Akademia Górniczo-Hutnicza
im. Stanisława Staszica
w Krakowie

Skrypt

Złożoność obliczeniowa

dr Marcin Stawiski

WMS
AGH

Wydział Matematyki ~~Stosowanej~~

Kraków/Graz 2024

Spis treści

0. Formalności

- Marcin Stawiski,
- e-mail: stawiski@agh.edu.pl,
- konsultacje: pokój 6.17 w C7 po wcześniejszym umówieniu się mailowo. Termin 10:00 w środy lub 17:30 w czwartki.

0.1. Zasady zaliczenia egzaminu

- egzamin ustny,
- na egzamin obowiązuje teoria z wykładów oraz ze skryptu,
- warunkiem uczestnictwa w egzaminie jest pozytywna ocena z ćwiczeń,
- ocena końcowa to zaokrąglone $\frac{1}{3}$ oceny z ćwiczeń plus $\frac{2}{3}$ oceny z egzaminu, jeśli ta ostatnia jest pozytywna,
- obecność na wykładzie nie jest obowiązkowa, ale bieżąca wiedza z wykładu JEST obowiązkowa na ćwiczeniach,
- przedmiot jest trudny i będzie wymagający na egzaminie. Studenci muszą znać treść wykładu ZE ZROZUMIENIEM, co jest istotne. Jeśli student będzie znał treść wykładu bez zrozumienia, to nadal może nie zdać egzaminu.
- Studenci na bieżąco powinni wyjaśniać wszelkie wątpliwości i zadawać pytania. W razie problemów ze zrozumieniem materiału lub w razie innych pytań zapraszam na konsultacje, o których wspomniałem wcześniej.
- Należy śmiać się z żartów prowadzącego!

0.2. Ćwiczenia

- kolokwium na 60 punktów oraz projekt na 40 punktów,
- ocenę może podnieść także aktywność podczas ćwiczeń i WYKŁADÓW,

- zamiast kolokwium zaliczeniowego proponuję drugi projekt.

0.3. Bibliografia

1. J. E. Hopcroft, R. Motwani, J. D. Ullman, *Wprowadzenie do teorii automatów, języków i obliczeń*, PWN, 2020.
2. G. S. Boolos, J. P. Burgess, R. C. Jeffrey, *Computability and Logic*, Cambridge University Press, 2007.
3. M. R. Garey, D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman, 1979.
4. A. Błaszczyk, S. Turek, *Teoria Mnogości*, PWN, 2015.
5. A. Piękosz, *Wstęp do teorii modeli*, Wydawnictwo Politechniki Krakowskiej, 2008.

Program wykładu będzie istotnie różny niż w poprzednich latach, więc notatki z poprzednich lat nie są ani konieczne, ani wystarczające. W zamian mamy pewną swobodę w doborze materiału i możemy pewne fragmenty skrócić, wydłużyć, dołożyć bądź usunąć w zależności od tego, jak będzie przebiegało tempo wykładu. Ważniejsze jest dla mnie to, aby studenci zrozumieli treść wykładu, a nie żebyśmy przerobili jak najwięcej materiału. Wykład wraz ze skryptem są samowystarczalne, to znaczy, że podana literatura nie jest obowiązkowa, ale może ułatwić zrozumienie pewnych pojęć i uzupełnić wiedzę.

Życzę miłej lektury!

1. Wprowadzenie

Jakie, Państwa zdaniem, działy matematyki zawierają się w podstawach matematyki?

Podstawy matematyki (foundations):
- ~~analiza matematyczna~~,
- ~~fizyka matematyczna~~,
- logika matematyczna,
- teoria mnogości,
- teoria modeli,
- teoria dowodu,
- złożoność obliczeniowa i obliczalność.

Będziemy zajmować się złożonością obliczeniową jako podstawami informatyki, ale też złożonością obliczeniową jako częścią (podstaw) matematyki. Informatyka teoretyczna jest w istocie działem matematyki mocno związana z logiką matematyczną. Granica między tym, co należy do informatyki, a co do matematyki często jest umowna, „sztuczna” i płynna. Właściwie wszystkie nazwiska, które będą się przewijać w trakcie wykładu czy ćwiczeń, to logicy matematyczni.

Jako że ten przedmiot zajmuje się teoretycznymi podstawy informatyki, to zaczynamy w tej kwestii od zera i nie ma żadnych wymagań wstępnych odnośnie informatyki, chociaż pewna intuicja związana z programowaniem czy algorytmami może być pomocna. Wynika to z tego, że do wielu zagadnień można podejść z punktu widzenia logiki matematycznej lub z punktu widzenia bardziej informatycznego.

Jeśli chodzi o matematykę, to niezbędna będzie podstawowa wiedza ze wstępu do logiki i teorii mnogości oraz teorii grafów. Większość tego, co potrzebne będzie w kwestii logiki i teorii mnogości, zostanie jednak przedstawione na wykładzie i ćwiczeniach.

Na jakie pytania odpowiemy na wykładzie?

1. Czy dla wszystkich problemów decyzyjnych (tj. takich, dla których odpowiedź to „tak” lub „nie”) istnieje algorytm pozwalający odpowiedzieć na to pytanie?
2. Co to znaczy, że problem jest obliczalny?
3. Co to znaczy, że problem jest wielomianowy?
4. Co oznacza „P vs. NP”? Jeden z problemów milenijnych. Czy słyszeli Państwo o tym problemie? Co oznaczają P i NP?
5. Czy zbiór aksjomatów matematyki (teorii mnogości) jest niesprzeczny lub zupełny?(twierdzenia Gödla)
6. Co oznacza, że zdanie jest niezależne od aksjomatów? (hipoteza continuum, aksjomat wyboru)

Z czego będzie składał się wykład? Trzy części: podstawy matematyki, obliczalność i złożoność obliczeniowa.

1. Podstawy matematyki.
2. Różne modele obliczeniowe (maszyny Turinga i jej modyfikacje, funkcje rekurencyjne), formalizacja pojęcia obliczalności, równoważność omawianych modeli.
3. Problemy nieobliczalne w informatyce.
4. Wpływ nieobliczalności na matematykę. Niedowodliwość w teoriach matematycznych. (Elementy logiki oraz teorii dowodu.)
5. „Właściwa” złożoność obliczeniowa - (heurystycznie) ilość zasobów (czasu, pamięci, operacji, . . .) potrzebnych do rozwiązania problemu obliczalnego. Klasy P i NP.
6. Problemy NP-zupełne.

Część I
Logika i podstawy matematyki

2. Logika pierwszego rzędu

Naszym pierwszym celem w tej części wykładu będzie „sformalizowanie matematyki”. W celu nadania matematycznym sformułowaniom dokładne, formalne i jednoznaczne znaczenie potrzebny nam będzie pewnego rodzaju język. Język polski, czy jakikolwiek inny „naturalny” język, w zwykłej formie nie nadaje się do tego, ponieważ zdania w naturalnym języku nie muszą być ani dokładne, ani formalne i przede wszystkim bardzo często bywają niejednoznaczne. Dodatkowym problemem w używaniu naturalnego języka do opisu matematyki jest problem z tłumaczeniem, który pogłębia wymienione wcześniej problemy.

W kolejnym rozdziale opiszemy system zwany logiką pierwszego rzędu lub rachunkiem predykatów. Podamy sposoby konstrukcji sformułowań matematycznych w logice pierwszego rzędu, czyli pewnych zdań lub ogólniej formuł logicznych. W logice istotne jest rozróżnienie między składnią danego języka, a jego znaczeniem w danym kontekście. Dla przykładu wprowadzamy rozróżnienie pomiędzy zdaniem „$\forall x\ \forall y\ x + y = y$” , a jego znaczeniem czy też prawdziwością. Dokładne znaczenie uzyska on dopiero wtedy, gdy przypiszemy symbolowi „$+$” dokładne znaczenie oraz uzgodnimy po jakim zbiorze przebiegają kwantyfikatory. Zawsze będziemy jednak zakładać, że kwantyfikatory przebiegają po niepustym zbiorze.

Najpierw zajmiemy się składnią logiki pierwszego rzędu.

2.1. Języki pierwszego rzędu

Językiem (pierwszego rzędu) L będziemy nazywać (niekoniecznie skończony) zbiór symboli postaci $Fun_L \cup Const_L \cup Rel_L$, gdzie Fun_L, $Const_L$ i Rel_L są parami rozłącznymi zbiorami, wraz z określoną na $Fun_L \cup Const_L \cup Rel_L$ funkcją arności zwaną też sygnaturą lub typem $\sigma = \sigma_L$. Elementy Fun_L nazywamy symbolami

funkcyjnymi, elementy $Const_L$ nazywamy symbolami stałych, a elementy Rel_L nazywamy symbolami relacyjnymi. Sygnatura działa w sposób następujący:
1. Każdemu symbolowi F z Fun_L przypisuje liczbę $\sigma(F) \in \mathbb{N}$.
2. Każdemu symbolowi C z $Const_L$ przypisuje liczbę 0.
3. Każdemu symbolowi R z Rel_L przypisuje liczbę $\sigma(R) \in \mathbb{N}$.

W praktyce będziemy domyślać się argumentowości odpowiednich symboli, będziemy pomijać sygnaturę i po prostu utożsamiać język L ze zbiorem $Fun_L \cup Const_L \cup Const_L$.

Elementy języka L możemy interpretować jako pewne symbole, którym następnie przypiszemy jakieś znaczenie. W szczególności symbole funkcyjne nie są funkcjami, a jedynie ich oznaczeniami. Wartość funkcji arności dla symbolu funkcyjnego informuje nas, ile argumentów będzie miała funkcja, której dopiero przypiszemy jakieś znaczenie. Analogiczna sytuacja dotyczy relacji i symboli relacyjnych. Stałe możemy też interpretować jako funkcje stałe, a funkcje jako relacje, ale w praktyce wygodniej jest rozdzielić funkcje od pozostałych relacji i stałych.

2.2. Logika pierwszego rzędu

Do konstrukcji systemu logiki pierwszego rzędu podamy potrzebne nam symbole, które będą pełnić rolę podobną do alfabetu, a następnie reguły tworzenia „napisów”: termów oraz formuł.

Dla danego języka L będziemy używać następujących symboli do jego opisu:
1. Symbole logiczne: $\wedge, \ \vee, \neg, \forall, \ \exists, \ =$.
2. Symbole zmiennych: $x, \ y, \ z, \dots, \ x_1, \ x_2, x_3, \dots$ (w przeliczalnej liczbie).
3. Symbole pozalogiczne, czyli symbole z języka L.
4. Symbole pomocnicze, czyli nawiasy oraz przecinek.

Uwaga: W logice pierwszego rzędu wszystkie stałe i zmienne są tego samego typu. Dla przykładu w teorii mnogości nie rozróżniamy między obiektami-zbiorami a obiektami-elementami. Każdy zbiór może być elementem innego zbioru, a każdy element zbioru sam jest zbiorem.

Uwaga: Symbol relacji „=” będzie traktowany jako symbol logiczny. Odnotujmy, że implikację oraz równoważność można zapisać przy pomocy pozostałych symboli logicznych, dlatego nie ma ich na liście.

Zdefiniujemy teraz pojęcie termu. O termie możemy myśleć jako o „wartości funkcji”, ale dopiero wtedy, gdy będziemy mieli daną interpretację odpowiednich symboli.

definicja 2.1. *Zbiorem termów języka L nazywamy skończone ciągi symboli powstałe w następujący sposób:*
1. *Każdy symbol stałej $C \in Const_L$ jest termem.*
2. *Każdy symbol zmiennej x jest termem.*

3. *Jeśli dany jest symbol funkcyjny* $F \in Fun_L$ *argumentowości* n *oraz termy* $t_1, \dots, t_n$*, to* $F(t_1, \dots, t_n)$ *też jest termem,.*
4. *Tylko te ciągi symboli, które powstały w skończeniu wiele krokach z powyższych reguł są termami języka* L*.*

Przykładami termów są: „$1 + 2$”, „$\arccos x$”, „0”, „x”, ...

Uwaga: Dla symboli funkcji dwuargumentowych często stosuje się zapis infiksowy, np. piszemy $1 + 2$ zamiast $+(1, 2)$.

definicja 2.2. *Termem stałym nazywamy term niezawierający symboli zmiennych.*

Podamy teraz definicję formuły. O formułach możemy myśleć jako o relacjach, które zachodzą (lub nie) pomiędzy termami, ale znów dopiero wtedy, gdy będziemy mieli interpretację odpowiednich symboli.

definicja 2.3. *Formułą atomiczną języka* L *nazywamy każdy skończony ciąg znaków postaci:*
$t_1 = t_2$*, gdzie* t_1 *oraz* t_2 *są termami* L*,*
$R(t_1, \dots, t_n)$*, gdzie* R *jest symbolem relacyjnym argumentowości* n*, a* $t_1, \dots, t_n$ *są termami* L*.*

definicja 2.4. *Zbiorem formuł języka* L *(ozn.* $Form_L$*) nazywamy zbiór otrzymany w następujący sposób:*
1. *Każda formuła atomiczna* L *jest formułą* L*,*
2. *Każdy ciąg symboli postaci* $\varphi \wedge \psi$, $\varphi \vee \psi$, $\neg\varphi$, $\forall x\ \varphi$, $\exists x\ \varphi$ *jest formułą* L*, gdzie* φ *i* ψ *są formułami języka* L*, a* x *jest dowolnym symbolem zmiennej,*
3. *Tylko te ciągi symboli, które powstały w skończeniu wiele krokach z powyższych reguł są formułami języka* L*.*

definicja 2.5. *Podformułą formuły* φ *języka* L *nazywamy każdą formułę, która posłużyła do skonstruowania formuły* φ *włącznie z samą* φ*.*

definicja 2.6. *Mówimy, że zmienna* x *jest wolna w termie* φ*, jeśli występuje w termie* φ *i nie jest związana w* φ *kwantyfikatorem* $\forall x$*, ani* $\exists x$*. Zmienne, które występują w formule* φ*, ale nie są wolne, nazywamy związanymi. Jeśli* $x_1, \dots$ *są zmiennymi wolnymi formuły* φ*, to przez* $\varphi(y_1, \dots)$ *oznaczamy formułę powstałą przez zastąpienie* $(x_1, \dots)$ *przez* $(y_1, \dots)$*.*

definicja 2.7. *Zdaniem nazywamy formułę bez zmiennych wolnych. Zbiór zdań języka* L *oznaczamy przez* $Sent_L$*.*

Porównaj z definicją zdania jako „obiektu” prawdziwego lub nie.

3. Teoria dowodu

W tym rozdziale omówimy formalnie pojęcie dowodu w systemie formalnym. Dzięki wprowadzonym pojęciom możemy uzyskać system aksjomatyczny. Różni się tym od systemu „półaksjomatycznego” tym, że mamy ściśle zdefiniowane nie tylko aksjomaty danej teorii, ale także ściśle zdefiniowane reguły wnioskowania, czyli tego, w jaki sposób uzyskujemy nowe twierdzenia z aksjomatów i poprzednio udowodnionych twierdzeń. Przykładem teorii półaksjomatycznej jest np. geometria Euklidesa.

definicja 3.1. *Systemem formalnym nazywamy zbiór* $\mathcal{S} = (L,\ A,\ B,\ \Sigma)$*, gdzie*
1. L *jest pewnym językiem.*
2. A *jest zbiorem aksjomatów logicznych.*
3. B *jest zbiorem reguł wnioskowania.*
4. Σ *jest pewnym zbiorem zdań języka* L*, a jego elementy nazywamy aksjomatami systemu* $\mathcal{S}$*.*

Zdefiniujemy teraz formalnie pojęcie dowodu. Poniższą definicję możemy zobrazować w taki sposób, że twierdzenie w jest dowodzone z aksjomatów lub poprzednio udowodnionych twierdzeń.

definicja 3.2. *Dowodem formalnym lub po prostu dowodem zdania* w *ze zbioru zdań* Σ *nazywamy skończony ciąg zdań* $w_1, \ldots, w_n = z$*, taki że dla każdego* $i \leqslant n$ *zdanie* w_i *jest aksjomatem systemu formalnego, elementem* Σ *lub istnieją liczby* $j_1, \ldots j_k \leqslant i$*, takie że* w_i *można uzyskać z* $w_{j_1}, \ldots, w_{j_k}$ *za pomocą jednej z reguł wnioskowania.*

Najważniejszą z reguł wnioskowania jest modus ponens, który mówi o tym, że jeśli mamy implikację i poprzednik implikacji jest prawdziwy, to możemy wywnioskować następnik implikacji.

definicja 3.3. *Modus ponens (lub reguła odrywania) to następująca reguła wnioskowania, jeśli $p \Rightarrow q$ oraz p, to wnioskujemy q.*

Uwaga: dla uproszczenia zwykle często zakłada się, że jedyną regułą wnioskowania jest modus ponens.

definicja 3.4. *Jeśli istnieje dowód zdania w ze zbioru zdań Σ, to mówimy, że w jest konsekwencją logiczną zbioru Σ i piszemy $\Sigma \models w$.*

definicja 3.5. *Jeśli zdanie w posiada dowód w systemie $\mathcal{S}$, to w nazywamy twierdzeniem systemu $\mathcal{S}$.*

definicja 3.6. *Domknięciem dedukcyjnym lub zbiorem konsekwencji logicznych zbioru zdań Σ nazywamy zbiór $Con_L(Z) = \{w \in Sent_L \colon \Sigma \models w\}$.*

definicja 3.7. *Mówimy, że zbiór zdań Σ jest dedukcyjnie domknięty, jeśli*

$$Con_L(\Sigma) = \Sigma.$$

definicja 3.8. *Mówimy, że zbiór zdań Σ jest sprzeczny, jeśli istnieje zdanie $\varphi \in Sent_L$, takie że $\Sigma \models \varphi$ oraz $\Sigma \models \neg\varphi$. W przeciwnym przypadku mówimy, że Σ jest niesprzeczny.*

definicja 3.9. *Mówimy, że zdanie φ jest niezależne od zbioru zdań Σ, jeśli $\Sigma \not\models \varphi$ oraz $\Sigma \not\models \neg\varphi$.*

Najbardziej znanym zdaniem niezależnym od standardowych aksjomatów teorii mnogości jest hipoteza continuum, która mówi o tym, że nie ma zbiorów o mocy pośredniej między mocą zbioru liczb naturalnych a mocą zbioru liczb rzeczywistych.

Twierdzenie 3.10. *Jeśli zdanie φ jest niezależne od zbioru zdań Σ, to zarówno $\Sigma \cup \{\varphi\}$ jak i $\Sigma \cup \{\neg\varphi\}$ są niesprzeczne.* ■

Twierdzenie 3.11 (Malcew 1936, o zwartości)**.** *Zbiór zdań Σ jest niesprzeczny wtedy i tylko wtedy, gdy każdy jego skończony podzbiór jest niesprzeczny.*

dowód. Implikacja w prawo jest oczywista, bo dowód sprzeczności w podzbiorze Σ' zbioru Σ jest też dowodem w Σ. Załóżmy więc dla dowodu nie wprost, że zbiór Σ jest sprzeczny i niech $w_1, \ldots, w_n$ będzie dowodem zdania $\varphi \vee \neg\varphi$ w Σ dla pewnego $\varphi \in Sent_L$. Wówczas dowód $w_1, \ldots, w_n$ jest skończony, więc znajduje się w nim tylko skończona liczba zdań z Σ. Oznaczmy go przez Σ'. Wówczas $w_1, \ldots, w_n$ jest także dowodem zdania $\varphi \vee \neg\varphi$ w Σ' oraz Σ' jest skończone. ■

definicja 3.12. *Zbiór zdań jednocześnie niesprzeczny i dedukcyjnie domknięty nazywamy teorią.*

definicja 3.13. *Mówimy, że zbiór zdań* Σ *jest zupełny, jeśli dla każdego zdania* $\varphi \in Sent_L$ *zachodzi* $\Sigma \models \varphi$ *lub* $\Sigma \models \neg\varphi$.

4. Teoria modeli

Teoria modeli jest działem matematyki zajmującym się związkiem między składnią języka, a jego znaczeniem, czyli semantyką. Na razie poznaliśmy sposoby tworzenia „sensownych” napisów w logice pierwszego rzędu. W kolejnym rozdziale podamy w jaki sposób możemy powiązać składnię, formuły czy termy z ich znaczeniem w danym kontekście matematycznym.

4.1. Modele

definicja 4.1. *Niech M, I, J, K będą zbiorami parami rozłącznymi. Ponadto niech $M \neq \emptyset$. Strukturą nazywamy zbiór*

$$\mathcal{M} = (M, \{f_i\}_{i\in I}, \{c_j\}_{j\in J}, \{r_k\}_{r\in K}), \text{ gdzie:}$$

1. *M nazywamy zbiorem podkładowym lub uniwersum struktury M.*
2. *Każde f_i jest odwzorowaniem $f_i\colon M^{a(i)} \to M$ zwanym funkcją pierwotną struktury $\mathcal{M}$, a liczbę $a(i) \in \mathbb{N}$ nazywamy arnością (argumentowością) funkcji f_i.*
3. *Każde c_j jest elementem M zwanym stałą struktury $\mathcal{M}$.*
4. *Każde r_k jest relacją $r_k \subseteq M^{a(k)}$ zwaną relacją pierwotną struktury $\mathcal{M}$, a liczbę $a(k) \in \mathbb{N}$ nazywamy arnością lub argumentowością relacji r_k.*

Przykładami modeli są $(\mathbb{N}, 0, 1, +, \cdot)$, $(\mathbb{R}, 1, \leqslant)$. Każda grupa, pierścień czy ciało również są modelami. Podobnie modelami są grafy, gdzie zbiór krawędzi będziemy interpretować jako pewną dwuargumentową relację, która jest przeciwzwrotna i symetryczna.

W celu powiązania modeli z językami przydatne będzie pojęcie L-struktury.

definicja 4.2. *Strukturą języka L lub L-strukturą nazywamy zbiór*

$$\mathcal{M} = (M, \{F^{\mathcal{M}}\}_{F\in Fun_L}, \{C^{\mathcal{M}}\}_{C\in Const_L}, \{R^{\mathcal{M}}\}_{R\in Rel_L}), \text{ gdzie:}$$

1. *M jest niepustym zbiorem będącym uniwersum L-struktury $\mathcal{M}$.*
2. *Każdemu symbolowi funkcyjnemu $F \in Fun_L$ przypisujemy funkcję pierwotną $F^{\mathcal{M}}: M^{\sigma_L(F)} \to M$ struktury $\mathcal{M}$ zwaną interpretacją symbolu F w $\mathcal{M}$.*
3. *Każdemu symbolowi stałej $C \in Const_L$ przypisujemy stałą pierwotną $C^{\mathcal{M}} \in M$ struktury $\mathcal{M}$ zwaną interpretacją symbolu F w $\mathcal{M}$.*
4. *Każdemu symbolowi relacyjnemu $R \in Rel_L$ przypisujemy relację pierwotną $R^{\mathcal{M}} \subseteq M^{\sigma_L(R)}$ struktury $\mathcal{M}$ zwaną interpretacją symbolu R w $\mathcal{M}$.*

W teorii grafów przez $|G|$ oznaczaliśmy nie tyle moc grafu jako zbioru, bo graf jako para ma zawsze 2 elementy, ale moc jego zbioru wierzchołków, a więc w języku teorii modeli - uniwersum grafu. Podobna konwencja dotyczy także innych struktur.

definicja 4.3. *Mocą struktury $\mathcal{M}$ nazywamy moc jej uniwersum i oznaczamy ją przez $|\mathcal{M}|$.*

Gdy dla języka L mamy daną jego strukturę $\mathcal{M}$, to możemy nadać termom i formułom tego znaczenie w naturalny sposób. Możemy wówczas mówić o wartości logicznej zdań, czyli temu czy są prawdziwe w strukturze $\mathcal{M}$ czy też są fałszywe.

definicja 4.4. *Zbiór zdań prawdziwych w strukturze $\mathcal{M}$ nazywamy teorią struktury $\mathcal{M}$ i oznaczamy ją przez $\mathcal{T}h(\mathcal{M})$.*

definicja 4.5. *Niech Σ będzie zbiorem pewnych zdań języka L (zbiorem aksjomatów). Mówimy, że struktura $\mathcal{M}$ jest modelem zbioru zdań Σ, jeśli $\Sigma \subseteq \mathcal{T}h(\mathcal{M})$.*

definicja 4.6. *Mówimy, że zbiór zdań Σ jest niesprzeczny semantycznie, jeśli posiada model.*

Bardzo ważnym pojęciem w matematyce są pojęcia homomorfizmu oraz izomorfizmu, które w szczególnych wersjach poznaliście między innymi na algebrze czy teorii grafów. Podamy teraz ich ogólniejszą formę.

definicja 4.7. *Niech $\mathcal{M}$ oraz $\mathcal{N}$ będą L-strukturami. Wówczas odwzorowanie $h: M \to N$ nazywamy homomorfizmem z $\mathcal{M}$ do $\mathcal{N}$, gdy spełnione są następujące warunki:*
1. *Dla każdego symbolu stałej C mamy $h(C^{\mathcal{M}}) = C^{\mathcal{N}}$.*
2. *Dla każdego symbolu funkcyjnego F arności n oraz $a_1, \dots, a_n \in M$ mamy $h(F^{\mathcal{M}}(a_1, \dots, a_n)) = F^{\mathcal{N}}(h(a_1), \dots, h(a_n))$.*
3. *Dla każdego symbolu relacyjnego R arności n oraz $a_1, \dots, a_n \in M$, z faktu, że $(a_1, \dots, a_n) \in R^{\mathcal{M}}$, wynika $(h(a_1), \dots, h(a_n)) \in R^{\mathcal{N}}$.*

definicja 4.8. *Mówimy, że homomorfizm z $\mathcal{M}$ do $\mathcal{N}$ jest izomorfizmem, jeśli jego funkcja odwrotna jest homomorfizmem z $\mathcal{N}$ do $\mathcal{M}$. Ponadto, izomorfizm z $\mathcal{M}$ do $\mathcal{M}$ nazywamy automorfizmem struktury $\mathcal{M}$.*

5. Arytmetyka Peana

Za przykład zastosowania logiki pierwszego rzędu posłuży nam arytmetyka liczb naturalnych pochodząca od Peana.

5.1. Aksjomaty Peana

definicja 5.1. *Niech $L = \{+, \cdot, 0, 1, \leqslant\}$. Arytmetyką Peana (pierwszego rzędu) (w skrócie PA) nazywamy następujący zbiór aksjomatów:*
1. $\forall x\ x + 1 \neq 0$,
2. $\forall x\ 0 \leqslant x$,
3. $\forall x\ (x = 0) \vee \neg(x \leqslant 0)$,
4. $\forall x\ x + 0 = x$,
5. $\forall x\ x \cdot 0 = 0$,
6. $\forall x\ \forall y\ x + (y + 1) = (x + y) + 1$,
7. $\forall x\ \forall y\ x \cdot (y + 1) = x \cdot y + x$,
8. $\forall x\ \forall y\ (x + 1 = y + 1) \Rightarrow x = y$,
9. $\forall x\ \forall y\ (y \leqslant x + 1) \Leftrightarrow (y \leqslant x \vee y = x + 1)$,
10. $\forall x\ \forall y\ (x + 1 \leqslant y) \Leftrightarrow (x \leqslant y \wedge x \neq y)$,

oraz następujący schemat aksjomatów indukcji mówiący o tym, że dla każdej formuły $\varphi(x_1, \ldots, x_n, y)$ języka L mamy aksjomat postaci:

$$\begin{aligned}&\forall x \ldots\ \forall x_n\ [(\varphi(x_1, \ldots, x_n, 0) \wedge \\ &\forall y\ (\varphi(x_1, \ldots, x_n, y) \Rightarrow (\varphi(x_1, \ldots, x_n, y + 1)))) \Rightarrow \forall y\ (\varphi(x_1, \ldots, x_n, y)].\end{aligned}$$

Pytanie: ile mamy aksjomatów w arytmetyce Peano?

Uwaga, ważne: schemat aksjomatów indukcji nie jest pojedynczym aksjomatem. Dla każdej formuły mamy osobny aksjomat! Dlatego też mówimy o schemacie aksjomatów indukcji, a nie o aksjomacie indukcji.

Uwaga: Istotne jest, że zbiór aksjomatów w arytmetyce Peano jest nie tylko przeliczalny, ale i rekurencyjnie przeliczalny, czyli "prosty"w sensie obliczalności (pojęcie rekurencyjnej przeliczalności poznamy przy okazji omawiania maszyn Turinga).

Na gruncie aksjomatyki Peano (i silniejszych systemach) da się zdefiniować zdanie mówiące o tym, że zbiór zdań Σ jest niesprzeczny, oznaczamy je przez $Con(\Sigma)$. Dokładniej, w aksjomatyce Peano da się ponumerować dowody (a jest ich przeliczalna liczba) oraz zdania i wyrazić formalnie zdania „A jest dowodem zdania B” oraz „istnieje dowód A zdania B”. W szczególności można wyrazić formalnie zdanie „istnieje dowód A zdania „$0 = 1$””. To zdanie nazywamy właśnie $Con(\Sigma)$.

5.2. Twierdzenie Goodsteina

Arytmetyka Peana jest w pewnym sensie „dziurawa” w tym sensie, że istnieją twierdzenia w teorii mnogości, które można wyrazić w języku arytmetyki Peana, ale nie można ich udowodnić za pomocą aksjomatów Peana. Pierwszym przykładem takiego twierdzenia jest twierdzenie udowodnione przez Goodsteina w 1944 roku. Opiszemy poniżej jego treść wraz z przykładem:

Wybieramy pewną liczbę naturalną k. Zapisujemy k używając tylko dodawania i naturalnych potęg liczby 2. Dla przykładu zacznijmy od liczby 11, która będzie pierwszym wyrazem G_0 pewnego ciągu:

$$G_0 = 11 = 2^{2+2^0} + 2^1 + 2^0.$$

Następnie zmieniamy wszędzie wystąpienia liczby 2 na 3 i odejmujemy od otrzymanej liczby 1, a następnie zapisujemy nowo otrzymaną liczbę w sposób podobny jak wcześniej, ale używając tylko potęg liczby 3, otrzymując kolejny wyraz G_1 ciągu.

$$G_1 = 3^{3+3^0} + 3^1 + 3^0 - 1 = 3^{3+3^0} + 3^1 = 1027.$$

Powtarzamy powyższą procedurę aż nie dostaniemy liczby 0.

Twierdzenie 5.2 (Goodsteina 1944)**.** *Dla każdej liczby naturalnej powyżej opisany ciąg osiąga liczbę* 0. ■

Paris i Kirby w 1982 roku udowodnili, że powyższego twierdzenia nie da się dowieść na gruncie arytmetyki Peana, mimo iż jest „intuicyjnie prawdziwe”. Dlatego nawet, gdy zajmujemy się tylko liczbami naturalnymi potrzebna będzie silniejsza aksjomatyka.

5.3. Logiki wyższych rzędów

Dotychczas mieliśmy do czynienia z logiką pierwszego rzędu (rachunkiem predykatów). Istnieją jednak inne „logiki". Najważniejszym z rozszerzeń logiki pierwszego rzędu jest logika drugiego rzędu. W logice pierwszego rzędu mogliśmy kwantyfikować po zmiennych, ale nie mogliśmy kwantyfikować po zbiorach, ani po formułach logicznych. W logice drugiego rzędu mamy dwa rodzaje zmiennych oraz stałych: x - element oraz X - zbiór. Mamy też dodatkowy symbol $\in$. Zmiennych i stałych obu typów nie można ze sobą mieszać tj. termowi odpowiada albo element, albo zbiór. Wprowadza się też dodatkowe aksjomaty logiczne (których nie będziemy podawać). Logika drugiego rzędu pozwala nam wyrazić w postaci zdań to, co było nieosiągalne w logice pierwszego rzędu. Dla przykładu, aby otrzymać z arytmetyki Peano pierwszego rzędu silniejszą arytmetykę Peano drugiego rzędu należy zastąpić schemat aksjomatów indukcji przez pojedynczy aksjomat indukcji:

$$\forall A \ (0 \in A \wedge (x \in A \Rightarrow (x+1) \in A) \Rightarrow \forall y \ y \in A).$$

Łatwo sprawdzić, że powyższy aksjomat indukcji implikuje schemat aksjomatów indukcji pierwszego rzędu. Zwróćmy uwagę, że arytmetyka Peano drugiego rzędu będąca rozszerzeniem arytmetyki Peano pierwszego rzędu ma skończenie wiele aksjomatów. Pokazuje to większą moc ekspresywną logiki drugiego rzędu.

Poza logiką drugiego rzędu istnieją jeszcze logiki wyższych rzędów. W logice trzeciego rzędu możemy mówić o zbiorach zbiorów, w logice czwartego rzędu o zbiorach zbiorów zbiorów, itd.

6. Aksjomatyczna teoria mnogości

Współczesna matematyka opiera się na logice i teorii mnogości. W pierwszym semestrze uczyli się Państwo o tzw. naiwnej teorii mnogości. Jest to teoria zbiorów bez formalnie zdefiniowanych aksjomatów. Potrzebę aksjomatyzacji teorii mnogości dobrze wyjaśnia sformułowany w 1901 roku paradoks Russela. Jest on znany w następującej opisowej formie (paradoksu golibrody) pochodzącej z książki „Pi razy drzwi" autorstwa Barrowa:

„Cyrulik sewilski goli w Sewilli wszystkich tych i tylko tych, którzy nie golą się sami. Czy cyrulik goli się sam?".

Jeśli cyrulik goli sam siebie, to nie może sam się golić. Jeśli cyrulik nie goli siebie, to musi sam się golić. Dochodzimy więc do sprzeczności. W języku teorii mnogości paradoks Russela przyjmuje następującą formę $X = \{x : x \notin X\}$. Analogicznie jak wcześniej, jeśli x należy do X, to X nie należy do X, a jeśli X nie należy do X, to X należy do X.

Naiwna teoria mnogości prowadzi więc do sprzeczności. Potrzebujemy zatem bardziej restrykcyjnej wersji teorii mnogości, która z jednej strony będzie pozwalała na możliwie „najbogatszą" matematykę, a z drugiej strony pozwoli uniknąć sprzeczności jak tej z paradoksu Russela.

W tym rozdziale poznamy współczesną wersję teorii mnogości, która opiera się na aksjomatach Zermela-Fraenkla-Skolema (ZFC). Pierwotna wersja aksjomatów Zermela powstała jako zbiór aksjomatów, które zostały przez niego użyte w dowodzie twierdzenia o tym, że każdy zbiór da się dobrze uporządkować. Aksjomatyka ta została następnie zmodyfikowana między innymi przez Skolema, Fraenkla i von Neumanna. Aksjomatykę ZFC możemy wyrazić w logice pierwszego rzędu. Zgodnie z tym w ZFC istnieją obiekty tylko jednego typu (zbiory). Każdy więc obiekt, który się pojawia jest zbiorem. Nie rozróżniamy więc między zbiorami, a elementami. Do języka aksjomatyki ZFC należy tylko jeden symbol $\in$, który odpowiada dwuargumentowej relacji należenia. Aksjomatyka ZFC opiera się na następujących aksjomatach:

I Aksjomat ekstensjonalności,
II Aksjomat pary,
III Aksjomat sumy,
IV Aksjomat zbioru potęgowego,
V Aksjomat nieskończoności,
VI Aksjomat regularności,
VII Schemat aksjomatów rozdzielania,
VIII Schemat aksjomatów zastępowania,
IX Aksjomat wyboru (AC).

Omówimy teraz pokrótce każdy z nich.

I Aksjomat ekstensjonalności mówi o tym, że dwa zbiory są sobie równe wtedy i tylko wtedy, gdy mają dokładnie te same elementy. Oznacza to, że każdy zbiór jest w sposób jednoznaczny wyznaczony przez wszystkie zawierające go elementy. Z aksjomatu ekstensjonalności wynika w szczególności, że dla dowolnych zbiorów A, B, jeśli $A \subseteq B$ oraz $B \subseteq A$, to $A = B$, gdzie $X \subseteq Y$ oznacza, że każdy element zbioru X jest elementem zbioru Y. Symbol $\subseteq$ służy więc tylko do krótszego zapisu i nie potrzebujemy go dodawać do języka teorii mnogości. Z aksjomatu ekstensjonalności wynika także, że istnieje co najwyżej jeden zbiór pusty. To, że co najmniej jeden zbiór pusty istnieje będzie wynikać z innych aksjomatów.

Ekstensjonalność jest przeciwieństwem intencjonalności. W systemie intencjonalnym dwa zbiory o tych samych elementach mogłyby się od siebie różnić, jeśli byłyby inaczej zdefiniowane. Dla przykładu zbiór liczb naturalnych oraz zbiór tych liczb całkowitych, które są większe lub równe od zera, mogłyby być, chociaż nie musiałyby być, innymi zbiorami, ponieważ są inaczej zdefiniowane (inna była intencja).

Aksjomat ekstensjonalności może wydawać się aksjomatem zubożającym teorię, ponieważ nie dopuszczamy istnienia nieekstensjonalnych zbiorów. Nie jest to jednak istotne ograniczenie z punktu widzenia matematyki. Dotyczy to zarówno teorii mnogości, jak i pozostałych działów matematyki. W teoriach ekstensjonalnych nie możemy wprawdzie uzyskać dwóch zbiorów o dokładnie tych samych elementach, ale możemy stworzyć „kopię” dowolnego niepustego (ważne!) zbioru, która będzie miała analogiczne pożądane przez nas własności (np. algebraiczne, teoriografowe czy porządkowe). Dla przykładu możemy skonstruować tyle kopii grafu K_1, ile byśmy chcieli.

Dodajmy jeszcze, że aksjomat ekstensjonalności jest niezależny od pozostałych aksjomatów ZFC.

II Aksjomat pary mówi o tym, że jeśli mamy dwa zbiory x i y, to istnieje zbiór

Z, którego elementami są dokładnie x i y. Zbiór Z nazywamy parą (nieuporządkowaną) i oznaczamy go przez $\{x, y\}$. Zwróćmy uwagę, że w aksjomacie pary nie zakładamy, że zbiory x i y są od siebie różne. Również w definicji pary nie ma takiego założenia. Oznacza to, że zbiór Z, którego jedynymi elementami są zbiory x oraz x, czyli $Z = \{x, x\}$ również jest parą, chociaż ma tylko jeden element! Zbiór $Z = \{x, x\}$ oznaczamy przez $Z = \{x\}$ i nazywamy go singletonem zbioru x. Aksjomat pary pozwala nam także na zdefiniowanie pary uporządkowanej. Niech a oraz b będą dowolnymi zbiorami. Wówczas zbiór $\{a, \{a, b\}\}$ nazywamy parą uporządkowaną o elementach a i b i oznaczamy ją przez (a, b). Powyższa definicja pochodzi od Kuratowskiego. Czasami używane są także inne definicje pary uporządkowanej, z których najważniejszą jest para w sensie Morse'a-Kelleya szczególnie przydatna, gdy mamy do czynienia z teorią klas (ogólniejszą niż teoria zbiorów). Najważniejsze własności, które powinna spełniać para uporządkowane są następujące. Po pierwsze para uporządkowana powinna być możliwa do utworzenia dla dowolnych i niekoniecznie różnych elementów a i b. Po drugie musi zachodzić własność: dla każdych a, b, c, d mamy $(a, b) = (c, d)$ wtedy i tylko wtedy, gdy $a = c$ oraz $b = d$.

Jak najprościej zdefiniować k-krotki uporządkowane?

III Aksjomat sumy mówi o tym, że dla dowolnej rodziny $\mathcal{A}$ istnieje zbiór Y, którego elementami są dokładnie te zbiory a, takie że $a \in A \in \mathcal{A}$ dla pewnego $A \in \mathcal{A}$. Innymi słowy zbiór Y składa się z tych zbiorów, które należą do pewnego zbioru z rodziny $\mathcal{A}$. Zbiór Y, którego istnienie zapewnia nam aksjomat, nazywamy sumą zbioru $\mathcal{A}$ i oznaczamy go przez $Y = \bigcup \mathcal{A}$.

IV Aksjomat zbioru potęgowego mówi o tym, że dla zbioru X istnieje zbiór $P(X)$, którego elementami są dokładnie wszystkie podzbiory X. Zbiór $P(X)$ nazywamy zbiorem potęgowym zbioru X. Zwróćmy uwagę, że sam aksjomat zbioru potęgowego nie mówi nam nic o postaci podzbiorów X, ani nawet o ich istnieniu. Do tego będą nam potrzebne inne aksjomaty.

V Aksjomat nieskończoności mówi o tym, że istnieje zbiór nieskończony. Aksjomat może być on wyrażony w różnej postaci. Zapewne najpopularniejszą formą tego aksjomatu jest postulowanie istnienia zbioru S, do którego należy zbiór pusty oraz jeśli x należy do zbioru S, to $x \ \cup \{x\}$ również należy do zbioru S. Zbiór S o tej własności nazywamy zbiorem induktywnym. Dla nas najwygodniej będzie przyjąć, że aksjomat nieskończoności postuluje istnienie zbioru liczb naturalnych, który formalnie zdefiniujemy w części poświęconej liczbom porządkowym.

VI Aksjomat regularności mówi o tym, że w każdym niepustym zbiorze X istnieje element minimalny ze względu na $\in$ (traktowanej jako relacja silnego częściowego porządku na zbiorze X. Dokładniej mówi on, że dla każdego niepustego zbioru X istnieje jego element z, taki że jeśli $u \in X$, to $u \notin z$. Jedną z konsekwencji aksjomatu regularności jest to, że dla każdego zbioru X mamy $X \notin X$.

W teorii, która zawiera aksjomat wyboru (o którym będzie mowa dalej) aksjomat regularności można sformułować w nieco bardziej intuicyjnej postaci: „Nie istnieje nieskończony ciąg $(x_0, \ldots)$, taki że $x_0 \ni x_1 \ni x_2 \ni \ldots$. Na ćwiczeniach poznamy dokładniej zastosowania aksjomatu regularności, jego wpływ na matematykę i to, dlaczego znalazł się wśród aksjomatów ZFC.

Aksjomat regularności jest niezależny od pozostałych aksjomatów ZFC.

VII Aksjomat rozdzielania, zwany także aksjomatem podzbiorów lub aksjomatem wycinania, dla formuły pierwszego rzędu φ mówi o tym, że dla każdego zbioru Y istnieje zbiór Z dokładnie tych elementów zbioru Y, które mają własność φ, czyli $Z = \{y \in Y : \varphi(z)\}$. Mówimy o schemacie aksjomatów rozdzielania dlatego, że w logice pierwszego rzędu nie możemy kwantyfikować po formułach logicznych, więc dla każdej formuły logicznej mamy osobny aksjomat rozdzielania.

W naiwnej teorii mnogości zbiory definiowane były jako ogół tych elementów, które spełniają jakąś formułę, czyli $Z = \{x : \varphi(x)\}$. Jest to tak zwany aksjomat nieograniczonego wycinania, który, jak pokazuje paradoks Russela, prowadzi do sprzeczności. Aksjomaty wycinania mają na celu uniknięcie paradoksu Russela przez ograniczenie się jedynie do elementów pewnego istniejącego zbioru a także ma nam zapewnić istnienie możliwie wielu „różnych" (w znaczeniu rozmaitych) zbiorów. W części drugiej skryptu postaramy się udzielić odpowiedzi na pytanie, czy zastąpienie aksjomatów nieograniczonego wycinania przez aksjomaty wycinania faktycznie pozwoliło nam na uniknięcie sprzeczności w aksjomatycznej teorii mnogości.

Zanim przedstawimy aksjomaty zastępowania podamy definicję formuły funkcyjnej. Mówimy, że formuła φ jest funkcyjna, jeśli dla każdego x istnieje dokładnie jeden y, taki że $\varphi(x, y)$.

VIII Aksjomat zastępowania dla formuły φ mówi o tym, że jeśli φ jest funkcyjna, to dla każdego A istnieje zbiór B, którego elementami są dokładnie te zbiory b, dla których istnieje $a \in A$, takie że $\varphi(a, b)$. Podobnie jak dla aksjomatów rozdzielania mamy osobny aksjomat dla każdej formuły. Innymi słowy schemat aksjomatów zastępowania mówi o tym, że jeśli funkcja jest zadana przez dziedzinę oraz formułę funkcyjną (np. przez wzór funkcji), to obraz tej funkcji jest zbiorem.

Selektorem rodziny $\mathcal{A}$ nazywamy zbiór S, taki że dla każdego $A \in \mathcal{A}$ istnieje dokładnie jeden $a \in A$, taki że $a \in S$. Selektor jest tym samym, co znany ze wstępu do matematyki dyskretnej system różnych reprezentantów. Używa się także nazwy transwersala. Funkcją wyboru f dla rodziny $\mathcal{A}$ nazywamy funkcję o dziedzinie $\mathcal{A}$, która każdemu zbiorowi należącemu do rodziny $\mathcal{A}$ przyporządkowuje jej element. Odnotujmy, że jeśli rodzina $\mathcal{A}$ jest rodziną zbiorów parami rozłącznych, to $\mathcal{A}$ ma funkcję wyboru wtedy i tylko wtedy, gdy istnieje selektor rodziny $\mathcal{A}$.

IX Aksjomat wyboru mówi, że dla każdej rodziny zbiorów parami rozłącznych istnieje jej selektor. Równoważnie mówi on, że każda rodzina ma funkcję wyboru. Zwróćmy uwagę, że w drugiej formie aksjomatu wyboru nie ma założenia o tym, że elementy rodziny są parami rozłączne. Jest ona więc „pozornie" silniejsza od pierwszej formy, ale tylko pozornie, bo obie wersje okazują się sobie równoważne. Aksjomat wyboru omówimy dokładniej w dalszej części skryptu oraz na ćwiczeniach.

Aksjomat wyboru jest niezależny od pozostałych aksjomatów ZFC. Teorię otrzymaną z ZFC poprzez usunięcie ze zbioru aksjomatów aksjomatu wyboru oznaczamy przez ZF. To, że dane twierdzenie jest równoważne aksjomatowi wyboru, należy rozumieć tak, że są one równoważne sobie na gruncie aksjomatyki ZF.

6.1. Zbiory dobrze uporządkowane

Przypomnimy najpierw podstawową terminologię dotyczącą zbiorów częściowo uporządkowanych.

Uwaga! Przyjmujemy tutaj konwencję, że częściowym porządkiem będziemy określać relację $<$ silnego porządku, a nie relację $\leqslant$ słabego porządku. Nieco później wyjaśnimy, dlaczego tak będzie nam wygodniej.

definicja 6.1. *Niech R będzie relacją dwuargumentową określoną na zbiorze X. Wówczas:*

I *Jeśli dla każdego elementu $x \in X$ zachodzi xRx, to mówimy, że relacja R jest zwrotna.*

II *Jeśli dla każdego elementu $x \in X$ zachodzi $\neg xRx$, to mówimy, że relacja R jest przeciwzwrotna.*

III *Jeśli dla każdych elementów $x, y \in X$ zachodzi $xRy \Rightarrow yRx$, to mówimy, że relacja R jest symetryczna.*

IV *Jeśli dla każdych elementów $x, y \in X$ zachodzi $xRy \Rightarrow \neg yRx$, to mówimy, że relacja R jest antysymetryczna.*

V *Jeśli dla każdych elementów $x, y, z \in X$ zachodzi $xRy \wedge rRz \Rightarrow \neg xRZ$, to mówimy, że relacja R jest przechodnia.*

definicja 6.2. *Niech $<$ będzie relacją dwuargumentową określoną na zbiorze X. Jeśli $<$ jest przechodnia, antysymetryczna i przeciwzwrotna, to $<$ nazywamy częściowym porządkiem na X. Wówczas parę uporządkowaną $(X, <)$ nazywamy zbiorem częściowo uporządkowanym. Ponadto przez $\leqslant$ oznaczamy relację słabego częściowego porządku na X skojarzonym z $<$. To znaczy $x \leqslant y \Leftrightarrow x < y \vee x = y$.*

definicja 6.3. *Jeśli w zbiorze częściowo uporządkowanym $(X, <)$ każde dwa elementy są ze sobą porównywalne, to $<$ nazywamy liniowym porządkiem na X, a $(X, <)$ nazywamy zbiorem liniowo uporządkowanym. Jeśli pewien podzbiór Y wraz*