Matematyka

15h dla studiów doktoranckich na kierunku Informatyka

Marcin Korzeń

Zachodniopomorski Uniwersytet Technologiczny, Wydział Informatyki, Katedra Metod Sztucznej Inteligencji i Matematyki Stosowanej

`mkorzen@wi.ps.pl`

1 Wstęp do matematyki współczesnej

Zbiory, relacje - własności, relacje równoważności, relacje porządkujące, liczby naturalne, zasada indukcji matematycznej, zasada minimum. Równoliczność, liczby kardynalne, twierdzenie Cantora, $\aleph$, $\mathfrak{c}$, twierdzenie Cantora-Bernsteina. [5], [3], [7].

Zadania

1. Udowodnić, że dla dowolnych zbiorów A, B, C zachodzą $\boxed{\text{0 pkt.}}$:
   (a) $A \cup (A \cap B) = A \cap (A \cup B) = A$
   (b) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$
   (c) $(A \setminus (B \cup C) = (A \setminus B) \setminus C)$
2. Znaleźć sumę $\bigcup_{i=1}^{\infty} A_i$ i iloczyn $\bigcap_{i=1}^{\infty} A_i$, dla następujących rodzin zbiorów $\boxed{\text{0 pkt.}}$:
   (a) $A_i = \{x \in \mathbb{R}\colon -\frac{1}{i} < x < \frac{1}{i}\}$
   (b) $A_i = \{x \in \mathbb{R}\colon -1 + \frac{1}{i} < x < 1 - \frac{1}{i}\}$
   (c) $A_i = \{x \in \mathbb{R}\colon 0 < x < \frac{1}{i}\}$
3. Udowodnić następujące prawa de Morgan'a $\boxed{\text{2 pkt.}}$:
   (a) $X - \bigcup_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty}(X - A_i)$
   (b) $X - \bigcap_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty}(X - A_i)$
4. Udowodnić wykorzystując *zasadę indukcji matematycznej*:
   (a) $n < 2^n$ $\boxed{\text{0 pkt.}}$,
   (b) $(1 + a)^n \geq 1 + na$, dla $a > -1$ $\boxed{\text{3 pkt.}}$
   (c) liczba wszystkich podzbiorów zbioru n-elementowego wynosi 2^n $\boxed{\text{1 pkt.}}$,
   (d) $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ $\boxed{\text{3 pkt.}}$
5. Napisać w ulubionym języku programowania funkcje wypisujące wszystkie $\boxed{\text{6 pkt.}}$:

(a) permutacje zbioru n–elementowego,
(b) k–elementowe podzbiory, zbioru n–elementowego,
(c) różnowartościowe funkcje ze zbioru $\{1, \ldots m\}$ do zbioru $\{1, \ldots, n\}$,
(d) funkcje ze zbioru $\{1, \ldots, m\}$ do zbioru $\{1, \ldots, n\}$.

6. Udowodnić, że:

   (a) zbiór wielomianów o współczynnikach naturalnych jest przeliczalny $\boxed{\text{1 pkt.}}$,
   (b) zbiór liczb niewymiernych ma moc $\mathfrak{c}$, $\boxed{\text{4 pkt.}}$
   (c) zbiór liczb algebraicznych (to takie, które są pierwiastkami wielomianów o współczynnikach wymiernych) jest przeliczalny, $\boxed{\text{3 pkt.}}$
   (d) zbiór liczb całkowitych ma moc $\aleph$. $\boxed{\text{1 pkt.}}$

7. Udowodnić, że zbiory $A = [0, 1)$ oraz $B = [0, 1]$ są równoliczne, $\boxed{\text{1 pkt.}}$

8. Bezpośrednio wskazać bijekcję pomiędzy zbiorami A i B $\boxed{\text{7 pkt.}}$.

9. Wskazać moc odpowiednich zbiorów:

   (a) zbiór liczb parzystych $\boxed{\text{0 pkt.}}$,
   (b) zbiór liczb pierwszych $\boxed{\text{2 pkt.}}$,
   (c) zbiór wszystkich funkcji rzeczywistych ($f : \mathbb{R} \to \mathbb{R}$) $\boxed{\text{2 pkt.}}$,
   (d) zbiór wszystkich ciągów binarnych ($f : \mathbb{N} \to \{0, 1\}$) $\boxed{\text{2 pkt.}}$,
   (e) zbiór wszystkich funkcji rzeczywistych ciągłych $\boxed{\text{8 pkt.}}$,
   (f) zbiór Cantora $\boxed{\text{4 pkt.}}$ (jaka jest miara tego zbioru? $\boxed{\text{1 pkt.}}$).

10. Udowodnić, że relacja przeciwzwrotna i przechodnia jest przeciwsymetryczna $\boxed{\text{4 pkt.}}$

11. Sprawdzić, że następujące relacje są relacjami równoważności, wskazać (nazwać) klasy abstrakcji:

    (a) $a \equiv b \mod 2$ (lub $a \equiv_2 b$) $\Leftrightarrow 2|b - a$, $a, b \in \mathbb{Z}$, $\boxed{\text{2 pkt.}}$
    (b) w danym grafie nieskierowanym $G = (E, V)$ relacja określona następująco: $a \varrho b \in V \times V \Leftrightarrow$ istnieje ścieżka z b do a, $\boxed{\text{2 pkt.}}$
    (c) relacja $\approx$ określona na parach liczb naturalnych:

    $$(m_1, n_1) \approx (m_2, n_2) \Leftrightarrow m_1 + n_2 = m_2 + n_1.$$

    Zinterpretować klasy abstrakcji tej relacji jako liczby całkowite, jak wyglądają liczby -1,0,1 $\boxed{\text{2 pkt.}}$. Określić działania $+$ i $\cdot$ na takich parach zgodne z arytmetyką liczb całkowitych. $\boxed{\text{2 pkt.}}$

12. Sprawdzić, że następujące relacje są relacjami porządku, wskazać elementy maksymalne i minimalne o ile istnieją, który z porządków jest liniowy, w każdym ze zbiorów podać przykład łańcucha:

    (a) relacja podzielności $| \subset \mathbb{N}^2$ określona następująco:

    $$a|b \Leftrightarrow \exists_{k \in \mathbb{N}} : b = k \cdot a, \quad \boxed{\text{2 pkt.}}$$

    (b) relacja zawierania zbiorów ($a \subset b$), określona na podzbiorach ustalonego zbioru, $a, b \subset X$ $\boxed{\text{2 pkt.}}$. Znaleźć następujące zbiory: $A = \{x \in \mathbb{N} : x|0\}$ oraz $B = \{x \in \mathbb{N} : 0|x\}$. $\boxed{\text{1 pkt.}}$

2 Ułamki łańcuchowe, aproksymacja oraz zastosowania do arytmetyki komputerowej

Elementy elementarnej teorii liczb: kongruencje, małe twierdzenie Fermat'a, chińskie twierdzenie o resztach. Twierdzenia o przybliżaniu liczb niewymiernych: tw. Dirichlet'a, tw. Liouville'a. Ułamki łańcuchowe, istnienie i jednoznaczność rozwinięcia w przypadku liczb rzeczywistych, znaczenie w aproksymacji, zastosowanie w arytmetyce komputerowej oraz faktoryzacji. Ciągi Farey'a, drzewo Sterna-Brocota. [4], [2], [6], [7].

Zadania

$\mathbb{INT}32$ oznacza podzbiór zbioru liczb całkowitych z przedziału $[0, 2^{32} - 1]$ z działaniami $+$ i $\cdot$ branymi modulo 2^{32}, zbiór ten jest pierścieniem standardowo oznaczanym $(\mathbb{Z}_{4294967296}, +, \cdot)$. Analogicznie definiuje się zbiór $\mathbb{INT}64$

$\mathbb{DOUBLE}$ oznacza podzbiór zbioru liczb wymiernych, które mogą reprezentowane w systemie zmiennopozycyjnym przy użyciu 64 lub 80 bitów, szczegóły można znaleźć w normie IEEE 754.

Zbiory te można i należy utożsamiać z odpowiednimi typami `int`, `long` i `double`, w szczególności wyniki działań dla konkretnych argumentów można uzyskać wykonując odpowiednie obliczenia na komputerze.

1. Znaleźć w zbiorze liczbę $x \in \mathbb{INT}32$ taką, że $1535 \cdot x \equiv 1$, powtórzyć to samo rozwiązanie dla zbioru $\mathbb{INT}64$. $\boxed{\text{1 pkt.}}$
2. Napisać w dowolnym języku programowania posiadającym typ `BigInteger` (liczby całkowite dowolnej długości)[1] następujące funkcję:
   (a) funkcję znajdującą największy wspólny dzielnik dwóch liczb typu `BigInteger`, $\boxed{\text{3 pkt.}}$
   (b) funkcję rozstrzygającą istnienie rozwiązań równania $ax + by = d$, dla dowolnych liczb a, b, d typu `BigInteger`, w przypadku gdy rozwiązania istnieją należy podać jedno przykładowe, $\boxed{\text{4 pkt.}}$
   (c) funkcję znajdującą odwrotność dla liczb typu `long`. $\boxed{\text{5 pkt.}}$
   (d) funkcją rozwijającą liczbę wymierną $\frac{a}{b}$ w ułamek łańcuchowy do wyboru dla a, b należących do typu `BigInteger` lub `long`. $\boxed{\text{5 pkt.}}$
3. Znaleźć znaleźć minimalna liczbę φ o tej własności że dla dowolnego odwracalnego $x \in \mathbb{INT}32$ ($\mathbb{INT}32$) dostaniemy $x^{\varphi} = 1$. $\boxed{\text{3 pkt.}}$
4. Znaleźć znaleźć rząd grupy elementów odwracalnych pierścienia $\mathbb{INT}32$ ($\mathbb{INT}32$). $\boxed{\text{1 pkt.}}$

[1] Przykładowo w języku Java mamy klasę `java.math.BigInteger`, dla tej klasy zdefiniowane są odpowiednie metody, można zajrzeć do źródeł dostępnych pod adresem `www.java.sun.com`, jednak rozwiązanie ma być własne bazujące na algorytmie Euklidesa.

5. Zaproponować w względnie szybki algorytm znajdowania odwrotności w zbiorze $\mathbb{INT}32$ lub $\mathbb{INT}64$ opierając się na powyższej własności. $\boxed{\text{5 pkt.}}$ Porównać szybkość działania z algorytmem bazującym na uogólnionym algorytmie Euklidesa. $\boxed{\text{2 pkt.}}$

6. Wskazać, które z aksjomatów ciała nie są spełnione dla liczb typu $\mathbb{INT}32$. $\boxed{\text{1 pkt.}}$

7. Wskazać, które z aksjomatów ciała nie są spełnione dla liczb typu $\mathbb{DOUBLE}$. $\boxed{\text{3 pkt.}}$

8. Obliczyć wartość wyrażenia: $(517647495.0/10843312.0, 2)^2 - 2279.0$, czy wszystko jest w porządku ? $\boxed{\text{2 pkt.}}$

9. Udowodnić, że zbiory że zbiory liczb wymiernych i niewymiernych: (1) są gęste oraz (2) są gęste w sobie. $\boxed{\text{5 pkt.}}$ (Wskazówka: wskazówka była podana na wykładzie)

10. Rozwinąć w ułamek łańcuchowy liczbę $\frac{31}{13}$. $\boxed{\text{0 pkt.}}$

11. Rozwinąć w ułamek łańcuchowy liczbę $\sqrt{29}$. $\boxed{\text{2 pkt.}}$

12. Co to za liczba $[3; 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \ldots]$ (wskazówka tw. Lagrange'a, proszę tylko o rozwiązania konstruktywne, a nie zgadywanie). $\boxed{\text{2 pkt.}}$

13. W twierdzeniu Dirichlet'a jest założenie, że x jest liczbą niewymierną. Prześledzić kroki dowodu i znaleźć miejsce gdzie istotnie korzysta się tego założenia $\boxed{\text{2 pkt.}}$. Rozstrzygnąć czy teza twierdzenia zachodzi dla liczb wymiernych. $\boxed{\text{5 pkt.}}$

14. Znaleźć 10, 100, 1000 cyfr rozwinięcia dziesiętnego liczby e wykorzystujące zależność $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots]$. $\boxed{\text{4 pkt.}}$

15. Obliczyć wartość wyrażenia $x = 1 + \frac{1}{x}$ wykonując rekurencję 10 razy porównać wynik z dziesiątym reduktem liczby φ. $\boxed{\text{4 pkt.}}$

16. Który redukt ułamka łańcuchowego (tzn. jakie n?) dla liczby φ należy wziąć pod uwagę, aby mieć pewność, że dostaniemy dokładność rozwinięcia dziesiętnego do 1000000 cyfr. $\boxed{\text{7 pkt.}}$ (uwaga: oczywiście milionowy redukt pewnie będzie dobry, ale chodzi o znalezienie znacznie lepszego (mniejszego) oszacowania liczby n, wskazówka: rozważyć rekurencję $a_k = a_{k-1} + a_{k-2}$)

17. Niech $x_0, x_1, x_2, \ldots$ bedzie ciągiem liczb rzeczywistych takich, że $x_i > \epsilon$, $\epsilon > 0$. Udowodnić że $\lim_{n\to\infty}[x_0; x_1, x_2, \ldots, x_n]$ istnieje. $\boxed{\text{7 pkt.}}$ (wskazówka 1: przeanalizować odpowiedni dowód z wykładów, wskazówka 2: D. Knuth, Sztuka programowania, tom 2 §4.5.2 zad. 5.)

18. Zadanie dla osób nie bojących się wykonywać obliczeń z użyciem komputera $\boxed{\text{10 pkt.}}$:

    (a) Napisać program, który dla danej liczby postaci $\sqrt{a}$ znajdzie okres rozwinięcia na ułamek łańcuchowy (tw. Lagrange'a gwarantuje istnienie takiego okresu).

    (b) Wykorzystać ten algorytm do znalezienia rozwinięcia liczby $\sqrt{a} = \sqrt{4729494}$ na ułamek łańcuchowy.

(c) Wykorzystać powyższe rozwinięcie do znalezienia całkowito-liczbowego rozwiązania równania $X^2 - aY^2 = 1$. (Rozwiązanie to podobno znane było Archimedesowi III w. p.n.e).

(d) Wypisać 5 przykładowych rozwiązań powyższego równania.

19. Napisać algorytm do faktoryzacji liczb całkowitych wykorzystujący ułamki łańcuchowe program powinien pracować na liczbach typu `BigInteger`, poeksperymentować z różną długością liczby wejściowej, (por. D. Knuth, Sztuka programowania, tom 2. §4.5.4 str. 435). $\boxed{\text{10 pkt.}}$. Oszacować eksperymentalnie czas działania (wyznaczać α lub β) przyjmując, że jest on typu N^α, lub $log(N)^\beta$. $\boxed{\text{5 pkt.}}$

20. Udowodnić, że dla każdego n oraz $0 \geq k \geq n$, $\binom{n}{k}$ jest liczba całkowitą. $\boxed{\text{0 pkt.}}$

21. Udowodnić, że jeżeli p jest liczba pierwszą $p|\binom{p}{k}$, to znaczy $\binom{p}{k}/p$ jest liczbą całkowitą, wnioskować na tej podstawie, że zachodzi małe twierdzenie Fermata: $a^{p-1} \equiv 1 \bmod p$. $\boxed{\text{5 pkt.}}$

22. Napisać program, który dla zadanego n wypisze n-ty ciąg Farey'a. $\boxed{\text{4 pkt.}}$

23. Napisać program, który wykorzystując drzewo Sterna–Brocota znajdzie rozwinięcie danej liczby wymiernej w ułamek łańcuchowy (uwaga: drzewo powinno być zbudowane do poziomu N jeżeli dana liczba nie znajduje się w drzewie program powinien zwracać aproksymację tej liczby). $\boxed{\text{4 pkt.}}$

24. Opierając się na własnościach ciągów Farey'a trochę wzmocnić tezę twierdzenia Dirichelt'a a mianowicie, że nierówność: $|x - \frac{p}{q}| < \frac{1}{2q^2}$, zachodzi dla nieskończenie wielu par $p, q \in \mathbb{Z}$. $\boxed{\text{6 pkt.}}$

3 Podstawy aproksymacji funkcji ciągłych i układy ortogonalne

Układy ortogonalne, aproksymacja w L^2. Aproksymacja L^∞, Twierdzenie Weierstrass'a, Pakiet `chebfun`. ([1], [8])

1. Niech $f\colon R \to [0,1]$ będzie dowolną rzeczywistą funkcją o następujących własnościach: $0 \leq f(t) \leq 1$, $f(t+2) = f(t)$. Określmy odwzorowanie $\Phi\colon R \to [0,1]^2$ takie, że $\Phi(t) = (x(t), y(t))$, gdzie:

$$x(t) = \sum_{n=1}^{\infty} 2^{-n} f(3^{2n-1}t) \tag{1}$$

$$y(t) = \sum_{n=1}^{\infty} 2^{-n} f(3^{2n}t) \tag{2}$$

Wykonać następujące zadania:

(a) Udowodnić, że Φ jest funkcją ciągłą. $\boxed{\text{4 pkt.}}$

(b) Udowodnić, że Φ odwzorowuje odcinek jednostkowy $[0,1]$ na kwadrat jednostkowy $[0,1]^2$. $\boxed{\text{6 pkt.}}$

(c) Narysować N-te przybliżenie krzywej przyjmując dowolną funkcję f. 6 pkt.

(wskazówka: W. Rudin, Podstawy analizy matematycznej, PWN Warszawa 1998 (rozdział 7. oraz zadania)

2. Narysować N-te przybliżenie dowolnej innej krzywej typu Peano (krzywej ciągłej wypełniającej kwadrat, np. orginalną krzywą Peano lub krzywą Hilberta) 6 pkt.

3. "Narysować" krzywą ciągłą niegdzie nieróżniczkowalną (nie posiadającą pochodnej w żadnym punkcie) – tak na prawdę to chodzi o N-te przybliżenie takiej krzywej. 6 pkt. Czy można zapewnić, aby to N-te przybliżenie było funkcją gładką. 4 pkt.

4. Uzasadnić, przynajmniej graficznie, że trójkąt Sierpińskiego jest ciągłym obrazem odcinka. 7 pkt.

5. Jak widać z poprzednich punktów odcinek można w sposób ciągły odwzorować na kwadrat, jednak odwzorowania takiego nie można odwrócić. Dzieje się tak między innymi dlatego, że odwzorowanie to nie jest różnowartościowe. Rozstrzygnąć czy istnieje jednak takie odwzorowanie, które odwzorowuje przedział jednostkowy $[0, 1]$ w pewien podzbiór w R^2, który posiada pole (dodatnią miarę w R^2), (oznaczałoby to, że odcinek jest homeomorficzny z pewnym zbiorem posiadającym pole). 10 pkt.

References

[1] N. I. Achiezer. *Teoria aproksymacji.* PWN Warszawa, 1957.

[2] D. E. Knuth. *Sztuka programowania, tom 2.* WNT, Warszawa, 2002.

[3] K. Kuratowski. *Wstęp do teorii mnogości i topologii.* PWN, Warszawa, 1980.

[4] W. Narkiewicz. *Teoria liczb.* WNT, Warszawa, 1977.

[5] H. Rasiowa. *Wstęp do matematyki współczesnej.* PWN, Warszawa, 1973.

[6] P. Ribenboim. *Mała księga wielkich liczb pierwszych.* WNT, Warszawa, 1997.

[7] K. A. Ross and Ch. R. B. Wright. *Matematyka dyskretna.* PWN, Warszawa, 1999.

[8] W. Rudin. *Podstawy analizy matematycznej.* PWN Warszawa, 1998.