym samym czasie. W socjologii hipergrafy mogą służyć do opisu relacji zachodzących w społeczeństwie. Osoby są opisane przez wierzchołki hipergrafu, a relacje łączące te osoby przez hiperkrawędzie.

[1] Dagmara Dudek, studentka matematyki, Wydział Podstaw Techniki, Politechnika Lubelska

1. Pojęcia wstępne

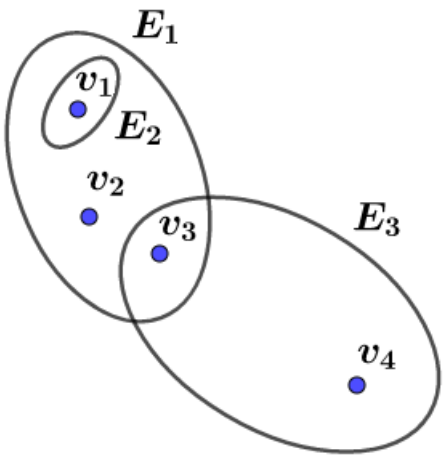
Definicja 1.1. [3] Parę zbiorów

$$H = (V,E) = (\{v_1, v_2, ..., v_p\}, \{E_1, E_2, ..., E_q\})$$

nazywamy hipergrafem, gdy E jest rodziną różnych i niepustych podzbiorów zbioru V. Elementy zbioru V nazywamy wówczas wierzchołkami hipergrafu H, a każdy zbiór E_k, $k = 1,2,...,q$, nazywamy krawędzią hipergrafu H.

Przykład hipergrafu H o czterech wierzchołkach i trzech hiperkrawędziach został pokazany na rysunku 1. Para zbiorów $H = (V,E)$ pokazana na rysunku 1 przedstawia się następująco:

$$H = (\{v_1, v_2, v_3, v_4\}, \{E_1, E_2, E_3\}),$$
$$V = \{v_1, v_2, v_3, v_4\},$$
$$E_1 = \{v_1, v_2, v_3\}, \;\; E_2 = \{v_1\}, \;\; E_3 = \{v_3, v_4\}$$



Rysunek 1. Przykład hipergrafu H
Źródło: Opracowanie własne

Definicja 1.2. [3] Wierzchołek v_i nazywa się incydentnym do krawędzi E_j, jeśli v_i należy do E_j.

Definicja 1.3. [3] Stopniem wierzchołka v_i nazywa się liczbę krawędzi incydentnych do wierzchołka v_i i oznacza jako $d_H(v_i)$.

Definicja 1.4. [3] Stopniem krawędzi E_j nazywa się liczebność zbioru wszystkich wierzchołków incydentnych do krawędzi E_j i oznacza jako $d_H(E_j)$.

Stopnie krawędzi hipergrafu pokazanego na rysunku 1 wynoszą: $d_H(E_1) = 3$, $d_H(E_2) = 1$ oraz $d_H(E_3) = 2$. Natomiast stopnie wierzchołków hipergrafu wynoszą: $d_H(v_1) = 2$, $d_H(v_2) = 1$, $d_H(v_3) = 2$ oraz $d_H(v_4) = 1$. Tradycyjny graf jest szczególnym przykładem hipergrafu, w którym wszystkie krawędzie są stopnia drugiego.

Definicja 1.5. [10] Grafem skierowanym nazywamy trójkę $G = (V,A,\gamma)$, gdzie V, A są zbiorami niepustymi i rozłącznymi. Natomiast γ: $A \to V \times V$ jest funkcją. Elementy zbioru V noszą nazwę węzłów grafu G, elementy zbioru A noszą nazwę łuków skierowanego grafu G.

Skończony hipergraf H o p wierzchołkach i q hiperkrawędziach jest jednoznacznie zdefiniowany przez macierz incydencji $B(H) = ||b_{ij}||$, gdzie $i = 1,\ldots,p$ oraz $j = 1,\ldots,q$, co można zapisać jako [3]:

$$b_{ij} = \begin{cases} 1 & \text{gdy } v_i \in E_j, \\ 0 & \text{gdy } v_i \notin E_j. \end{cases}$$

Macierz incydencji dla hipergrafu H z rysunku 1 przedstawia się następująco:

$$B(H) = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Więcej informacji na temat teorii grafów oraz hipergrafów można znaleźć w pozycjach [2, 8, 9].

2. Modelowanie cząsteczek chemicznych

Reprezentacja struktur molekularnych za pomocą grafów jest szeroko stosowana w chemii obliczeniowej i teoretycznych badaniach chemicznych. Grafy wykorzystuje się do reprezentowania cząsteczek, w których wierzchołki odpowiadają atomom, a krawędzie wiązaniom chemicznym. Taki rodzaj grafu nazywamy grafem molekularnym. Niestety, zwykłe grafy nie opisują odpowiednio wszystkich związków chemicznych. Najistotniejszą wadą zastosowania takiej metody modelowania

jest brak odpowiedniej reprezentacji cząsteczki, która posiada zdelokalizowane wiązania wielocentrowe. Związki metaloorganiczne są przykładem struktur, które posiadają co najmniej jedno wiązanie metal-węgiel, gdzie występują tzw. wiązania rozmyte. Zdarza się, że do modelowania takich struktur stosuje się niepołączone grafy molekularne. Niestety, taka metoda nie pozwala na analizę struktury jako całości, ponieważ nie ma połączenia pomiędzy poszczególnymi podgrafami prezentującymi oddzielnie elementy jednej cząsteczki. Lepiej ilustrujące, ale wciąż niepozbawione wad, są połączone grafy molekularne, w których wszystkie wierzchołki odpowiadające atomom węgla są połączone z „metalowym" wierzchołkiem, który odpowiada atomowi metalu. W takim grafie stopień „metalowego" wierzchołka jest równy liczbie połączonych krawędzi i niekoniecznie jest równy wartościowości atomu metalu.

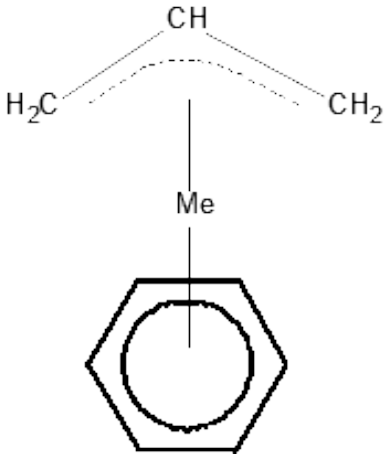
Wszystkie wspomniane powyżej wady reprezentacji cząsteczek są wyeliminowane, jeśli zastosuje się do ich modelowania hipergrafy.

2.1. Modelowanie cząsteczki za pomocą hipergrafu

Pierwsze związki, które obecnie nazywa się metaloorganicznymi, zostały odkryte w wieku XIX. W latach 50. XX wieku nastąpił intensywny rozwój chemii metaloorganicznej i od tego czasu odkryto oraz zbadano liczną grupę kompleksów metaloorganicznych. Kompleksy metaloorganiczne są częścią chemii organicznej. Związki metaloorganiczne zbudowane są z tzw. centrum metalicznego, którym może być pojedynczy lub kilka atomów metalu i z otaczających ten atom lub atomy ligandów, którymi są pojedyncze atomy niemetalu bądź rozmaite grupy organiczne oraz nieorganiczne [4].

Podrozdział prezentuje przykład modelowania cząsteczki kompleksu zawierającej ligand allilowy (trójwęglowy) oraz ligand sześcioelektronowy w postaci pierścienia. Zarówno w ligandzie allilowym, jak i w pierścieniu występują zdelokalizowane wiązania wielocentrowe.

Do tego celu posłużymy się hipergrafem molekularnym $H = (V,E)$, czyli hipergrafem, który reprezentuje strukturę F, w której wierzchołki należące do $V(H)$ odpowiadają pojedynczym atomom cząsteczki, hiperkrawędzie należące do $E(H)$ o stopniu większym niż 2 odpowiadają zdelokalizowanym wiązaniom wielocentrowym, a hiperkrawędzie o stopniu równym 2 odpowiadają zwykłemu wiązaniu kowalencyjnemu. Aby pokazać różnicę pomiędzy zwykłym wiązaniem kowalencyjnym a zdelokalizowanym wielocentrowym przyjęto, że hiperkrawędzie o stopniu równym dwa zostaną pokazane jako zwyczajne krawędzie. Rysunek 2 przedstawia schemat cząsteczki kompleksu z ligandem sześcioelektronowym i trójelektronowym ligandem allilowym z atomem metalu pomiędzy ligandami. Schemat cząsteczki został stworzony w programie ChemSketch.



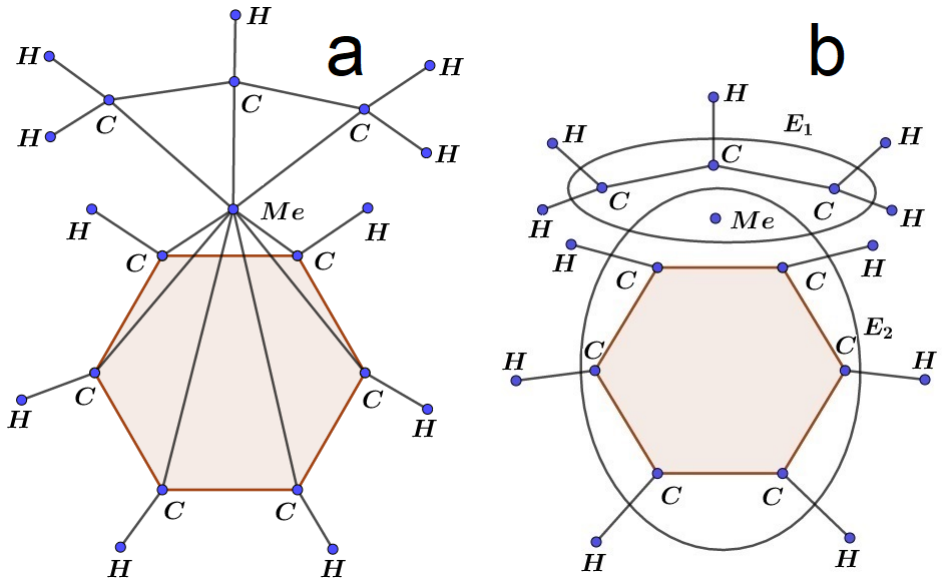
Rysunek 2. Schemat kompleksu metaloorganicznego zawierający dwa ligandy: ligand allilowy oraz sześcioelektronowy pierścień
Źródło: Opracowanie własne

Na rysunku 3 pokazano model reprezentacji cząsteczki w postaci grafu i hipergrafu tego samego kompleksu przedstawionego na rysunku 2.

W przypadku zwykłego grafu widocznego na rysunku 3 wiązania metal-ligand w kompleksie są przedstawione jako dziewięć krawędzi łączących wierzchołek odpowiadający metalowi *Me* z dziewięcioma innymi wierzchołkami reprezentującymi atomy węgla. Jak wspomniano wcześniej, nie odpowiada to rzeczywistej wartościowości atomu metalu. Jeśli do reprezentacji wykorzystany zostanie hipergraf, ta wada, która pojawia się przy grafie, zostanie wyeliminowana. Hiperkrawędzie E_1 i E_2 na rysunku 3 odpowiadają zdelokalizowanym wiązaniom π pomiędzy metalem i ligandami. Istotną zaletą takiej reprezentacji jest zachowanie wartościowości atomu metalu w kompleksie. Stopień wierzchołka, który odpowiada cząsteczce metalu jest równy dwa w przypadku hipergrafu. Można zauważyć, iż wartościowość atomów węgla również zostaje zachowana w przypadku hipergrafu. Dodatkową korzyścią wynikającą z reprezentacji kompleksu metaloorganicznego za pomocą hipergrafu jest wizualne zobrazowanie różnicy pomiędzy wiązaniem σ (węgiel-węgiel i węgiel-wodór) a wiązaniem π.

2.2. Metody prezentacji hipergrafu molekularnego

W pozycji [6] opisane są trzy metody reprezentacji hipergrafów molekularnych. Poniżej metody te zostaną przedstawione na przykładzie cząsteczki kompleksu metaloorganicznego pokazanego na rysunku 2.



Rysunek 3. Odpowiednio: a) graf i b) hipergraf cząsteczki pokazanej na rysunku 2
Źródło: Opracowanie własne

Metoda nr 1

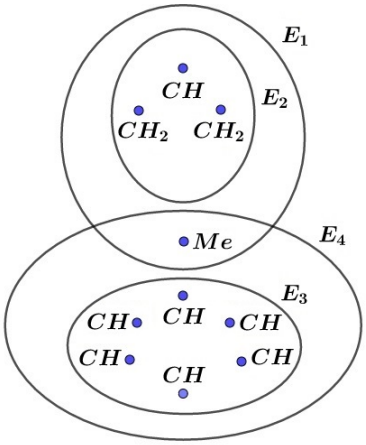
Struktury molekularne mogą być przedstawione jako hipergraf, w którym wierzchołki oraz hiperkrawędzie są oznaczone symbolicznie za pomocą liter. Rysunek 4 przedstawia hipergraf, w którym zbiór wierzchołków prezentuje się w postaci $V(H) = \{CH, CH_2, Me\}$, a zbiór krawędzi $E(H) = \{E_1, E_2, E_3, E_4\}$. Wierzchołki oznaczone są za pomocą symboli chemicznych atomów wchodzących w skład danego wierzchołka, czyli reprezentują całą grupę funkcyjną (tzn. CH lub CH_2).

Metoda nr 2

W metodzie nr 2 hiperkrawędzie reprezentować będą jedynie zdelokalizowane wiązania pomiędzy metalem i ligandami. Wierzchołki struktury molekularnej mogą być oznaczone numerycznie. Jako numeryczne oznaczenie wierzchołków można przyjąć całkowitą masę atomową pierwiastków wchodzących w skład danej grupy funkcyjnej tworzącej wierzchołek. Dla przykładu:

$$v(CH) = m_c + m_h = 12.01 + 1.01 = 13.02,$$

gdzie m_c odpowiada masie atomowej węgla, m_h masie atomowej wodoru. Masa Me będzie zależała od tego, jaki metal będzie wchodził w skład kompleksu. Dla przykładu można przyjąć, że będzie to atom żelaza o masie atomowej 55.85. Na



Rysunek 4. Hipergraf z wierzchołkami opisanymi zgodnie z metodą nr 1
Źródło: Opracowanie własne

rysunku 5 przestawiono ten sam hipergraf z wierzchołkami oznaczonymi w sposób numeryczny.

Metoda nr 3

Metoda ta nazywa się oznaczeniem strukturalnym. Wyróżnić można dwa rodzaje takiego oznaczenia:
— substytucja,
— transformacja.

Poniżej skupimy się na transformacji.

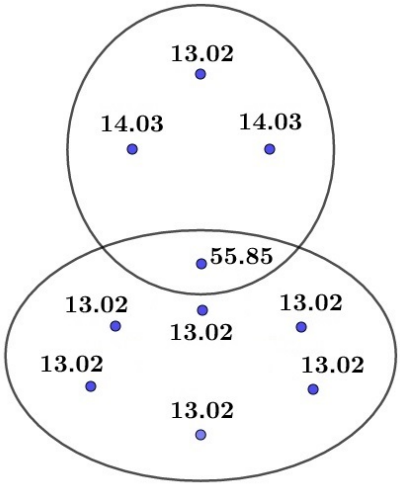
Definicja 2.1. [6] Transformacją γ skończonego zbioru elementów $X = \{1,\ldots,n\}$ nazywamy przekształcenie zbioru w siebie.

Transformację ogólnie można przedstawić jako:

$$\gamma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

gdzie $i_j \in \{1,\ldots,n\}$, $j = \{1,\ldots,n\}$. W przypadku tego przekształcenia dwa i więcej elementów ze zbioru X mogą być przekształcone w ten sam element.

Cząsteczkę z rysunku 2 z krawędziami opisanymi z wykorzystaniem transformacji przedstawia rysunek 6. Hipergraf ten posiada cztery krawędzie, więc transformacja jest określona na zbiorze $\{1,2,3,4\}$ zgodnie z zasadami:
— jeśli $v_i \in E_j$, to $\gamma(j) = j$,
— jeśli $v_i \notin E_j$, to $\gamma(j) = \min\{j_i\colon\ j_i \neq j\}$.



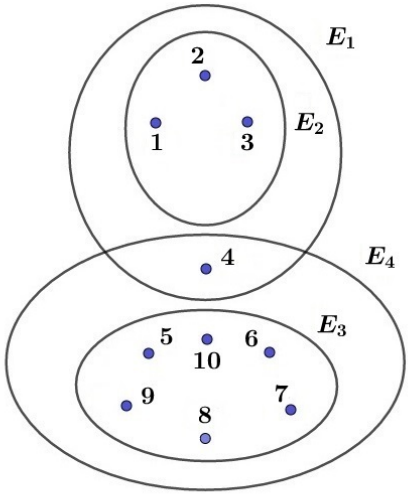
Rysunek 5. Hipergraf z wierzchołkami opisanymi zgodnie z metodą nr 2
Źródło: Opracowanie własne

Dla przykładu wierzchołek v_3 jest oznaczony jako transformacja $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 1 & 1 \end{pmatrix}$. Zgodnie z zasadą opisaną powyżej wierzchołek v_3 należy do E_1 więc 1 przekształca się w 1. Tak samo 2 przekształca się w 2, ponieważ v_3 jest incydentny do E_2. Wierzchołek v_3 nie należy do krawędzi E_3 i E_4, więc 3 i 4 przekształcają się w najmniejsze j różne odpowiednio od 3 i 4. Dlatego 3 i 4 przekształciły się w 1. Zgodnie z tą samą zasadą oznaczone zostały pozostałe wierzchołki hipergrafu.

Do komputerowej reprezentacji hipergrafów wykorzystuje się macierze incydencji pozwalające odpowiedzieć na pytanie, czy dane dwa hipergrafy są izomorficzne. Mówi się, że dwa hipergrafy są izomorficzne, jeśli istnieje bijekcja pomiędzy wierzchołkami hipergrafu H_1 a wierzchołkami hipergrafu H_2 taka, że jeśli dane dwa wierzchołki należą do hiperkrawędzi w jednym z hipergrafów, to odpowiadające im wierzchołki w drugim hipergrafie również należą do hiperkrawędzi.W celu rozstrzygnięcia czy dane dwa hipergrafy są izomorficzne, wykorzystuje się kanoniczną macierz sąsiedztwa. Jest to zagdanienie o wiele bardziej skomplikowane niż w przypadku klasycznych grafów. Więcej na temat tego procesu można przeczytać w pozycji [5].

3. Modelowanie sieci Petriego

Kolejną dziedziną, w której hipergrafy znajdują szerokie zastosowanie jest technika. Obecnie tworzone są coraz bardziej skomplikowane układy cyfrowe, co wymusza



$$V(H)=\left\{\begin{pmatrix}1&2&3&4\\1&2&1&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&1&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&1&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&1&1&4\end{pmatrix},\right.$$
$$\begin{pmatrix}1&2&3&4\\3&3&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&3&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&3&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&3&3&4\end{pmatrix},$$
$$\left.\begin{pmatrix}1&2&3&4\\3&3&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&3&3&4\end{pmatrix}\right\}$$

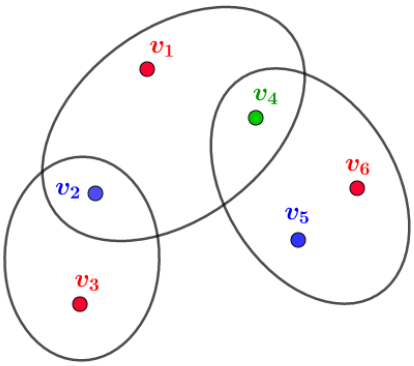
Rysunek 6. Reprezentacja wierzchołków hipergrafu w postaci transformacji
Źródło: Opracowanie własne

modyfikację powstałych już algorytmów w taki sposób, żeby abstrakcyjne modele w sposób intuicyjny oraz zwarty odzwierciedlały najważniejsze cechy projektowanych układów.

Częstym zjawiskiem podczas projektowania układów cyfrowych jest przekroczenie przez ten układ fizycznych możliwości dostępnego elementu. Sytuacja taka wymusza na projektancie wybór większego elementu cyfrowego albo wykorzystanie dekompozycji, czyli podział tego układu na kilka mniejszych podukładów. Liczne metody dekompozycji systemów dyskretnych wykorzystują do analizy układów cyfrowych tradycyjne grafy nieskierowane. Stosowanie hipergrafów do badań w technice cyfrowej wydaje się bardziej przejrzyste oraz efektywniejsze niż wykorzystanie grafów nieskierowanych.

W tej części pracy zostanie zaprezentowane wykorzystanie teorii hipergrafów do podziału sieci Petriego na moduły współbieżne, takie że każdy z modułów może być syntetyzowany oraz optymalizowany z zastosowaniem tradycyjnej teorii automatów cyfrowych. Opisana w rozdziale metoda dekompozycji nazywa się dekompozycją

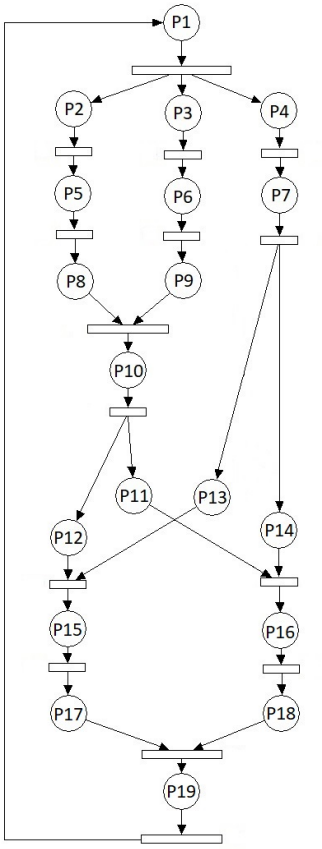
równoległą systemów dyskretnych, która będzie przeprowadzana z wykorzystaniem dekompozycji hipergrafów. W tym celu wykorzystane zostanie kolorowanie wierzchołkowe hipergrafów. Kolorowanie wierzchołkowe hipergrafu (tzw. silne kolorowanie hipergrafu) to przyporządkowanie każdemu wierzchołkowi hipergrafu jednego koloru tak, aby dwa sąsiadujące wierzchołki (czyli połączone hiperkrawędzią) nie posiadały takiego samego koloru. Przykład pokolorowanego hipergrafu przedstawia rysunek 7. Kolorowanie hipergrafu może odbywać się w oparciu o tzw. algorytmy zachłanne. Schemat takiego algorytmu został opisany w pozycji [7].



Rysunek 7. Przykład silnego kolorowania hipergrafu
Źródło: Opracowanie własne

Teoria sieci Petriego stworzona została przez Carla Adama Petriego. Obecnie sieci Petriego znajdują szerokie zastosowanie m.in. w informatyce, automatyce, analizie danych. Najczęściej omawianą siecią jest sieć Petriego zwyczajna, nazywana także siecią klasy pozycja/tranzycja. Do reprezentacji sieci wykorzystuje się skierowany graf dwudzielny, zawierający dwa typy węzłów połączonych łukami. Do węzłów zalicza się:
— miejsca – oznaczane jako okręgi;
— tranzycje – oznaczane jako prostokąty bądź kreski.
Przez sieć Petriego rozumie się trójkę $N = (P,T,D)$, gdzie:
— P to zbiór miejsc $|P| = m$;
— T to zbiór tranzycji $|T| = n$;
— D to macierz incydencji o wymiarze $m \times n$, która opisuje relacje zachodzące pomiędzy zbiorami miejsc i tranzycji.

Poniżej przedstawiono proces dekompozycji sieci przedstawionej na rysunku 8. Sieć Petriego została stworzona z wykorzystaniem programu „Symulator sieci Petriego" na podstawie pozycji [1]. Miejsca zostały przedstawione jako okręgi, tranzycje jako prostokąty, a strzałki odpowiadają łączącym je łukom.

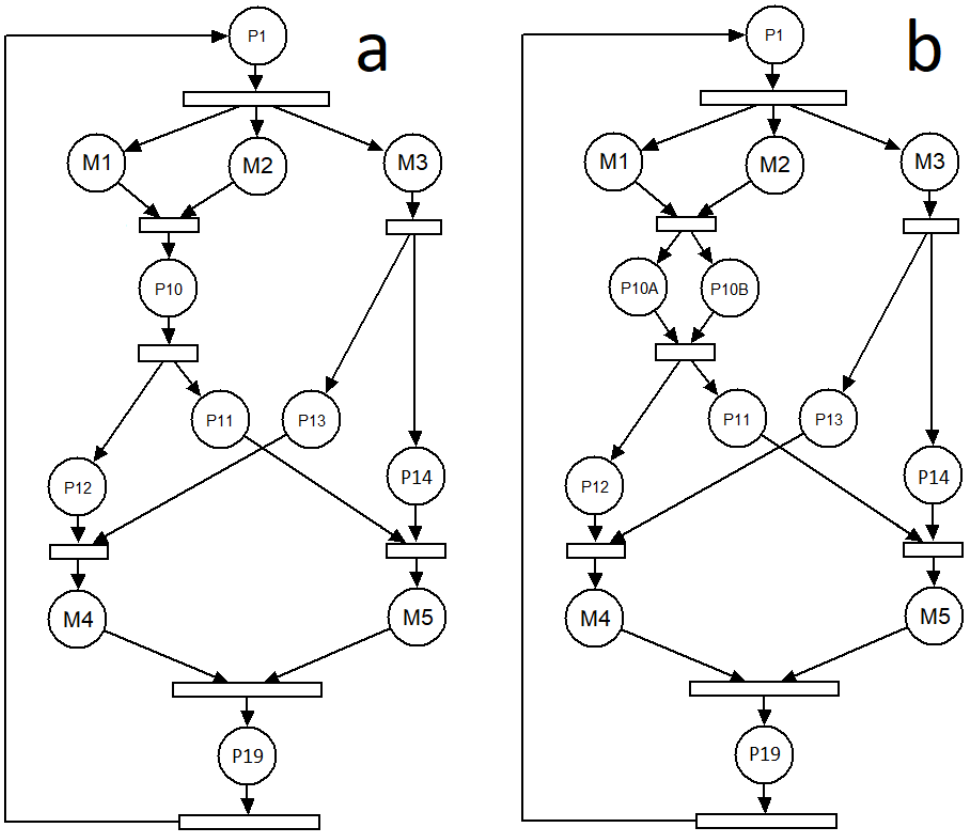


Rysunek 8. Sieć Petriego przedstawiająca algorytm sterowania
Źródło: Opracowanie własne na podstawie [1]

3.1. Konstrukcja makrosieci

Pierwszy etap ma na celu określenie makrosieci, czyli tzw. skondensowanej wersji tej samej sieci Petriego. Makrosieć zachowuje podstawową strukturę oraz własności sieci. Po wykonaniu tej operacji eliminowane są z sieci fragmenty sekwencyjne, czyli takie, które nie wpływają na ostateczny wynik procesu, a wydłużają jedynie jego czas trwania. Powstałe makromoduły posiadają tylko tranzycje wielowejściowe lub wielowyjściowe. Na rysunku 9a pokazano makrosieć utworzoną z sieci z rysunku 8. W makrosieci powstało pięć makromiejsc, przy czym:
— M_1 odpowiada miejscom P_2, P_5 oraz P_8;
— M_2 odpowiada miejscom P_3, P_6 oraz P_9;
— M_3 odpowiada miejscom P_4 oraz P_7;
— M_4 odpowiada miejscom P_{15} oraz P_{17};

— M_5 odpowiada miejscom P_{16} oraz P_{18}.



Rysunek 9. Sieć Petriego z rysunku 8 z makromiejscami (a) i makrosieć z rozszczepionym miejscem P_{10} (b)

Źródło: Opracowanie własne

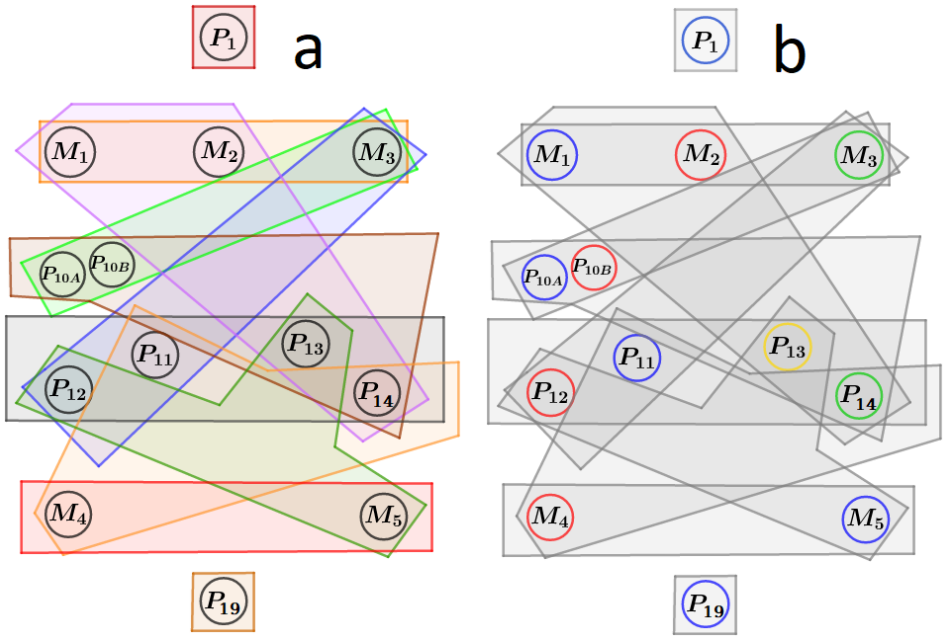
Aby możliwa była dalsza dekompozycja sieci, miejsce P_{10} zostało rozszczepione na dwa oddzielne miejsca: P_{10A} oraz P_{10B}. Takie rozszczepienie jest możliwe, ponieważ dwa sygnały lub procesy wchodzące do jednego urządzenia (bloku) są przetwarzane niezależnie oraz nie wchodzą ze sobą w interakcję. Rysunek 9b przedstawia sieć gotową do dalszego procesu dekompozycji z rozdzielonym miejscem P_{10}.

3.2. Wyznaczenie hipergrafu osiągalności

Drugim etapem modelowania jest wyznaczenie hipergrafu osiągalności na podstawie wcześniej wyznaczonej makrosieci. Hipergraf osiągalności wyznaczany jest

poprzez analizę kolejnych odpaleń sieci i zapisywanie kolejnych możliwych stanów układu. Wierzchołki hipergrafu oznaczają miejsca i makromiejsca sieci, a hiperkrawędzie wyznaczają zbiór miejsc i makromiejsc oznakowanych w poszczególnym stanie. Z analizy makrosieci z rysunku 9b wynika, że istnieje 11 możliwych stanów sieci. Wszystkie otrzymane podzbiory zbioru hiperkrawędzi hipergrafu z rysunku 10a przedstawiają się następująco:

$$\{\{P_1\},\{M_1,M_2,M_3\},\{M_1,M_2,P_{13},P_{14}\},\{P_{10A},P_{10B},M_3\},$$
$$\{M_3,P_{11},P_{12}\},\{P_{10A},P_{10B},P_{13},P_{14}\},\{P_{12},P_{11},P_{13},P_{14}\},$$
$$\{P_{12},P_{13},M_5\},\{P_{11},P_{14},M_4\},\{M_4,M_5\},\{P_{19}\}\}.$$



Rysunek 10. Hipergraf osiągalności wyznaczony dla makrosieci z rysunku 9b (a) oraz ten sam hipergraf z silnym kolorowaniem wierzchołków (b)
Źródło: Opracowanie własne

3.3. Kolorowanie wierzchołków hipergrafu

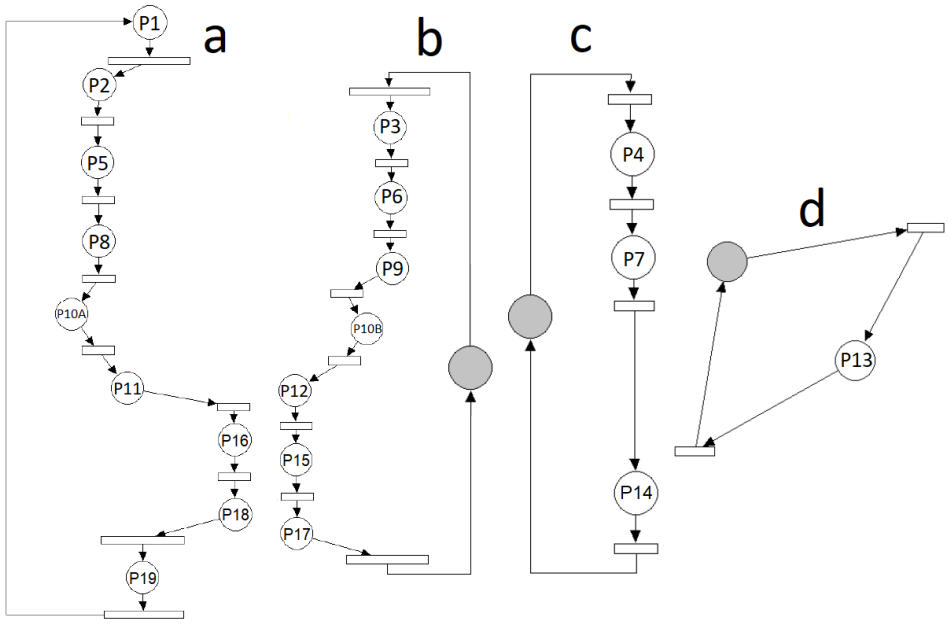
Silne kolorowanie wierzchołków hipergrafu będzie się odbywało w następujący sposób: dany kolor wyznaczać będzie zbiór miejsc lub makromiejsc niewspółbieżnych, czyli tzw. sekwencyjnych.

Hipergraf osiągalności z rysunku 10a został pokolorowany czterema kolorami. Pokolorowany hipergraf osiągalności przedstawia rysunek 10b. Kolor niebieski został przypisany do wierzchołków: $P_1, M_1, P_{10A}, P_{11}, M_5, P_{19}$. Kolorem czerwonym zostały oznaczone wierzchołki: $M_2, P_{10B}, P_{12}, M_4$. Kolor zielony przypisany został do M_3 oraz P_{14}. Wierzchołek P_{13} oznaczony został kolorem żółtym.

3.4. Dekompozycja sieci

Ostatnim krokiem jest dekompozycja sieci Petriego na podsieci typu automatowego. Każdy z kolorów przypisanych do wierzchołków hipergrafu wyznacza oddzielną podsieć. Sieć została podzielona na cztery niezależne podsieci. Utworzone nowe układy zostały pokazane na rysunku 11. W przypadku kiedy podsieć nie zawiera znakowania początkowego, do podsieci dodane jest tzw. miejsce spoczynkowe (na rysunkach oznaczone jako szare miejsce).

Zaprezentowana metoda dekompozycji upraszcza dalszy proces projektowania całego systemu. Wygodniej jest projektować kilka mniejszych sieci niż jedną dużą i złożoną. Nowo powstałe, mniejsze cztery podsieci mogą być dalej projektowane oraz analizowane niezależnie.



Rysunek 11. Podsieci typu automatowego otrzymane w wyniku procesu dekompozycji
Źródło: Opracowanie własne

4. Podsumowanie

Wykorzystanie hipergrafów w chemii jest korzystne w przypadku modelowania niektórych cząsteczek chemicznych, głównie z dziedziny chemii organicznej. W szczególności zastosowanie hipergrafów do modelowania cząsteczek posiadających zdelokalizowane wiązania wielocentrowe wykazuje szereg zalet. Do tych zalet można zaliczyć m.in.: zachowanie wartościowości wszystkich atomów wchodzących w skład danej cząsteczki (zarówno atomów metalu i atomów węgla) oraz prezentacja różnicy pomiędzy zwykłymi wiązaniami typu kowalencyjnego (węgiel-węgiel, węgiel-wodór) oraz wiązaniami zdelokalizowanymi (ligand-atom metalu).

Zaprezentowana w rozdziale metoda dekompozycji sieci Petriego na podsieci typu automatowego, wykorzystująca teorię hipergrafów, okazuje się bardzo istotnym zagadnieniem w projektowaniu układów cyfrowych. Silne kolorowanie wierzchołków hipergrafu pozwala na podział sieci na moduły współbieżne. Zdekomponowana sieć umożliwia uproszczenie procesu projektowania, ponieważ o wiele łatwiejsze jest projektowanie kilku mniejszych systemów cyfrowych posiadających mniejszą złożoność niż projektowanie jednej dużej sieci. Dodatkowo sama możliwość podziału sieci Petriego na mniejsze moduły świadczy o jej realnej możliwości implementacji sprzętowej.

Podsumowując, hipergrafy są stosunkowo nowym narzędziem w modelowaniu. Mimo to obecnie znajdują szerokie zastosowanie w wielu dziedzinach nauki, zarówno w naukach ścisłych jak i humanistycznych. Teoria hipergrafów wydaje się być dobrym uzupełnieniem w sytuacjach, kiedy nie da się zastosować do modelowania teorii grafów.

Literatura

[1] M. Adamski, M. Kołopieńczyk, K. Mielcarek, *Doskonała sieć Petriego w projektowaniu współbieżnych układów sterujących*, PAK, 2011, s. 656–660.
[2] C. Berge, *Graphs and Hipergraphs*, Mathematical Library, Amsterdam, 1976.
[3] A. Bretto, *Hypergraph Theory: An Introduction*, Springer, 2013.
[4] M. Cieślak-Golonka, J. Starosta, M. Wasilewski, *Wstęp do chemii koodrynacyjnej*, Wydawnictwo Naukowe PWN, Warszawa, 2013.
[5] E. V. Konstantinova, V. A. Skorobogatov, *Application of hypergraph theory in chemistry*, Discrete Mathematics, 2001, s. 365–383.
[6] E. V. Konstantinova, V. A. Skorobogatov, *Molecular structures of organoelement compounds and their representation as labeled molecular hypergraphs*, Journal of Structural Chemistry, 1998, s. 268–276.
[7] M. Kubale, P. Obszarski, K. Piwakowski, *Kolorowanie hipergrafów*, Zeszyty Naukowe Politechniki Śląskiej, 2006, s. 83–90.
[8] W. T. Tutte, *Graph Theory*, Cambridge University Press, 2001.
[9] V. Voloshin, *Introduction to Graph and Hypergraph Theory*, Nova Science Publishers, 2009.
[10] R. Wilson, *Wprowadzenie do teorii grafów*, PWN, 1999.

Marcin Dziadosz[1], **Matylda Jankowska**[2]

Liczby przestępne

Streszczenie

W pracy tej przedstawione zostały liczby przestępne, ich własności oraz wybrane przykłady. Szczegółowo opisane zostały liczba π oraz liczba e, czyli dwie najbardziej znane liczby przestępne. Praca zawiera również najważniejsze fakty historyczne dotyczące etapów odkrywania oraz badania tych liczb.

Słowa kluczowe: liczby przestępne, liczby niealgebraiczne, liczby Liouville'a

Wstęp

Liczba przestępna to liczba zespolona, która nie jest liczbą algebraiczną. Innymi słowy jest to liczba niealgebraiczna. Oznacza to, że nie jest pierwiastkiem żadnego niezerowego wielomianu o współczynnikach wymiernych. Najbardziej znanymi liczbami przestępnymi są liczba π oraz liczba e. [5]

Pomimo tego, że znanych liczb przestępnych jest mało, ponieważ dowiedzenie prawdziwości takiej tezy potrafi być bardzo trudne, liczby przestępne nie są zjawiskiem rzadkim. Tak naprawdę większość liczb rzeczywistych i zespolonych jest przestępna, gdyż liczby algebraiczne tworzą jedynie pewien przeliczalny zbiór, a zbiory liczb rzeczywistych i zespolonych są nieprzeliczalne, a więc większe od każdego zbioru przeliczalnego.

Wrażenie częstszego występowania liczb algebraicznych wynika z tego, że są one znacznie częściej wykorzystywane przez modele matematyczne, które często opisują zjawiska i procesy w sposób uproszczony. Ponadto, liczby rzeczywiste są o wiele łatwiejsze w interpretacji i operowaniu nimi.

Wszystkie rzeczywiste liczby przestępne są liczbami niewymiernymi, ponieważ wszystkie liczby wymierne są algebraiczne. Odwrotne stwierdzenie nie jest jednak prawdziwe – nie wszystkie liczby niewymierne są przestępne.

Dobrym przykładem jest pierwiastek kwadratowy z liczby 2 – jest to liczba niewymierna, ale nieprzestępna, bo jest pierwiastkiem równania wielomianowego $x^2 - 2 = 0$.

[1] Marcin Dziadosz, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

[2] Matylda Jankowska, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

Niewymierna liczba $\frac{1+\sqrt{5}}{2}$, zwana złotym stosunkiem i oznaczana symbolami φ lub ϕ, nie jest liczbą przestępną, bo jest pierwiastkiem równania algebraicznego $x^2 - x - 1 = 0$.

Historia

Liczbami przestępnymi interesowało się wielu znanych matematyków, na przykład Leibniz, który udowodnił, że $\sin x$ nie jest funkcją algebraiczną [1], czy chociażby Euler, który prawdopodobnie jako pierwszy zdefiniował liczby przestępne.

Johann Heinrich Lambert w swojej pracy z 1768 roku wysunął hipotezę, że liczby e i π są liczbami przestępnymi. Udało mu się udowodnić, że π jest liczbą niewymierną i sporządzić wstępny zarys dowodu przestępności tej liczby.

Jednak to Joseph'owi Liouville przypisuje się odkrycie tych liczb w 1844 roku. Liouville przedstawił przykład liczby – stałą Liouville'a, należącą do klasy liczb przestępnych, które można dobrze aproksymować przy pomocy liczb wymiernych.

W 1873 roku Charles'owi Hermite udało się udowodnić, że liczba e jest liczbą przestępną.

Georg Cantor w 1874 roku udowodnił, że zbiór liczb algebraicznych jest zbiorem przeliczalnym, a rzeczywistych nieprzeliczalnym, jak również przedstawił nową metodę konstruowania liczb przestępnych. Udowodnił także, że istnieje tyle liczb przestępnych, co rzeczywistych.

Dokładnie osiem lat później, Ferdinand von Lindemann dowiódł przestępności liczby π.

Liczby Liouville'a

W teorii liczb, liczba Liouville'a to taka liczba rzeczywista x, że dla dowolnej liczby naturalnej n istnieje nieskończenie wiele par liczb całkowitych (p,q), $q > 1$, względnie pierwszych i takich, że

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}.$$

Liczby Liouville'a, jak wspominaliśmy już wcześniej, mogą być oszacowane całkiem dokładnie za pomocą liczb wymiernych.

W 1844 roku Joseph Liouville pokazał, że wszystkie liczby Liouville'a są przestępne, udowadniając tym samym po raz pierwszy istnienie liczb przestępnych.

Teoria liczb przestępnych

Teoria liczb przestępnych to część teorii liczb, która bada liczby przestępne zarówno pod względem jakościowym, jak i ilościowym.

Zasadnicze twierdzenie algebry mówi nam, że jeśli mamy niezerowy wielomian dodatniego stopnia ze współczynnikami całkowitymi, to ten wielomian ma pierwiastek w zbiorze liczb zespolonych. Oznacza to, że dla dowolnego wielomianu W, ze współczynnikami całkowitymi, będzie istniała taka liczba zespolona z, że $W(z) = 0$.

Teoria liczb przestępnych zajmuje się następującym pytaniem: jeśli mamy daną liczbę zespoloną z, to czy istnieje taki wielomian W ze współczynnikami całkowitymi, że $W(z) = 0$? Jeśli taki wielomian nie istnieje, oznacza to, że liczba z jest przestępna.

Własności

— Zbiór liczb przestępnych jest nieprzeliczalny. Zbiór wielomianów o współczynnikach wymiernych, a także zbiór liczb algebraicznych, jest przeliczalny. Metoda przekątniowa Cantora dowodzi, że liczby rzeczywiste (a także liczby zespolone) są zbiorem nieprzeliczalnym. Liczby rzeczywiste składają się ze zbioru liczb algebraicznych oraz zbioru liczb przestępnych. Oba te zbiory nie mogą być więc przeliczalne. Dowodzi to, że zbiór liczb przestępnych jest nieprzeliczalny.

— Żadna liczba wymierna nie jest przestępna. Wszystkie liczby przestępne są niewymierne. Zbiór liczb niewymiernych zawiera wszystkie rzeczywiste liczby przestępne oraz podzbiór liczb algebraicznych.

— Jeśli argument dowolnej algebraicznej funkcji (niebędącej funkcją stałą) jednej zmiennej będzie przestępny, to jej wartość również będzie przestępna. Na przykład, wiedząc, że π jest liczbą przestępną, łatwo wywnioskować, że liczby typu 7π lub $\pi + 7$ są również przestępne.

— Wartość algebraicznej funkcji kilku zmiennych może jednak być liczbą algebraiczną, mimo tego, że jej argumenty są liczbami przestępnymi, jeśli argumenty te nie są algebraicznie niezależne. Przykładowo, zarówno π, jak i $7 - \pi$ są liczbami przestępnymi. Jednak ich suma $\pi + (7 - \pi) = 7$ jest liczbą algebraiczną.

— Nie wiadomo, czy liczba $e + \pi$ jest liczbą przestępną. Wiemy natomiast, że co najmniej jedna liczba ze zbioru $\{e + \pi; e\pi\}$ musi być liczbą przestępną. Dla dowolnych dwóch liczb przestępnych z_1 i z_2, przynajmniej jedna liczba ze zbioru $\{z_1 + z_2; z_1 z_2\}$ musi być przestępna. Rozważmy to na następującym przykładzie wielomianu: $(x - z_1)(x - z_2) = x^2 - (z_1 + z_2)x + z_1 z_2$. Jeśli obie liczby $(z_1 + z_2)$ i $z_1 z_2$ byłyby algebraiczne, to byłby to wielomian o współczynnikach algebraicznych. Ponieważ liczby algebraiczne tworzą ciało algebraicznie domknięte,

pierwiastki tego wielomianu z_1 i z_2 musiałyby być liczbami algebraicznymi. Dochodzimy do sprzeczności, a więc oznacza to, że przynajmniej jeden ze współczynników jest przestępny.

— Liczby, których nie można wyznaczyć z dowolną, pożądaną precyzją za pomocą pewnego skończonego algorytmu, są podzbiorem liczb przestępnych.

— Wszystkie liczby Liouville'a są przestępne, ale nie wszystkie liczby przestępne są liczbami Liouville'a.

Liczba π

Liczba π od wieków była obiektem zainteresowań wielu wybitnych matematyków. Starożytni Babilończycy określali π jako liczbę o wartości 3.

Już w III w. p.n.e. Archimedes otrzymał jej przybliżenie, wyznaczając długość obwodu dwóch 96-kątów foremnych, jednego opisanego na okręgu, drugiego wpisanego w ten okrąg, a wartość π obliczył jako średnią tych dwu długości. Oszacowanie $\frac{223}{71} < \pi < \frac{22}{7}$ jest dziełem Archimedesa. Ponieważ $\frac{223}{71} \approx 3,140845$ oraz $\frac{22}{7} \approx 3,142857$, to, w dzisiejszym języku, Archimedes oszacował wartość liczby π z dokładnością do dwóch cyfr po przecinku.

Aby uzyskać oszacowanie liczby π z dokładnością do czterech cyfr po przecinku, potrzeba było aż 600 kolejnych lat, po których chiński matematyk Liu Hui, używając metody Archimedesa, obliczył wartość π z pomocą wieloboku o 3072 kątach.

Ludolph Ceulen pracował całe życie nad wyznaczeniem oszacowania liczby π z jak największą dokładnością. Udało mu się otrzymać aż 35 cyfr po przecinku. Po jego śmierci ta część rozwinięcia liczby π dostała nawet, na jego cześć, nazwę „ludolfina".

Inny historyczny sposób wyznaczania przybliżonej wartości π polegał na wykorzystaniu słynnego zadania o igle Buffona. To jeden z pierwszych i najbardziej popularnych problemów prawdopodobieństwa geometrycznego, który został rozwiązany w 1777 roku. Nazwa ta pochodzi od George'a-Louisa Leclerca, hrabiego Buffon. Zagadnienie polegało na tym, że jeżeli rzucalibyśmy n razy igłą o długości l na podłogę z desek o szerokości t ($l \leqslant t$), to prawdopodobieństwo, że igła przetnie którąś z krawędzi deski wynosi $\frac{2l}{t\pi}$. Oznacza to, że można uzyskać przybliżoną wartość liczby π, rzucając igły na podłogę, następnie dzieląc liczbę przecięć krawędzi przez liczbę wszystkich rzutów igłą, a na końcu przyrównując otrzymany wynik do $\frac{2l}{t\pi}$. Oczywiście im więcej rzutów, tym większa jest dokładność uzyskanego przybliżenia. [4]

Ciekawostką jest wydarzenie z 1798 roku, kiedy to Napoleon podbił Egipt, a wraz z nim do tego kraju przybyli naukowcy, którzy zainteresowali się piramidą Cheopsa, zbudowaną w III w. p.n.e. Któryś z nich obliczył stosunek sumy długości

dwóch boków podstawy piramidy do jej wysokości i otrzymał wartość liczby π z dokładnością do czterech liczb po przecinku. [6] Wśród towarzyszących Napoleonowi naukowców był francuski inżynier, geograf i archeolog Edme-Francois Jomard, który we współpracy z innymi naukowcami określił, w tamtym momencie, że wysokość piramidy to 144 m. Oznaczałoby to, że długości boków podstawy piramidy musiałyby mierzyć około $226,19$ m, a biorąc pod uwagę fakt, iż według aktualnych pomiarów ta długość to 227 m, możemy ten wynik zakwestionować.

Również w przypadku problemu kwadratury koła, jednego z trzech największych problemów matematyki starożytnej Grecji, liczba π narobiła dużo kłopotu. Chodzi w nim o narysowanie przy pomocy linijki bez podziałki i cyrkla takiego kwadratu, którego pole jest równe polu danego koła. Obecnie wiadomo, że jest to niemożliwe, ponieważ π należy do zbioru liczb przestępnych.

Liczba e

Liczba e, zwana też liczbą Eulera lub Nepera, będąca podstawą logarytmu naturalnego, jest stałą matematyczną, wykorzystywaną w wielu dziedzinach matematyki i fizyki.

W odróżnieniu od liczby π, która była znana ludziom już w starożytności, liczba e pojawiła się dopiero w XVI wieku, za sprawą szkockiego matematyka Johna Nepera, który ułożył tablice logarytmów, pomocne przy skomplikowanych obliczeniach astronomicznych. Praca ta nie zawierała przybliżonej wartości liczby e, a jedynie wartości logarytmów na jej bazie. Liczbę e odkrył Jacob Bernoulli w 1683 roku, analizując wartości procentu składanego. Pierwsze udokumentowane wykorzystanie liczby e, oznaczanej jeszcze wtedy symbolem b, pojawiło się w latach 1690-1691. Wykorzystanie stałej znacząco rozwinął Leonhard Euler, nadając jej również znane nam dzisiaj oznaczenie symbolem e, co zresztą nie było wynikiem jakiejś szczególnej filozofii, a bardziej wykorzystania pierwszego lepszego znaku alfabetu.

Liczbę e definiujemy jako granicę

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n.$$

Liczba e jest liczbą niewymierną, otoczoną liczbami $2,71$ i $2,72$.

W 1873 roku Charles Hermite pokazał, że e jest przestępna (czyli niealgebraiczna). Była to pierwsza liczba przestępna, której nie trzeba było specjalnie konstruować by udowodnić jej przestępność.

Liczba e jest wykorzystywana w matematyce finansowej, np. w bankowości. Inwestując pewną sumę pieniędzy, przy z góry ustalonym procencie p, po n latach wartość zainwestowanego kapitału jest określona wzorem

$$x \cdot \left(1 + \frac{p}{100}\right)^n,$$

gdzie x to kwota zainwestowana. Może to być narzędzie do obliczania kolejnych przybliżeń liczby e.

Możemy wziąć pod uwagę kilka wariantów. Jeden z nich zakłada, że przewidujemy kapitalizację roczną i $p = 100$, a więc

$$V_1 = \left(1 + \frac{1}{1}\right)^1 = 2.$$

Analogicznie możemy definiować kolejne warianty, tzn.

$$V_2 = \left(1 + \frac{1}{2}\right)^2 = 2,25,$$

$$V_{12} = \left(1 + \frac{1}{12}\right)^{12} \approx 2,613,$$

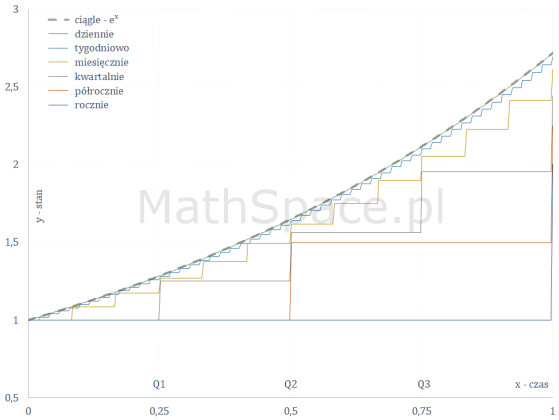
$$V_{365} = \left(1 + \frac{1}{365}\right)^{365} \approx 2,715,$$

$$V = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = e \approx 2,718,$$

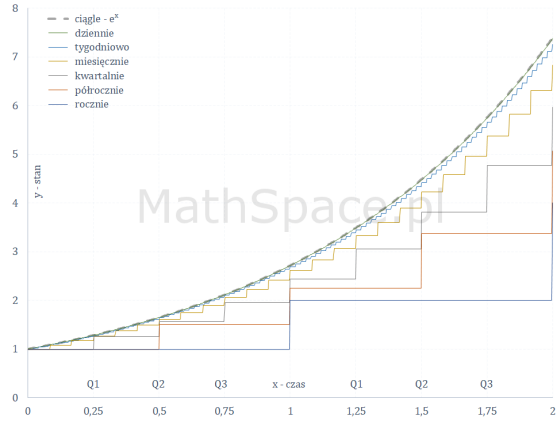
gdzie V_i, dla $i \in \{1,2,12,365\}$, oznaczają odpowiednio kapitalizację roczną, półroczną, miesięczną, dzienną, natomiast V to kapitalizacja ciągła.

Kapitalizacja ciągła jest granicznym przypadkiem kapitalizacji z procentem składanym w podokresach, gdy odsetki są dopisywane w sposób ciągły, a liczba podokresów zmierza do nieskończoności.

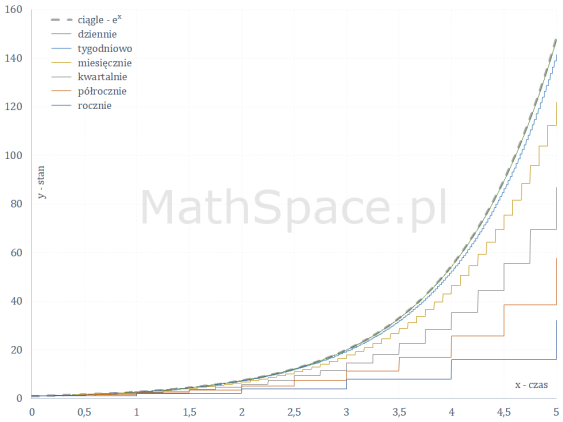
Na rysunkach 1, 2 oraz 3 znajdują się wykresy, ilustrujące wzrost wartości zainwestowanego kapitału $x = 1$ dla rocznej, półrocznej, kwartalnej, miesięcznej, tygodniowej i dziennej kapitalizacji odsetek dla rocznego, dwuletniego i pięcioletniego okresu oszczędzania. Im częstsza kapitalizacja, tym bardziej krzywa reprezentująca saldo jest „gładsza". Można również łatwo zauważyć, że wykres kapitalizacji ciągłej to w rzeczywistości funkcja e^x.



Rysunek 1. Wykres zmiany (wzrostu) wartości kapitału w okresie jednego roku dla różnych sposobów kapitalizacji odsetek
Źródło: MathSpace.pl



Rysunek 2. Wykres zmiany (wzrostu) wartości kapitału w okresie dwóch lat dla różnych sposobów kapitalizacji odsetek
Źródło: MathSpace.pl



Rysunek 3. Wykres zmiany (wzrostu) wartości kapitału w okresie pięciu lat dla różnych sposobów kapitalizacji odsetek
Źródło: MathSpace.pl

Przykłady liczb przestępnych

Zbiór znanych liczb przestępnych nie jest bardzo liczny. W dalszej części pracy podamy wybrane przykłady takich liczb. Dowody ich przestępności są w większości przypadków złożone i obszerne, dlatego ograniczamy się wyłącznie do zaprezentowania najbardziej znanych przykładów tych liczb, świadomie rezygnując z uzasadnienia ich przestępności. Celem tego podrozdziału jest jedynie wskazanie różnorodności tego zbioru.

— e^a, jeśli a jest liczbą algebraiczną i niezerową.
— π.
— Stała Liouville'a [7]

$$L = \sum_{n=1}^{\infty} 10^{-n!}.$$

— Stała Gelfonda e^{π}, a także $e^{-\pi/2} = i^i$, gdzie i to jednostka urojona. [9]
— a^b gdzie a jest liczbą algebraiczną, ale różną od 0 i 1, b zaś jest liczbą niewymierną i algebraiczną, na przykład: $2^{\sqrt{2}}$, nazywane stałą Gelfonda-Schneidera lub liczbą Hilberta. [10]
— $\sin a$, $\cos a$, $\operatorname{tg} a$, $cosec\, a$, $\sec a$, $\operatorname{ctg} a$ i ich hiperboliczne odpowiedniki dla dowolnej niezerowej algebraicznej liczby a, wyrażonej w radianach.
— Liczba rzeczywista x, która jest rozwiązaniem równania $\cos x = x$ (x jest wyrażone w radianach i nazywa się punktem stałym funkcji cosinus), $x \approx 0,739085133$. [8]

— Stała Gaussa [3]

$$G \approx 0,8346268,$$

czyli odwrotność średniej arytmetyczno-geometrycznej liczb 1 oraz $\sqrt{2}$.

— $\ln a$, jeśli a jest liczbą algebraiczną, różną od 0 i 1.

— $W(a)$, jeśli a jest liczbą algebraiczną, niezerową dla dowolnej gałęzi funkcji W Lamberta (czyli funkcji wielowartościowej, odwrotnej do funkcji $f(w) = we^w$, gdzie w jest dowolną liczbą zespoloną, a e^w funkcją wykładniczą), na przykład: stała Ω, czyli $W(1)$.

— $\sqrt{x}_s = e^{W(\ln x)} = \frac{\ln x}{W(\ln x)}$, zdefiniowane przy pomocy funkcji W Lamberta, dla dowolnej liczby naturalnej jest albo liczbą całkowitą, albo liczbą przestępną.

— Stała Cahena [2]

$$C = \sum \frac{(-1)^i}{s_i - 1} = \frac{1}{1} - \frac{1}{2} + \frac{1}{6} - \frac{1}{42} + \frac{1}{1806} - ... \approx 0,64341054629,$$

czyli nieskończony szereg ułamków jednostkowych, z naprzemiennymi znakami, zdefiniowany przy pomocy ciągu Sylvestera (ciągu liczb całkowitych, w którym każdy element ciągu jest iloczynem wszystkich poprzednich wyrazów powiększonym o 1).

— Niektóre wartości funkcji gamma: $\Gamma(1/3)$, $\Gamma(1/4)$ oraz $\Gamma(1/6)$. [11]

Nierozwiązane zagadnienia dotyczące liczb przestępnych

Pomimo tego, że Aleksander Gelfond i Theodor Schneider udowodnili przestępność wielu liczb, istnieją nadal takie matematyczne stałe, o których nie wiadomo, czy są przestępne, czy nie. W pewnych przypadkach nie określono również, czy należą one do liczb wymiernych, czy niewymiernych.

Dużym problemem w teorii liczb przestępnych jest pokazanie, że pewien zbiór liczb jest algebraicznie niezależny (podzbiór S ciała L jest algebraicznie niezależny od podciała K, jeśli elementy S nie spełniają żadnego nietrywialnego równania wielomianowego o współczynnikach w K). Pokazanie, że pojedyncze elementy zbioru są przestępne nie dostarcza dużej ilości informacji. Wiemy na przykład, że liczby π i e są przestępne. Nie można jednak na tej podstawie stwierdzić, czy na przykład ich suma jest przestępna.

Istnieje również tak zwany problem tożsamościowy, który polega na trudności określenia czy dane wyrażenie jest równe 0.

Podsumowanie

Liczby przestępne to bardzo ciekawy i obszerny problem z zakresu teorii liczb. Chociaż przez lata liczbami niealgebraicznymi interesowało się bardzo wielu matematyków, do tej pory odkryto jedynie małą ich część. Ponadto, wciąż istnieje dużo nierozwiązanych problemów dotyczących tych liczb. Liczby przestępne to zagadnienie, które nadal wymaga wielu badań oraz analiz matematycznych.

Literatura

[1] N. Bourbaki, *Elements of the history of mathematics*, Springer, 1994
[2] J. L. Davison, J. O. Shallit, *Continued fractions for some alternating series*, Monatshefte für Mathematik, 1991
[3] S. R. Finch, *Mathematical constants*, Cambridge University Press, 2003
[4] J. Jakubowski, R. Sztencel, *Wstęp do teorii prawdopodobieństwa*, Warszawa, 2001
[5] W. Narkiewicz, *Teoria liczb*, Wydawnictwo Naukowe PWN, 2003
[6] R. Tadeusiewicz, *Fascynująca historia odkrywania liczby Pi*, Kurier Lubelski, 18.04.2019
[7] E. W. Weisstein, *Liouville's constant* from MathWorld - a Wolfram Web Resource, https://mathworld.wolfram.com/LiouvilleNumber.html, (dostęp 07.01.2021)
[8] E. W. Weisstein, *Dottie number* from MathWorld - a Wolfram Web Resource, https://mathworld.wolfram.com/DottieNumber.html, (dostęp 07.01.2021)
[9] E. W. Weisstein, *Gelfond's constant* from MathWorld - a Wolfram Web Resource, https://mathworld.wolfram.com/GelfondsConstant.html, (dostęp 07.01.2021)
[10] E. W. Weisstein, *Gelfond-Schneider constant* from MathWorld - a Wolfram Web Resource, https://mathworld.wolfram.com/Gelfond-SchneiderConstant.html, (dostęp 07.01.2021)
[11] G. V. Chudnovsky, *Algebraic independence of values of exponential and elliptic functions*, Inventiones Mathematicae, 1984

Alicja Hołowiecka [1]

Enigma (nie) do złamania

Streszczenie

Niniejszy rozdział przybliża historię i metody łamania szyfru Enigmy. Przedstawione są podstawowe pojęcia związane z kryptografią oraz definicje matematyczne dotyczące permutacji. Opisano proces rozwiązywania problemu szyfru Enigmy, zarówno od strony historycznej, jak i matematycznej. Podkreślony został wkład kryptologów polskich oraz brytyjskich. Krótko wspomniane są także losy zaangażowanych osób po wojnie.

Słowa kluczowe: Enigma, kryptologia, kryptografia, historia, szyfr

Wstęp

Złamanie kodu Enigmy to jeden z bardziej kontrowersyjnych punktów w historii XX wieku. Z powodów historycznych i politycznych, sprawa tego, kto i jak rozwiązał zagadkę tego szyfru, była szeroko dyskutowana przez wiele lat, i nadal nie jest w pełni jasna. W mojej pracy postaram się przybliżyć, jak działała najsłynniejsza na świecie maszyna szyfrująca oraz opowiedzieć o matematycznych metodach kryptoanalitycznych, wspominając także o historycznym tle tych wydarzeń.

1. Ogólnie o szyfrowaniu

Zanim przejdziemy do opowieści o Enigmie, warto krótko przybliżyć pojęcia związane z szyfrowaniem.

Szyfrem nazywamy funkcję matematyczną, która jest wykorzystywana do szyfrowania tekstu jawnego lub jego deszyfrowania [16].

Tekst jawny to wiadomość przed zaszyfrowaniem, a wiadomość zaszyfrowana to **szyfrogram**. Proces zamiany tekstu jawnego na szyfrogram nazywamy szyfrowaniem.

Szyfr nazywamy inaczej kryptograficznym **algorytmem szyfrującym**. Algorytmy szyfrujące możemy podzielić na algorytmy ograniczone oraz algorytmy z kluczem.

O **algorytmie ograniczonym** mówimy, jeżeli sama jego znajomość pozwala na odszyfrowanie szyfrogramu. Nie zapewnia on wysokiego poziomu bezpieczeństwa.

[1] Alicja Hołowiecka, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

Innym, nieco bardziej bezpiecznym rodzajem szyfrów są **algorytmy z kluczem**. Zazwyczaj stosujemy w nich dwa klucze: jeden do szyfrowania i drugi do deszyfrowania. Wyróżniamy dwa rodzaje takich algorytmów:

— **algorytmy symetryczne** – klucz deszyfrujący da się wyznaczyć na podstawie szyfrującego i odwrotnie;
— **algorytmy z kluczem publicznym** – klucz szyfrujący (nazywany także kluczem publicznym) jest inny niż klucz deszyfrujący (prywatny) i nie można wyznaczyć klucza deszyfrującego na podstawie znajomości klucza szyfrującego.

Historycznie szyfry musiały być na tyle proste, aby człowiek był w stanie zaszyfrować i odszyfrować wiadomość. Obecnie dzięki możliwościom komputerów szyfry mogą być znacznie bardziej skomplikowane.

1.1. Steganografia

Jeszcze przed pierwszymi przypadkami szyfrowania, stosowano **steganografię**, czyli starano się ukryć sam fakt prowadzenia komunikacji, a nie jej treść.

Pierwsze wzmianki o użyciu technik steganograficznych sięgają piątego wieku przed naszą erą. W 499 r. p.n.e. tyran Miletu Histiajos był przetrzymywany w Suzach przez króla perskiego. Chciał przekazać wiadomość do swojego zięcia w Milecie, aby ten rozpoczął powstanie przeciwko Persom. Aby nie wzbudzać podejrzeń przeciwników, Histiajos ogolił głowę swojemu słudze, wytatuował na niej wiadomość, a kiedy włosy odrosły, wysłał posłańca do Miletu. Tam ogolono mu głowę, odczytano wiadomość i rozpoczęto powstanie[10].

Z kolei w starożytnych Chinach wiadomości zapisywano na kawałkach jedwabiu, które następnie zwijano w ciasny rulonik, pokrywano woskiem i zmuszano gońców do ich połykania. Nie ma dokładnej informacji na temat tego, jak odbiorca odzyskiwał tak ukrytą wiadomość.

Poza tym już od czasów starożytnych stosowano atrament sympatyczny, to jest substancje, które są bezbarwne w momencie pisania lub bardzo szybko tracą barwę. Wiadomość można potem odczytać po podgrzaniu, w świetle ultrafioletowym lub przy użyciu odpowiednich substancji chemicznych [15].

Jedną z bliższych współczesności metod steganograficznych jest metoda mikrokropek, wynaleziona przez Niemców podczas drugiej wojny światowej. Polegała ona na użyciu urządzenia będącego połączeniem mikroskopu i aparatu fotograficznego. Dzięki niemu zdjęcia o wysokiej rozdzielczości można pomniejszyć do bardzo małych rozmiarów, np. kartkę A4 można pomniejszyć do rozmiaru kropki.

Pierwsze próby przesyłania wiadomości z pomocą mikrofotografii podejmowano już w 1871 r., kiedy to informacje udawało się pomniejszać do rozmiaru prostokąta 3cm x 4cm. Pomniejszanie zdjęć do rozmiaru kropki dawało jeszcze większe możliwości. Obecnie ta metoda jest wykorzystywana także komercyjnie, np. do

zabezpieczenia przed podrabianiem żetonów w kasynie, do znakowania cennych przedmiotów [13].

Steganografia umożliwiała zatem całkiem skuteczne ukrycie wiadomości. Jednakże jeśli wiadomość została odkryta, natychmiast była zrozumiała. Dlatego zaczęto się zastanawiać nad ukryciem także treści komunikatu. W ten sposób narodziła się kryptografia.

1.2. Kryptografia

Jednym z najstarszych i jednocześnie najprostszych szyfrów jest **szyfr podstawieniowy**. Polega on na tym, że każdy znak zastępujemy innym znakiem, np. literę *A* zastępujemy przez *P*, literę *B* przez *T* itd.

Najprostsza wersja tego algorytmu jest nazywana **szyfrem Cezara**. Polega ona na przesunięciu każdej z liter o taką samą liczbę pozycji, np. przy przesunięciu o 3 pozycje literę *A* zapisujemy jako *D*, literę *B* jako *E* i tak dalej. Ten szyfr nazwany jest na cześć Juliusza Cezara, który stosował w swojej korespondencji przesunięcie o jedną lub o trzy pozycje.

Wersja algorytmu podstawieniowego z przesunięciem o 13 jest nazywana **ROT13**. W alfabecie łacińskim, który ma 26 znaków, ROT13 ma taką własność, że jego dwukrotne zastosowanie pozwala wrócić do oryginalnej litery, tzn. ROT13(ROT13(x))=x.

Powyższe przykłady są prostymi szyframi podstawieniowymi. Wyróżniamy jeszcze kilka rodzajów szyfrów podstawieniowych, np. szyfr homofoniczny. Polega on na tym, że każdy znak tekstu jawnego jest zastępowany jednym z wielu przyporządkowanych mu znaków.

Na przykład, szyfr książkowy zazwyczaj polega na szyfrowaniu każdej litery za pomocą trzech liczb: numeru strony, numeru wiersza i numeru znaku w tym wierszu. Deszyfrowanie polega na znalezieniu odpowiednich liter w książce, która jest kluczem. Obie strony muszą uzgodnić dokładnie, jaka książka i które wydanie będzie używane. Główną wadą tego szyfru jest czasochłonność.

1.3. Kryptoanaliza

Szyfry podstawieniowe dawały się złamać za pomocą **kryptoanalizy statystycznej** – wystarczyło zbadać częstotliwość występowania liter w tekście (przykładowo dla języka angielskiego częstości prezentują się jak na rysunku 1).

Należy sprawdzić, z jaką częstotliwością występują litery w tekście zaszyfrowanym. Jeżeli zauważymy, że na przykład litera ”S” pojawia się w szyfrogramie najczęściej, to prawdopodobnie zastępuje ona literę ”E”, i tak dalej.

Letter	Percentage	Letter	Percentage
a	8.2	n	6.7
b	1.5	o	7.5
c	2.8	p	1.9
d	4.3	q	0.1
e	12.7	r	6.0
f	2.2	s	6.3
g	2.0	t	9.1
h	6.1	u	2.8
i	7.0	v	1.0
j	0.2	w	2.4
k	0.8	x	0.2
l	4.0	y	2.0
m	2.4	z	0.1

Rysunek 1. Częstość występowania liter w języku angielskim (źródło [5])

2. Pojęcia matematyczne

Do opisu Enigmy oraz sposobów łamania szyfru, którego używała, będą potrzebne pojęcia matematyczne związane z permutacjami. W tym rozdziale zostaną przypomniane najbardziej potrzebne z tych pojęć.

Permutacją nazywamy wzajemnie jednoznaczne przekształcenie pewnego zbioru na siebie [14]. Zbiór wszystkich permutacji zbioru X oznaczamy przez $S(X)$. Jeżeli $X = \{1,2,\ldots,n\}$ to zbiór wszystkich jego permutacji możemy oznaczyć przez S_n. Niech $\sigma \in S_n$. Wówczas permutację σ można zapisać jako

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix},$$

gdzie $a_i = \sigma(i)$ dla $i = 1,\ldots,n$.

Inaczej mówiąc, permutacja zbioru n-elementowego to dowolny n-elementowy ciąg utworzony ze wszystkich wyrazów tego zbioru. Liczba permutacji n-elementowego zbioru wynosi $n!$.

Zbiór $S(X)$ wraz z działaniem składania permutacji stanowi grupę nazywaną **grupą permutacji**.

Złożeniem permutacji $\sigma_1, \sigma_2 \in S(X)$ nazywamy permutację $\sigma_2 \circ \sigma_1 \in S(X)$ daną wzorem

$$(\sigma_2 \circ \sigma_1)(x) = \sigma_2(\sigma_1(x)) \text{ dla } x \in X.$$

Przykład złożenia permutacji:

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

Permutacją odwrotną do permutacji $\sigma\in S_n$, $\sigma\in S_n$, odwzorowującej wiersz górny na dolny, jest permutacja $\sigma^{-1}\in S_n$ odwzorowująca dolny wiersz na górny: aby uzyskać jej zapis, należy zamienić porządek wierszy i (dla wygody) uporządkować rosnąco kolumny. Przykład permutacji odwrotnej:

$$\text{Jeżeli } \sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \text{ to } \sigma^{-1}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}=\begin{pmatrix}2&1&3\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

Cyklem nazywamy permutację postaci

$$\begin{pmatrix}a_1&a_2&\dots&a_{k-1}&a_k&a_{k+1}&a_{k+2}&\dots&a_n\\a_2&a_3&\dots&a_k&a_1&a_{k+1}&a_{k+2}&\dots&a_n\end{pmatrix}.$$

W zapisie cyklu pomijamy te elementy permutacji, które są jej punktami stałymi. Uproszczony zapis powyższego cyklu wygląda następująco:

$$(a_1,a_2,\dots,a_k)$$

Przykładem cyklu jest permutacja

$$\begin{pmatrix}1&3&5&8&2&4&6&7\\3&5&8&1&2&4&6&7\end{pmatrix}=\begin{pmatrix}1&3&5&8\\3&5&8&1\end{pmatrix}=(1,3,5,8)$$

Każdą permutację można przedstawić jako złożenie k rozłącznych cykli, gdzie oczywiście $k<n!$. Przykład rozkładu na cykle:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&4&8&6&7&2&1&5\end{pmatrix}=\begin{pmatrix}1&3&8&5&7&2&4&6\\3&8&5&7&1&4&6&2\end{pmatrix}$$

$$=\begin{pmatrix}1&3&8&5&7&2&4&6\\3&8&5&7&1&2&4&6\end{pmatrix}\circ\begin{pmatrix}1&3&8&5&7&2&4&6\\1&3&8&5&7&4&6&2\end{pmatrix}$$

$$=\begin{pmatrix}1&3&8&5&7\\3&8&5&7&1\end{pmatrix}\circ\begin{pmatrix}2&4&6\\4&6&2\end{pmatrix}=(1,3,8,5,7)\circ(2,4,6)$$

Transpozycją nazywamy cykl długości 2.

3. Enigma

Rozdział ten przedstawia historię powstania, budowę i zasadę działania maszyny szyfrującej Enigma. Przedstawione zostaną również procedury szyfrowania używane przez niemieckie wojsko.

3.1. Historia i zasada działania

Zanim do użycia weszły maszyny szyfrujące, należało zachować równowagę między bezpieczeństwem szyfru a jego użytecznością. Na przykład, ciężko było korzystać z szyfru jednorazowego, który do każdej litery stosował inny szyfr podstawieniowy. Z kolei zwykły szyfr podstawieniowy był bardzo łatwy do złamania. Kompromisem był m. in. **szyfr Vigenere'a**, ale został on złamany w 1854 r. Z tego powodu szukano nowych metod szyfrowania.

Szyfrowanie za pomocą maszyny otworzyło możliwość używania większej ilości szyfrów podstawieniowych, jednocześnie szyfrogram był prosty do odszyfrowania – wystarczyło mieć odpowiednią maszynę. Najbardziej znana – niemiecka **Enigma** – została wyprodukowana w latach 20. XX w.

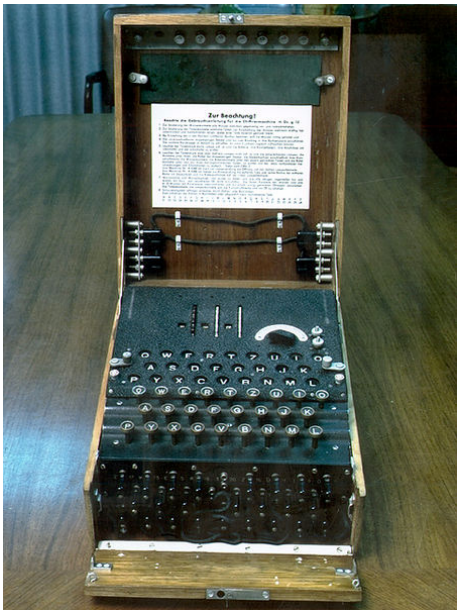
Produkcję maszyny szyfrującej Enigma rozpoczęto w roku 1918 w Niemczech w firmie Scherbius & Ritter. Była używana od lat 20. XX wieku, początkowo komercyjnie, a następnie także wojskowo. Artur Scherbius opatentował Enigmę w 1928 r. Co ciekawe, nie była to pierwsza maszyna szyfrująca oparta na mechanizmie wirników. Scherbius musiał najpierw w 1918 r. wykupić patent od holenderskiego wynalazcy Hugo Kocha.

Zaletą Enigmy było to, że nawet gdyby wróg posiadał maszynę, to kombinacji było tak wiele, że (jak się zdawało) niemożliwe było rozszyfrowanie wiadomości w rozsądnym czasie.

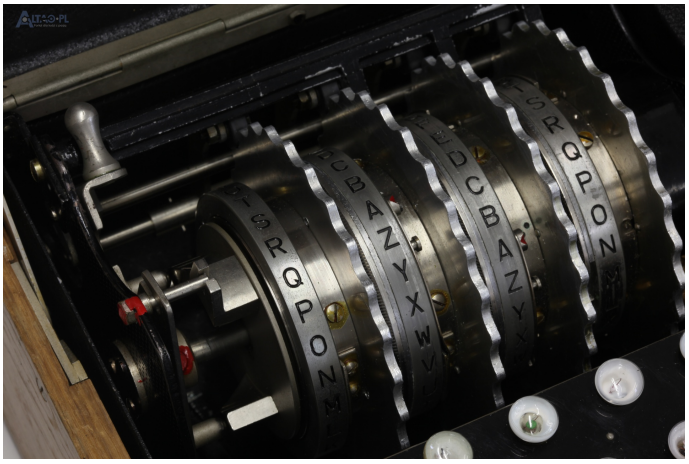
Z punktu widzenia szyfranta, obsługa tego urządzenia niewiele się różniła od pisania na maszynie. Należało wcisnąć klawisz z literą, którą chce się zaszyfrować. Powyżej klawiatury, podświetlał się zaszyfrowany odpowiednik tej litery. Deszyfrowanie wyglądało w ten sam sposób, należało jedynie mieć Enigmę z takimi samymi ustawieniami jak ta, która wcześniej zaszyfrowała wiadomość.

Enigmę zazwyczaj obsługiwały dwie osoby – jedna naciskała klawisze, a druga zapisywała szyfrogram. Zaszyfrowaną wiadomość wysyłano radiowo przy użyciu alfabetu Morse'a.

Podstawowa, komercyjna wersja Enigmy, składała się z klawiatury, trzech wirników i podświetlanego panelu z literami. Dookoła każdego wirnika znajdowało się 26 styków, każdy odpowiadający jednej literze alfabetu. Po każdym zaszyfrowaniu pojedynczej litery, prawy wirnik obracał się o 1/26 pełnego obrotu. Kiedy wykonał pełny obrót, wówczas środkowy wirnik obracał się o 1/26 obrotu. Podobnie lewy



Rysunek 2. Enigma (źródło: Wikipedia)

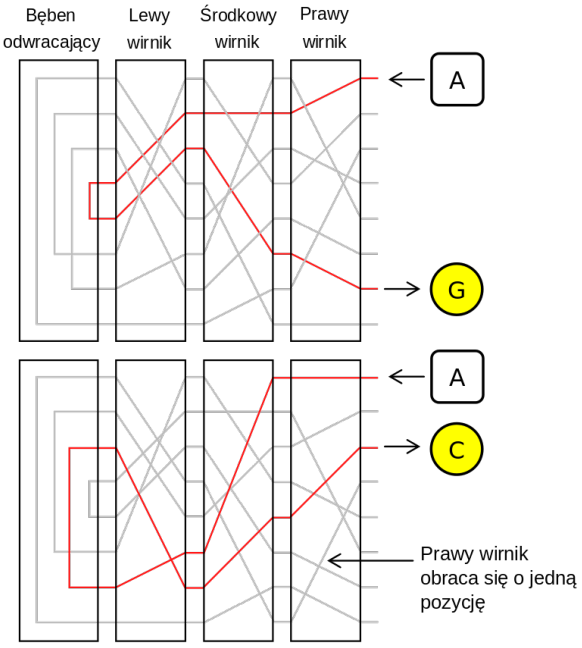


Rysunek 3. Wirniki Enigmy (źródło: Wikipedia)

wirnik obracał się o 1/26, kiedy środkowy wirnik zakończył pełny obrót. W ten sposób każda litera była szyfrowana za pomocą innego szyfru, a skoro każdy wirnik miał 26 możliwych pozycji, to w sumie uzyskujemy 26^3 możliwości.

Dodatkowo, 3 wirniki można było ustawić na 3! sposobów, tak więc liczbę 26^3 należałoby przemnożyć przez 6, co daje 105 456 możliwych położeń.

Impuls elektryczny przepływał przez 3 wirniki, a następnie trafiał do bębna odwracającego, który wysyłał go z powrotem, inną drogą. Ten sposób szyfrowania zapewniał symetryczność – szyfrogram dało się odszyfrować, mając Enigmę z dokładnie takimi samymi ustawieniami początkowymi.



Rysunek 4. Przepływ prądu w Enigmie – wersja bez łącznicy (źródło: Wikipedia)

Tak wyglądała komercyjna wersja Enigmy, dostępna publicznie (używano jej np. w bankach). Następnie stworzono wersję wojskową. Ogólna zasada działania nie różniła się od powyższej, a ulepszenia były tajne. Sposoby zdobycia tych informacji zostaną przedstawione w dalszych rozdziałach.

3.2. Enigma wojskowa

Zanim Enigma znalazła zastosowanie militarne, używano maszyn w wersji handlowej. Taka Enigma była produkowana parami: dane dwie maszyny miały identyczne ustawienia skrajnych, nieruchomych bębnów, więc tylko one były w stanie się ze sobą komunikować. Maszyny wojskowe wszystkie miały identyczne ustawienia bębna wstępnego oraz odwracającego, tak więc każda maszyna wojskowa mogła

się komunikować z każdą. Wersja wojskowa Enigmy posiadała także dodatkowy element w postaci łącznicy, gdzie dowolne dwie litery dało się połączyć kablem, co zwiększało poziom skomplikowania szyfru.

Budowa Enigmy wojskowej ulegała zmianom. Początkowo szyfranci mieli do dyspozycji 3 wirniki, a na łącznicy łączono 6 par liter. W ramach ulepszeń procesu szyfrowania, liczbę wirników w trakcie wojny zwiększono do 5 (z których wybierano 3 na każdy dzień), a liczba par na łącznicy wynosiła 8, a jeszcze później 10.

Na liczbę możliwych ustawień Enigmy składały się następujące czynniki:

— pierwszy rotor wybieramy z pięciu, potem drugi z czterech i trzeci z trzech, co daje $5 \cdot 4 \cdot 3$ lub w innym zapisie $\frac{5!}{(5-3)!}$;

— każdy z rotorów ma 26 możliwych pozycji wyjściowych, co daje 26^3;

— na łącznicy 20 z 26 liter można połączyć w pary na $\frac{26!}{(26-20)!}$ sposobów, ale kolejność łączenia w pary nie ma znaczenia (A połączone z B to to samo co B połączone z A), więc dla każdej pary trzeba by ten wynik podzielić przez 2, czyli dla 10 par dzielimy przez 2^{10}. Dodatkowo, nie ma znaczenia kolejność, w jakiej podłączymy 10 kabli, dlatego dzielimy przez 10!, co daje $\frac{26!}{(26-20)! \cdot 2^{10} \cdot 10!}$.

Ostatecznie mamy wynik

$$\frac{5!}{(5-3)!} \cdot 26^3 \cdot \frac{26!}{(26-20)! \cdot 2^{10} \cdot 10!} = 158\,962\,555\,217\,826\,360\,000$$

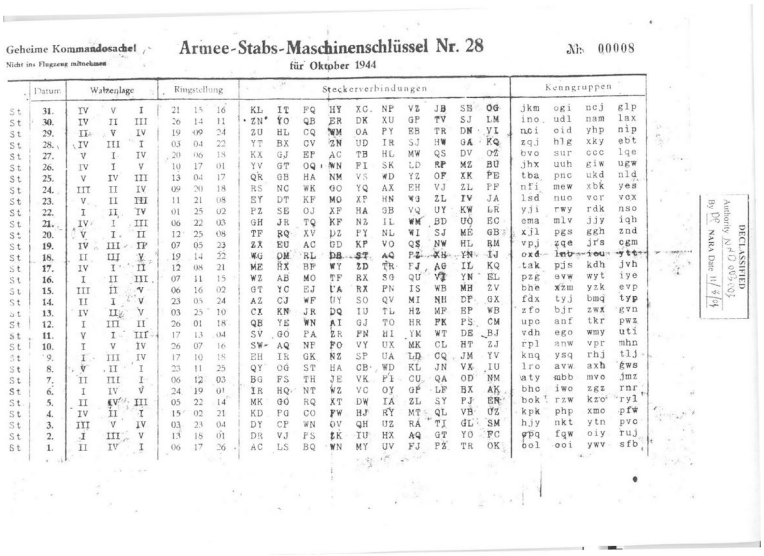
możliwych ustawień Enigmy, czyli ponad 158 kwadrylionów [7]. Liczba ta jest o tyle wątpliwa, że Niemcy często wprowadzali ulepszenia do militarnego modelu Enigmy, i pod koniec wojny być może tych ustawień było jeszcze więcej [3].

3.3. Procedury szyfrowania

Procedury szyfrowania zmieniały się wielokrotnie przed i podczas drugiej wojny światowej. Dla przykładu przedstawimy te, które były stosowane od roku 1938, a w rozdziale dotyczącym łamania kodu Enigmy będziemy wspominać, jakie procedury były aktualne w danym momencie.

Na dany kwartał wybierano kolejność bębenków ruchomych (które trzy z pięciu wirników będą używane i w jakiej kolejności, np. II, IV, I). Oprócz tego, każdego dnia należało inaczej ustawić wirniki, był to tzw. **klucz dzienny** (początkowe ustawienie wirników na dany dzień, np. *A*, *L*, *R*). Te informacje były podane w specjalnych tabelach wyłącznie do wiadomości niemieckiego wojska. Dla zwiększenia bezpieczeństwa, klucza dziennego używano w każdej depeszy tylko i wyłącznie po to, żeby

zaszyfrować kolejny klucz, tzw. **klucz indywidualny**, inny dla każdej depeszy. Były to trzy litery (indywidualne ustawienie początkowe), szyfrowane na początku każdej depeszy dwukrotnie, aby uniknąć niebezpieczeństwa pomyłki. Potem okazało się, że podwójne szyfrowanie klucza było błędem.



Geheime Kommandosache! Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

№ 00008

	Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
St	31.	IV V I	21 15 16	KL IT FQ HY XG NP VZ JB SB OG	jkm ogi ncj glp
St	30.	IV II III	26 14 11	ZN YO QB ER DK XU GP TV SJ LM	ino udl nam lnx
St	29.	II V IV	19 09 24	ZU HL CQ WM OA PY EB TR DW VI	noi oid yhp nlp
St	28.	IV III I	03 04 22	YT BX CV ZN UD IR SJ HW GA FQ	xqj hlg xky ebt
St	27.	V I IV	20 06 18	KX GJ EP AC TB HL MW QS DV OZ	bvo sur ccc lqe
St	26.	IV I V	10 17 01	YV GT OQ WN FI SK LD RP MZ BU	jhx uuh giw ugw
St	25.	V IV III	13 04 17	QR GB HA NM VS WD YZ OF XK PB	tba pnc ukd nld
St	24.	III II IV	09 20 18	RS NC WK GO YQ AX EH VJ ZL PF	nfi mew xbk yes
St	23.	V II III	11 21 08	EY DT KF MQ AT HN WJ ZL IV JA	lsd nuo vor vox
St	22.	I II IV	01 25 02	PZ SE OJ XF HA GB VQ UY KW LR	yji rwy rdk nso
St	21.	IV I III	06 22 03	GH JR TQ KF NS IL WM BD UQ EC	oma mlv jjy iqh
St	20.	V I II	12 25 08	TF RQ XV DZ FY NL WI SJ ME GB	xjl pgs gch znd
St	19.	IV III II	07 05 23	ZX EU AC DD KP VO QS NW HL RM	vpj zqe jrs egm
St	18.	II III V	19 14 22	WG OM RL DB ST AQ PZ XS YN IJ	oxd imp yeu ytt
St	17.	IV I II	12 08 21	ME BX BP WY ZD TR FJ AG IL KQ	tak pjs kdh jvh
St	16.	I II III	07 11 15	WZ AB MO TF RX SG QU VE YN EL	pzg eww wyt iye
St	15.	III II V	06 16 02	GT YC EJ UA RX PN IS WB MH ZV	bne xzm yzk evp
St	14.	II I V	23 05 24	AZ CJ WF UN SO QV MI NH DF GX	fdx tyj bmq typ
St	13.	IV III V	03 25 10	CX KN JR DQ TJ TL HZ MP EP WB	zfo bjr zwx gyn
St	12.	I III II	26 01 18	QB YE WN AI GJ TO HR FK PS CM	upo anf tkr pwz
St	11.	V I III	17 13 04	SV GO FA ZR FN HI YM WT DE BJ	vdh ego wmy uti
St	10.	I V IV	26 07 16	SW AQ NF FO VY UX MK CL HT ZJ	rpl anw vpr mhn
St	9.	I III IV	17 10 18	EH IR GK NZ SP UA LD CQ JM YV	knq ysq rhj tlj
St	8.	V II I	23 11 25	QY OG ST HA CB WD KL JN VX IU	lro avw axh gws
St	7.	II III I	06 12 03	BG FS TH JE VK FI CU QA OD NM	aty mbb mvo jmz
St	6.	I IV V	24 19 01	IR HQ NT WZ VC OY GF LF BX AK	bhc iwo zgz rnr
St	5.	II V III	05 22 14	MK GO RQ XT DW IA ZL SY PJ ER	bok rzw kzo ryl
St	4.	IV II I	15 02 21	KD PG CO FW HJ RY MT QL VB UZ	kpk php xmo gfw
St	3.	III V IV	03 23 04	DY CF WN QX QH UZ HA TJ GL SM	hjy nkt ytn pvc
St	2.	I III V	13 18 01	DR VJ FS EK IU HX AQ GT YO FC	gpq fqw oiy ruj
St	1.	II IV I	06 17 26	AC LS BQ WN MY UV FJ PZ TR OK	bol ooi ywv sfb

DECLASSIFIED
Authority NND 969192
By DP NARA Date 11/4/04

Rysunek 5. Tabele szyfrów, rok 1944 (źródło [6])

Aby dokonać deszyfracji, odbiorca ustawiał Enigmę według klucza dziennego, i za jego pomocą odszyfrowywał klucz indywidualny. Następnie przestawiał swoją maszynę zgodnie z kluczem indywidualnym, i dopiero wtedy mógł rozszyfrować depeszę.

4. Łamanie kodu Enigmy

W tym rozdziale zostaną opisane różne metody łamania szyfru Enigmy, które były stosowane przez Polaków, a następnie ulepszane i używane przez Brytyjczyków.

4.1. Polska

Kiedy zaczęto wyłapywać niemieckie depesze zaszyfrowane Enigmą, nikt nie sądził, że to prawdziwe wiadomości, bo brzmiały jak bełkot. Myślano, że to podstęp Niemców, aby zmusić wrogów do straty czasu na próby rozszyfrowania. Jednakże „enigmatycznych" wiadomości było coraz więcej, aż w końcu stały się głównym środkiem komunikacji niemieckiego wojska.

Moment, kiedy polskie wojsko zaczęło się interesować Enigmą, można datować na przełom 1927 i 1928. Wtedy przez przypadek do Polski trafiła tajemnicza przesyłka. Niemcy zażądali natychmiastowego zwrotu, co wzbudziło czujność urzędników celnych. Ci zawiadomili Biuro Szyfrów (ponieważ przesyłka rzekomo zawierała sprzęt radiowy). Pracownicy Biura potajemnie otworzyli paczkę, która – jak się okazało – zawierała Enigmę. Była to tylko komercyjna wersja maszyny, więc nie przydała się zbytnio polskiemu wojsku. Jednakże był to pierwszy kontakt Biura Szyfrów z Enigmą. Maszynę sfotografowano, a następnie zapakowano i odesłano, bez śladów otwierania przesyłki.

Polskie Biuro Szyfrów bardzo szybko zorientowało się, że będą potrzebni naprawdę świetni kryptolodzy, aby rozwiązać problem Enigmy. Już na przełomie lat 1928 i 1929 na uniwersytecie w Poznaniu otworzono kurs kryptologii dla studentów kończących studia matematyczne i biegle władających językiem niemieckim (jak się potem miało okazać, ważniejsza była znajomość matematyki niż języka).

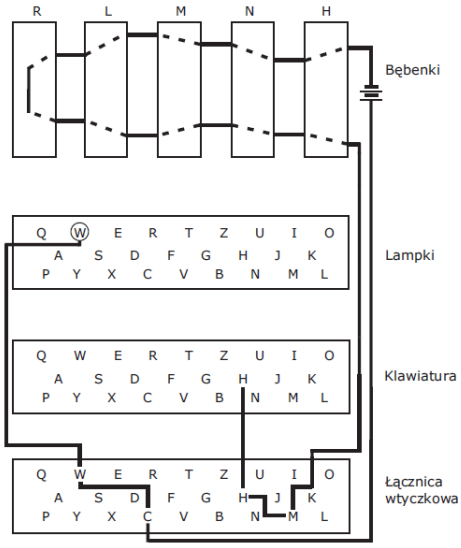
Od strony wywiadu wojskowego, niemożliwa do przecenienia jest rola Francuzów, m. in. generała (a wtedy jeszcze kapitana) Gustave Bertranda. W 1932 r. zdobył on i dostarczył polskiemu wojsku bardzo cenne materiały, także na temat Enigmy, przy pomocy innej ważnej postaci w historii łamania kodu Enigmy, jaką był Hans-Thilo Schmidt, ps. Aché lub Źródło D. Był on pracownikiem niemieckiego Biura Szyfrów oraz młodszym bratem generała Rudolfa Schmidta („ulubiony generał Hitlera"). Od lat 30. XX w. sprzedawał Francuzom m. in. instrukcje i bieżące kody do obsługi Enigmy, a także inne informacje wojskowe i dyplomatyczne. W 1943 r. został aresztowany i popełnił samobójstwo w celi. Materiały dotyczące Enigmy zdobyte przez Aché początkowo zostały uznane przez wywiad francuski (a następnie brytyjski) za nieistotne, ponieważ nie potrafili ich wykorzystać do rozszyfrowania kodu Enigmy. Dopiero po przekazaniu tych informacji Polakom okazały się one niezwykle pomocne [11].

Najważniejszymi postaciami w Polsce związanymi z Enigmą byli trzej absolwenci poznańskiego kursu kryptologii: Marian Rejewski, Jerzy Różycki oraz Henryk Zygalski.

4.1.1. Matematyczny opis Enigmy

Z trzech polskich kryptologów, początkowo jedynie Mariana Rejewskiego wtajemniczono w istnienie Enigmy i poproszono o pracę nad złamaniem kodu. Spróbował on zbudować matematyczny model opisujący tą maszynę szyfrującą.

Każde ustawienie Enigmy można zapisać jako pewną permutację, która danej literze przyporządkowuje inną literę. Z powodu opisanych wcześniej obrotów bębenków, po każdym naciśnięciu klawisza dostajemy inną permutację.



Rysunek 6. Przepływ prądu w Enigmie wojskowej z łącznicą (źródło: Wikipedia)

Przyjmując oznaczenia takie jak na rysunku 6, oraz oznaczając permutacje łącznicy jako S, przepływ prądu w Enigmie można by zapisać jako iloczyn permutacji.

$$SHNMLRL^{-1}M^{-1}H^{-1}S^{-1}$$

Jednakże po każdym naciśnięciu klawisza bęben N wykona 1/26 obrotu. Zatem i-tą literę każdej depeszy przekształcała permutacja

$$A_i = S^{-1}H^{-1}P^{-i}N^{-1}P^iM^{-1}L^{-1}RLMP^{-i}NP^iHS,\ i = 1,2,3...$$

gdzie P = (1 2 3 ... 24 25 26) była permutacją spowodowaną obrotem wirnika N (liczby od 1 do 26 oznaczały kolejne litery alfabetu). Dzięki budowie bębenka R mamy $A_i = A_i^{-1}$

Warto zaznaczyć, że w momencie rozpoczynania obliczeń Rejewski miał do dyspozycji jedynie komercyjną wersję Enigmy, nie znał okablowania ani dokładnej budowy Enigmy wojskowej, korzystał z zaszyfrowanych depesz przejmowanych każdego dnia.

Procedura szyfrowania wyglądała następująco: szyfranci mieli do dyspozycji 3 wirniki, których kolejność była zmieniana co kwartał. Początkowe ustawienia

wirników zmieniano codziennie o północy, a klucz indywidualny szyfrowano dwukrotnie.

Pierwsza rzecz jaka rzuciła się w oczy polskiemu matematykowi, to fakt, że każda depesza zaczyna się od grupy 6 znaków – domyślił się, że to zaszyfrowany klucz dla każdej depeszy.

Przykładowe klucze 6-literowe:

auq amn	maw uxp	sug smf
bnh chl	nxd qtu	tmn eby
cik bzt	nlu qfz	taa axb
ddb vdv	obu dlz	use nwh
ejp ips	pvj feg	vii pzk
fbr kle	qga lyb	vii pzk
gpb zsv	rjl wpx	vqz pvr
ikg jkf	syx scw	xrs gnm
khb xjv	syx scw	ypc osq
khb xjv	syx scw	ypc osq
maw uxp	sug smf	zsj ywg

Pamiętamy, że 3-literowy klucz był szyfrowany dwukrotnie, zatem czwarta litera to ta sama co pierwsza, piąta to ta sama co druga, a szósta to ta sama co trzecia.

Te permutacje, generowane przez pierwszych 6 liter, oznaczamy jako A, B, C, D, E, F. Następnie należy wypisać wszystkie cykle, najpierw dla pierwszej i trzeciej litery, a następnie kolejno dla dwóch pozostałych par.

Na przykładzie podanych wyżej kluczy, patrząc na pierwszą i trzecią literę, łatwo zauważyć na przykład, że a przechodzi w a (pierwszy klucz), więc jest to cykl długości jeden. Z drugiego i trzeciego klucza widzimy, że b przechodzi w c, a c w b, co daje cykl długości dwa (bc).

W przykładzie podanym przez Rejewskiego w jego wspomnieniach mamy [9]:

$$AD = (a)(bc)(dvpfkxgzyo)(eijmunqlht)(rw)(s)$$
$$BE = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$$
$$CF = (abvikt jgfcqny)(duzrehlxwpsmo)$$

Oczywiście układ ten każdego dnia był inny, ale zawsze posiadał następującą cechę:

Cykle danej długości występowały w każdym wierszu (AD, BE oraz CF) zawsze w liczbie parzystej.

Rejewski nazywał taki układ **układem charakterystycznym** lub w skrócie **charakterystyką** danego dnia.

Polski kryptolog skorzystał z dwóch twierdzeń, gdzie drugie jest odwrotne do pierwszego.

Twierdzenie 4.1. *Jeżeli dwie permutacje X i Y tego samego stopnia składają się z samych transpozycji rozłącznych, to w iloczynie XY występują cykle rozłączne tej samej długości w liczbie parzystej*

Twierdzenie 4.2. *że jeżeli w jakiejkolwiek permutacji (stopnia parzystego) cykle rozłączne tej samej długości występują w liczbie parzystej, to permutację tę można uważać za iloczyn XY dwóch permutacji X i Y, z których każda utworzona jest z samych transpozycji rozłącznych.*

Zastosowanie powyższych twierdzeń w przypadku Enigmy było uzasadnione tym, że dzięki bębenkowi odwracającemu np. jeżeli A przechodziło w W, to przy tym samym ustawieniu W przechodziło w A – permutacje faktycznie składały się z samych transpozycji.

Rejewski wykazał także, że

1. litery wchodzące do jednej transpozycji permutacji X lub Y wchodzą zawsze do dwóch różnych cykli permutacji XY
2. jeżeli dwie litery znajdujące się w dwóch różnych cyklach tej samej długości w permutacji XY należą do tej samej transpozycji, to sąsiadujące z nimi litery (jedna z prawej, druga z lewej strony) też należą do tej samej transpozycji.

W tej pracy nie zostaną przedstawione dowody powyższych twierdzeń, ponieważ ma ona charakter raczej popularnonaukowy, więc większy nacisk będzie położony na to, jak kryptolodzy wykorzystali te twierdzenia w praktyce.

Oprócz tego, że posiadali wiedzę matematyczną, pracownicy Biura Szyfrów dobrze poznali zwyczaje niemieckich szyfrantów, i wiedzieli, że ci na klucze jednorazowe wybierali często kombinacje liter takie jak *aaa*, *bbb* i tym podobne.

Załóżmy więc, że wśród naszych kluczy znajduje się klucz *aaa*. Ponieważ w iloczynie AD litery a i s tworzą cykle jednoliterowe, to litera a po zaszyfrowaniu powinna przejść w s.

Niech dane będą przykładowo klucze

$$sug\ smf$$

$$sjm\ spo$$

$$syx\ scw$$

Pierwszy klucz: *sug smf*, nie mógł powstać z zaszyfrowania liter *aaa*. Patrząc bowiem na permutację BE, mamy, że litera u wchodzi w skład cyklu 9-literowego, podczas gdy litera a znajduje się w cyklu trzyliterowym.

Drugi klucz: *s jm spo* nie mógł powstać z zaszyfrowania *aaa* z podobnych powodów jak powyżej.

Trzeci klucz: *syx scw* mógł powstać z zaszyfrowania *aaa*, ponieważ:
y i *a* znajdują się w dwóch różnych cyklach trzyliterowych permutacji BE,
x i *a* znajdują się w dwóch różnych cyklach 13-literowych permutacji CF,
c i *a* znajdują się w dwóch różnych cyklach 3-literowych permutacji BE,
w i *a* znajdują się w dwóch różnych cyklach 13-literowych permutacji CF.

Oczywiście powyższe rozważania nie stanowią dowodu, że ten szyfr faktycznie oznaczał *aaa*, ale dla danych z tamtego dnia, przy założeniu że *syx scw* oznacza *aaa aaa*, wiele z pozostałych kluczy dało się rozszyfrować jako *bbb*, *ccc* i tym podobne.

Co ciekawe, do osiągnięcia tego wyniku nie była potrzebna znajomość ustawień bębenków ani kluczy dziennych. Wystarczyło jedynie mieć sporą ilość depesz z danego dnia (około 60 sztuk) a także znajomość zwyczajów szyfrantów.

Rejewski w sposób podany powyżej odczytywał pierwsze wiadomości w ostatnich dniach 1932 r. Był to pierwszy przełom jeśli chodzi o Enigmę.

W późniejszej fazie wojny szyfranci byli dokładniej pilnowani, m. in. zabroniono używania kluczy, które składały się z 3 takich samych liter. Jednakże jest niemożliwe, aby człowiek wybrał 3 całkowicie losowe litery, więc zamiast tego zwyczaju pojawiły się inne, np. *qwe*, *asd* i inne związane z ułożeniem liter na klawiaturze.

4.1.2. Okablowanie Enigmy

Rejewski posiadał jedynie wersję handlową Enigmy, zachodziła więc potrzeba poznania okablowania maszyny wojskowej.

Zgodnie ze wcześniejszymi oznaczeniami i opisem przepływu prądu w maszynie, permutacje A-F można przedstawić jako

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1}$$
$$\dots$$
$$F = SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1}$$

W tych równaniach zakładamy, że dla pierwszych sześciu znaków obracał się jedynie prawy bębenek (założenie to jest słuszne w $\frac{21}{26} \approx 80\%$ przypadków).

Podstawiając

$$Q = MLRL^{-1}M^{-1}$$

mamy

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$

$$B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$$

$$\dots$$

$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

gdzie niewiadome są permutacje S, H, N, Q.

W Enigmie handlowej permutacja H bębenka wstępnego miała następującą postać:

$$H = \begin{pmatrix} q & w & e & r & t & z & \cdots & n & m & l \\ a & b & c & d & e & f & \cdots & x & y & z \end{pmatrix}$$

Czyli górny wiersz przedstawia ułożenie liter na klawiaturze, a dolny kolejność alfabetyczną.

Rejewski przyjął założenie, że w wojskowej Enigmie ta zależność jest taka sama. Zatem pozostawały trzy niewiadome S, N i Q.

Pod koniec 1932 r. dostarczono Rejewskiemu fotokopie dwóch tablic kluczy dziennych na wrzesień i październik 1932 r. Tablice zawierały m. in. połączenia na łącznicy, więc permutacja S była teraz znana.

Zatem permutacje H i S można przenieść na lewą stronę równań.

$$H^{-1}S^{-1}ASH = PNP^{-1}QPN^{-1}P^{-1}$$
$$H^{-1}S^{-1}BSH = P^2NP^{-2}QP^2N^{-1}P^{-2}$$

$$\dots$$

$$H^{-1}S^{-1}FSH = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

Następnie każde z równań przemnażamy lewostronnie przez P^{-i} oraz prawostronnie przez P^i. Lewe strony równań oznaczamy przez $U, V, \dots, Z$.

$$U = P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$
$$V = P^{-2}H^{-1}S^{-1}BSHP^2 = NP^{-1}QPN^{-1}$$

$$\dots$$

$$Z = P^{-6}H^{-1}S^{-1}FSHP^6 = NP^{-1}QPN^{-1}$$

Teraz tworzymy iloczyny, przemnażając po dwa kolejne równania.

$$UV = NP^{-1}(QP^{-1}QP)PN^{-1}$$
$$VW = NP^{-2}(QP^{-1}QP)P^2N^{-1}$$

$$\ldots$$

$$YZ = NP^{-5}(QP^{-1}QP)P^5N^{-1}$$

Po wyeliminowaniu wspólnego wyrażenia $QP^{-1}QP$ otrzymujemy układ czterech równań z jedną niewiadomą NPN^{-1}.

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(VW)NPN^{-1}$$
$$XY = NP^{-1}N^{-1}(WX)NPN^{-1}$$
$$YZ = NP^{-1}N^{-1}(XY)NPN^{-1}$$

Widać, że wyrażenie VW jest przekształcone z wyrażenia UV za pomocą permutacji NPN^{-1}, podobnie wyrażenie WX jest przekształcone z VW.

Podstawiając VW pod UV na wszystkie możliwe sposoby otrzymujemy kilkadziesiąt możliwych rozwiązań.

Analogicznie dla WX podstawianego pod VW. Jedno z tych kilkudziesięciu rozwiązań powinno być identyczne w obu powyższych przypadkach.

W powyższy sposób otrzymaliśmy szukaną permutację NPN^{-1}. Teraz mamy 26 przypadków dla permutacji P, zależnie od skręcenia bębenka (pozycji początkowej).

Jednakże, Rejewskiemu nie udało się znaleźć ani jednego rozwiązania. Analizując swój tok myślenia, doszedł do wniosku, że jedyny błąd mógł popełnić przy permutacji H, ponieważ była to jedyna rzecz, którą zgadł, a nie obliczył.

Rejewski pomyślał, że skoro litery nie są połączone w kolejności alfabetycznej, to może przekształcenie H jest identycznością. Przy tym założeniu udało się rozwiązać równania, a więc odkryć okablowanie wirników Enigmy.

Jako ciekawostkę warto dodać, że brytyjscy kryptolodzy natrafili na taki sam problem z permutacją H, ale odrzucili pomysł, że H może być identycznością, ponieważ wydawał im się zbyt prosty.

4.1.3. Metody dekryptażu

Polacy wynaleźli kilka metod łamania kodu Enigmy, które były rozwijane wraz z ulepszeniami wprowadzanymi przez niemieckie wojsko:

— metoda rusztu;
— metoda „anx”;
— metoda zegarowa;
— karty charakterystyk;
— płachty Zygalskiego;
— bomba Rejewskiego.

4.1.4. Metoda „anx”

Metoda wykorzystywała fakt, że wiele niemieckich depesz zaczynało się od słowa „an” („do”) oraz litery „x”, która oznaczała odstęp.

Przyjmując przypuszczenie, że depesza zaczyna się od „anx”, i znając uprzednio klucz dzienny, postępować należało w sposób opisany poniżej.

Przykładowo niech depesza zaczyna się od liter „tuv”. Zakładając, że przypuszczenie było poprawne, oznaczałoby to, że litera „a” została zaszyfrowana jako „t”. Pamiętając, że szyfr jest symetryczny, należy teraz wciskać literę „t” tak długo, aż zapali się „a”. Gdy zapali się „a”, należy sprawdzić, czy litery „u” i „v” w tym ustawieniu szyfrują „n” i „x”.

Była to metoda niezawodna, ale w najgorszym przypadku trzeba by wcisnąć klawisz „t” 17 576 razy.

4.1.5. Metoda zegara

Metoda zegara była jednyną metodą niezwiązaną z teorią grup, ale raczej ze statystyką i z wiedzą o języku.

Metoda zegara miała na celu ustalenie, który wirnik zajmuje skrajną prawą („najszybszą”) pozycję.

Wśród depesz z danego dnia należało znaleźć dwa klucze, które różniły się tylko na trzeciej pozycji, np. `CCE` i `CCH`.

Depesze takie należało zapisać jedna pod drugą, z odpowiednim przesunięciem, tak, aby litery szyfrowane w ten sam sposób były w jednej kolumnie. W przypadku kluczy `CCE` i `CCH` oznaczałoby to przesunięcie o trzy znaki.

Jeżeli depesza liczyła kilkadziesiąt znaków, to na pewno musiał nastąpić przeskok środkowego wirnika. W każdym z wirników zaczep przesuwu znajdował się w innym miejscu, więc znalezienie przesunięcia pozwalało jednoznacznie zidentyfikować wirnik.

Miejsce przeskoku można było znaleźć dzięki koincydencjom (w danej kolumnie pojawiają się dwie takie same litery).

Miara częstości występowania par takich samych liter bywa określana indeksem koincydencji.

Dla języka niemieckiego indeks koincydencji wynosi około $\frac{1}{13}$, a dla przypadkowo ustawionych liter ta wartość spada do $\frac{1}{26}$.

Układając szyfrogramy w sposób opisany powyżej, jeżeli zostały zaszyfrowane przy użyciu tego samego klucza, to prawdopodobieństwo wystąpienia dwóch takich samych liter powinno wynosić około 8%. Jeżeli ta częstość była niższa, oznaczało to, że nastąpił przeskok.

Polskim kryptologom ta metoda skojarzyła się z wpatrywaniem się w zegar i czekaniem, aż wybije kolejna godzina, stąd nazwa.

4.1.6. Metoda rusztu

Metoda rusztu służyła do zidentyfikowania połączeń na łącznicy. Używana była w latach 1936-1938.

W momencie używania tej metody, Polacy umieli już znajdować klucze indywidualne, znali także okablowanie wirników, więc permutacja na łącznicy była jedyną niewiadomą.

Pamiętając o tym, że permutacja bębenka wstępnego H jest identycznością, możemy dla i-tej litery w depeszy zapisać:

$$A_i = S^{-1}P^{-x-i+1}N^{-1}P^{x+i-1}QP^{-x-i+1}NP^{x+i-1}S, \qquad i = 1,\ldots,6$$

gdzie

$$Q = P^{-y}M^{-1}P^{y}P^{-z}N^{-1}P^{z}RP^{-z}NP^{z}P^{-y}MP^{y}, \quad x,y,z = 0,\ldots,25.$$

Równanie to przekształcono tak, aby Q było po lewej stronie.

$$Q = P^{-x-i+1}NP^{x+i-1}SA_iS^{-1}P^{-x-i+1}N^{-1}P^{x+i-1}, \qquad i = 1,\ldots,6,$$

gdzie niewiadomymi są x oraz permutacja S.

Dla kolejnych wartości wykładnika x wypisywano wszystkie 6 wartości Q. Dla wszystkich wykładników oprócz jednego te wartości się różniły.

Wykładnik x, dla którego wszystkie wartości Q były równe, wyznaczał pozycję startową pierwszego wirnika.

Dla usprawnienia procesu, kolejne potęgi permutacji wirników były wypisane na arkuszach papieru, w których wycięto 6 otworów (właśnie od tych arkuszy, tak zwanych rusztów, metoda wzięła swoją nazwę).

Permutacje A-F były wypisane na drugim arkuszu, który przesuwano pod rusztem. W teorii w jednym z położeń permutacje Q we wszystkich 6 otworach powinny być równe.

Jednakże w rzeczywistości te permutacje różniły się, ze względu na działanie łącznicy. Były jednak na tyle podobne, że dawało się rozpoznać właściwe rozwiązanie.

W otrzymanej w ten sposób pozycji należało dokonać takiej zamiany liter, aby wszystkie permutacje Q faktycznie były równe. Te zamienione litery były szukanymi parami połączeń na łącznicy.

4.1.7. Cyklometr

Cyklometr był pierwszą maszyną, którą Polacy skonstruowali, by pomóc sobie w rozszyfrowywaniu depesz.

Maszyna składała się z podwójnego zestawu wirników takich jak w Enigmie (każdy wirnik był podwojony, z czego jeden był przesunięty w stosunku drugiego o 3 pozycje, jak w kluczu dziennym).

Rysunek 7. Cyklometr (źródło: https://enigma.umww.pl/)

Urządzenie to miało na celu wyznaczanie długości cykli odpowiadających danemu ustawieniu początkowemu. Możliwych ustawień było $3! \cdot 26^3 = 105456$. Maszyna posłużyła do ułożenia tzw. **kart charakterystyk**, z których następnie można było odczytać ustawienia początkowe na dany dzień na podstawie długości cykli.

Skatalogowanie wszystkich charakterystyk zajęło ponad rok, ale dzięki nim dało się ustalić klucz dzienny już w kilkanaście minut (mowa tu o roku 1935).

Najbardziej cenione były cykle jednoliterowe, ponieważ te dało się odnaleźć na podstawie pojedynczej depeszy. Polscy kryptolodzy nazywali je „samiczkami", stąd cyklometr bywał żartobliwie określany „seksmaszyną".

4.1.8. Płachty Zygalskiego

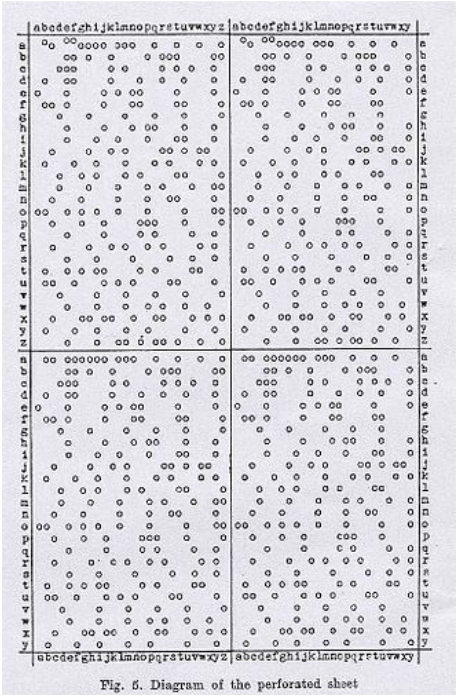
Płachty Zygalskiego stanowiły nową wersję kart charakterystyk cyklicznych Rejewskiego.

Zaczęto ich używać w roku 1938, po ulepszeniach ze strony niemieckiej (wymiana walca odwracającego w listopadzie 1937).

Każda płachta odpowiadała jednemu z 26 ustawień lewego wirnika, który obracał się najrzadziej, więc najprawdopodobniej był nieruchomy. Płachta na krawędziach miała wypisane litery alfabetu. Oś pozioma odpowiadała środkowemu wirnikowi, a pionowa prawemu. W ten sposób na płachcie były wszystkie możliwe kombinacje dla danego ustawienia wirnika lewego. Na płachcie wycinano otwory w miejscach, gdzie znajdowały się punkty stałe w danej permutacji.

Ze względu na oszczędność miejsca i wygodę, na każdym arkuszu znajdowały się cztery matryce 26x26.

Zestaw do deszyfracji składał się z 6 kompletów po 26 perforowanych arkuszy. Każdy komplet odpowiadał ustawieniu trzech wirników w danej kolejności. W sumie dawało to 156 arkuszy, każdy miał ponad tysiąc otworów.



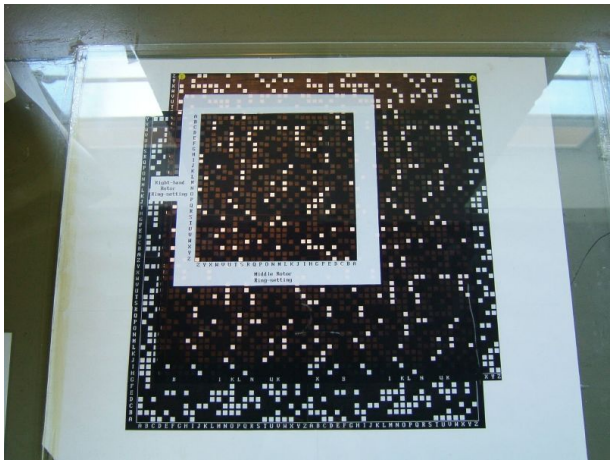
Rysunek 8. Płachta Zygalskiego. Dla oszczędności drukowano po 4 płachty na jednym arkuszu (źródło: Wikipedia)

W procesie deszyfrowania należało wybrać klucze, w których pojawiał się cykl długości 1, np.

syx scw

Na początku trzeba było podjąć decyzję, od jakiego ustawienia bębnów i od jakiej litery zacząć sprawdzanie.

Układano na sobie płachty odpowiadające kolejnym indykatorom. Czynności te wykonywano na podświetlanym stole. Jeżeli pojawiała się sytuacja, że światło prześwietlało przez dokładnie jeden otwór, to można było z tego położenia odczytać ustawienie początkowe bębnów. Jeżeli wszystkie otwory były przesłonięte, to należało powtórzyć proces dla innego ustawienia.



Rysunek 9. Nałożone na siebie dwie płachty Zygalskiego, ekspozycja w muzeum w Bletchley Park (źródło: Wikipedia)

Zastosowanie płacht Zygalskiego znacznie przyspieszyło proces dekryptażu. Teoretycznie w najgorszym przypadku należałoby wykonać 156 prób, ale w praktyce zwykle wystarczała około połowa tej liczby.

Płachty Zygalskiego przyczyniły się do zbudowania bomby kryptologicznej Rejewskiego.

Symulator online płacht Zygalskiego:
https://www.codesandciphers.org.uk/virtualbp/poles/ppoles.htm

4.1.9. Bomba

Bomba była drugą z maszyn skonstruowaną przez polskich kryptologów. Nikt właściwie nie wie, skąd się wzięła ta nazwa. Jedna z teorii głosi, że chodzi o tykanie, gdy obracały się wirniki (analogiczne do tych w Enigmie). Inni mówili, że nazwa pochodziła od ulubionego deseru trójki matematyków. Rejewski twierdził, że maszyna została nazwana Bombą „z braku lepszego pomysłu".

Bomba wykorzystywała podwójne szyfrowanie klucza depeszy. Sprawdzała, czy dla któregoś z 26^3 ustawień litery się powtarzały. Jeżeli tak, mogło to sugerować, że trafiła na właściwe ustawienie.

Polacy posiadali 6 bomb – każda odpowiadała jednemu ustawieniu wirników.

Rysunek 10. Bomba Rejewskiego (źródło: enigma.umww.pl)

4.2. Wielka Brytania

4.2.1. Zmiany w procesie szyfrowania

W 1938 r. agent polskiego wywiadu w Niemczech doniósł, że od teraz w Enigmach będzie stosowanych aż 5 wirników zamiast 3 (liczba wirników w maszynie nadal wynosiła 3, ale wybierano je spośród pięciu dostępnych).

Co prawda stare metody łamania szyfrów nie straciły przez to aktualności, ale liczba kombinacji znacząco wzrosła, co wydłużało czas potrzebny do odtworzenia klucza. Mamy bowiem

$$\binom{5}{3} \cdot 3! = 60$$

możliwości ustawienia wirników, podczas gdy wcześniej było ich 10 razy mniej.

Jednakże, po raz kolejny przeciwnik nie zawiódł kryptologów, i popełnił błąd. Sieć Sicherheitdienst (służby bezpieczeństwa) jeszcze przez 3 miesiące pozostała przy starych metodach szyfrowania. Dzięki temu udało się odkryć okablowanie dwóch nowych wirników.

Wcześniej Biuro Szyfrów posiadało sześć maszyn typu Bomba – dla każdego z możliwych ustawień 3 wirników. Już budowa tych maszyn stanowiła prawie roczną wysokość budżetu Biura, więc zamówienie 60 Bomb było niemożliwe. Dodatkowo od roku 1939 Enigma na łącznicy zamieniała 10 par liter zamiast dotychczasowych 6.

Technika płacht Zygalskiego także traciła skuteczność – należałoby sporządzić aż 60 kompletów płacht, co równało się około 2 milionom ręcznie perforowanych otworów.

Był to moment, kiedy polskie metody łamania szyfru Enigmy zawiodły. Wtedy pałeczkę przejęli kryptolodzy i matematycy z Bletchley Park, na czele ze słynnym Alanem Turingiem. Polscy kryptolodzy (po ucieczce za granicę do Rumunii a stamtąd do Francji) nadal pracowali nad szyframi, ale już nie w związku z Enigmą.

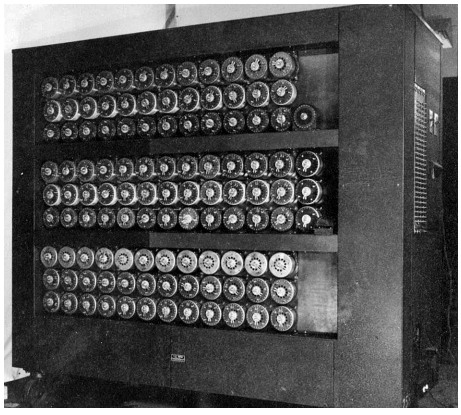
4.2.2. Bletchley Park

W Bletchley Park operacja łamania kodu Enigmy otrzymała kryptonim „Ultra" – najbardziej tajna z możliwych.

Jesienią 1939 r. brytyjscy kryptolodzy zbudowali 60 maszyn takich jak Bomba Rejewskiego. W 1940 r. Niemcy wprowadzili dalsze ulepszenia – klucz indywidualny był szyfrowany tylko jeden raz. W tym momencie dalsze rozwijanie metod wynalezionych przez polskich kryptologów byłoby bezcelowe – wszystkie one opierały się na cyklach, a nie można mówić o cyklach w przypadku jednokrotnego szyfrowania klucza.

Do złamania szyfru Brytyjczykom posłużyła specjalna maszyna, zaprojektowana głównie przez Alana Turinga, przy pomocy Gordona Welchmana. Maszyna Turinga została nazwana „Bombe", na cześć wspomnianej wcześniej polskiej Bomby.

Turing w swojej maszynie wykorzystał fakt, że żadna litera nie może być zaszyfrowana jako ona sama. Celem Alana Turinga było znalezienie ustawień początkowych oraz ustawień na łącznicy.



Rysunek 11. Maszyna „Bombe" Turinga (źródło: Wikipedia)

Każdego dnia o godz. 6 Niemcy wysyłali prognozę pogody. Dzięki temu można było się domyślić, że w depeszy pojawi się sformułowanie „prognoza pogody"

(niem. „Wetterbericht”). Oczywiście wiele depesz kończyło się słowami „Heil Hitler” – to zdanie także można było wykorzystać podobnie jak słowo „Wetterbericht”.

Działanie Bomby Turinga opierało się na następującej idei: należałoby napisać na kartce słowo „Wetterbericht”, a następnie przesuwać kartkę pod depeszą tak długo, aż żadne litery w pionie się nie pokryją [8].

```
jxatqbggywcrybgdt
 wetterbericht
```

Widać, że w powyższym przypadku litera *t* pojawia się dwukrotnie w tej samej kolumnie. Musimy więc przesuwać się dalej:

```
jxatqbggywcrybgdt
  wetterbericht
```

W tym przypadku żadna litera się nie pokrywa. Sprawdźmy, co by się stało, gdyby przesunąć słowo o jeszcze jeden znak:

```
jxatqbggywcrybgdt
   wetterbericht
```

Teraz litery *r* się powtarzają. Pozostaniemy więc przy drugim ustawieniu, czyli:

```
jxatqbggywcrybgdt
  wetterbericht
```

Widać na przykład, że $t \to e$.

Oznacza to, że *t* po przejściu kolejno przez łącznicę, wirniki i znów przez łącznicę zamieniło się w *e*.

Czyli $t \to$ (łącznica) $\to$ (rotory) $\to$ (łącznica) $\to e$

Ustawienie wirników przyjmujemy jako znane w danym momencie (później być może będzie trzeba je skorygować).

Turing rozumował podobnie jak w matematycznej metodzie przeprowadzania dowodów „nie wprost” – przyjmował pewne założenie, które mogło doprowadzić do wystąpienia sprzeczności.

Załóżmy zatem przykładowo, że jedno z połączeń na łącznicy to *ta*, czyli *t* po przejściu przez łącznicę daje *a*.

Ponieważ znamy ustawienia wirników Enigmy, to możemy odczytać, jaką literą stanie się a po przejściu przez rotory, niech dla przykładu będzie to *p*.

Na wyjściu otrzymaliśmy *e*, więc teraz wiemy, że *e* jest połączone na łącznicy z *p*.

t $\to$ a (założenie) $\to$ (rotory) $\to$ p (wniosek) $\to$ e

Postępujemy dalej w analogiczny sposób, dla kolejnych liter z depeszy, i odkrywamy kolejne połączenia, dopóki nie trafimy na sprzeczność. Jeżeli dla połączenia *ta* trafimy na sprzeczność, to trzeba by sprawdzać *tb*, *tc*, itd., razem 26 możliwości (25 możliwości połączenia lub brak połączenia). Jeżeli dla każdego z 26 połączeń otrzymamy sprzeczność, oznacza to, że błędnie wybraliśmy ustawienia początkowe Enigmy. Należałoby wtedy zmienić ustawienia i zacząć procedurę od nowa.

Turing odkrył także drobne ułatwienie: jeżeli założenie początkowe (w przykładzie było to połączenie *ta*) okaże się fałszywe, to wszystkie połączenia otrzymane „po drodze" do sprzeczności także są niepoprawne, więc można od razu odrzucić je wszystkie.

Liczba kombinacji nadal byłaby zbyt duża dla człowieka, ale tu z pomocą przyszły maszyny – Turing niejako „przy okazji" zbudował coś w rodzaju pierwszego komputera.

Bomba (ang. *Bombe*) sprawdzała po kolei połączenia na łącznicy w sposób opisany powyżej, i zatrzymywała się, gdy trafiła na właściwe.

4.3. Skrót historyczny

— 1918 – opatentowanie Enigmy przez Niemców
— 1926 – pozyskanie przez Polaków komercyjnej Enigmy do badań
— 1929 – Gwido Langer szefem Biura Szyfrów. Początek kursu kryptologii na Uniwersytecie Poznańskim
— 1930 – początek użytkowania Enigmy Wehrmachtu (model z łącznicą)
— 1932 – złamanie pierwszych depesz przez Rejewskiego
— 1936 – wprowadzenie comiesięcznych, a następnie codziennych zmian układu wirników, zmiana liczby połączeń w łącznicy
— 1938 – klucze Enigmy są zmieniane dla każdej depeszy, wprowadzenie dwóch nowych wirników
— 1939 – liczba połączeń w łącznicy zwiększona do 7–10; dwie konferencje X, Y, Z (w Polsce i w Paryżu); przybycie Turinga do Bletchley Park
— 1940 – koniec podwójnego szyfrowania klucza depeszy; uruchomienie prototypowej Bomby w Bletchley Park

4.4. Po wojnie

Marian Rejewski po wojnie wrócił do Polski, pracował jako urzędnik w Bydgoszczy, dopiero w 1967 r. ujawnił swój udział w łamaniu kodu Enigmy. Henryk Zygalski pozostał na emigracji w Wielkiej Brytanii i uczył tam matematyki. Jerzy Różycki nie doczekał końca wojny, zginął na Morzu Śródziemnym w 1942 r. w katastrofie statku podczas powrotu z Algieru do ośrodka dekryptażu we Francji. W 2000 r. trzej

panowie zostali odznaczeni Krzyżem Wielkim Orderu Odrodzenia Polski przez Prezydenta Aleksandra Kwaśniewskiego.

Po wojnie Alan Turing zaprojektował jeden z pierwszych cywilnych brytyjskich komputerów. W 1950 r. opublikował założenia testu Turinga (definicja sztucznej inteligencji). W roku 1952 włamano się do domu Turinga, który zgłosił to na policję. W trakcie śledztwa udowodniono Turingowi homoseksualizm, co w tamtych czasach było przestępstwem. Turing miał do wyboru więzienie lub terapię hormonalną (tzw. chemiczna kastracja) – wybrał to drugie. Poza okropnymi skutkami ubocznymi przyjmowania estrogenu, Turing cierpiał z powodu odsunięcia od badań nad komputerami. 7 czerwca 1954 r., w wieku 41 lat, Alan Turing popełnił samobójstwo w swojej sypialni. Przyczyną śmierci było zatrucie cyjankiem. Obok łóżka znajdowało się nadgryzione jabłko. Nieudowodniona hipoteza mówi, że to ono było nośnikiem trucizny. W biografii naukowca zasugerowano, że Turing w ten sposób chciał odtworzyć scenę ze swojej ulubionej baśni – Królewny Śnieżki [12]. Turing został pośmiertnie ułaskawiony w 2013 r.

W 2014 r. powstał film „Gra Tajemnic" opowiadający historię Alana Turinga.

5. Podsumowanie

Mówi się, że złamanie szyfru Enigmy skróciło wojnę o około 2 lata. Dyskusyjnym problemem jest to, że Brytyjczycy nie mogli korzystać ze wszystkich wiadomości wyciągniętych z „enigmatycznych" depesz – nie chcieli się zdradzać z tym, że udało im się złamać szyfr, więc używali tylko tych informacji, dla których mogli znaleźć wiarygodną „przykrywkę".

Proces łamania Enigmy był właściwie narodzinami matematycznej kryptoanalizy, a także miał wpływ na początki informatyki.

Ze względu na obawę przed III wojną światową oraz na wysoki stopień tajności operacji „Ultra", po II wojnie światowej zapanowała dezinformacja na temat tego, czyją zasługą jest złamanie niemieckiego szyfru. Udział Polaków został ujawniony dopiero w latach 70. przez Rejewskiego w jego wspomnieniach oraz przez emerytowanego generała francuskiego Gustave'a Bertranda. Wśród Polaków panuje przekonanie, że Brytyjczycy przypisali sobie nasze zasługi. Z kolei w Wielkiej Brytanii postać Alana Turinga jest kultowa, a o polskich kryptologach mało kto słyszał.

Mam nadzieję, że z mojej pracy wynika, że zarówno polscy kryptolodzy, jak i brytyjscy, mieli duży udział w łamaniu kodu Enigmy, a to wszystko nie byłoby możliwe bez świetnego wywiadu francuskiego. Należy docenić wszystkie zaangażowane osoby, ponieważ mimo że faktycznie to Polacy złamali szyfr Enigmy jako

pierwsi, to po roku 1940 dalsze odczytywanie szyfru było możliwe tylko dzięki maszynie Turinga – słusznie uważanego za geniusza i ojca informatyki.

Literatura

[1] Corvus, *How the Enigma machine works | Animation*, https://www.youtube.com/watch?v=QwQVMqfoB2E, (dostęp: 06.01.2021)

[2] Crypto-IT, *Proste szyfry*, http://www.crypto-it.net/pl/proste/index.html

[3] Grajek M., *Enigma. Bliżej prawdy*, Dom Wydawniczy Rebis, 2007

[4] Guzicki W., *Enigma* – zapis odczytu wygłoszonego w sierpniu 2007 w Warszawie

[5] eKryptografia, *Szyfry klasyczne*, http://ekryptografia.pl/kryptografia/szyfry-klasyczne/, (dostęp: 28.13.2019)

[6] karol221-10, *Procedury szyfrowania*, https://www.dobreprogramy.pl/karol221-10/Kryptologia-XX-wieku-Enigma,71701.html, (dostęp: 08.07.2020)

[7] Numberphile, *158,962,555,217,826,360,000 (Enigma Machine)*, https://www.youtube.com/watch?v=G2_Q9FoD-oQ, (dostęp: 06.01.2021)

[8] Numberphile, *Flaw in the Enigma Code*, https://www.youtube.com/watch?v=V4V2bpZlqx8, (dostęp: 06.01.2021)

[9] Rejewski M. *Jak matematycy polscy rozszyfrowali Enigmę*, Roczniki Polskiego Towarzystwa Matematycznego, Seria II: Wiadomości Matematyczne XXIII, 1980

[10] du Sautoy M., *Poker z Pitagorasem. Matematyka za milion dolarów*, Wydawnictwo Carta Blanca, 2012

[11] Turing D., *X, Y, Z. Prawdziwa historia złamania szyfru Enigmy*, Dom Wydawniczy Rebis, 2019

[12] Wikipedia, *Alan Turing*, https://pl.wikipedia.org/wiki/Alan_Turing, (dostęp: 09.01.2021)

[13] Wikipedia, *Mikrokropka*, https://pl.wikipedia.org/wiki/Mikrokropka, (dostęp: 06.01.2021)

[14] Wikipedia, *Permutacja*, https://pl.wikipedia.org/wiki/Permutacja, (dostęp: 06.01.2021)

[15] Wikipedia, *Steganografia,* https://pl.wikipedia.org/wiki/Steganografia, (dostęp: 06.01.2021)

[16] Wikipedia, *Szyfr*, https://pl.wikipedia.org/wiki/Szyfr, (dostęp: 18.07.2019)

Magdalena Majewska[1]

Co wpływa na wysokość składki netto w ubezpieczeniach komunikacyjnych?

Streszczenie

W pracy przeprowadzona została analiza wartości składki ubezpieczeniowej netto. W części teoretycznej zaprezentowano metody kalkulacji składki netto oraz rozkłady wartości szkód najczęściej wykorzystywane w ubezpieczeniach komunikacyjnych. W części praktycznej przedstawiona została kalkulacja składki netto z użyciem różnych zasad obliczania składek ubezpieczeniowych, dla wybranych rozkładów wartości szkód.

Słowa kluczowe: składka ubezpieczeniowa, rozkład wartości szkody, kalkulacja składki netto

Wstęp

Podstawowym zadaniem matematyki ubezpieczeniowej jest wyznaczanie wartości składek netto. Ubezpieczenie jest ceną, jaką klient płaci zakładowi ubezpieczeń za przejęcie od niego części ryzyka związanego z prowadzoną działalnością. Wyznaczenie składki na odpowiednim poziomie jest niezwykle trudnym zadaniem. Z jednej strony zbyt niska składka może nie zagwarantować oczekiwanej sumy odszkodowań, a składka na zbyt wysokim poziomie zmniejsza konkurencyjność i atrakcyjność zakładu ubezpieczeń.

Celem niniejszego artykułu jest analiza porównawcza składek ubezpieczeniowych netto dla różnych rozkładów wartości szkód oraz wybranych zasad kalkulacji składek netto w ubezpieczeniach komunikacyjnych. W pracy przedstawione zostały zarówno zagadnienia teoretyczne (opis metod kalkulacji składek netto oraz rozkładów wartości szkód najczęściej wykorzystywanych w obliczeniach aktuarialnych), jak i praktyczne obliczenia polegające na szacowaniu wartości składek netto.

1. Pojęcia wstępne

1.1. Metody kalkulacji składek netto

Przyjmijmy, że X będzie zmienną losową oznaczającą wartość szkody wygenerowaną przez określone ryzyko ubezpieczeniowe. Przez $E(X)$, $D^2(X)$, γ, γ_2 oraz $M_X(t)$ oznaczamy odpowiednio: wartość oczekiwaną, wariancję, współczynnik skośności,

[1] Magdalena Majewska, studentka matematyki, Wydział Podstaw Techniki, Politechnika Lubelska, e-mail: magdalena.majewska1@pollub.edu.pl

kurtozę oraz funkcję generującą momenty zmiennej losowej X. $\Pi(X)$ symbolizować będzie natomiast wysokość składki netto na pokrycie szkody X.

Poniżej zaprezentowane zostaną najpopularniejsze metody kalkulacji składki netto $\Pi(X)$.

1. Zasada równoważności składki:

$$\Pi(X) = E(X).$$

2. Zasada wartości oczekiwanej:

$$\Pi(X) = (1+\theta)E(X),$$

gdzie parametr $\theta > 0$ oznacza współczynnik bezpieczeństwa.

3. Zasada wariancji:

$$\Pi(X) = E(X) + \theta D^2(X), \ \theta > 0.$$

4. Zasada odchylenia standardowego:

$$\Pi(X) = E(X) + \theta |D(X)|, \ \theta > 0.$$

5. Zasada percentylu (kwantyla rzędu ε):

$$\Pi(X) = \min\{p\colon F_X(p) \geqslant 1-\varepsilon\},$$

gdzie $0 < \varepsilon < 1$ oznacza maksymalną wartość prawdopodobieństwa straty w wyniku wystąpienia szkody X.

1.2. Rozkłady wartości szkód w ubezpieczeniach komunikacyjnych

W modelowaniu wartości szkód w ubezpieczeniach komunikacyjnych wykorzystuje się pewne ciągłe rozkłady prawdopodobieństwa. Przypomnijmy ponownie, że zmienna losowa X oznacza wartość szkody wypłacanej w ramach polisy ubezpieczeniowej związanej z określonym ryzykiem ubezpieczeniowym.

Poniżej zaprezentowane zostaną najpopularniejsze rozkłady prawdopodobieństwa zmiennej losowej X wykorzystywane w obliczeniach aktuarialnych oraz ich funkcje gęstości.

Rozkład gamma

Funkcja gęstości prawdopodobieństwa rozkładu gamma opisana jest wzorem:

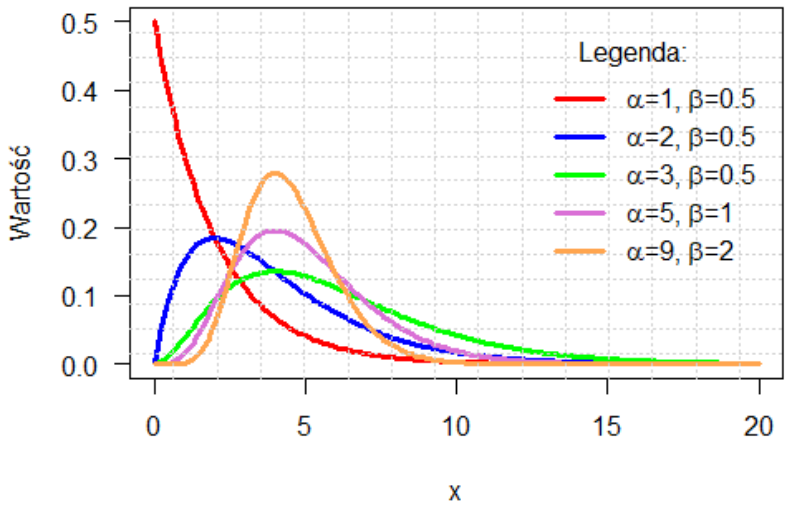
$$f(x) = \begin{cases} \frac{\beta^\alpha}{\Gamma(\alpha)} x^{\alpha-1} \exp(-\beta x) & \text{dla } x > 0, \\ 0 & \text{dla } x \leqslant 0, \end{cases}$$

gdzie

$$\Gamma(\alpha) = \int_0^{\infty} x^{\alpha-1} \exp(-x)\, \mathrm{dx} \quad \text{dla} \quad \alpha > 0.$$

Liczba α jest nazywana parametrem kształtu, a liczba $\beta > 0$ parametrem skali.

Na rysunku 1 przedstawiono wykresy funkcji gęstości rozkładu gamma dla wybranych wartości parametrów α i β.



Rysunek 1. Wykres funkcji gęstości rozkładu gamma dla wybranych parametrów α i β
Źródło: Opracowanie własne

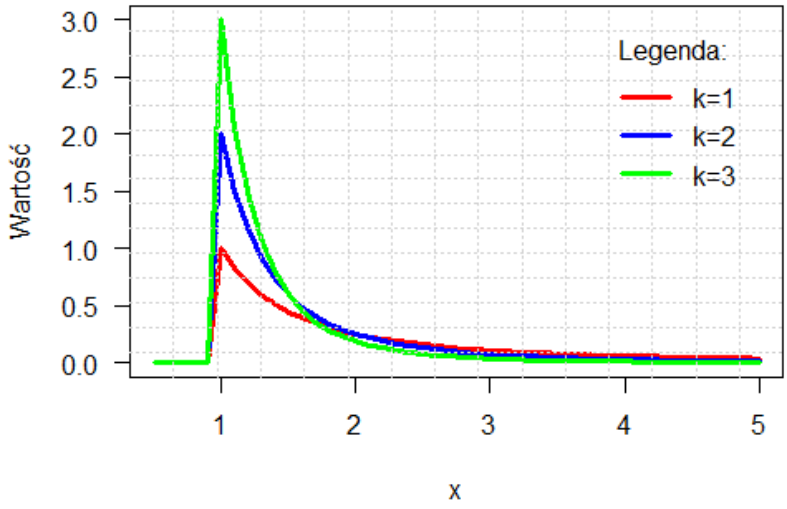
Rozkład Pareto

Funkcja gęstości prawdopodobieństwa rozkładu Pareto opisana jest wzorem:

$$f(x) = \begin{cases} \dfrac{k\theta^k}{x^{k+1}} & \text{dla} \quad x > \theta, \\ 0 & \text{dla} \quad x \leqslant \theta, \end{cases}$$

gdzie $k > 0$ jest parametrem kształtu, a $\theta > 0$ parametrem skali.

Na rysunku 2 przedstawiono wykresy funkcji gęstości rozkładu Pareto dla parametru $\theta = 1$ oraz różnych wartości parametru k.



Rysunek 2. Wykres funkcji gęstości rozkładu Pareto dla różnych wartości parametru k oraz $\theta = 1$
Źródło: Opracowanie własne

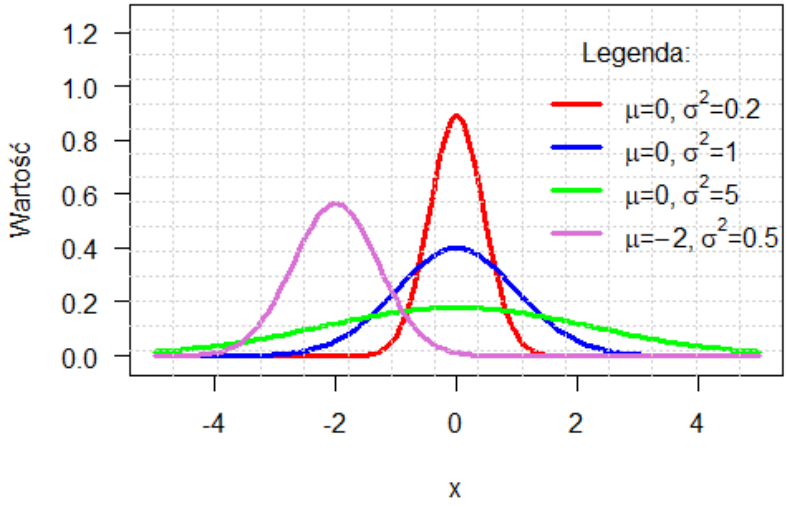
Rozkład normalny

Funkcja gęstości prawdopodobieństwa rozkładu normalnego opisana jest wzorem:

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{(x-\mu)^2}{2\sigma^2}\right\} \quad \text{dla} \quad x \in \mathbb{R},$$

gdzie $\mu \in \mathbb{R}$, $\sigma > 0$ są parametrami.

Na rysunku 3 przedstawiono wykresy funkcji gęstości rozkładu normalnego dla wybranych wartości parametrów μ i σ.



Rysunek 3. Wykres funkcji gęstości rozkładu normalnego dla różnych wartości parametrów μ i σ

Źródło: Opracowanie własne

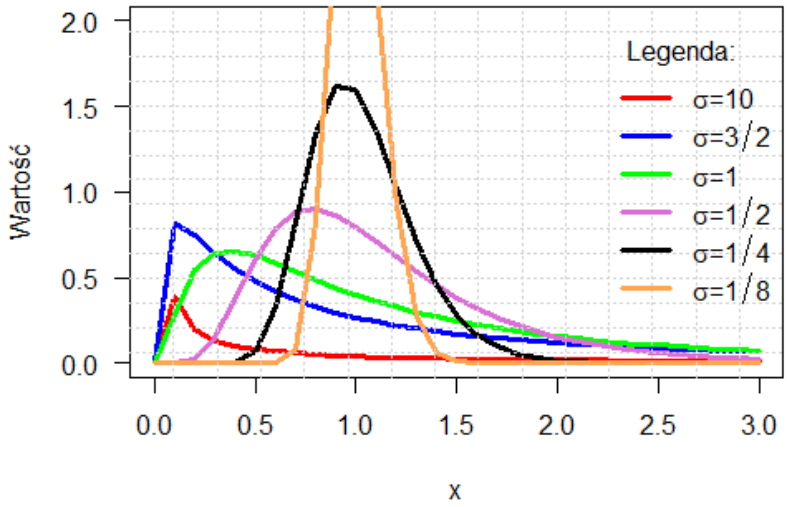
Rozkład logarytmiczno-normalny

Funkcja gęstości prawdopodobieństwa rozkładu logarytmiczno-normalnego opisana jest wzorem:

$$f(x) = \begin{cases} \dfrac{1}{\sigma\sqrt{2\pi}x} \exp\left[-\dfrac{(\ln x - \mu)^2}{2\sigma^2}\right] & \text{dla } x > 0, \\ 0 & \text{dla } x \leqslant 0, \end{cases}$$

gdzie $\mu \geqslant 0$, $\sigma > 0$ są parametrami.

Na rysunku 4 przedstawiono wykresy funkcji gęstości rozkładu logarytmiczno-normalnego dla parametru $\mu = 0$ oraz wybranych wartości parametru σ.



Rysunek 4. Wykres funkcji gęstości rozkładu logarytmiczno-normalnego dla parametru $\mu = 0$ oraz różnych wartości parametru σ
Źródło: Opracowanie własne

2. Kalkulacja składki netto w zastosowaniach praktycznych

2.1. Opis eksperymentu

W celu przeprowadzenia eksperymentu rozważono szacowanie składek netto dla rozkładów wartości szkód typu: gamma, Pareto, normalny oraz logarytmiczno-normalny, przy pomocy wybranych metod kalkulacji składek netto. W pierwszym etapie eksperymentu przyjęto określone wielkości dla wartości oczekiwanych oraz wariancji wybranych rozkładów. Są one proporcjonalne do średniej i wariancji wartości szkód w ubezpieczeniach komunikacyjnych OC publikowanych przez Polską Izbę Ubezpieczeń (PIU). Miary te prezentują się następująco:

— rozkład gamma: $E(X) = 9.98$, $D^2(X) = 41.3449$;
— rozkład Pareto: $E(X) = 9.95$, $D^2(X) = 39.3129$;
— rozkład normalny: $E(X) = 9.96$, $D^2(X) = 40.3225$;
— rozkład log-normalny: $E(X) = 9.97$, $D^2(X) = 41.3449$.

Można zauważyć, że poszczególne wartości odpowiednich charakterystyk w przybliżeniu są równe.

W kolejnym kroku, na podstawie określonych wyżej miar, obliczono parametry rozkładów. Otrzymano następujące wartości:
— rozkład gamma: $\alpha = 2.409012962$, $\beta = 0.2413840643$;
— rozkład Pareto: $\theta = 6.489995477$, $k = 2.875718784$;
— rozkład normalny: $\mu = 9.96$, $\sigma = 6.35$;
— rozkład log-normalny: $\mu = 2.125683455$, $\sigma = 0.5897408401$.

Z rozkładów o uzyskanych w wyniku obliczeń parametrach wygenerowane zostały cztery próby populacyjne o liczebności 20000 elementów każda. Dla ułatwienia wyżej wymienione próby będą w dalszej części pracy nazywane populacjami, choć w rzeczywistości nimi nie są. Następnie, z każdej z otrzymanych populacji wylosowano po 10 razy próby o liczebności 1000.

Dla wygenerowanych prób oraz populacji obliczono następujące wielkości:
— $E(X)$ – wartość oczekiwana populacji;
— $D(X)$ – odchylenie standardowe populacji;
— $D^2(X)$ – wariancja populacji;
— Me – mediana populacji;
— As – współczynnik asymetrii populacji;
— $\overline{x}_{min}$ – minimalna wartość średnich arytmetycznych z n-elementowej próby dla k repetycji;
— $\overline{x}_{max}$ – maksymalna wartość średnich arytmetycznych z n-elementowej próby dla k repetycji;
— $\widetilde{x} = \frac{1}{k}\sum_{j=1}^{k} \overline{x}_j$ – estymator średniej arytmetycznej dla próby o liczebności n z k repetycji;
gdzie $\overline{x}_j = \frac{1}{n}\sum_{i=1}^{n} x_i^{(j)}$ – średnia arytmetyczna dla j-tej repetycji;
— $MSE(\hat{\theta}) = E((\hat{\theta} - \theta)^2) = \frac{1}{k}\sum_{j=1}^{k} (\overline{x}_j - EX)^2$ – błąd średniokwadratowy estymatora $\hat{\theta} = EX$;
— S_{min} – minimalna wartość odchyleń standardowych z n-elementowej próby dla k repetycji;
— S_{max} – maksymalna wartość odchyleń standardowych z n-elementowej próby dla k repetycji;
— $\widetilde{S}$ – średnia arytmetyczna odchyleń standardowych z k repetycji;
— Me_S – mediana odchyleń standardowych z n-elementowej próby dla k repetycji;

— $\widetilde{S}_x^2 = \frac{1}{nk}\sum_{l=1}^{nk} x_l^2 - (\widetilde{x})^2$ – estymator wariancji dla próby o liczebności n z k repetycji;
— V_S^{min} – minimalna wartość współczynników zmienności z n-elementowej próby dla k repetycji;
— V_S^{max} – maksymalna wartość współczynników zmienności z n-elementowej próby dla k repetycji;
— Me_{min} – minimalna wartość median z n-elementowej próby dla k repetycji;
— Me_{max} – maksymalna wartość median z n-elementowej próby dla k repetycji;
— $\widetilde{Me} = \frac{1}{k}\sum_{j=1}^{k} Me_j$ – średnia arytmetyczna median z k repetycji;
gdzie Me_j – mediana z j-tej repetycji;
— $d_{Me} = \frac{1}{k}\sum_{j=1}^{k} |Me_j - Me|$ – odchylenie przeciętne mediany.

Tabela 1 przedstawia klasyczne i pozycyjne miary struktury obliczone dla populacji i prób wylosowanych z wybranych rozkładów wartości szkód.

2.2. Szacowanie składek netto dla wybranych rozkładów wartości szkód

W kolejnym etapie eksperymentu oszacowano składki dla uprzednio wymienionych rozkładów wartości szkód (rozkład gamma, Pareto, normalny, logarytmiczno-normalny) oraz wybranych metod kalkulacji składki netto (zasada równoważności składki, wartości oczekiwanej, wariancji, odchylenia standardowego oraz kwantyla rzędu ε).

W tabelach 2, 3, 4, 5 przedstawione zostały wartości składek netto obliczone odpowiednio dla rozkładów: gamma, Pareto, normalnego i logarytmiczno-normalnego. Składki te oszacowano na podstawie minimalnych i maksymalnych wartości mediany i średniej arytmetycznej, estymatorów parametrów populacji otrzymanych w 10 repetycjach, a także na podstawie parametrów populacji.

Dla wszystkich tabel przyjęto następujące oznaczenia:

— próba (min) – wartość składki netto wyznaczona na podstawie minimalnych wartości średniej arytmetycznej i mediany otrzymanych z 10 repetycji;
— próba (est) – wartość składki netto wyznaczona na podstawie estymatorów wartości oczekiwanej i mediany otrzymanych z 10 repetycji;
— próba (max) – wartość składki netto wyznaczona na podstawie maksymalnych wartości średniej arytmetycznej i mediany otrzymanych z 10 repetycji;
— populacja – wartość składki netto wyznaczona na podstawie parametrów populacji.

Tabela 1. Wartości miar dla populacji i prób losowanych z badanych rozkładów

	Rozkład gamma	Rozkład Pareto	Rozkład normalny	Rozkład log-normalny
$E(X)$	9.98	9.95	9.96	9.97
$D(X)$	6.43	6.27	6.35	6.43
$D^2(X)$	41.3449	39.3129	40.3225	41.3449
Me	8.5769	8.2589	9.96	8.3786
As	1.2886	-34.4180	0	2.2030
$\bar{x}_{min}$	9.5780	9.7692	9.5387	9.5733
$\bar{x}_{max}$	10.1277	10.3458	9.8964	10.0359
$\widetilde{x}$	9.9027	10.0432	9.7551	9.7808
$MSE(\hat{\theta})$	0.0367	0.0452	0.0525	0.0518
S_{min}	6.3266	4.6536	6.1912	5.8320
S_{max}	6.6262	11.2780	6.6035	7.0216
$\widetilde{S}$	6.4277	6.0616	6.3566	6.2679
Me_S	6.4006	5.3115	6.3675	6.2365
$\widetilde{S_x^2}$	41.3241	40.3397	40.4213	39.3806
V_S^{min}	62.8543	47.0652	63.2306	60.9190
V_S^{max}	67.0257	109.0104	67.7904	69.9648
Me_{min}	8.0864	8.1902	9.3513	7.9181
Me_{max}	8.9041	8.4575	10.1710	8.5445
$\widetilde{Me}$	8.5577	8.2880	9.7963	8.2541
d_{Me}	0.1922	0.0737	0.2296	0.1761

Źródło: Opracowanie własne

Tabela 2. Wartości składek netto oszacowane różnymi metodami dla rozkładu wartości szkód typu gamma

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	9.5780	14.367	30.24005	12.79219	8.0864
próba (est)	9.9027	14.85405	30.56475	13.11689	8.5577
próba (max)	10.1277	15.19155	30.78975	13.34189	8.9041
populacja	9.98	14.97	30.65245	13.195	8.5769

Źródło: Opracowanie własne

Tabela 3. Wartości składek netto oszacowane różnymi metodami dla rozkładu wartości szkód typu Pareto

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	9.7692	14.6538	29.93905	12.94488	8.1902
próba (est)	10.0432	15.0648	30.21305	13.21888	8.2880
próba (max)	10.3458	15.5187	30.51565	13.52148	8.4575
populacja	9.95	14.925	29.60645	13.085	8.2589

Źródło: Opracowanie własne

Tabela 4. Wartości składek netto oszacowane różnymi metodami dla rozkładu wartości szkód typu normalnego

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	9.5387	14.30805	29.74935	12.71759	9.3513
próba (est)	9.7551	14.63265	29.96575	12.93399	9.7963
próba (max)	9.8964	14.8446	30.10705	13.07529	10.1710
populacja	9.96	14.94	30.12125	13.135	9.96

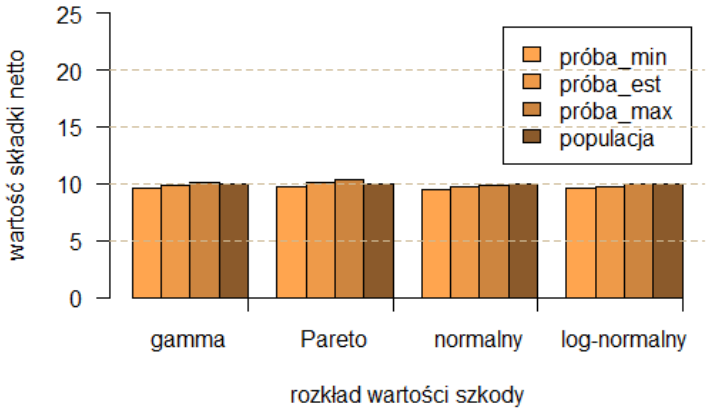
Źródło: Opracowanie własne

Tabela 5. Wartości składek netto oszacowane różnymi metodami dla rozkładu wartości szkód typu logarytmiczno-normalnego

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	9.5733	14.35995	29.2636	12.711	7.9181
próba (est)	9.7808	14.6712	29.4711	12.9185	8.2541
próba (max)	10.0359	15.05385	29.7262	13.1736	8.5445
populacja	9.97	14.955	30.64245	13.185	8.3786

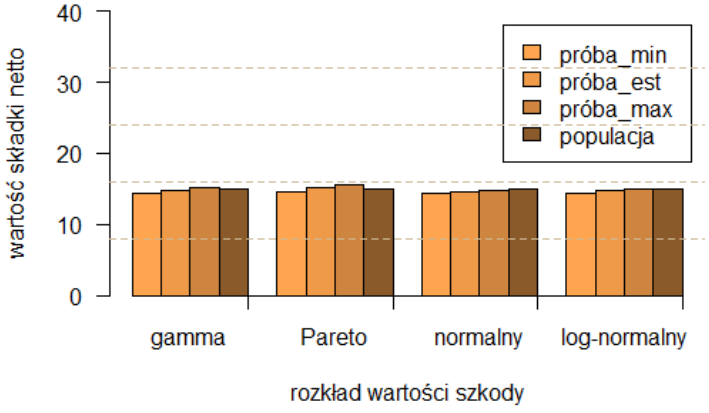
Źródło: Opracowanie własne

Na wykresach zaprezentowanych na rysunkach 5–9 przedstawione zostały wartości składek netto oszacowane dla kolejnych metod kalkulacji składek netto: zasady równoważności składki, zasady wartości oczekiwanej, zasady wariancji, zasady odchylenia standardowego oraz zasady kwantyla rzędu 0.5. Współczynnik bezpieczeństwa θ ponownie równy jest 0.5.



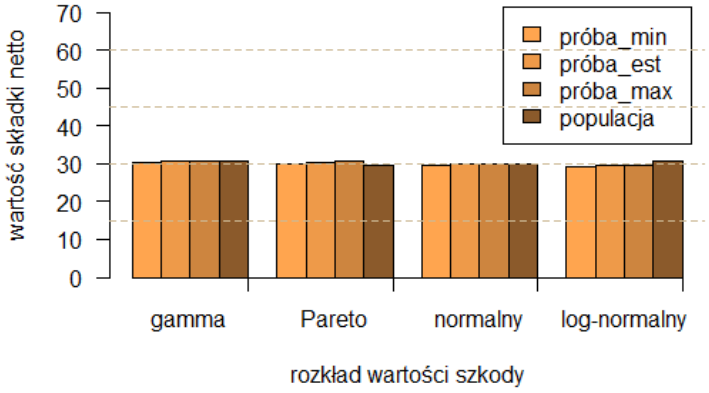
Rysunek 5. Wartość składki netto wyznaczonej przy pomocy zasady równoważności składki dla różnych rozkładów wartości szkód

Źródło: Opracowanie własne

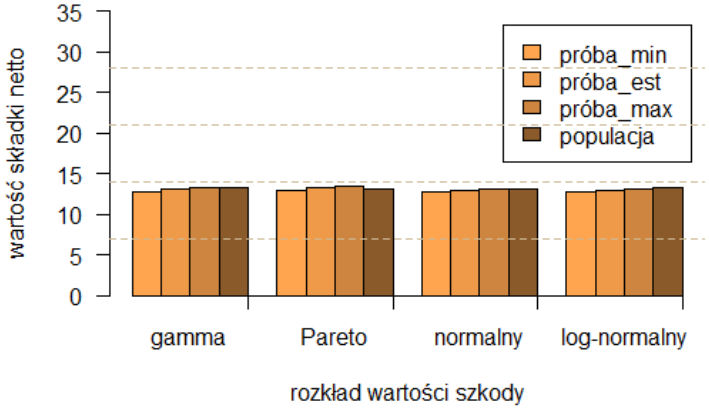


Rysunek 6. Wartość składki netto wyznaczonej przy pomocy zasady wartości oczekiwanej dla różnych rozkładów wartości szkód

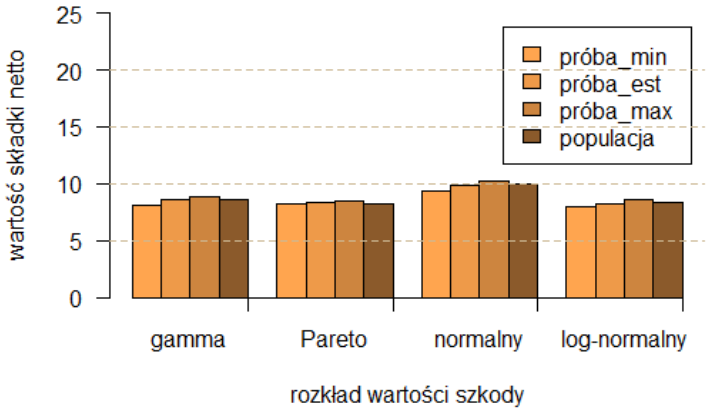
Źródło: Opracowanie własne



Rysunek 7. Wartość składki netto wyznaczonej przy pomocy zasady wariancji dla różnych rozkładów wartości szkód
Źródło: Opracowanie własne



Rysunek 8. Wartość składki netto wyznaczonej przy pomocy zasady odchylenia standardowego dla różnych rozkładów wartości szkód
Źródło: Opracowanie własne



Rysunek 9. Wartość składki netto wyznaczonej przy pomocy zasady kwantyla rzędu 0.5 **dla różnych rozkładów wartości szkód**
Źródło: Opracowanie własne

2.3. Szacowanie składek netto dla rozkładu gamma wartości szkód

W kolejnym etapie obliczeń analizie zostały poddane wartości składek netto oszacowane dla różnych wartości parametrów rozkładu gamma oraz wybranych zasad wyznaczania składek netto. Składki oszacowano dla przypadku, w którym parametr α jest stale równy jeden, podczas gdy parametr β dla kolejnych przypadków wzrasta.

Tabele 6–9 przedstawiają wartości składek netto obliczone dla rozkładu gamma z różnymi parametrami α i β przy pomocy wybranych metod kalkulacji składek (zasada równoważności składki, zasada wartości oczekiwanej, zasada wariancji, zasada ochylenia standardowego, zasada kwantyla rzędu ε). Składki te, podobnie jak poprzednio, oszacowano na podstawie minimalnych i maksymalnych wartości mediany i średniej arytmetycznej, estymatorów parametrów populacji otrzymanych w 10 repetycjach, a także na podstawie parametrów populacji.

Tabela 6. Wartości składek netto oszacowane różnymi metodami kalkulacji składek dla rozkładu wartości szkód typu gamma z parametrami $\alpha = 1$, $\beta = 2$

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	0.4899	0.7349	0.6176	0.7426	0.3257
próba (est)	0.5068	0.7602	0.6345	0.7595	0.3455
próba (max)	0.5380	0.8070	0.6656	0.7906	0.3629
populacja	0.5	0.75	0.625	0.75	0.3451

Źródło: Opracowanie własne

Tabela 7. Wartości składek netto oszacowane różnymi metodami kalkulacji składek dla rozkładu wartości szkód typu gamma z parametrami $\alpha = 1$, $\beta = 3$

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	0.3266	0.4899	0.38346	0.4951	0.2171
próba (est)	0.3379	0.5068	0.3946	0.5063	0.23046
próba (max)	0.3587	0.5380	0.4154	0.5271	0.2419
populacja	0.3333	0.5	0.3889	0.5	0.2301

Źródło: Opracowanie własne

Tabela 8. Wartości składek netto oszacowane różnymi metodami kalkulacji składek dla rozkładu wartości szkód typu gamma z parametrami $\alpha = 1$, $\beta = 4$

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	0.2450	0.3675	0.2769	0.3713	0.1629
próba (est)	0.2534	0.3801	0.2853	0.3797	0.1728
próba (max)	0.2690	0.4035	0.3009	0.3953	0.1814
populacja	0.25	0.375	0.2813	0.375	0.1725

Źródło: Opracowanie własne

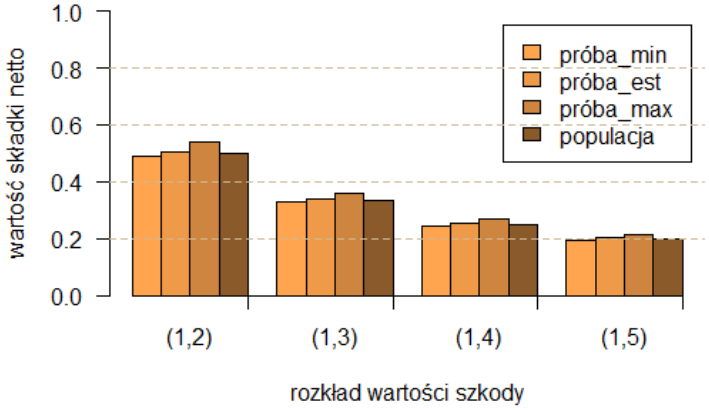
Tabela 9. Wartości składek netto oszacowane różnymi metodami kalkulacji składek dla rozkładu wartości szkód typu gamma z parametrami $\alpha = 1$, $\beta = 5$

Sposób doboru parametrów	Zasada wyznaczania składki netto				
	równoważności składki	wartości oczekiwanej $\theta = 0.5$	wariancji $\theta = 0.5$	odchylenia standardowego $\theta = 0.5$	kwantyla rzędu 0.5
próba (min)	0.1960	0.2940	0.2164	0.2970	0.1303
próba (est)	0.2027	0.3041	0.2232	0.3038	0.1382
próba (max)	0.2152	0.3228	0.2356	0.3162	0.1451
populacja	0.2	0.3	0.22	0.3	0.1380

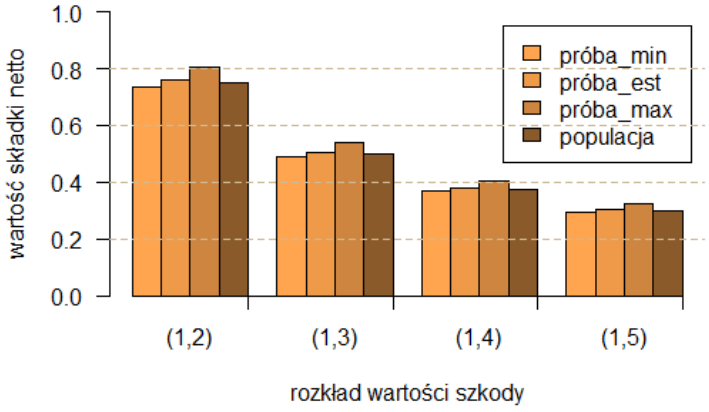
Źródło: Opracowanie własne

Wykresy zaprezentowane na rysunkach 10–14 przedstawiają wartości składek netto oszacowane dla kolejnych zasad wyznaczania składek netto oraz różnych parametrów rozkładu gamma. Przyjęto następujące oznaczenia:
— $(1,2)$ – rozkład gamma z parametrami $\alpha = 1$ i $\beta = 2$;
— $(1,3)$ – rozkład gamma z parametrami $\alpha = 1$ i $\beta = 3$;

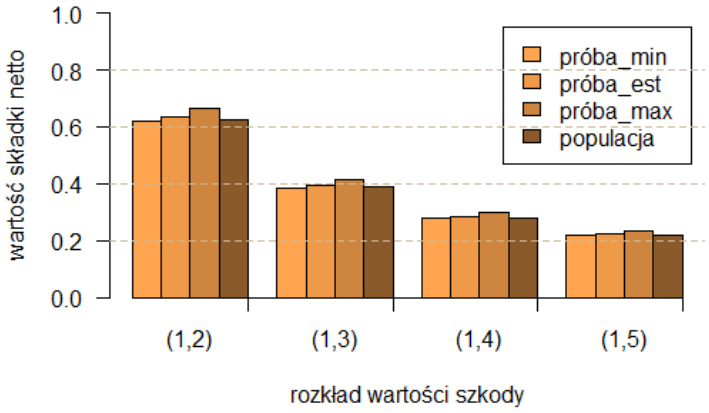
— $(1,4)$ – rozkład gamma z parametrami $\alpha = 1$ i $\beta = 4$;
— $(1,5)$ – rozkład gamma z parametrami $\alpha = 1$ i $\beta = 5$.



Rysunek 10. Wartości składek netto oszacowane przy pomocy zasady równoważności składki dla różnych wartości parametrów rozkładu gamma
Źródło: Opracowanie własne

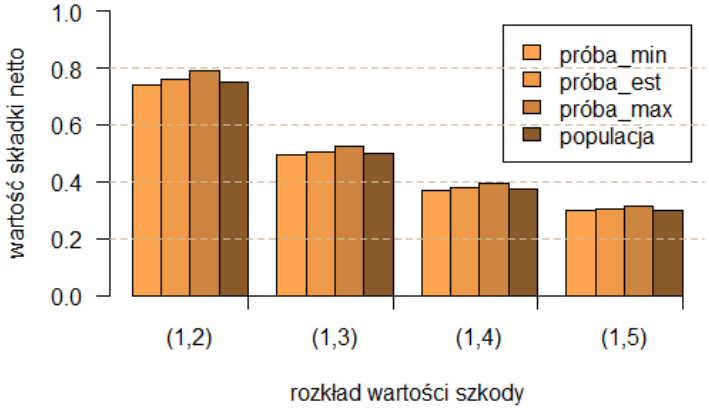


Rysunek 11. Wartości składek netto oszacowane przy pomocy zasady wartości oczekiwanej dla różnych wartości parametrów rozkładu gamma
Źródło: Opracowanie własne



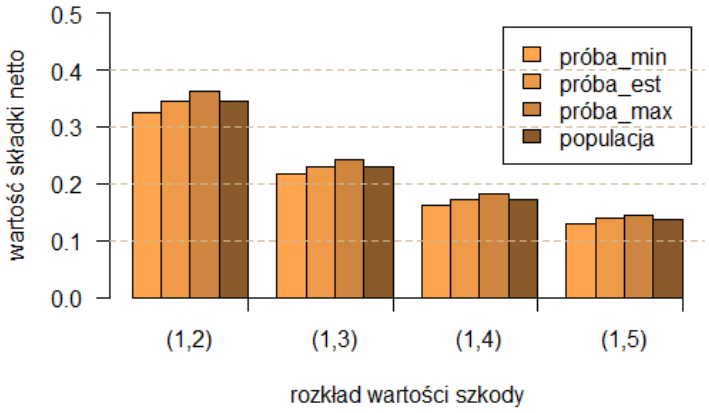
Rysunek 12. Wartości składek netto oszacowane przy pomocy zasady wariancji dla różnych wartości parametrów rozkładu gamma

Źródło: Opracowanie własne



Rysunek 13. Wartości składek netto oszacowane przy pomocy zasady odchylenia standardowego dla różnych wartości parametrów rozkładu gamma

Źródło: Opracowanie własne



Rysunek 14. Wartości składek netto oszacowane przy pomocy zasady kwantyla rzędu ε dla różnych wartości parametrów rozkładu gamma
Źródło: Opracowanie własne

Z przeprowadzonych obliczeń wynika, że wartości składek oszacowane wybranymi metodami kalkulacji składek netto dla prób i populacji istotnie się od siebie różnią. Ponadto składki wyznaczone przy pomocy tych samych zasad kalkulacji składek, dla minimalnych i maksymalnych wartości średniej arytmetycznej i mediany nie różnią się od siebie istotnie. Znaczny wpływ na wysokość składki ma dobór metody jej kalkulacji. Składka obliczona przy pomocy zasady wariancji przyjmuje wartości największe, znacznie wyróżniające się na tle składek oszacowanych przy pomocy pozostałych metod. Dla rozkładu wartości szkód typu gamma również nie ma znaczenia dobór metody kalkulacji składki, a jedynie wybór parametrów tego rozkładu. Im mniejszą wartość osiągnie parametr β tym większa będzie wartość składki ubezpieczeniowej netto.

3. Podsumowanie

Na wysokość składki ubezpieczeniowej netto może wpływać wiele czynników. Wartość składki może różnić się w zależności od wyboru metody jej wyznaczania, rozkładu wartości szkody, doboru parametrów tego rozkładu oraz wartości współczynnika bezpieczeństwa mającego na celu zabezpieczenie i ochronę ubezpieczyciela przed bankructwem.

Wartości składek oszacowane wybranymi metodami kalkulacji składek dla prób i populacji istotnie różnią się od siebie. Świadczy to o tym, że wylosowana próba o liczebności 1000 niezbyt dobrze opisuje parametry populacji oraz wartości składek netto.

W rozdziale tym oszacowano również składki dla minimalnych i maksymalnych wartości średniej arytmetycznej i mediany uzyskanych w 10 repetycjach. Wyniki pokazują, że nie ma istotnych, co do wartości, różnic między składkami wyznaczonymi tymi samymi metodami. Dla wszystkich analizowanych rozkładów największe różnice widać w przypadku zasady wartości oczekiwanej.

Wartości składek netto obliczone przy pomocy tej samej zasady kalkulacji składki oraz dla rozkładów wartości szkód typu: gamma, Pareto, normalnego i logarytmiczno-normalnego są w przybliżeniu równe. Jest to spowodowane doborem bardzo zbliżonych charakterystyk $E(X)$ oraz $D^2(X)$ tych rozkładów. Można więc stwierdzić, że na wartość składki nie ma istotnego wpływu wybór rozkładu, a jedynie dobór jego parametrów.

Znaczny wpływ na wartość składki ma zasada jej kalkulacji. Składka obliczona przy pomocy zasady wariancji przyjmuje wartości największe, znacznie wyróżniające się na tle składek oszacowanych za pomocą pozostałych metod.

Kolejnym aspektem poddanym analizie jest szacowanie składek netto na podstawie różnych wartości parametrów α i β rozkładu gamma. Podobnie jak poprzednio można zauważyć, że nie ma istotnych różnic między wartościami składek wyznaczanych dla kolejnych sposobów doboru parametrów α i β rozkładów. Składki netto przyjmują wartości największe dla zasady wartości oczekiwanej i zasady odchylenia standardowego oraz wartości najmniejsze dla zasady kwantyla rzędu 0.5. W oparciu o przeprowadzone obliczenia można stwierdzić, że dobór parametrów rozkładu gamma istotnie różnicuje wartości składek netto. Wraz ze wzrostem parametru β maleją wartości składek netto oszacowanych dla kolejnych zasad wyznaczania składek. Składki przyjmują wartości największe dla rozkładu gamma z parametrami $\alpha = 1$ i $\beta = 2$ oraz wartości najmniejsze dla parametrów $\alpha = 1$ i $\beta = 5$.

Literatura

[1] N. L. Bowers, H. U. Gerber, J. C. Hickman, D. A. Jones, C. J. Nesbitt, *Actuarial Mathematics*, The Society od Actuaries, 1997.

[2] H. Bühlmann, *Mathematical Methods in Risk Theory*, Springer-Verlag, Berlin, Heidelberg 2005.

[3] C. D. Daykin, T. Pentikainen, M. Pesonen, *Practical Risk Theory for Actuaries*, Chapman and Hall, London 1993.

[4] Cz. Domański, K. Pruska, *Nieklasyczne metody statystyczne*, PWE, Warszawa 2000.

[5] R. Kaas, M. Goovaerts, J. Dhaene, M. Denuit, *Modern Actuarial Risk Theory*, Kluwer, Boston 2001.
[6] P. Kowalczyk, E. Poprawska, W. Ronka-Chmielowiec, *Metody aktuarialne*, Wydawnictwo Naukowe PWN, Wrocław 2006.
[7] W. Królikowski, *Zastosowanie matematyki w ubezpieczeniach. Zasady i metody liczenia składek ubezpieczeniowych*, Wydawnictwo Naukowe Wyższej Szkoły Kupieckiej, Łódź 2006.
[8] J. Lemaire, *Bonus-Malus System in Automobile Insurance*, Kluwer Nijhoff, Boston 1995.
[9] A. Szymańska, *Wyznaczanie składki netto na podstawie próby dla różnych rozkładów wielkości szkód w ubezpieczeniach komunikacyjnych*, Katedra Metod Statystycznych, Wydział Ekonomiczno-Socjologiczny, Uniwersytet Łódzki, Łódź 2012.
[10] Strona internetowa Polskiej Izby Ubezpieczeń, dostęp: https://piu.org.pl (data dostępu 25.09.2020).

Aleksandra Pawłowska[1], **Izabela Szady**[2]

Złota liczba

Streszczenie

W artykule tym poruszone zostały zagadnienia związane ze złotą liczbą. Znajdują się tutaj wyjaśnienie tego pojęcia, sposób wyznaczenia złotego podziału, jego własności, a także związek z ciągiem Fibonacciego. Podane są przykłady, w których wykorzystywana jest złota proporcja.

Słowa kluczowe: złota liczba, złota proporcja, złoty podział, ciąg Fibonacciego

Wstęp

> Nauki matematyczne szczególną uwagę zwracają na ład, symetrię i ograniczenie, a są to najwyższe formy piękna.
>
> Arystoteles

W matematyce znajdujemy wiele stałych matematycznych, jednak szczególną uwagę chcemy zwrócić na złotą liczbę. W przeciwieństwie do innych stałych, z proporcją wyznaczoną przez tę liczbę spotykamy się codziennie, ale zwykle nie jesteśmy tego świadomi. Przyjrzyjmy się tej liczbie i zobaczmy, gdzie w naszym życiu codziennym możemy ją odnaleźć.

1. Złota proporcja

1.1. Wyznaczanie złotej liczby

Mając dany odcinek można go podzielić tak, by stosunek długości dłuższej części do krótszej był taki sam, jak całego odcinka do części dłuższej. Zagadnienie to znane jest jako problem złotego podziału odcinka. Idea tego podziału przedstawiona jest

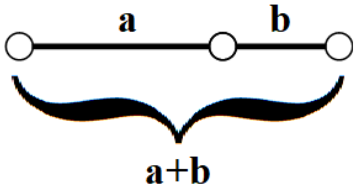
[1] Aleksandra Pawłowska, studentka matematyki, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

[2] Izabela Szady, studentka matematyki, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

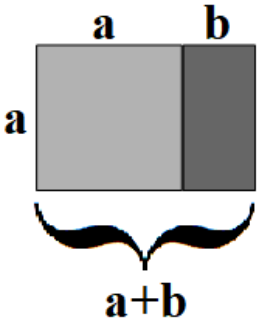
na rysunku 1. Niech a oznacza długości części dłuższej, zaś b – części krótszej odcinka, który chcemy podzielić. Algebraicznie oznacza to wyznaczenie proporcji:

$$\frac{a+b}{a} = \frac{a}{b}. \tag{1}$$

Otrzymaną liczbę $\varphi = \frac{a}{b}$ nazywamy **złotą liczbą**. Rysunek 2 przedstawia prostokąt, w którym boki pozostają do siebie w złotej proporcji



Rysunek 1. Złota proporcja odcinka
Źródło: własne



Rysunek 2. Złoty prostokąt
Źródło: własne

Korzystając z wprowadzonego oznaczenia wzór (1) możemy zapisać w postaci równania:

$$1 + \frac{1}{\varphi} = \varphi, \tag{2}$$

równoważnego równaniu:

$$\varphi^2 - \varphi - 1 = 0. \tag{3}$$

Równanie to ma dwa pierwiastki, z których dodatni:

$$\varphi = \frac{1+\sqrt{5}}{2} = 1,6180339887... \tag{4}$$

jest właśnie naszą złotą liczbą.

1.2. Własności złotej liczby

— Odwrotność liczby φ

Odwrotność złotej liczby wynosi

$$\frac{1}{\varphi} = 0,6180339887....$$

Otrzymujemy ją poprzez odjęcie 1 od liczby φ.

— Ułamek łańcuchowy liczby φ

Złotą liczbę można przedstawić w postaci ułamka łańcuchowego (więcej informacji o ułamkach łańcuchowych możemy znaleźć w [7])

$$\varphi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + ...}}}.$$

— Z równości (3) zapisanej w postaci

$$\varphi^2 = \varphi + 1$$

wynika (przez pomnożenie obydwóch stron przez φ^{n-2}) równość:

$$\varphi^n = \varphi^{n-1} + \varphi^{n-2}.$$

Przypadki szczególne to:
— $\varphi^2 = 2,6180339887...$, co oznacza, że $\varphi^2 = \varphi + 1$,
— $\varphi^3 = \varphi^2 + \varphi = 2\varphi + 1$,
— $\varphi^4 = \varphi^3 + \varphi^2 = (\varphi + 1) + (2\varphi + 1) = 3\varphi + 2$.

2. Złota liczba a ciąg Fibonacciego

2.1. Ciąg Fibonacciego

Ciąg Fibonacciego to ciąg rekurencyjny liczb naturalnych określony jako:

$$f_n = \begin{cases} 0 & \text{dla } n = 0 \\ 1 & \text{dla } n = 1 \\ f_{n-1} + f_{n-2} & \text{dla } n > 1 \end{cases}. \tag{5}$$

Pierwszymi wyrazami ciągu Fibonacciego są:

$$0,1,1,2,3,5,8,13,21,34,55,89,144,233,377,610,\ldots .$$

2.2. Jaki jest związek między złotą proporcją a ciągiem Fibonacciego?

Twierdzenie 2.1. *(Wzór Eulera-Bineta* [1]*) Wzór jawny na ciąg Fibonacciego ma postać:*

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \tag{6}$$

Przed przystąpieniem do dowodu równości (6) przypomnimy pewne określenia i fakty.

Będziemy rozważać równania rekurencyjne postaci:

$$t_n = at_{n-1} + bt_{n-2}, \tag{7}$$

gdzie $a,b \in \mathbb{R}, n \geqslant 2$.

Rozwiązaniem równania (7) nazywamy każdy ciąg (t_n), $n \geqslant 0$, spełniający powyższą równość.

Niech c_1, c_2 będą liczbami zespolonymi. Rozważmy funkcję

$$n \to f(n; c_1, c_2) \tag{8}$$

zmiennej całkowitej $n \geqslant 0$, o wartościach w zbiorze liczb zespolonych, gdzie c_1, c_2 pełnią rolę parametrów.

Jeżeli dla każdego rozwiązania $(t_n), n \geqslant 0$ równania (7) da się dobrać takie wartości parametrów c_1, c_2, że równość

$$t_n = f(n; c_1, c_2) \tag{9}$$

zachodzi dla wszystkich $n \geqslant 0$, to mówimy, że wzór (9) opisuje rozwiązanie ogólne równania rekurencyjnego (7).

Równaniem charakterystycznym równania (7) nazywamy równanie kwadratowe

$$x^2 - ax - b = 0 \tag{10}$$

z niewiadomą x.

Następujący lemat pochodzi z książki [6] (z niewielkimi zmianami redakcyjnymi).

Lemat 2.2. *Dane jest równanie rekurencyjne postaci:*

$$t_n = at_{n-1} + bt_{n-2} \tag{11}$$

gdzie $a, b \in \mathbb{R}, n \geqslant 2$. *Jeżeli jego równanie charakterystyczne ma dwa różne pierwiastki* $x_1 \neq x_2$, *to rozwiązanie ogólne równania rekurencyjnego ma postać:*

$$t_n = c_1 x_1^n + c_2 x_2^n. \tag{12}$$

Dowód twierdzenia 2.1. Równanie charakterystyczne ciągu Fibonacciego ma postać:

$$x^2 - x - 1 = 0. \tag{13}$$

Pierwiastki równania to:

$$x_1 = \frac{1+\sqrt{5}}{2}, \quad x_2 = \frac{1-\sqrt{5}}{2}. \tag{14}$$

Żaden z ciągów:

$$x_1^n = \left(\frac{1+\sqrt{5}}{2}\right)^n, \quad x_2^n = \left(\frac{1-\sqrt{5}}{2}\right)^n, \quad n \geqslant 1$$

nie jest ciągiem Fibonacciego.

Zgodnie z lematem 2.2, ciąg Fibonacciego ma postać

$$f_n = c_1 x_1^n + c_2 x_2^n \tag{15}$$

i wystarczy wyznaczyć wartości stałych c_1, c_2. Wiemy, że $f_0 = 0$ i $f_1 = 1$. Otrzymujemy więc układ równań z niewiadomymi c_1, c_2 postaci

$$\begin{cases} f_0 = c_1 + c_2, \\ f_1 = c_1 x_1 + c_2 x_2, \end{cases} . \tag{16}$$

czyli:

$$\begin{cases} c_1 + c_2 = 0, \\ \left(\frac{1+\sqrt{5}}{2}\right) c_1 + \left(\frac{1-\sqrt{5}}{2}\right) c_2 = 1 \end{cases} \tag{17}$$

Jego rozwiązaniami są liczby:

$$c_1 = \frac{1}{\sqrt{5}}, \quad c_2 = -\frac{1}{\sqrt{5}}.$$

Wstawiając te liczby do wzoru (15) otrzymujemy

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right],$$

czyli wzór Eulera-Bineta (6). □

Zauważmy ponadto, że:

$$\lim_{n\to\infty}\left(\frac{1-\sqrt{5}}{2}\right)^n = 0. \tag{18}$$

Otrzymujemy stąd:

$$f_n \simeq \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n = \frac{1}{\sqrt{5}}\varphi^n. \tag{19}$$

Następne twierdzenie pokazuje związek między ciągiem Fibonacciego a liczbą φ.

Twierdzenie 2.3. *(Twierdzenie Keplera) Granicą ilorazów sąsiednich elementów ciągu Fibonacciego jest liczba* φ*:*

$$\lim_{n\to\infty}\frac{f_{n+1}}{f_n} = \varphi. \tag{20}$$

Dowód twierdzenia 2.3. Z (6) wiemy, że

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \tag{21}$$

Zatem:

$$\lim_{n\to\infty}\frac{f_{n+1}}{f_n} = \lim_{n\to\infty}\frac{\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right]}{\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n}\right]}$$

$$= \lim_{n\to\infty} \frac{\frac{1+\sqrt{5}}{2} - \left(\frac{1-\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^n}{1-\left(\frac{1-\sqrt{5}}{2}\cdot\frac{2}{1+\sqrt{5}}\right)^n}$$

$$= \frac{\frac{1+\sqrt{5}}{2} - \left(\frac{1-\sqrt{5}}{2}\right)\lim\limits_{n\to\infty}\left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^n}{1-\lim\limits_{n\to\infty}\left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^n}$$

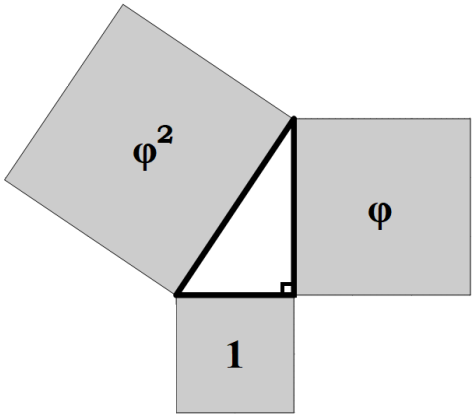
$$= \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\cdot 0}{1-0} = \frac{1+\sqrt{5}}{2} = \varphi. \tag{22}$$

□

3. Złota liczba w życiu codziennym

Matematycy od starożytności w swoich działaniach nawiązywali do złotego podziału. Fidiasz (490–430 p.n.e.), od którego pochodzi nazwa złotej liczby φ, stworzył figury Partenonu zachowując złote proporcje, a Platon (427–347 p.n.e.), opisywał połączone ze złotym podziałem wielościany foremne. Również wspomniany wcześniej stosunek kolejnych wyrazów ciągu Fibonacciego tworzy złoty podział.

Ważną postacią związaną ze złotą liczbą jest Michael Maestlin (1550–1631), który jako pierwszy obliczył wartość przybliżenia odwrotności tej liczby w postaci dziesiętnego ułamka $(0,6180339887...)$. Natomiast Johannes Kepler uważał, że najważniejszymi skarbami są: twierdzenie Pitagorasa oraz złoty podział, które zostały zawarte w trójkącie Keplera przedstawionego na rysunku 3.

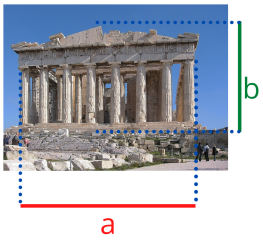


Rysunek 3. Trójkąt Keplera
Źródło: własne

3.1. Złota liczba w architekturze

Złota liczba jest w sposób szczególny obecna w architekturze. Bardzo wiele słynnych zabytkowych obiektów było projektowanych z wykorzystaniem złotej proporcji. W tym podrozdziale prezentujemy przykłady najsłynniejszych z nich.

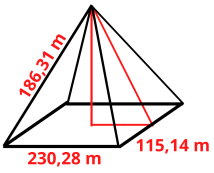
— Partenon (świątynia Ateny na Akropolu) – fronton tej świątyni, przedstawiony na rysunku 4, mieści się w złotym prostokącie, którego stosunek boków wynosi φ.



Rysunek 4. Fronton Partenonu
Źródło: opracowanie własne na podstawie [10]

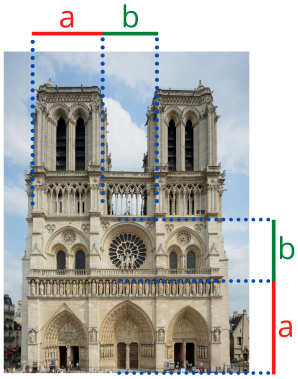
— Piramida Cheopsa – stosunek krawędzi bocznej ściany piramidy do połowy podstawy jest bliski liczby φ, Wymiary piramidy zostały przedstawione na rysunku 5.

$$\frac{186,31}{115,14} = 1,61811 \approx \varphi$$



Rysunek 5. Wymiary Piramidy Cheopsa
Źródło: opracowanie własne na podstawie [4]

— Katedra Notre-Dame w Paryżu – stosunki wymiarów a i b zaznaczonych na rysunku 6 wynoszą φ.



Rysunek 6. Katedra Notre-Dame
Źródło: opracowanie własne na podstawie [11]

3.2. Złota liczba w sztuce

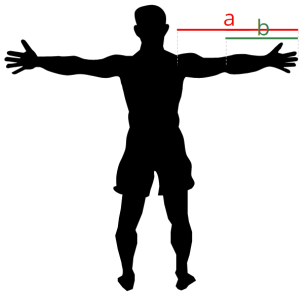
Złotą proporcję stosowali w swych dziełach również wybitni artyści, zarówno ci starożytni i renesansowi jak i współcześni.

— Mona Lisa Leonarda da Vinci – proporcje ciała na obrazie zachowują złoty podział, np. prostokąt konstruowany wokół twarzy jest złotym prostokątem.
— Obrazy mają wymiary złotego prostokąta, ponieważ jest on "przyjemny dla oka", np. Sakrament Ostatniej Wieczerzy Salvadora Dali.
— Wenus z Milo – rzeźba jest tak idealna, że zachowuje złote proporcje i uchodzi za symbol doskonałego ludzkiego ciała.

3.3. Złota liczba w naturze

Przykłady złotej proporcji znajdujemy również w naturze.

— Rośliny – układ nasion słonecznika jest stworzony przez 34 spirale prawoskrętne oraz 55 spirali lewoskrętnych. Stosunek spirali $\frac{55}{34}$ zbliżony jest do złotej proporcji. Takie rozmieszczenie nasion słonecznika pozwala im wykorzystać w pełni miejsce w kwiatostanie.
— Człowiek – proporcje naszego ciała są zbliżone do złotego podziału, np. odległość pomiędzy końcem palców a ramieniem i między końcem palców a łokciem, co widzimy na rysunku 7.

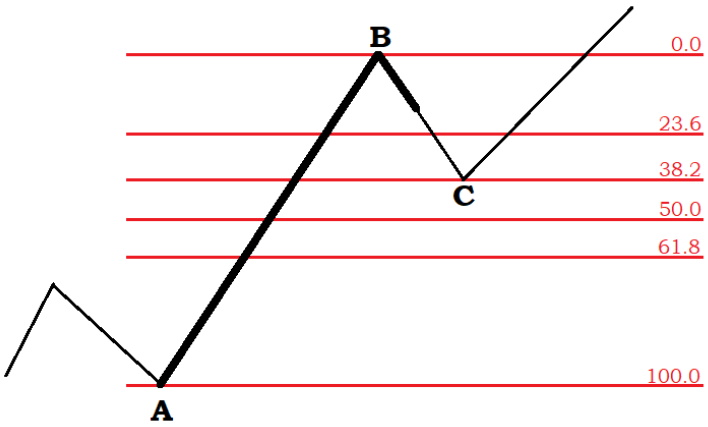


Rysunek 7. Proporcje ciała człowieka
Źródło: własne

3.4. Złota liczba w finansach

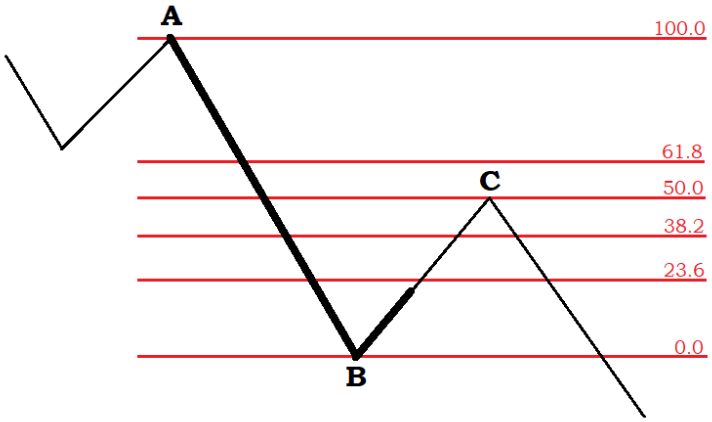
Finanse, to kolejny obszar, gdzie liczba φ, złota liczba, znajduje zastosowanie.

— Poziomy Fibonacciego – służą do wyznaczenia zniesień czyli miejsc, gdzie występuje koniec impulsów i początek korekty lub zachodzi sytuacja odwrotna. Impulsem nazywamy ruch zgodny z obecnym trendem, a korektą, ruch przeciwny do trendu. Pozwala to przewidzieć zachowania rynku przy zmniejszonym ryzyku i zwiększonym zysku. Poziomy Fibonacciego mają zastosowanie między innymi w analizie cen akcji na giełdzie. W celu wyznaczenia poziomów Fibonacciego korzystamy z potęg złotej liczby: $\varphi^{-3} = 23,6\%$, $\varphi^{-2} = 38,2\%$, $\varphi^{-1} = 61,8\%$. Dodatkowo uwzględnia się poziom 50%, ponieważ reprezentuje on środek przedziału cenowego.



Rysunek 8. Przykład zniesienia w trendzie wzrostowym
Źródło: własne

Na rysunku 8 widoczna jest fala wzrostowa AB, po której następuję korekta. Zatrzymała się ona na poziomie 38,2% zniesienia poprzedniego impulsu. W punkcie C nastąpił powrót do wzrostowego trendu.



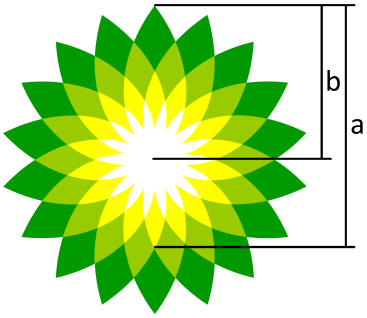
Rysunek 9. Przykład zniesienia w trendzie spadkowym
Źródło: własne

Na rysunku 9 przedstawiona jest fala spadkowa AB. Korekta zakończyła się w punkcie C na poziomie 50% zniesienia impulsu AB. W tym miejscu nastąpił powrót fali do trendu pierwotnego.

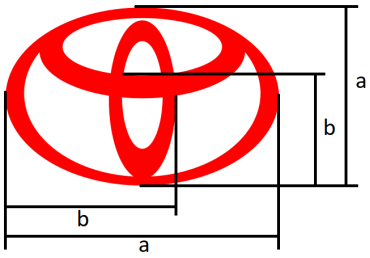
3.5. Złota liczba a rozrywka i marketing

Złota proporcja i przypisywane jej już od starożytności wyjątkowe walory estetyczne są powodem, dla którego wydawcy książek i specjaliści od marketingu stosują jej zasady.

— Wymiary książek – dawniej zachowanie tej proporcji było tak ważne, że wydawcy zachowywali ją z dokładnością do 0,5 mm.
— Loga znanych marek – złotą proporcję zachowują znaki takich przedsiębiorstw jak: National Geographic, Google, Apple, Pepsi, BP (rysunek 10), Toyota (rysunek 11).
— Karty do gry, plakaty, zdjęcia to też przykłady stosowania złotego podziału.



Rysunek 10. Logo BP
Źródło: opracowanie własne na podstawie [13]



Rysunek 11. Logo Toyoty
Źródło: opracowanie własne na podstawie [14]

4. Podsumowanie

Jak możemy zauważyć, złoty podział jest związany z wieloma aspektami naszego życia. Szczególną uwagę powinniśmy zwrócić na jego związek z ciągiem Fibonacciego, który ma wiele praktycznych zastosowań. Doszukiwanie się takich zależności w praktyce nie zawsze wydaje się być racjonalne, ale mimo wszystko często można odnaleźć reguły, które odzwierciedlają cechy złotej liczby. Ze złotej proporcji podświadomie korzystano zanim odkryto jej własność np. w architekturze, natomiast dalsze badania umożliwiły rozszerzenie tego pojęcia na inne dyscypliny, dzięki czemu w wielu pracach dąży się do ładu, estetyki i harmonii.

Literatura

[1] R. L. Graham, D. E. Knuth, O. Patashnik, *Matematyka konkretna*, Wydawnictwo Naukowe PWN, Warszawa, 2001
[2] R. Knott, *The Golden section ratio: Phi*, www.maths.surrey.ac.uk(sprawdzono: 16.06.2020)
[3] K. Nowicka K, *W poszukiwaniu złota, czyli coś o złotej liczbie*, Pismo PG, maj 2011, nr 5 (164)/11 rok XIX, s. 44
[4] A.S. Posamentier, I. Lehmann, *The Fabulous Fibonacci Numbers*, New York, Prometheus Book 2007
[5] M, Rachelski, *Liczby Fibonacciego*, www.smurf.mimuw.edu.pl (sprawdzono: 15.06.2020)
[6] K. A. Ross, C. R. B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa, 1996
[7] W. Sierpiński, *Arytmetyka teoretyczna*, PWN, Warszawa 1966
[8] https://pl.tradingview.com/ideas/fibonacci/ (sprawdzono: 25.06.2020)

[9] https://analizy.investio.pl/impulsy-i-korekty/(sprawdzono: 08.07.2020)
[10] https://pl.wikipedia.org/wiki/Partenon (sprawdzono: 08.07.2020)
[11] https://www.budowle.pl/budowla/katedra-notre-dame (sprawdzono: 08.07.2020)
[12] https://analizy.investio.pl/seria-analiza-techniczna-techniki-fibonacciego-zniesienia\
\-wewnetrzne (sprawdzono: 03.09.2020)
[13] https://en.wikipedia.org/wiki/BP (sprawdzono: 22.01.2021)
[14] https://pl.wikipedia.org/wiki/Toyota (sprawdzono: 22.01.2021)

Emilia Popławska [1], **Monika Sowa** [2]

Niezwykłe zero i jeden

Streszczenie

Liczby towarzyszą ludzkości od dawna, lecz moment ich pierwszego użycia nie jest konkretnie określony. W pracy zaprezentowano okoliczności powstania i pierwszych użyć liczb *zero* oraz *jeden*. Ponadto, przedstawiono podstawowe własności tych liczb, pokazano je na przykładach i w zastosowaniach matematycznych.

Słowa kluczowe: zero, jeden, liczby

Wstęp

Liczby, zarówno kiedyś jak i dziś, odgrywają znaczącą rolę w świecie. Kiedyś, nawet poszczególne liczby, były utożsamiane z konkretnymi bóstwami. [1] Jednocześnie, niektóre z nich były nawet imionami tychże bogów. Magowie babilońscy każdemu z bogów panteonu przypisywali numer. Tworzyli w ten sposób hierarchię wyrażającą wyższość. Dla przykładu, liczba 60 była przypisana bogu nieba, 50 było nadane Enlilowi – bogu ziemi, 40 – bogu wód Ea. Teraz liczby są w powszechnym użyciu, są miarami zbiorów, (np. 3 długopisy), są wykorzystywane do porównywania wielkości. Liczby naturalne są używane także jako identyfikatory, np. numery telefonów, dróg, rachunków bankowych, PESEL, ISBN itp. Wraz z rozwojem matematyki dokonano rozszerzenia liczb na abstrakcyjne, takie jak liczby zespolone, p-adyczne, kwaterniony, czy sedeniony. Liczby zespolone znalazły zastosowanie w wielu dziedzinach nauki m.in. w grafice komputerowej, analizie obwodów elektrycznych prądu przemiennego, teorii płynów, fizyce kwantowej, czy teorii względności. Kwaterniony znalazły zastosowanie w grafice trójwymiarowej, zaś liczby p-adyczne w kryptografii.

O liczbach można powiedzieć wiele. My jednak skupimy się na najbardziej podstawowych, ale jakże niezwykłych: *zero* oraz *jeden*.

1. O umiejętności liczenia

Mogłoby się wydawać, że w dzisiejszych czasach każdy potrafi liczyć, lecz nic bardziej mylnego. [1] Zulusi i Pigmeje w Afryce, szczepy Aranda i Kamilarai

[1] Emilia Popławska, Monika Sowa, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

[2] Monika Sowa, Studenckie Koło Naukowe „KWATERNION", Wydział Podstaw Techniki, Politechnika Lubelska

w Australi, krajowcy z wysp Murraya i Botokudzi w Brazylii są przykładami plemion, u których umiejętność liczenia nie jest rozwinięta. Używają tylko dwóch liczb: *jeden* i *dwa*. Mają trudności z wyobrażeniem sobie liczby większej, np. *sześć*. Nasuwa się więc pytanie, w jaki sposób radzą sobie w sytuacji, gdy muszą określić ilość przedmiotów, których jest więcej niż *jeden* czy *dwa*. W takich przypadkach używają słowa: *dużo*.

Nasi dalecy przodkowie, podobnie jak dzisiejsi Pigmeje z Afryki, byli na zerowym poziomie liczenia. Widzieli różnicę tylko między jednością, parą i wielością.

Takie rozróżnienie można odnaleźć w językach i pismach. Na przykład w starożytnej grece `ho lykos` znaczyło „wilk”, `to lyko` „dwa wilki”, a `hoj lykoj` „wilki”. W napisach obrazkowych w Egipcie, aby zaznaczyć, że chodzi o trzy lub wiele rzeczy, powtarza się trzy razy ten sam hieroglif albo dodaje się trzy pionowe kreski do piktogramu. W jednej z początkowych faz nauki liczenia dziecka również można zauważyć takie rozróżnienie. Dziecko uczy się odróżniać jeden, dwa lub kilka przedmiotów.

W języku sumeryjskim, jedynce odpowiadało słowo `gesh` oznaczające mężczyznę, dwójce słowo `min`, które znaczyło kobieta. Trójka w tym języku określona była słowem `esh` oznaczającym „wiele”. W innych językach możemy również napotkać podobne przykłady. Przykładowo, w języku łacińskim „trójka” określana jest słowem `tres`, które jest spokrewnione z wyrazem `ter` oznaczającym „wiele”.

2. Jedynka

Jednymi z pierwszych liczb są, bez wątpienia, *jeden* oraz *dwa*, którym możemy przypisać pewne znaczenia. *Jeden* oznacza człowieka aktywnie uczestniczącego w dziele tworzenia, jednostkę w społeczeństwie, samotną w obliczu śmierci. *Jeden* można również łączyć z symbolem oznaczającym istotę żywą pionowo stojącą. *Dwa* symbolizuje dwoistość płci, podział, opozycję, rywalizację, konflikt, antagonizm, np. życie i śmierć, dobro i zło itd.

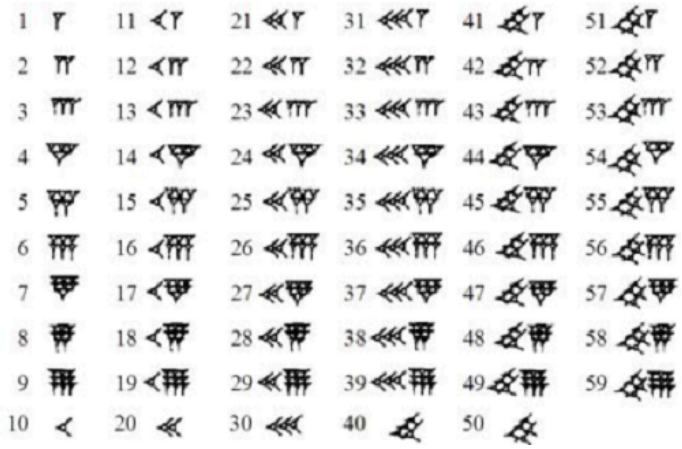
Sumerowie, w IV tys. p.n.e., używali małego glinianego stożka (Rys. 1), oznaczającego *jeden*. *Dwójkę* reprezentowały dwa stożki. Aby wyrazić „dziesiątkę” wykorzystywali glinianą kulę, która reprezentowała 10 sztuk jakiegoś towaru. W przypadku nieco większych liczb, np. 60, nie używano 6 glinianych kul, ale dużego glinianego stożka. W ten sposób materialnie zaczęto wyrażać kolejne liczby naturalne.

W III tys. p.n.e. system ten przekształcił się w system znaków i symboli przypominający dobrze nam znany system rzymski (Rys. 2).

Elementem podstawowym w wspomnianych systemach jest *jeden*.

Starożytni Grecy *jedynkę* uważali za *praliczbę*. Oznaczało to, że służyła ona do

Rysunek 1. Sumeryjskie gliniane stożki reprezentujące *jeden*
Źródło: [3]

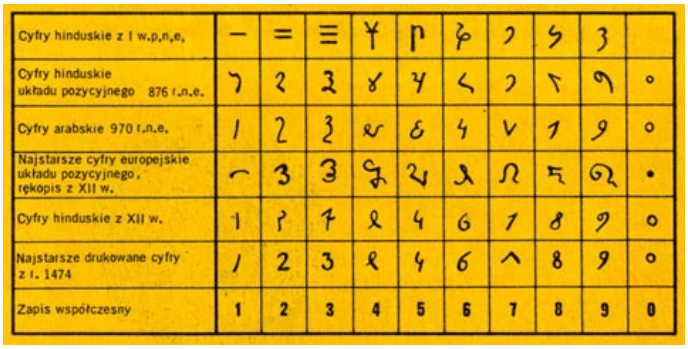


Rysunek 2. Zapis sumeryjskich liczb od 1 do 59
Źródło: [4]

tworzenia prawdziwych liczb. Za pierwszą liczbę uważali dopiero *dwójkę*. *Jedynka* była zaś generatorem liczb.

Jedynka używana jest do zapisu liczb we wszystkich systemach pozycyjnych. W szczególności dotyczy to takich jak: binarny, ósemkowy, dziesiętny, szesnastkowy.

Kształt zapisu *jedynki* zmieniał się na przestrzeni wieków. Obrazuje to tabelka przedstawiona na Rys. 3.



Rysunek 3. Zapis cyfr indyjsko-arabskich
Źródło: [5]

Hinduska *jedynka* z I wieku p.n.e. była poziomą kreską. Taki zapis nadal jest stosowany w Chinach. Współczesny zapis *jedynki* jest połączeniem rzymskiego zapisu I ze znakiem hinduskim.

2.1. Jedynka w matematyce

W algebrze, w dowolnym pierścieniu element neutralny mnożenia nazywany jest *jedynką* i często oznaczany jest symbolem 1.

Jedynka odgrywa ważną rolę w podstawowych matematycznych działaniach. [2] Dla dowolnego $a \in \mathbb{R}$ mamy następujące własności *jedynki* w podstawowych działaniach arytmetycznych.

Mnożenie i dzielenie

$$a \cdot 1 = \frac{a}{1} = a, \quad \text{gdy} \quad a \in \mathbb{R}, \quad \text{oraz} \quad \frac{a}{a} = 1, \quad \text{gdy } a \in \mathbb{R}, \quad a \neq 0.$$

Jeden jest elementem neutralnym mnożenia. Podzielenie dowolnej liczby a przez *jeden* daje tę samą liczbę. *Jedynkę* można też otrzymać poprzez podzielenie dowolnej liczby przez tę samą liczbę.

Potęgowanie

$$a^1 = a, \quad 1^a = 1, \quad \text{gdy} \quad a \in \mathbb{R}, \quad \text{oraz} \quad a^0 = 1, \quad \text{gdy} \quad a \in \mathbb{R}, \quad a \neq 0.$$

Dowolna liczba podniesiona do potęgi pierwszej daje tę samą liczbę. *Jedynka* jest wynikiem potęgowania *jedynki* o dowolnym wykładniku oraz potęgowania o zerowym wykładniku.

Logarytmowanie

$$\log_a 1 = 0 \quad \text{oraz} \quad \log_a a = 1, \quad \text{gdy} \quad a \in (0,\infty), \quad a \neq 1.$$

Funkcje trygonometryczne

Dla funkcji trygonometrycznych sinus i cosinus, maksymalną wartością jest *jeden*.

Tożsamość zwana „jedynką trygonometryczną”:

$$\sin^2 x + \cos^2 x = 1$$

spełniona jest dla każdego rzeczywistego x.

Dla funkcji tangens i cotangens mamy:

$$\operatorname{tg} x \cdot \operatorname{ctg} x = 1, \quad \text{dla} \quad x \in \mathbb{R} \setminus \left\{ \frac{\pi}{2} + \frac{k\pi}{2} : k \in \mathbb{Z} \right\}.$$

Pochodna

Pierwsza pochodna funkcji $f(x) = x$, dla $x \in \mathbb{R}$ jest równa *jeden*:

$$f(x) = x \implies f'(x) = 1, \quad \text{dla} \quad x \in \mathbb{R}.$$

Rachunek prawdopodobieństwa

Niech f będzie dowolną funkcją gęstości prawdopodobieństwa, a F jej dystrybuantą. Wtedy:

$$\int_{-\infty}^{\infty} f(x)dx = 1,$$

$$\lim_{x \to +\infty} F(x) = 1.$$

Jedynka ma tylko jeden dzielnik naturalny (samą siebie). Nie jest ona liczbą ani pierwszą ani złożoną. Wynika to z definicji liczby pierwszej mówiącej, że liczba pierwsza ma dokładnie dwa dzielniki, (jeden i siebie samą). W przypadku *jedynki* nie są to różne liczby.

3. Zero

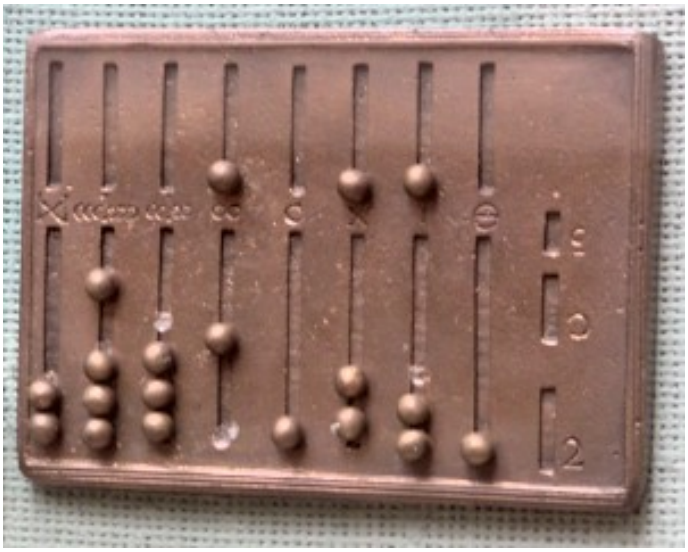
Kolejna z liczb, to *zero*. W dzisiejszym rozumieniu *zero*, symbolizujące bezwartościowość oraz nicość, pojawiło się zaskakująco późno. Praktyczna potrzeba dokonywania obliczeń zmobilizowała do powstania symbolu *zera*, a więc *zera* jako cyfry a nie jako liczby.

W dziele Ashtadhyayi, czyli w formalnej gramatyce sanskrytu z V wieku p.n.e. autorstwa hinduskiego gramatyka Panini, można odnaleźć użycie *zera*.

Prawdopodobnie pierwszy raz, system pozycyjny, do zapisu liczb, wykorzystali mieszkańcy Sumeru i Elamu ok. roku 3200 p.n.e. Podstawę zapisu stanowiła liczba 60 (kopa). Początkowo, sumeryjska cywilizacja brak wartości w jednym z rzędów oznaczała pustym miejscem.

W starożytnym Babilonie, w wieku III przed naszą erą, użyto po raz pierwszy *zera*. W babilońskim systemie *zero* służyło, mniej więcej, do odróżnienia liczb dziesiętnych, takich jak: dziesięć, sto, tysiąc itd. i oznaczano je jako dwa małe trójkąciki.

Rzymianie nie znali *zera*. Dowodem na to jest brak symbolu i pozostawienie pustej przestrzeni symbolizującej *zero* w rzymskim sposobie zapisu liczb. Do obliczeń zaczęli wykorzystywać specjalny przyrząd zwany „abakusem", którego zasada działania przypominała dzisiejsze liczydło.



Rysunek 4. Rekonstrukcja rzymskiego abakusa z brązu
Źródło: [6]

Grecy natomiast do liczenia używali zwykłych stołów z odpowiednimi krążkami, w których wpisywali cyfry. Chcąc zapisać *zero* wstawiano pusty krążek bez żadnego uzupełnienia. Pod koniec średniowiecza zaczęto wykonywać działania na tanim papierze, dostępnym już w tamtych czasach. Rysowano na nim zwykłe kółko, które przypominało krążek bez cyfry, aby symbolizowało miejsce *zera*.

W Mezopotamii przed około 300 rokiem p.n.e. ustalono *zero* jako jeden z symboli interpunkcyjnych. Jednakże, nie był on traktowany jako liczba, lecz jako cyfra *zero*. Zapisywany był podwójnym ukośnym znakiem klinowym.

Na kontynencie amerykańskim, a dokładnie przez cywilizację Majów, *zero* zostało wykorzystane w kalendarzu, co jest ewenementem w stosunku do większości kalendarzy, gdzie *zero* zostało pominięte. Mianowicie, rok przed pierwszym rokiem naszej ery nazywany jest pierwszym rokiem przed naszą erą.

Symbol *zero* był utożsamiany z pustym miejscem. Pozostawione puste miejsce, czyli brak cyfry w zapisie liczby służyło za pewną formę interpunkcji, która niestety nie zapewniała właściwego odczytu liczby. Przykładem może być liczba 40057, która zapisana z użyciem wielkiej spacji przyjmowała postać (4 57). Taki zapis mógł być błędnie odczytywany jako 4057 lub 457.

W 130 r. naszej ery, Ptolemeusz na podstawie babilońskiego sześćdziesiątkowego systemu liczbowego opartego na alfabecie greckim używał znacznika „braku" w formie „O".

Matematycy indyjscy, żeby zaznaczyć „brak", wykorzystywali małe kropeczki pod numerami. Brahmagupta chciał ustalić zasady dla działań arytmetycznych zawierających *zero*. Przedstawił je następująco:

— „suma liczby ujemnej i *zero* jest ujemna",
— „suma liczby dodatniej i *zero* jest dodatnia",
— „suma *zero* i *zero* wynosi *zero* ",
— „liczba ujemna odjęta od *zero* jest dodatnia",
— „dodatnia liczba odjęta od *zero* jest ujemna",
— „ *zero* odjęte od liczby ujemnej jest ujemne",
— „ *zero* odjęte od liczby dodatniej jest dodatnie",
— „ *zero* odjęte od *zera* to *zero* ".

Idąc w ślady Brahmagupty po 200 latach, czyli w około 830 roku, Mahavira napisał swoje dzieło pt. "Ganita Sara Samgraha", gdzie rozszerzył myśl Brahmagupty dodając nową zasadę.

„Liczba pomnożona przez *zero* wynosi *zero*. Liczba pozostaje bez zmian, kiedy *zero* zostaje od niej odjęte."

W Europie *zero* pojawiło się w XI wieku za sprawą papieża-uczonego Sylwestra II, który starał się je popularyzować. Natomiast w około 1202 roku we Włoszech Leonardo z Pizy, zwany Fibonaccim, wydał dzieło arytmetyki „Liber Abaci". W tym podręczniku opisał nie tylko *zero*, które nazywał zephirum, ale również dziewięć hinduskich symboli matematycznych. Fibonacci wyróżnił *zero* spośród wszystkich cyfr, nazywając *zero* zerem, a pozostałe symbole (1,2,3,4,5,6,7,8,9) liczbami. Obecna nazwa tej wyjątkowej, a zarazem „pustej", liczby stała się rozpowszechniona i stosowana dopiero od 1491 roku.

3.1. Zero w matematyce

Zero symbolizuje początek w odniesieniu do szeregu liczb występujących w większości działów matematyki.

Cyfra *zero* jest wykorzystywana w arytmetyce przy zapisie liczb w systemach pozycyjnych.

W algebrze w dowolnym pierścieniu element neutralny dodawania jest nazywany *zerem* i jest oznaczany zwykle symbolem 0:

$$a+0=a.$$

Niektóre definicje liczb naturalnych nie obejmują liczby *zero*, zazwyczaj wtedy kiedy nie są związane z logiką i teorią mnogości. W przypadku kiedy jednak zawierają symbol 0, oznacza ono najmniejszą liczbę naturalną.

Termin „zero funkcji" używany jest czasem w potocznym żargonie matematycznym jako synonim miejsca zerowego funkcji.

Dodawanie, czy odjęcie od liczby dodatniej lub ujemnej (zapisanej jako a) liczby 0 daje nam tę samą liczbę:

$$a+0=a;$$

$$a-0=a.$$

Pomnożenie dowolnej liczby a przez 0 daje w wyniku *zero*:

$$a\cdot 0=0.$$

W dzieleniu, dzielenie przez *zero* jest nieokreślone, ponieważ w definicji dzielenia wymagane jest, aby dzielnik był różny od *zera*.

Definicja potęgowania mówi, że liczba rzeczywista różna od *zera* podniesiona do potęgi *zero* daje jeden:

$$a^0=1.$$

Logarytm przy dowolnej podstawie dodatniej i różnej od 1 z *jedynki* jest równy *zero*:

$$\log_a 1=0, \quad a>0, \quad a\neq 1.$$

Dla dowolnej stałej $a\in\mathbb{R}$, pochodna funkcji stałej, danej wzorem $f(x)=a$, dla $x\in\mathbb{R}$, jest równa 0 :

$$\frac{d}{dx}(a)=0, \text{ dla } x\in\mathbb{R}.$$

Podsumowanie

W pracy przedstawiono wybrane, ciekawe fakty dotyczące rozwoju pojęcia liczby, a w szczególności niezwykłych, jak się okazało liczb: *zero* oraz *jeden*. Podstawowe ich własności zaprezentowano w pracy. Mimo, że niektóre własności, czy też sama postać tych liczb, były odkryte wiele wieków temu, to ich historia odkrywania jest wciąż mało znana i niekiedy zaskakuje.

Literatura

[1] C. Ifrah, *Dzieje liczby czyli historia wielkiego wynalazku*, Wydawnictwo Ossolineum, 1990
[2] *1(liczba)*, https://pl.wikipedia.org/wiki/1_(liczba), (dostęp: 10.07.2020)
[3] *Matematyka Sumeru i Babilonu*, https://www.swiatmatematyki.pl/index.php?p=865, (dostęp: 06.07.2020)
[4] *Matematyka*, https://www.starozytnysumer.pl/podstrony/nauka/matematyka.html, (dostęp: 06.07.2020)
[5] *Cyfrowa historia*, https://swiatmatematyki.pl/index.php?p=44, (dostęp: 06.07.2020)
[6] *Abakus (liczydło)*, https://pl.wikipedia.org/wiki/Abakus_(liczyd%C5%82o), (dostęp: 06.07.2020)

ISBN: 978-83-7947-457-8