Logika dla informatyków

wykład 5

4 listopada 1999

1 Teoria mocy, cd.

Twierdzenie Cantora-Bernsteina. Jeśli $|A| \leq |B|$ oraz $|B| \leq |A|$, to $|A| = |B|$.

Definicja. Mówimy że moc zbioru A jest mniejsza niż moc zbioru B i piszemy $|A| < |B|$, jeśli $|A| \leq |B|$ oraz $A \not\sim B$.

Twierdzenie.

1. $|A| \leq |A|$
2. jeśli $|A| \leq |B|$ i $|B| \leq |C|$, to $|A| \leq |C|$
3. jeśli $n < m$, to $|\underline{n}| < |\underline{m}|$
4. $|\underline{n}| < \aleph_0$

Definicja. Jeśli $X \subseteq A$, to $f : A \to \{0,1\}$ jest *funkcją charakterystyczną* zbioru A, jeśli dla dowolnego $a \in A$

$$f(a) = \begin{cases} 0, & \text{gdy } a \notin X; \\ 1, & \text{gdy } a \in X. \end{cases}$$

Fakt. $\underline{2}^A \sim \mathcal{P}(A)$.

Twierdzenie. Niech A i B będą zbiorami, przy czym $|B| \geq 2$. Wtedy

$$|\mathcal{P}(A)| \leq |B^A|$$

gdzie $B^A = \{f : A \to B\}$ a $\mathcal{P}(A)$ oznacza zbiór potęgowy zbioru A.

Twierdzenie Cantora. Dla żadnego A nie istnieje funkcja z A *na* zbiór potęgowy $\mathcal{P}(A)$.

Dowód. Przypuśćmy przeciwnie, że pewna funkcja $f : A \to \mathcal{P}(A)$ przekształca A *na* $\mathcal{P}(A)$. Niech

$$A_0 \quad = \quad \{a \in A \mid a \notin f(a)\}$$

Ponieważ $A_0 \subseteq A$ i f odwzorowuje A *na* $\mathcal{P}(A)$, więc istnieje $a_0 \in A$, takie że $f(a_0) = A$. Mamy wtedy

$$a_0 \in A_0 \iff a_0 \in f(a_0) \iff a_0 \notin A_0$$

Założenie istnienia funkcji f doprowadziło do sprzeczności.

Dowód twierdzenia Cantora dla przypadku $A = \mathbb{N}$. Przypuśćmy przeciwnie, że pewna funkcja $f : \mathbb{N} \to \underline{2}^{\mathbb{N}}$ przekształca $\mathbb{N}$ *na* $\underline{2}^{\mathbb{N}}$. Tworzymy nieskończoną tablicę

$$\begin{array}{cccccc}
\boxed{\text{(f(0))(0)}} & (f(0))(1) & (f(0))(2) & (f(0))(3) & (f(0))(4) & \cdots \\
(f(1))(0) & \boxed{\text{(f(1))(1)}} & (f(1))(2) & (f(1))(3) & (f(1))(4) & \cdots \\
(f(2))(0) & (f(2))(1) & \boxed{\text{(f(2))(2)}} & (f(2))(3) & (f(2))(4) & \cdots \\
(f(3))(0) & (f(3))(1) & (f(3))(2) & \boxed{\text{(f(3))(3)}} & (f(3))(4) & \cdots \\
(f(4))(0) & (f(4))(1) & (f(4))(2) & (f(4))(3) & \boxed{\text{(f(4))(4)}} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Tworzymy nową funkcję charakterystyczną

$$g(i) \quad = \quad 1 - (f(i))(i)$$

dla każdego $i \in \mathbb{N}$. Wtedy $g \neq f(i)$ dla dowolnego $i \in \mathbb{N}$, gdyż $g(i) = 1 - (f(i))(i) \neq f(i)$. Otrzymaliśmy sprzeczność z założeniem, że f jest *na*.

Twierdzenie. Dla każdego zbioru A, $|\mathcal{P}(A)| > |A|$. Jeśli $|B| > 2$, to $|B^A| > |A|$.

2 Zbiory przeliczalne

Definicja. Zbiór A jest *przeliczalny*, gdy A jest skończony lub jest równoliczny ze zbiorem liczb naturalnych.

Twierdzenie. Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy $A = \emptyset$ lub istnieje funkcja z $\mathbb{N}$ *na* A.

Definicja. *Ciągiem elementów zbioru* A nazywamy funkcję $f : \mathbb{N} \to A$.

Fakt. Zbiór niepusty jest przeliczalny, gdy jego elementy można ustawić w ciąg.

Twierdzenie.

1. Podzbiór zbioru przeliczalnego jest przeliczalny.
2. Jeśli $f : A \to B$ oraz $X \subseteq A$ jest zbiorem przeliczalnym, to $f(X)$ też jest zbiorem przeliczalnym.
3. Jeśli A i B są przeliczalne, to $A \times B$ jest przeliczalny.
4. Jeśli $\{A_i \mid i \in I\}$ jest przeliczalną rodziną zbiorów przeliczalnych (tzn. I jest przeliczalny i każdy ze zbiorów A_i jest przeliczalny), to $\bigcup_{i \in I} A_i$ jest zbiorem przeliczalnym.

Twierdzenie. Zbiór liczb rzeczywistych jest równoliczny ze zbiorem $\{0,1\}^{\mathbb{N}}$. Zatem zbiór $\{0,1\}^{\mathbb{N}}$ ma moc continuum.

3 Porządki częściowe

Definicja. Relacja R jest *słabo antysymetryczna*, jeśli dla dowolnych a, b

$$\text{jeśli } aRb \text{ oraz } bRa \text{ to } a = b$$

Definicja. *Częściowym porządkiem* w zbiorze A nazywamy relację „$\leq$" (będącą podzbiorem A^2), która jest *zwrotna*, *przechodnia* i *słabo antysymetryczna*, tzn.

$$\forall a. a \leq a$$
$$\forall a, b. (a \leq b \wedge b \leq a \Rightarrow a = b)$$
$$\forall a, b, c. (a \leq b \wedge b \leq c \Rightarrow a \leq c)$$

Oznaczenie. Jeśli $\leq$ jest częściowym porządkiem na A, to $a < b$ oznacza $a \leq b \wedge a \neq b$.

Definicja. *Zbiór częściowo uporządkowany* to zbiór A z relacją częściowego porządku $\leq$. Zbiór częściowo uporządkowany oznaczamy czasem $\langle A, \leq \rangle$.

Przykłady zbiorów częściowo uporządkowanych:

1. $\langle \mathcal{P}(A), \subseteq \rangle$ (rodzina podzbiorów zbioru A z relacją inkluzji);
2. $\langle \mathbb{N}, \leq \rangle$ (zbiór liczb naturalnych ze zwykłym porządkiem);
3. $\langle \mathcal{B}, \subseteq \rangle$, gdzie $\mathcal{B} \subseteq \mathcal{P}(A)$;
4. $\langle \mathbb{N}, | \rangle$, gdzie $a|b \Leftrightarrow \exists x. (ax = b)$.

4 Słowa

Definicja. Niech A będzie dowolnym zbiorem. Będziemy nazywać go *alfabetem*. *Słowem* nad alfabetem A nazywamy dowolny skończony ciąg elementów zbioru A. Słowo puste (ciąg długości zero) oznaczamy ε. Przez A^* oznaczamy zbiór wszystkich słów nad alfabetem A. Jeżeli $u = u_1u_2\ldots u_n$ i $w = w_1w_2\ldots w_m$, to uw oznacza *złożenie* (*konkatenację*) słów u i w, tj. słowo $u_1u_2\ldots u_nw_1w_2\ldots w_m$. Słowo U jest *przedrostkiem* (*prefiksem*) słowa w, jeśli istnieje słowo v, takie że $uv = w$.

Fakt. Niech A będzie dowolnym zbiorem i niech $u \leq w$ oznacza, że u jest przedrostkiem w. Wtedy $\langle A, \leq\rangle$ jest zbiorem częściowo uporządkowanym.