Lista egzaminacyjna zadań z matematycznych podstaw informatyki, część 1.

Niektóre zadania są raczej zagadnieniami, na które należy zwrócić uwagę.

Funkcje pierwotnie rekurencyjne.

* Zapoznaj się z teorią funkcji pierwotnie rekurencyjnych. Ważne są definicje klasy funkcji pierwotnie rekurencyjnych, algorytmy, za pomocą których można obliczać wartości takich funkcji, operacje (sposoby definiowania) nie wyprowadzające poza klasę funkcji pierwotnie rekurencyjnych, zbiory (relacje) pierwotnie rekurencyjne, twierdzenia o zamkniętości klasy tych relacji, lemat o podstawianiu, funkcja β Gödla i kodowanie ciągów, zbiory rekurencyjnie przeliczalne, twierdzenia o zamkniętości klasy zbiorów rekurencyjnie przeliczalnych.

Zad. 1. Wykaż, że różne znane funkcje naturalne są rekurencyjne, a najczęściej także są pierwotnie rekurencyjnie. Mowa tu o funkcjach takich jak iloraz, reszta (z różnie sprecyzowanymi definicjami), silnia, potęga, część całkowita logarytmu itd.

Zad. 2. Udowodnij, że następujące funkcje są pierwotnie rekurencyjne:

1) $\max(m_1, \ldots, m_n) =$ największej liczbie spośród $m_1, \ldots, m_n$,

2) zwykła funkcja pary $f(n, m) = \dfrac{(n+m)(n+m+1)}{2} + n$,

3) $\langle x_1, \ldots, x_n \rangle = \mu y \left(\beta(y, 0) = n \wedge \bigwedge_{i<n} \beta(y, i+1) = x_i \right)$, gdzie β oznacza zwykła funkcję Gödla, przyporządkowująca liczbom $x_1, \ldots, x_n$ kod ciągu $(x_1, \ldots, x_n)$.

Zad. 3. Udowodnij, że jeżeli f jest funkcją pierwotnie rekurencyjną, to następujące funkcje są pierwotnie rekurencyjne:

1) $\max_f(n, \vec{x}) = \max\{f(0, \vec{x}), f(1, \vec{x}), \ldots, f(n-1, \vec{x})\}$,

2) $c(a, b) = \mu x \left(\beta(x, 0) = lh(a) + 1 \wedge \bigwedge_{i<lh(a)} (x)_i = (a)_i \wedge (x)_{lh(a)} = b \right)$,

3) $\langle f \rangle(n, \vec{x}) = \langle f(0, \vec{x}), f(1, \vec{x}), \ldots, f(n-1, \vec{x}) \rangle$

Zad. 4. Udowodnij, że funkcje takie, jak n-ta liczba pierwsza lub najmniejsza liczba pierwsza przynajmniej równa n są pierwotnie rekurencyjnie. Wskazówka: gdyby Euklides (autor klasycznego twierdzenia o liczbach pierwszych) znał rozwiązanie poprzednich, to umiałby rozwiązać także to zadanie.

Zad. 5. Udowodnij, że jeżeli f i g są funkcjami pierwotnie rekurencyjnymi, to pierwotnie rekurencyjna jest też całkowita funkcja h taka, że

$$h(x) = \mu y \ (f(x, y) = 0) \leqslant g(x)$$

dla wszystkich x. (Funkcja definiowana za pomocą pętli, o której z góry wiadomo, ile razy jest wykonywana, jest pierwotnie rekurencyjna.)

Zad. 6. (trudne) Udowodnij, że funkcje

$$f(n) = \text{część całkowita } e^n$$

oraz

$$g(0) = 2 \ \text{ oraz } \ g(n) = n\text{-ta cyfra rozwinięcia dziesiętnego liczby } e$$

(dla $n > 0$) są pierwotnie rekurencyjne. Przynajmniej pokaż ich rekurencyjność.

Zad. 7. Pokaż, że jeżeli funkcje g_0, g_1 oraz h są pierwotnie rekurencyjne, to także funkcja f zdefiniowana równościami

$$f(\vec{x},0) = g_0(\vec{x}),\ f(\vec{x},1) = g_1(\vec{x}),\ f(\vec{x},n+2) = h(f(\vec{x},n), f(\vec{x},n+1), n, \vec{x})$$

jest pierwotnie rekurencyjna. W szczególności, pierwotnie rekurencyjna jest funkcja przyporządkowująca liczbie n wyraz F_n ciągu Fibonacciego.

Zad. 8. Pokaż, że jeżeli funkcje g_1, g_2, h_1 oraz h_2 są pierwotnie rekurencyjne, to także funkcje f_1 i f_2 zdefiniowana równościami

$$f_1(\vec{x},0) = g_1(\vec{x}),\ f_1(\vec{x},n+1) = h_1(f_1(\vec{x},n), f_2(\vec{x},n), n, \vec{x})$$

$$f_2(\vec{x},0) = g_2(\vec{x}),\ f_2(\vec{x},n+1) = h_2(f_1(\vec{x},n), f_2(\vec{x},n), n, \vec{x})$$

są pierwotnie rekurencyjne. Wywnioskuj stąd, że funkcje **div** i **mod** są pierwotnie rekurencyjne.

Definiowalność relacji.

* Ważne są pojęcie definiowalności, formuły i relacje klasy Σ_0 (dawniej Δ_0, uwaga na zmianę oznaczeń), także Σ_1 i Π_1, twierdzenie o postaci normalnej, interpretacja informatyczna tego twierdzenia, fragmenty rozumowania pozwalającego dowieść to twierdzenie, np. o możliwości zastąpienia w definicji dwóch kwantyfikatorów egzystencjalnych jednym, odpowiedniość między własnościami informatycznymi i sposobem definiowania, zależność między postacią definicji, a rekurencyjnością.

Zad. 9. Pokaż, że relacje definiowane formułami klasy Σ_0 są pierwotnie rekurencyjne.

Dowody i twierdzenia. Formalizacja logiki, przejście od języka naturalnego do sformalizowanego.

* Z logiki proszę dobrze zapoznać się z podstawowymi pojęciami logicznymi, jak term, formuła atomowa, formuła, podstawianie, term podstawialny, zdanie, dowód, twierdzenie, teoria, teoria niesprzeczna, teoria zupełna, i z systemem logicznym Shoenfielda (lub jakimś innym). Aby przećwiczyć te pojęcia, dobrze jest dowieść na przykład twierdzenie o dedukcji.

Zad. 10. Podaj formalne dowody w wybranym systemie logicznym formuł następujących postaci:

1) $((p \wedge q) \Rightarrow r) \Leftrightarrow (p \Rightarrow (q \Rightarrow r))$ (p, q, r to dowolne formuły, zmienne zdaniowe lub zeroargumentowe symbole relacyjne),
2) $p \Leftrightarrow \neg\neg p$,
3) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$,
4) $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$,
5) $p \vee \neg p$,
6) $(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r))$,
7) $\forall x(\varphi \Rightarrow \psi) \Rightarrow (\forall x\varphi \Rightarrow \forall x\psi)$,
8) $\forall x(\varphi \Rightarrow \psi) \Rightarrow (\exists x\varphi \Rightarrow \exists x\psi)$,
9) $\forall x(\varphi \Rightarrow \psi) \Leftrightarrow (\exists x\varphi \Rightarrow \psi)$ pod warunkiem, że x nie jest wolna w ψ,
10) $\exists x \forall y \varphi \Rightarrow \forall y \exists x \varphi$.

Zad. 11. Sprawdź, że każdy term, w którym występuje najwyżej zmienna x jest podstawialny w dowolnej formule za zmienną x.

Zad. 12. Podaj przykłady rozumowań świadczące o tym, że nieprzestrzeganie ograniczeń stosowania reguł dowodzenia prowadzi do błędów.

Zad. 13. Udowodnij, że w teorii T można dowieść formułę φ wtedy i tylko wtedy, gdy w teorii T można dowieść formułę $\forall x\varphi$. Udowodnij, że formuły $\forall x\varphi \Rightarrow \varphi$ są twierdzeniami (że $\vdash \forall x\varphi \Rightarrow \varphi$). Udowodnij, że niektóre z formuł postaci $\varphi \Rightarrow \forall x\varphi$ nie dają się dowieść.

Zad. 14. Udowodnij twierdzenie o dedukcji dla rachunku zdań: Formuła φ daje się wyprowadzić z aksjomatu ψ wtedy i tylko wtedy, gdy implikacja $\psi \Rightarrow \varphi$ jest prawem rachunku zdań.

Zad. 15. Przypuśćmy, że stała c nie występuje w formule φ, ani w aksjomatach teorii T. Jeżeli formuła $\varphi[x \leftarrow c]$ jest twierdzeniem teorii T, to w teorii T można dowieść także formuły $\forall x\varphi$ oraz φ. Co więcej, można to zrobić nie używając w tych dowodach stałej c (formuły te można dowieść w języku bez stałej c).

Zad. 16. Jeszcze raz twierdzenie o dedukcji: formuła φ jest twierdzeniem teorii T uzupełnionej o aksjomat ψ będący zdaniem wtedy i tylko wtedy, gdy $\psi \Rightarrow \varphi$ jest twierdzeniem teorii T. Podaj kontrprzykład świadczący o istotności założenia, że ψ jest zdaniem. Wskazówka do dowodu w trudniejszą stronę: jeżeli każdą formułę w dowodzie φ zastąpimy mechanicznie przez implikację $\psi \Rightarrow \ldots$ o poprzedniku ψ, to otrzymamy schemat dowodu implikacji $\psi \Rightarrow \varphi$.

Zad. 17. Udowodnij, że jeżeli φ jest zdaniem, które nie ma dowodu w teorii T, to teoria $T \cup \{\neg\varphi\}$ jest niesprzeczna.

Gödlizacja logiki, czyli „implementacja" pojęć logicznych za pomocą liczb naturalnych.

* Definicje, pierwotna rekurencyjność większości pojęć logicznych po gödlizacji, teorie aksjomatyzowalne, rekurencyjna przeliczalność pojęcia twierdzenia.

Arytmetyki i reprezentowalność

* Arytmetyki Q i Peano, reprezentowalność funkcji pierwotnie rekurencyjnych w teorii Q (i bogatszych), mocna reprezentowalność relacji pierwotnie rekurencyjnych w Q, reprezentowalność relacji mocno reprezentowalnych, teorie ω-niesprzeczne, reprezentowalność relacji rekurencyjnie przeliczalnych w teoriach ω-niesprzecznych.

Twierdzenie Gödla, oryginalne

*

Funkcje rekurencyjne.

* Zapoznaj się z teorią funkcji rekurencyjnych. Ważne są definicje klasy całkowitych funkcji rekurencyjnych i częściowych funkcji rekurencyjnych, intuicje związane z obliczalnością, operacje nie wyprowadzające poza klasę funkcji rekurencyjnych całkowitych i lub częściowych, zbiory (relacje) rekurencyjne, twierdzenia o zamkniętości klas tych relacji. Zależności między pojęciami z teorii funkcji rekurencyjnych, na przykład funkcja jest rekurencyjna wtedy i tylko wtedy, gdy jej wykres jest rekurencyjnie przeliczalny.

Zad. 18. Pokaż, że dla dowolnej funkcji rekurencyjnej f istnieje funkcja pierwotnie rekurencyjna g taka, że

$$f(\vec{x}) = (\mu y\ (g(\vec{x}, y) = 0))_0$$

dla wszystkich $\vec{x}$. Wskazówka: dowodziłbym to korzystając z twierdzenia o definiowalności. Jest to wersja twierdzenia o postaci normalnej. Można to zadanie zinterpretować w następujący sposób: każdy program wykonuje określone obliczenia na wyniku znalezionym w pętli while, jedynej w programie. Pozostałe obliczenia polegają na wykonywaniu pętli for, a więc pętli, o której z góry wiadomo, ile razy będzie wykonywana.

Zad. 19. Jakie funkcje są definiowane wzorami

$$f(x) = \mu y\ (y^2 \geqslant x),\ g(x) = \mu y\ (y^2 = x),\ h(x) = \mu y\ (y^2 \leqslant x)?$$

Opisz je. Czy są to funkcje pierwotnie rekurencyjne?

Zad. 20. Niech $f : N \to N$ będzie różnowartościową funkcją rekurencyjną. Udowodnij, że funkcja odwrotna f^{-1} też jest rekurencyjna.

Zad. 21. Pokaż, że

1) zbiór wartości funkcji rekurencyjnej jest rekurencyjnie przeliczalny,

2) niepusty zbiór rekurencyjnie przeliczalny $A \subseteq N$ jest zbiorem wartości całkowitej funkcji rekurencyjnej,

3) niepusty, rekurencyjnie przeliczalny zbiór $A \subseteq N^2$ jest postaci

$$\{\langle f(n), g(n)\rangle \in N^2 : n \in N\},$$

gdzie f i g są całkowitymi funkcjami rekurencyjnymi określonymi na zbiorze liczb naturalnych N.

Zad. 22. Udowodnij, że funkcja f jest rekurencyjna wtedy i tylko wtedy, gdy jej wykres

$$W_f = \{(\vec{x}, y) : f(\vec{x}) \text{ jest określona oraz } f(\vec{x}) = y\}$$

jest rekurencyjnie przeliczalny. Wskazówka: można skorzystać z twierdzeń o definiowalności.

Zad. 23. Klasa funkcji rekurencyjnych całkowitych zamknięta ze względu na definiowanie warunkowe.

Zad. 24. Załóżmy, że rekurencyjna funkcja $f : N \to N$ jest różnowartościowa. Czy funkcja f^{-1} jest rekurencyjna? Czy założenie całkowitości f coś zmienia?

Twierdzenie Gödla według Churcha

*

Rozstrzygalność i obliczalność, teza Churcha

* Zagadnienia: Teza Churcha i odpowiedniość między pojęciami z teorii funkcji rekurencyjnych i obliczalnością: funkcje obliczalne to częściowe funkcje rekurencyjne, zbiory rozstrzygalne to zbiory rekurencyjne, zbiory semirozstrzygalne (rozpoznawalne) to zbiory rekurencyjnie przeliczalne. Kodowanie pojęć logicznych za pomocą liczb naturalnych, własności kodowania, szkic dowodu twierdzenia Churcha o nierozstrzygalności arytmetyki i konsekwencje informatyczne tego twierdzenia. Trzy charakteryzacje obliczalności: rekurencyjność, definiowalność i reprezentowalność, zależności między tymi charakteryzacjami.

Zad. 25. Rozstrzygalność zbioru twierdzeń teorii w pewnym stopniu jest równoważna zupełności teorii. Rozważmy następujący algorytm: dane jest zdanie φ, pytamy się, czy φ jest twierdzeniem (pewnej ustalonej) teorii T?

1) var d : string; $d := \varepsilon$;

2) while true do begin

   (a) $d :=$ następny po d,

   (b) if d jest dowodem φ w T, then return 'φ jest twierdzeniem T',

   (c) if d jest dowodem $\sim \varphi$ w T, then return 'φ nie jest twierdzeniem T'.

3) end

W tym algorytmie $\sim \varphi$ oznacza $\neg\varphi$, jeżeli φ nie jest negacją, oraz ψ, jeżeli $\varphi = \neg\psi$ ($\sim \varphi$ to negacja φ, ale gdyby miała zaczynać się podwójną negacją, to bez tych dwóch negacji), a procedura badająca dowody nie może o żadnym napisie twierdzić, że jest jednocześnie dowodem zdania i jego negacji (np. zakłada, że udowodniona może zostać tylko ostatnia formuła dowodu)

Pokaż, że

1) Podany algorytm jest poprawny wtedy i tylko wtedy, gdy teoria T jest niesprzeczna.

2) Podany algorytm zatrzymuje się po uruchomieniu z dowolnym zdaniem wtedy i tylko wtedy, gdy teoria T jest zupełna.

Tak więc najprostszy algorytm szukania dowodu rozstrzyga zbiór twierdzeń T wtedy i tylko wtedy, gdy teoria T jest niesprzeczna i zupełna.

Pojęcie spełniania, twierdzenie o pełności.

* Proszę zapoznać się z pojęciem struktury, wartościowania, wartości termu, spełniania przy danym wartościowaniu, spełnianiu modelu, a także z twierdzeniem o pełności i może ze szkicem jego dowodu. Jakie jest znaczenie tego twierdzenia? Następne zadanie jest ćwiczeniem z definicji spełniania.

Pierwsza część zadania wyjaśnia sens operacji podstawiania.

Zad. 26. Niech x będzie ustaloną zmienną, a t – dowolnym termem. Dla danego wartościowania zmiennych h definiujemy wartościowanie h_t przyjmując, że $h_t(y) = h(y)$ dla wszystkich zmiennych $y \neq x$ oraz $h_t(x) = t[h]$. Udowodnij, że

1) $s[x \leftarrow t][h] = s[h_t]$ dla dowolnego termu s,

2) $\mathcal{A} \models \varphi[x \leftarrow t][h]$ wtedy i tylko wtedy, gdy $\mathcal{A} \models \varphi[h_t]$ dla dowolnej struktury $\mathcal{A}$, dowolnej formuły φ i dowolnego wartościowania zmiennych h.

Zad. 27. Udowodnij twierdzenie o poprawności: jeżeli φ jest twierdzeniem teorii T, to jest spełnione w każdym modelu teorii T. Pełny dowód może okazać się żmudny, ale można znaleźć plan dowodu i przeprowadzić niektóre rachunki.

Twierdzenie Herbranda

* Zapoznaj się ze sformułowaniem i szkicem dowodu twierdzenia Herbranda (także z algorytmem Herbranda).

Zad. 28. Przypomnij sobie pojęcie postaci normalnej formuły rachunku zdań, zwłaszcza postaci koniunkcyjnej. Scharakteryzuj formuły w koniunkcyjnej postaci normalnej będące tautologiami.

Zad. 29. Udowodnij twierdzenie o pełności dla rachunku zdań: dowolna formuła (rachunku zdań) jest tautologią wtedy i tylko wtedy, gdy jest prawem rachunku zdań.

Zad. 30. Zbadaj metodą Davisa - Putnama, czy koniunkcja następujących alternatyw jest sprzeczna.

1) $P \vee Q \vee R$

2) $P \vee \neg Q \vee \neg R$

3) $P \vee \neg W$

4) $\neg Q \vee \neg R \vee \neg W$

5) $\neg P \vee \neg Q \vee R$

6) $U \vee X$

7) $U \vee \neg X$

8) $Q \vee \neg U$

9) $\neg R \vee \neg U$

Zad. 31. Przypuśćmy, że formuła φ nie zawiera kwantyfikatorów i zdanie $\exists x \forall y \varphi$ jest tautologią. Podaj dowód tego zdania. Wskazówka. Trudno napisać dowód, ale można korzystając z twierdzenia Herbranda opisać metodę konstruowania dowodu. Taka metoda powinna składać się z dwóch części: z metody konstruowania dowodu tautologii rachunku zdań (na poziomie rachunku zdań) i rozumowania dotyczącego kwantyfikatorów. Pierwsza część powinna być znana z logiki, można też posłużyć się koniunkcyjną postacią, druga część nie jest trudna, zawiera dość oczywiste rozumowanie. Reszta rozumowania to pewien trick. Twierdzenie Herbranda w tym przypadku mówi, że pewna alternatywa postaci $\bigvee \varphi(t, f(t))$ (f to symbol skolemowski) jest tautologią w sensie rachunku zdań. W tej tautologii, dla poszczególnych t wszystkie wystąpienia termu $f(t)$ zastępujemy zmiennymi wyznaczonymi przez t, biorąc dla różnych t różne zmienne. Ta alternatywa po tej zamianie nadal będzie tautologią. Po zamianie dowodzimy tautologię, a następnie wyprowadzamy z niej wyjściową formułę. W ten sposób z twierdzenia Herbranda wyprowadzamy twierdzenie o pełności, a także otrzymujemy ogólną metodę konstruowania dowodów w rachunku kwantyfikatorów.

Zad. 32. Zmodyfikuj równoważność z poprzedniego zadania tak, aby była prawdziwa dla formuł φ, w których mogą dodatkowo występować stałe.

Zad. 33. Korzystając z algorytmu Herbranda pokaż, że formuła

$$\exists x \; \forall y \; R(x, y) \rightarrow \forall y \; \exists x \; R(x, y)$$

jest tautologią, natomiast formuła

$$\forall x \; \exists y \; R(x, y) \rightarrow \exists y \; \forall x \; R(x, y)$$

nie jest. Druga część zadania dzięki twierdzeniu Herbranda sprowadza się do problemu unifikacji.

Zad. 34. Niech Φ oznacza formułę

$$\exists x \exists y \forall z ((A(x, y) \Rightarrow A(y, z) \wedge A(z, z)) \wedge (A(x, y) \wedge B(x, y) \Rightarrow B(x, z) \wedge B(z, z)))$$

(jest to formuła wykorzystywana do testowania programu Gilmora). Udowodnij, że Φ jest tautologią (prawem logiki). Zrób to wprost oraz korzystając z algorytmu Herbranda.

Zad. 35. Rozważamy formuły bez stałych i symboli funkcyjnych, formuła φ nie zawiera ponadto kwantyfikatorów. Udowodnij, że zdanie $\exists x_1 \ \ldots \ \exists x_n \ \varphi$ jest tautologią wtedy i tylko wtedy, gdy formuła φ jest spełniona przy każdym (jedynym możliwym) wartościowaniu w każdej strukturze o jednoelementowym uniwersum. Jak sprawdzić warunek z prawej strony tej równoważności posługując się metodą zerojedynkową? Zbadaj, czy formuła

$$\exists x \ \exists y \ \exists z \ ((F(x,y) \Rightarrow F(y,z) \wedge F(z,z)) \wedge (F(x,y) \wedge G(x,y) \Rightarrow G(x,z) \wedge G(z,z)))$$

jest tautologią.

Zad. 36. Zmodyfikuj równoważność z poprzedniego zadania tak, aby była prawdziwa dla formuł φ, w których mogą dodatkowo występować stałe.

Zad. 37. Czy istnieje algorytm, który odpowiada na pytanie, czy zdanie

$$\forall x_1 \ \ldots \ \forall x_n \ \exists y_1 \ \ldots \ \exists y_m \ \varphi$$

jest tautologią? Także w tym zadaniu φ nie zawiera kwantyfikatorów.

Zad. 38. Przypuśćmy, że φ i ψ są zdaniami w preneksowej postaci normalnej, a ψ^1 oznacza formułę otrzymaną z ψ po wykonaniu jednego kroku skolemizacji (po usunięciu jednego kwantyfikatora egzystencjalnego). Zdania $\varphi_1, \ldots, \varphi_k$ są sprzeczne, wtedy i tylko wtedy, gdy nie ma modelu, w którym są spełnione.

Algorytm Herbranda jest oparty o lemat, który stwierdza, że zdanie ψ jest sprzeczne wtedy i tylko wtedy, gdy zdanie ψ^1 jest sprzeczne. Uogólnij ten lemat i pokaż, że zdania φ i ψ są sprzeczne wtedy i tylko wtedy, gdy zdania φ i ψ^1 są sprzeczne.

Zad. 39. Wywnioskuj z poprzedniego zadania i twierdzenia o pełności, że następujące warunki są równoważne:

1) zdania φ i ψ są sprzeczne,

2) zdania φ i ψ^* są sprzeczne,

3) zdania φ^* i ψ^* są sprzeczne,

4) $\vdash \varphi \Rightarrow \neg\psi$.

Zad. 40. Przypuśćmy, że w teorii T dowiedliśmy formułę $\exists y \ \varphi$, skorzystaliśmy z reguły opuszczania kwantyfikatora egzystencjalnego otrzymując formułę $\varphi[y \leftarrow f(\vec{x})]$, a następnie w teorii T uzupełnionej o aksjomat $\varphi[y \leftarrow f(\vec{x})]$ dowiedliśmy zdanie Ψ. Pokaż, że zdanie Ψ daje się dowieść w teorii T (i to bez korzystania z dodatkowych symboli).