Zaawansowana logika dla informatyków
Zbiór zadań 2023

Jerzy Marcinkowski, Jakub Michaliszyn
Uniwerystet Wrocławski

0 Zadania na dobry początek

Problem postawiony poniższym zadaniu jest wyabstrahowanym fragmentem rozumowania z pewnego zaawansowanego dowodu twierdzenia informatycznego. Samo zadanie nie jest trudne, ale żeby je zrozumieć, trzeba przebrnąć przez kilka mniej lub bardziej oczywistych definicji. Treść tego zadania nie jest napisana jednoznacznie – po stronie czytelnika leży dobranie niuansów tak, by treść miała sens.

Zadanie A1 (P). Funkcja częściowa to taka funkcja, która — oprócz normalnych wartości — może też zwracać specjalną wartość $\perp$; jeśli $f(x) = \perp$ to mówimy, że f jest *niezdefiniowana* dla x.

Powiemy, że funkcja częściowa $f\colon \mathbb{N} \to \mathbb{N}$ jest *kanibalką*, jeśli dla każdego $n \geq 1$ mamy $f(n) \neq \perp$ wtedy i tylko wtedy, gdy dla pewnego $k < n$ mamy $f(k) = n$. Funkcję częściową $f\colon \mathbb{N} \to \mathbb{N}$ nazwiemy *niemal monotoniczną*, jeśli istnieje co najwyżej jedna para liczb x, y takich, że $x \leq y$, f jest niezdefiniowana dla wszystkich liczb między x a y, f nie jest niezdefiniowana dla x i y oraz mamy $f(x) > f(y)$.

Udowodnij, że każda kanibalka jest niemal monotoniczna.

Tak naprawdę, duża część informatyki, zarówno praktycznej jak i teoretycznej, polega na tym, żeby dla problemu, który chce się rozwiązać, znaleźć właściwą abstrakcję, rozwiązać wyabstrahowany problem (lub odnaleźć istniejące rozwiązanie), a następnie to wyabstrahowane rozwiązanie przetłumaczyć na prawdziwe rozwiązanie.

A to ładne zadanie jest oczywiste i nieintuicyjne jednocześnie.

Zadanie A2 (P). Rozważmy algorytm kompresji bezstratnej. Udowodnij, że jeśli istnieje plik, który po skompresowaniu tym algorytmem ma mniejszy rozmiar, to istnieje też plik, który po skompresowaniu ma większy rozmiar.

Pozostałe zadania w tym rozdziale wymagają przede wszystkim pomysłu.

Zadanie A3 (P). W barze *Niezmiennik* stali bywalcy oddają się dziwnej zabawie. Barman ustawia na stole długi rząd kieliszków i napełnia niektóre z nich. Po czym uczestnik zabawy na którego akurat wypada kolej podchodzi do stołu, znajduje na nim jakiś pełny kieliszek, wypija jego zawartość, po czym przesuwa się, kieliszek po kieliszku, w prawo, napełniając każdy napotkany pusty a opróżniając każdy napotkany pełny kieliszek. Posuwa się tak wzdłuż ciągu kieliszków aż mu się znudzi, a jeśli jest odporny na nudę to do kieliszka stojącego najdalej na prawo. Następnie oddala się, a do gry przystępuje kolejny uczestnik. Czy możemy być pewni że ta niezdrowa zabawa kiedyś się skończy?

Zadanie A4 (P). W pewnym mieście jest 2009 klubów. Każdy ma 45 członków. Każde dwa kluby mają dokładnie jednego wspólnego członka. Pokaż, że jest ktoś taki, kto należy do wszystkich klubów.

Zadanie A5 (P). Wierzchołki pięciokąta etykietujemy liczbami całkowitymi o sumie większej od zera. W każdym kolejnym ruchu pewnej jednoosobowej gry, jeśli x, y, z są etykietami kolejnych wierzchołków, i jeśli $y < 0$, to x, y, z możemy zastąpić przez, odpowiednio, $x+y$, $-y$, $y+z$. Czy dla każdego początkowego układu pięciu etykiet, opisana gra zatrzyma się po skończonej liczbie kroków?

Zadanie A6 (P). 199 elektorów Uniwersytetu Wrocławskiego siedzi przy okrągłym stole. Każdy z nich popiera, w wyborach rektora, Fizyka lub Historyka. Co pięć minut każdy z nich wygłasza głośno swoją opinię. Następnie elektor zmienia swoją opinię na przeciwną wtedy i tylko wtedy, gdy jego obaj sąsiedzi mają opinię mu przeciwną. Udowodnij, że po pewnym czasie zmiany opinii ustaną. *Autorem zadania jest János Pach.*

Zadanie A7 (P). Na pewnym statku jest n zwykłych pasażerów oraz jeden oszust, znany jako Impostor. Wiadomo, że wszyscy obecni znają Impostora, a on nie zna nikogo. Na statek przybył tajemniczy don Pedro, detektyw brytyjskiej policji. Jego zadaniem jest rozpoznać Impostora, Ale don Pedro, biedaczek, nie zna ani Impostora, ani nikogo innego na sali. Jedynym zaś pytaniem jakie potrafi zadać po polsku jest „czy znasz tę osobę” („tę osobę” wskazuje wtedy palcem).

a. Ile pytań musi (pesymistycznie) zadać don Pedro obecnym, żeby rozpoznać Impostora? To znaczy jaka jest liczba pytań, która, przy odpowiedniej strategii, na pewno okaże się wystarczająca? Pokaż też, że liczba o 1 mniejsza nie wystarczy.

b. Jaka jest minimalna optymistyczna liczba pytań, prowadząca do rozpoznania Impostora? To znaczy ile przynajmniej pytań musiałby zadać don Pedro aby rozpoznać Impostora, gdyby miał pewność, że odpowiedzi na te pytania będą zawsze takie, jak sobie życzy?

Zadanie A8 (P). Rozpatrzmy sieć społecznościową, w której użytkownicy mogą zawierać (symetryczne) znajomości. W pewnym momencie pojawia się silnie polaryzujący temat i każdy z użytkowników sieci ma w tym temacie opinię: jest albo ZA, albo PRZECIW. Użytkownik jest *stropiony*, jeśli przynajmniej połowa jego znajomych ma inną opinię niż on. Pokaż, że niezależnie od kształtu sieci mogło się tak zdarzyć, że wszyscy użytkownicy są stropieni.

1 Relacje równoważności

Przed rozwiązaniem tych zadań należy się zapoznać z definicjami z rozdziału 5 z Materiałów do zajęć, dostępnych w systemie SKOS.

Zadanie A9 (P). Załóżmy, że $R \subseteq A \times A$ jest słabo antysymetryczną relacją równoważności, a $S \subseteq A \times A$ jest relacją antyzwrotną. Pokaż, że wobec tego R i S nie zawierają ani jednego wspólnego elementu (czyli że $R \cap S = \emptyset$).

Zadanie A10 (P). Pokaż, że relacja R jest przechodnia wtedy i tylko wtedy, gdy $RR \subseteq R$.

Zadanie A11 (P). Niech A będzie zbiorem, a f — bijekcją przekształcającą zbiór A w A. Zdefiniujmy relację $R \subseteq A^2$ przyjmując, że

$$xRy \;\Leftrightarrow\; f(x) = y.$$

Symbolem R_∞ oznaczamy przechodnie domknięcie relacji R, czyli relację $\bigcup_{n=1}^{\infty} R^n$, gdzie $R^1 = R$ oraz $R^{n+1} = R^n R$. Czy R_∞ jest relacją równoważności? Czy R_∞ jest relacją równoważności, jeśli A jest zbiorem skończonym?

1.1 Zadania z indeksami

Zapoznaj się z definicją słów z Materiałów do zajęć (rozdział 9).

Niech Σ będzie skończonym zborem symboli („alfabetem”) i niech $L \subseteq \Sigma^*$. Relację $\sim_L \subseteq \Sigma^* \times \Sigma^*$ definiujemy w następujący sposób: $w \sim_L w'$ w.t.w gdy $\forall v \in \Sigma^*$ $(wv \in L \Leftrightarrow w'v \in L)$.

Podobnie możemy zdefiniować relację $\sim_L^{inf}$. Mianowicie $w \sim_L^{inf} v$ zachodzi wtedy i tylko wtedy gdy $\forall x, y \in \Sigma^*$ $(xwy \in L \Leftrightarrow xvy \in L)$.

Zadanie A12 (P). Pokaż, że $\sim_L$ i $\sim_L^{inf}$ są relacjami równoważności.

Niech i_L (od słowa *indeks*) będzie równe $|\Sigma^*/\sim_L|$ (czyli i_L to liczba klas abstrakcji na jakie $\sim_L$ dzieli Σ^*). Podobnie, niech $i_L^{inf} = |\Sigma^*/\sim_L^{inf}|$.

Zadanie A13 (P). Znajdź przykłady zbioru L dla których i_L jest równe 4, 17 i jest nieskończone.

Kolejne zadania dotyczą wzajemnych relacji między liczbami i_L i i_L^{inf}.

Udowodnij, że jeśli jedna z liczb i_L, i_L^{inf} jest skończona, to obie są skończone. Dokładniej mówiąc:

Zadanie A14 (P). Pokaż, że jeśli $|\Sigma| = 1$ to $i_L^{inf} = i_L$.

Zadanie A15 (P). Udowodnij, że $i_L \leq i_L^{inf}$;

Zadanie A16 (Z). Udowodnij, że $i_L^{inf} \leq (i_L)^{i_L}$.

Poniższe zadanie nie jest związane z wykładem, ale pokazuje, gdzie się przydają powyższe definicje.

Zadanie A17 (Z). Przez *problem decyzyjny* rozumiemy dowolną funkcję, dla której wejściem jest słowo nad pewnym alfabetem Σ, a wynikiem jest 1 albo 0. Podobnie jak utożsamiamy zbiory i ich funkcje charakterystyczne, tak możemy utożsamiać problemy decyzyjne i odpowiadające im języki (to znaczy zbiór słów, dla którego wynikiem jest 1).

Ustalmy jakiś „normalny” język programowania. Powiemy, że program P w tym języku *rozstrzyga* problem decyzyjny L, jeśli dla każdego wejścia $w \in \Sigma^*$ program P uruchomiony na w się zatrzymuje i zwraca 1 jeśli $w \in L$ oraz 0 w przeciwnym przypadku.

Udowodnij, że problem decyzyjny L można rozstrzygać w stałej pamięci komputera wtedy i tylko wtedy, gdy i_L jest skończone.

1.2 Definiowanie liczb

Zadanie A18 (P). Na wykładzie zdefiniowaliśmy liczby całkowite, a na nich dwie operacje: sumy i różnicy. Pokaż, że te definicje są poprawne. Czy da się (poprawnie) zdefiniować mnożenie?

Zadanie A19 (P). Pokaż, jak na zbiorze liczb wymiernych zdefiniowanych jak na wykładzie (poprawnie) zdefiniować dodawania, odejmowanie, mnożenie i relację „$\leq$”.

Zadanie A20 (P). Na zbiorze $\mathfrak{R}$ wszystkich ciągów rosnących, ograniczonych, o elementach wymiernych, definiujemy relację $\sim$: $\{a_n\}_{n\in\mathbb{N}} \sim \{b_n\}_{n\in\mathbb{N}} \iff \lim_{n\to\infty} |a_n - b_n| = 0$.

Pokaż, że $\sim$ jest relacją równoważności. Zdefiniuj na $\mathfrak{R}/\sim$ dodawanie, mnożenie i relację $\leq$ w naturalny sposób, jako relacje odziedziczone z $\mathbb{Q}$. Pokaż że definicje są poprawne. *Komentarz: Przy takiej definicji, mnożenie przez -1 jest nieco uciążliwe. ale da się zrobić.*

1.3 Relacje na programach

Ustalmy jakiś „normalny” język programowania oraz alfabet Σ. Niech $\mathcal{P}$ będzie zbiorem wszystkich programów *offline* w tym języku, to znaczy takich, które wczytują jakieś słowo nad alfabetem Σ, następnie coś liczą i albo się nigdy nie kończą, albo w końcu kończą działanie (być może zwracając wynik), przy czym to zachowanie zależy tylko od słowa wejściowego (tzn. program nie komunikuje się z internetem itd.).

Zadanie A21 (P). Zdefiniujmy relację $=_{eks} \subseteq \mathcal{P}^2$ taką, że dla dowolnych dwóch programów A, B zachodzi $A =_{eks} B$ wtedy i tylko wtedy, gdy dla każdego słowa w na alfabetem Σ, program A uruchomiony na w zatrzymuje się wtedy i tylko wtedy, gdy program B uruchomiony na słowie w się zatrzymuje. Czy $=_{eks}$ jest relacją równoważności?

Zadanie A22 (P). Zdefiniujmy relację $=_{roz} \subseteq \mathcal{P}^2$ taką, że dla dowolnych dwóch programów A, B zachodzi $A =_{roz} B$ wtedy i tylko wtedy, gdy dla każdego słowa w na alfabetem Σ, co najwyżej jeden z programów A, B się zatrzymuje na słowie w. Czy $=_{roz}$ jest relacją równoważności?

2 Logiki i ich moc wyrazu

2.1 Rachunek zdań

Zadanie A23 (P). Korzystając z podanej w *Materiałach do zajęć* zasady indukcji strukturalnej udowodnij, że dla każdej formuły logiki zdaniowej można skonstruować równoważną jej formułę logiki zdaniowej zbudowaną tylko ze spójników boolowskich $\vee$ oraz $\neg$.

Uwaga! Rozwiązanie powinno zaczynać się tak: Niech X będzie zbiorem (...) Korzystając z twierdzenia 23 udowodnimy, że X zawiera wszystkie formuły logiki zdaniowej.

Zadanie A24 (Z). Czy każda tautologia ma dowód w systemie dedukcji naturalnej dla rachunku zdań?

2.2 Rachunek kwantyfikatorów

Przeczytaj rozdział drugi ze skryptu *Logika dla informatyków* — Jerzy Tiuryn, Jerzy Tyszkiewicz, Paweł Urzyczyn: `http://www.mimuw.edu.pl/~urzy/calosc.pdf`.

Niech L będzie zbiorem wszystkich ludzi, jacy żyli na Ziemi od czasu Adama i Ewy. Wyobraźmy sobie, że dysponujemy relacjami M, T, oraz funkcją r, których sens jest następujący. Otóż dla pary dowolnych ludzi $\langle x, y\rangle$ napis $\langle x, y\rangle \in M$ będzie znaczył, że x jest matką y. Podobnie napis $\langle x, y\rangle \in T$ będzie znaczył, że x jest ojcem y. Wreszcie, dla człowieka x, napis $r(x)$ będzie oznaczał liczbę[1], będącą datą urodzenia x (zatem im mniejsze $r(x)$ tym wcześniej x się urodził).

Zadanie A25 (P). Rozszyfruj znaczenie następujących napisów:

a. $\{x \in L : \forall y \in L \;\; \neg\langle y, x\rangle \in M\}$. Jaka jest moc tego zbioru?

b. $|\{x \in L : \langle y, x\rangle \in T\}|$

c. $\max\{|\{y \in L : \langle y, x\rangle \in M\}| : x \in L\}$. Jaka jest wartość tej liczby?

d. $\min\{r(x) - r(y) : \langle y, x\rangle \in M\}$

Zapisz, podobnie jak powyżej następujące obiekty matematyczne.

a. Zbiór takich mężczyzn, którzy mieli dzieci z dokładnie jedną kobietą.

b. Zbiór takich x którzy są starsi od całego swojego rodzeństwa (w tym przyrodniego).

c. Zbiór tych mężczyzn, którzy mieli więcej dzieci, niż ich ojciec.

d. Zbiór takich x którzy urodzili się ze związku rodzeństwa (być może przyrodniego).

e. Zbiór takich x którzy mają rodzeństwo młodsze niż najstarsze z ich dzieci.

Zadanie A26 (P). Rozwiąż ćwiczenia 6, 8 i 9.

Zadanie A27 (P). Udowodnij fakt 1.7.

Definicje potrzebne do rozwiązania poniższego zadania są w rozdziale 4.2 *Materiałów do zajęć*.

Zadanie A28 (P). Dla danych liczb rzeczywistych x, y przez $N_x(y)$ oznaczamy zbiór $\{z : |z-y| \leq x\}$. Co to jest $\bigcup_{y\in\mathbb{Q}} \bigcap_{x\in\mathbb{Q}} N_x(y)$? Co to jest $\bigcap_{x\in\mathbb{Q}} \bigcup_{y\in\mathbb{Q}} N_x(y)$?

[1] Język który tu rozważamy wychodzi zatem nieco poza definicję języka pierwszego rzędu.

Zadanie A29 (P). O poniższych parach formuł wiesz, że w każdej parze jedna formuła jest prawdziwa. Przeczytaj je starannie, wyjaśnij w języku naturalnym ich znaczenie i dojdź do tego która jest która. Przez $\mathbb{N}_0$ rozumiemy tu zbiór liczb naturalnych wraz z zerem.

$\exists u \in \mathbb{N}_0\ \forall x \in \mathbb{N}_0\ \exists y, z, r, s \in \mathbb{N}_0\ \ x > u \Rightarrow x = y^2 + z^2 + r^2 + s^2$
$\exists u \in \mathbb{N}_0\ \forall x \in \mathbb{N}_0\ \exists y, z, r \in \mathbb{N}_0\ \ x > u \Rightarrow x = y^2 + z^2 + r^2$

$\forall x \in \mathbb{N}\ \ \exists y \in \mathbb{N}\ \ \forall r, s \in \mathbb{N}\ \ x^2 \leq y \wedge y < (x+1)^2 \wedge (rs \neq y \vee r = 1 \vee s = 1)$
$\forall x \in \mathbb{N}\ \ \exists y \in \mathbb{N}\ \ \forall r, s \in \mathbb{N}\ \ x \leq y \wedge y < 2x \wedge (rs \neq y \vee r = 1 \vee s = 1)$

Zadanie A30 (P). Sygnatura Σ, którą w tym zadaniu rozważamy, składa się z jednego binarnego symbolu relacyjnego $\leq$ i dwóch unarnych symboli relacyjnych P i R. Wszystkie struktury nad Σ jakie w tym zadaniu rozważamy są **skończonymi** liniowymi porządkami z relacją $\leq$. Taka struktura może być w naturalny sposób traktowana jako zakodowane (binarnie) dwie liczby naturalne p i r (myślimy że p ma jedynkę tam gdzie P jest prawdziwe, a zero tam gdzie P jest fałszywe; podobnie z r i R). Napisz zdanie logiki pierwszego rzędu nad sygnaturą Σ, które jest prawdziwe dokładnie w tych spośród rozważanych struktur w których $p = r + 1$.

Zadanie A31 (Z). *Wybierz dowolną liczbę naturalną n większą od 0. Tak długo jak długo n jest różne od 1 wykonuj następującą operację: Jeśli n jest parzyste, podziel je przez 2 i wynik podstaw za n. Jeśli jest nieparzyste, pomnóż je przez 3, iloczynu dodaj 1 i wynik podstaw za n.* Hipoteza Collatza mówi, że niezależnie od wyboru początkowego n wykonywanie powyższej pętli się kiedyś zakończy.

Napisz, w logice pierwszego rzędu, zdanie arytmetyki liczb naturalnych z funkcjami $+, \times, \uparrow$ (dodawanie mnożenie i potęgowanie) które jest prawdziwe w standardowym świecie liczb naturalnych wtedy i tylko wtedy gdy prawdziwa jest hipoteza Collatza. *Wskazówka. Będziesz musiał(a) jakoś zakodować ciąg liczb o nieznanej z góry długości. Skorzystaj z jednoznaczności przedstawienia liczby naturalnej jako iloczynu liczb pierwszych. Na przykład ciąg $\langle 3, 6, 2 \rangle$ możemy elegancko przedstawić jako $2^3 \times 3^6 \times 5^2$.*

Zadanie A32 (Z). Napisz, w logice pierwszego rzędu, zdanie arytmetyki liczb naturalnych z funkcjami $+, \times$ (dodawanie i mnożenie) które jest prawdziwe w standardowym świecie liczb naturalnych wtedy i tylko wtedy gdy prawdziwa jest hipoteza Collatza. *Wskazówka. Chińskie twierdzenie o resztach. Ciąg przedstawisz teraz jako parę liczb.*

Zadanie A33 (P). Rozważamy tu taką samą sygnaturę i takie same struktury jak w poprzednim zadaniu. Napisz zdanie logiki pierwszego rzędu nad sygnaturą Σ, które jest prawdziwe dokładnie w tych strukturach w których dla każdego elementu x zachodzi:

$$R(x) \Leftrightarrow |\{y : y \leq x \wedge P(y)\}| \text{ jest liczbą parzystą}$$

Wyjaśnij czemu powyższa formuła nie jest formułą logiki pierwszego rzędu.

Zadanie A34 (P). Napisz w języku geometrii na płaszczyźnie (zawierającym dwa symbole relacyjne Między(_,_,_) i Równe(_,_,_,_) zdanie mówiące że proste zawierające przeciwległe boki równoległoboku nigdy się nie przecinają. *Uwaga: ponieważ to zdanie jest prawdziwe, literalnie rzecz biorąc poprawnym rozwiązaniem tego zadania byłaby formuła $\forall x\ x = x$ (dlaczego?). Takie rozwiązanie pozostawi nas jednak z uczuciem pewnego niedosytu.*

Zadanie A35 (P). Udowodnij że dla każdej formuły logiki I rzędu Ψ istnieje formuła logiki I rzędu Φ, w postaci preneksowej, mająca te same zmienne wolne $x_1, \ldots x_l$ i równoważna Ψ, to znaczy taka, że dla każdej struktury $\mathbb{M}$ i każdej krotki $a_1, \ldots a_l$ elementów $\mathbb{M}$ zachodzi równoważność $\mathbb{M} \models \Phi(a_1, \ldots a_l)$ wtedy i tylko wtedy gdy $\mathbb{M} \models \Psi(a_1, \ldots a_l)$.

Zadanie A36 (Z). Rozważmy sygnaturę Σ składającą się z jednego binarnego symbolu relacyjnego E i dwóch stałych s (jak *source*) i t (jak *target*). Pokaż, że nie istnieje zdanie pierwszego rzędu Φ nad tą sygnaturą takie że dla dowolnej skończonej struktury $\mathbb{M}$ nad Σ zachodzi $\mathbb{M} \models \Phi$ wtedy i tylko wtedy gdy w $\mathbb{M}$ jest skierowana ścieżka z s do t.

2.3 Moc wyrazu logiki pierwszego rzędu

Zadanie A37 (Z). Udowodnij, że spójność grafu skierowanego nie da się wyrazić w logice pierwszego rzędu, tzn. że nie ma formuły logiki pierwszego rzędu prawdziwej dokładnie w tych grafach skierowanych, które są spójne.

Zadanie A38 (Z). Udowodnij, że spójność grafu nieskierowanego nie da się wyrazić w logice pierwszego rzędu, tzn. że nie ma formuły logiki pierwszego rzędu prawdziwej dokładnie w tych grafach nieskierowanych, które są spójne.

Zadanie A39 (Z). Czy spójność grafu można wyrazić w monadycznej logice drugiego rzędu (zob. rozdział 12.2 ze skryptu *Logika dla informatyków* — Jerzy Tiuryn, Jerzy Tyszkiewicz, Paweł Urzyczyn)?

Zadanie A40 (P, dość proste). Pokaż, że dla każdego $n \geq 1$ istnieje formuła logiki pierwszego rzędu z $n+1$ zmiennymi, która nie jest równoważna żadnej formule z n zmiennymi.

Zadanie A41 (P). Pokaż, że istnieje wielomianowy algorytm, który dla formuły logiki pierwszego rzędu w preneksowej postaci normalnej zwraca równoważną jej formułę w preneksowej postaci normalnej, która po ciągu kwantyfikatorów jest w postaci CNF (która jest zdefiniowana analogicznie do przypadku logiki zdaniowej).

Powiemy, że dwie formuły (być może ze zmiennymi wolnymi) φ, ψ są *równoważne*, jeśli dla każdej struktury $\mathfrak{A}$ oraz wartościowania v mamy $\mathfrak{A} \models \varphi[v]$ wtedy i tylko wtedy, gdy $\mathfrak{A} \models \psi[v]$. Powiemy (podobnie, ale jednak inaczej), że dwie formuły φ, ψ są *różnoważne*, jeśli dla każdej struktury $\mathfrak{A}$ oraz **różnowartościowego** wartościowania v mamy $\mathfrak{A} \models \varphi[v]$ wtedy i tylko wtedy, gdy $\mathfrak{A} \models \psi[v]$.

Zadanie A42 (P). Czy dwie formuły są równoważne wtedy i tylko wtedy, gdy są różnoważne?

Zadanie A43 (P). Czy dwie formuły bez równości są równoważne wtedy i tylko wtedy, gdy są różnoważne?

2.4 Zadania o rozmiarach formuł

Zadanie A44 (P). Niech $p_0, p_1, \ldots$ będą zmiennymi zdaniowymi a *Parity* będzie funkcją taką, że $Parity(0) = p_0$ oraz, dla każdego $n \in \mathbb{N}$, $Parity(n+1) = (Parity(n) \Leftrightarrow p_{n+1})$. Istnienie dokładnie jednej takiej funkcji wynika z Twierdzenia 176. Czy istnieje wielomian p taki, że

1. ...dla każdego n istnieje formuła ψ_n w CNF równoważna $Parity(n)$ taka, że $|\psi_n| \leq p(n)$?
2. ...dla każdego n istnieje formuła ψ_n w używająca wyłącznie spójników ze zbioru $\{\wedge, \vee, \neg\}$ równoważna $Parity(n)$ taka, że $|\psi_n| \leq p(n)$? *Dla uproszczenia możesz założyć w tym podpunkcie, że n jest potęgą dwójki.*

Zadanie A45 (P). Niech $A = \{\wedge, \Rightarrow\}$ oraz $B = A \cup \{\Leftrightarrow\}$. Czy istnieje taki wielomian p, że dla każdej formuły φ używającej spójników za zbioru B (i zmiennych zdaniowych) istnieje równoważna formuła ψ używająca spójników ze zbioru A (i zmiennych zdaniowych) taka, że $|\psi| \leq p(|\varphi|)$?

Zadanie A46 (Z). Niech $A = \{\vee, \wedge, \neg, \Rightarrow\}$ oraz $B = A \cup \{\Leftrightarrow\}$. Czy istnieje taki wielomian p, że dla każdej formuły φ używającej spójników za zbioru B (i zmiennych zdaniowych) istnieje równoważna formuła ψ używająca spójników ze zbioru A (i zmiennych zdaniowych) taka, że $|\psi| \leq p(|\varphi|)$?

2.5 Arytmetyka Peano

Przyjmijmy następujące aksjomaty Peano:

A1	$\forall x, y, z.(x + y) + z = x + (y + z)$	A2	$\forall x, y.x + y = y + x$
A3	$\forall x.x + 0 = x$	A4	$\forall x, y, z.(x \cdot y) \cdot z = x \cdot (y \cdot z)$
A5	$\forall x, y.x \cdot y = y \cdot x$	A6	$\forall x, y, z.x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
A7	$\forall x.x \cdot 0 = 0$	A8	$\forall x.x \cdot 1 = x$
A9	$\forall x, y, z.x < y \wedge y < z \Rightarrow x < z$	A10	$\forall x.\neg(x < x)$
A11	$\forall x, y.x < y \vee x = y \vee y < x$	A12	$\forall x, y, z.x < y \Rightarrow x + z < y + z$
A13	$\forall x, y, z.0 < z \wedge x < y \Rightarrow x \cdot z < y \cdot z$	A14	$\forall x, y.x < y \Rightarrow \exists z\ (x + z = y)$
A15	$0 < 1 \wedge \forall x.x > 0 \Rightarrow x \geq 1$	A16	$\forall x.x \geq 0$

Zadanie A47 (P). Skonstruuj strukturę nad sygnaturą zawierającą symbol stałej 0, symbole funkcyjne S, $+$ i $*$ oraz symbol relacyjny $\leq$, która **nie jest** standardowym światem liczb naturalnych (i żadnego oszukiwania – nie może być *izomorficzna* z $\mathbb{N}$) i w której prawdziwe są wszystkie aksjomaty arytmetyki Peano dotyczące porządku i dodawania.

Zadanie A48 (Z). Skonstruuj strukturę nad sygnaturą zawierającą symbol stałej 0, symbole funkcyjne S, $+$ i $*$ oraz symbol relacyjny $\leq$, która **nie jest** standardowym światem liczb naturalnych (i żadnego oszukiwania – nie może być *izomorficzna* z $\mathbb{N}$) i w której prawdziwe są wszystkie aksjomaty arytmetyki Peano dotyczące porządku, dodawania i mnożenia.

2.6 Definiowalność funkcji

(n, k)-kratą nazywamy strukturę składającą się ze zbioru $\{a_{i,j} \mid i, j \in \mathbb{N} \wedge i < n \wedge j < k\}$ oraz dwóch relacji binarnych H, V[2] takich, że

- $a_{i,j} H a_{i',j'}$ w.t.w., gdy $j = j'$ oraz $i' = i + 1$,
- $a_{i,j} V a_{i',j'}$ w.t.w., gdy $i = i'$ oraz $j < j'$.

Formuła Φ, która może używać symboli relacyjnych H i V oraz dodatkowo z unarnego predykatu P, *definiuje* funkcję $f : \mathbb{N} \to \mathbb{N}$ wtedy i tylko wtedy, gdy dla każdych n, k następujące warunki są równoważne:

- dla (n, k)-kraty K istnieje taka interpretacja predykatu P, że krata K z tą interpretacją P jest modelem formuły Φ[3],
- $n = f(k)$.

$$\begin{tikzcd} a_{0,1} \arrow[r, "H"] & a_{1,1} \arrow[r, "H"] & a_{2,1} \\ a_{0,0} \arrow[r, "H"] \arrow[u, "V"] & a_{1,0} \arrow[r, "H"] \arrow[u, "V"] & a_{2,0} \arrow[u, "V"] \end{tikzcd}$$

Rysunek 1: Przykładowa $(3, 2)$-krata.

Przykład. Rozważmy formułę $\Phi = \forall x\, \neg\exists y\, xHy$. Modelami tej formuły są wszystkie $(1, k)$-kraty (w tym przypadku niezależnie od interpretacji predykatu P), zatem formuła ta definiuje funkcję stale równą 1.

Zadanie A49 (P). Czy istnieje formuła logiki pierwszego rzędu definiująca funkcję $f(x) = 2x$?

Zadanie A50 (P). Czy istnieje formuła logiki pierwszego rzędu definiująca funkcję $f(x) = x^2$?

Zadanie A51 (Z). Czy istnieje formuła logiki pierwszego rzędu definiująca funkcję $f(x) = 2^x$?

Zadanie A52 (Z). Czy istnieje formuła logiki pierwszego rzędu definiująca funkcję $f(x) = 2^{2^x}$?

[2] H jak Horizontal i V jak Vertical.

[3] W logice drugiego rzędu powiedzielibyśmy po prostu: formuła $\exists P.\Phi$ jest spełniona

2.7 Punkty stałe

Dla danej formuły logiki z punktami stałymi Φ oraz ciągu zmiennych $\vec{y}$, niech

$$F^{\Phi}_{\vec{y}}(R) = \{\vec{u} \in U^n \mid M \models \Phi(\vec{u}, \vec{y}, R)\}$$

Zadanie A53 (P). Udowodnij, że jeśli R występuje tylko pozytywnie[4] w formule Φ, to dla każdego możliwego ciągu zmiennych $\vec{y}$ funkcja $F^{\Phi}_{\vec{y}}$ jest monotoniczna.

Zadanie A54 (Z). Czy jeśli dla pewnej formuły Φ funkcja $F^{\Phi}_{\vec{y}}$ jest monotoniczna dla każdego możliwego ciągu zmiennych $\vec{y}$, to Φ jest równoważna pewnej formule, w której R występuje wyłącznie pozytywnie?

Zadanie A55 (P, 4 punkty). Rozwiąż wszystkie zadania z rozdziału 10.3 z *Materiałów do zajęć.*

Rozpatrzmy logikę I rzędu z dwiema zmiennymi bez równości. Wiadomo, że każdą formułę w tej logice można sprowadzić do równospełnialnej formuły w postaci normalnej Scotta, tzn. postaci

$$\forall x \forall y \psi \wedge \bigwedge_{i=1}^{k} \forall x \exists y \varphi_i$$

gdzie ψ oraz φ_i nie zawierają kwantyfikatorów. Rozpatrzmy następujący algorytm sprawdzający, czy taka formuła ma model. Algorytm przyjmuje jako U koniunkt $\forall x \forall y \psi$, a jako E koniunkt $\bigwedge_{i=1}^{k} \forall x \exists y \varphi_i$.

```
procedure GENERATE-MODEL(U, E)
    A := SINGLETON_SET(GUESS-1TYPE(U))
    if VIOLATED(A, U) then return false
    while NOT ALL-SATISFIED(A, E) do
        A := UNION(A, GUESS-WITNESSES(A, E, U))
        if VIOLATED(A, U) then return false
    return true
```

Zauważ, że ten algorytm oblicza pewien punkt stały.

Zadanie A56 (P). Uzupełnij powyższy algorytm tak, aby każde wywołanie algorytmu trwało najwyżej wykładniczo dużo czasu względem rozmiaru wejścia, oraz:

- Jeśli formuła U $\wedge$ E ma model, to żeby istniały zgadnięcia, po których algorytm zwróci true.
- Jeśli formuła U $\wedge$ E nie ma modelu, to żeby dla każdych zgadnięć algorytm zwracał false.

Zadanie A57 (Z). Co trzeba zmienić w powyższym algorytmie, żeby obsługiwać również równość?

(n, k)-kratk**ą** nazywamy strukturę składającą się ze zbioru $A = \{a_{i,j} \mid i, j \in \mathbb{N} \wedge i \ < n \wedge j < k\}$ oraz dwóch relacji binarnych H, V takich, że $a_{i,j} H a_{i',j'}$ w.t.w., gdy $j = j'$ oraz $i' = i + 1$, a także $a_{i,j} V a_{i',j'}$ w.t.w., gdy $i = i'$ oraz $j < j'$.

Powiemy, że formuła logiki z punktami stałymi Φ, która może używać tylko symboli relacyjnych H i V, *stałopunktowo definiuje* funkcję $f : \mathbb{N} \to \mathbb{N}$ wtedy i tylko wtedy, gdy (n, k)-kratka jest modelem formuły Φ wtedy i tylko wtedy, gdy $n = f(k)$.

Zadanie A58 (P). Czy istnieje formuła logiki pierwszego rzędu stałopunktowo definiująca funkcję $f(n) = 2n$?

Zadanie A59 (Z). Czy istnieje formuła logiki pierwszego rzędu stałopunktowo definiująca funkcję $f(n) = n^3 + 2n^2 - 2n$?

Zadanie A60 (Z). Czy istnieje formuła logiki pierwszego rzędu stałopunktowo definiująca funkcję $f(n) = 2^{2^n}$?

[4] tzn. pod parzystą liczbą negacji zakładając, że jedynymi spójnikami w formule są $\neg, \wedge$ i $\vee$

2.8 Rezolucja

Zadanie A61 (Z). Udowodnij, że jeśli zbiór $\mathcal{F}$ jest sprzeczny, to istnieje rezolucyjny dowód sprzeczności $\mathcal{F}$, tzn. twierdzenie o zupełności rezolucji (completeness).

Zadanie A62 (P). Udowodnij, że jeśli zbiór $\mathcal{F}$ nie jest sprzeczny, to nie istnieje rezolucyjny dowód sprzeczności $\mathcal{F}$.

Zadanie A63 (P). Udowodnij, że metoda rezolucji nie jest zupełna w następującym sensie: istnieją zbiór klauzul X oraz klauzula ψ takie, że ψ jest logiczną konsekwencją zbioru X, ale ψ nie można wyprowadzić z X metodą rezolucji.

Zadanie A64 (Z). Jakie reguły wnioskowania wystarczy dodać do metody rezolucji, aby stała się ona zupełna, pozostając niesprzeczną?

Zadanie A65 (Z, twierdzenie o zwartości). Udowodnij, że jeśli zbiór klauzul $\mathcal{F}$ jest przeliczalny oraz skończenie spełnialny (tzn. każdy skończony jego podzbiór jest spełnialny), to jest spełnialny. Następnie udowodnij, że założenie o przeliczalności nie jest potrzebne.

Zadanie A66 (P). Rozpatrzmy zbiory zawierające klauzule nieskończone. Czy dla takich zbiorów twierdzenie o zwartości jest prawdziwe?

Zadanie A67 (P). Pokaż, że istnieją przykłady sprzecznych zbiorów klauzul o n zmiennych, dla których rezolucyjny dowód sprzeczności wymaga wykładniczej liczby kroków w stosunku do n.

Czy takie przykłady będą istniały również wtedy, gdy zażądamy, aby:

Zadanie A68 (P). Każda początkowa klauzula miała co najwyżej dwa literały?

Zadanie A69 (P). Każda zmienna występowała w początkowym zbiorze klauzul najwyżej dwa razy?

3 Teoria mocy

Zadanie A70 (P). Niech A, B, C będą dowolnymi zbiorami. Napisz definicję dowolnej funkcji $f : (A^B)^C \to A^{B \times C}$.

Zadanie A71 (P). Inwolucją nazywamy odwzorowanie $f : A \to A$ takie, że ff jest identycznością na A. Czy każda inwolucja jest bijekcją na A? Pokaż, że każdą bijekcję można przedstawić jako złożenie dwóch inwolucji.

Zadanie A72 (P). Udowodnij że zbiór $\mathbb{R}$ ma moc taką samą, jak zbiór $\{0,1\}^{\mathbb{N}}$. W tym celu pokaż że:

a. $\mathbb{R} \sim (0,1) \sim [0,1) \sim [0,1]$

b. Istnieje funkcja różnowartościowa z $\{0,1\}^{\mathbb{N}}$ w któryś z odcinków z punktu **a**.

c. Istnieje funkcja różnowartościowa z któregoś z odcinków z punktu **a** w $\{0,1\}^{\mathbb{N}}$.
Należy pamiętać, że $2 = 1.(9)$.

Zadanie A73 (P). Przeczytaj i zrozum definicję termów z Materiałów do zajęć (rozdział 12). Następnie skonstruuj bijekcję pomiędzy liczbami naturalnymi a zbiorem termów $\mathcal{T} = (\{-\}, \{x_i \mid i \in \mathbb{N}\})$, gdzie $-$ jest 1-argumentowym symbolem funkcyjnym.

Zadanie A74 (Z). Przeczytaj i zrozum definicję termów z Materiałów do zajęć (rozdział 12). Następnie skonstruuj bijekcję pomiędzy liczbami naturalnymi a zbiorem termów $\mathcal{T} = (\{+\}, \{x\})$, gdzie $+$ jest 2-argumentowym symbolem funkcyjnym.

Zadanie A75 (P). Udowodnij, że następująca funkcja $f : \mathbb{N}^2 \to \mathbb{N}$ jest bijekcją:

$$f(n,m) = \frac{(n+m)(n+m+1)}{2} + m$$

Zadanie A76 (P). Ciąg cyfr dziesiętnych $a_1a_2\ldots$ nazwiemy w tym zadaniu *wymiernym*, jeśli istnieje taka liczba wymierna q, że ten ciąg stanowi jej część ułamkową, tzn. dla pewnej liczby całkowitej c mamy $q = c + \sum_{i=1}^{\infty} 10^{-i} \cdot a_i$. Ile jest ciągów wymiernych?

Zadanie A77 (P). Niech $f : \mathbb{R} \to \mathbb{R}$. Mówimy, że $x \in \mathbb{R}$ jest lokalnym maksimum funkcji f, jeżeli istnieje taka dodatnia liczba rzeczywista r, że dla każdego $y \in \mathbb{R}$ jest spełniony warunek

$$(x - r < y < x + r \wedge x \neq y) \Rightarrow f(x) > f(y)$$

Udowodnij, że dla każdej funkcji $f : \mathbb{R} \to \mathbb{R}$ zbiór jej lokalnych maksimów jest przeliczalny.

Zadanie A78 (P). Niech K będzie rodziną podzbiorów zbioru liczb naturalnych taką, że relacja zawierania na tej rodzinie jest porządkiem regularnym. Pokaż, że każdy łańcuch w tym porządku jest przeliczalny.

Zadanie A79 (P). Niech $\mathcal{C} = \{0,1\}^{\mathcal{A}}$, gdzie $\mathcal{A} = \{1,2,3,4,5,6,7,8,9,10\}$. Relację $\equiv_0$ określmy na $\mathcal{C}$ tak, że $f \equiv_0 g$ wtedy i tylko wtedy gdy:

$$\exists i \in \mathcal{A}\ \exists j \in \mathcal{A}\ \forall k \in \mathcal{A}\ \ f(i) = g(j) \wedge f(j) = g(i) \wedge (k \neq i \wedge k \neq j \Rightarrow f(k) = g(k))$$

Niech $\equiv$ będzie najmniejszą relacją równoważności zawierającą $\equiv_0$. Jaka jest moc zbioru $\mathcal{C}/\equiv$?

Zadanie A80 (Z). Jak zmieni się odpowiedź w poprzednim zadaniu, gdy założymy, że $\mathcal{A} = \mathbb{N}$?

Zadanie A81 (P). Powiemy, że zbiór X jest *efektywnie przeliczalny*, jeśli istnieje program (deterministyczny, bez efektów ubocznych), który wczytuje liczbę naturalną i wypisuje na wyjście jakiś element X, przy czym każdy element X jest wartością programu dla przynajmniej jednego argumentu. Udowodnij, że suma efektywnie przeliczalnej rodziny zbiorów efektywnie przeliczalnych jest efektywnie przeliczalna[5][6].

4 Porządki, izomorfizmy i homomorfizmy

4.1 Porządki

Przeczytaj w *Materiałach do zajęć* rozdział o porządkach.

Zadanie A82 (P). Czy porządek leksykograficzny na $\mathbb{R} \times \{0,1\}$ jest izomorficzny z $\langle \mathbb{R}, \leq \rangle$?

Zadanie A83 (P). Czy porządek leksykograficzny na $\{0,1\} \times \mathbb{R}$ jest izomorficzny z $\langle \mathbb{R}, \leq \rangle$? Czy porządek leksykograficzny na $\{0,1\} \times \mathbb{Q}$ jest izomorficzny z $\langle \mathbb{Q}, \leq \rangle$?

Zadanie A84 (P). Niech $\mathcal{P}$ będzie zbiorem wszystkich odcinków początkowych $\mathbb{Q}$, uporządkowanym relacją inkluzji. Opowiedz dokładnie przedstawiony szybko na wykładzie dowód twierdzenia, że $\langle \mathcal{P}, \subseteq \rangle$ jest **porządkiem zupełnym**, tzn. każdy niepusty ograniczony z góry podzbiór $\mathcal{P}$ ma kres górny.

Zadanie A85 (P). Niech $\langle X, \leq \rangle$ będzie liniowym porządkiem. Czy z tego że każdy niepusty ograniczony z góry podzbiór X ma w X kres górny wynika że każdy niepusty ograniczony z dołu podzbiór X ma w X kres dolny?

[5] Inaczej: wyobraźmy sobie, że mamy program, który dla zadanej liczby zwraca program, który dla każdej liczby coś zwraca. Pokaż, że można stworzyć jeden program, który zwraca (dla jakichś argumentów) wszystkie wartości wszystkich tamtych programów.

[6] Co ciekawe, to analogiczne twierdzenie dla przekroju nie zachodzi (z nietrywialnych powodów).

Zadanie A86 (P). Zbiór $A \subseteq X$ jest *gęsty* w linowym porządku $\langle X, \leq \rangle$ jeśli pomiędzy kazdymi dwoma elementami X istnieje element ze zbioru A. Pokaż że jeżeli $h : \langle \mathbb{R}, \leq \rangle \to \langle X, \leq \rangle$ jest izomorfizmem porządkowym to obraz $h(\mathbb{Q})$ zbioru liczb wymiernych jest gęsty w $\langle X, \leq \rangle$.

Zadanie A87 (Z). Czy porządek leksykograficzny na $\mathbb{R} \times \mathbb{R}$ jest izomorficzny z $\langle \mathbb{R}, \leq \rangle$? *Wskazówka:* Skorzystaj z Zadania 86.

Zadanie A88 (Z). Czy istnieje porządek $(P, \leq_P)$ który jest jednocześnie:

- gęsty, czyli między każdymi dwoma różnymi elementami istnieje trzeci, różny od nich,
- liniowy,
- bez końców,
- taki, że każda para elementów $x, y \in P$ ma w P ograniczenie górne
- nieizomorficzny z $\langle \mathbb{R}, \leq \rangle$?

Zadanie A89 (P). Ile jest możliwych relacji dobrego porządku na $\mathbb{N}$? A ile jest możliwych relacji na $\mathbb{N}$, które są jednocześnie porządkami oraz relacjami równoważności? Odpowiedzi uzasadnij.

Zadanie A90 (P). Pokaż, że zbiór liczb wymiernych ze zwykłym porządkiem i zbiór niepustych skończonych ciągów liczb wymiernych z porządkiem leksykograficznym są izomorficzne (rozważamy porządek leksykograficzny generowany przez zwykły porządek na liczbach wymiernych).

Przypominamy, że $\preceq$ jest porządkiem leksykograficznym generowanym przez porządek $\leq$, jeśli

$$\langle a_0, a_1, \ldots a_m \rangle \preceq \langle b_0, b_1, \ldots, b_n \rangle$$

wtedy i tylko wtedy, gdy $\langle a_0, a_1, \ldots a_m \rangle$ jest prefiksem $\langle b_0, b_1, \ldots, b_n \rangle$ lub

$$(\exists\, k) \Big(k \leq m \wedge k \leq n \wedge a_k < b_k \wedge (\forall\, i{<}k)\ a_i = b_i \Big).$$

Zadanie A91 (P). Rozważamy algebry sygnatury Σ zawierającej jeden symbol funkcji jednoargumentowej f i jeden symbol funkcji zero-argumentowej (stałej) a. Wiemy, że $\mathcal{A} = \langle A, f^{\mathcal{A}}, a^{\mathcal{A}} \rangle$ jest algebrą taką, że A jest zbiorem skończonym oraz

a. Istnieje homomorfizm algebry $\mathcal{A}$ na (surjekcja) pewną algebrę $\mathcal{B} = \langle B, f^{\mathcal{B}}, a^{\mathcal{B}} \rangle$. taką, że B ma 5 elementów.

b. Istnieje homomorfizm algebry $\mathcal{A}$ na (surjekcja) pewną algebrę $\mathcal{C} = \langle C, f^{\mathcal{C}}, a^{\mathcal{C}} \rangle$ taką, że $C = \{0, 1, 2, 3, 4\}$, $a^{\mathcal{C}} = 0$ oraz $f^{\mathcal{C}}$ jest dodawaniem modulo 5.

Jaka jest moc zbioru A przy założeniu a? Jaka jest moc zbioru A przy założeniu b?

Zadanie A92 (P). Niech K będzie rodziną podzbiorów zbioru liczb naturalnych taką, że relacja zawierania na tej rodzinie jest porządkiem regularnym. Pokaż, że każdy łańcuch w tym porządku jest przeliczalny.

Zadanie A93 (P). Udowodnij, że $(\mathbb{N} \times \mathbb{Q}, \leq_{lex})$ i $(\mathbb{Q}, \leq)$ są izomorficzne porządkowo. *Wolno Ci skorzystać z faktu, że funkcja $h\colon Q \to (0, 2)$ dana wzorem $h(x) = (1 + x/(1 + |x|))$ jest izomorfizmem porządkowym.*

Zadanie A94 (P). Niech Fin będzie zbiorem wszystkich skończonych podzbiorów liczb naturalnych. Definiujemy relację $\preccurlyeq\colon Fin \times Fin$ taką, że dla $X, Y \in Fin$ zachodzi $X \preccurlyeq Y$ wtedy i tylko wtedy, gdy

$$X = Y \text{ lub } \max(X \dot{-} Y) \in Y$$

gdzie $\dot{-}$ oznacza różnicę symetryczną zbiorów, a $\max(A)$ jest największą w sensie naturalnego porządku liczbą w zbiorze A. Udowodnij, że $(Fin, \preccurlyeq)$ jest dobrym porządkiem.

4.2 Homomorfizmy

Przedstaw następujące problemy jako problem istnienia homomorfizmu. Innymi słowy pokaż, jak mając efektywny algorytm rozwiązujący problem istnienia homomorfizmu rozwiązywać poniższe problemy.

Zadanie A95 (P). Rozwiązywanie sudoku. Dane jest częściowe rozwiązanie, pytamy czy można je rozszerzyć do pełnego rozwiązania.

Zadanie A96 (P). Ustawianie hetmanów na szachownicy. Na szachownicy stoi kilka hetmanów. Żadne dwa z nich się nawzajem nie szachują. Czy można dostawić jeszcze parę hetmanów, żeby w sumie było ich 8 i dalej się nie szachowały?

Zadanie A97 (P). Niech $\Sigma = \{+, a\}$ będzie sygnaturą zawierającą dwuargumentowy symbol funkcji $+$ i symbol stałej a. Dla dowolnej dodatniej liczby naturalnej n niech $A_n = \{0, 1, \ldots, n-1\}$, $\oplus_n$ oznacza dodawanie modulo n, zaś $a_n = 0$. Rozważmy algebry $\mathcal{A}_n = \langle A_n, \oplus_n, a_n \rangle$. Udowodnij, że jeżeli $k = l \cdot m$, to istnieje homomorfizm h algebry $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$ (surjekcja) taki, że $|\vec{h}^{-1}(\{0\})| = m$. Podaj przykład takich k, l i m, dla których istnieją co najmniej dwa takie homomorfizmy. Ile jest takich homomorfizmów, jeśli zamiast sygnatury Σ będziemy rozważać sygnaturę $\Sigma' = \{+, a, b\}$ zawierajacą dwa symbole stałych a i b oraz algebry $\mathcal{A}'_n = \langle A_n, \oplus_n, a_n, b_n \rangle$, gdzie $b_n = 1$?

5 Liczby porządkowe

Zadanie A98 (P). Wskaż przykłady porządków z klas $\omega + 2$ i $2 + \omega$.

Zadanie A99 (P). Wskaż przykłady porządków z klas $\omega * 2$ i $\omega * 17$.

Zadanie A100 (P). Dla każdego k wskaż przykład porządku z klasy ω^k.

Niech (standardowo) $\mathbb{N}^{<\omega}$ oznacza zbiór wszystkich ciągów skończonych o wyrazach naturalnych i niech $F \subseteq \mathbb{N}^{<\omega}$ będzie *zbiorem wygrywających (dla nas) pozycji końcowych*. W *F-grze* na $\mathbb{N}^{<\omega}$ bierze udział dwóch graczy: parzysty (nasz przeciwnik) i nieparzysty (my). Aktualną pozycją w grze jest zawsze ciąg $\mathbf{w} \in \mathbb{N}^{<\omega}$. Jeśli długość $\mathbf{w}$ jest parzysta, to gracz parzysty wybiera liczbę $n \in \mathbb{N}$ i zmienia aktualną pozycję na $\mathbf{w}n$ (gdzie przez $\mathbf{w}n$ rozumiemy ciąg $\mathbf{w}$ wydłużony o nowy element n) . Podobnie, jeśli długość $\mathbf{w}$ jest nieparzysta to gracz nieparzysty wybiera liczbę $n \in \mathbb{N}$ i zmienia aktualną pozycję na $\mathbf{w}n$. Początkową pozycją jest ciąg pusty. Gra kończy się (naszym zwycięstwem), gdy aktualna pozycja jest ciągiem ze zbioru F.

Zdefiniujmy $W \subseteq \mathbb{N}^{<\omega}$ jako najmniejszy (w sensie inkluzji) zbiór mający następujące własności:

- $F \subseteq W$;
- Jeśli $\mathbf{w}$ ma długość nieparzystą i istnieje takie $n \in \mathbb{N}$ że $\mathbf{w}n \in W$ to również $\mathbf{w} \in W$;
- Jeśli $\mathbf{w}$ ma długość parzystą i dla każdego $n \in \mathbb{N}$ ciąg $\mathbf{w}n \in W$ to również $\mathbf{w} \in W$.

Zadanie A101 (P). Jaki jest intuicyjny sens zbioru W? Co to znaczy „najmniejszy taki zbiór”? I czemu taki najmniejszy zbiór ma niby istnieć?

Zdefiniujmy funkcję h, przyporządkowującą każdemu elementowi W liczbę porządkową, następująco:

- Jeśli $\mathbf{w} \in F$ to $h(\mathbf{w}) = 0$.
- Jeśli $\mathbf{w} \in W$ ma długość nieparzystą to $h(\mathbf{w}) = min\{h(\mathbf{w}n) : \mathbf{w}n \in W\}$.
- Jeśli $\mathbf{w} \in W$ ma długość parzystą to $h(\mathbf{w}) = min\{\gamma : \forall n \in \mathbb{N}\ \gamma > h(\mathbf{w}n)\}$.

Zadanie A102 (P). Jaki jest intuicyjny sens funkcji h? Pokaż że (dla ustalonego F) istnieje dokładnie jedna funkcja h spełniająca powyższe warunki.

Zadanie A103 (P). Znajdź taki zbiór F dla którego $h(\varepsilon) = \omega$.

Zadanie A104 (P). Znajdź taki zbiór F dla którego $h(\varepsilon) = \omega 2$.

Zadanie A105 (Z). Znajdź taki zbiór F dla którego $h(\varepsilon) = \omega * \omega$.

Zadanie A106 (Z). Znajdź taki zbiór F dla którego $h(\varepsilon) = \omega * \omega * \omega * \omega * \omega$.

Potęgowanie liczb porządkowych zdefiniowane jest indukcyjnie w sposób następujący:

- $\alpha^1 = \alpha$ dla każdej liczby porządkowej α;
- $\alpha^{\beta+1} = \alpha^\beta \alpha$;
- jeśli β jest liczbą porządkową nie mającą poprzednika (czyli nie równającą się $\gamma + 1$ dla żadnej liczby γ) to $\alpha^\beta = \bigcup_{\gamma<\beta} \alpha^\gamma$. Innymi słowy α^β jest najmniejszą liczbą porządkową większą (lub równą) od każdej liczby α^γ gdzie γ jest liczbą porządkową mniejszą od β.

Zadanie A107 (P). Co to jest 1^ω? Co to jest 2^ω? Co to jest 3^ω? Co to jest $2^{(\omega+1)}$?

Zdefiniujmy działanie $\uparrow$ na liczbach porządkowych w sposób następujący: dla dobrych porządków α i β przez $\alpha \uparrow \beta$ oznaczać będziemy typ porządkowy porządku, którego elementami są funkcje z β w α które tylko dla skończenie wielu argumentów przyjmują wartość różną od zera (czyli od najmniejszego elementu porządku α) uporządkowane w sposób następujący: $g < f$ jeśli $x \in \beta$ jest największym (w sensie porządku na β) argumentem którym funkcje g i f się różnią (czemu taki argument musi istnieć?) i $g(x) < f(x)$.

Zadanie A108 (P). Co to jest $1 \uparrow \omega$? Co to jest $2 \uparrow \omega$? Co to jest $3 \uparrow \omega$? Co to jest $2 \uparrow (\omega + 1)$?

Zadanie A109 (Z). Rozwiązania poprzednich zadań prowadzą ku pewnej hipotezie. Sformułuj ją i udowodnij.

Przeczytaj ze zrozumieniem rozdział 2 ze skryptu *Teoria mnogości* Piotra Zakrzewskiego `https://www.mimuw.edu.pl/~piotrzak/TM-skrypt.pdf`.

Zadanie A110 (P, 4 punkty). Potraf udowodnić twierdzenie 2.31 (wraz z wszystkimi twierdzeniami/lematami/wnioskami, z których dowód korzysta).

Zadanie A111 (P). Potraf udowodnić twierdzenie 2.52 (tym razem możesz założyć, że wcześniejsze twierdzenia/wnioski są udowodnione).

Zadanie A112 (P). Potraf udowodnić twierdzenie 2.54 (tym razem możesz założyć, że wcześniejsze twierdzenia/wnioski są udowodnione).

6 Unifikacja

Zadanie A113 (P, za 3 punkty). Rozwiąż zadania z rozdziału „Problem unifikacji" z *Materiałów do zajęć*.

Zadanie A114 (Z). Pokaż, że mając symbol łączny i przemienny, dla którego algorytm unifikacji działa w czasie wielomianowym, da się stworzyć algorytm rozwiązujący problem trzykolorowania grafu w czasie wielomianowym.

7 Kącik misiowy

W ramach tych zajęć będziemy rozwiązywać kilka zadań o niedźwiedziach, a jedno z nich (gdzieś w styczniu) będzie szczególnie ważne. Zaczynamy jednak od prostego zadania, luźno powiązanego z kursem.

Zadanie A115 (P). Myśliwy pojmał dwa niedźwiedzie. I mówi im tak:

Zaraz was rozdzielę i przed jednym z was postawię standardową szachownicę, a na każdym jej polu położona będzie jedna moneta – albo orłem do góry, albo reszką. Spośród tych 64 monet, 63 będą zatrute, a jedna nie. Temu, przed którym postawię szachownicę, powiem, która moneta nie jest zatruta, a on będzie musiał wskazać jedną z monet, którą ja odwrócę. Wtedy zaniosę szachownicę do tego drugiego i on będzie musiał podnieść jedną z monet. Jak podniesie jedną z zatrutych, to umrze, a ja zrobię z was zabójczy bigos. A jeśli wybierze dobrą monetę, to puszczę was wolno. A teraz się możecie namówić co robić.

Czy niedźwiedzie mają sposób, żeby się wyratować?

7.1 Zadania z kartami

Myśliwy pojmał dwa niedźwiedzie. I mówi im tak: Zaraz was rozdzielę i jednemu z was dam pięć kart wybranych z ...

Zadanie A116 (P). ...talii zawierającej 28 różnych kart.

Zadanie A117 (P). ...pełnej talii (czyli talii zawierającej 52 karty).

Zadanie A118 (Z). ...talii zawierającej 126 różnych kart.

On zaś będzie miał jedną z tych kart odłożyć na bok, a pozostałe dać mi w ustalonej przez siebie kolejności. Wtedy zaniosę te cztery karty do tego drugiego i podam mu je w tej samej kolejności, a on będzie musiał powiedzieć, jaką kartę ten pierwszy odłożył na bok. Jeśli powie źle, to zrobię z was bigos, a jak powie dobrze, to puszczę was wolno. A teraz się możecie namówić co robić.

Czy niedźwiedzie mają sposób, żeby się wyratować?

7.2 Wariacje na temat zadania z kapeluszami

Zadanie A119 (P). Myśliwy pojmał nieskończenie wiele niedźwiedzi. I mówi im tak:

— Zaraz wam na wasze durne łby założę kapelusze. Jednym białe innym czarne. Każdy będzie widział wszystkie inne kapelusze ale swojego nie. Na dany znak każdy napisze na kartce jaki ma na głowie kapelusz. Jak się tylko skończenie wielu z was pomyli to was wszystkich wypuszczę. A jak się nieskończenie wielu pomyli to zrobię z was bigos. A teraz się możecie namówić co robić.

Zapisz w języku logiki/teorii mnogości (nad odpowiednio dobraną sygnaturą) zdanie mówiące, że niedźwiedzie mają strategię, żeby się wyratować.

Zadanie A120 (P). Myśliwy pojmał jednego niedźwiedzia. I mówi mu tak:

Zaraz ustalę sobie funkcję $f\colon\mathbb{R}\to\mathbb{R}$. Ty zaś wybierzesz jedną liczbę $x\in\mathbb{R}$, a ja wtedy podam Ci wartości tej funkcji dla wszystkich liczb poza x (tzn. $\{(y,f(y)) \mid y\in\mathbb{R}\setminus\{x\}\}$). Ty zaś będziesz musiał mi podać wartość $f(x)$. Jeśli powiesz źle, to zrobię z Ciebie bigos, a jak powiesz dobrze, to puszczę Ciebie wolno. A teraz się możesz zastanowić, co robić.

Udowodnij, że niedźwiedź ma strategię, która pozwala mu się uratować z prawdopodobieństwem 1.

Zadanie A121 (P). Myśliwy pojmał continuum niedźwiedzi. I mówi im tak:

— Zaraz wam na wasze durne łby założę kapelusze. Na każdym będzie napisana liczba rzeczywista. Każdy będzie widział wszystkie inne kapelusze ale swojego nie. Na dany znak każdy napisze na kartce jaką liczbę ma na kapeluszu. Jak się tylko skończenie wielu z was pomyli, to was wszystkich wypuszczę. A jak się nieskończenie wielu pomyli, to zrobię z was bigos. A teraz się możecie namówić co robić.

Czy mają sposób żeby się wyratować?

Wskazówka: Miśki zaliczyły logikę i wiedzą, co to jest relacja równoważności, klasy abstrakcji, znają też aksjomat wyboru i nie zawahają się go użyć.