Koło Matematyków Studentów UJ

XIII Międzynarodowe Warsztaty dla Młodych Matematyków

Logika i podstawy matematyki

Kraków 2011

Zespół redakcyjny:
Agnieszka Dutka
Michał Handzel
Tomasz Kisielewski
Piotr Wójcik

Korekta językowa:
Agnieszka Dutka
Maria Kowtunenko

Projekt okładki: **Maria Dudek**

Opieka naukowa:
prof. dr hab. Paweł Maria Idziak
prof. dr hab. Andrzej Wroński
prof. dr hab. Marek Zaionc
dr hab. Krzysztof Nowak

ISBN 978-83-929547-2-9

Koło Matematyków Studentów UJ
im. prof. Stanisława Zaremby
ul. Łojasiewicza 6/1008
30-348 Kraków

Druk i oprawa: Drukarnia GS sp. z o.o.

Spis treści

Przedmowa

Piotr Wójcik

XIII Warsztaty dla Młodych Matematyków odbyły się w dniach 19–24 września 2010 r. Podobnie jak w ubiegłych latach, wydarzenie miało charakter studenckiej konferencji, podczas której młodzi adepci matematyki mieli okazję do dzielenia się wiedzą oraz zaprezentowania własnych wyników. Zaproponowany temat – logika i podstawy matematyki – zachęcał uczestników do podejmowania interdyscyplinarnych poszukiwań na pograniczu dziedzin takich jak: logika, teoria złożoności, teoria algorytmów oraz filozofia. Zaowocowało to niezwykłą różnorodnością tekstów, która odzwierciedla rzeczywistą mnogość kierunków badań i metod współczesnej matematyki, a zwłaszcza tej jej części, która poszukuje solidnych podstaw teoretycznych dla nauk ścisłych. Niniejsza publikacja zawiera referaty wygłoszone podczas warsztatowych sesji plenarnych. Ich autorami są zarówno wybitni specjaliści o uznanym dorobku, jak również nasi koledzy i koleżanki, stawiający swoje pierwsze kroki na ścieżce naukowej. Mamy nadzieję, że ten wybór będzie stanowił interesujący przegląd problemów, z którymi mierzyli się uczestnicy Warsztatów.

Na koniec pragniemy złożyć serdeczne podziękowania instytucjom i firmom, bez pomocych których istnienie Warsztatów w ich obecnej formie nie byłoby możliwe:

Polskiej Akademii Umiejętności

Wydziałowi Matematyki i Informatyki UJ

Instytutowi Matematyki UJ

Radzie Kół Naukowych UJ

Funduszowi im. Jana Kochanowskiego

Fundacji Studentów i Absolwentów UJ „Bratniak”

serwisowi `www.kalkulatory.pl`

A model-theoretic solution to Hilbert's XVIIth problem

Maksymilian Grab

Abstract. Hilbert's XVIIth problem asks whether every non-negative rational function over field of real numbers is the sum of squares of real rational functions. Using model completness of the theory of real closed fields we will prove that the answer is affirmative. We found this proof as an interesting application of model theory in solving pure algebraic problem.

1. Formulation of the problem

Problem 1 (Hilbert's XVIIth problem)**.** *Let* $f \in \mathbb{R}(x_1, \ldots, x_n)$ *be non-negative, i.e.*

$$\forall_{a_1,\ldots,a_n \in \mathbb{R}} \; f(a_1, \ldots, a_n) \geq 0.$$

We want to know if there exists $g_1, \ldots g_m \in \mathbb{R}(x_1, \ldots, x_n)$*, such that*

$$f = \sum_{i=1}^{m} g_i^2.$$

Our aim is to show that:

Theorem 2. *The answer to the Hilbert's XVIIth problem is positive.*

Remark 3. Note that if we require $g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_n]$, then the answer is negative. The counterexample is $f(x_1, x_2) = x_1^4 x_2^2 + x_1^2 x_2^4 - x_1^2 x_2^2 + 1$. We left the details to the reader as an interesting excercise (proof can be found in [3]).

Maksymilian Grab
maksymilian.grab@gmail.com
student matematyki
Uniwersytet Jagielloński

1.1. A short historical note

The problem was published among 23 famous other problems by David Hilbert in 1900. The first solution was due to Artin ([1]) who used algebraic methods (Artin-Schreier theory of real closed fields). The idea to use model completness comes from Robinson ([5]). For references to better elaboration on historical background see [4].

2. Elementary facts from real closed field theory (cf. [2])

We recall the notion of ordered field, real closed field and the fact that every ordered field is contained in some real closed field. Next we develop a series of easy but technical results culminating in Lemma 11, which will be very important step in the proof of the main theorem.

Let k be a field.

2.1. Basic notions and existence of real closure

Definition 4. A pair $(k, \leq)$ is said to be an ordered field if $\leq$ is a linear order on k such that:

(i) If $x, y, z \in k$ and $x \leq y$ then $x + z \leq y + z$

(ii) If $x, y \in k$ and $x \geq 0,\ y \geq 0$ then $xy \geq 0$.

Definition 5. We say that ordered field $(k, \leq)$ is a real closed field if every positive element of k is a square and every polynomial from $k[x]$ of odd degree has a root in k. In particular the field of real numbers is real closed field.

Theorem 6. *For every ordered field $(k, \leq)$ there exists a real closed field $(K, \leq_K)$ such that k is a subfield of K and for every $x, y \in k$ we have $x \leq y \iff x \leq_K y$.*

Proof. In fact one can require that $k \subset K$ is algebraic extension. Then this result is nothing else than well-known existence of real closure of ordered field. One can find a proof for example in [2]. □

2.2. Cones and lemma on extending orders

Definition 7. $S \subset k$ is said to be a cone of k if

(i) $SS \subset S$

(ii) $S + S \subset S$

(iii) If $x \in k$ then $x^2 \in S$.

A cone S is said to be proper if $-1 \notin S$. A proper cone is said to be positive if $S \cup -S = k$.

Proposition 8. *If $S \subset k$ is a positive cone then defining $x \leq y \overset{\text{def}}{\iff} y - x \in S$ we obtain that $(k, \leq)$ is an ordered field and $S = \{x \in k\colon\ x \geq 0\}$. We call $\leq$ the ordering associated with S.*

Proof. This is an easy calculation which we left to the reader. □

Lemma 9. *If $S \subset k$ is a cone, $-a \notin S$ then $S_a := \{x + ay\colon\ x, y \in S\}$ is a proper cone containing a.*

Proof. A simple calculation shows that S_a is a cone. Moreover S_a is proper, for if

$$-1 = x + ay, \quad x, y \in S$$

then $y \neq 0$ (as $-1 \notin S$) and $-a = (1/y)^2 y(1 + x) \in S$ - a contradiction. Of course

$$a = 0 + 1 \cdot a \in S_a.$$

□

Proposition 10. *Positive cones of k are exactly maximal cones in the sense of inclusion. In particular every cone of k is contained in some positive cone.*

Proof. If S is a maximal cone then S is positive by the previous lemma. On the other hand if S is positive cone $S' \supsetneq S$ is a cone and $a \notin S' \setminus S$ then $-a \in S \subset S'$ and $-1 = (1/a)^2(-a)a \in S'$, so S' is not proper and S is maximal. The second part of the proposition follows easily from the first part and Zorn's lemma. □

Lemma 11 (A lemma on extending orders)**.** *Assume that $(k, \leq)$ is an ordered field such that every positive element of k is a square, $k \subset K$ is a field extension and a is not a sum of squares from K.*

Then there exists an ordering $\leq_*$ on K such that $x \leq y \iff x \leq_* y$ for every $x, y \in k$ and $a < 0$.

Proof. Note that $S := \left\{\sum_{i=1}^{l} x_i^2\colon\ x_i \in K,\ l \geq 1\right\}$ is a cone of K containing $\{x \in k\colon\ x \geq 0\}$. Then the proper cone S_a satisfies $-a \in S_a,\ S_0 \subset S_a$. Extending S_a to the positive cone S' and taking as $\leq_*$ the order associated with S' we obtain the desired result. □

3. Model completness (cf. [3])

Observe that the axioms of RCF (real closed fields theory) can be written in the first order language. This fact allows us to use model theory in proving certain statements involving real closed fields. Here we recall the definition of elementary submodel, state the definition of model complete theory and observe that RCF is a model complete theory as it admits the quantifier elimination. Model completness of RCF will be the crucial argument in the proof of main theorem which we give in the next section.

Definition 12. Let M, N be the models for theory T such that $M \subset N$ (i.e. M is a submodel of N). We write $M \prec N$ (M is an elementary submodel of N) if for every formula φ of free variables $v_1, \ldots, v_l$ and every $a_1, \ldots, a_l \in M$ we have the following equivalence:

$$a_1, \ldots, a_l \text{ satisfies } \varphi \text{ in } M \iff a_1, \ldots, a_l \text{ satisfies } \varphi \text{ in } N.$$

Definition 13. A first order theory T is said to be model complete if for every models $M \subset N$ of T we have $M \prec N$.

Proposition 14. *RCF is model complete.*

Proof. This follows immediately from quantifier elimination for RCF. □

4. Proof of the main theorem (cf. [3])

Now we are ready to present the proof of main theorem. This will be done in four simple steps.

4.1. Reduction to the case of non-negative polynomial

Let $f = G/H$ where $G, H \in \mathbb{R}[x_1, \ldots, x_n]$. Then $\forall_{a \in \mathbb{R}^n} f(a) \geq 0 \implies \forall_{a \in \mathbb{R}^n} GH(a) \geq 0$ and if $GH = \sum_{i=1}^m g_i^2$ then $f = \sum_{i=1}^m \left(\frac{g_i}{H}\right)^2$ so w.l.o.g. we may assume that f is a polynomial.

4.2. Extension of order on $\mathbb{R}$ to the $\mathbb{R}(x_1, \ldots, x_n)$

Suppose that $f \in \mathbb{R}[x_1, \ldots, x_n]$ is a counterexample to the main theorem. Then Lemma 11 for $k = \mathbb{R}$, $K = \mathbb{R}(x_1, \ldots, x_n)$, $a = f$, yields an ordering $\leq_*$ on $\mathbb{R}(x_1, \ldots, x_n)$ extending the ordering on $\mathbb{R}$ and such that $f <_* 0$.

4.3. Passage to the real closure of $\mathbb{R}(x_1, \ldots, x_n)$

By Theorem 6 there exists real closed field extension $R \supset \mathbb{R}(x_1, \ldots, x_n)$ with ordering extending $\leq_*$. In particular $R \supset \mathbb{R}$ is the extension of fields, order on R extends the order on $\mathbb{R}$, and both this fields are real closed. In other words $\mathbb{R}, R$ are the models of RCF and $\mathbb{R} \subset R$ in the sense of model theory.

4.4. Model completness of RCF finishes the proof

Note that when in the sentence $\exists_{a_1, \ldots, a_n} f(a_1, \ldots, a_n) < 0$ we treat a coefficients $c_1, \ldots, c_l \in \mathbb{R}$ of f as a variables $v_1, \ldots, v_l$ then we obtain a formula of free variables $v_1, \ldots, v_l$ in the first order language of ring theory. This formula is satisfiable by $c_1, \ldots, c_l$ in the model R of RCF, as $f(x_1, \ldots, x_n) <_* 0$. Since RCF is model complete and $\mathbb{R} \subset R$, we know that $\mathbb{R} \prec R$. Hence our formula is satisfiable by $c_1, \ldots, c_l$ also in $\mathbb{R}$, namely f attain a negative value for some n-tuple of real numbers. But this is a contradiction with the non-negativity of f. □

Acknowledgment

I would like to thank dr hab. Krzysztof Nowak, for his advice and interesting discussions about model theory which not only helped me in preparing my talk and this article, but also gave me some general insight in this field of mathematics.

References

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Abh. Math. Sem. Univ. Hamburg, 5 (1927), 85–99.

[2] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*, Springer, Berlin 1998.

[3] W. Weiss, C. D'Mello, *Fundamentals of the model theory*, University of Toronto 1997. The book is available on the Internet, `http://www.math.toronto.edu/weiss/model_theory.html`.

[4] B. Reznick, *Some concrete aspects of Hilbert's 17th problem*, Cont. Math., 253 (2000), 251–272.

[5] A. Robinson, *On ordered fields and definite forms*, Math. Ann. 130 (1955), 257–271.

Dziwne zbiory na prostej

Alicja Kierus

Lemat 1. *Istnieją parami rozłączne zbiory borelowskie $A, B, C \subseteq \mathbb{R}$, takie że*

$$\left(\forall_{(a,b)\subseteq\mathbb{R}}\right)\left(\lambda\left((a,b)\cap A\right)>0 \wedge \lambda\left((a,b)\cap B\right)>0\right) \wedge \lambda\left((a,b)\cap C\right)>0.$$

Twierdzenie 2. *Istnieje zbiór niemierzalny $E \subseteq \mathbb{R}$, taki że*

$$\lambda_*\left((a,b)\cap E\right)>0, \quad \lambda_*\left((a,b)\cap \mathbb{R}\backslash E\right)>0$$

oraz $(a,b)\cap E$ jest niemierzalny dla wszystkich $(a,b)\subseteq\mathbb{R}$, gdzie λ_* oznacza wewnętrzną miarę Lebesgue'a.

Dowód. Niech A, B, C będą takie jak w tezie lematu. Oznaczmy $\mathfrak{c} = |\mathbb{R}|$. Niech $\mathcal{F} = \{F_\xi\colon\ \xi < \mathfrak{c}\}$ będzie numeracją domkniętych podzbiorów C w topologii indukowanej, takich że $\lambda(F\cap C)>0$. Niech $F \in \mathcal{F}$. Wówczas istnieje taki domknięty zbiór $F' \subseteq \mathbb{R}$, że $F = F'\cap C$. Ponieważ C jest zbiorem borelowskim, więc F jest również borelowski. Ponadto $|F| = \mathfrak{c}$, gdyż F jest zbiorem borelowskim miary dodatniej. Można zdefiniować przez indukcję dwa rozłączne zbiory $\{a_\xi\colon\ \xi<\mathfrak{c}\}$ i $\{b_\xi\colon\ \xi<\mathfrak{c}\}$, takie że

$$F\cap\{a_\xi\colon\ \xi<\mathfrak{c}\}\neq\emptyset\neq F\cap\{b_\xi\colon\ \xi<\mathfrak{c}\}$$

dla wszystkich $F\in\mathcal{F}$. Połóżmy $E = \{a_\xi\colon\ \xi<\mathfrak{c}\}\cup A$. Wtedy E spełnia tezę twierdzenia. □

Uwaga 3. Wiadomo, że każdy zbiór o mierze dodatniej lub drugiej kategorii mający własność Baire'a spełnia warunek:

$$0\in\operatorname{int}(A-A). \tag{1}$$

Mówią o tym odpowiednio twierdzenia Steinhausa oraz Picarda. Znanych jest wiele uogólnień tych twierdzeń. Często zamiast warunku (1) wykorzystywany jest warunek:

$$\operatorname{int}(A-A)\neq\varnothing. \tag{2}$$

Alicja Kierus
amayor3.14@gmail.com
studentka matematyki
Politechnika Łódzka

Twierdzenie 4. *Istnieje taki zbiór* $A \subseteq \mathbb{R}$*, że* $\operatorname{int}(A-A) \neq \varnothing$ *oraz* $0 \notin \operatorname{int}(A-A)$.

Dowód. Niech V będzie zbiorem niemierzalnym Vitalego utworzonym w $[0,1]$, takim że $0 \in V$. Niech $\{a_n\}_{n=1}^{\infty}$ będzie numeracją wszystkich liczb wymiernych w $[-1,1]$. Stworzymy ciąg $\{V_n\}_{n=0}^{\infty}$ poprzesuwanych zbiorów Vitalego, taki że $A = \bigcup_{n=0}^{\infty} V_n$ będzie spełniał tezę. Niech $V_0 = V$ oraz

$$V_n = \begin{cases} V + 2n, & \text{gdy } n \text{ jest parzyste,} \\ V + 2n + a_{\frac{n+1}{2}}, & \text{gdy } n \text{ jest nieparzyste} \end{cases}$$

dla $n \geq 1$. Pokażemy teraz, że $[2,3] \subseteq A - A$. Niech $v' \in V_n$, gdzie n jest nieparzyste. Wtedy $v' = v + 2n + a_{\frac{n+1}{2}}$ dla pewnych $v \in V$. Ponieważ $0 \in V$, więc $2(n-1) \in V_{n-1}$. Wówczas $v' - 2(n-1) \in A - A$ oraz

$$v' - 2(n-1) = v + 2n + a_{\frac{n+1}{2}} - 2n + 2 = v + a_{\frac{n+1}{2}} + 2.$$

Stąd $v + a_{\frac{n+1}{2}} + 2 \in A - A$ dla wszystkich $v \in V$. Zatem $V + a_{\frac{n+1}{2}} + 2 \subseteq A - A$. Podobnie $V + a_n + 2 \subseteq A - A$ dla wszystkich $n \in \omega$. Wynika stąd, że

$$\bigcup_{n=1}^{\infty} (V + a_n + 2) \subseteq A - A$$

oraz

$$\bigcup_{n=1}^{\infty} (V + a_n + 2) = 2 + \bigcup_{n=1}^{\infty} (V + a_n) = 2 + \bigcup_{q \in \mathbb{Q} \cap [-1,1]} (V + q) \supseteq 2 + [0,1].$$

Zatem $[2,3] \subseteq A - A$ oraz $(2,3) = \operatorname{int}([2,3]) \subseteq \operatorname{int}(A - A)$. □

Dziesiąty problem Hilberta

Tomasz Kobos

1. Wstęp

W 1900 r. David Hilbert opublikował listę dwudziestu trzech problemów matematycznych, które uważał za kluczowe dla dalszego rozwoju ówczesnej matematyki. Niektóre z nich, jak na przykład słynna hipoteza Riemanna o zerach funkcji ζ-Riemanna, pozostają nierozwiązane aż do dzisiaj. Część z problemów podanych przez Hilberta nie była również sformułowana wystarczająco precyzyjnie, aby udzielić na nie jednoznacznej odpowiedzi.

Poniższa praca dotyczy problemu dziesiątego, który przez długie lata spędzał matematykom sen z powiek. Rozwiązanie dziesiątego problemu Hilberta zawdzięczamy trzem amerykańskim matematykom: Martinowi Davisowi, Hilary Putnam, Julii Robinson oraz rosyjskiemu matematykowi Yuriemu Matiyasevichowi, który podał ostatni fragment dowodu w 1970 r., podczas gdy pierwsze rezultaty osiągnięte zostały na początku lat 50. Ponieważ kompletne rozwiązanie problemu stanowi materiał na książkę, a nie na jeden artykuł, celem poniższej pracy jest tylko wprowadzenie czytelnika w zagadnienie dziesiątego problemu Hilberta. Skupimy się na formalnej interpretacji pytania, przedstawimy historię zmagań z problemem oraz zasygnalizujemy główne idee dowodu.

2. Dziesiąty problem Hilberta

Treść dziesiątego problemu Hilberta jest następująca:

Problem 1 (Hilbert)**.** *Czy istnieje skończony algorytm, który rozstrzyga istnienie rozwiązania dowolnego równania diofantycznego?*

Tomasz Kobos
tkobos@wp.pl
student matematyki
Uniwersytet Jagielloński

Dzisiaj wiemy już, że odpowiedź na to pytanie jest negatywna, ale problem został rozwiązany dopiero po 70 latach. Warto w tym momencie zaznaczyć, że starając się wiernie przetłumaczyć problem postawiony przez Hilberta, jego treść powinna wyglądać raczej tak:

Problem 2. *Znaleźć skończony algorytm, który rozstrzyga istnienie rozwiązania dowolnego równania diofantycznego.*

Hilbert, pytając o sposób, w jaki znaleźć taki algorytm, nie brał pod uwagę możliwości, że może on nie istnieć. W tym momencie trzeba również zwrócić uwagę na słowo „algorytm" padające w treści pytania. Każdy intuicyjnie rozumie, co to jest algorytm, jednak pełna matematyczna interpretacja tego pojęcia podana została dopiero pod koniec lat 40., a więc długo po sformułowaniu problemu. Hilbert wierzył, że poszukiwany algorytm można przedstawić, i to w taki sposób, że nikt nie miałby wątpliwości, iż za jego pomocą można uzyskać ogólną metodę rozstrzygania rozwiązywalności danego równania diofantycznego. Chcąc jednak udowodnić, że taki algorytm nie istnieje, z całą pewnością nie zdołamy uniknąć pełnego zdefiniowania – a raczej zinterpretowania – pojęcia algorytmu. W dalszej części pracy wprowadzimy ścisłe pojęcie algorytmu, zdefiniowane poprzez maszyny Turinga, na razie jednak trzymajmy się intuicyjnego rozumienia tego słowa.

Należy również sprecyzować pojęcie równania diofantycznego. W tym wypadku mamy na myśli równanie postaci:

$$P(x_1, x_2, \ldots, x_n) = 0,$$

gdzie P jest wielomianem n zmiennych o współczynnikach całkowitych. Rozwiązań tego równania poszukujemy w liczbach całkowitych $x_1, x_2, \ldots, x_n$.

Dla przykładu, równanie

$$5x^7 + 42xy^3 - 19z^2 + 31 = 0$$

uznajemy za równanie diofantyczne, ale równania

$$3^x + 2^y = 5^z$$

już nie.

Zwróćmy jeszcze uwagę, że zadaniem poszukiwanego algorytmu nie jest rozwiązywanie dowolnego równania diofantycznego, a jedynie stwierdzenie, czy rozwiązania istnieją.

3. Przykłady

Na początek rozważmy jedno z najprostszych równań diofantycznych – równanie diofantyczne liniowe

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c.$$

W tym wypadku warunkiem równoważnym istnieniu rozwiązania w liczbach całkowitych jest podzielność $\mathrm{NWD}(a_1, a_2, \ldots, a_n)|c$ – czyli dla równań liniowych poszukiwany algorytm istnieje i można go łatwo podać.

Kolejny krok mógłby polegać na rozważeniu równań drugiego stopnia dwóch zmiennych, tzn. postaci

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

gdzie a, b, c, d, e i f są liczbami całkowitymi. W przypadku tego typu równań możemy podać algorytm, który stwierdza istnienie rozwiązań, jest on jednak już dosyć skomplikowany. Wraz ze wzrostem ilości niewiadomych i ilości zmiennych sytuacja drastycznie się pogarsza.

4. Proste obserwacje

Hilbert pytał o algorytm stwierdzający rozwiązywalność pojedynczego równania diofantycznego. Można jednak pójść dalej i jedno równanie zastąpić układem równań diofantycznych. Na pierwszy rzut oka wydaje się być to trudniejsze niż jest w rzeczywistości. Okazuje się, że jeśli istniałby algorytm, o który pytał Hilbert, to za jego pomocą można by również rozstrzygać istnienie rozwiązania układu równań diofantycznych. Rzeczywiście, układ równań

$$\begin{aligned} P_1(x_1, x_2, \ldots, x_n) &= 0, \\ P_2(x_1, x_2, \ldots, x_n) &= 0, \\ &\vdots \\ P_k(x_1, x_2, \ldots, x_n) &= 0, \end{aligned}$$

posiada rozwiązanie w liczbach całkowitych $x_1, x_2, \ldots, x_n$ wtedy i tylko wtedy, gdy rozwiązanie posiada pojedyncze równanie diofantyczne:

$$P_1^2(x_1, x_2, \ldots, x_n) + P_2^2(x_1, x_2, \ldots, x_n) + \ldots + P_k^2(x_1, x_2, \ldots, x_n) = 0.$$

Czasami warto zrobić operację odwrotną – tzn. pojedyncze równanie rozbić na układ prostszych równań diofantycznych. Weźmy na przykład równanie:

$$4x^3y - 2x^2z^3 - 3y^2x + 5z = 0.$$

Przepiszmy je najpierw w postaci:

$$4x^3y + 5z = 2x^2z^3 + 3y^2x.$$

Wprowadźmy teraz 14 nowych zmiennych, aby otrzymać układ równań równoważny powyższemu równaniu:

$$\begin{array}{lllll} p_1 = 4x & q_1 = 5z & r_1 = 2x & s_1 = 3y & t_1 = p_4 + q_1 \\ p_2 = p_1x & & r_2 = r_1x & s_2 = s_1y & u_1 = r_5 + s_3 \\ p_3 = p_2x & & r_3 = r_2z & s_3 = s_2x & t_1 = u_1 \\ p_4 = p_3y & & r_4 = r_3z & & \\ & & r_5 = r_4z & & \end{array}$$

Łatwo zauważyć, że analogiczną metodę możemy zastosować w przypadku dowolnego równania diofantycznego. W efekcie dostajemy równoważny układ równań, w którym każde równanie ma stopień co najwyżej 2. Jeśli teraz zastosujemy wcześniej opisywaną operację z sumą kwadratów, to znowu dostaniemy pojedyncze równanie, ale tym razem takie, w którym nie występuje składnik o stopniu większym niż 4. A więc rozwiązywalność danego równania diofantycznego może być sprowadzona do rozwiązywalności równania diofantycznego o stopniu co najwyżej 4 (oczywiście przy zwiększeniu liczby zmiennych).

W rozważanym problemie szukamy rozwiązań równań diofantycznych w liczbach całkowitych. Ciekawą wersję problemu otrzymamy, dopuszczając jedynie rozwiązania będące liczbami naturalnymi. Weźmy na przykład równanie:

$$(x+1)^n + (y+1)^n = (z+1)^n,$$

gdzie $n \geq 3$ jest liczbą naturalną. Łatwo zauważyć, że posiada ono rozwiązanie $x = 0$, $y = -1$, $z = 0$. Jeśli jednak zapytamy o rozwiązania w liczbach naturalnych, to sprawa jest dużo trudniejsza. Dopiero kilkanaście lat temu Andrew Wiles wykazał, że takich rozwiązań to równanie nie posiada. A więc w przypadku konkretnego równania diofantycznego rozstrzygnięcie jego rozwiązywalności w liczbach całkowitych i rozstrzygnięcie jego rozwiązywalności w liczbach naturalnych są dwoma oddzielnymi zagadnieniami.

Z punktu widzenia dziesiątego problemu Hilberta nie ma jednak różnicy, czy szukamy rozwiązań całkowitych, czy naturalnych. Rzeczywiście, załóżmy, że mamy algorytm, który rozstrzyga rozwiązywalność równań diofantycznych w liczbach całkowitych. Łatwo możemy go teraz wykorzystać do rozstrzygania rozwiązywalności w liczbach naturalnych. Weźmy bowiem dowolne równanie:

$$P(x_1, x_2, \ldots, x_n) = 0$$

i załóżmy, że szukamy rozwiązań naturalnych. Wystarczy zastosować nasz algorytm do równania:

$$P(y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2, \ldots, y_{n,1}^2 + y_{n,2}^2 + y_{n,3}^2 + y_{n,4}^2) = 0.$$

Jeśli bowiem drugie równanie posiada rozwiązanie, to równanie pierwsze posiada rozwiązanie w liczbach naturalnych. Natomiast jeśli pierwsze równanie posiada rozwiązanie w liczbach naturalnych, to drugie równanie posiada rozwiązanie w liczbach całkowitych, gdyż na mocy twierdzenia Lagrange'a każda liczba naturalna jest sumą czterech kwadratów liczb całkowitych.

Załóżmy teraz, że istnieje algorytm, który rozstrzyga rozwiązywalność równań diofantycznych w liczbach naturalnych. Chcemy wykorzystać go do rozstrzygania rozwiązywalności w liczbach całkowitych. Rozważmy dowolne równanie:

$$P(x_1, x_2, \ldots, x_n) = 0.$$

Wystarczy teraz zastosować nasz algorytm, aby sprawdzić, czy pewne z 2^n równań postaci:

$$P(\pm x_1, \pm x_2, \ldots, \pm x_n) = 0$$

ma rozwiązanie naturalne. W ten sposób rozstrzygniemy rozwiązywalność wyjściowego równania w liczbach całkowitych.

Pokazaliśmy więc, że istnienie algorytmu rozstrzygającego rozwiązywalność równań diofantycznych w liczbach całkowitych jest równoważne istnieniu algorytmu rozstrzygającego rozwiązywalność równań diofantycznych w liczbach naturalnych. Z tego powodu większość prac dotycząca dziesiątego problemu Hilberta operuje na rozwiązaniach naturalnych.

5. Maszyny Turinga

Aby wykazać, że nie istnieje konstrukcja algorytmiczna, o której mówi dziesiąty problem Hilberta, musimy dysponować precyzyjnym pojęciem algorytmu. W czasie, gdy Hilbert postawił swój problem, nie było ścisłej, matematycznej definicji tego słowa. Intuicyjnie algorytm to zestaw instrukcji, które można wykonać w sposób nie wymagający kreatywności, tzn. „mechanicznie". Dopiero na początku lat trzydziestych XX wieku ukazało się kilka niezależnie opracowanych matematycznych modeli algorytmów. Najsłynniejszym została maszyna Turinga, zaproponowana w pracy *On Computable Numbers* autorstwa Alana Turinga. W paru słowach opiszemy zasadę działania Maszyn Turinga.

Maszyna Turinga jest abstrakcyjnym urządzeniem, którego najważniejszą częścią jest taśma podzielona na pola. Przyjmujemy, że istnieje lewy koniec taśmy i że taśma może być nieskończona prawostronnie, ale czasem przyjmuje się również, że taśma może być nieskończona obustronnie. W każdym polu moze znajdować się symbol należący do pewnego skończonego zbioru symboli zwanego *alfabetem* lub pole może być puste. Jeden z symboli oznacza lewy koniec taśmy i nie pojawia się w żadnym innym miejscu. Maszyna zawsze jest ustawiona nad jednym z pól i znajduje się w jednym z M stanów, przy czym M jest skończone. Jeden ze stanów jest stanem początkowym i ponadto jeden lub więcej ze stanów są stanami końcowymi i oznaczają zakończenie pracy maszyny. Zależnie od kombinacji stanu maszyny i pola maszyna zapisuje nową wartość w polu, zmienia stan, a następnie może przesunąć się o jedno pole w prawo, w lewo lub pozostać na tym samym polu. Taka operacja nazywana jest instrukcją lub rozkazem. Maszyna Turinga jest sterowana listą zawierającą dowolną liczbę takich instrukcji. Każdej parze składającej się z pewnego niekończowego stanu i pewnego symbolu z alfabetu (lub pustemu polu) odpowiada dokładnie jedna instrukcja. Lista rozkazów dla maszyny Turinga nazywana jest czasem jej programem.

Na początku pewien spójny fragment taśmy jest wypełniony symbolami z alfabetu, zaś reszta potencjalnie nieskończonej taśmy jest pusta. Maszyna jest ustawiona nad jednym z pól i jest w stanie początkowym. Następnie maszyna pracuje krok po kroku według instrukcji. Praca maszyny kończy się, gdy maszyna przejdzie w jeden ze stanów końcowych. Dopuszcza się sytuację, w której stan końcowy nigdy nie zostanie osiągnięty i maszyna będzie pracować w nieskończoność.

Warto w tym miejscu dodać, że można przyjmować wiele różnych wariantów maszyny Turinga. Dowodzi się jednak, że większość z nich jest równoważna.

Po opracowaniu modelu teoretycznej maszyny możemy łatwo zdefiniować pojęcie algorytmu. Algorytm to zestaw instrukcji, które może wykonać pewna maszyna Turinga.

Wraz z pojawieniem się maszyny Turinga pojawiły się pierwsze dowody, że niektórych problemów nie da się na niej rozwiązać – na przykład problemu stopu. Oznacza to, że dla niektórych problemów nie da się znaleźć algorytmów, ktore je rozwiązują. Takim właśnie problemem jest dziesiąty problem Hilberta, choć po wprowadzeniu modelu maszyny Turinga potrzeba było jeszcze ponad 30 lat na to, aby wykazać, że maszyna Turinga nie jest w stanie rozstrzygnąć rozwiązywalności dowolnego równania diofantycznego.

6. Trzy ważne definicje

Definicja 3. Podzbiór S zbioru liczb naturalnych nazwiemy *diofantycznym*, jeśli istnieje wielomian $P(k, x_1, x_2, \ldots, x_n)$ o współczynnikach całkowitych posiadający następującą własność:

$$k \in S \iff \exists_{x_1,x_2,\ldots,x_n \in \mathbb{N}} P(k, x_1, x_2, \ldots, x_n) = 0.$$

Dla przykładu, rozważmy równanie Pella:

$$x^2 - dy^2 = 1,$$

gdzie d jest liczbą naturalną. Wiadomo, że równanie to posiada rozwiązanie wtedy i tylko wtedy, gdy d jest równe 0 lub nie jest kwadratem liczby naturalnej. A zatem, wielomian $x^2 - dy^2 - 1$ definiuje zbiór diofantyczny $\{0, 2, 3, 5, 6, 7, 8, 10, \ldots\}$.

Równanie $a = (2x + 3)y$ definiuje zbiór liczb naturalnych, które nie są potęgami liczby 2, zaś równanie $a = (x + 2)(y + 2)$ definiuje zbiór liczb naturalnych, które są większe niż 1 i nie są pierwsze.

Definicja 4. Podzbiór S zbioru liczb naturalnych nazwiemy *rekurencyjnym* (lub *obliczalnym*), jeśli istnieje algorytm, który w skończonym czasie rozstrzyga, czy dana liczba należy do zbioru S, czy też nie.

Dla przykładu, zbiór pusty i zbiór liczb naturalnych są obliczalne w oczywisty sposób, tak samo jak każdy skończony zbiór liczb naturalnych lub każdy zbiór liczb naturalnych o skończonym dopełnieniu. Obliczalny jest też na przykład zbiór liczb pierwszych.

Definicja 5. Podzbiór S zbioru liczb naturalnych nazwiemy *rekurencyjnie przeliczalnym*, jeśli istnieje algorytm, który pobiera na wejściu pewną liczbę naturalną, a następnie zatrzymuje się wtedy i tylko wtedy, gdy ta liczba należy do zbioru S . Równoważnie, istnieje algorytm, który wypisuje elementy zbioru S i w razie potrzeby działa w nieskończoność.

Jasne jest, że każdy zbiór rekurencyjny jest również rekurencyjnie przeliczalny. Odwrotna inkluzja nie jest jednak prawdziwa, czyli istnieją zbiory rekurencyjnie przeliczalne, które nie są rekurencyjne. Konstrukcja takiego zbioru nie jest jednak oczywista, można ją przeprowadzić odwołując się do problemu stopu.

Nietrudno zauważyć, że zbiory diofantyczne są rekurencyjnie przeliczalne. Istotnie, jeśli S jest zbiorem diofantycznym zdefiniowanym przez wielomian $P(k, x_1, x_2 \ldots, x_n)$, to wystarczy aby szukany algorytm wstawiał po kolei wszystkie $(n+1)$-tki liczb całkowitych (bo można oczywiście ustawić je w ciąg) do wielomianu P i wypisywał te wszystkie liczby k, dla których

$$P(k, x_1, x_2, \ldots, x_n) = 0.$$

Nasz algorytm wypisze dokładnie elementy zbioru S.

Co na pierwszy rzut oka może być bardzo zaskakujące, okazuje się, że twierdzenie odwrotne jest również prawdziwe – zbiory rekurencyjnie przeliczalne są diofantyczne.

7. Historia

W 1949 r. matematyk amerykański Martin Davis otrzymał równoważną postać zbiorów rekurencyjnie przeliczalnych, która przypominała definicję zbiorów diofantycznych. Wysnuł na tej podstawie hipotezę, że te dwie klasy zbiorów są w rzeczywistości identyczne. Wykazanie tego rozwiązałoby problem postawiony prawie 50 lat wcześniej przez Hilberta. Jak już bowiem wspomnieliśmy, istnieją zbiory rekurencyjnie przeliczalne, które nie są rekurencyjne, a zatem w szczególności, gdyby te dwie klasy się pokrywały, to istniałby nierekurencyjny zbiór diofantyczny. Załóżmy więc, że S jest takim zbiorem, zdefiniowanym przez wielomian $P(k, x_1, x_2, \ldots, x_n)$. Gdyby istniał algorytm, który rozstrzygałby rozwiązywalność dowolnego równania diofantycznego, to dla danego parametru $k \in \mathbb{Z}$ potrafiłby on stwierdzić, czy $P(k, x_1, x_2, \ldots, x_n) = 0$ przy pewnych $x_1, x_2, \ldots, x_n$. Potrafiłby więc stwierdzić, czy $k \in S$ – ale to stoi w sprzeczności z tym, że zbiór S nie jest obliczalny.

W 1950 r. Julia Robinson, pracując zupełnie niezależnie od Martina Davisa, skoncentrowała się na zbiorach *wykładniczo-diofantycznych*, czyli zdefiniowanych przez równania, w których niewiadome mogą występować w wykładnikach. Starała się udowodnić, że klasa takich zbiorów w rzeczywistości nie jest szersza niż klasa zwykłych zbiorów diofantycznych – czyli że zbiory rozwiązań równań diofantycznych wykładniczych można przedstawić za pomocą zbiorów rozwiązań równań diofantycznych wielomianowych, co z początku może nie wydawać się intuicyjne. Musiała w tym celu udowodnić, że zbiór trójek liczb naturalnych (a, b, c), takich że $a = b^c$, jest zbiorem diofantycznym (w takim sensie, że istnieje wielomian $P(a, b, c, x_1, x_2, \ldots, x_n)$, który zeruje się w pewnym punkcie o początkowych współrzędnych a, b, c wtedy i tylko wtedy, gdy $a = b^c$). Jej próby skończyły się niepowodzeniem, ale postawiła hipotezę, której prawdziwość jest wystarczająca do stwierdzenia, że zbiory wykładniczo-diofantyczne są diofantyczne. Oto jej treść:

Hipoteza 6. *Istnieje taki zbiór diofantyczny D par liczb naturalnych, że jeśli $(a, b) \in D$, to $b < a^a$, ale dla dowolnego $k > 0$ istnieje taka para $(a, b) \in D$, że $b > a^k$.*

Powyższa hipoteza okazała się kluczem do rozwiązania dziesiątego problemu Hilberta.

Dziewięć lat później, w 1959 r., Davis i Hilary Putnam, pracując wspólnie, również skupili swoją uwagę na zbiorach wykładniczo-diofantycznych. Przy założeniu nieudowodniej wówczas

hipotezy, że istnieją dowolnie długie ciągi arytmetyczne złożone z liczb pierwszych (hipoteza ta została udowodniona dopiero w 2004 r. przez B. Greena i T. Tao), wykazali oni, że każdy zbiór rekurencyjnie przeliczalny jest zbiorem wykładniczo-diofantycznym. Rok później Julii Robinson udało się uprościć ich dowód tak, aby uniknąć korzystania z niedowiedzionej hipotezy. Dziesiąty problem Hilberta został więc sprowadzony do wykazania hipotezy postawionej dziesięć lat wcześniej przez Robinson.

Na to potrzeba było następnych dziesięciu lat. W 1970 r. młody matematyk rosyjski Yuri Matiyasevich (mający wówczas 23 lata) podał w swojej rozprawie doktorskiej ostatni fragment dowodu. Znalazł on układ 10 równań diofantycznych pierwszego i drugiego stopnia, które definiują zbiór diofantyczny par (a, b), takich że $b = F_{2a}$, gdzie F_n oznacza n-tą liczbę Fibonacciego. Ten przykład zbioru diofantycznego ostatecznie dowiódł hipotezy postawionej przez Robinson. Tym samym zbiory rekurencyjnie przeliczalne są diofantyczne, a więc istnieją zbiory diofantyczne, które nie są obliczalne, co zamyka dziesiąty problem Hilberta.

8. Podsumowanie

Historia dziesiątego problemu Hilberta kończy się pozytywnie. Po 70 latach problem został rozwiązany dzięki wspólnej i wytężonej pracy kilku matematyków. Wysiłki włożone w wykazanie nieistnienia algorytmu rozstrzygającego rozwiązywalność równań diofantycznych przyczyniły się znacznie do rozwoju działu matematyki zwanego dzisiaj teorią obliczalności (rekursji). Sam Hilbert najprawdopodobniej nie byłby zadowolony z tego, że odpowiedź na jego pytanie jest negatywna. Matematyka nie zawsze jest taka, jak oczekujemy.

Czytelnicy pragnący w większym stopniu zgłębić zagadnienie dziesiątego problemu Hilberta powinni sięgnąć po książkę Yuriego Matiyasevicha *Hilbert's Tenth Problem*. Można dzięki niej poznać kompletne rozwiązanie problemu zaczynając z bardzo podstawową wiedzą. Zawiera ona ponadto wiele cennych komentarzy i uwag na temat pokrewnych zagadnień.

Literatura

[1] Yuri V. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, Cambridge, Massachusetts, 1993.

Paradoksy logiczne i matematyczne

Maciej Malaczewski, Paulina Pabiańska

Streszczenie. Celem niniejszej pracy jest prezentacja kilkunastu najciekawszych paradoksów logicznych i matematycznych. Omówione zostaną: paradoks kół Arystotelesa, róg Gabriela, paradoks stosu, paradoks Bertranda oraz kilka innych.

1. Co to jest paradoks?

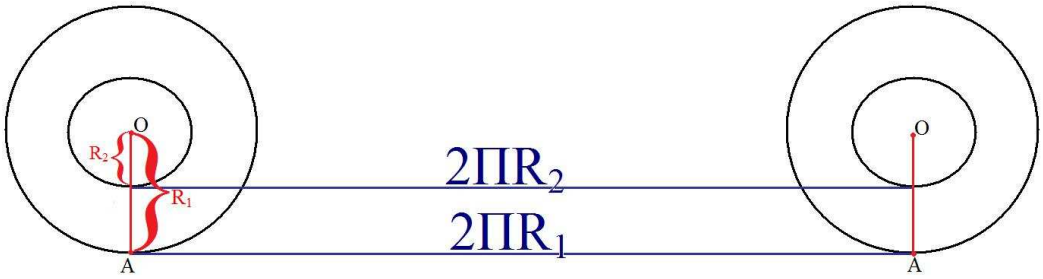
paradoks (gr. *paradoksos* 'sprzeczny z powszechnym mniemaniem') 1. *pot.* 'twierdzenie, pogląd niewiarygodny, zaskakujący; również rozumowanie prowadzące do takich wniosków' 2. 'twierdzenie, pogląd niezgodne z mniemaniem danej grupy ludzi; ten sam pogląd może być paradoksem dla jednej grupy ludzi, a nie być nim dla innej' 3. 'antynomia' 4. 'zaskakujące, często w warstwie literalnej wewnętrznie sprzeczne sformułowanie, z którego dopiero właściwa interpretacja znaczeń, przenośni, idiomów itp. wydobywa – często uderzająco trafną, intrygującą – ogólną myśl, obserwację, hasło itp.'

2. Paradoks kół Arystotelesa

Jednym z najciekawszych paradoksow jest problem poruszony przez Arystotelesa w *Mechanice*. Arystoteles rozważa dwa współśrodkowe koła o promieniach R_1 i R_2, gdzie $R_2 < R_1$. Koła te są sztywno połączone, dlatego żadne z nich nie może wykonać jakiegokolwiek ruchu, gdy drugie się nie poruszy. Po tej prostej obserwacji Arystoteles zadaje pytanie: jaką drogę pokonują te koła podczas pełnego obrotu wokół własnej osi – czy drogę, którą rozwija mniejsze z tych kół, równą $2\pi R_2$, czy trasę rozwijaną przez większe koło, równą $2\pi R_1$? Problem ten ilustruje rysunek 1. Powyższe rozumowanie prowadzi do paradoksalnego wniosku, że $2\pi R_1 = 2\pi R_2$, co jest niezgodne z naszym założeniem, że $R_2 \neq R_1$. Zatem równość $2\pi R_1 = 2\pi R_2$ nie może zachodzić. Jaką więc drogę przebywają te koła?

dr Maciej Malaczewski
mmalaczewski@uni.lodz.pl
Instytut Ekonomii
Uniwersytet Łódzki

Paulina Pabiańska
ppabianska@gmail.com
studentka ekonomii
Uniwersytet Łódzki



Rysunek 1. Paradoks kół Arystotelesa

3. Piłeczka od tenisa i kula ziemska

Paradoks ten ma za zadanie zobrazować zwodniczość naszej intuicji. W tym celu rozważmy dwie kule: K_1 o wielkości w przybliżeniu równej kuli ziemskiej (i promieniu $R_1 = 6300000$ m) oraz kulę K_2 o wielkości piłeczki tenisowej (czyli promieniu $R_2 = 3$ cm $= 0{,}03$ m). Następnie kule K_1 i K_2 otaczamy wzdłuż ich największych obwodów taśmą o 1 m dłuższą od tych obwodów, czyli o długości odpowiednio $2\pi R_1 + 1$ m oraz $2\pi R_2 + 1$ m. Jaka jest odległość między taśmą rozpiętą wokół równików tych kul a powierzchnią kul? Intuicja podpowiada, że w przypadku kuli mniejszej odległość od równika do taśmy powinna być większa niż w przypadku kuli większej. Tymczasem po wykonaniu prostych rachunków okazuje się, że odległość ta wcale nie zależy od promienia kuli! Rzeczywiście, jeżeli przez R_1^* oznaczymy promień okręgu utworzonego przez taśmę, o środku równym środkowi kuli K_1 (analogicznie R_2^* dla kuli K_2), to dostajemy:

$$R_1^* = \frac{2\pi R_1 + 1\text{ m}}{2\pi} = R_1 + \frac{1\text{ m}}{2\pi},$$

$$R_2^* = \frac{2\pi R_2 + 1\text{ m}}{2\pi} = R_2 + \frac{1\text{ m}}{2\pi}.$$

Zatem zarówno dla kuli K_1, jak i dla K_2 odległość ta jest równa $\frac{1\text{ m}}{2\pi}$ i zależy wyłącznie od dodanej długości do taśmy.

4. Czarny kruk

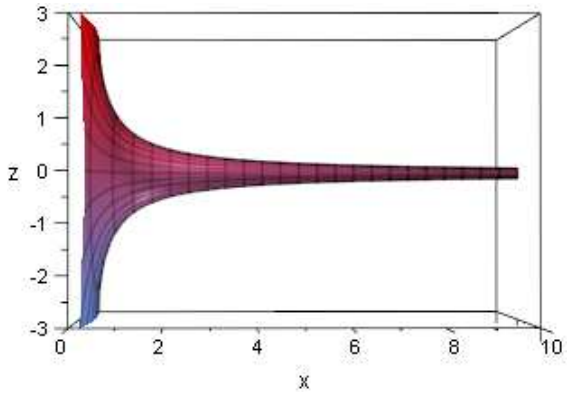
Załóżmy, że chcemy przekonać się, że wszystkie kruki są czarne. Oczywiście, *de facto*, powinniśmy obejrzeć wszystkie kruki na świecie i zobaczyć, jakiego są koloru, by móc to stwierdzić. Oglądanie jednak kolejnych kruków i stwierdzanie prostego faktu, że są czarne, podnosi nasze przekonanie o tym, iż zdanie „wszystkie kruki są czarne" jest prawdziwe. Prowadzi to jednak do ciekawego wniosku logicznego. Zdanie „Wszystkie kruki są czarne" jest równoważne zdaniu „wszystko, co nie jest czarne, nie jest krukiem". Jeżeli zatem widzimy, np. szarego bądź różowego słonia, zielone jabłko, żółte słońce, to ich widok podnosi nasze przekonanie o prawdziwości zdania

„wszystko, co nie jest czarne, nie jest krukiem”, a tym samym o prawdziwości zdania „wszystkie kruki są czarne”.

5. Róg Gabriela

Pojęcie nieskończoności, mimo iż pozostaje w zgodzie z zasadami logicznego rozmuowania, należy do najmniej intuicyjnych konstrukcji z matematyce. Wprowadzenie idei np. szeregów zbieżnych i rozbieżnych jest oczywiście matematycznie poprawne, ale intuicyjnie trudne do zrozumienia. Można np. wskazać istnienie figury, zwanej rogiem Gabriela, która ma skończoną objętość, ale nieskończone pole powierzchni bocznej.

Róg Gabriela powstaje poprzez obrót wokół osi x wykresu funkcji $\frac{1}{x}$ na dziedzinie od 1 do nieskończoności (rysunek 2).



Rysunek 2. Róg Gabriela

Objętość V i pole powierzchni bocznej A dla tej figury od 1 do pewnego punktu a dane są wzorami:

$$V = \pi \int_1^a \frac{1}{x^2} dx = \pi(1 - \frac{1}{a}),$$

$$A = 2\pi \int_1^a \frac{\sqrt{1 + \frac{1}{x^4}}}{x} dx > 2\pi \int_1^a \frac{\sqrt{1}}{x} dx = 2\pi \ln a.$$

Przechodząc z a do granicy w nieskończoności, otrzymujemy:

$$\lim_{a \to +\infty} \pi(1 - \frac{1}{a}) = \pi,$$

$$\lim_{a \to +\infty} 2\pi \ln a = +\infty.$$

6. Paradoks nauczyciela prawa

Anegdota ta podobno miała rzeczywisty przebieg w dawnej Grecji. Protagoras wziął do siebie na naukę sztuki prawniczej ucznia Euathlosa. Mistrz Protagoras nie przyjął od Euathlosa od razu zapłaty za swe nauki, umawiając się z nim, że Euathlos zapłaci należną kwotę jedynie wtedy, gdy wygra swój pierwszy proces sądowy. Jednak nauka się skończyła, a Euthalos wciąż nie przyjmował żadnego procesu. Czas mijał i sytuacja nie ulegała zmianie. W końcu zdenerwowany Protagoras postanowił zaskarżyć swego krnąbrnego ucznia do sądu. Przed sądem miała miejsce taka oto wymiana argumentów pomiędzy pozywającym i pozwanym:

Protagoras:

„Albo Euathlos ten proces, który jest jego pierwszym procesem, wygra, albo przegra. Jeśli go wygra, to winien mi zapłacić na mocy umowy, która zobowiązuje go do zapłaty, jeśli swój pierwszy proces wygra. Jeśli go zaś przegra, to winien mi zapłacić na mocy wyroku sądowego".

Euthalos:

„Albo ja, Euthalos, proces wygram, albo przegram. Jeśli go wygram, to znaczy, iż wyrok sądowy uwolni mnie od obowiązku zapłaty, jeśli przegram, to wobec umowy, która zobowiązywała mnie do zapłaty tylko w wypadku, gdybym mój pierwszy proces wygrał, od obowiązku zapłaty będę wolny".

Kto miał rację?

7. Paradoks stosu

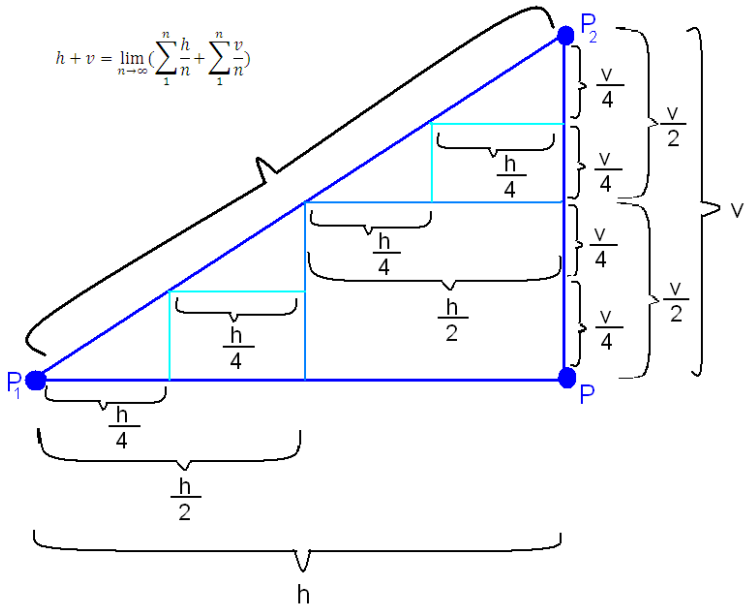
Autorem tego paradoksu jest Eubulides z Miletu. Przypuśćmy, że mamy kopiec 30000 ziaren. Tworzy on stos. Usuńmy teraz jedno ziarenko z tego kopca. Otrzymany kopiec jest bardzo podobny do poprzedniego – również stwierdzamy, że tworzy on stos. W kolejnych krokach usuwamy kolejne ziarenka. Otrzymywane kopce ciągle tworzą stos. Postępując dalej konsekwentnie w ten sposób, zmuszeni jesteśmy przyznać, że po 29999. kroku, pozostałe jedno ziarenko także tworzy stos.

Bardzo podobny do paradoksu stosu jest paradoks łysego, który również opiera się na zagadnieniu różnic minimalnych. Pojawia się tu bowiem problem braku ostrości definicji.

8. Antypitagoras

Załóżmy, że rozważamy drogę pomiędzy punktami P_1 i P_2. Oczywiście istnieje taki punkt P, przez który droga pomiędzy tymi punktami przebiega pod kątem prostym. Niech odległość od punktu P_1 do punktu P wynosi h, a między P i P_2 – v. Zmierzając zatem od P_1 do P_2 przez punkt P, pokonujemy drogę $h + v$. Teraz zauważmy, że możemy podzielić drogę z P_1 do P_2 na dwie równe części i dla każdej z nich również znaleźć analogiczne do punktu P punkty tak, by (jak na rysunku) droga była równa dokładnie $h/2 + v/2 + h/2 + v/2 = h + v$. Teraz można każdą z połówek drogi podzielić jeszcze na pół itd. – dzielimy drogę z P_1 do P_2 na coraz mniejsze kawałki. Cały czas

jednak droga okrężna wynosi $h + v$. Przechodząc do granicy, otrzymujemy, że droga pomiędzy P_1 i P_2 jest równa $h + v$.



Rysunek 3. Antypitagoras

9. Paradoks Bertranda

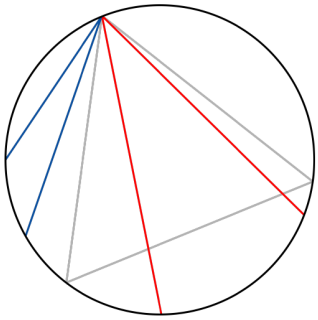
Na okręgu o promieniu równym 1 skonstruowano losowo cięciwę OP. Jaka jest szansa, że cięciwa będzie dłuższa, niż bok trójkąta równobocznego wpisanego w ten okrąg?

(i) Za zdarzenie elementarne przyjmujemy wybór kąta α, tworzonego przez środek okręgu oraz punkty O i P (rysunek 4).

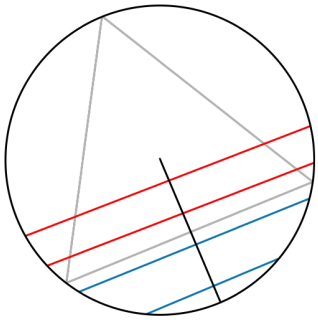
- $\Omega = [0, \pi]$
- Zdarzenie sprzyjające $A = [\frac{2}{3}\pi, \pi]$
- $P(A) = \frac{1}{3}$

(ii) Za zdarzenie elementarne przyjmujemy odległość środka skonstruowanej cięciwy od środka okręgu (rysunek 5).

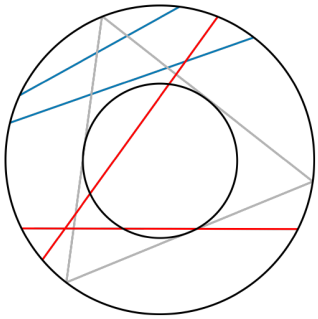
- $\Omega = [0, 1]$
- Zdarzenie sprzyjające $B = [0, \frac{1}{2}]$
- $P(B) = \frac{1}{2}$



Rysunek 4. Paradoks Bertranda, A



Rysunek 5. Paradoks Bertranda, B



Rysunek 6. Paradoks Bertranda, C

(iii) Za zdarzenie elementarne przyjmujemy wybór dowolnego punktu wewnątrz naszego koła. Zdarzenie sprzyjające zachodzi, gdy wybrany punkt znajdzie się wewnątrz koła wpisanego w rozważany trójkąt równoboczny (rysunek 6).

- $\Omega = K(0,1)$
- Zdarzenie sprzyjające $C = K(0, \frac{1}{4})$
- $P(C) = \frac{1}{2}$

10. Paradoks petersburski

Paradoks petersburski pochodzi od Daniela Bernoullego. Nie jest to paradoks w ścisłym sensie tego słowa. Za to pokazuje on, że w warunkach niepewności istnieją sytuacje, w których ludzie nie zachowują się racjonalnie z punktu widzenia kryterium maksymalizacji pieniężnej wartości oczekiwanej.

Rozważmy grę losową, która polega na rzucie symetryczną monetą. Trwa ona do czasu otrzymania pierwszego orła. Jeżeli już w pierwszym rzucie pojawił się orzeł, to gracz otrzymuje nagrodę w wysokości 1 zł. Jeżeli natomiast w pierwszym rzucie wyrzucono reszkę, a orła dopiero w drugim, wygrana gracza zostaje podwojona i wynosi 2 zł. Każde opóźnienie wyrzucenia orła skutkuje dalszymi podwojeniami wygranej gracza. Zatem wygrana gracza wynosi ogólnie $w_i = 2^{i-1}$ zł, gdzie i to numer rzutu, w którym otrzymano orła. Łatwo wyliczyć również prawdopodobieństwo p_i wyrzucenia orła po raz pierwszy w i-tym rzucie. Wynosi ono $p_i = \frac{1}{2^i}$.

Pytanie, jakie zadaje Bernoulli, związane jest z wysokością wpisowego, które należy uiścić przed przystąpieniem do gry. Do jakiej wysokości wpisowego potencjalnym graczom opłaca się przystąpienie do gry? Aby odpowiedzieć na to pytanie, obliczmy wartość oczekiwaną gry:

$$EX = \sum_{i=1}^{+\infty} p_i w_i = \sum_{i=1}^{+\infty} \frac{1}{2^i} 2^{i-1} = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots = +\infty.$$

Zatem uczestnik gry kierujący się maksymalizacją wartości oczekiwanej powinien zdecydować się uczestniczyć w grze niezależnie od tego, ile musi zapłacić wpisowego. Pomimo tego, większość ludzi nie zdecydowałaby się w niej uczestniczyć już wtedy, gdyby koszt ten przewyższał 25 zł.

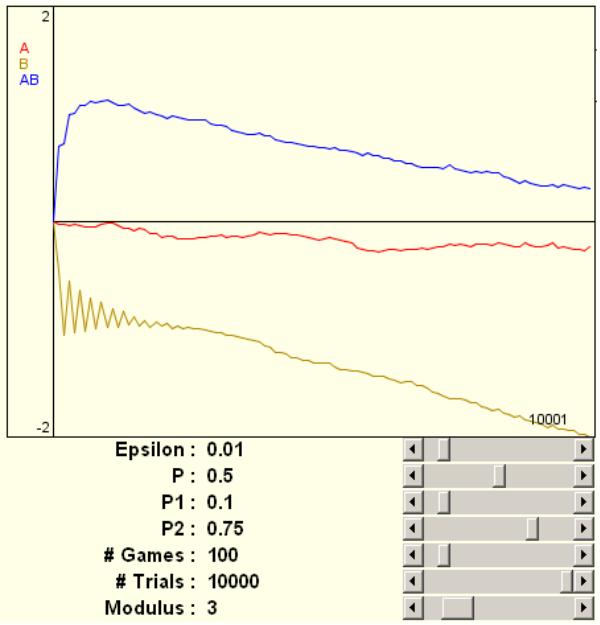
11. Parodoks gier Parrondo

Autorem jest Juan Parrondo. Zaczynamy z zerowym dorobkiem. Załóżmy, że mamy dwie gry. Obie polegają na rzucaniu obciążoną monetą:

- W grze A z prawdopodobieństwem 0,49 wygrywamy 1, z prawdopodobieństwem 0,51 – przegrywamy 1.

- W grze B rozpoczynamy od obserwacji, czy nasz aktualny kapitał jest całkowitą wielokrotnością liczby 3.
  - Jeśli tak – rzucamy monetą z prawdopodobieństwem wygrania i uzyskania 1 równym 0,09 oraz prawdopodobieństwem porażki i straty 1 równym 0,91.
  - Jeśli nie – rzucamy monetą z prawdopodobieństwem wygrania i uzyskania 1 równym 0,74 oraz prawdopodobieństwem porażki i straty 1 równym 0,26.

Nietrudno zauważyć, że gra A jest daje w długim okresie przegraną. Podobnie gra B (przeciętne prawdopodobieństwo wygranej jest równe 0,491308). Jeżeli jednak będziemy grać w te dwie gry kolejno jedna po drugiej (ABABABAB itd.), to tak skonstruowana gra w długim okresie ma prawdopodobieństwo wygranej 0,503011. Rysunek 7 pokazuje zysk w poszczególnych grach w przykładowej symulacji.



Rysunek 7. Parodoks gier Parrondo

12. Antynomia Richarda

Załóżmy, że mamy listę definicji określających różne własności liczb naturalnych, np. bycie liczbą parzystą. Listę tę porządkujemy, np. według długości definicji lub alfabetycznie. Każdą kolejną pozycję numerujemy kolejnymi liczbami naturalnymi. Może się zdarzyć, że liczba odpowiadająca kolejnej pozycji spełnia definicję pod tym numerem zawartą, np. liczba 15 spełnia piętnastą z kolei definicję pewnej własności. Taką liczbę nazywamy *nierichardowską*, a wszystkie pozostałe liczby

nazwiemy *richardowskimi*. Oczywiście „bycie liczbą richardowską" też jest definicją, a zatem definicja ta także znajduje się na liście i ma pewien kolejny numer. Czy liczba odpowiadająca temu numerowi będzie richardowska? Jeśli jest to liczba richardowska, to nie ma własności bycia liczbą richardowską. Jeśli nie jest richardowska, to ma własność określoną przez definicję, jest zatem richardowska.

13. Paradoks Curry'ego

Autorem tego paradoksu jest Haskel Curry. Jest to typowy paradoks logiczny, nieco przypominający antynomię kłamcy. Curry proponuje, aby rozważyć zdanie: „jeśli to zdanie jest prawdziwe, to słońce jest czarne". Jest to implikacja o poprzedniku p: „to zdanie jest prawdziwe" i następniku q: „słońce jest czarne". Codzienne doświadczenie podpowiadają nam, że słońce nie jest czarne, zatem to zdanie musi być fałszywe. Z podstaw logiki zaś wiemy, że implikacja jest fałszywa tylko wtedy, gdy prawda implikuje fałsz. Zatem poprzednik p musi być prawdziwy. Orzeka on jednak, że to zdanie jest prawdziwe. Jednakże prawdziwe być nie może, ponieważ słońce nie jest czarne. Zatem p nie jest prawdziwe. W implikacji z fałszu wynika zawsze prawda, więc słońce jednak jest czarne... itd.

Literatura

[1] K. Ajdukiewicz (1931), *Paradoksy starożytnych*, w: *Język i poznanie*, t. 1, Wydawnictwo Naukowe PWN, Warszawa 1985, s. 135–144.

[2] A. Bogolmolny, *Parrondo Paradox* from Interactive Mathematics Miscellany and Puzzles `http://www.cut-the-knot.org/ctk/Parrondo.shtml`.

[3] T. Kühne, *The "No Shortcuts" Paradox* `http://homepages.ecs.vuw.ac.nz/~tk/no-shortcuts/`.

[4] P. Łukowski, *Paradoksy*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2006.

[5] T. Nadzieja, *Galileusz (1564–1642)*, „Matematyka" 2005, nr 2. Dostępny w internecie: `http://www.math.uni.opole.pl/~tnadzieja/Galileusz.pdf`.

[6] E. Piotrowski, *Problemy z paradoksem Astumiana*, 30 sierpnia 2004. Dostępny w internecie: `http://alpha.uwb.edu.pl/ep/RePEc/sla/eakjkl/121PL.pdf`.

Co to jest czas?

Piotr Mironowicz

1. Motywacja logik temporalnych

Problem: czym właściwie jest czas nurtował uczonych już od starożytności. Ma on tak długą historię jak pierwsze rozważania dotyczące logiki klasycznej.

1.1. Problemy związane z opisem czasu

Rozważmy następujące rozumowanie:

(i) Każde zdanie może być albo prawdziwe, albo fałszywe.

(ii) W szczególności każde zdanie dotyczące przyszłości jest albo prawdziwe, albo fałszywe.

(iii) Zatem z całą pewnością zdarzy się wszystko opisywane przez zdania prawdziwe i nie może się zdarzyć nic opisanego przez zdanie fałszywe.

(iv) Zatem wszystko, co można opisać zdaniami, dzieje się z konieczności.

Pogląd głoszący, że wszystko, co się dzieje, dzieje się z konieczności, nazywany jest *fatalizmem*.

Jednym z wczesnych krytyków fatalizmu był Arystoteles. W dziele *Hermeneutyka* stwierdza, że „nie jest konieczne, ażeby każde twierdzenie czy przeciwne mu przeczenie musiało być jedno prawdziwe, a drugie fałszywe". Zdaniem Arystotelesa zasada sprzeczności odnosi się do tego, co istnieje, a nie do tego, co może być lub nie być.

Do poglądów Arystotelesa należało również przypisywanie Wszechświatowi wiecznego istnienia, gdyż materia, z której się składa, nie mogła być wynikiem rozwoju (materia sama jest warunkiem rozwoju).

Piotr Mironowicz
piotr.mironowicz@gmail.com
student matematyki
Politechnika Gdańska

Znacznie bardziej radykalne od fatalizmu poglądy głosili eleaci. Zaprzeczali oni mianowicie możliwości wszelkiej zmiany. Najważniejszy ich przedstawiciel, Zenon z Elei (V wiek p.n.e.), jest autorem kilku znanych paradoksów, m.in.: żółwia i Achillesa, strzały, dychotomii oraz stadionu.

Efektownie zostały one obalone przez Diogenesa z Synopy, a następnie wyjaśnione przez matematyków. Diogenes, usłyszawszy o „dowodach" niemożliwości wszelkiej zmiany, powiedział, że udowodni, iż dowody te nie są prawdziwe, po czym odskoczył w bok i stwierdził, że zmiany są możliwe.

Diodorus był greckim filozofem żyjącym na przełomie IV i III wieku p.n.e. Jego przydomek „Cronus" znaczy mniej więcej „stary piernik" [3]. Inaczej niż eleaci, nie zaprzeczał istnieniu zmian, jednak utrzymywał, że nie można wskazać chwili w czasie, w których one zaszły. Diodorus dowodził jedynie tego, że wszelki ruch jest niemożliwy. Wśród licznych jego paradoksów szczególnie ciekawe są poniższe:

(i) Jeśli coś się porusza, to albo porusza się w tym miejscu, w którym jest, albo w tym, do którego się porusza. W tym drugim nie może się poruszać, bo go tam nie ma. W tym pierwszym również nie może się poruszać, bo zajmuje je całe.

(ii) To, co się porusza, jest w jakimś miejscu, jednak będąc w miejscu, nie można się poruszać.

Paradoks (ii) pokrewny jest paradoksowi strzały Zenona z Elei.

Duży wkład w logikę temporalną wniósł doktor Kościoła – Święty Augustyn (354–430). Mówił on (w dużym skrócie), że przeszłości już nie ma, a przyszłości jeszcze nie ma. Teraźniejszość nie ma charakteru trwania, natomiast czas ma taki charakter. Zatem nie ma czasu teraźniejszego. Ponieważ nie ma też przyszłości ani przeszłości, zatem nie ma czasu w ogóle. Podobną argumentację stosował Arystoteles.

W zasadzie większość kwestii poruszanych w późniejszych okresach związanych z czasem w ten czy inny sposób widoczna była u Augustyna. Rozważał problemy Wieczności, początku i końca czasu, a także istotną kwestię „szybkości" trwania czasu. Rozważania dotyczące natury czasu podjęła następnie w średniowieczu scholastyka.

Bezpośrednią motywacją skłaniającą Łukasiewicza do utworzenia pierwszej logiki wielowartościowej były jego poglądy dotyczące wolności woli. Był on indeterministą i „atak" na dwuwartościowość logiki stanowił atak na fatalizm.

W artykule z 1920 r. *O logice trójwartościowej* Łukasiewicz rozważa zdanie „Od dziś za rok będę w Warszawie". Jako zwolennik wolności woli Łukasiewicz twierdzi, że nie można przypisać temu zdaniu wartości logicznej prawdy ani fałszu. Wprowadza zatem pośrednią wartość logiczną, $\frac{1}{2}$, którą nazywa „możliwością".

Łukasiewicz definiuje spójniki logiczne negacji i implikacji w sposób przedstawiony w tablicach 1 i 2. Za pomocą tych dwóch spójników można wprowadzić pozostałe trzy.

f	$\neg f$
0	1
$\frac{1}{2}$	$\frac{1}{2}$
1	0

Tablica 1. Tabela prawdziwościowa negacji trójwartościowej logiki Łukasiewicza.

$\Longrightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	0	$\frac{1}{2}$	1

Tablica 2. Tabela prawdziwościowa implikacji trójwartościowej logiki Łukasiewicza.

1.2. Redukcjonizm vs. platonizm

Inną istotną kwestią podnoszoną w sprawie czasu był spór między stanowiskami zwanymi redukcjonizmem i platonizmem[1]. Poniższa problematyka została opisana szczegółowiej w [2].

Spór ten związany jest z próbą odpowiedzi na pytania takie jak:

(i) Czy czas może istnieć bez zmiany?

(ii) Czy możemy w jakikolwiek sposób wykluczyć, że w pewnym momencie cały ruch na świecie zatrzymał się całkowicie na milion lat?

(iii) Czy ma sens przyjmowanie, że czas płynął, jeśli nie zachodziła żadna zmiana?

Redukcjonizm stwierdza, że czas nie może płynąć, jeśli nie zachodzą w świecie żadne zmiany. Pogląd ten szczególnie bliski jest pozytywistom, dla których bez sensu jest przyjmowanie istnienia czegoś, czego nie można zmierzyć ani zaobserwować. Wszak jeśli nie zaszłyby żadne zmiany, to również zegary by się nie przesunęły, czyli nie ma empirycznej możliwości, aby stwierdzić, że czas upłynął.

Przeciwną odpowiedź daje platonizm. Stanowisko to głosi, że czas istnieje niezależnie od tego, czy zmiany zachodzą, czy nie.

Dla obrony platonizmu Sydney Shoemaker opisuje następującą sytuację wskazującą, że idea mówiąca, iż w pewnym momencie wszelka zmiana ustaje na jakiś czas, a czas płynie wciąż, jest jak najbardziej sensowna.

[1] Zarówno „redukcjonizm”, jak i „platonizm” są określeniami na pewne stanowiska w różnych kwestiach filozoficznych. Tutaj chodzi oczywiście o redukcjonizm lub platonizm w pojmowaniu natury czasu.

Niech dane będą trzy sąsiadujące ze sobą części świata. W jednej raz na 2 lata zachodzi niezwykłe zjawisko: przedmioty zaczynają lśnić na czerwono, po czym ruch w niej całkowicie zamiera tak, że nie można się do niej nawet dostać. W pozostałych dwóch częściach świata wszystko w tym czasie dzieje się normalnie, a po godzinie (mierzonej z tych dwóch części świata) ruch w pierwszej części jest kontynuowany.

W drugiej części identyczne zjawisko następuje raz na 3 lata, a w trzeciej raz na 5 lat.

Wynika stąd, że raz na 30 lat zjawisko lśnienia na czerwono zachodzi we wszystkich trzech częściach, jednak tym razem nikt nie obserwuje zamierania ruchu, gdyż zamarł on tak samo we wszystkich trzech częściach świata.

Sensownie jest przyjąć, że czas płynie przez ową godzinę mimo braku jakichkolwiek zmian.

2. Logiki modalne

W celu matematycznego podejścia do problemów związanych z czasem i opisem upływu czasu powstały tzw. logiki temporalne.

Logiki temporalne są jednymi z tzw. logik modalnych, dlatego zaczniemy od wprowadzenia ogólnego formalizmu.

2.1. Formalizm logik modalnych

Szczegółowy opis logik modalnych, w tym logik temporalnych, znajduje się w [4].

Kluczową ideą dla logik modalnych jest pojęcie tzw. „światów możliwych", a także zdań koniecznych i możliwych. Do zapisania tego, że dane zdanie jest możliwe, stosuje się zazwyczaj symbol $\Diamond$ (np. $\Diamond f$ oznacza, że możliwe jest f). Podobnie dla oznaczenia, że dane zdanie jest konieczne, stosuje się symbol $\Box$.

Nietrudno zauważyć, że pojęcia te są wzajemnie definiowalne. Możliwe jest to, dla czego nie jest konieczne, aby nie było ($D_\Diamond : \Diamond p \iff \neg\Box\neg p$). Podobnie można definiować konieczność, jako niemożliwość, by coś nie było.

W kontekście czasowym symbol $\Diamond$ rozumie się często jako „w pewnej chwili w przyszłości", zaś $\Box$ jako „w przyszłości zawsze będzie zachodzić".

W celu matematycznego wyjaśnienia, czym są światy możliwe, wprowadza się pojęcie struktury relacyjnej:

Definicja 1 (Struktura relacyjna)**.** Niech U będzie niepustym zbiorem, $R \subseteq U \times U$ relacją. Parę $\langle U, R\rangle$ nazywa się *strukturą relacyjną*, zbiór U nazywa się *uniwersum* lub *zbiorem światów*. Elementy $u \in U$ nazywa się *światami*, a w kontekście czasowym *stanami świata* lub *momentami historycznymi*, zaś R nazywa się *relacją osiągalności* lub *relacją następowania*.

W kontekście czasowym relacja R określa następstwo stanów świata po sobie, zaś strukturę relacyjną nazywa się *strukturą czasową*.

Gdy ustalony jest zbiór światów, należy jeszcze ustalić przeliczalny zbiór zmiennych zdaniowych $V = \{p, q, r, \ldots\}$ oraz funkcję $V\colon V \to 2^U$, zwaną *wartościowaniem*, która przyporządkowuje każdej zmiennej zdaniowej podzbiór światów, w których jest ona spełniona.

Mając zdefiniowane wartościowanie V, wprowadza się następujące bardzo ważne pojęcie:

Definicja 2 (Model Kripkego)**.** Niech U będzie niepustym zbiorem, $R \subseteq U \times U$ relacją, a V wartościowaniem modelu Kripkego. Wtedy trójkę $\mathcal{M} = \langle U, R, V\rangle$ nazywamy *modelem Kripkego*, lub w skrócie *modelem*, a w kontekście czasowym – *historią*.

Historię, a także strukturę czasową, oznacza się często jako $\mathcal{T}$.

Mając zdefiniowany model, wprowadza się dość intuicyjne pojęcie spełnienia danej formuły w danym modelu.

Stwierdzenie, że formuła f jest *spełniona* w świecie u modelu $\mathcal{M}$, zapisuje się symboliczne jako $(\mathcal{M}, u) \vDash f$.

Formalna definicja spełnienia jest rekurencyjna. Dla poszczególnych spójników logicznych wprowadza się następujące warunki:

(i) $(\mathcal{M}, u) \vDash p$ wtedy i tylko wtedy, gdy $u \in V(p)$,

(ii) $(\mathcal{M}, u) \vDash \neg f$ wtedy i tylko wtedy, gdy: nieprawda, że $(\mathcal{M}, u) \vDash f$,

(iii) $(\mathcal{M}, u) \vDash f_1 \wedge f_2$ wtedy i tylko wtedy, gdy: $(\mathcal{M}, u) \vDash f_1$ i $(\mathcal{M}, u) \vDash f_2$,

(iv) $(\mathcal{M}, u) \vDash f_1 \vee f_2$ wtedy i tylko wtedy, gdy: $(\mathcal{M}, u) \vDash f_1$ lub $(\mathcal{M}, u) \vDash f_2$,

(v) $(\mathcal{M}, u) \vDash f_1 \implies f_2$ wtedy i tylko wtedy, gdy: jeśli $(\mathcal{M}, u) \vDash f_1$, to $(\mathcal{M}, u) \vDash f_2$,

(vi) $(\mathcal{M}, u) \vDash f_1 \iff f_2$ wtedy i tylko wtedy, gdy: $(\mathcal{M}, u) \vDash f_1$ wtedy i tylko wtedy, gdy $(\mathcal{M}, u) \vDash f_2$.

Dla symboli modalnych $\Box$ i $\Diamond$ spełnienie definiuje się w następujący sposób:

(i) $(\mathcal{M}, u) \vDash \Box f$ wtedy i tylko wtedy, gdy: dla każdego $t \in U$ jeśli uRt, to $(\mathcal{M}, t) \vDash f$,

(ii) $(\mathcal{M}, u) \vDash \Diamond f$ wtedy i tylko wtedy, gdy: istnieje $t \in U$, uRt, takie że $(\mathcal{M}, t) \vDash f$.

Gdy zdefiniowane jest pojęcie spełnienia w danym świecie, można zdefiniować spełnienie na całym modelu Kripkego. Mianowicie mówimy, że dana formuła jest *spełniona w modelu* $\mathcal{M}$, gdy jest spełniona w każdym świecie tego modelu.

Uogólniając nieco pojęcie spełnienia, można wprowadzić pojęcie *spełnienia w strukturze*. Mówimy o nim, gdy dana formuła jest spełniona w danym modelu przy dowolnym wartościowaniu V.

Jeszcze ogólniej mówimy, że f jest *spełniona w klasie struktur* wtedy i tylko wtedy, gdy jest spełniona w każdej strukturze tej klasy.

W logikach modalnych wprowadza się następujące typowe schematy[2] aksjomatów:

[2] Określenie „schemat aksjomatów” należy rozumieć jako zbiór wszystkich formuł przyjmujących daną postać.

(i) K: $\Box(p \implies q) \implies (\Box p \implies \Box q)$,

(ii) T: $\Box p \implies p$,

(iii) D: $\Box p \implies \neg\Box\neg p$,

(iv) 4: $\Box p \implies \Box\Box p$,

(v) B: $p \implies \Box\neg\Box\neg p$,

(vi) 5: $\neg\Box p \implies \Box\neg\Box p$.

Jako schemat aksjomatów często przyjmuje sie definicję możliwości za pomocą konieczności:

$$D_\Diamond : \Diamond p \iff \neg\Box\neg p.$$

Szczególnie ważny schemat K można odczytać następująco: jeśli konieczna jest implikacja $p \implies q$ i konieczne jest p, to konieczne jest też q.

Dla określenia logiki oprócz aksjomatów potrzebne również jest określenie dozwolonych reguł, za pomocą których z jednych zdań można wyciągać wnioski o innych zdaniach. W logikach modalnych często stosuje się następujące reguły wnioskowania:

Reguła 1 (Odrywania (MP)). Jeśli zachodzi p i $p \implies q$, to zachodzi również q.

Reguła 2 (Regularność (RR)). Jeśli zachodzi $p \implies q$, to zachodzi również $\Box p \implies \Box q$.

Reguła 3 (Konieczność (RN)). Jeśli zachodzi p, to zachodzi również $\Box p$.

2.2. System $\mathcal{K}$

Jednym z najprzydatniejszych systemów logik modalnych jest tzw. system $\mathcal{K}$.

Definiuje się go jako następujący zbiór schematów aksjomatów i reguł wnioskowania:

$$\mathcal{K} = \{K, D_\Diamond; MP, RN\}.$$

Pominięto w tym zapisie zbiór aksjomatów klasycznego rachunku zdań, jednak przyjmuje się, że każda logika modalna zawiera wszystkie schematy klasyczne.

System $\mathcal{K}$ zawiera zatem przede wszystkim schemat K, czyli:

$$\Box(p \implies q) \implies (\Box p \implies \Box q),$$

oraz regułę konieczności (jeśli zachodzi p, to zachodzi również $\Box p$).

Można udowonić, że zachodzi następujące twierdzenie:

Twierdzenie 3 (Twierdzenie o pełności systemu $\mathcal{K}$)**.** *Dla dowolnej formuły języka logiki modalnej f zachodzi: f jest twierdzeniem (posiada dowód) systemu $\mathcal{K}$ wtedy i tylko wtedy, gdy dla każdej struktury relacyjnej $\mathcal{A}$ jest $\mathcal{A} \vDash f$.*

Innymi słowy, pełność systemu $\mathcal{K}$ względem klasy wszystkich struktur relacyjnych oznacza, że dana formuła posiada dowód za pomocą aksjomatów i reguł systemu $\mathcal{K}$ wtedy i tylko wtedy, gdy ta formuła spełniona jest w każdej ze struktur relacyjnych.

Kwestia pełności różnych systemów modalnych względem określonych klas struktur (np. struktur, w których relacja R jest zwrotna) jest ważnym zagadnieniem logiki modalnej.

3. Logiki temporalne

Jak wspomniano wyżej, logiki modalne dostarczają niebędnego aparatu do wprowadzenia logik temporalnych, służących do opisu czasu. Opis logik temporalnych znaleźć można w [4] i [1].

Historycznie pierwszą logiką temporalną była tzw. *logika czasowa* (ang. *Tense Logic*). Została ona zaproponowana przez 38-letniego wówczas Artura Priora, którego zainspirowały z kolei prace Jana Łukasiewicza i dominikanina Józefa Marii Bocheńskiego.

Artur Prior wprowadził do logiki opisane dalej symbole F, P, G i H.

3.1. Relacja następowania

Aby odzwierciedlić intuicje dotyczące upływu czasu, od relacji R w modelu (historii) wyrażającej następstwo w czasie stanów świata wymaga się, aby była ona:

(i) przeciwzwrotna (chwila nie następuje po sobie samej),

(ii) przeciwsymetryczna (jeśli jedna chwila następuje po drugiej, to druga nie następuje po pierwszej),

(iii) przechodnia (jeśli jedna chwila następuje po drugiej, a druga po trzeciej, to ta pierwsza następuje też po trzeciej).

Relację taką oznacza się często symbolem $<$.

Jeśli relacja jest zwrotna (zamiast przeciwzwrotności), to oznacza się ją często jako $\leq$.

Wprowadza się wiele różnych określeń charakteryzujących relację, oddających intuicyjne właściwości, które można orzekać o czasie. Wiele z nich opisanych jest w [1]. Przykładowo ograniczoność lub nieograniczoność czasu można zdefiniować w następujący sposób:

Definicja 4 (Ograniczoność i nieograniczoność czasu)**.** Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *lewostronnie ograniczoną*, gdy zachodzi:

$$\neg \left(\forall_{t_1 \in T} \exists_{t_2 \in T} \; t_2 < t_1 \right).$$

Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *prawostronnie ograniczoną*, gdy zachodzi:

$$\neg \left(\forall_{t_1 \in T} \exists_{t_2 \in T} \; t_1 < t_2 \right).$$

Struktura czasowa, która nie jest ograniczona ani lewostronnie, ani prawostronnie, nazywana jest *nieograniczoną*.

Innym istotnym określeniem stosowanym wobec czasu jest stwierdzenie, że jest on ciągły (jak np. zbiór liczb rzeczywistych) lub że jest dyskretny (czyli np. chwile można ponumerować liczbami naturalnymi).

Definicja 5 (Czas ciągły)**.** Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *ciągłą*, jeśli

$$\forall_{t_1, t_2 \in T} \exists_{t_3}\ t_1 < t_2 \wedge t_3 < t_2.$$

Definicja 6. Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *prawostronnie dyskretną*, jeśli

$$\forall_{t_1, t_2 \in T}\ t_1 < t_2 \implies \exists_{t_3}\ (t_1 < t_3) \wedge \neg\left(\exists_{t_4}\ t_1 < t_4 \wedge t_4 < t_3\right).$$

Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *lewostronnie dyskretną*, jeśli

$$\forall_{t_1, t_2 \in T}\ t_2 < t_1 \implies \exists_{t_3}\ (t_3 < t_1) \wedge \neg\left(\exists_{t_4}\ t_3 < t_4 \wedge t_4 < t_1\right).$$

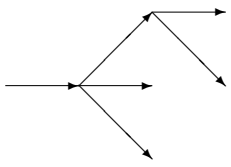
Struktura czasowa lewostronnie i prawostronnie dyskretna nazywana jest *dyskretną*.

Intuicyjnie czas pojmuje się jako *liniowy*, tzn. że dla każdych dwóch chwil albo jedna następuje po drugiej, albo na odwrót. Tym samym czas w żadnym punkcie się nie „rozwidla". Formalna definicja struktury, w której relacja następowania jest liniowa, jest następująca:

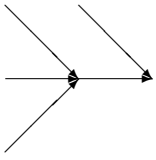
Definicja 7 (Struktura liniowa)**.** Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *liniową*, gdy zachodzi:

$$\forall_{t_1, t_2, t_3 \in T}\ t_1 < t_2 \vee t_2 < t_1 \vee t_1 = t_2.$$

Tym niemniej, dla uwzględnienia możliwości potoczenia się wydarzeń na różne sposoby, często przyjmuje się, że po danym stanie świata mogą nastąpić różne możliwości. Strukturę umożliwiającą rozgałęzienia w przyszłości nazywa się *lewostronnie liniową*.



Analogicznie, jeśli uwzględnia się, że dla aktualnego stanu świata różne stany mogłyby być przeszłością, wprowadza się tak zwaną strukturę *prawostronnie liniową*, umożliwiającą rozgałęzienia „w przeszłości".



Formalne definicje są następujące:

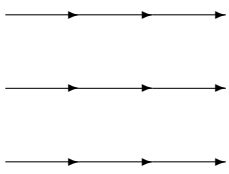
Definicja 8 (Struktura lewostronnie i prawostronnie liniowa)**.** Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *lewostronnie liniową*, gdy zachodzi:

$$\forall_{t_1,t_2,t_3 \in T}\, t_2 < t_1 \wedge t_3 < t_1 \implies t_2 < t_3 \vee t_3 < t_2 \vee t_2 = t_3.$$

Struktura czasowa $\mathcal{T} = (T, <)$ nazywana jest *prawostronnie liniową*, gdy zachodzi:

$$\forall_{t_1,t_2,t_3 \in T}\, t_1 < t_2 \wedge t_1 < t_3 \implies t_2 < t_3 \vee t_3 < t_2 \vee t_2 = t_3.$$

Struktura może również wyrażać również niezależny bieg różnych „torów" czasu. Strukturę taką nazywa się *równoległą*.



Definicję struktury równoległej można zapisać za pomocą pojęć lewostronnej i prawostronnej liniowości w następujący sposób:

Definicja 9 (Struktura równoległa)**.** Struktura czasowa nazywana jest *równoległą*, gdy jest lewostronnie i prawostronnie liniowa.

Rozważać można też wiele innych określeć czasu, np. moc zbioru następników poszczególnych chwil, czyli kwestię, czy dana chwila ma kontinuum następników itp.

3.2. System K_t

Najprostszą logiką temporalną jest tzw. system K_t, opisany dokładniej w [4]. Wprowadza się w nim (zamiast $\Diamond$ i $\Box$) następujące symbole: P, F, G i H.

Dalej, niech f będzie formułą.

Pf oznacza „była taka chwila, w której f była spełniona" (P oznacza „past"). Ff (od „future") oznacza „będzie taka chwila, w której f będzie spełniona".

Za pomocą P można zdefiniować symbol H (od „have been") oznaczający „zawsze tak było, że f była spełniona": $Hf \iff \neg P \neg f$.

Analogicznie definiuje się symbol G (od „going to") mówiący, że „f już zawsze będzie spełniona": $Gf \iff \neg F \neg f$.

Formuły pozbawione symboli czasowych odnoszą się do chwili „obecnej".

Dla specyficznych symboli systemu K_t spełnienie w modelu $\mathcal{M}$ definiuje się w sposób analogiczny jak dla $\Diamond$ i $\Box$:

(i) $(\mathcal{M}, u) \vDash Ff$ wtedy i tylko wtedy, gdy: istnieje $t \in U$, uRt, że $(\mathcal{M}, t) \vDash f$,

(ii) $(\mathcal{M}, u) \vDash Gf$ wtedy i tylko wtedy, gdy: dla każdego $t \in U$ jeśli uRt, to $(\mathcal{M}, t) \vDash f$,

(iii) $(\mathcal{M}, u) \vDash Pf$ wtedy i tylko wtedy, gdy: istnieje $t \in U$, tRu, że $(\mathcal{M}, t) \vDash f$,

(iv) $(\mathcal{M}, u) \vDash Hf$ wtedy i tylko wtedy, gdy: dla każdego $t \in U$ jeśli tRu, to $(\mathcal{M}, t) \vDash f$.

W logice K_t przyjmuje się następujące schematy aksjomatów. Pierwsze dwa są analogiczne do schematu aksjomatów K.

(i) $G\,(f_1 \implies f_2) \implies (Gf_1 \implies Gf_2)$,

(ii) $H\,(f_1 \implies f_2) \implies (Hf_1 \implies Hf_2)$,

(iii) $f \implies HFf$,

(iv) $f \implies GPf$.

W logice K_t jako reguły wnioskowania przyjmuje się regułę MP (odrywania) oraz regułę regularności dla symboli G i H.

Podobnie jak dla systemu $\mathcal{K}$, można udowodnić, że twierdzenia systemu K_t zachodzą dla każdej struktury (przy dowolnej relacji następowania).

Poniższy przykład ilustruje, jak przebiega typowe dowodzenie w logikach modalnych:

Przykład 10. Twierdzeniem systemu K_t jest formuła:

$$H(\varphi \implies \psi) \implies (P\varphi \implies P\psi).$$

Dowód.

(i) $H(\neg\psi \implies \neg\varphi) \implies (H\neg\psi \implies H\neg\varphi)$ (aksjomat),

(ii) $(H\neg\psi \implies H\neg\varphi) \implies (\neg H\neg\varphi \implies \neg H\neg\psi)$ (transpozycja),

(iii) $H(\neg\psi \implies \neg\varphi) \implies (\neg H\neg\varphi \implies \neg H\neg\psi)$ (1, 2, sylogizm),

(iv) $(\varphi \implies \psi) \implies (\neg\psi \implies \neg\varphi)$ (transpozycja),

(v) $H(\varphi \implies \psi) \implies H(\neg\psi \implies \neg\varphi)$ (4, reguła regularności dla H),

(vi) $H(\varphi \implies \psi) \implies (\neg H\neg\varphi \implies \neg H\neg\psi)$ (3, 5, sylogizm),

(vii) $H(\varphi \implies \psi) \implies (P\varphi \implies P\psi)$ (definicja P za pomocą H).

□

Twierdzenie to można wysłowić jako: jeśli w przeszłości zawsze tak było, że z φ wynikało ψ, to jeśli choć raz w przeszłości zaszło φ, to zaszło choć raz[3] również ψ.

[3] Właśnie wtedy, co φ, ale tego, kiedy, twierdzenie nie określa.

3.3. Liniowa logika temporalna

Opisana wyżej logika K_t jest tylko jedną z wielu logik temporalnych. Inną ważną logiką temporalną, opisaną szczegółowiej w [1], jest tak zwana liniowa logika temporalna.

W 1968 r. Jan Kamp wprowadził do logiki temporalnej dwa dodatkowe operatory:

(i) operator U (ang. *Until*) oznaczający „dopóki" (pUq znaczy: p zachodzi do momentu w którym zajdzie q),

(ii) operator S (ang. *Since*) oznaczający „odkąd" (pSq znaczy: p zachodzi od momentu w którym zaszło q).

Wprowadza się często również operator X (ang. *neXt*), oznaczający „w następnej chwili", jeśli tylko w danym kontekście można zdefiniować, co znaczy „następna chwila".

Opisany system K_t nie narzucał żadnych warunków na relację R. W liniowej logice temporalnej sytuacja jest inna.

Niech S będzie zbiorem stanów świata i $\rho\colon S \to S$ będzie funkcją, która każdemu stanowi świata przypisuje jednoznacznie stan „następny".

Niech ρ^n ($n \geq 0$) oznacza n–krotne złożenie funkcji ρ (np. $\rho^3(x) = \rho(\rho(\rho(x)))$).

Zdefiniujmy relację R:

$$\forall_{s_1,\, s_2 \in S} \left(s_1 R s_2 \iff \exists_{n \in \mathbf{N} \cup \{0\}} \, \rho^n(s_1) = s_2 \right),$$

tzn. dwa stany s_1 i s_2 są w relacji R wtedy i tylko wtedy, gdy z s_1 można dojść w skończonej liczbie kroków ρ do stanu s_2.

Gdy do zbioru stanów świata S i zdefiniowanej tak relacji R dołączy się wartościowanie w poszczególnych światach V, to tak uzyskana trójka $\mathcal{T} = \langle S, R, V \rangle$ jest modelem Kripkego (czyli w tym kontekście historią).

Ograniczmy rozważania do symboli temporalnych G (zawsze w przyszłości), F (kiedyś w przyszłości), X (w następnej chwili) i U (dopóki).

Pojęcie spełnienia formuł z symbolami G i F pozostaje bez zmian:

(i) $(\mathcal{T}, s) \vDash Ff$ wtedy i tylko wtedy, gdy: istnieje $t \in S$, sRt, że $(\mathcal{T}, t) \vDash f$,

(ii) $(\mathcal{T}, s) \vDash Gf$ wtedy i tylko wtedy, gdy: dla każdego $t \in S$ jeśli sRt, to $(\mathcal{T}, t) \vDash f$.

Spełnienie formuł z symbolami X i U wygodnie jest wprowadzić za pomocą funkcji następnego stanu ρ:

(i) $(\mathcal{T}, s) \vDash Xf$ wtedy i tylko wtedy, gdy $(\mathcal{T}, \rho(s)) \vDash f$,

(ii) $(\mathcal{T}, s) \vDash f_1 U f_2$ wtedy i tylko wtedy, gdy:

$$\exists_{j \geq 0} \left(\left(\mathcal{T}, \rho^j(s)\right) \vDash f_2 \wedge \forall_{i<j} \left(\mathcal{T}, \rho^i(s)\right) \vDash f_1 \right).$$

Można wprowadzić następujące pojęcie tautologii:

Definicja 11 (Tautologia)**.** *Tautologiami* liniowej logiki temporalnej (LTL) są formuły spełnione w każdym modelu Kripkego (historii) $\mathcal{T} = \langle S, R, V \rangle$ utworzonego w wyżej opisany sposób (z relacjami określonymi za pomocą funkcji następnego stanu).

4. Czas nie istnieje

Na zakończenie, aby pokazać, że wysiłki włożone w zrozumienie, czym jest czas, nie były bezowocne, przedstawię dowód McTaggarta [5], że czas nie istnieje.

McTaggart w 1908 r. opublikował esej *Nierealność czasu* (*The Unreality of Time*), w którym przedstawił swój pogląd na temat istnienia czasu.

Czas można jego zdaniem opisywać za pomocą tak zwanych ciągów A i B[4] (ang. *series A and B*).

Mianowicie, w ciągu A wydarzenia określa się jako należące do odległej przeszłości, do przeszłości, do bliskiej przeszłości, teraźniejszości, bliskiej przyszłości, ...

Inne możliwe podejście, ciąg B, mówi: „wydarzenie a nastąpiło po b, które nastąpiło po c, ..."

Ciąg B nie zawiera właściwie czasowości, tylko porządek zachodzenia zdarzeń.

Ciąg A jest wewnętrznie sprzeczny, gdyż to samo wydarzenie raz należy do przyszłości, raz do przeszłości. Stwierdzenie, że nie „jednocześnie" samo odwołuje się do czasu i wprowadza błędne koło.

Zatem czas nie istnieje.

Literatura

[1] R. Klimek, *Wprowadzenie do logiki temporalnej*, Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 1999.

[2] N. Markosian, *Time*, Stanford Encyclopedia of Philosophy, 2008.

[3] D. Sedley, *Diodorus Cronus*, Stanford Encyclopedia of Philosophy, 2009.

[4] K. Świrydowicz, *Podstawy logiki modalnej*, Wydawnictwo Naukowe UAM, Poznań 2004.

[5] J. M. E. McTaggar, *The Unreality of Time*, 1908 (dostępny na WikiSource).

[4] Wyróżnia on jeszcze ciągi C, nieistotne w przedstawionej tu uproszczonej wersji rozważań.

Gdzie matematyk nie może, tam komputer pośle?

Bartosz Naskręcki

W ostatnich latach można zaobserwować w matematyce tendencję do konstruowania dowodów twierdzeń, których istotna część jest oparta na obliczeniach komputerowych. To zjawisko wywołuje zarówno entuzjazm – w szczególności wśród autorów rzeczonych dowodów – jak i wzbudza lęk – wśród zwolenników tradycyjnego uprawiania matematyki.

W niniejszym artykule omówimy szereg zagadnień związanych z szeroko pojętym wykorzystaniem komputerów w praktyce matematycznej. Poprzez przykłady z logiki, geometrii czy algebry Czytelnik będzie mógł sam ocenić, jak ważny jest udział maszyn obliczeniowych w argumentacji dedukcyjnej.

Czym jest dowód matematyczny? W szerokim znaczeniu (czyli takim, jakim go widzi przeciętny matematyk) dowód to pewna argumentacja, używająca precyzyjnych reguł dedukcyjnych, która ma na celu przekonać czytelnika o poprawności stawianej tezy. Mówiąc krótko – dowód to pewien ciąg zdań, które w sposób „logiczny" wyprowadzają z założeń danego twierdzenia pewne z góry ustalone tezy. Na początku XX wieku wielu matematyków, w tym David Hilbert, zamierzało doprecyzować tę definicję i sprowadzić całość wnioskowania matematycznego do pewnej formalnej gry symbolami i zdaniami – aksjomatami, które uznajemy w danej teorii za prawdziwe z góry.

W żadnym przypadku nie mówi się natomiast, kto właściwie ma dany dowód przeprowadzić ani kto jest właściwie kompetentny do sprawdzenia wszystkich kroków w danym dowodzie twierdzenia.

Ze względu na subtelność i niejednoznaczność wielu kwestii, warto będzie omówić problem na przykładach.

1. Geometryczne dowody wspierane komputerowo

Twierdzenia z zakresu geometrii euklidesowej stanowią naturalne źródło formalnych argumentacji, które (po pewnych współczesnych modyfikacjach) można uważać za jedne z bardziej argumentacji logicznych.

Bartosz Naskręcki
nasqret@gmail.com
student matematyki
Uniwersytet Adama Mickiewicza w Poznaniu

Połączenie metod geometrii elementarnej z geometrią analityczną (lub bardziej poprawnie zwaną algebraiczną) dało zestaw metod pozwalających rozwiązywać zagadnienia geometryczne w sposób całkowicie zautomatyzowany.

Metoda, o której mowa, nazywa się metodą zbiorów charakterystycznych. Została opracowana w poźnych latach 70. przez chińskiego matematyka Wen-Tsun Wu. Ogólny schemat wygląda następująco:

$$\text{własność geometryczna figury } \rightarrow \text{ warunek algebraiczny kodujący tę własność.}$$

Do zdefiniowania takich warunków potrzebujemy sposobu kodowowania figur geometrycznych. Najlepszy rezultat daje nam wprowadzenie układu współrzędnych, gdzie wierzchołki badanych figur opisujemy jako uporządkowane ciągi współrzędnych $(x_1, \ldots, x_n)$, natomiast wszelkie własności figur kodujemy jako pewne układy równań algebraicznych w zmiennych x_i.

Przykład 1. Udowodnimy w sposób sformalizowany twierdzenie Pitagorasa. Niech $A = (x_1, y_1)$, $B = (x_2, y_2)$ oraz $C = (x_3, y_3)$ będą współrzędnymi trójkąta (przez brak dodatkowych założeń o współrzędnych wprowadzamy szereg przykładów zdegenerowanych trójkątów). Zakodujmy teraz własność: odcinek $\overline{AB}$ jest prostopadły do $\overline{AC}$:

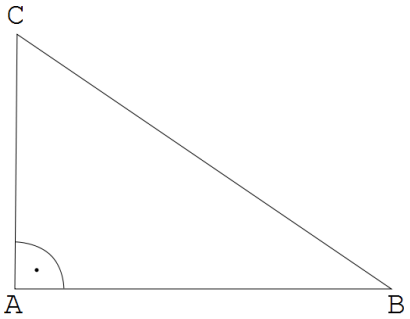
$$Z\colon (x_2 - x_1)(x_3 - x_1) + (y_2 - y_1)(y_3 - y_1) = 0.$$

Warunek wynika z definicji iloczynu skalarnego dwóch wektorów. Twierdzenie Pitagorasa mówi nam, że

$$|AB|^2 + |AC|^2 = |BC|^2,$$

co w terminach algebraicznych zapiszemy jako:

$$T : (x_2 - x_1)^2 + (y_2 - y_1)^2 + (x_3 - x_1)^2 + (y_3 - y_1)^2 = (x_3 - x_2)^2 + (y_3 - y_2)^2.$$



Rysunek 1. Twierdzenie Pitagorasa: $|AB|^2 + |AC|^2 = |BC|^2$

Klasyczny dowód twierdzenia Pitagorasa można przeprowadzić na wiele różnych sposobów. My musimy jedynie pokazać:

$$\forall_{x_1,x_2,x_3,y_1,y_2,y_3 \in \mathbb{R}}\ Z \Rightarrow T.$$

Jak łatwo się przekonać (po nieco żmudnych obliczeniach):

$$(x_2-x_1)^2+(y_2-y_1)^2+(x_3-x_1)^2+(y_3-y_1)^2-((x_3-x_2)^2+(y_3-y_2)^2)= \\ =2((x_2-x_1)(x_3-x_1)+(y_2-y_1)(y_3-y_1)), \quad (1)$$

co dowodzi naszego twierdzenia w wersji algebraicznej (włącznie z wszystkimi przypadkami zdegenerowanymi). W terminach algebraicznych sprowadza się to do pokazania, że ideał

$$Z_I=((x_2-x_1)(x_3-x_1)+(y_2-y_1)(y_3-y_1))$$

w pierścieniu wielomianów $\mathbb{R}[x_1,x_2,x_3,y_1,y_2,y_3]$ zawiera w sobie ideał

$$T_I=((x_2-x_1)^2+(y_2-y_1)^2+(x_3-x_1)^2+(y_3-y_1)^2-((x_3-x_2)^2+(y_3-y_2)^2)).$$

Uwaga 2. Abyśmy mogli stosować pełną równoważność ideałów i układów równań algebraicznych, ciało $\mathbb{R}$ powinno być zastąpione ciałem domkniętym algebraicznie, np. $\mathbb{C}$.

Konsekwentne rozwinięcie tej metody z użyciem geometrii algebraicznej prowadzi do prostego kryterium, które na współczesnych komputerach może być sprawdzane w sposób całkowicie zautomatyzowany. Jedyny wkład pracy, jaki jest potrzebny podczas dowodzenia twierdzeń tą metodą, polega na odpowiednim zakodowaniu zadania o figurach geometrycznych w terminach układów równań wielomianowych.

2. Komputery w logice matematycznej

Odkryte w XIX wieku przez brytyjskiego matematyka George'a Boole'a struktury algebraiczne, zwane od jego nazwiska algebrami Boole'a, mają wielkie znaczenie w matematyce, w szczególności w teorii krat, w logice matematycznej, a nawet w elektronice cyfrowej. Formalnie algebra Boole'a $\mathbb{B}$ składa się ze zbioru B, dwóch operatorów dwuargumentowych $\cap$ i $\cup$ oraz operatora jednoargumentowego $\neg$, a także dwóch wyróżnionych elementów zbioru B: 0 i 1. Operacje i wyróżnione symbole spełniają ponadto warunki:

$$\begin{aligned} x\cup(y\cup z)&=(x\cup y)\cup z,\\ x\cup y&=y\cup z,\\ x\cup(x\cap y)&=x,\\ x\cup(y\cap z)&=(x\cup y)\cap(x\cup z),\\ x\cup\neg x&=1 \end{aligned}$$

i analogiczne warunki powstałe przez konsekwentne zastąpienie $\cup$ przez $\cap$ oraz 0 przez 1.

W tak zdefiniowanej strukturze algebraicznej można dowodzić różnorakich identyczności.

Przykład 3. Pokażemy, że każdy element algebry Boole'a jest idempotentny, tzn.

$$x \cup x = x = x \cap x.$$

Z aksjomatów wynika:

$$x \cup (x \cap (x \cup x)) = x.$$

Ponadto $x \cap (x \cup x) = x$, stąd $x \cup x = x$. Podobnie:

$$x \cap (x \cup (x \cap x)) = x$$

i stąd $x \cap x = x$.

Jednym z podstawowych zagadnień teorii algebr Boole'a jest podanie minimalnej aksjomatyzacji takiej algebry. W 1933 r. E. V. Huntington zaproponował następujący układ aksjomatów:

$$\begin{aligned} x \cup y &= y \cup x, \\ x \cup (y \cup z) &= (x \cup y) \cup z, \\ \neg(\neg x \cup \neg y) \cup \neg(\neg x \cup y) &= x. \end{aligned}$$

Ponadto symbole 0 i 1 oraz operacja $\cap$ są definiowane w terminach $\cup$ i $\neg$.

Huntington udowodnił, że algebra z takim układem aksjomatów istotnie jest algebrą Boole'a. W drugą stronę łatwo jest też udowodnić, że każda algebra Boole'a spełnia wszystkie trzy aksjomaty.

Zastąpienie warunku trzeciego przez:

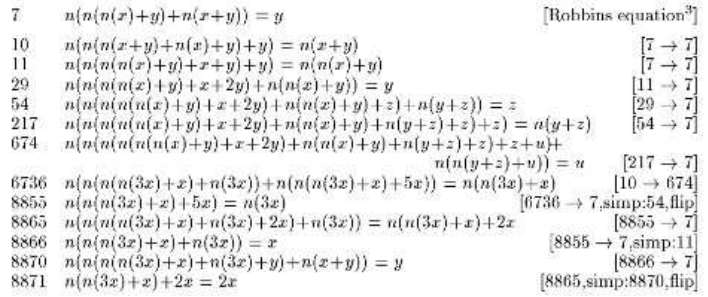
$$\neg(\neg(x \cup y) \cup \neg(x \cup \neg y)) = x$$

daje nam inną algebrę, w której podobnie jak w poprzedniej symbole 0 i 1 oraz $\cap$ są definiowane w terminach operacji $\cup$ i $\neg$.

Hipoteza postawiona przez Herberta Robbinsa w latach 30. XX wieku mówiła, że powyższa algebra również jest algebrą Boole'a, co w połączeniu z łatwym do wykazania twierdzeniem odwrotnym, dawałoby nową, nieco prostszą charakteryzację algebr Boole'a.

Mimo wysiłku wielu matematyków, w tym Alfreda Tarskiego, hipoteza pozostała nieudowodniona do 1996 r., kiedy to William McCune pokazał z użyciem programu komputerowego EQP (Equational Prover), że hipoteza istotnie jest prawdziwa. Co więcej, wyprodukowany przez komputer dowód daje się zapisać w sposób formalny na kilku stronach A4 i jest w miarę łatwo weryfikowalny przez człowieka.

Program oparty jest na technice paramodulacji, która jest metodą generowania coraz to nowych równości termów w logice równościowej, opierając się na założonych aksjomatach oraz na możliwości podstawiania pod zmienne konkretnych termów.



Rysunek 2. Fragment oryginalnego dowodu McCune'a (wyciąg z programu EQP).

3. Twierdzenie o czterech barwach

Każdy, kto kiedykolwiek oglądał dobrze sporządzoną mapę, zauważył na pewno, że do odróżnienia dwóch sąsiadujących krajów wystarczy używać tylko czterech różnych kolorów. Ta intuicja, podparta dobrym opisem z użyciem teorii grafów, wiedzie nas do zadziwiającego twierdzenia, że każdą mapę na sferze bądź płaszczyźnie można pokolorować co najwyżej czterema kolorami.

Definicja 4. *Łukiem* na płaszczyźnie $\mathbb{R}^2$ nazywamy obraz różnowartościowego odwzorowania ciągłego z $[0,1]$ do $\mathbb{R}^2$.

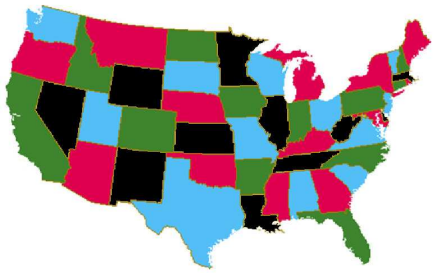
Definicja 5. *Mapa* to skończony zbiór łuków na płaszczyźnie, takich że ich przecięcie jest puste albo zawiera się we wspólnych końcach. Dopełnienie mapy w $\mathbb{R}^2$ składa się ze skończenie wielu składowych spójności, które nazywamy *państwami*.

Definicja 6. Odwzorowanie ze zbioru państw do skończonego podzbioru liczb naturalnych nazywamy *kolorowaniem*. Kolorowanie jest *dopuszczalne*, jeśli dwa sąsiadujące państwa (posiadające niepuste przecięcie brzegów) mają różne kolory.

Hipoteza o czterech kolorach została postawiona przez Francisa Guthriego w 1852 r. Rozpowszechniona przez Augustusa de Morgana stała się celem licznych prób wielu matematyków. Jeden z pierwszych publicznie zaakceptowanych dowodów opublikowany przez Alfreda Kempego okazał się fałszywy (pomyłka wyszła na jaw dopiero po 10 latach). W 1890 r. Percy Heawood udowodnił twierdzenie o pięciu barwach, lecz pełen dowód hipotezy dla czterech kolorów został przeprowadzony z użyciem komputerów dopiero w latach 70. XX wieku.

Twierdzenie 7 (Appel, Haken, 1976)**.** *Dla każdej mapy istnieje kolorowanie dopuszczalne co najwyżej czterema kolorami.*

W powyższej wersji twierdzenie jest trudne do udowodnienia. Pierwszym krokiem do właściwego dowodu jest tzw. normalizacja mapy, czyli usunięcie wszelkich łuków, które nie oddzielają od siebie żadnych dwóch państw.



Rysunek 3. Przykład dopuszczalnego kolorowania czterema barwami.

W dowodzie pokazuje się, że nie istnieje minimalny kontrprzykład, czyli taka mapa, która ma dopuszczalne kolorowanie co najmnniej pięcioma kolorami i posiada najmniejszą możliwą liczbę państw.

Szereg nietrudnych lematów prowadzi do przeformułowania twierdzenia do postaci kombinatorycznej, w której wystarczy rozważać klasyczne kolorowania grafów planarnych, w dodatku takich, które są triangulacjami.

Część dowodu przeprowadzana na komputerze polega na analizie przypadków tzw. konfiguracji nieuniknionych, czyli takich, które musiałyby się pojawić, gdybyśmy szukali minimalnego kontrprzykładu grafu, dla którego nie istnieje właściwe kolorowanie.

Współczesny dowód twierdzenia o czterech barwach dla grafów został całkowicie zautomatyzowany w systemie wspierającym automatyczne dowodzenie – programie Coq. W poniższej części artykułu omówimy pobieżnie właściwości takich programów.

4. Automatyczne systemy dowodzenia

Programy wspomagające automatyczne dowodzenie (a także interaktywni asystenci dowodów) są rodziną systemów komputerowych, które posiadają wbudowane mechanizmy potrafiące interpretować logikę klasyczną, logiki równościowe oraz logiki predykatywne pierwszego rzędu. Oprócz ich oczywistego zastosowania do sprawdzania dowodów twierdzeń matematycznych, programy te mają zastosowanie w przemyśle, np. przy produkcji procesorów czy wysoce niezawodnego oprogramowania – do sprawdzania logicznej poprawności wykonywanych instrukcji i ich zgodności z przyjętymi założeniami.

Warto wymienić kilka takich systemów, m.in. HOL, Isabelle, Coq, Mizar, Otter czy EQP. System Mizar jest rozwijany aktywnie przez polskich matematyków i przy jego pomocy udało się sformalizować m.in. dowód twierdzenia Hahna-Banacha, dowód twierdzenia Gödla o zupełności rachunku zdań pierwszego rzędu oraz twierdzenie Brouwera o punkcie stałym. System Coq z kolei pozwala przeprowadzić formalny dowód twierdzenia o czterech barwach.

Każdy z systemów posiada unikalnie wybrany system logiczny, wiele z nich opartych jest na logikach intuicjonistycznych, a także na aksjomatyce teorii mnogości wzbogaconej o pewne

```
theorem Th11:
  i gcd m = 1 & i is_quadratic_residue_mod m &
    i,j are_congruent_mod m
  implies j is_quadratic_residue_mod m
proof
  assume
A1: i gcd m = 1 &
    i is_quadratic_residue_mod m &
    i,j are_congruent_mod m;
  then consider x being Integer such that
A2: (x^2 - i) mod m = 0 by Def2;
  m divides (i - j) by A1,INT_2:19;
  then
A3: (i - j) mod m = 0 by Lm1;
  (x^2 - j) mod m
     = ((x^2 - i) + (i - j)) mod m
    .= (((x^2 - i) mod m) + ((i - j) mod m))
            mod m by INT_3:14
    .= 0 by A2,A3,INT_3:13;
  hence thesis by Def2;
end;
```

Rysunek 4. Fragment dowodu w systemie Mizar.

specyficzne aksjomaty.

Omówimy poniżej bardziej szczegółowo konstrukcję systemu Coq.

4.1. System Coq

System Coq rozwijany przez francuską grupę programistów i matematyków wspiera logikę bez prawa wyłączonego środka i reguły podwójnego przeczenia. Korzystając z korespondencji pomiędzy formułami w prostym rachunku λ i konstruktywnymi dowodami w intuicjonistycznej logice (izomorfizm Howarda-Curry'ego-de Bruijna), program potrafi z pomocą ludzkiego wsparcia budować dowody, które wewnątrz programu interpretowane są jako programy komputerowe. Przeprowadzenie dowodu jest równoważne z poprawnym wykonaniem napisanego programu (rachunek funkcyjny). Ponadto teza twierdzenia odpowiada tu konstrukcji nagłówka funkcji, której ciałem jest przeprowadzany algorytm (czyli dowód).

Formuły poprawnie zbudowane w programie Coq:

(i) Zmienne zdaniowe i predykaty.

(ii) Stała $\bot$ (odpowiadająca klasycznie wartości logicznej fałszu).

(iii) Stała $\top$ (odpowiadająca klasycznie wartości logicznej prawdy).

(iv) Jeśli A, B są formułami poprawnie zbudowanymi, to jest nią również formuła $A \to B$.

(v) Jeśli A, B są formułami poprawnie zbudowanymi, to jest nią również formuła $A \wedge B$.

(vi) Jeśli A, B są formułami poprawnie zbudowanymi, to jest nią również formuła $A \vee B$.

(vii) Jeśli A jest formułą poprawnie zbudowaną, to jest nią również formuła $\neg A := A \to \bot$.

(viii) Jeśli A jest formułą poprawnie zbudowaną, a x jest zmienną wolną w A, to $\forall x.A$ jest formułą poprawnie zbudowaną.

(ix) Jeśli A jest formułą poprawnie zbudowaną, a x jest zmienną wolną w A, to $\exists x.A$ jest formułą poprawnie zbudowaną.

Możemy teraz wprowadzić reguły dowodzenia.

Reguła wprowadzania założeń:

$$A^x$$

oznacza możliwość wprowadzenia założenia z indeksem x, które w regule wprowadzania implikacji musi zostać następnie wykorzystane:

$$\dfrac{\begin{array}{c}\vdots\\ B\end{array}}{A \to B}\ I[x] \to$$

Reguła eliminacji implikacji pozwala nam oderwać następnik:

$$\dfrac{\begin{array}{cc}\vdots & \vdots\\ A \to B & A\end{array}}{B}\ E \to$$

Reguła wprowadzania koniunkcji wygląda następująco:

$$\dfrac{\begin{array}{cc}\vdots & \vdots\\ A & B\end{array}}{A \wedge B}\ I\wedge$$

Reguły eliminacji koniunkcji mamy dwie – lewą i prawą:

$$\dfrac{\begin{array}{c}\vdots\\ A \wedge B\end{array}}{A}\ El\wedge \qquad \dfrac{\begin{array}{c}\vdots\\ A \wedge B\end{array}}{B}\ Er\wedge$$

Mamy też odpowiednie reguły wprowadzania alternatywy:

$$\dfrac{\begin{array}{c}\vdots\\ A\end{array}}{A \vee B}\ Il\wedge \qquad \dfrac{\begin{array}{c}\vdots\\ B\end{array}}{A \vee B}\ Ir\wedge$$

Reguła eliminacji alternatywy:

$$\frac{\begin{array}{ccc}\vdots & \vdots & \vdots \\ A \vee B & A \to C & B \to C\end{array}}{C} \; E\vee$$

Reguła prawdy orzeka:

$$\top$$

natomiast reguła falsum:

$$\frac{\begin{array}{c}\vdots \\ \bot\end{array}}{A}$$

Pozostają jeszcze reguły wprowadzania dużego i małego kwantyfikatora:

$$\frac{\begin{array}{c}\vdots \\ A\end{array}}{\forall x.A} \; I\forall \qquad \frac{\begin{array}{c}\vdots \\ A[x := M]\end{array}}{\exists x.A,} \; I\exists$$

gdzie wyrażenie $A[x := M]$ oznacza podstawienie pod zmienną wolną x w A wyrażenia M. Pozostały jeszcze tylko reguły eliminacji kwantyfikatorów.

$$\frac{\begin{array}{c}\vdots \\ \forall x.A\end{array}}{A[x := M]} \; E\forall \qquad \frac{\begin{array}{cc}\vdots & \vdots \\ \exists x.A & \forall x.(A \to B)\end{array}}{B} \; E\exists$$

Przykładem dedukcji w tym systemie może być dowód tautologii

$$(A \to B \to C) \to (A \to B) \to A \to C$$

W praktyce jednak system Coq nie wykorzystuje reguł dowodzenia w logice, tylko stosuje rachunek λ, który pokrótce omówimy i pokażemy, jak formuły w nim tłumaczą się na język tautologii.

Typy proste w rachunku λ:

(i) Zmienne są typami prostymi.

(ii) Jeśli A i B są typami prostymi, to $A \to B$ jest typem prostym.

Definiujemy także funkcję przyporządkowującą zmiennej x typu A wartość M:

$$\lambda x : A.M$$

Piszemy ponadto FN, gdy chcemy zasygnalizować, że funkcja F działa na argumencie N. Rachunek λ w Coq posiada trzy reguły produkowania nowych typów z typów istniejących (przez Γ będziemy oznaczali kolekcję zmiennych określonych typów). Reguła zmiennej:

$$\Gamma, x : A \vdash x : A$$

Reguła abstrakcji pozwalająca definiować nowe typy funkcyjne:

$$\frac{\begin{array}{c}\vdots \\ \Gamma, x : A \vdash M : B\end{array}}{\Gamma \vdash (\lambda x : A.M) : A \to B}$$

i reguła przyporządkowania, która niejako odpowiada „ewaluacji” funkcji na argumencie:

$$\frac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \vdash F : A \to B & \Gamma \vdash N : A\end{array}}{\Gamma \vdash (FN) : B}$$

```
Theorem P6 : (a:nat)(b:nat)(ge (mult a b) b)\/((mult a b) = 0).
Proof.
Intros.
Induction a.
Right.
Reflexivity.
Left.
Unfold mult.
Unfold ge.
Fold plus.
Fold mult.
Rewrite (P4 b (mult a b)).
Apply P5.
Qed.

Theorem P7 : (a:nat)(b:nat)(lt a b) -> (le b a) -> False.
Proof.
Intros a b p1.
Induction p1.
Apply Le.le_Sn_n.
Intros.
Apply Hrecp1.
Apply Le.le_trans_S.
Assumption.
Qed.
```

Rysunek 5. Kod w systemie Coq.

Korzystając z powyższych reguł, możemy skonstruować typ odpowiadający wcześniejszej tautologii $(A \to B \to C) \to (A \to B) \to A \to C$, mianowicie:

$$\vdash \lambda x : A \to B \to C.\lambda y : A \to B.\lambda z : A.xz(yz) : (A \to B \to C) \to (A \to B) \to A \to C$$

Jest to jeden z przykładów realizacji izomorfizmu Howarda-Curry'ego-de Bruijna, gdzie zmiennym logicznym odpowiadają zmienne typowe, symbol $\rightarrow$ odpowiada konstruktorowi opatrzonemu tym samym symbolem, ogólne formuły logiczne odpowiadają bardziej skomplikowanym typom funkcyjnym.

Z kolei dowody odpowiadają termom, a reguła wprowadzenia implikacji odpowiada regule abstrakcji, podobnie reguła eliminacji implikacji odpowiada regule aplikacji.

Bardziej subtelne reguły logiczne odpowiadające np. zasadzie indukcji zupełnej również dają się zrealizować w terminach (wzbogaconego) rachunku lambda, co w praktyce wykorzystane jest w systemie Coq.

Literatura

[1] Appel, Kenneth; Haken, Wolfgang, *Every planar map is four colorable*, Bull. Amer. Math. Soc. 82 (1976), no. 5, 711–712.

[2] Coq Development Team, *The Coq reference manual*, LogiCal Project, `http://coq.inria.fr/`.

[3] Gonthier, Georges, *Formal proof—the four-color theorem*, Notices Amer. Math. Soc. 55 (2008), no. 11, 1382–1393.

[4] McCune, William, *Solution of the Robbins problem*, J. Automat. Reason. 19 (1997), no. 3, 263–276.

[5] Paulin-Mohring, Christine; Werner, Benjamin, *Synthesis of ML programs in the system Coq*, J. Symbolic Comput. 15 (1993), no. 5–6, 607–640.

[6] Wen Tsun,Wu, *Basic principles of mechanical theorem proving in elementary geometries*, J. Systems Sci. Math. Sci. 4 (1984), no. 3, 207–235.

Quantifier elimination and its geometric applications

Krzysztof J. Nowak

Abstract. The main purpose of model theory is a comprehensive investigation into mathematical structures along with a deeper analysis of the language involved. It is perhaps this semantic feature of model theory that makes a basic difference between the model theorist and the ordinary mathematician in their approach to the subject. I will touch the classical issue of quantifier elimination, going back to A. Tarski, and present a model theoretic criterion due to A. Robinson. My attention focuses on their geometric applications to the theories of algebraically closed and real closed fields. In this fashion, one can obtain short, model theoretic proofs of many fundamental results from algebraic geometry such as Chevalley's constructible set theorem, the Tarski-Seidenberg theorem or the Nullstellensatz (Hilbert's and real).

The first systematic programme for model theory was connected with the issue of quantifier elimination, whose name was introduced by A. Tarski at his seminar in the late 1920s, and which can be formulated as follows:

Given a class K of structures in a (first-order) language $\mathcal{L}$, to find for K an elimination set of $\mathcal{L}$-formulas.

A set Φ of $\mathcal{L}$-formulas is called an elimination set for K if, for every formula $\varphi(x)$, $x = (x_1, \ldots, x_n)$, there is a boolean combination $\psi(x)$ of formulas from Φ that is equivalent to $\varphi(x)$ in every structure in K.

We can always take Φ to be the set of all $\mathcal{L}$-formulas. Nevertheless, the goal is to discover an appropriate elimination set Φ which is as small as possible in a given situation. The name "quantifier elimination" refers either to discovering such an appropriate set Φ or to the method of reducing a formula to a boolean combination of formulas from Φ.

We say that an $\mathcal{L}$-theory T has (or admits) quantifier elimination (QE for short) if the set of atomic formulas is an elimination set for the class of all models of T. This means that every formula is equivalent modulo T to a quantifier-free formula. In other words, the hierarchy of $\mathcal{L}$-formulas reduces modulo T to the quantifier-free formulas. This can be directly translated into the hierarchy of definable sets in the models of T.

dr hab. Krzysztof J. Nowak
krzysztof.jan.nowak@uj.edu.pl
Instytut Matematyki
Uniwersytet Jagielloński

We say that a theory T is model complete (the concept introduced by A. Robinson in the 1950s) if every $\mathcal{L}$-formula $\varphi(x)$ is equivalent modulo T to an existential $\mathcal{L}$-formula $\psi(x)$. Then the hierarchy of $\mathcal{L}$-formulas reduces modulo T to the quantifier-free and existential formulas. Obviously, every theory which has QE is model complete. It is easy to check that a theory T is model complete if every universal $\mathcal{L}$-formula is equivalent modulo T to an existential $\mathcal{L}$-formula. This means, in geometric language, that if E is a projection of a quantifier-free definable subset, so is its complement.

In the following examples, we shall indicate a language by writing down its signature.

Ex. 1) $\mathcal{L} = \{<\}$,

K = class of all dense linear orderings without endpoints,

Φ = set of atomic formulas.

In other words, the theory of dense linear orderings without endpoints has QE (Langford).

Ex. 2) $\mathcal{L} = \{+, -, \cdot, 0, 1\}$ the language of rings,

K = class of all algebraically closed fields,

Φ = set of atomic formulas.

In other words, the theory of algebraically closed fields has QE (Chevalley, Tarski).

Ex. 3) $\mathcal{L} = \{+, -, \cdot, 0, 1\}$, K = class of all real closed fields,

Φ consists of the formulas $\exists_y\ t(x) = y^2$ where t ranges over all terms not containing the variable y; this formula expresses $t(x) \geq 0$.

Consequently, the theory of real closed fields has QE in the language of ordered rings (Tarski, Seidenberg).

Ex. 4) $\mathcal{L}$ = language of ordered rings $\{<, +, -, \cdot, 0, 1\}$ augmented by the names of those functions f which are analytic in the vicinity of the compact cube $[-1, 1]^n$, $n \in \mathbb{N}$,

$K = \{\mathbb{R}_{an}\}$, where $\mathbb{R}_{an}$ is the real field with restricted analytic functions; each function f as above is construed as the restricted function:

$$\widetilde{f}(x) = \begin{cases} f(x) & \text{if } x \in [-1, 1]^n \\ 0 & \text{otherwise.} \end{cases}$$

While the structure $\mathbb{R}_{an}$ is model complete (Gabrielov's complement theorem), it does not admit QE, as shown in an example below. However, one can take here as an elimination set Φ the atomic formulas and the formulas $\exists_y\ y \cdot t(x) = 1$ where t ranges over all terms not containing the variable y. Therefore, the structure $\mathbb{R}_{an}$ has QE in the language $\mathcal{L}$ augmented by the name of the reciprocal function $1/x$ (a result by Denef–van den Dries).

In view of the above examples, it is clear that the problem under study may be also expressed by the question how to appropriately augment the language in order to achieve quantifier elimination.

Example 1. Consider the sets

$$F := \{(1, y, z) \in \mathbb{R}^3 \colon\ z = e^y,\ 0 \leq y \leq 1\} \subset \mathbb{R}^3$$

and

$$E := \{0\} \cup \{(x, y, z) \in \mathbb{R}^3 \colon\ z/x = e^{y/x},\ 0 < x \leq 1,\ 0 \leq y \leq x\} \subset \mathbb{R}^3.$$

Clearly, the set F is semianalytic but not semialgebraic, and E is a bounded subset of the cone $[0, \infty) \cdot F$ generated by F. Hence the set E is subanalytic but not semianalytic, because every semianalytic cone is semialgebraic.

Criteria for QE and for model completeness are powerful tools of model theory. We wish to present one due to A. Robinson (at least in Robinson's style). It relies essentially on model-theoretic compactness.

Theorem 2 (Criterion for Quantifier Elimination.)**.** *A necessary and sufficient condition for a theory T to admit quantifier elimination is the following:*

Let $\mathfrak{M}$ and $\mathfrak{M}'$ be models of T, $\mathfrak{N} \subset \mathfrak{M}$ a substructure, $f : \mathfrak{N} \longrightarrow \mathfrak{M}'$ an isomorphic embedding, $\varphi(y_1, \ldots, y_n)$ be a primitive formula (i.e. a formula of the form $\exists_x\, \alpha(x, y_1, \ldots, y_n)$, where α is a conjunction of atomic or negated atomic formulas) and $(b_1, \ldots, b_n) \in N^n$. Then

$$\mathfrak{M} \models \varphi\,[b_1, \ldots, b_n] \qquad \textit{iff} \qquad \mathfrak{M}' \models \varphi\,[f(b_1), \ldots, f(b_n)].$$

We may formulate the above in a less formal language as follows:

$$\exists_{x \in M}\ \alpha(x, b_1, \ldots, b_n) \qquad \textit{iff} \qquad \exists_{x \in M'}\ \alpha(x, f(b_1), \ldots, f(b_n)).$$

We say that a theory T is almost universal if, for any two of its models $\mathfrak{M}$ and $\mathfrak{M}'$ and their substructures $\mathfrak{N} \subset \mathfrak{M}$, $\mathfrak{N}' \subset \mathfrak{M}'$, each isomorphism between those substructures extends to an isomorphism between some of their submodels. If the theory T is almost universal, the foregoing, necessary and sufficient condition reduces to the following one:

Theorem 3. *Let $\mathfrak{N} \subset \mathfrak{M}$ be models of T, $\varphi(y_1, \ldots, y_n)$ be a primitive formula and $(b_1, \ldots, b_n) \in N^n$. Then*

$$\mathfrak{N} \models \varphi\,[b_1, \ldots, b_n] \qquad \textit{whenever} \qquad \mathfrak{M} \models \varphi\,[b_1, \ldots, b_n].$$

In a less formal language:

$$\exists_{x \in N}\ \alpha(x, b_1, \ldots, b_n) \qquad \textit{whenever} \qquad \exists_{x \in M}\ \alpha(x, b_1, \ldots, b_n).$$

The theories of algebraically closed and real closed fields are, of course, almost universal. It is not difficult to verify the above sufficient condition for quantifier elimination in these two cases. In geometric language, we recover two basic theorems of the classical, complex and real, algebraic geometry to the effect that if E is a constructible or a semialgebraic subset, so is its projection $p(E)$.

Algebraically closed and real closed fields are, a fortiori, model complete. In these algebraic cases, model completeness is equivalent to the Nullstellensatz, Hilbert's or real, respectively. Therefore, model-theoretic methods allow us to look at these fundamental theorems of algebraic geometry from a unified perspective. Also, Hilbert's 17th problem can be solved through model completeness of real closed fields.

Rozstrzygalność problemu istnienia modelu na formuły logiki FO_2 oraz jego wariantów

Michał Pilipczuk

1. Co to jest FO_2?

Z punktu widzenia zastosowań w informatyce logika pierwszego rzędu często okazuje się zbyt silna ze względu na nierozstrzygalność swojej teorii. Dlatego rozpatruje się szereg osłabień i modyfikacji, które co prawda mają słabszą siłę wyrazu, jednak są obejmowalne w ramy algorytmiczne. Jedną z nich jest FO_2.

Powiemy, że formuła pierwszego rzędu nad pewną sygnaturą relacyjną τ należy do $FO_2[\tau]$, jeśli w jej zapisie używa się co najwyżej dwóch różnych nazw na zmienne. Oznacza to w szczególności, że każdy kwantyfikator poniżej zagłębienia 2 musi przy pomocy kwantyfikowanej zmiennej zakryć jedną z poprzednich. O logice FO_2 można myśleć jako o formułach patrzących na co najwyżej dwa elementy modelu w jednostce czasu. To porównanie jest o tyle trafne, że logika FO_2 ściśle wiąże się z logikami nawigacyjnymi, takimi jak modalne czy temporalne. Zauważmy, że definicja przechodniości relacji potrzebuje kwantyfikacji po trzech różnych zmiennych. Brak definiowalności przechodniości okaże się jedną z najbardziej symptomatycznych różnic pomiędzy logikami FO_2 a FO.

2. Problem istnienia modelu

Niech τ będzie pewną sygnaturą relacyjną. Standardowy problem istnienia modelu możemy zdefiniować następująco:

Michał Pilipczuk
mp248287@students.mimuw.edu.pl
student Jednoczesnych Studiów Informatyczno-Matematycznych
Uniwersytet Warszawski

ISTNIENIE MODELU (SATISFIABILITY) **Wejście:** Formuła $\varphi \in FO[\tau]$ **Pytanie:** Czy istnieje model M taki, że $M \models \varphi$?

Nierozstrzygalność powyższego problemu dla dowolnych formuł pierwszego rzędu φ nad pewną sygnaturą τ jest klasycznym wynikiem teorii obliczeń. Podstawową przyczyną tego fenomenu jest to, że w logice pierwszego rzędu da się wydefiniować kratę. Wówczas, biorąc dowolną maszynę Turinga, możemy na jej podstawie zbudować taką formułę pierwszego rzędu φ, której model będzie biegiem tejże maszyny, zakończonym akceptacją, zapisanym w kolejnych wierszach kraty. Tym samym rozwiązując problem istnienia modelu dla dowolnej formuły pierwszego rzędu φ, umielibyśmy rozwiązać problem stopu.

Okaże się, że logika FO_2 jest dużo słabsza od FO – problem istnienia modelu dla formuł FO_2 jest rozstrzygalny, nawet jeśli sygnatura jest elementem wejścia dla algorytmu. Co więcej, logika FO_2 ma własność modelu skończonego, tzn. jeśli będzie istniał pewien model, to będzie istniał również model skończony.

3. Postać normalna Scotta

Logika FO_2 jest o tyle poręczna dla informatyka, że jej formułę można sprowadzić do bardzo prostej postaci, tzw. postaci normalnej Scotta.

Twierdzenie 1 (Postać normalna Scotta)**.** *Istnieje algorytm, który mając daną sygnaturę τ oraz formułę $\varphi \in FO_2[\tau]$, znajduje sygnaturę τ' o relacjach co najwyżej binarnych oraz formułę $\psi \in FO_2[\tau']$ o następujących własnościach. Istnienie modelu dla φ jest równoważne istnieniu modelu dla ψ oraz ψ jest koniunkcją:*

(i) *formuły ograniczającej postaci $\forall_x \forall_y\, \alpha(x, y)$, gdzie $\alpha(x, y)$ jest alternatywą sprawdzeń możliwych podstruktur generowanych przez x, y,*

(ii) *formuł świadkujących postaci*

$$\forall_x \left[R(x) \implies \exists_y \left[C_1(x, y) \wedge C_2(y, x) \wedge (R_1(y) \vee R_2(y) \vee R_3(y) \vee \ldots \vee R_k(y))\right]\right],$$

(iii) *formuł startowych postaci $\exists_x R(x)$,*

(iv) *aksjomatyzacji relacji unarnych oraz binarnych: każdy element jest w dokładnie jednej relacji unarnej, każda uporządkowana para różnych elementów jest w dokładnie jednej relacji binarnej, elementy w relacjach binarnych są różne.*

O relacjach unarnych i binarnych będziemy myśleć jako o kolorowaniu elementów modelu oraz krawędzi skierowanych łączących je.

Przyjrzyjmy się formułom świadkującym. Mówią one, że każdy element określonego koloru musi mieć świadka: inny element, z którym łączą go krawędzi określonych kolorów i który sam ma kolor z pewnej listy. Postać Scotta można rozumieć jako pewnego rodzaju warunek na kompromis: z jednej strony mamy potrzebę istnienia świadków dla elementów określonego koloru, z drugiej zaś niektóre układy przestrzenne są zabronione.

4. Rozstrzygalność problemu istnienia modelu dla logiki FO_2

Uzbrojeni w postać normalną Scotta możemy przejść do dowodu, że FO_2 jest istotnie słabsze niż pełna logika pierwszego rzędu.

Twierdzenie 2. *Problem istnienia modelu dla logiki FO_2 jest rozstrzygalny, nawet gdy sygnatura jest częścią wejścia dla algorytmu. Co więcej, dla każdej sygnatury relacyjnej τ logika $FO_2[\tau]$ ma własność modelu skończonego.*

Dowód. Bez utraty ogólności możemy założyć, że dana formuła φ jest w postaci normalnej Scotta, gdyż sprowadzenie do tej postaci zachowuje własność modelu skończonego. Pokażemy, że jeśli φ ma model, to ma model skończony i mocy ograniczonej przez pewną funkcję rozmiarów τ oraz φ. Wówczas dowiedziemy całej tezy, gdyż istnienie modelu można będzie sprawdzić poprzez brutalne rozpatrzenie wszystkich modeli mocy nie większej od uzyskanego ograniczenia. Powiedzmy, że τ ma k kolorów wierzchołkowych i l krawędziowych.

Załóżmy więc, że M jest pewnym modelem dla φ. Skonstruujemy model N dla φ o mocy ograniczonej. Konstrukcję zaczynamy od formuł startowych: świadczą one o istnieniu elementów pewnych kolorów w modelu M, dołączamy więc te elementy do modelu N. Każdy z nich ma pewnych świadków w modelu M, których istnienie wynika z klauzul świadkujących. Dołączamy więc tych świadków do modelu N i kolorujemy krawędzie, po których nastąpiło świadkowanie na odpowiedni kolor, jak w modelu M. Żadnych innych krawędzi nie kolorujemy. Następnie ci świadkowie mają swoich świadków, tamci swoich itd. – dołączamy świadków, którzy jeszcze nie są w modelu N. Postępujemy tak ω kroków. Następnie kolorujemy wszystkie niepokolorowane krawędzie tak jak w modelu M. Zauważmy, że każdy element tak stworzonego modelu N ma potrzebnych mu świadków oraz wszystkie krawędzie są pokolorowane w sposób dopuszczalny, więc $N \models \varphi$.

Oczywiście tak stworzone N nie musi być w ogóle skończone, więc musimy nieco zmodyfikować konstrukcję. Załóżmy, że w danym kroku konstrukcji element x o kolorze P ma dostać nowego świadka o kolorze Q po krawędziach o kolorach C_1, C_2. Załóżmy ponadto, że istnieje element y o kolorze Q dołączony już do modelu, taki że kolory krawędzi pomiędzy x a y nie są jeszcze ustalone (lub już pokolorowane zgodnie z kolorami C_1, C_2). Wówczas zamiast dodawać nowy element do modelu N, zadamy na parach (x, y) oraz (y, x) kolory C_1, C_2 i zadeklarujemy, że teraz y będzie szukanym świadkiem.

Zauważmy, że każdy element może wymagać co najwyżej l^2 różnych świadków danego koloru Q. Załóżmy, że w pewnym momencie konstrukcji pojawi się już co najmniej l^2 elementów

koloru Q. Wówczas każdy element dołączony do modelu co najmniej trzy fazy później już nie będzie tworzył (jako swoich świadków) nowych elementów koloru Q – gdyż ze wszystkimi starymi elementami koloru Q nie będzie miał określonych kolorów krawędzi, więc zawsze uda nam się przenieść świadka. Zatem począwszy od trzeciej fazy konstrukcji po tym momencie „wysycenia" koloru Q, żaden nowy element koloru Q już się nie pojawi.

Wyciągamy stąd wniosek, że konstrukcja modelu N zakończy się niedodaniem żadnego nowego świadka po liczbie faz ograniczonej przez $k(l^2 + 3)$. W przeciwnym razie dobralibyśmy z każdej fazy po jednym dodanym elemencie i z zasady szufladkowej Dirichleta któryś kolor byłby dodawany w co najmniej $l^2 + 3$ fazach, co przeczyłoby wcześniejszym rozważaniom.

Ponieważ w każdej fazie model N może powiększyć się co najwyżej tyle razy, ile jest formuł świadkujących, wielkość uzyskanego modelu jest ograniczona przez funkcję od τ, φ. □

5. Rozszerzenia problemu

Jak widzimy, rozwiązanie problemu istnienia modelu dla zwykłego FO_2 było dość techniczne, ale w gruncie rzeczy nietrudne. Spróbujmy zbadać, gdzie leży granica pokazanej rozstrzygalności: ile można do FO_2 dodać „artefaktów", by ją zachować?

Zastanówmy się, jak to pytanie sformalizować. Oznaczmy przez ψ pewien ustalony warunek, aksjomat niewyrażalny w FO_2, który chcemy dodać do formuły φ. Teraz pytanie w problemie istnienia modelu będzie następujące: czy istnieje takie M, że $M \models \varphi \wedge \psi$?

Jak powiedzieliśmy we wstępie, podstawową własnością niewyrażalną w FO_2 jest przechodniość relacji. Skupimy się więc na zdaniach ψ, które kodują, że $1, 2, 3, \ldots$ relacje z sygnatury są relacjami równoważności, porządkami liniowymi lub – bardziej ogólnie – porządkami częściowymi.

Zobaczmy, jak wówczas kształtuje się sprawa rozstrzygalności:

	relacje równoważności	porządki liniowe	porządki częściowe
1	**+**	**+**	**?**
2	**+**	**+**	**–**
≥ 3	**–**	**?** pomiędzy 3 a 7, **–** dla ≥ 8	**–**

W powyższej tabeli przez „**+**" oznaczyliśmy przypadek rozstrzygalności, przez „**–**" nierozstrzygalności, a przez „**?**" brak znanej odpowiedzi.

6. Przypadki rozstrzygalności

Metody używane do pokazywania rozstrzygalności FO_2 z dodanym aksjomatem bazują na stopniowym upraszczaniu modelu, aż osiągnie on pewną ustaloną, „sprawdzalną" strukturę. Możemy

tu zawsze korzystać z pewnej odmiany postaci Scotta, charakterystycznej dla aksjomatu. Omówimy to pokrótce na przykładzie jednej relacji równoważności.

Na początku dowodzimy, że każdą klasę abstrakcji relacji da się zamienić na sztuczny „substytut", który ma takie same interakcje z resztą modelu w sensie istnienia świadków, lecz posiada ograniczony rozmiar. Podmieniamy każdą klasę abstrakcji w dany sposób. Zauważmy teraz, że różnych ograniczonych klas abstrakcji jest tylko skończenie wiele. Wykazujemy zatem, że liczbę takich samych klas abstrakcji w modelu możemy zawsze zredukować do ograniczonej przez pewną stałą. Po tych redukcjach wielkość modelu jest ograniczona przez funkcję od sygnatury i formuły, więc możemy sprawdzić wszystkie struktury aż do ustalonej wielkości.

7. Przypadki nierozstrzygalności

Podstawową metodą dowodzenia nierozstrzygalności problemu istnienia modelu dla danej logiki jest wyaksjomatyzowanie w niej kraty i pokazanie sposobu takiego przetłumaczenia maszyny Turinga na formułę, by jej model musiał być obliczeniem maszyny zapisanym w kolejnych wierszach kraty. Tym samym, odpowiadając na pytanie o istnienie modelu dla formuły, rozwiązujemy problem stopu. Okazuje się, że maszyna Turinga nie jest problemem dla FO_2 – problemem jest sama krata.

Spróbujmy formalnie zdefiniować kratę. Kratą $G_{\mathbb{N}}$ nazwiemy strukturę nad sygnaturą z dwiema relacjami binarnymi H, V, której dziedziną jest $\mathbb{N} \times \mathbb{N}$, zaś relacje H, V są zbiorami par odpowiednio postaci $((p,q),(p,q+1))$ i $((p,q),(p+1,q))$ dla wszystkich $p,q \in \mathbb{N}$. Analogicznie definiujemy pełną kratę $G_{\mathbb{Z}}$ oraz kraty toroidalne G_m – gdzie zamiast liczb naturalnych używamy grupy $\mathbb{Z}_m$.

Teraz powiemy, że klasa struktur $\mathfrak{G}$ nad sygnaturą relacyjną zawierającą H, V jest *bogata*, jeśli

(i) co najmniej jedna z krat $G_{\mathbb{N}}$, $G_{\mathbb{Z}}$ należy do $\mathfrak{G}$,

(ii) dla każdego n istnieje takie k, że G_{nk} należy do $\mathfrak{G}$.

Przez należenie rozumiemy tu bycie izomorficznym z pewnym elementem z zapomnianymi wszystkimi relacjami poza H, V.

Sformułujemy teraz kluczowe twierdzenie, które wyraża intuicję, że wydefiniowanie kraty pociąga za sobą nierozstrzygalność problemu istnienia modelu.

Twierdzenie 3. *Załóżmy, że bogata klasa $\mathfrak{G}$ jest definiowalna w FO_2 z dodatkowym aksjomatem ψ, tzn. istnieje taka formuła $\varphi \in FO_2$, że $M \models \varphi \wedge \psi$ wtedy i tylko wtedy, gdy $M \in \mathfrak{G}$. Załóżmy dodatkowo, że struktury w $\mathfrak{G}$ spełniają warunki:*

(i) $\forall_x \exists_y H(x,y)$, $\forall_x \exists_y V(x,y)$,

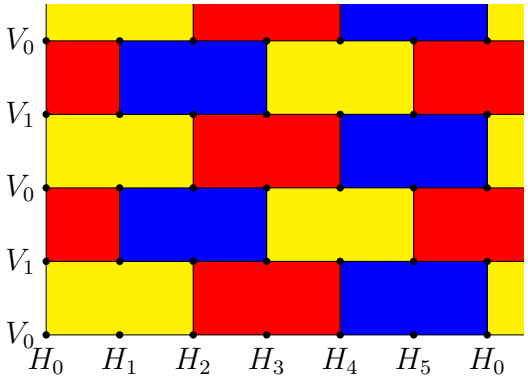
(ii) $\forall_{x,y,z,w} [[H(x,y) \wedge V(x,z) \wedge V(y,w)] \implies H(z,w)]$.

Wówczas problem istnienia modelu dla logiki FO_2 z aksjomatem ψ nad pewną sygnaturą relacyjną jest nierozstrzygalny.

Pierwszy warunek nie jest problemem – wyraża się w FO_2, więc wystarczy go zawrzeć w formule φ. Dopiero drugi jest esencją bycia kratą: definiuje pojedynczy kwadracik. Do jego sprawdzenia musimy używać informacji spoza FO_2, zawartej w aksjomacie ψ.

8. Krata w akcji na przykładzie trzech relacji równoważności

Pokażemy, że problem istnienia modelu dla FO_2 z trzema relacjami równoważności jest nierozstrzygalny. Będziemy chcieli tak zbudować formułę φ, by modelem była krata, taka jak na rysunku.



Cegiełki odpowiednich kolorów odpowiadają klasom abstrakcji trzech relacji równoważności – każda z nich (oprócz niepełnych cegiełek na brzegu) jest 6-elementowa i zawiera wierzchołki na brzegu cegiełki. Wierzchołki niebędące w jednej cegiełce danego koloru nie są w odpowiadającej mu relacji równoważności.

Dodatkowo dodamy osiem predykatów unarnych $H_0, H_1, \ldots, H_5, V_0, V_1$. Każdy element modelu spełnia dokładnie jeden predykat H_i oraz jeden V_j – definiują one reszty odpowiednio modulo 6 i modulo 2 ze współrzędnych elementu na kracie.

Przejdźmy zatem do budowy formuły φ. Na początku definiujemy w niej proste aksjomatyzacje predykatów H_i, V_j oraz pierwszy warunek z Twierdzenia 3. Wszystko to oczywiście należy do FO_2. Następnie przechodzimy do stwierdzania, jak może wyglądać sytuacja przestrzenna pomiędzy elementami w relacji H. Zapisujemy to w formie

$$\forall_x \forall_y \left[H(x,y) \implies (\varphi_1 \vee \varphi_2 \vee \ldots \vee \varphi_{12}) \right],$$

gdzie φ_i to formuły kodujące każdy z 12 możliwych układów przestrzennych pomiędzy x i y, występujących zależnie od reszt modulo 6 oraz 2 współrzędnych x i y. Przykładowo:

$$\varphi_1 = \mathit{Yellow}(x,y) \wedge \mathit{Red}(x,y) \wedge H_0(x) \wedge V_0(x) \wedge H_1(y) \wedge V_0(y).$$

Analogicznie zapisujemy formuły dla relacji V. Na koniec dodajemy kluczowy warunek wystarczający na relację H. Zapisujemy go jako

$$\forall_x \forall_y \left[(\psi_1 \vee \psi_2 \vee \ldots \vee \psi_{12}) \implies H(x,y) \right],$$

gdzie ψ_i znów kodują możliwe stosunki przestrzenne pomiędzy x i y, przykładowo:

$$\psi_1 = Red(x,y) \wedge H_0(x) \wedge V_0(x) \wedge H_1(y) \wedge V_0(y).$$

Uwaga 4. O ile w formułach φ_i zapisywaliśmy informacje o wszystkich relacjach równoważności pomiędzy x i y, to w ψ_i wymagamy jedynie tej pochodzącej z cegły poniżej krawędzi kraty.

Czytelnik łatwo sprawdzi, że kraty $G_{\mathbb{N}}, G_{\mathbb{Z}}$ oraz G_{6n} dla $n \geq 1$ są modelami skonstruowanej formuły. Do sprawdzenia wszystkich założeń Twierdzenia 3 potrzeba nam jedynie upewnienia się co do prawdziwości drugiego warunku. Dobierzmy więc takie x, y, z, w, że $H(x,y)$, $V(x,z)$ oraz $V(y,w)$. Skoro $H(x,y)$, to x, y muszą być w jednym z 12 stosunków przestrzennych określonych przez formuły φ_i. Załóżmy, że to φ_1 jest spełnione, tzn. x ma reszty z dzielenia współrzędnych równe $(0,0)$, zaś y ma $(1,0)$. Korzystając z formuł dodanych analogicznie dla V, wiemy już dokładnie, jakie są reszty z dzielenia współrzędnych z oraz w: są to $(0,1)$ oraz $(1,1)$. Dodatkowo z tychże formuł wiemy, że pary (x,y), (x,z), (y,w) są równoważne w relacji $Yellow$. Używamy więc przechodniości żółtej relacji równoważności: (z,w) są też żółto równoważne. Teraz wystarczy użyć warunku koniecznego na H, by wykazać, że $H(z,w)$.

Pozostałe 11 przypadków pozostawiamy Czytelnikowi w charakterze ćwiczenia.

9. Jeden porządek częściowy

Kwestia rozstrzygalności problemu istnienia modelu dla FO_2 z aksjomatem gwarantującym, że jedna relacja jest porządkiem częściowym, jest nadal otwarta. Wszystko wskazuje na to, że problem będzie rozstrzygalny. Za pomocą sztuczek technicznych da się wyeleminować wszystkie relacje binarne oprócz porządku oraz zapisać formułę w odpowiedniej postaci Scotta. Niestety, głównie z tego powodu, problem wydaje się bardzo skomplikowany technicznie i trudny.

Skończona aksjomatyzowalność matryc logicznych i problemy z nią związane

Rafał Polek, Monika Porębska

Streszczenie. Praca ma charakter poglądowy. Rozważamy trzy sposoby rozumienia skończonej aksjomatyzowalności systemu logicznego zadanego przez skończony zbiór wartości i pewien skończony zbiór spójników. Podajemy definicje matrycy logicznej, tautologii i poprawnej reguły wnioskowania. W oparciu o literaturę przytaczamy przykłady skończonych matryc, których zbiory tautologii lub zbiory reguł poprawnych nie dają się skończenie zaksjomatyzować. Otwartym problemem jest, czy własność skończonej aksjomatyzowalności jest niezależna od języka.

1. Wstęp

Teorie matematyczne staramy się często opisać przy pomocy prostego, skończonego zbioru aksjomatów i reguł. Klasyczny rachunek zdań (KRZ) jest przykładem takiej teorii. Jak dobrze wiadomo, tautologie klasycznego rachunku to te formuły, które przy każdym wartościowaniu przyjmują wartość 1. Wiadomo także, że wszystkie tautologie KRZ zapisane przy użyciu spójników $\to$ i $\neg$ można w sposób formalny wyprowadzić z pewnego zbioru trzech aksjomatów używając podstawień i reguły odrywania (czyli Modus Ponens, w skrócie (MP)):

$$\text{(MP)} \quad \frac{x \to y, x}{y}.$$

Aksjomaty KRZ:

(i) $x \to (y \to x)$,

(ii) $(x \to (y \to z)) \to ((x \to y) \to (x \to z))$,

(iii) $(\neg x \to \neg y) \to (y \to x)$.

Rafał Polek
polek_rafal@wp.pl
student matematyki
Politechnika Krakowska

Monika Porębska
monika.porebska@poczta.onet.pl
studentka matematyki
Politechnika Krakowska

Ten zbiór trzech aksjomatów jest przykładem *skończonej aksjomatyzacji* KRZ.

Podstawowa definicja tautologii odwołuje się do dwuelementowej algebry Boole'a $\{0, 1\}$ z działaniami $\vee, \wedge, \neg, \rightarrow$ określonymi dobrze znanymi tabelkami zero-jedynkowymi oraz wyróżnioną wartością 1, przy czym, z uwagi na wyrażalność jednych spójników przez inne, można zmniejszyć zestaw działań i na przykład użyć tylko $\rightarrow$ i $\neg$. Taki układ zbioru z działaniami i wyróżnioną wartością jest przykładem tzw. *matrycy logicznej* (patrz definicja 1 poniżej). Dla każdej matrycy można zdefiniować zbiór jej *tautologii* (Definicja 4) i pytać, czy istnieje skończony zbiór aksjomatów, z których można wyprowadzić wszystkie te tautologie. W przypadku dowolnych matryc często trzeba przyjąć inne niż Modus Ponens reguły wnioskowania i dlatego pytanie o skończoną aksjomatyzację zawiera też pytanie o skończony zbiór *reguł wnioskowania*, których w takim wyprowadzeniu można używać.

2. Pojęcia podstawowe

Pojęcia podstawowe przedstawione w tym rodziale pochodzą z literatury. Zainteresowanego czytelnika odsyłamy do [12].

Definicja 1. *Matrycą logiczną* (w skrócie: matrycą) nazywamy układ

$$\mathfrak{M} = \langle M, f_1, \ldots, f_m, D\rangle$$

złożony z niepustego zbioru M, działań $f_1, \ldots, f_m$ określonych na zbiorze M oraz niepustego podzbioru $D \subset M$. Elementy zbioru D nazywamy *wartościami wyróżnionymi* matrycy $\mathfrak{M}$.

W praktyce najczęściej używa się działań jedno- i dwuargumentowych, ale w powyższej definicji dopuszczamy działania o dowolnej argumentowości $n \in \mathbb{N}$.

Przykład 2. Dwuelementowa matryca boole'owska:

$$\mathfrak{B}_1 = \langle\{0, 1\}, \rightarrow, \neg, \{1\}\rangle.$$

Zanim zdefiniujemy pojęcie tautologii matrycy, wprowadzimy najpierw pojęcie termu w jej języku. Niech M będzie niepustym zbiorem, $\mathcal{F}$ skończonym zbiorem działań na M, $D \subset M$. Każde działanie f ze zbioru $\mathcal{F}$ jest oznaczone pewnym znakiem – symbolem tego działania. Niech λ_f będzie symbolem oznaczającym działanie f, a $\Lambda = \{\lambda_f \colon f \in \mathcal{F}\}$.

Definicja 3. Niech V oznacza zbiór zmiennych, a $\mathcal{F}$ pewien skończony zbiór działań. Symbolem $\mathrm{Te}_{\mathcal{F}}(V)$ oznaczamy najmniejszy taki zbiór wyrażeń, dla którego spełnione są następujące warunki:

- $V \subset \mathrm{Te}_{\mathcal{F}}(V)$,
- dla dowolnych $t_1, \ldots, t_n \in \mathrm{Te}_{\mathcal{F}}(V)$ i dowolnego n-argumentowego działania f wyrażenie $\lambda_f(t_1, \ldots, t_n)$ należy do $\mathrm{Te}_{\mathcal{F}}(V)$.

Elementy zbioru $\mathrm{Te}_{\mathcal{F}}(V)$ nazywać będziemy *termami* języka $\mathcal{F}$ nad zbiorem zmiennych V.

Zbiór $\mathrm{Te}_{\mathcal{F}}(V)$ z działaniami odpowiadającymi działaniom ze zbioru $\mathcal{F}$ w naturalny sposób tworzy strukturę algebraiczną. Jeśli $\mathfrak{M} = \langle M, \mathcal{F}, D\rangle$ jest matrycą, to *wartościowaniem* w $\mathfrak{M}$ nazywamy dowolny homomorfizm z $\mathrm{Te}_{\mathcal{F}}(V)$ w $(M, \mathcal{F})$.

Przykładami termów w języku algebry Boole'a $\mathfrak{B}_1$ są:

$$x, \quad x \to y, \quad (\neg x \to \neg y) \to (y \to x).$$

Ponieważ tradycyjnie takie wyrażenia nazywa się formułami w KRZ, to termy będziemy też nazywać formułami.

Definicja 4. Dla danej matrycy $\mathfrak{M} = \langle M, \mathcal{F}, D\rangle$ oraz $t \in \mathrm{Te}_{\mathcal{F}}(V)$ mówimy, że t jest *tautologią* $\mathfrak{M}$, jeżeli dla każdego wartościowania $w\colon \mathrm{Te}_{\mathcal{F}}(V) \to M$, mamy: $w(t) \in D$.

Definicja 5. *Regułą* nazywamy parę (X, α), gdzie $X \cup \{\alpha\}$ jest pewnym skończonym podzbiorem zbioru formuł. Elementy zbioru X nazywamy przesłankami, zaś formułę α wnioskiem tej reguły.

Regułę (X, α) zapisujemy $\dfrac{X}{\alpha}$ i czytamy „z X dedukuj α".

Definicja 6. Powiemy, że reguła $\dfrac{X}{\alpha}$ jest *poprawna w* $\mathfrak{M}$, jeśli dla dowolnego wartościowania w zachodzi warunek: jeśli $w(X) \subset D$, to $w(\alpha) \in D$.

Wspomniana wcześniej reguła odrywania (MP) jest przykładem poprawnej reguły wnioskowania dla matrycy $\mathfrak{B}_1$. Zauważmy bowiem, że przy dowolnym wartościowaniu, jeżeli przesłanki (MP) przyjmują wartość wyróżnioną 1, to wówczas jej wniosek również musi przyjąć wartość wyróżnioną.

Rozważać można także matryce związane z logikami nieklasycznymi. Przykładem są trójelementowe matryce Łukasiewicza i Heytinga zaprezentowane poniżej.

Przykład 7. Trójelementowa matryca Łukasiewicza:

$$\mathfrak{L}_3 = \Big\langle \{0, \frac{1}{2}, 1\}, \wedge, \vee, \to, \neg, \{1\} \Big\rangle,$$

gdzie działania opisane są za pomocą poniższych tabelek:

$\wedge$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

$\vee$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

$\to$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	0	$\frac{1}{2}$	1

x	$\neg x$
0	1
$\frac{1}{2}$	$\frac{1}{2}$
1	0

Przykład 8. Trójelementowa matryca Heytinga:

$$\mathfrak{H}_3 = \Big\langle \{0, \frac{1}{2}1\}, \wedge, \vee, \rightarrow, \neg, \{1\} \Big\rangle,$$

gdzie działania opisane są za pomocą poniższych tabelek:

$\wedge$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

$\vee$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

$\rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	1	1
1	0	$\frac{1}{2}$	1

x	$\neg x$
0	1
$\frac{1}{2}$	0
1	0

Warto zauważyć, że matryce Łukasiewicza i Heytinga różnią się w niewielkim stopniu, mianowicie jedyna różnica występuje w definicjach działań $\rightarrow$ i $\neg$, a konkretnie w wartościach $\frac{1}{2} \rightarrow 0$ i $\neg\frac{1}{2}$. Ta różnica wystarcza, by zbiory ich tautologii nie pokrywały się. Zauważmy, że term $\neg\neg x \rightarrow x$ jest tautologią matrycy $\mathfrak{L}_3$, ale nie jest tautologią matrycy $\mathfrak{H}_3$. Podobnie term $\neg(x \wedge \neg x)$ jest tautologią matrycy $\mathfrak{H}_3$, ale nie jest tautologią matrycy $\mathfrak{L}_3$.

3. Skończona aksjomatyzowalność

Zakładamy, że pojęcie *wyprowadzenia*, którym posługujemy sie w tym rozdziale, jest intuicyjnie jasne. *Wyprowadzić* to znaczy wskazać dowód z wykorzystaniem aksjomatów i reguł. Formalną definicję można znaleźć w [12]. Formułę lub regułę, która ma dowód, nazywa się dowiedlną.

Niech dana będzie matryca logiczna $\mathfrak{M}$, dla której (MP) jest regułą poprawną. Można pytać, czy istnieje skończony zbiór aksjomatów, z którego wszystkie tautologie $\mathfrak{M}$ dają się wyprowadzić przy użyciu (MP) i podstawiania. Mamy więc następujący

Problem 9. *Czy dla dowolnej skończonej matrycy $\mathfrak{M}$ da się wskazać taki skończony zbiór aksjomatów, z których przy użyciu jedynie reguły Modus Ponens wszystkie jej tautologie byłyby dowiedlne?*

O matrycy, dla której taki zbiór aksjomatów istnieje, powiemy, że jest *skończenie aksjomatyzowalna względem reguły Modus Ponens.* Problem ten rozważano już w I połowie XX wieku i okazało się, że tak być nie musi. W 1935 r. M. Wajsberg ([9], patrz też [11], skąd zaczerpnęliśmy tę informację) podał następujące kontrprzykłady, po jednym dla każdego $k \geq 1$.

Przykład 10 ([9])**.** k-elementowa matryca Wajsberga, $k \geq 1$:

$$\mathfrak{M}_k = \Big\langle \{0, 1, \ldots, k\}, \neg, \rightarrow, \{0\} \Big\rangle,$$

gdzie $\forall_{x,y\in\{0,1,\ldots,k\}}\ x \rightarrow y = y$ i $\neg x = 0$.

Powyższe matryce $\mathfrak{M}_k$ są przykładami skończonych matryc, które nie są skończenie aksjomatyzowalne względem (MP). Na rezultat Wajsberga można też popatrzeć tak: reguła Modus Ponens to za mało, by wskazać skończony zbiór aksjomatów, z których wszystkie tautologie tej matrycy byłyby dowiedlne [11]. Jednak jeśli dopuścimy inny skończony zbiór reguł, to okazuje się, że matryce Wajsberga dają się skończenie zaksjomatyzować przy użyciu tych innych reguł (szczegóły i wyjaśnienie można znaleźć np. w [6]). P. Wojtylak w [11] zaproponował następującą modyfikację pytania o skończoną aksjomatyzację:

Problem 11. *Czy dla dowolnej skończonej matrycy $\mathfrak{M}$ da się wskazać taki skończony zbiór reguł, niekoniecznie zawierający (MP), że wszystkie tautologie matrycy $\mathfrak{M}$ da się dowieść przy użyciu tych reguł z jakiegoś skończonego zbioru aksjomatów podstawowych?*

W [10] P. Wojtylak przypisuje postawienie tego problemu W. Rautenbergowi. Matryca $\mathfrak{M}$, dla której taki zbiór reguł istnieje, nazywa się *skończenie aksjomatyzowalną.* Pytanie o skończoną aksjomatyzowalność jest więc pytaniem o istnienie skończonego zbioru aksjomatów i reguł pozwalających wyprowadzić wszystkie tautologie danej matrycy. Jeśli $\mathfrak{M}$ jest skończenie aksjomatyzowalna, to można też pytać dalej, czy istnieje skończony zbiór jej reguł poprawnych, które wystarczają do wyprowadzenia z nich wszystkich reguł poprawnych w $\mathfrak{M}$. Mamy więc

Problem 12. *Czy dla każdej skończonej matrycy $\mathfrak{M}$ istnieje taki skończony zbiór $\mathcal{R}$ reguł poprawnych $\mathfrak{M}$, że z $\mathcal{R}$ da się wyprowadzić wszystkie pozostałe reguły poprawne tej matrycy?*

Jeśli taki zbiór reguł istnieje, to mówimy, że matryca jest *skończenie bazowalna.* Pojęcie to wprowadził R. Suszko (informacja z [13]). Początkowo przypuszczano [1], że wszystkie skończone matryce są skończenie bazowalne. Najpierw wykazano, że wszystkie dwuelementowe matryce posiadają tę własność [7, 2]. Naturalne było więc pytanie, czy tak jest też dla większych matryc skończonych. Jednak w literaturze pojawiły się przykłady matryc, kolejno: 6- i 5-elementowych, które skończenie bazowalne nie są [13, 8]. W końcu znaleziono też [14] przykład matrycy trójelementowej, która nie posiada skończonej bazy. Przykład 14 poniżej zawiera dwie matryce: $\mathfrak{M}_{\mathrm{I}}$ i $\mathfrak{M}_{\mathrm{II}}$, które nie są skończenie bazowalne. Druga z nich jest jej nieznaczną równoważną modyfikacją matrycy z [14].

Trzy rozważane tu pojęcia: skończonej aksjomatyzowalności względem ustalonego zbioru reguł, skończonej aksjomatyzowalności, jak i skończonej bazowalności nie są sobie nawzajem równoważne. Zachodzą jednak pewne nietrudne do zaobserwowania zależności:

Obserwacja 13.

(i) *Jeśli matryca $\mathfrak{M}$ jest skończenie aksjomatyzowalna względem pewnego ustalonego, skończonego zbioru reguł, to jest ona skończenie aksjomatyzowalna.*

(ii) *Jeśli matryca $\mathfrak{M}$ jest skończenie bazowalna, to jest ona skończenie aksjomatyzowalna.*

Implikacja odwrotna do tej, o której mowa w punkcie (ii), nie zachodzi, o czym świadczy na przykład matryca $\mathfrak{M}_{\mathrm{II}}$ z Przykładu 14, która jest skończenie aksjomatyzowalna, ale nie jest skończenie bazowalna (patrz Twierdzenie 15).

Przykład 14. Dla $i \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}\}$ rozważamy matryce $\mathfrak{M}_i = \langle\{0,1,2\}, \cdot_i, \{2\}\rangle$, gdzie działanie $\cdot_i$ zadane jest jedną z poniższych tabel:

$\cdot_{\mathrm{I}}$	0	1	2
0	2	2	2
1	2	2	2
2	**1**	2	2

$\cdot_{\mathrm{II}}$	0	1	2
0	2	2	2
1	**1**	2	2
2	2	2	2

$\cdot_{\mathrm{III}}$	0	1	2
0	**1**	2	2
1	2	2	2
2	2	2	2

Okazuje się, że mimo nieznacznych różnic w definicjach działań, matryce te bardzo różnią się jedna od drugiej, jeśli chodzi o skończoną aksjomatyzowalność. Prawdziwe jest następujące twierdzenie:

Twierdzenie 15 ([14, 11, 3])**.** *Matryce z przykładu 14 posiadają następujące własności:*

(i) $\mathfrak{M}_{\mathrm{I}}$ *nie jest skończenie aksjomatyzowalna i nie jest skończenie bazowalna.*

(ii) $\mathfrak{M}_{\mathrm{II}}$ *jest skończenie aksjomatyzowalna, ale nie jest skończenie bazowalna.*

(iii) $\mathfrak{M}_{\mathrm{III}}$ *jest skończenie aksjomatyzowalna i jest skończenie bazowalna.*

Matryce $\mathfrak{M}_{\mathrm{I}}$ i $\mathfrak{M}_{\mathrm{II}}$ dostarczają przykładów na to, że jeśli matryca $\mathfrak{M}$ nie jest skończenie bazowalna, to nie możemy nic wnioskować na temat jej skończonej aksjomatyzowalności, zaś matryce $\mathfrak{M}_{\mathrm{II}}$ i $\mathfrak{M}_{\mathrm{III}}$ pokazują, że jeśli matryca $\mathfrak{M}$ jest skończenie aksjomatyzowalna, to nie możemy nic wnioskować na temat jej skończonej bazowalności.

4. Matryce równoważne

Matryca boole'owska $\mathfrak{B}_1$ z Przykładu 2 została zdefiniowana przy użyciu działań $\to$ i $\neg$. Wiadomo, że można ją też zdefiniować równoważnie używając zbiorów innych działań.

Przykład 16.

$$\mathfrak{B}_2 = \langle\{0,1\}, \wedge, \neg, \{1\}\rangle \qquad \mathfrak{B}_4 = \langle\{0,1\}, |, \{1\}\rangle$$
$$\mathfrak{B}_3 = \langle\{0,1\}, \vee, \neg, \{1\}\rangle \qquad \mathfrak{B}_5 = \langle\{0,1\}, \downarrow, \{1\}\rangle$$

Symbol $|$ oznacza kreskę Shefera (NAND), natomiast $\downarrow$ strzałkę Pierce'a (NOR).

Matryce $\mathfrak{B}_1 - \mathfrak{B}_5$ są sobie wzajemnie w pewien sposób równoważne. Jest to tak zwana *termalna równoważność*, w której chodzi o to, że działania matrycy $\mathfrak{B}_i$ i działania matrycy $\mathfrak{B}_j$ (dla $i, j = 1, 2, 3, 4, 5$) dają się nawzajem wyrazić jedne przez drugie. Na przykład:

$$x|y = \neg x \vee \neg y,\ x \vee y = (x|x)|(y|y),\ \neg x = x|x.$$

Wprowadźmy definicję równoważności termów:

Definicja 17. Niech dany będzie niepusty zbiór M oraz zbiory $\mathcal{F}$ i $\mathcal{K}$ działań określonych na M, być może różne. Niech $t \in \mathrm{Te}_{\mathcal{F}}(V)$, $s \in \mathrm{Te}_{\mathcal{K}}(V)$. Mówimy, że termy t, s są *równoważne* i piszemy $t \equiv s$ wtedy i tylko wtedy, gdy dla dowolnego wartościowania zmiennych $\hat{v}\colon\ V \to M$ zachodzi warunek $v_1(t) = v_2(s)$, gdzie $v_1,\ v_2$ są odpowiednio rozszerzeniami $\hat{v}$ na zbiory $\mathrm{Te}_{\mathcal{F}}(V),\ \mathrm{Te}_{\mathcal{K}}(V)$.

Definicja 18. Mówimy, że matryce logiczne $\mathfrak{M} = \langle M, \mathcal{F}, D\rangle$, $\mathfrak{N} = \langle M, \mathcal{K}, D\rangle$ są *termalnie równoważne* i piszemy $\mathfrak{M} \equiv \mathfrak{N}$, jeżeli spełnione są warunki:

(i) $\forall_{f\in\mathcal{F}}\, \exists_{\beta\in\mathrm{Te}_{\mathcal{K}}(V)}\ \lambda_f(x_1, \ldots, x_n) \equiv \beta$,

(ii) $\forall_{g\in\mathcal{K}}\, \exists_{\alpha\in\mathrm{Te}_{\mathcal{F}}(V)}\ \lambda_g(x_1, \ldots, x_k) \equiv \alpha$.

Symbole $x_1, \ldots, x_n$ oznaczają n początkowych zmiennych ze zbioru V, gdzie n jest argumentowością działania f, podobnie $x_1, \ldots, x_k$ oznaczją k początkowych zmiennych ze zbioru V, gdzie k jest argumentowością g.

Prościej powiemy, że dwie matryce $\mathfrak{M}$ i $\mathfrak{N}$ z działaniami z różnych zbiorów są równoważne, jeżeli każde działanie w matrycy $\mathfrak{M}$ da się wyrazić przy użyciu symboli działań z matrycy $\mathfrak{N}$ i podobnie każde działanie w matrycy $\mathfrak{N}$ zapiszemy przy użyciu działań matrycy $\mathfrak{M}$. Posługując się nieformalną definicją równoważności matryc, łatwo stwierdzić, że zdefiniowane wcześniej matryce $\mathfrak{B}_2$, $\mathfrak{B}_3$ są termalnie równoważne. Istotnie, na mocy praw de Morgana każde działanie z matrycy $\mathfrak{B}_2$ da się zapisać za pomocą działań z matrycy $\mathfrak{B}_3$ i na odwrót.

Łatwo także widać, że matryce $\mathfrak{B}_1 - \mathfrak{B}_5$ są parami termalnie równoważne. W przypadku matryc boole'owskich z Przykładów 2 i 16 nietrudno jest przenieść aksjomatyzację tautologii w jednym języku na drugi, tak by otrzymać aksjomatyzację w innym. Nie wiadomo jednak, czy podobnie będzie dla każdej pary matryc termalnie równoważnych. Stąd pytanie, które zadał W. Rautenberg:

Problem 19. *Czy każda matryca termalnie równoważna matrycy, która (nie) jest skończenie bazowalna, również (nie) jest skończenie bazowalna?*

Podobnie można postawić pytanie o skończoną aksjomatyzowalność matryc logicznych.

Problem 20. *Czy każda matryca termalnie równoważna matrycy, która (nie) jest skończenie aksjomatyzowalna, również (nie) jest skończenie aksjomatyzowalna?*

Do tej pory w literaturze odnotowano dwa pozytywne rezultaty. Pierwszy wiąże się ze wspomnianym wcześniej faktem, że wszystkie dwuelementowe matryce są skończenie bazowalne [7, 2], a co za tym idzie, są skończenie aksjomatyzowalne. Ponieważ dotyczy to wszystkich dwuelementowych matryc, niezależnie od użytych działań, to wnioskujemy, że własności skończonej aksjomatyzowalności i skończonej bazowalności są niezmiennicze względem termalnej równoważności dla wszystkich matryc dwuelementowych.

Wiadomo także [4], że brak istnienia skończonej bazy dla matrycy $\mathfrak{M}_{\mathrm{II}}$ przenosi się przez termalną równoważność. Prawdziwe jest twierdzenie:

Twierdzenie 21 ([4])**.** *Żadna matryca termalnie równoważna matrycy $\mathfrak{M}_{\mathrm{II}}$ nie jest skończenie bazowalna.*

Warto odnotować także nieopublikowany do tej pory fakt, że dla każdej z matryc $\mathfrak{M}_{\mathrm{I}} - \mathfrak{M}_{\mathrm{III}}$ z Przykładu 14 własność skończonej aksjomatyzowalności – lub jej brak – podobnie jak własność skończonej bazowalności – lub jej brak – przenoszą się na wszystkie matryce im termalnie równoważne.

Zbadano również inne trójelementowe matryce o podobnych tabelach działań.

Przykład 22.

$$\mathfrak{M}_i = \big\langle \{0,1,2\}, \cdot_i, \{2\} \big\rangle, \quad i = \mathrm{IV}, \ldots, \mathrm{VIII}$$

$\cdot_{\mathrm{IV}}$	0	1	2
0	1	2	2
1	1	2	2
2	1	2	2

$\cdot_{\mathrm{V}}$	0	1	2
0	1	2	2
1	1	2	2
2	2	2	2

$\cdot_{\mathrm{VI}}$	0	1	2
0	2	2	2
1	1	2	2
2	1	2	2

$\cdot_{\mathrm{VII}}$	0	1	2
0	2	2	2
1	2	2	2
2	2	2	2

$\cdot_{\mathrm{VIII}}$	0	1	2
0	1	2	2
1	2	2	2
2	1	2	2

Matryce $\mathfrak{M}_{\mathrm{IV}}$, $\mathfrak{M}_{\mathrm{VI}}$ oraz $\mathfrak{M}_{\mathrm{VII}}$ są skończenie bazowalne, a co za tym idzie, skończenie akjomatyzowalne i własność ta przenosi się na wszystkie matryce im termalnie równoważne. Matryca $\mathfrak{M}_{\mathrm{V}}$ nie jest skończenie bazowalna, ale jest skończenie aksjomatyzowalana i wszystkie matryce jej termalnie równoważne mają tę własność [5]. Z kolei $\mathfrak{M}_{\mathrm{VIII}}$ nie jest skończenie aksjomatyzowalna [3] i sprawdzono, że żadna matryca jej termalnie równoważna nie jest skończenie akjomatyzowalna (informacja ustna od K. Pałasińskiej).

Literatura

[1] S. L. Bloom, *A representation theorem for the lattice of standard consequence operation*, Studia Logica 34, 1975, pp. 235–237.

[2] B. Herrmann, W. Rautenberg, *Finite Replacement and Finite Hilbert-style Axiomatizability*, ZML 38, 1992, s. 327–344.

[3] K. Pałasińska, *Three-element nonfinitely axiomatizable matrices*, Studia Logica 53, 1994, s. 361–372.

[4] K. Pałasińska, *No Matrix Term-Equivalent to Wroński's 3-element Matrix is Finitely Based*, Studia Logica 77, 2004, s. 413–423.

[5] R. Polek, *Zagadnienie niezmienniczości własności skończonej aksjomatyzowalności matryc logicznych względem równoważności termalnej*, Praca licencjacka, Politechnika Krakowska, 2010.

[6] M. Porębska, *Własności skończonej aksjomatyzowalności dla małych matryc logicznych*, Praca licencjacka, Politechnika Krakowska, 2010.

[7] W. Rautenberg, *Two-element Matrices*, Studia Logica 40, 1981, s. 315–353.

[8] A. Urquhart, *A finite matrix whose consequence relation is not finitely axiomatizable*, Reports on Mathematical Logic 9, 1977, s. 71–73.

[9] M. Wajsberg, *Logical works – On Axiomatizability of Matrices*, Polish Academy of Sciences, Institute of Philosophy and Sociology, 1977, s. 93–106.

[10] P. Wojtylak, *Strogly Finite Logics: Finite Axiomatizability and the Problem of Supremum*, Bulletin of the Section of Logic, PAN 8, 1979, s. 99–111.

[11] P. Wojtylak, *An example of a finite though finitely non-axiomatizable matrix*, Reports on Mathematical Logic 17, 1984, s. 39–46.

[12] R. Wójcicki, *Theory of Logical Calculi*, Kluwer Publ, Dordrecht 1988.

[13] A. Wroński, *On finitely based consequence operations*, Studia Logica 35, 1976, s. 453–458.

[14] A. Wroński, *A Three-element Matrix whose Consequence Operation is not Finitely Based*, Bulletin of the Section of Logic PAN 8, 1979, s. 68–71.

Nieskończone maszyny Turinga rozwiązują problem odpowiedniości Posta

Wojciech Rosa

Streszczenie. Celem referatu jest pokazanie sposobu działania i możliwości nieskończonych maszyn Turinga (NMT). Przedstawimy definicję super-zadania oraz przykłady takich zadań. Następnie zostanie postawiony problem odpowiedniości Posta. Głównym rezultatem, który zaprezentujemy, jest twierdzenie (wraz z dowodem) o rozstrzygalności języka PCP w sensie NMT.

1. Wstęp

Każdego dnia rzesze ludzi pracują nad przyspieszeniem komputerów. Wyobraźmy sobie, że pewnego dnia w tym pościgu została osiągnięta granica – człowiek stał się posiadaczem nieskończenie szybkich maszyn. Jak moglibyśmy wykorzystać ich możliwości? Nieskończone maszyny Turinga są matematycznym modelem odpowiadającym na to pytanie. Model ten jest analogiczny do klasycznych maszyn Turinga z tym wyjątkiem, że jest on rozszerzony na pozaskończoną liczbę konfiguracji, jaką może osiągać maszyna w trakcie swojej pracy. Kroki obliczeniowe są wykonywane w czasie tak jak liczby porządkowe, więc jeśli maszyna nie zatrzyma się na żadnym z etapów: 0, 1, 2, ... to przechodzi w pierwszy etap graniczny ω, potem zaś przechodzi kolejno przez etapy $\omega + 1$, $\omega + 2, \ldots$ i jeśli znowu maszyna się nie zatrzymała to kontynuuje ona pracę w następnym etapie granicznym $\omega + \omega$, dalej $\omega + \omega + 1$, $\omega + \omega + 2$, ... itd. zgodnie z liczbami porządkowymi.

Moglibyśmy zadać sobie pytanie: czy osiągnięcie granicy jest w ogóle możliwe? Odpowiedź nie jest jednoznaczna. Rozważania, które prowadził Mycka [4], pozwalają wyciągnąć wniosek, że bardziej niż *tak*, możemy powiedzieć, że *nie jest to niemożliwe*. Xia [7] pokazał, że nieskończona liczba mechanicznych zdarzeń może mieć miejsce w skończonym odcinku czasu. Zatem wydaje się, że nie ma przeszkód, abyśmy rozważali maszyny zdolne do nieskończonych obliczeń. Do wykonania tak dużej ilości obliczeń potrzeba algorytmu, który będzie wymagał takiej ilości kroków, algorytm ten zaś jest wyznaczony przez klucz do teorii nieskończonych obliczeń – super-zadania.

Wojciech Rosa
roswoj@gmail.com
student matematyki
Politechnika Lubelska

Definicja 1. *Super-zadanie* jest to zadanie wymagające wykonania nieskończenie wielu kroków obliczeniowych.

Prawdopodobnie pierwszym zmagającym się z super-zadaniami był grecki filozof Zenon z Elei, który słynął z paradoksu o niemożności ruchu. Dowodził tego, twierdząc, że zanim ktoś przybędzie do celu, musiałby przebyć połowę drogi, ale zanim znajdzie się w połowie drogi, musiałby przebyć połowę drogi pomiędzy startem a punktem wyznaczającym połowę drogi... i tak w nieskończoność. W związku z tym, że nikt nie jest w stanie wykonać tych nieskończenie wielu zadań – cały ruch jest niemożliwy. Zenon z Elei podobnie argumentował inne paradoksy (z których także słynął) takie jak np. paradoks Achillesa i żółwia lub paradoks strzały.

Najprostszym i praktycznym przykładem super-zadania może być wypisanie wszystkich cyfr rozwinięcia binarnego (równoważnie dziesiętnego) liczby π (lub dowolnej liczby niewymiernej) albo dodanie do siebie dwóch liczb rzeczywistych zadanych poprzez ich rozwinięcia (samo wpisanie danych wejściowych jest również przykładem super-zadania).

„Chuck Norris policzył do nieskończoności – dwa razy".

Popularny żart dowodzi, że również super-bohaterowie potrafią wykonywać super-zadania. Kolejna sytuacja będąca przedmiotem żywych dyskusji pomiędzy filozofami i logikami związana jest ze zwyczajną żarówką. Załóżmy, że żarówka jest włączona przez 1/2 minuty, następnie jest wyłączona przez 1/4 minuty, następnie jest włączona na 1/8 minuty i tak dalej. Czy po jednej minucie (suma szeregu geometrycznego o pierwszym wyrazie i ilorazie równym 1/2) od momentu rozpoczęcia operacji żarówka jest włączona czy wyłączona?

Dla następnego przykładu załóżmy, że istnieje hotel, w którym jest nieskończenie wiele pokoi, a co więcej, w danym momencie każdy z nich jest zajęty. Czy hotel byłby w stanie przyjąć w swoje progi jeszcze jednego gościa i wynająć mu pokój? Oczywiście, że tak. Wystarczy gościa z pokoju nr 1 przenieść pod nr 2, gościa z nr 2 przenieść pod 3 itd. W ten sposób (po wykonaniu ω kroków) możemy otrzymać nie tylko jeden, ale nawet dowolną skończoną ilość wolnych pokoi. Jak pokaże następny przykład, jesteśmy w stanie przyjąć do tego samego hotelu nadal nieskończenie wielu gości.

Wyobraźmy sobie, że jesteśmy posiadaczami nieskończenie wielkiej fortuny, a konkretniej posiadaczami nieskończenie (ale przeliczalnie) wielu banknotów o nominale 10 złotych. Do tego wszystkiego spotykamy diabła, który proponuje nam (ze względu na sentyment do posiadanych przez nas banknotów) wymianę każdego posiadanego przez nas banknotu na dwa banknoty o tym samym nominale, ale pochodzące od diabła. Czy powinniśmy zgodzić się na taką umowę? Przyjmijmy, że wejdziemy w układ z diabłem. W związku z tym, że taka transakcja wymaga sporego sprytu, diabeł proponuje, że pierwszą wymianę wykona przez 1/2 godziny, drugą przez 1/4 godziny... itd. – cała transakcja potrwa godzinę. Po godzinie stresu i rozmyślań nad poprawnością decyzji okazuje się, że nie zostało nam nic! Jak to się stało? Ponumerujmy każdy z naszych banknotów liczbami nieparzystymi $1, 3, 5, \ldots$ Diabeł wykonywał wymiany w następujący sposób: na początku zgodnie z umową zabrał banknot nr 1, a nam dał banknoty z numerami 2 i 4; następnie zabrał od nas banknot nr 2, a zostawił nam banknoty nr 6 i 8 itd. Przyczyną tego, że zostali-

śmy z niczym, był fakt, że w każdym kroku diabeł zostawiał sobie banknot, który później już nie uczestniczył w transakcji – natomiast nasze banknoty były w ciągłym obiegu.

2. Podstawowe pojęcia

Przypomnijmy podstawowe definicje i oznaczenia niezbędne w dalszej części rozważań:

Definicja 2 ([6])**.** *Alfabet* to niepusty i skończony zbiór. Elementy alfabetu to *symbole*. *Słowo* to skończony ciąg symboli z danego alfabetu, a *podsłowo* słowa w to spójny fragment słowa w. *Język* to zbiór słów.

Przykład 3. Rozpatrzmy trójelementowy alfabet $\{a, b, c\}$. Symbolami w tym alfabecie są a, b i c. Przykładowymi słowami nad tym alfabetem mogą być $abbbca$ lub ccc. Podsłowem słowa $abbbca$ jest np słowo bbc. Zbiór $\{abbbca, ccc\}$ jest przykładowym językiem nad danym alfabetem.

Definicja 4 ([3])**.** Mówimy, że relacja R *dobrze porządkuje* zbiór X, jeśli relacja ta liniowo porządkuje X (tzn. jest zwrotna, antysymetryczna, przechodnia i spójna w X) i każdy niepusty podzbiór zbioru X zawiera element najmniejszy (ze względu na R).

Przykład 5. Relacja niewiększości $\leqslant$ wprowadza dobry porządek w zbiorze $\mathbb{N}$. Relacja ta nie wprowadza dobrego porządku w zbiorach $\mathbb{Z}, \mathbb{Q}$ i $\mathbb{R}$.

Przykład 6. Relacja inkluzji (zawierania) $\subset$ wprowadza dobry porządek w przykładowej rodzinie zbiorów $\mathcal{A} = \{A_n : n \in \mathbb{N}\}$ dla $A_0 = \{0\}$ i $A_{n+1} = A_n \cup \{n + 1\}$. Relacja ta nie wprowadza dobrego porządku w przykładowej rodzinie $\mathcal{B} = 2^{\{0,1\}} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$, gdyż nie istnieje najmniejszy element w $\{\{0\}, \{1\}\}$.

Definicja 7. *Typem* zbioru dobrze uporządkowanego nazywamy klasę dobrych porządków izomorficznych, do której ten zbiór należy.

Definicja 8 ([3])**.** *Liczbami porządkowymi* nazywamy typy zbiorów dobrze uporządkowanych.

Przykład 9. Zbiór $A = \{1\}$ jest dobrze uporządkowany w typ 1 (przez relację $\leqslant$), a zbiór $B = \{1 - \frac{1}{n} : n \in \mathbb{N}\}$ jest dobrze uporządkowany w typ ω. Zbiór $A \cup B = \{1 - \frac{1}{n} : n \in \mathbb{N}\} \cup \{1\}$ jest uporządkowany w typ $\omega + 1$.

Warto zwrócić uwagę, że definicję zbiorów dobrze uporządkowanych oraz liczb porządkowych jako pierwszy wrowadził George Cantor, na którego cześć została nazwana przestrzeń z następnej definicji. W topologii przestrzeń Cantora jest rozumiana jako przestrzeń topologiczna homeomorficzna ze zbiorem Cantora. My jednak będziemy używać tej definicji w uproszczonym znaczeniu:

Definicja 10. *Przestrzeń Cantora* to zbiór wszystkich nieskończonych ciągów binarnych. Zbiór ten będziemy oznaczać jako 2^ω.

Zdefiniujemy teraz kluczowe pojęcie dla naszej prezentacji – jednotaśmową Maszynę Turinga.

Definicja 11 ([6])**.** *Maszyna Turinga* (MT) to uporządkowana siódemka

$$(Q, \Sigma, \Gamma, \delta, q_0, q_{\text{akceptuj}}, q_{\text{odrzuć}}),$$

gdzie:

(i) Q jest zbiorem stanów,

(ii) Σ jest alfabetem wejściowym, do którego nie należy znak pusty $\square$,

(iii) Γ jest alfabetem taśmy, gdzie $\square \in \Gamma$ oraz $\Sigma \subseteq \Gamma$,

(iv) $\delta\colon Q \times \Gamma \to Q \times \Gamma \times \{L, R, S\}$ jest funkcją przejścia,

(v) $q_0 \in Q$ jest stanem początkowym,

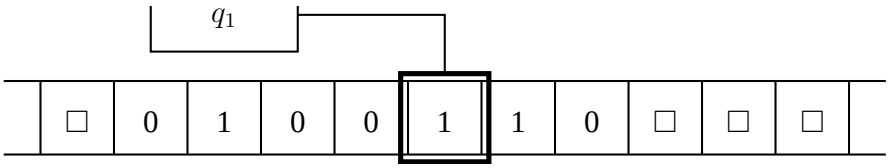
(vi) q_{akceptuj} jest stanem akceptującym,

(vii) $q_{\text{odrzuć}}$ jest stanem odrzucającym oraz $q_{\text{akceptuj}} \neq q_{\text{odrzuć}}$.

Uwaga 12. W wielu momentach będziemy mówić o wielotaśmowych MT, które są jedynie rozszerzeniem klasycznej definicji. Ich definicja jest identyczna, z wyłączeniem punktu (iv), który dla nich wygląda następująco: $\delta\colon Q \times \Gamma^k \to Q \times \Gamma^k \times \{L, R, S\}^k$ jest funkcją przejścia, zaś $k \in \mathbb{N}_+$ oznacza liczbę taśm.

Definicja 13 ([6])**.** Zestawienie stanu, zawartości taśmy (taśm) oraz pozycji głowicy (głowic) nazywamy *konfiguracją* MT. Pierwszą z osiąganych konfiguracji podczas pracy maszyny dalej będziemy nazywać *konfiguracją początkową*. Konfigurację, dla której wartością stanu jest stan q_{akceptuj} lub $q_{\text{odrzuć}}$, będziemy nazywać *konfiguracją końcową*.

Przykład 14. Rysunek 1 przedstawia pewną MT w przykładowej konfiguracji.



Rysunek 1. Maszyna Turinga w konfiguracji $0100q_1110$.

Definicja 15. *Obliczeniem maszyny Turinga* nazywamy skończony ciąg konfiguracji C_n, gdzie $n \in \mathbb{N}_+$, taki że C_1 jest konfiguracją początkową, z każdej konfiguracji C_i maszyna przechodzi do C_{i+1} (gdzie $i \in \mathbb{N}_+$ oraz $1 \leqslant i \leqslant n-1$) oraz C_n jest konfiguracją końcową. Jeżeli dla danego słowa x MT kończy obliczenie w stanie q_{akceptuj}, to mówimy, że maszyna *akceptuje* słowo x. Analogicznie zakończenie obliczenia w stanie $q_{\text{odrzuć}}$ oznacza, że maszyna *odrzuca* słowo x.

Definicja 16. Język J nazywamy *rozstrzygalnym*, jeśli istnieje dla niego maszyna Turinga M, taka że:

$$\forall_{x \in J}\ M \text{ akceptuje } x; \quad \forall_{x \notin J}\ M \text{ odrzuca } x.$$

Mówimy wtedy również, że J jest *rozstrzygany* przez M lub że M *rozstrzyga* J.

Przykład 17. Rozważmy język $A = \{(01)^n | n \in \mathbb{N}\}$, czyli język złożony ze wszystkich ciągów binarnych postaci $0101..01$. Nietrudno zauważyć, że jest to język rozstrzygalny. Jako dowód pokażemy taką maszynę Turinga M_0, która rozstrzyga język A. Nieformalny opis M_0 jest następujący:

$M_0 =$'Dla słowa wejściowego w:

(1) Jeżeli głowica znajduje się nad jedynką, to *odrzuć*, a jeśli nad symbolem pustym, to *akceptuj*. Jeśli głowica odczytuje zero, to przesuń głowicę w prawo i przejdź do kroku **(2)**.

(2) Jeżeli głowica znajduje się nad zerem lub nad symbolem pustym, to *odrzuć*. Jeśli głowica odczytuje jedynkę, to przesuń głowicę w prawo i przejdź do kroku **(1)**'.

Podajmy teraz formalny opis $M_0 = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{akceptuj}}, q_{\text{odrzuć}})$:

(i) $Q = \{q_0, q_1, q_{\text{akceptuj}}, q_{\text{odrzuć}}\}$,

(ii) $\Sigma = \{0, 1\}$,

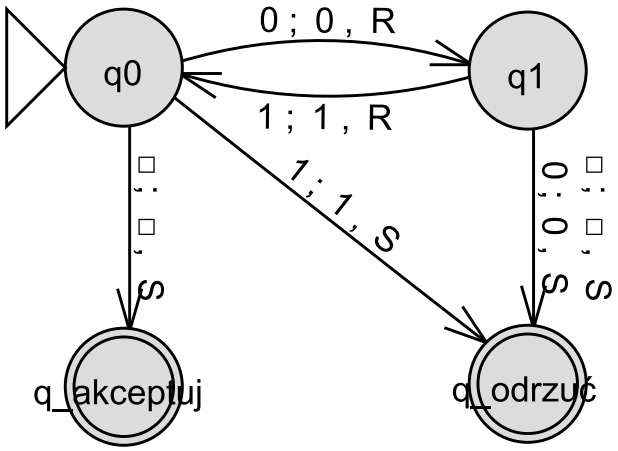
(iii) $\Gamma = \{0, 1, \square\}$,

(iv) Funkcja przejścia δ jest przedstawiona za pomocą diagramu przejścia na rysunku 2.

(v) Stanami: początkowym, akceptującym i odrzucającym są odpowiednio: q_0, q_{akceptuj} i $q_{\text{odrzuć}}$.

3. Jak działają NMT?

Definicja NMT jest identyczna do klasycznej MT z wyłączeniem definicji obliczenia takiej maszyny. Dla wygody będziemy używać modelu maszyny z trzema taśmami: jedną z danymi wejściowymi, zwaną dalej taśmą wejścia, drugą do bieżących obliczeń, zwaną dalej taśmą roboczą, i trzecią zawierającą ostateczny efekt pracy maszyny, którą będziemy nazywać taśmą wyjścia. Kroki obliczeniowe przebiegają w klasyczny sposób: głowica czyta symbole w danym miejscu na taśmach i w zależności od stanu, w którym się znajduje, pisze w ich miejscu nowe, porusza głowicą w lewo, prawo lub stoi w miejscu i przechodzi w nowy stan wyznaczony przez funkcję przejścia.



Rysunek 2. Funkcja przejścia M_0.

Definicja 18. *Obliczeniem nieskończonej maszyny Turinga* nazywamy ciąg konfiguracji C_n, gdzie n jest liczbą porządkową, taki że C_1 jest konfiguracją początkową, z każdej konfiguracji C_i maszyna przechodzi do C_{i+1} (gdzie i jest liczbą porządkową oraz $1 \leqslant i \ \leqslant n-1$) oraz C_n jest konfiguracją końcową. Jeżeli dla danego słowa x NMT kończy obliczenie w stanie q_{akceptuj}, to mówimy, że maszyna *akceptuje* słowo x. Analogicznie zakończenie obliczenia w stanie $q_{\text{odrzuć}}$ oznacza, że maszyna *odrzuca* słowo x.

Definicja 19. Język J nazywamy *rozstrzygalnym w sensie NMT*, jeśli istnieje dla niego nieskończona maszyna Turinga M, taka że:

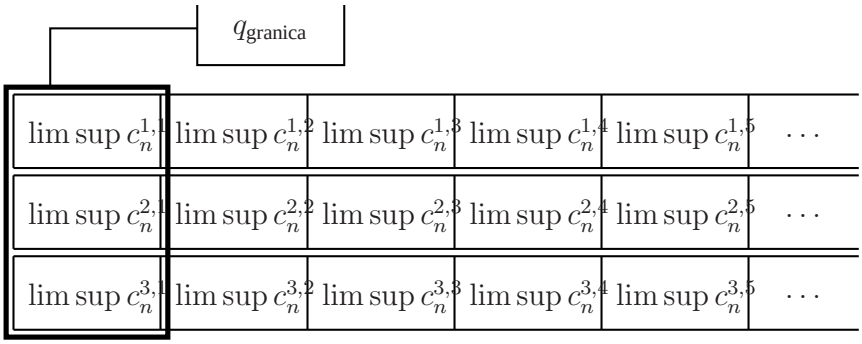
$$\forall_{x \in J}\ M \text{ akceptuje } x; \quad \forall_{x \notin J}\ M \text{ odrzuca } x.$$

Mówimy wtedy również, że J jest *rozstrzygany w sensie NMT* przez M lub że M *rozstrzyga w sensie NMT* język J.

Z podanych definicji widać, że jedyną różnicą jest to, że podczas obliczenia maszyna jest wzbogacona o możliwość wykonania pozaskończonej liczby konfiguracji. Ponadto definiujemy zachowanie maszyny w stanach granicznych ω, $\omega + \omega$, $\omega + \omega + \omega$ itd. Dla klasycznych i współcześnie pracujących maszyn jest to rodzaj błędu (maszyna zapętla się) – wynik jest odrzucany, nawet jeśli maszyna wypisuje na taśmach cenne dla nas informacje. NMT zachowują te dane poprzez obliczenie pewnego rodzaju granicy poprzednich konfiguracji.

W szczególności, jeśli maszyna wchodzi w etap graniczny, głowica przesuwa się w lewo na początek taśm, a maszyna przechodzi w stan q_{granica} – jeden ze skończenie wielu zdefiniowanych stanów. Dla konkretnej maszyny będziemy przyjmowali umowę, że maszyna wchodzi w stan q_{granica} wtedy i tylko wtedy, gdy wykona dokładnie „granica” kroków obliczeniowych. Dokładnie w momencie wejścia w graniczny etap każda z komórek taśmy zawiera symbol, który jest (zgodnie z ustalonym porządkiem w zbiorze symboli) górną granicą ciągu poprzednich wartości komórki.

Przykładowo, jeżeli od pewnego momentu obliczeń wartość komórki nie zmienia się, to w stanie q_{granica} na taśmie w tej komórce pojawi się właśnie ta niezmienna wartość. Natomiast w przypadku gdy wartość komórki oscyluje pomiędzy 0 i 1 – w komórce tej otrzymamy 1. W tej konfiguracji (głowica na początku taśm, stan q_{granica} i obliczone górne granice w komórkach) maszyna kontynuuje pracę (rysunek 3).



Rysunek 3. NMT na etapie granicznym.

Maszyna ma dużo czasu na przeanalizowanie danych wejściowych, wykonanie obliczeń i wypisanie wyniku – zatem danymi wejściowymi mogą być nieskończone ciągi binarne. W związku z tym NMT są modelem maszyn operujących na liczbach rzeczywistych (czyli działają w przestrzeni Cantora).

Przykład 20. Pouczającym przykładem zastosowań NMT jest wypisywanie rozwinięć dziesiętnych liczb przestępnych.

Definicja 21. *Liczbą przestępną* nazywamy liczbę rzeczywistą niebędącą pierwiastkiem żadnego niezerowego wielomianu o współczynnikach całkowitych.

Przykładem takich liczb są liczby π, e, liczby Liouville'a – a w szczególności stała Liouville'a.

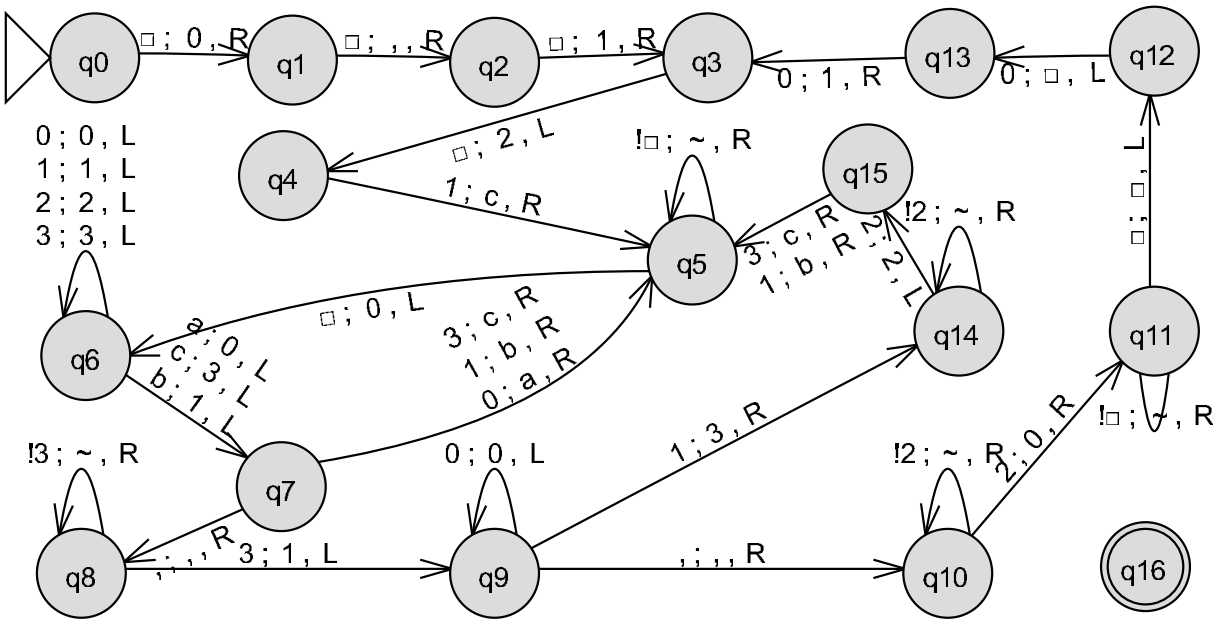
Definicja 22. *Stałą Liouville'a* nazywamy taką liczbę L, że:

$$L = \sum_{j=1}^{\infty} 10^{-j!}.$$

Ogólny zarys pracy maszyny M_1 wypisującej na taśmę stałą L przedstawia się następująco: w pierwszym kroku maszyna wypisuje ciąg trzech znaków: $0\ ,\ 1$. Umówmy się, że po wypisaniu n–tej jedynki maszyna wchodzi w $n+1$-szy etap. Po pierwszym kroku zatem maszyna wchodzi w drugi etap. W $n+1$-szym etapie maszyna ma $n!$ niepustych znaków wypisanych po przecinku. Tyle samo zer ($n!$) maszyna dopisuje na końcu i wykonuje ten krok n razy (czyli tyle razy, ile jest jedynek wypisanych na taśmie). Maszyna dopisała za ostatnią jedynką $n \cdot n!$ zer, czyli ostatnie 0

stoi na $n! + n \cdot n! = (n+1)!$-szym miejscu, zatem maszyna zamienia to zero na jedynkę, kończąc tym samym etap $n+1$-szy.

Szczegółowy przebieg pracy przedstawia diagram przejścia tej NMT (rysunek 4).



Rysunek 4. Funkcja przejścia M_1.

4. Problem odpowiedniości Posta

Niech $\varphi(n, x)$ oznacza wyrażenie, które dla danego n oraz x jest akceptowane bądź odrzucane przez pewną klasyczną MT. Jedną z podstawowych możliwości NMT jest rozstrzyganie prawdziwości zdania:

$$\exists_{n \in \mathbb{N}} \, \varphi(n, x). \tag{1}$$

Własność ta odróżnia NMT od zwykłych MT, które są w stanie jedynie stwierdzić, że zdanie jest prawdziwe – w przypadku, gdy tak rzeczywiście jest. Jeśli natomiast zdanie (1) jest fałszywe – MT przetwarzająca problem pracuje nieskończenie długo – wciąż nie dając nam odpowiedzi... Taki właśnie jest problem, który postawił matematyk i logik polskiego pochodzenia – Emil Leon Post [5].

Definicja 23. *Problemem odpowiedniości Posta* lub krócej: *PCP* (ang. *Post correspondence problem*) nazywamy pytanie: Czy dla danego ciągu par słów $(\alpha_i, \beta_i)_{1 \leqslant i \leqslant k \in \mathbb{N}}$ nad pewnym alfabetem złożonym przynajmniej z dwóch symboli istnieje skończony ciąg indeksów (w_m), taki że $\alpha_{w_1}\alpha_{w_2} \ldots \alpha_{w_m} = \beta_{w_1}\beta_{w_2} \ldots \beta_{w_m}$?

Uwaga 24. W dalszych rozważaniach bez zmniejszenia ogólności rozumowania przyjmujemy, że alfabetem domyślnym jest zbiór $\{a, b\}$.

Przykładowo, dla ciągu par słów $((a, ab), (abb, b), (bba, baa))$ pozytywną odpowiedź realizuje ciąg $(1, 3, 1, 2)$. Istotnie:

$$\alpha_1\alpha_3\alpha_1\alpha_2 = a + bba + a + abb = abbaaabb = ab + baa + ab + b = \beta_1\beta_3\beta_1\beta_2.$$

Równie szybko jesteśmy w stanie dać negatywną odpowiedź PCP dla ciągu par słów $((a, ab), (ab, bab), (a, bbb), (bb, baa))$, – gdyż w każdej parze (α_i, β_i) słowo β_i jest dłuższe od słowa (α_i); albo dla ciągu $((b, aa), (a, bab), (ba, ab), (bbabba, ababa))$ – gdyż nie istnieje para słów (α_i, β_i), w której obydwa słowa zaczynałyby się od tego samego symbolu. Oczywistym jest fakt, że jeśli dany ciąg spełnia warunek zadany w PCP, to prędzej czy później znajdziemy ciąg, który pozwoli nam udzielić pozytywnej odpowiedzi. A jeśli tak nie będzie? Możemy jedynie mieć nadzieję, że uda się zauważyć coś, co pozwoli odrzucić ten ciąg. Co więcej, wyniki teorii algorytmów skutecznie zniechęcają do podejmowania dalszych poszukiwań:

Twierdzenie 25 ([6])**.** *Język PCP jest nierozstrzygalny.*

To znaczy, że nie istnieje MT (lub równoważnie algorytm podejmujący skończenie wiele kroków), która w ogólnym przypadku dawałaby odpowiedź na PCP. Prostym wnioskiem z tego twierdzenia jest fakt, że PCP jest super-zadaniem. Ponadto, dla danego ciągu par słów (α_i, β_i) odpowiedź na PCP jest równoważna zdaniu: istnieje takie $n \in \mathbb{N}$, że: istnieje n-wyrazowy ciąg indeksów (w_n), taki że $\alpha_{w_1}\alpha_{w_2} \ldots \alpha_{w_n} = \beta_{w_1}\beta_{w_2} \ldots \beta_{w_n}$. Nietrudno zauważyć, że jest to zdanie postaci (1), a więc istnieje NMT, która by dawała odpowiedź na PCP.

5. NMT rozstrzygająca język PCP

Alfabetem wejściowym dla naszej maszyny (zwanej dalej M_2) jest zbiór $\{0, 1, 2, 3\}$, zaś alfabet taśmy rozszerzony jest o symbol znaku pustego – $\square$. Zbiór stanów Q liczy ponad 50 elementów, w związku z tym nie będziemy ich wymieniać. Stanami: początkowym, akceptującym i odrzucającym są odpowiednio: start, TAK oraz NIE.

Uwaga 26. NMT działają na ciągach binarnych, my zaś dla klarowności modelu M_2 będziemy używać alfabetu złożonego w sumie z pięciu symboli. Maszynę operującą na ciągach binarnych możemy otrzymać, kodując każdy z symboli w bloku 3-bitowym i programując maszynę w taki sposób, aby analizowała bloki, a nie symbole. Ogólny tok pracy maszyny pozostaje bez zmian.

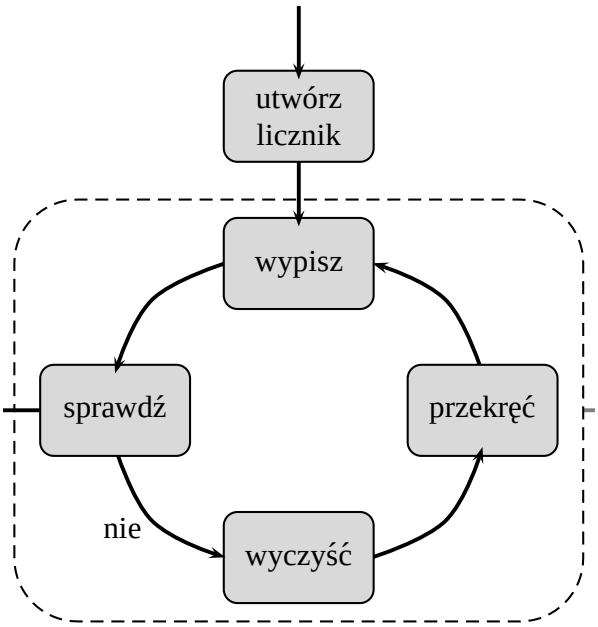
Ponadto M_2 wchodzi w stan NIE wtedy i tylko wtedy, gdy wykona ω kroków obliczeniowych. Warto zaznaczyć, że istnieje techniczna możliwość zagwarantowania wykonania dokładnie ω kroków – poprzez wprowadzenie dodatkowego licznika, który będzie kontrolował specjalne dwa bity umieszczone na którejś z taśm. Maszyna jest wtedy zaprogramowana w taki sposób, że tworzy na początku dwa bity o różnych wartościach (np. 0 i 1), a po każdym zakończonym etapie pracy

zmienia wartość każdego z bitów na przeciwną (czyli na 1 i 0). Kontrola wykonywana przez licznik polega na sprawdzeniu, czy dane bity są równe – nastąpi to dopiero, gdy maszyna wykona ω kroków obliczeniowych.

Aby wprowadzić ciąg par słów do maszyny, używamy następującej konwencji: 0 i 1 odpowiadają symbolom alfabetu, 2 jest symbolem oddzielającym słowa w parze, natomiast 3 symbolem oddzielającym pary. Dalej będziemy się posługiwać przykładowym ciągiem par słów: $((a, b), (b, ab), (ba, b))$. Dla tego przykładu instrukcja wejściowa dla maszyny wygląda następująco:

dane	a	,	b	;	b	,	a	b	;	b	a	,	b
taśma wejścia	0	2	1	3	1	2	0	1	3	1	0	2	1

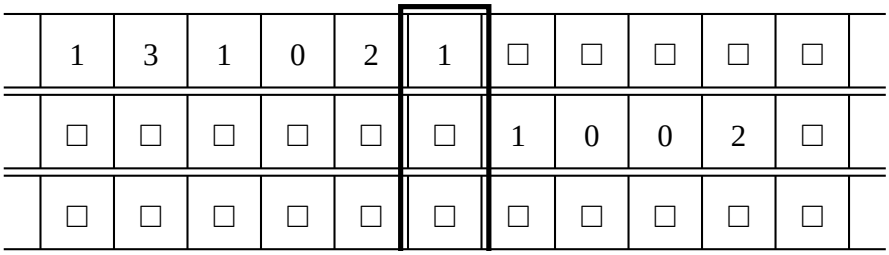
Ogólny szkic pracy M_2 jest prosty: maszyna na n-tym etapie generuje kolejno każdą n-elementową permutację z powtórzeniami z zadanych elementów, jednocześnie sprawdzając, czy dla danej permutacji spełniony jest warunek podany w PCP. Jeżeli okazałoby się, że dla którejś z permutacji jest to prawda – maszyna kończy pracę, wypisując ciąg indeksów realizujący odpowiedź na PCP na taśmę wyjścia. W innym przypadku maszyna przechodzi do etapu $n + 1$ (rysunek 5).



Rysunek 5. Schemat pracy M_2.

Na początku maszyna wykrywa, jak wiele par zostało jej przekazanych – oznaczmy tę liczbę naturalną jako p. *Licznikiem w pozycji* k będziemy dalej nazywali ciąg złożony z $p-1$ zer i jedynki,

taki że jedynka stoi na k-tym miejscu (czyli jest poprzedzona przez dokładnie $k-1$ zer). Wykrycie ilości par polega na wpisaniu za danymi wejściowymi, ale już na taśmie roboczej licznika w pozycji 1. Za każdym licznikiem (tuż po jego utworzeniu) maszyna wpisuje symbol 2 – jako znak oddzielający liczniki (rysunek 6).



Rysunek 6. Utworzenie pierwszego licznika.

Idea liczników pozwala na generowanie kolejnych permutacji z powtórzeniami oraz na ich analizę: liczba liczników na taśmie oznacza etap, w którym znaduje się maszyna (liczbę elementów permutacji właśnie sprawdzanej), natomiast każdy licznik w zależności od pozycji wskazuje na któryś z zadanych elementów. Generowanie kolejnych permutacji przebiega w następujący sposób: maszyna *przekręca* pierwszy z prawej licznik na taśmie, tzn. że jeżeli licznik ten jest w pozycji innej niż p, to zwiększa jego pozycję o jeden, a jeśli licznik jest w pozycji p, to maszyna ustawia go w pozycji 1 i *przekręca* pierwszy licznik na lewo od danego. Jeśliby taki licznik nie istniał, to znaczy, że pierwszy (licząc od lewej) licznik był w pozycji p i maszyna próbuje go przekręcić. Onacza to, że wszystkie permutacje na danym etapie zostały sprawdzone, czyli maszyna ustawia pierwszy licznik w pozycji 1, przesuwa się za wszystkie dotychczasowe liczniki i tworzy tam nowy licznik w pozycji 1. Tablica 1 przedstawia przykłady wykonania procedury *przekręć* na taśmie roboczej dla różnych zestawów liczników.

liczniki	*przekręć*
1002	0102
10020012	01021002
00120012	100210021002

Tablica 1. Wykonanie procedury przekręć.

Po każdym zakończeniu *przekręć* maszyna dokonuje *sprawdzenia* danej permutacji. Procedurę tę wywołujemy początkowo, gdy głowica jest ustawiona na pierwszym liczniku (tzn. na pierwszym licząc od lewej). *Sprawdzenie* przebiega w ten sposób, że maszyna wykrywa, w jakiej pozycji jest dany licznik, a następnie wpisuje na końcu taśmy roboczej (tzn. zaczynając od miejsca, które jest poprzedzone przez ostatni niepusty symbol na danej taśmie) pierwsze słowo z pary wskazanej przez licznik. Po tym maszyna dopisuje na taśmie wyniku drugie słowo z danej pary, przy czym

robi to, zaczynając od końca – czyli od pierwszej pustej komórki po niepustych symbolach, a jeżeli owa nie istnieje, to zaczynając od komórki będącej w tej samej kolumnie co początek słowa utworzonego w taśmie roboczej (rysunek 7).

	1	□	□	□	□	□	□	□	□	□	□	
	□	0	0	1	2	1	0	□	□	□	□	
	□	□	□	□	□	1	□	□	□	□	□	

Rysunek 7. *Sprawdzenie.*

Jeżeli podczas wykonywania tych kroków komórki znajdujące się w tej samej kolumnie na taśmie roboczej i taśmie wyniku zawierają różne symbole – maszyna odnotowuje błąd, usuwa tymczasowe symbole i *przekręca* ostatni licznik. W innym przypadku zostaje uruchomiona procedura *sprawdzenie* dla pierwszego licznika na prawo od danego – jeśli taki licznik nie istnieje, procedura jest zakończona.

W tym miejscu maszynie pozostało do sprawdzenia, czy uzyskane słowo na jednej z taśm nie jest „podsłowem" słowa z drugiej taśmy. Jeżeli tak, dotychczasowy wynik pracy *sprawdzenie* zostaje skasowany, a maszyna *przekręca* ostatni licznik. Jeżeli nie, tzn. że maszyna odnalazła ciąg realizujący odpowiedź na PCP – następuje przepisanie liczników na taśmę wyjściową i przejście w stan końcowy TAK (rysunek 8).

	□	□	□	□	□	□	□	□	□	□	□	
	0	0	1	2	0	1	0	2	1	0	1	
	□	□	□	□	□	□	0	2	1	0	1	

Rysunek 8. Maszyna kończy pracę – przepisywanie liczników.

Jeżeli maszyna znajduje się w stanie ω, to znaczy, że wykonała ω kroków obliczeniowych. Oznacza to, że przeszła przez wszystkie etapy bez znalezienia poszukiwanej permutacji, zatem maszyna przechodzi w stan końcowy NIE.

Funkcję przejścia maszyny przedstawia diagram przejścia zamieszczony na rysunku 9. Oczywistym wnioskiem z powyższych rozważań jest następujące twierdzenie:

Twierdzenie 27. *Język PCP jest rozstrzygalny w sensie NMT.*

Dowód. Jako dowód podamy nieformalny zapis maszyny M_2 rozstrzygającej język PCP:
$M_2 =$‘Dla słowa wejściowego w:

(1) Dopisz na taśmie roboczej licznik w pozycji 1. Jeżeli taśma ta jest pusta, to rozpocznij dopisywanie od komórki położonej pod pierwszą komórką za danymi wejściowymi. Przesuń głowicę nad pierwszy (licząc od lewej) licznik. Przejdź do kroku **(2)**.

(2) Wykryj pozycję licznika (nazwijmy tę liczbę k) i dopisz pierwsze słowo z k-tej pary na taśmie roboczej; jeśli komórka na taśmie wyjścia umieszczona pod właśnie wpisywaną jest niepusta i zawiera inny symbol niż wpisywany, to przejdź do kroku **(4)**. Dopisz na taśmie wyjścia (jeśli taśma jest pusta, rozpocznij dopisywanie od pierwszej komórki za licznikami) drugie słowo z k-tej pary, jeśli komórka na taśmie roboczej umieszczona nad właśnie wpisywaną jest niepusta i zawiera inny symbol niż wpisywany, to przejdź do kroku **(4)**. Przesuń głowicę na prawo od danego (na początku kroku) licznika i powtórz krok. Jeżeli taki licznik nie istnieje, to przesuń głowicę na pierwszą komórkę za licznikami i przejdź do kroku **(3)**.

(3) Przesuwaj głowicę w prawo wtedy i tylko wtedy, gdy na taśmie roboczej i taśmie wyjścia znajdują się takie same niepuste symbole. W przypadku gdy na jednej z taśm napotkasz □ i jednocześnie na drugiej z taśm niepusty symbol – przejdź do kroku **(4)**. Gdy napotkasz na dwa symbole znaku pustego □ jednocześnie, przejdź do kroku **(6)**.

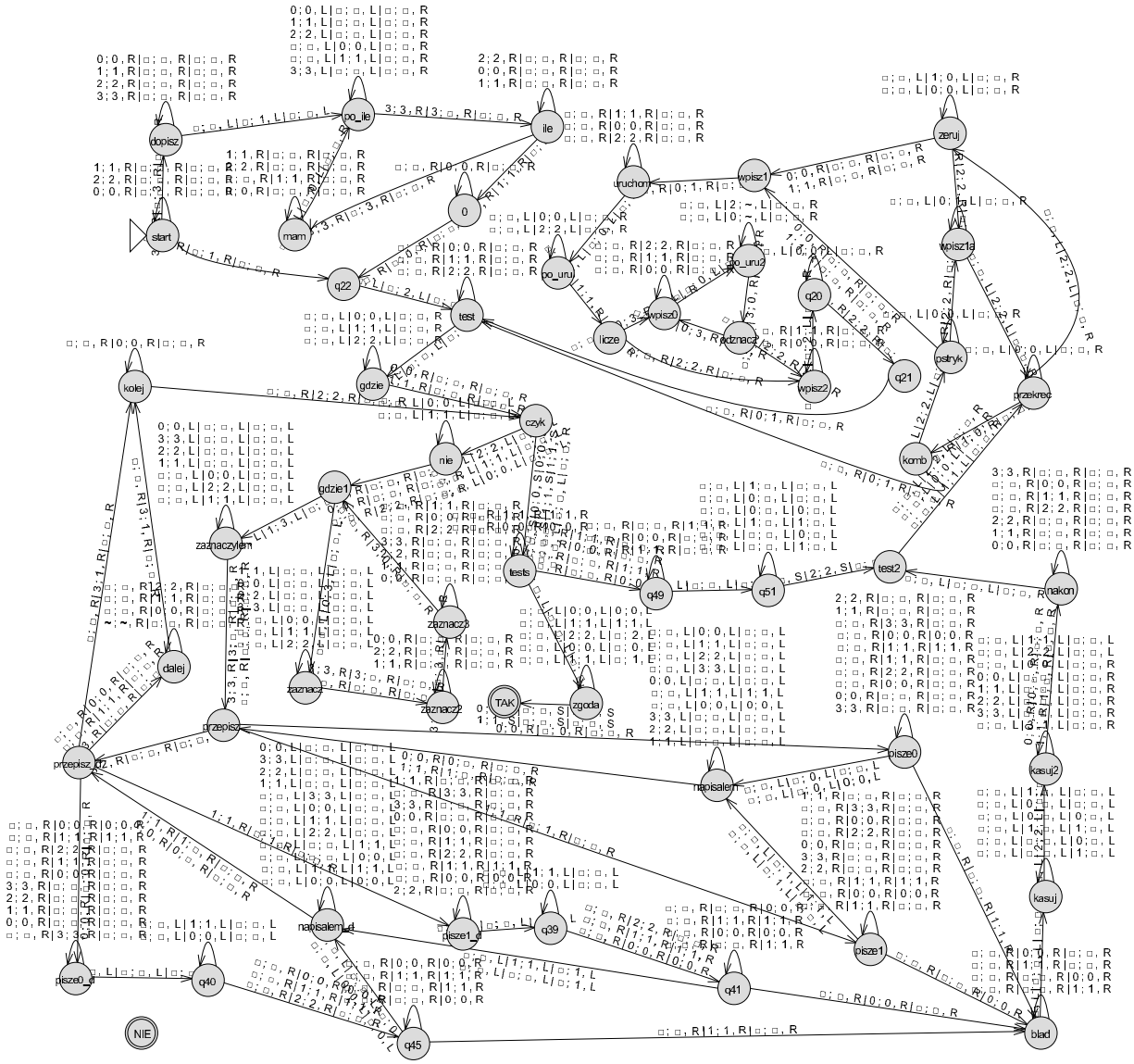
(4) Usuń dotychczasowe sprawdzane słowa z taśmy wyjścia i z taśmy roboczej. Ustaw głowicę nad ostatnim (licząc od lewej) liczniku i przejdź do kroku **(5)**.

(5) Zwiększ pozycję licznika o 1. Jeśli to niemożliwe, ustaw licznik w pozycji 1, przesuń głowicę nad licznik na lewo od danego i powtórz ten krok. Jeśli to niemożliwe, to ustaw licznik w pozycji 1 i przejdź do kroku **(1)**. Przejdź do kroku **(2)**.

(6) Przepisz liczniki z taśmy roboczej na taśmę wyjścia i *zaakceptuj*.

(7) Przejdź do tego kroku po wykonaniu ω kroków. *Odrzuć*’.

□



Rysunek 9. Funkcja przejścia M_2.

6. Podsumowanie

NMT rzucają wiele nowego światła na teorię nieskończonych obliczeń oraz na zadania, z którymi nie radzą sobie dzisiejsze komputeryi, tzw. super-zadania. Jakie inne praktyczne zastosowania mają NMT? Istnieje wiele problemów, które wymagają tych maszyn do ich rozwiązania. Przedmiotami moich obecnych badań są: porównanie NMT z rzeczywistymi funkcjami rekurencyjnymi oraz poszukiwanie odpowiedzi na pytanie: czy NMT potrafią rozwiązywać problem Cauchy'ego?

Podziękowania

Chciałbym podziękować dr. Jerzemu Mycce za inspirację, cenne uwagi merytoryczne i edytorskie oraz za poświęcony czas. Dziękuję również dr. Pawłowi Wlaziowi za pomoc w rozpoczęciu pracy.

Literatura

[1] J. D. Hamkins, *Infinite time Turing machines*, Minds and Machines, 12(4):521–539, 2002.

[2] J. D. Hamkins, D. Seabold, *Infinite time Turing machines with only one tape*, Mathematical Logic Quarterly, 47(2):271–287, 2001.

[3] K. Kuratowski, A. Mostowski *Teoria mnogości*, Monografie Matematyczne t. XXVII, Warszawa-Wrocław 1952.

[4] J. Mycka, Analog computation beyond the Turing limit, *Applied Mathematics and Computation 178*, s. 103–117, 2006.

[5] E. L. Post, A variant of a recursively unsolvable problem, *Bulletin of the AMS*, 1946.

[6] M. Sipser, *Wprowadzenie do teorii obliczeń*, Wydawnictwa Naukowo-Techniczne, Warszawa 2009.

[7] Z. Xia, The existence of noncollision singularities in newtonian systems, *Annals of Mathematics 135*, s. 411–468, 1992.

Automatyczne dowodzenie twierdzeń geometrycznych

Maciej Skórski

Streszczenie. Twierdzenia elementarnej geometrii są nie tylko ważnym testem dla technik automatycznego dowodzenia, ale i same stają się celem ataku. Znanych jest wiele metod pozwalających dowodzić i wyprowadzać twierdzenia w elementarnej geometrii bez wkładu (ludzkiej) inteligencji.

W referacie naszkicowana zostanie metoda algebraiczna, opierająca się o obliczenia w układzie współrzędnych, bliska warsztatowi geometrii analitycznej poznanemu w szkole. Omówione zostaną jej ograniczenia oraz możliwości ich przezwyciężenia dzięki zastosowaniu eliminacji kwantyfikatorowej.

1. Wprowadzenie

Badania w zakresie automatycznego dowodzenia twierdzeń geometrycznych (AGTP od ang. *Automated Geometry Theorem Proving*) trwają od ponad 50 lat. Podejścia stosowane w systemach AGTP można podzielić dwie kategorie: metody dedukcyjne oraz algebraiczne. Ogólnie rzecz ujmując, pierwsza grupa, związana blisko z AI, pozwala generować przejrzyste dowody, ustępuje jednak pod względem efektywności metodom algebraicznym.

Pierwszym praktycznym sukcesem na tym polu były prace Gelerntera z końca lat 50. Przełomowa okazała się jednak implementacja metod algebraicznych, za pomocą których przeprowadzono automatyczne dowody setek twierdzeń z geometrii elementarnej. Najwcześniejszą i zarazem najbardziej efektywną wśród metod algebraicznych jest technika oparta na obliczeniach w układzie współrzędnych, wprowadzona po raz pierwszy w pracach Wu (około 1977 r.). Od tamtego czasu metody algebraiczne rozwinięto, badając inne narzędzia do przeprowadzania obliczeń (triangulacja Wu, bazy Gröbnera, metoda zbiorów charakterystycznych, użycie liczb zespolonych), jak też zupełnie odmienne techniki, niezwiązane z układem współrzędnych, np. korzystające z niezmienników geometrycznych (metoda pól oraz metoda kątów) i umożliwiające generowanie bardziej czytelnych dowodów.

Maciej Skórski
maciej.skorski@gmail.com
student matematyki
Uniwersytet Warszawski

W referacie przedstawiona zostanie metoda obliczeń w układzie współrzędnych. Następnie pokażemy, jak przezwyciężyć ograniczenia, wynikające z różnic pomiędzy zespoloną a rzeczywistą geometrią algebraiczną, poprzez zastosowanie eliminacji kwantyfikatorów. Ponadto omówione zostanie zastosowanie nie tylko do dowodzenia, ale i do odkrywania twierdzeń. Jako że intencją autora referatu jest przybliżenie praktycznych aspektów omawianego zagadnienia, treść ilustrowana będzie przykładami twierdzeń z geometrii elementarnej, wraz z kodem umożliwiającym przeprowadzenie obliczeń w wolnodostępnych pakietach [1, 2].

2. Metoda algebraiczna

Zaczniemy od przedstawienia algorytmu na dość wysokim poziomie ogólności. Przebiega on według następującego schematu:

(i) Dobierz odpowiedni (upraszczający obliczenia) układ współrzędnych.

(ii) Wprowadź zmienne: niezależne $\mathbf{u} \in \mathbb{R}^p$ (dane dowolnie) oraz zależne $\mathbf{x} \in \mathbb{R}^q$ (zadane przez warunki).

(iii) Opisz założenia i tezę przez równania wielomianowe zmiennych $\mathbf{u}$ oraz $\mathbf{x}$.

(iv) Pokaż, że równania tezy są konsekwencją równań opisujących założenia, przez odpowiednie operacje na zapisanych równaniach.

Dobór właściwego układu współrzędnych oznacza w praktyce skorzystanie z dowolności położenia pewnych punktów i możliwości przypisania im, bez straty ogólności, ustalonego położenia. Dla przykładu, mając dany środek okręgu, możemy założyć, że jest nim punkt $\mathbf{0}$, redukując w ten sposób dwie zmienne. Rozróżnienie pomiędzy dwoma rodzajami zmiennych, jak dalej będzie pokazane, jest pomocne przy wykluczaniu z konfiguracji przypadków zdegenerowanych. Takie rozróżnienie pojawia się często w sposób naturalny, jeśli explicite wymienione są punkty zadane dowolnie, oraz punkty otrzymane wtórnie, przez konstrukcje geometryczne.

W naturalny sposób pojawia się pytanie, jakie geometryczne związki możemy wyrazić przez równania wielomianowe:

Lemat 1. *Niech A, B, C, D, E, F będą punktami płaszczyzny. Każda z następujących własności geometrycznych może być wyrażona za pomocą równań wielomianowych:*

(i) *AB jest równoległy do CD,*

(ii) *AB jest prostopadły do CD,*

(iii) *Długości AB i CD są równe, tj. $|AB| = |CD|$,*

(iv) *C leży na okręgu o środku A i promieniu $|AB|$,*

(v) *C jest środkiem AB,*

(vi) *zachodzi równość ostrych kątów $\angle ABC = \angle DEF$,*

(vii) *BD jest dwusieczną kąta ABC.*

Dowód, jako bardzo prosty, pomijamy. Ograniczymy się dalej do problemów wyrażających się przez formuły w postaci uniwersalnej klauzuli Horna:

$$\forall_{(\mathbf{u},\mathbf{x})\in\mathbb{R}^{p+q}} \quad \bigwedge_{i=1,\ldots,n} [h_i(\mathbf{u},\mathbf{x}) = 0] \Rightarrow c(\mathbf{u},\mathbf{x}) = 0, \tag{1}$$

gdzie $h_i \in \mathbb{R}[\mathbf{u},\mathbf{x}]$ to wielomiany opisujące założenia (geometryczną konfigurację), a $c \in \mathbb{R}[\mathbf{u},\mathbf{x}]$ to wielomian opisujący tezę (do tego przypadku sprowadza się również koniunkcja równań w tezie). Zauważmy, że taki warunek na postać formuły jest spełniony przez szeroką klasę problemów geometrycznych, w tym przez wszystkie twierdzenia mające postać sformułowania „domknięciowego", tj. stwierdzenia, że dla określonej konfiguracji, pewne z punktów leżą na jednej prostej, okręgu, pokrywają się, etc. Jako przykład podać można twierdzenie Cevy, Pappusa, okręgu 9 punktów itd.

Formuła powyżej zakłada użycie tylko równości wielomianowych. W praktyce pojawiają się często negacje równań wielomianowych, będące konsekwencją geometrycznych warunków niedegenerujących, tzn. wykluczania pewnych konfiguracji. Dla przykładu, dodatkowym warunkiem może być żądanie, żeby dwie proste nie były równoległe bądź by pewne dwa punkty były różne. Co więcej, takie przypadki nie są rozważane bez powodu, na ogół bowiem twierdzenia geometryczne bywają nieprawdziwe w przypadkach zdegenerowanych. Formuła taka, przy pojedynczym warunku niedegeneracji $d(\mathbf{u}) \neq 0$ bądź ich koniunkcji $d = d_1 \cdots d_s \neq 0$, ma następującą postać:

$$\forall_{(\mathbf{u},\mathbf{x})\in\mathbb{R}^{p+q}} \quad \bigwedge_{i=1,\ldots,n} [h_i(\mathbf{u},\mathbf{x}) = 0] \wedge [d(\mathbf{u}) \neq 0] \Rightarrow c(\mathbf{u},\mathbf{x}) = 0. \tag{2}$$

Zauważmy, że ponieważ warunek $d \neq 0$ jest równoważny $\exists_z\, d \cdot z = 1$, powyższą formułę możemy sprowadzić do podobnej postaci jak poprzednia:

$$\forall_{(\mathbf{u},\mathbf{x},z)\in\mathbb{R}^{p+q+1}} \quad \bigwedge_{i=1,\ldots,n} [h_i(\mathbf{u},\mathbf{x}) = 0] \wedge [d(\mathbf{u}) \cdot z - 1 = 0] \Rightarrow c(\mathbf{u},\mathbf{x}) = 0. \tag{3}$$

Ze względu na istotną rolę, jaką odgrywają zdegenerowane konfiguracje, wprowadzamy rozróżnienie pomiędzy obydwoma przypadkami.

Definicja 2. Jeżeli prawdziwa jest formuła (1), wtedy twierdzenie geometryczne jest zawsze (uniwersalnie) prawdziwe. Mówimy też, że teza $c = 0$ wynika *ściśle* z założeń $h_1 = 0 \wedge \ldots \wedge h_n = 0$. Jeżeli zachodzi (2), wtedy twierdzenie geometryczne zachodzi *generycznie*, poza przypadkami zdegenerowanymi $d(\mathbf{u}) = 0$. Mówimy też, że c generycznie wynika z $h_1 = 0 \wedge \ldots \wedge h_n = 0$.

Zauważmy, że odpowiedź na pytanie o generyczne bądź uniwersalne zachodzenie geometrycznego stwierdzenia jest podobna, z uwagi na podobną postać (uniwersalna klauzula Horna). Następujący prosty fakt podaje częściowe rozwiązanie tego problemu.

Propozycja 3. *Jeżeli* $c \in \sqrt{\mathbf{I}(h_1, \ldots, h_n)}$*, w pierścieniu* $\mathbb{R}[\mathbf{u}, \mathbf{x}]$*, to* c *wynika ściśle z założeń* h_i*. Jeżeli* $c \in \sqrt{\mathbf{I}_{\mathbb{R}(\mathbf{u})}(h_1, \ldots, h_n)}$*, w pierścieniu* $\mathbb{R}(\mathbf{u})[\mathbf{x}]$*, to* c *wynika generycznie z* h_i*, przy pewnym warunku niedegeneracji zależnym tylko od* $\mathbf{u}$*.*

Dowód. Wystarczy pokazać tylko drugą część. Załóżmy, że $c^s = \sum_i A_i h_i$, gdzie A_i są wielomianami nad ciałem $\mathbb{R}(\mathbf{u})$. Wielomiany A_i są więc w istocie ilorazami wielomianów o licznikach z $\mathbb{R}[\mathbf{x}]$ i mianownikach $\mathbb{R}[\mathbf{u}]$. Zatem mnożąc przez wspólny mianownik $d \in \mathbb{R}[\mathbf{u}]$, dostajemy $d \cdot c^s = \sum_i \tilde{A}_i h_i$, gdzie $\tilde{A}_i \in \mathbb{R}[\mathbf{u}, \mathbf{x}]$. Jeśli teraz zachodzi teza i zerują się wszystkie h_i, to przy założeniu $d \neq 0$ musi zerować się c, a zatem zachodzi generyczne wynikanie po założeniu $d(\mathbf{u}) \neq 0$. □

Warto nadmienić, że w wielu algorytmach przy stosowaniu drugiej części powyższego kryterium, dla uproszczenia obliczeń wykonuje się najpierw test przynależności do ideału (co często zachodzi), dopiero gdy ten zawiedzie, testuje się radykał [4].

Odwrócenie tego kryterium jest prawdziwe dopiero nad $\mathbb{C}$ i wymaga użycia twierdzenia Hilberta o zerach. Obserwacja ta pokazuje również pierwsze ograniczenia powyższej metody, do których jeszcze powrócimy.

Dla kompletności podamy kryterium umożliwiające efektywne (obliczeniowe) sprawdzenie przynależności do radykału.

Propozycja 4. *Dla wielomianów* h_i *oraz* c *nad dowolnym ciałem zachodzi:*

$$c \in \sqrt{\mathbf{I}(h_1, \ldots, h_n)} \Leftrightarrow 1 \in \mathbf{I}(h_1, \ldots, h_n, c \cdot z - 1).$$

Dowód. Dla dowodu z prawej strony w lewą, wystarczy rozpisać odpowiednią kombinację, podstawić $z = c^{-1}$, a następnie pomnożyć przez dostatecznie dużą potęgę c^s. Z kolei, jeżeli wiemy, że $c^s \in I$ oraz $1 - cz \in I$, to $1 - c^s z^s \in I$ zatem $1 \in I$. □

W praktyce, oprócz twierdzenia egzystencjalnego, jesteśmy zainteresowani charakteryzacją przypadków zdegenerowanych. Zajmiemy się teraz tym opisem.

Warto odnotować, że wynikanie generyczne można zdefiniować w bardziej geometryczny sposób, jak w książce [4]. Wiemy z geometrii algebraicznej, że zbiór zer równań h_i rozkłada się na nierozkładalne składowe $\mathbf{V} = \mathbf{V}(h_1, \ldots, h_n) = \bigcup_i \mathbf{V}_i$. Z definicji, jeśli warunek niedegeneracji ma postać $d(\mathbf{u}) \neq 0$, to wielomian $d \cdot c$ zeruje się na $\mathbf{V}$, a więc na każdej składowej. Z nierozkładalności otrzymujemy, że dla każdego i albo c, albo d znika na $\mathbf{V}_i$. Mamy zatem $\mathbf{V} = \bigcup_i \mathbf{W}_i \cup \bigcup_j \mathbf{U}_j$, gdzie c znika na składowych $\mathbf{W}_j$, d zaś znika na $\mathbf{U}_j$. W szczególności, za $\mathbf{W}_i$ możemy przyjąć składowe, na których zmienne $\mathbf{u}$ są *algebraicznie niezależne*, wtedy bowiem d jako wielomian $\mathbf{u}$ nie znika. Na odwrót, załóżmy, że mamy takie przedstawienie oraz że c znika na składowych $\mathbf{W}_i$. Istnieją wielomiany $d_j \in \mathbb{R}[\mathbf{u}] \cap \mathbf{I}(\mathbf{U}_j)$. Wielomian $d = \prod_j d_j \in \mathbb{R}[\mathbf{u}]$ znika na wszystkich składowych $\mathbf{U}_j$, zatem jeśli $d \neq 0$, to c znika na $\mathbf{V}$. Otrzymujemy zatem:

Wniosek 5. *Teza c wynika generycznie z h_i poza przypadkami zdegenerowanymi zależnymi od* $\mathbf{u}$ *wtedy i tylko wtedy, gdy zachodzi na sumie składowych* $\mathbf{V}(h_1,\ldots,h_n)$*, na których* $\mathbf{u}$ *są algebraicznie niezależne.*

Powyższy wniosek nawiązuje do intuicji związanej ze zmiennymi $\mathbf{u}$. Zmienne te nazwaliśmy niezależnymi. Dobre wytypowanie zmiennych niezależnych zawęża poszukiwania warunków niedegeneracji. Zwróćmy uwagę, że choć odrzucenie składowych, na których $\mathbf{u}$ są zależne, daje rozwiązanie, nie musi być to optymalny (tj. najsłabszy) warunek. Dalej podamy sposób obliczania wielomianu d (bez rozkładu $\mathbf{V}$).

Propozycja 6. *Jeżeli* $d \in \mathbf{I}(h_1,\ldots,h_n,c\cdot z-1)\cap\mathbb{R}[\mathbf{u}]$*, to c wynika generycznie z h_i, poza przypadkami zdegenerowanymi* $d(\mathbf{u})=0$*. Odwrotny fakt, przy zastąpieniu wielomianu d pewną jego potęgą, zachodzi nad* $\mathbb{C}$*.*

Dowód. Załóżmy, że $d=\sum_i A_i\cdot h_i + A\cdot(cz-1)$. Podstawiając $z=c^{-1}$ i mnożąc przez dostatecznie wysoką potęgę c, otrzymujemy $d\cdot c^s=\sum_i \tilde{A}_i\cdot h_i$, gdzie $\tilde{A}_i\in\mathbb{R}[\mathbf{u},\mathbf{x}]$. Dzieląc przez $d(\mathbf{u})$, dostajemy $c\in\sqrt{\mathbf{I}_{\mathbb{R}(\mathbf{u})}(h_1,\ldots,h_n)}$ i korzystamy z poprzednich faktów. Dla dowodu odwrotnego kryterium zauważmy, że jeśli zachodzi (3), to z twierdzenia Hilberta o zerach mamy

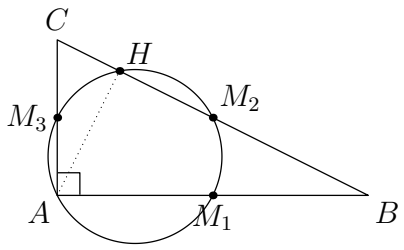
$$1\in\mathbf{I}(h_1,\ldots,h_n,c\cdot z_1-1,d\cdot z_2-1).$$

Podstawiając tu $z_2=d^{-1}$ i mnożąc następnie przez d^s, dostajemy żądane przedstawienie. □

Oczywiście wielomian d jest dobrym warunkiem niedegeneracji wtedy i tylko wtedy, gdy jest nim d^s. Z powyższego faktu wynika więc, że warunków niedegeneracji poszukujemy w praktyce obliczając bazę $\mathbf{I}(h_1,\ldots,h_n,c\cdot z-1)\cap\mathbb{R}[\mathbf{u}]$.

Dla zilustrowania powyższych twierdzeń przedstawiamy przykład automatycznego dowodu wraz z szukaniem warunków niedegenerujących.

Przykład 7 (Twierdzenie Apoloniusza)**.** Niech $\triangle ABC$ będzie trójkątem z kątem prostym A. Wówczas środki trzech boków oraz spodek H wysokości opuszczonej z A na bok BC leżą na jednym okręgu.



Dowód. Dla obliczeń, przyjmijmy:

$$\begin{array}{lll} A=(0,0), & M_1=(x_1,0), & H=(x_6,x_6),\\ B=(u_1,0), & M_2=(x_2,x_3), & O=(x_7,x_8).\\ C=(0,u_2), & M_3=(x_4,x_0), & \end{array}$$

Liczymy w SINGULAR:

```
 ring R = (0,u1,u2),(x1,x2,x3,x4,x5,x6,x7,x8,z),lp;
 poly h1 = 2*x1-u1;
 poly h2 = 2*x2-u1;
 poly h3 = 2*x3-u2;
 poly h4 = 2*x4-u2;
 poly h5 = -x5*u1 + x6*u2;
 poly h6 = (x6-0)*(0-x5)-(x5-u1)*(u2-x6);
 poly h7 = (x7-x1)^2+(x8-0)^2-(x7-x2)^2-(x8-x3)^2;
 poly h8 = (x7-x1)^2+(x8-0)^2-(x7-0)^2-(x8-x4)^2;
 poly c = (x7-x1)^2+(x8-0)^2 - (x7-x5)^2-(x8-x6)^2;
 ideal I = (h1,h2,h3,h4,h5,h6,h7,h8,1-c*z);
 std(I);
_[1]=1
```

Pierwsze cztery równania opisują środki boków, równanie h_5 opisuje punkt H, a pozostałe równania relację leżenia na okręgu dla odpowiednich punktów. Obliczenia bez parametryzacji zmiennych u_1, u_2 nie dają pozytywnego rezultatu, natomiast nad ciałem $\mathbb{R}[\mathbf{u}]$ test wypada pozytywnie. W myśl (3), twierdzenie zachodzi tylko generycznie, pod warunkiem $d(u_1,u_2)\neq 0$. Żeby wyznaczyć ten warunek, korzystamy z (6):

```
 ring R = (0),(x1,x2,x3,x4,x5,x6,x7,x8,u1,u2,z),lp;
 ... // definicje równań jak poprzednio
 std(I);
_[1]=u2;
_[2]=u1;
_... // inne wielomiany
```

Otrzymujemy dwa równouprawnione warunki niedegeneracji: $u_1\neq 0$ lub $u_2\neq 0$. Jeśli jeden z nich jest spełniony, w każdym z przypadków trójkąt jest niezdegenerowany bądź redukuje się do odcinka i punkty również wtedy leżą na jednym okręgu (istnieje nieskończenie wiele takich okręgów). □

Jak wcześniej zasygnalizowano, za pomocą metod algebraicznych można również poszukiwać twierdzeń. Można to zrobić, wyszukując specyficzne relacje (np. zawierające tylko wskazane zmienne) w radykale założeń. Z poprzednich faktów otrzymujemy:

Propozycja 8. *Jeżeli* $c \in \sqrt{\mathbf{I}_{\mathbb{R}(\mathbf{u})}(h_1, \ldots, h_n)} \cap \mathbb{R}[\mathbf{y}]$*, to* c *zależy od zmiennych* $\mathbf{y}$ *i wynika generycznie z* h_i*, poza przypadkami zdegenerowanymi określonymi równaniem zależnym od* $\mathbf{u}$*.*

Dla zilustrowania powyższego twierdzenia wyprowadźmy wzór Herona. Zauważmy, że potrzebujemy wybrać jeden z wielomianów z ideału określonego w twierdzeniu. Obliczenie ideału oznacza obliczenie bazy, tę zaś można łatwo obliczyć dzięki specyficznym właściwościom baz Gröbnera. Nie wdając się w szczegóły techniczne, wykraczające poza zakres tego referatu, wspomnieć należy, że posiadają one własność eliminacji. Odpowiednio uporządkowane zmienne prowadzą do uporządkowanej bazy w postaci trójkątnej: wielomiany zależne od jednej, dwóch, trzech i kolejno coraz więcej zmiennych, analogicznie jak w eliminacji Gaussa układu równań liniowych.

Przykład 9. Wyznaczyć pole s trójkąta $\triangle ABC$ w zależności od długości jego boków.

Wyprowadzenie wzoru Herona. Przyjmijmy $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$. Obliczenia wyglądają następująco:

```
 ring R = (0),(u_1,u_2,u_3,s,c,b,a),lp;
// uporządkowanie zmiennych jest istotne!
 poly h1 = c^2-u_1^2;
 poly h2 = a^2-(u_2-u_1)^2-u_3^2;
 poly h3 = b^2-u_2^2-u_3^2;
 poly h4 = 4s^2-u_1^2*u_3^2;
 ideal I = (h1,h2,h3,h4);
 std(I);
// wielomian pojawiający się w pierwszej kolejności w bazie!
_[1]=64*s^2+c^4-2*c^2*b^2-2*c^2*a^2+b^4-2*b^2*a^2+a^4
_... inne wielomiany
```

Równanie, które otrzymaliśmy jako pierwsze, to rozwinięta formuła Herona. □

3. Ograniczenia

Po pokazaniu, jak można efektywnie zastosować aparaturę algebraiczną do dowodzenia w geometrii, kolej odnieść się do jej ograniczeń.

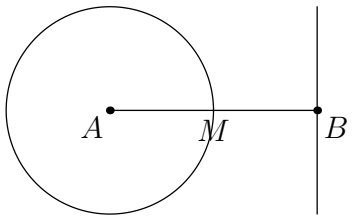
(i) Metoda jest zupełna jedynie nad $\mathbb{C}$. Nie potrafimy rozstrzygać o fałszywości danego stwierdzenia. Znalezione dostateczne warunki niedegeneracji nie są na ogół konieczne, zatem nie dowodzimy twierdzenia w jego najmocniejszej wersji. Jednakże, jest ciekawym i zadziwiającym faktem, że ogromna liczba twierdzeń z płaskiej geometrii, zawierających punkty, okręgi linie, stożkowe, zachodzi również nad $\mathbb{C}$.

(ii) Formuły tłumaczące konfigurację na język algebry ograniczają się do uniwersalnych formuł Horna.

(iii) Formuły nie zawierają nierówności porządkowych $\geqslant$.

Ostatnie ograniczenie uniemożliwia nie tylko dowodzenie nierówności geometrycznych. Na przykład nie jesteśmy w stanie zdefiniować równaniami pojęcia „wnętrze trójkąta", rozróżnić półpłaszczyzny po jednej stronie prostej od drugiej, dwusiecznej kąta wewnętrznego od zewnętrznego itd. Drugie wspomniane ograniczenie nakłada kolejne obostrzenia na możliwości wyrażania twierdzeń, w szczególności na kwantyfikowanie zmiennych. Na koniec, pierwszy punkt pozostawia obawę, że formuła geometryczna, na którą się natkniemy, nie jest spełniona w $\mathbb{C}$. Takie też przykłady, pochodzące z pracy [3], przedstawimy poniżej. Jedną z możliwości wykolejenia rozważanej metody jest konfiguracja wyjściowa, która nie może zajść nad $\mathbb{R}$, za to zachodzi nad $\mathbb{C}$.

Przykład 10 (Chou)**.** Niech A, B będą różnymi punktami, niech M będzie środkiem AB. Niech C leży na przecięciu okręgu $A, |AM|$ z prostą l przechodzącą przez B i prostopadłą do AB. Wtedy $|AC| = |AB|$.



Mniej trywialnym przykładem jest własność, która zachodzi w $\mathbb{R}$, ale nie w $\mathbb{C}$.

Przykład 11 (MacLane)**.** Rozważmy 8 punktów $A_1, \ldots, A_8$, takich że każde wymienione 3 są współliniowe: $A_i A_{i+1} A_{i+3}$, dla $i = 1, \ldots, 8$. Wtedy wszystkie punkty są współliniowe.

4. Eliminacja kwantyfikatorowa

Celem tego rozdziału jest odpowiedź na pytanie zadane w rozdziale poprzednim: jak efektywnie poradzić sobie z ograniczeniami opisanej konwencjonalnej metody algebraicznej. Przypomnijmy w tym celu rezultat Tarskiego:

Twierdzenie 12 (Tarski, 1930)**.** *Dla języka pierwszego rzędu* $\{\mathbb{R}, +, *, =, >\}$ *istnieje procedura eliminacji kwantyfikatorów.*

Niestety, procedura podana przez Tarskiego ma złożoność nieelementarną [3]. W praktyce zaimplementowano inne algorytmy eliminacji kwantyfikatorów [3]:

(i) Cylindrical Algebraic Decomposition (w QECAD),

(ii) Virtual Substitutions of Test Terms (w REDLOG/REDUCE),

(iii) Gröbner Bases with Multivariate Real Root Counting (w QERRC).

Dalej zakładać będziemy, że formuła, z którą pracujemy, jest zapisana (po wyrażeniu w języku algebry) w postaci

$$Q_1 u_1 \dots Q_p u_p \, Q_{p+1} x_1 \dots Q_{p+q} x_q \, \psi(\mathbf{u}, \mathbf{x}), \quad Q_i \in \{\forall, \exists\}, \tag{4}$$

gdzie ψ jest kombinacją logiczną równości, nierówności i porządkowych nierówności wielomianowych. Żeby pokazać (4), można użyć eliminacji kwantyfikatorowej, by otrzymać formułę równoważną, pozbawioną kwantyfikatorów $\psi^*(\mathbf{u}, \mathbf{x})$. Formuła ta nie zawiera kwantyfikowanych zmiennych $\mathbf{u}, \mathbf{x}$, tak więc $\psi^*(\mathbf{u}, \mathbf{x}) = \psi^*$ zawiera jedynie stałe logiczne. Stąd

Propozycja 13. *Twierdzenie geometryczne 4 jest uniwersalnie prawdziwe wtedy i tylko wtedy, gdy* $\psi^* =$ true*, gdzie* ψ^* *jest rezultatem procedury QE zastosowanej do* ψ*.*

Wykazaliśmy jak pokazać, że twierdzenie jest uniwersalnie prawdziwe. Dalej użyjemy procedury QE, żeby dowodzić zachodzenie generyczne twierdzenia, w szczególności będziemy zainteresowani dodatkowymi warunkami, jakie trzeba nałożyć, żeby twierdzenie było prawdziwe. Rozważać będziemy dwa przypadki:

(i) Znamy warunek dostateczny.

(ii) Nie znamy warunków dostatecznych.

Pierwszy z przypadków jest banalny, wystarczy bowiem dołączyć warunki do założeń. Czasem – aczkolwiek, jak zaznaczaliśmy, rzadko – dodatkowe warunki nie są potrzebne.

Przykład 14 (Nierówność Pedoe)**.** Rozważmy dwa trójkąty $\triangle ABC$, $\triangle A'B'C'$ z bokami a, b, c, a', b', c' odpowiednio. Pola S, S' trójkątów spełniają następującą nierówność:

$$a'^2(b^2 + c^2 - a^2) + b'^2(c^2 + a^2 - b^2) + c'^2(a^2 + b^2 - c^2) \geqslant 16SS'. \tag{5}$$

Dowód. Połóżmy $A = A' = (0,0)$, $B = (u_1, 0)$, $B' = (u_2, 0)$, $C = (u_3, u_4)$, $C' = (u_5, u_6)$. Wyrażając boki w terminach wprowadzonych zmiennych, otrzymujemy formułę równoważną twierdzeniu ψ:

$$\begin{aligned}\forall_{[a,b,c,a',b',c',d',S,S']} \, (a^2 = (u_1 - u_3)^2 + u_4^2 \wedge b^2 = u_3^2 + u_4^2 \wedge c^2 = u_1^2 \wedge a'^2 = \\ = (u_2 - u_5)^2 + u_6^2 \wedge b'^2 = u_5^2 + u_6^2 \wedge c'^2 = u_2^2 \wedge 4S^2 = (cu_4)^2 \wedge 4S'^2 = (c'u_6)^2) \\ \Rightarrow a'^2(b^2 + c^2 - a^2) + b'^2(c^2 + a^2 - b^2) + c'^2(a^2 + b^2 - c^2) \geqslant 16SS'.\end{aligned} \tag{6}$$

Po przeprowadzeniu QE w REDUCE otrzymujemy $\psi =$ true. □

Żeby znaleźć warunek dostateczny dla zachodzenia twierdzenia, zależny od $\mathbf{u}$, pozostawiamy zmienne $\mathbf{u}$ jako wolne (niekwantyfikowane) i przeprowadzamy eliminację

$$Q_1 x_1 \dots Q_q x_q \, \psi(\mathbf{u}, \mathbf{x}) \Leftrightarrow \psi^*(\mathbf{u}), \tag{7}$$

gdzie $\psi^*(\mathbf{u})$ jest formułą wolną od kwantyfikatorów. Warunkiem dostatecznym i koniecznym przy uniwersalnym kwantyfikowaniu $\mathbf{u}$ jest $\psi^*(\mathbf{u}) =$ true.

Propozycja 15. *Procedura QE, zastosowana do formuły powyżej, dostarcza zarazem koniecznych i dostatecznych warunków (zależnych od* $\mathbf{u}$*).*

Wadą powyższego podejścia jest fakt, że rezultat jest bardziej skomplikowany niż rozważane wcześniej warunki niedegeneracji i trudniej jest go odczytać jako własność geometryczną. Żeby otrzymać proste warunki dostateczne, można użyć generycznej eliminacji (*generic quantifier elimination algorithm*), która dostarcza warunków dostatecznych w formie negacji równań [3].

Zaletą jest fakt, że warunki otrzymane z QE są w ogólności dowolną kombinacją logiczną równań, negacji równań i nierówności, podczas gdy konwencjonalne warunki niedegeneracji ograniczają się do negacji równań, w związku z czym wykluczają zawsze zbiór miary 0. Dla przykładu, w QE możemy otrzymać dodatkowy warunek typu: twierdzenie jest prawdziwe jedynie dla trójkątów równobocznych. Tego faktu nie można wyrazić, odrzucając przypadki zdegenerowane. Co więcej, eliminacja kwantyfikatorowa pozwala rozstrzygać zdania, nie tylko dowodzić ich prawdziwości.

Jako kolejny wniosek otrzymujemy następujący fakt:

Wniosek 16. *Przez znalezienie warunków dostatecznych, możemy zastosować QE do wykrywania twierdzeń.*

Przykład 17 (Wzór Herona)**.** Wyznaczyć pole S trójkąta $\triangle ABC$ w zależności od długości boków.

Dowód. Kładziemy $A = (-u_1, 0), B = (u_1, 0), C = (u_2, u_3)$. Wtedy

$$a^2 = (u_1 - u_2)^2 + u_3^2,\ b^2 = (-u_1 - u_2)^2 + u_3^2,\ c^2 = 4u_1^2,\ S^2 = u_1^2 u_3^2.$$

Problem zapisuje się w postaci następującej formuły:

$$\exists_{u_1} \exists_{u_2} \exists_{u_3} [S^2 = u_1^2 u_3^2 \wedge a^2 = (u_1 - u_2)^2 + u_3^2 \wedge b^2 = (u_1 + u_2)^2 + u_3^2 \wedge c^2 = (2u_1)^2] \quad (8)$$

Generyczna eliminacja kwantyfikatorów daje dodatkowy warunek $u_1 \neq 0$ oraz

$$a^4 - 2a^2b^2 - 2a^2c^2 + b^4 - 2a^2b^2 + c^4 + 16S^2 = 0$$

(i pewne redundantne formuły). □

5. Podsumowanie

Eliminacja kwantyfikatorów jest ciekawym narzędziem powiększającym możliwości przeprowadzania automatycznych dowodów w sposób algebraiczny. Jakkolwiek mniej efektywna w praktyce, z teoretycznego punktu widzenia nie posiada dyskutowanych wcześniej ograniczeń. Celem referatu było przedstawienie jedynie najważniejszych aspektów teoretycznych i praktycznych najpopularniejszej (najprostszej?) metody, zainteresowanego Czytelnika zachęcam zatem do samodzielnej lektury bogatej literatury dotyczącej AGTP. Przyjaznym wprowadzeniem do podstaw geometrii

algebraicznej i klasycznej metody automatycznego dowodzenia twierdzeń jest książka [4]. Z kolei bardzo dobrą pozycją w temacie QE jest praca [3], w której znajduje się m.in. zbiór przedyskutowanych przykładów z automatycznego dowodzenia przy zastosowaniu QE. Publikacje i monografie poruszające zastosowanie tak obliczeniowo-algebraicznych, jak i bardziej innowacyjnych metod w AGTP łatwo można wyszukać pod hasłem Automated Geometry Theorem Proving.

Literatura

[1] W. Decker, G. M. Greuel, G. Pfister, H. Schönemann: SINGULAR 3-1-2 – *A computer algebra system*, `http://www.singular.uni-kl.de` (2010).

[2] REDUCE 3-8 – *A computer algebra system*, `http://www.reduce-algebra.com/` (2010).

[3] T. Sturm, *Real Quantifiers Elimination in Geometry*, PhD thesis, University of Passau, Germany 1999.

[4] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag New York, 1992.

Topological properties of infinite computations

Michał Skrzypczak

Abstract. The in-out model of computer programs is not suitable for "reactive" systems (e.g. servers). Appropriate model for them is an idea of infinite computation — a sequence of states, indexed by natural numbers. But how to define (or better automatically check) properties of such objects? It turns out, that this problem naturally connects logic, topology and combinatorics.

This document presents basic notions and results from the area, including ω-regular languages, the MSO logic and the Borel hierarchy. At the end of the article, some current problems are discussed.

1. Motivation

Computer systems are becoming more and more complicated. Moreover, they control many important elements of our environment: traffic lights, flight parameters or even medical equipment. Therefore, sometimes we need to make sure, that a program does not contain any error.

Usually this task is divided into the following steps:

(i) Define a semantics of programs,

(ii) express expected properties in some formal language,

(iii) proof or better automatically check that a given program fulfils given specification.

There are well known methods of performing this tasks, for example programmers can:

- write programs in declarative languages, where program itself is a kind of a specification,
- define a formal semantics of the given programming language (e.g. small steps, big steps or continuations semantics),
- use induction, Hoare logic, etc. to create formal proofs of correctness,
- ...

Michał Skrzypczak
mskrzypczak@mimuw.edu.pl
student Jednoczesnych Studiów Informatyczno-Matematycznych
Uniwersytet Warszawski

But all this methods implicitly treat a program as some kind of a (partial) in→out function: program reads an input, performs some computations step by step and outputs the result. This schema is appropriate for many programs, including `pdflatex` used to create this article. But what about servers that run potentially forever?

Example 1. Mail server has three states: `receiving`, `reordering`, `sending`. We want to ensure that the server will infinitely often receive:

$$\forall_{n\in\mathbb{N}}\, \exists_{k\geq n}\, S(k) = \text{receiving}.$$

Imagine we obtained a source code of some mail server. How can we check that it satisfies the property defined above? The following problems occur:

- We cannot just simulate the whole computation — its infinite,
- First order logic over $(\mathbb{N}, +, \cdot)$ is undecidable, so even simple properties of moments of time cannot be automatically checked.
- Servers are parallel — they communicate one with another. Therefore, testing a server may not expose possible errors: for example the time when an error may occur during a communication is too short for currently used hardware.

The solution presented in this paper is based on the following ideas (explained in detail later):

(i) model a server as a finite state machine with states denoted by Σ,

(ii) treat an infinite computation as a sequence $\alpha \in \Sigma^\omega$,

(iii) use *Monadic Second Order logic* to express and check properties of such computations.

2. MSO Logic

In this section we define the MSO logic, show some properties definable in it and present the decidability theorem of Büchi.

Definition 2. MSO logic is second order logic with additional restriction that second order quantification may bind only sets of elements.

In other words, it is a set of formulas containing:

- $x \in X$ for variables x, X,
- $R_i(x_1, \ldots, x_n)$ for every relational symbol R_i,
- $\varphi \vee \psi$,

- $\neg\varphi$,
- $\exists_x\ \varphi(x)$, where x is a variable valued in elements of the structure,
- $\exists_X\ \varphi(X)$, where X is a variable valued in subsets of the structure,

where φ, ψ denote simpler MSO formulas.

The semantics of such formulas is defined in the natural way.

We will restrict ourselves to structures representing infinite words.

Definition 3. Every $\alpha \in \Sigma^\omega$ can be treated as a relational structure of the form $\langle \omega, \leq, \Sigma \rangle$, where

- $\omega = \{0, 1, 2, \ldots\}$ is a carrier of the structure,
- $\leq$ is a binary relation of order on ω,
- for each $A \in \Sigma$ there is an unary predicate A, defined by equation

$$A(n) \Leftrightarrow \alpha_n = A.$$

Definition 4. For a given MSO formula φ, we construct *a language defined by* φ

$$L(\varphi) = \{\alpha \in \Sigma^\omega : \alpha \models \varphi\},$$

that is a set of such $\alpha \in \Sigma^\omega$ that (when treated as a structure) satisfy φ.

To make things easy the signature of the language contains only $\leq$ and elements of Σ. But it is easy to see that using $\leq$ we can define a constant $0 \in \omega$ and a function $s(n) = n + 1$.

Example 5. Take $\Sigma = \{A, B\}$ and consider a MSO formula

$$\varphi = \exists_P \forall_n\ \ (n \in P \Leftrightarrow s(n) \notin P) \wedge 0 \in P \wedge \exists_k\ k \in P \wedge A(k).$$

There is exactly one set $P \subseteq \omega$ satisfying property $\forall_n\ n \in (P \Leftrightarrow s(n) \notin P) \wedge 0 \in P$ — the set of even numbers. So $\alpha \models \varphi$ if and only if there exists an even number k such that $\alpha_k = A$.

Definition 6. The family of all sets of the form $L(\varphi) \subseteq \Sigma^\omega$ will be called the family of ω-regular languages (over alphabet Σ).

Sometimes we will consider the following logic.

Definition 7. By WMSO (Weak Monadic Second Order logic) we denote a logic with the same syntax as MSO logic. The only difference is that second order quantifiers in WMSO range over finite sets only. So for example $\exists_X\ \varphi(X)$ means that there exists *finite* set X such that $\varphi(X)$.

Since MSO logic enables us to express that a given set X is finite, every formula of WMSO can be rewritten to the equivalent MSO formula.

Now we proceed to the most important theorem.

Theorem 8 (Büchi 1960)**.** *The emptiness problem for* MSO *over infinite words is decidable. That means, there exists an algorithm that reads a formula φ and outputs 0 if $L(\varphi) = \emptyset$ and 1 if $L(\varphi) \neq \emptyset$.*

Before we sketch the proof, first observe that solving an emptiness problem can be used to solve the following problems:

- given φ, ψ, answer whether $L(\varphi) \subseteq L(\psi)$ — consider $\gamma = \varphi \wedge \neg\psi$,
- given φ, ψ, answer whether $L(\varphi) \cap L(\psi) = \emptyset$ — consider $\gamma = \varphi \wedge \psi$,
- given φ, answer whether $L(\varphi) = \Sigma^\omega$ — consider $\gamma = \neg\varphi$.

Idea of the proof of Theorem 8. The sketch of the proof is explained in the following steps.

(i) Define a model of finite automata that read an infinite word and accept or reject it.

(ii) Show that each MSO formula φ can be automatically transformed into an equivalent automaton $\mathcal{A}$.

(iii) Write a program that reads $\mathcal{A}$ and answers whether $\mathcal{A}$ is able to accept any infinite word.

The construction of the automata and an insight into second step of the proof are presented in the next section. □

3. Automata

In the original paper of Büchi so called "nondeterministic Büchi automata" were used. To simplify, we will work with other (equivalent) model.

Definition 9. Deterministic parity automaton is a tuple $\mathcal{A} = \langle q_0, Q, \delta, \Omega \rangle$ where

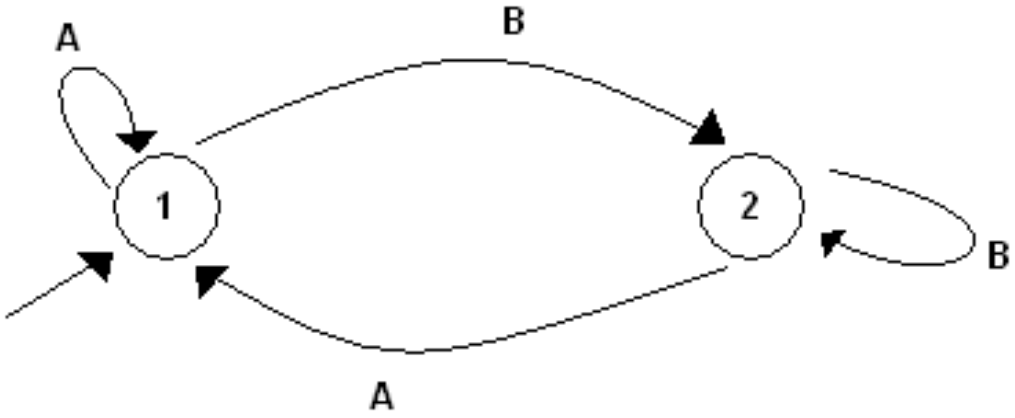
- q_0 is an element of Q called *initial state*,
- Q is a finite set of *states*,
- $\delta\colon Q \times \Sigma \to Q$ is a *transition function*,
- $\Omega\colon Q \to \mathbb{N}$ maps a state $q \in Q$ into its *rank* $\Omega(q) \in \mathbb{N}$.

For a given word $\alpha \in \Sigma^\omega$, we define the *run* $\tau \in Q^\omega$ inductively $\tau_0 = q_0$ and $\tau_{n+1} = \delta(\tau_n, \alpha_n)$. We say that $\mathcal{A}$ accepts a word α iff

$$\liminf_{n\to\infty} \ \Omega(\tau_n) \equiv 1 \mod 2.$$

By $L(\mathcal{A})$ (language recognised by automaton $\mathcal{A}$) we denote the set of all words $\alpha \in \Sigma^\omega$ accepted by $\mathcal{A}$.

Example 10. Consider automaton $\mathcal{A}$: $Q = \{1, 2\}$, $q_0 = 1$, $\Omega(q) = q$, $\delta(q, A) = 1$ and $\delta(q, B) = 2$. Then $\mathcal{A}$ accepts $\alpha \in \{A, B\}^\omega$ iff α contains infinitely many A's.



Now, after defining the automata model, we can start transforming MSO formulas into automata.

Proof of the second step of the Büchi's theorem. Firstly, using a little of combinatorics, one can show that given automata $\mathcal{A}_1, \mathcal{A}_2$, we can construct automata $\mathcal{A}_\cup, \mathcal{A}_\cap, \mathcal{A}_\neg$ with properties

- $L(\mathcal{A}_\cup) = L(\mathcal{A}_1) \cup L(\mathcal{A}_2)$,
- $L(\mathcal{A}_\cap) = L(\mathcal{A}_1) \cap L(\mathcal{A}_2)$,
- $L(\mathcal{A}_\neg) = \Sigma^\omega \setminus L(\mathcal{A}_1)$.

Additionally, there are simple automata: one reading a word encoding $x \in \mathbb{N}, X \subseteq \mathbb{N}$ and checking whether $x \in X$, the second reading a word encoding $x, y \in \mathbb{N}$ and checking whether

$x \leq y$ and the third one reading a word encoding $x \in \mathbb{N}$ and checking whether $A(x)$ for fixed $A \in \Sigma$.

So, using the above remarks, we can inductively transform the formula into the automaton, changing logic operators (like $\wedge$) into set theory operators (like $\cap$) and building more and more complicated automata. The only construction of MSO logic that remains is quantification.

Lemma 11. *For a given automaton $\mathcal{A}$ over alphabet $\Sigma \times \Gamma$, there exists an automaton $\mathcal{B}$ over Σ with a property*

$$L(\mathcal{B}) = \{\alpha \in \Sigma^\omega \colon\ \exists_{\beta \in \Gamma^\omega}\ (\alpha, \beta) \in L(\mathcal{A})\}\,,$$

so the automaton recognising a projection of $L(\mathcal{A})$ to Σ^ω.

The proof of this lemma is very technical and involves a lot of tricky combinatorics. But after showing it, we can proceed as follows.

- Given a formula of the form $\exists_X\ \varphi(X)$ create an automaton $\mathcal{A}$ over alphabet $\Sigma \times 2$ such that $(\alpha, X) \in L(\mathcal{A})$ iff $\alpha \models \varphi(X)$. The construction of $\mathcal{A}$ is inductive over the structure of φ.
- Use the construction from Lemma 11 to construct the automaton $\mathcal{B}$ recognising $\pi(L(\mathcal{A}))$.
- Easily show that $L(\mathcal{B}) = L\left(\exists_X\ \varphi(X)\right)$.

Formulas starting with $\exists_x, \forall_x, \forall_X$ can be transformed into formulas of the form $\exists_X$ using syntactical tricks. This ends the proof. □

The other transformation is also possible.

Theorem 12. *Given an automaton $\mathcal{A}$ one can construct a* WMSO *formula φ such that*

$$L(\varphi) = L(\mathcal{A}).$$

Moreover, one can construct a MSO *formula φ with the same property and additionally $\varphi = \exists_{\overline{X}}\, \psi(\overline{X})$ for some first order formula ψ.*

The proof is rather simple and we will skip it.

Remark 13. The family of ω-regular languages can be equivalently defined as a family of languages that:

- are definable by MSO formulas,
- are definable by WMSO formulas,
- are recognisable by deterministic parity automata,
- are recognisable by nondeterministic Büchi's automata.

More about the MSO logic and automata can be found in a paper [3].

4. Topology

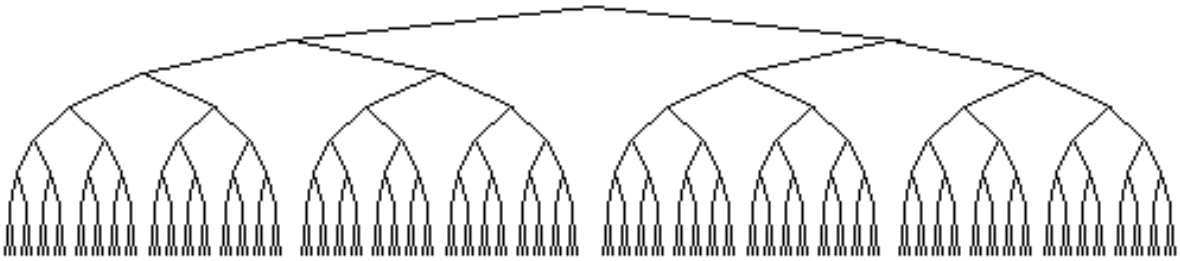
Since ω-regular languages are subsets of Σ^ω, there is a natural idea of using topological methods to investigate their complexity.

Definition 14. Consider a topology on Σ^ω generated by sets

$$[s] := \left\{\alpha \in \Sigma^\omega \colon \ \alpha|_{|s|} = s\right\},$$

for $s \in \Sigma^*$.

The topology of Σ^ω can be illustrated by the following picture, where elements of Σ^ω are infinite branches of the tree.



Fact 15. *For every Σ such that $2 \leq |\Sigma| < \infty$ the space Σ^ω is homeomorphic to the Cantor's discontinuum.*

In the following two subsections we will construct tools of measuring the complexity of subsets of a given topological space.

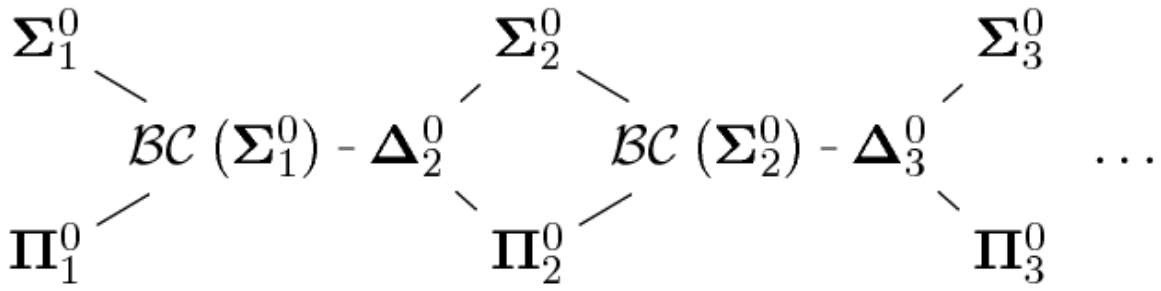
4.1. The Borel hierarchy

It is easy to see that the countable intersection of open sets may be no longer open. The same holds for sums of closed sets. Using this observation, we define a hierarchy of more and more complicated subsets of given topological space.

Definition 16. Inductively, for $\eta < \omega_1$, define

- $\mathbf{\Sigma}^0_1$ as a family of all open sets,
- $\mathbf{\Pi}^0_1$ as a family of all closed sets,
- $\mathbf{\Sigma}^0_\eta$ as a family of countable unions of sets from $\bigcup_{\tau<\eta} \mathbf{\Pi}^0_\tau$,
- $\mathbf{\Pi}^0_\eta$ as a family of complements of sets from $\mathbf{\Sigma}^0_\eta$,
- $\mathcal{BC}\left(\mathbf{\Sigma}^0_\eta\right)$ as the smallest boolean algebra containing $\mathbf{\Sigma}^0_\eta$,
- $\Delta^0_\eta = \mathbf{\Sigma}^0_\eta \cap \mathbf{\Pi}^0_\eta$.

The key property of this hierarchy is the fact that it is strict — every inclusion at this diagram is not an equality.



Definition 17. The family $\mathcal{B} = \bigcup_{\eta<\omega_1} \mathbf{\Sigma}_\eta^0$ is called a family of Borel sets.

Fact 18. *The family $\mathcal{B}$ is an σ-algebra.*

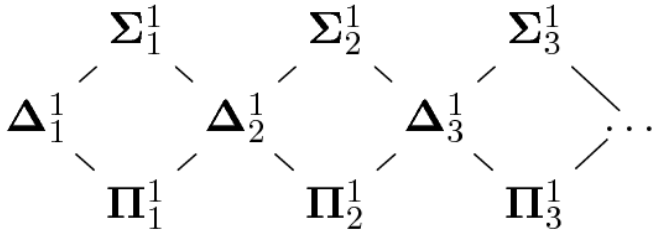
4.2. The projective hierarchy

To go beyond the Borel hierarchy we have to consider more powerful constructions than countable unions and intersections. Since a countable union can be seen as a projection $\pi\colon X \times \mathbb{N} \to X$, the natural candidates are general projections $\pi\colon X \times Y \to X$.

Definition 19. A set $A \subseteq X$ is called *analytic* (den. $\mathbf{\Sigma}_1^1$) iff it is a projection of some Borel set in $X \times Y$. By an induction on $n < \omega$ we define

- $\mathbf{\Pi}_n^1$ as complements of sets from $\mathbf{\Sigma}_n^1$,
- $\mathbf{\Sigma}_{n+1}^1$ as projections of sets from $\mathbf{\Pi}_n^1$,
- $\mathit{\Delta}_n^1 = \mathbf{\Sigma}_n^1 \cap \mathbf{\Pi}_n^1$.

The same as before the hierarchy is strict. This time its length is ω.



Additionally, the following strong result holds.

Theorem 20 (Souslin)**.** *Borel sets are exactly $\mathit{\Delta}_1^1$ sets, that is*

$$\mathcal{B} = \mathit{\Delta}_1^1 = \mathbf{\Sigma}_1^1 \cap \mathbf{\Pi}_1^1.$$

4.3. Continuous reductions

The families defined in the previous two sections will be called *topological complexity classes* and denoted by $\mathcal{C}$. We will say that a set $A \subseteq X$ has a complexity $\mathcal{C}$ iff $A \in \mathcal{C}$ and for each complexity class $D \subsetneq C$ we have $A \notin \mathcal{D}$.

The main tool for finding a complexity of a given set are so called continuous reductions.

Definition 21. A function $f\colon X \to Y$ is called a *continuous reduction* of $A \subseteq X$ to $B \subseteq Y$ iff f is continuous and $f^{-1}(B) = A$.

In other words, f is a reduction of A to B if to check whether given $x \in X$ belongs to A it is enough to check if $f(x) \in B$.

Definition 22. A set $B \subseteq X$ is called *hard* for a class $\mathcal{C}$ (or $\mathcal{C}$-hard) iff for every $A \in \mathcal{C}$ there exists continuous reduction of A to B.

If additionally $B \in \mathcal{C}$ then B is called *complete* in class $\mathcal{C}$ (or $\mathcal{C}$-complete).

Theorem 23. *There exist complete sets for every class of the form* $\mathbf{\Sigma}^0_\eta, \mathbf{\Pi}^0_\eta, \mathbf{\Sigma}^1_n, \mathbf{\Pi}^1_n$.

Example 24. The set $\{\alpha \in \{0,1\}^\omega\colon\ \exists_{i\in\mathbb{N}}\ \alpha_i = 1\}$ is $\mathbf{\Sigma}^0_1$-complete.

Moreover, for $i \in \mathbb{N}$ the set

$$\left\{\alpha \in 2^{\mathbb{N}^i}\colon\ \exists_{m_i}\forall_{m_{i-1}}\exists_{m_{i-2}}\ldots\forall_{m_1}\ \alpha(m_i, m_{i-1}, \ldots, m_1) = 1\right\}$$

is $\mathbf{\Sigma}^0_i$-complete.

The following fact is easy but powerful.

Fact 25. *Assume that $\mathcal{C} \subsetneq \mathcal{D}$ are topological complexity classes. Let $C \subseteq X$ satisfy $C \in \mathcal{C}$ and let $D \subseteq X$ be $\mathcal{D}$-complete.*

- *If D reduces to $E \subseteq X$ then E is $\mathcal{D}$-hard.*
- *If $B \subseteq X$ reduces to C then $B \in \mathcal{C}$.*
- *$D \notin \mathcal{C}$.*

5. Complexity of ω-regular languages

In this section we will investigate topological complexity of ω-languages and some extensions of this family.

The fundamental fact follows.

Fact 26. *Therefore, the topological complexity of ω-regular language is $\mathcal{BC}$ ($\mathbf{\Sigma}^0_2$).*

Proof. Deterministic automaton $\mathcal{A}$ induces a continuous reduction of $L(\mathcal{A})$ to the set

$$\mathcal{S} = \left\{ \tau \in Q^\omega : \ \liminf_{n\to\infty} \Omega(\tau_n) \equiv 1 \mod 2 \right\}.$$

It is easy to show that $\mathcal{S} \in \mathcal{BC}(\mathbf{\Sigma}^0_2)$. Therefore every ω-regular language is in $\mathcal{BC}(\mathbf{\Sigma}^0_2)$. Language defined in Example 10 is $\mathbf{\Sigma}^0_2$-complete, so a simple combination of this language and its complement gives us a set that is ω-regular but does not belong to $\mathbf{\Sigma}^0_2 \cup \mathbf{\Pi}^0_2$. □

Using this observation we can easily show that certain sets are not ω-regular languages.

Example 27. Language $\{a^{n_0}ba^{n_1}b\ldots : \ \lim_{i\to\infty} n_i = \infty\}$ is $\mathbf{\Pi}^0_3$-complete, therefore it is not ω-regular.

It is possible to show the above fact using combinatorical methods, but this way seems to be more straightforward.

One should not directly connect topological complexity and decidability. The following two examples explain the difference.

Example 28. There are only countably many ω-regular languages. Therefore, there exist $\mathbf{\Sigma}^0_1$ sets that are not ω-regular.

So very simple (from topological point of view) sets may not be ω-regular.

Example 29. Fix some very complex set, e.g. $P \subseteq \Sigma^\omega$ that is $\mathbf{\Sigma}^1_{100}$-complete.

Consider a language $\mathcal{L}$ build up from one atom Φ and boolean operators $\vee, \wedge, \neg$. Let the semantics of Φ be as follows

$$\alpha \models \Phi \quad \Leftrightarrow \quad \alpha \in P.$$

Of course emptiness problem is decidable for $\mathcal{L}$ — complexity of P does not play any role here. But the formula $\Phi \in \mathcal{L}$ defines P, so a $\mathbf{\Sigma}^1_{100}$-complete set.

This example shows that there exist languages defining very complicated sets and still decidable.

More about connections of topology and infinite computations can be found in [4].

5.1. Extensions of the MSO logic

Currently, various extensions of ω-regular languages are studied. We will concentrate on one of them.

There are natural properties not expressible in MSO logic, for example "the time between receiving and sending forward a message is bounded". Based on this observation one can add to standard MSO logic additional predicates to express such properties.

Definition 30. Formula $\mathrm{U}X.\varphi(X)$ holds iff

$$\forall_{n\in\mathbb{N}}\, \exists_{X\subset\omega}\; n \leq |X| < \infty \wedge \varphi(X).$$

Let $\mathrm{MSO} + \mathrm{U}$ denote logic MSO extended with U and analogously for $\mathrm{WMSO} + \mathrm{U}$.

The concept of $\mathrm{WMSO} + \mathrm{U}$ logic was studied by Mikołaj Bojańczyk. His paper [1] contains the following observations.

Fact 31. $\mathrm{WMSO} + \mathrm{U}$ *is a strict extension of* MSO.

Theorem 32. *Logic* $\mathrm{WMSO} + \mathrm{U}$ *is decidable over infinite words.*

The idea of the proof of this theorem also goes through the concept of automata. In this case these are deterministic $\max$-automata. Such automaton is similar to the construction of deterministic parity automaton but additionally it is equipped with counters. Such counters are not read during a run. The acceptance condition is a boolean combination of statements "counter c_i is bounded during the run".

Fact 33. *Topological complexity of languages definable in* $\mathrm{WMSO} + \mathrm{U}$ *is* $\mathcal{BC}\,(\mathbf{\Sigma}^0_2)$ *— the same as of* ω*-regular languages.*

The natural question about analogous results for full $\mathrm{MSO} + \mathrm{U}$ still remains open. The most important of them is the following conjecture.

Conjecture 34. *Logic* $\mathrm{MSO} + \mathrm{U}$ *is decidable over infinite words.*

Currently there is no adequate automata model for $\mathrm{MSO} + \mathrm{U}$ known. One of the ideas how to treat this problem is to estimate the topological complexity of languages definable in $\mathrm{MSO} + \mathrm{U}$ and compare it with known automata models. The following theorem from [2] provides a lower estimation.

Theorem 35. *There exists* $\mathbf{\Sigma}^1_1$*-complete (e.g. non Borel) set definable in* $\mathrm{MSO} + \mathrm{U}$.

An easy corollary follows.

Corollary 36. *There is no nondeterministic Borel automata model catching full* $\mathrm{MSO} + \mathrm{U}$.

The following questions still remain open:

- is there any decidable automata model catching $\mathrm{MSO} + \mathrm{U}$,
- does such automata model has decidable emptiness problem,
- what is an exact topological complexity of $\mathrm{MSO} + \mathrm{U}$.

References

[1] M. Bojańczyk, *Weak MSO with the Unbounding Quantifier*, STACS 2009, p. 159–170.

[2] S. Hummel, M. Skrzypczak, S. Toruńczyk, *On the Topological Complexity of MSO+U and Related Automata Models*, MFCS 2010, p. 429–440.

[3] W. Thomas, *Languages, Automata and Logics*, Kiel 1996.

[4] W. Thomas, H. Lescow, *Logical Specifications of Infinite Computations*, REX School/Symposium 1993, p. 583–621.

Prawda logiczna rośnie na drzewach

Szymon Szymczak

Streszczenie. Celem będzie przedstawienie i opis – w pewnym sensie ujednoliconych – drzew (tablic) semantycznych dla pewnej gamy logik zdaniowych: logiki klasycznej, rodziny logik modalnych, logiki intuicjonistycznej i relewantnej. Metoda drzew jest interesująca z następujących powodów. W przeciwieństwie do innych systemów dowodowych jest algorytmiczna: przeprowadzenie dowodu nie wymaga „sprytnego pomysłu". Upraszcza dowody trafności i pełności. W końcu, formalizuje pewien naturalny sposób rozumowania. Semantyką dla logik nieklasycznych obecną w tle będzie semantyka światów możliwych.

1. Wstęp

Logika, w moim przekonaniu, dotyczy głównie wynikania logicznego. Podstawowe pytanie logiki to: co (i kiedy) sprawia, że jeden wniosek wynika z danych informacji, a drugi – nie? Zazwyczaj relację wynikania logicznego określa się dla pewnego języka standardowo sformalizowanego, czyli takiego, dla którego został ściśle określony sposób tworzenia wyrażeń w formie skończonych ciągów ustalonych znaków (tj. mamy precyzyjnie podane alfabet i gramatykę). Jest to tzw. *język przedmiotowy*. Określanie wynikania dla takiego języka dokonuje się normalnie w języku bogatszym i mniej sformalizowanym niż przedmiotowy, zwanym *metajęzykiem*.

Główne intuicje dotyczące wynikania logicznego są natury semantycznej. Uważamy, że wniosek wynika logicznie z przesłanek, gdy we wszystkich sytuacjach, w których prawdziwe są przesłanki, prawdziwy jest również ów wniosek. Innymi słowy: nie istnieje sytuacja, w której przesłanki są prawdziwe, a wniosek fałszywy. Dwa pytania, jakie od razu się nasuwają, to: czym jest *sytuacja* oraz co znaczy *być prawdziwym*. Sytuacja, czymkolwiek by nie była, określa wartość prawdziwościową opisującego ją zdania. Technicznie, używamy pojęcia *intepretacji*, która – mówiąc ogólnie – jest sposobem przyporządkowania wartości prawdziwościowych formułom rozważanego języka. Tym, co różni logiki, są pojęcia interpretacji, jakich używają.

Wiedząc z grubsza, czym jest wynikanie logiczne (metajęzykowo oznaczane symbolem $\models$), chcielibyśmy mieć metodę wykazywania, że dany wniosek wynika z przesłanek. Czymś takim jest

Szymon Szymczak
s.szymczak@iphils.uj.edu.pl
student filozofii
Uniwersytet Jagielloński

dobra *relacja dedukowalności* (metajęzykowo oznaczana symbolem $\vdash$). Dedukowalność wniosku z przesłanek ma demonstrować krok po kroku, że ów wniosek wynika z nich logicznie. Procedurę dedukowania formalizujemy, tworząc *system dedukcyjny*, który używając ustalonego zbioru reguł, określa, co liczy się jako dopuszczalny krok w dedukcji. Mówimy, że system dedukcyjny jest *trafny*, gdy wszystko, co da się wydedukować z danych przesłanek, także z nich logicznie wynika. Gdy wszystko, co wynika logicznie z przesłanek, da się też z nich wydedukować, mówimy, że system jest *pełny*. Pokrywanie się syntaktycznej relacji dedukowalności z semantyczną relacją wynikania jest przez logików zawsze pożądane, choć nie zawsze osiągalne.

Najbardziej naturalnymi systemami dedukcyjnymi dla wielu logik są *dedukcja naturalna* i *rachunek sekwentów*. Skupimy się jednak na metodzie drzew semantycznych, i to z kilku powodów. Po pierwsze, budowanie drzew semantycznych – a poprzez to wykazywanie, co wynika, a co nie wynika z danych przesłanek – jest relatywnie proste, w istocie mechaniczne. W przypadku drzew pomysłowe triki mogą pomóc, lecz z pewnością nie są konieczne. Systematycznie stosując reguły, zawsze otrzymamy rezultat, jeśli tylko takowy istnieje. Po drugie, drzewa semantyczne znacznie upraszczają dowody trafności i pełności logik. Ponieważ dowody te są integralną częścią współczesnych badań logicznych, zamieścimy jeden z nich. Po trzecie, drzewa, wbrew powszechnej opinii, formalizują bardzo naturalny sposób rozumowania. Systemy aksjomatyczne wyznaczają zbiór aksjomatów oraz dostarczają reguł inferencyjnych transmitujących prawdziwość. W takim ujęciu wniosek wynika z przesłanek, gdy istnieje „logiczna droga" wyznaczana przez system kolejnymi zastosowaniami jego reguł do zbioru przesłanek i aksjomatów. Drzewa oferują inną strategię. Można by ją nazwać *eksplikacją możliwości*. Aby sprawdzić, czy wniosek wynika z przesłanek, zakładamy, że przesłanki są prawdziwe, a wniosek fałszywy, i badamy, w jakich okolicznościach mogłoby tak być. Jeśli nie ma takich okoliczności – wynikanie zachodzi, jeżeli są – nie.

Przedstawimy dalej zastosowania drzew semantycznych dla pewnej gamy logik zdaniowych: logiki klasycznej, rodziny logik modalnych, logiki intuicjonistycznej i relewantnej. Powodem, dla którego ograniczamy się do logiki zdaniowej, nie jest brak nieklasycznych logik pierwszego rzędu – przykładem jest chociażby logika wolna – ale możliwość opisania fenomenów nieklasyczności już na poziomie zdaniowym.

Naczelna technika semantyczna dla logik nieklasycznych to Kripke'owska *semantyka możliwych światów*. Wszystkie logiki prezentowane w niniejszej pracy mają semantykę tego rodzaju i to ona będzie używana.

2. Drzewa klasyczne

Określmy bliżej język przedmiotowy klasycznej logiki zdań. Jego alfabet $\mathbb{A}$ złożony jest z przeliczalnie nieskończonego zbioru zmiennych zdaniowych $p_1, p_2, p_3 \ldots$ oraz spójników: $\neg$ (negacji), $\wedge$ (koniunkcji), $\vee$ (alternatywy), $\rightarrow$ (implikacji) i $\leftrightarrow$ (równoważności).

Zbiór wyrażeń sensownych (formuł) tego języka składa się ze wszystkich, i tylko nich, ciągów symboli utworzonych rekursywnie ze zmiennych zdaniowych za pomocą następującej reguły:

Jeżeli α i β są formułami, to formułami są także $\neg\alpha$, $(\alpha \vee \beta)$, $(\alpha \wedge \beta)$, $(\alpha \rightarrow \beta)$, $(\alpha \leftrightarrow \beta)$.

Sam język utożsamiamy z tak otrzymanym zbiorem formuł.

Ustalmy użyteczne konwencje. Dla wygody będziemy: po pierwsze, kolejne zmienne zdaniowe oznaczać $p, q, r, \ldots$, po drugie – opuszczać najbardziej zewnętrzne nawiasy formuł. $\alpha, \beta, \gamma, \ldots$ będziemy traktować jako metazmienne przebiegające po formułach języka przedmiotowego, zaś $X, Y, \ldots$ jako zbiory formuł. W przypadku zbiorów skończonych zamiast $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ będziemy pisać po prostu $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Interpretacją stosowną dla naszego języka jest funkcja v, która posyła zbiór zmiennych zdaniowych w dubleton wartości logicznych, tzn. każdej zmiennej zdaniowej przypisuje albo 1 (prawdę), albo 0 (fałsz).

Każdą interpretację da się jednoznacznie rozszerzyć na cały język, czyli do funkcji przypisującej każdej formule pewną wartość logiczną. Rozszerzenie to odbywa się przy pomocy następujących warunków:

$$v(\neg\alpha) = \begin{cases} 1, & \text{gdy } v(\alpha) = 0, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

$$v(\alpha \wedge \beta) = \begin{cases} 1, & \text{gdy } v(\alpha) = v(\beta) = 1, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

$$v(\alpha \vee \beta) = \begin{cases} 1, & \text{gdy } v(\alpha) = 1 \text{ lub } v(\beta) = 1, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

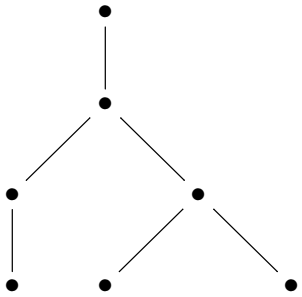
$$v(\alpha \to \beta) = \begin{cases} 1, & \text{gdy } v(\alpha) = 0 \text{ lub } v(\beta) = 1, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

$$v(\alpha \leftrightarrow \beta) = \begin{cases} 1, & \text{gdy } v(\alpha) = v(\beta), \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

Niech X będzie zbiorem formuł (przesłanek). Wówczas α (wniosek) *wynika logicznie* z X ($X \models \alpha$) wtedy i tylko wtedy, gdy nie istnieje interpretacja, przy której wszystkie formuły z X są prawdziwe, a α – fałszywa; inaczej: każda interpretacja, przy której prawdziwe są wszystkie elementy z X, uprawdziwia także α.

Mówimy, że α jest *prawdą logiczną* (*tautologią*) ($\models \alpha$) wtedy i tylko wtedy, gdy wynika logicznie z pustego zbioru przesłanek ($\varnothing \models \alpha$), czyli jest prawdziwa przy każdej interpretacji.

Przejdźmy do drzew semantycznych. *Drzewo* to obiekt, który w przykładowym zarysie wygląda następująco:

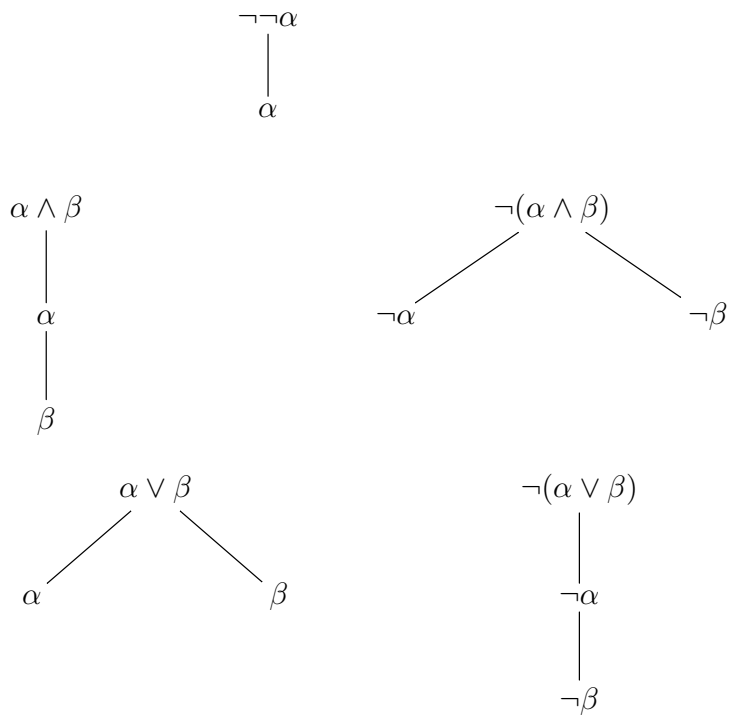


Kropki nazywane są *węzłami*; kropka górna to *korzeń* drzewa, kropki na samym dole to *liście*. Każda ścieżka od korzenia idąca po krawędziach tak daleko, jak tylko może, nazywana jest *gałęzią*.

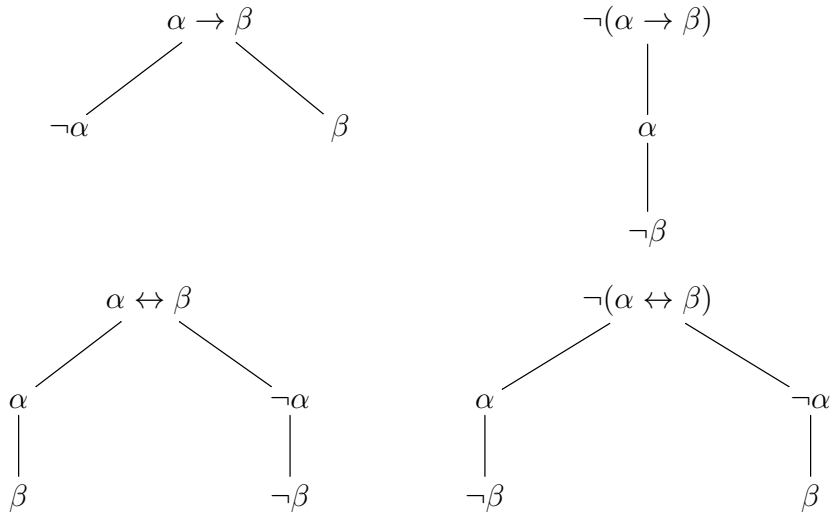
Teoriomnogościowo rzecz ujmując, (skończone) drzewo jest częściowym porządkiem z jedynym elementem maksymalnym a_0, takim że dla każdego elementu a_n istnieje dokładnie jeden skończony łańcuch elementów $a_n \leqslant a_{n-1} \leqslant \cdots \leqslant a_1 \leqslant a_0$[1].

Aby sprawdzić, czy zachodzi wynikanie, konstruujemy drzewo, w którego korzeń wpisujemy wszystkie przesłanki (jeśli są jakieś) i negację wniosku. Będzie to nasza *lista początkowa*. Dalej stosujemy odpowiednie reguły, które pozwalają na rozrastanie się gałęzi.

Z każdym spójnikiem stowarzyszone są pewne reguły. Oto one:



[1] Jeszcze inaczej podchodząc do rzeczy, można powiedzieć, że drzewo jest po prostu *grafem skierowanym*, czyli obiektem matematycznym składającym się ze zbioru wierzchołków i zbioru krawędzi łączących w pary uporządkowane niektóre z tych wierzchołków.



Jaki sens mają takie drzewa? Intuicyjnie: jeżeli stosujemy regułę do formuły prawdziwej (w interpretacji), to prawdziwa będzie także formuła w przynajmniej jednej z gałęzi, którą generuje reguła (oczywiście, czasami może być tylko jedna taka gałąź). Intuicje te mają charakter semantyczny, ale, co istotne, oficjalnie reguły są ściśle syntaktyczne.

Mówimy, że drzewo jest *dojrzałe* wtedy i tylko wtedy, gdy każda reguła możliwa do zastosowania została zastosowana. Ustawicznie stosując reguły, zawsze możemy wyhodować dojrzałe drzewo. W bieżącym przypadku gałęzie dojrzałego drzewa będą skończone; przekonamy się, że w innych przypadkach może tak nie być.

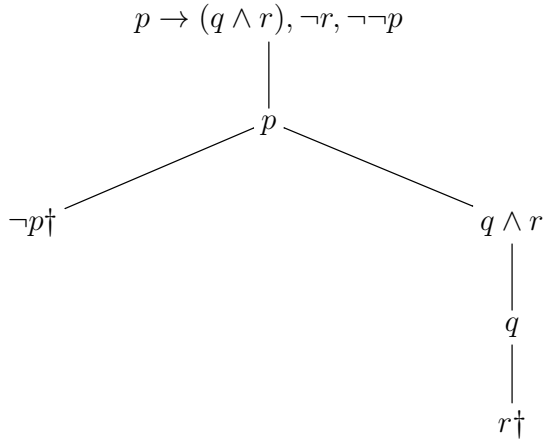
Powiemy, że gałąź jest *uschnięta* wtedy i tylko wtedy, gdy w dwóch jej węzłach występują formuły postaci α i $\neg\alpha$; w przeciwnym wypadku gałąź *żyje*. Gałąź uschniętą oznaczamy symbolem † pisanym przy jej liściu. Drzewo jest *uschnięte* wtedy i tylko wtedy, gdy każda z jego gałęzi jest uschnięta; w przeciwmym wypadku drzewo *żyje*.

Tak opisana procedura konstruowania drzew ma charakter czysto syntaktyczny (kwalifikuje się jako postepowanie teoriodowodowe) i zaprojetowana została z myślą o wykazywaniu, że dany wniosek wynika logicznie z danych przesłanek. Możemy więc potraktować ją jako pewien system dedukcyjny, uznając, że $X \vdash \alpha$ wtedy i tylko wtedy, gdy istnieje dojrzałe uschnięte drzewo, którego lista początkowa składa się ze wszystkich elementów zbioru X oraz negacji α. Będziemy pisać $\vdash \alpha$ w znaczeniu $\varnothing \vdash \alpha$, tj. gdy lista początkowa drzewa składa się wyłącznie z $\neg\alpha$.

Pragmatyka konstruowania drzew podpowiada pewne prawidła, ułatwiające tę czynność:

- Gdy spotykamy sprzeczność w gałęzi, nie ma sensu rozwiajać jej dalej. Wiemy, że gałąź uschnie, cokolwiek by do niej nie dodać.
- Gdy tylko to możliwe, najpierw stosujemy reguły nierozgałęziające. Nie jest to istotne, ale upraszcza drzewa.
- Wygodnie jest „odptaszyć” formułę, do której zastosowano regułę. Widać potem, czego nie trzeba brać już pod uwagę.

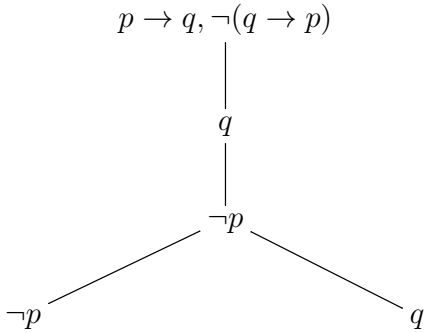
Rozważmy wszystko na przykładzie. Wykażemy, że $p \to (q \wedge r), \neg r \vdash \neg p$. Konstruujemy następujące drzewo.



Trzy formuły w korzeniu to obie przesłanki i negacja wniosku. Następna formuła produkowana jest przez zastosowanie reguły dla podwójnej negacji wobec zanegowanego wniosku. Rozgałęzienie otrzymujemy przez zastosowanie reguły implikacyjnej wobec pierwszej przesłanki. Lewa gałąź od razu usycha (mamy w niej p i $\neg p$), prawa – rozrasta się przez zastosowanie reguły koninkcyjnej wobec formuły $q \wedge p$, po czym i tak usycha, gdyż w gałęzi są r i $\neg r$. Każda z gałęzi drzewa jest uschnięta, a więc całe drzewo usycha, zatem wniosek jest dedukowalny z przesłanek.

Konstruowanie drzew jest w istocie systematycznym poszukiwaniem interpretacji, przy której wszystkie formuły z listy początkowej będą prawdziwe. Każda z żyjących gałęzi dojrzałego drzewa niesie ze sobą taką interpretację. Drzewa są wobec tego dobrym narzędziem do budowania kontrmodeli demonstrujących, że wynikanie nie zachodzi (gdy na liście początkowej są wszystkie przesłanki i negacja wniosku, a dojrzałe drzewo żyje).

Skonstruujmy drzewo wykazujące, że $p \to q \nvdash q \to p$.



Obie gałęzie drzewa żyją. Z każdej z nich możemy odczytać interpretację, przy której prawdziwe są wszystkie formuły z listy początkowej. Recepta jest prosta. Wybieramy żyjącą gałąź. Jeżeli dowolna, ustalona zmienna zdaniowa p występuje w jakimkolwiek węźle tej gałęzi, przypisujemy jej 1; jeżeli w którymkolwiek z jej węzłów występuje $\neg p$, to p przypisujemy 0. (Jeżeli ani p, ani $\neg p$ nie występują w gałęzi, możemy p przypisać jakąkolwiek z wartości logicznych).

W naszym przypadku wybierzmy lewą gałąź. Zgodnie z przepisem otrzymamy interpretację v taką, że $v(p) = 0$, a $v(q) = 1$. Wówczas $v(p \to q) = 1$, a $v(q \to p) = 0$. Przedstawiliśmy *kontrmodel* – interpretację, przy której przesłanki są prawdziwe, a wniosek nie, co upewnia nas, że wynikanie nie zachodzi.

Jak można mieć nadzieję, metoda drzew jest trafna i pełna, co znaczy, że jeżeli X jest kończonym zbiorem formuł[2], to $X \vdash \alpha$ wtedy i tylko wtedy, gdy $X \models \alpha$. Mówi to, że nasza procedura poszukiwawcza naprawdę działa. Jeśli tylko istnieje interpretacja, przy której prawdziwe są wszystkie formuły z listy początkowej, dojrzałe drzewo będzie miało żyjącą gałąź, która ją wyznaczy. Jeśli takiej interpretacji nie ma – każda gałąź uschnie. Fakty te nie są jednak oczywiste i wymagają dowodu, który przeprowadzimy poniżej.

Definicja 1. Niech v będzie interpretacją, a b dowolną gałęzią drzewa. Powiemy, że v *wisi na* b wtedy i tylko wtedy, gdy dla każdej formuły α z tej gałęzi, $v(\alpha) = 1$.

Lemat 2 (o trafności)**.** *Jeżeli v wisi na gałęzi b danego drzewa, a dana reguła została zastosowana w b, to v wisi na przynajmniej jednej z gałęzi wyrosłych.*

Dowód. Dowód przebiega przez kolejne sprawdzenie wszystkich reguł. Rozważmy tylko regułę dla $\to$. Załóżmy, że v wisi na b.

Załóżmy dalej, że $\neg(\alpha \to \beta)$ występuje w b i do niej właśnie stosujemy regułę. Gałąź rośnie, choć się nie rozwidla – w b przybywa o α i $\neg\beta$. Ponieważ v wisi na b, jest tak, że czyni każdą formułę z b prawdziwą. W szczególności $v(\neg(\alpha \to \beta)) = 1$. Zatem $v(\alpha \to \beta) = 0$, a więc $v(\alpha) = 1$, a $v(\beta) = 0$. Stąd $v(\neg\beta) = 1$, czyli v uprawdziwia wszystkie formuły z b.

Załóżmy teraz, że w b występuje $\alpha \to \beta$ i to do niej stosujemy regułę. Wówczas gałąź się rozwidla; w lewe rozwidlenie rozwija b o $\neg\alpha$, prawe – o β. Ponieważ v wisi na b, uprawdziwia każdą formułę z b; w szczególności $v(\alpha \to \beta) = 1$. Mamy wówczas $v(\alpha) = 0$, czyli $v(\neg\alpha) = 1$ lub $v(\beta) = 1$. W pierwszym wypadku v wisi na lewej gałęzi, w drugim – na prawej. Podobnie wykazujemy dla pozostałych spójników. □

Twierdzenie 3 (o trafności)**.** *Dla skończonego X, jeżeli $X \vdash \alpha$, to $X \models \alpha$.*

Dowód. Dowód przeprowadzimy przez kontrapozycję. Załóżmy, że $X \not\models \alpha$. Wykażemy, że $X \not\vdash \alpha$.

Na mocy założenia istnieje interpretacja v, która uprawdziwia każdy element zbioru X, natomiast falsyfikuje α, czyli czyni prawdziwym $\neg\alpha$. Rozważmy dojrzałe drzewo dla $X \vdash \alpha$. Wówczas v wisi na liście początkowej. Zatem na mocy lematu o trafności jakąkolwiek regułę zastosujemy do tej listy, v będzie wisiało na przynajmniej jednej z otrzymanych gałęzi. Stosując wielokrotnie lemat o trafności, otrzymamy całą gałąź b, taką że v wisi na każdej jej początkowej sekcji. Gdyby b była uschnięta, to w pewnej jej początkowej sekcji byłyby formuły postaci β i $\neg\beta$. Ale to jest niemożliwe, bo v wisi także na tej sekcji, czyli $v(\beta) = v(\neg\beta) = 1$, co nie zachodzi. Zatem $X \not\vdash \alpha$. □

[2] Ograniczenie się do skończonych X podyktowanie jest tym, że drzewa zadefiniowaliśmy wyłącznie dla skończonego zbioru przesłanek. Metodę drzew można rozszerzyć na nieskończone zbiory przesłanek – nie wprowadzamy ich wówczas wszystkich na raz i na samym początku, ale kolejno, w regularnych turach, idąc w dół gałęzi. Drzewa takie wciąż mają własność trafności i pełności.

Przejdziemy teraz do dowodu pełności.

Definicja 4. Niech b będzie żyjącą gałęzią drzewa. Interpretacja *niesiona* przez b to dowolna interpretacja v taka, że dla każdej zmiennej zdaniowej p, jeżeli p występuje w jakimś węźle gałęzi b, to $v(p) = 1$, a jeśli $\neg p$ występuje w jakimś węźle gałęzi b, to $v(p) = 0$. (Jeżeli żadna z tych okoliczności nie zachodzi, $v(p)$ może być dowolne). Definicja powyższa jest poprawna, ponieważ b żyje, a więc nie może mieć obu p i $\neg p$.

Lemat 5 (o pełności)**.** *Niech b będzie żyjącą gałęzią dojrzałego drzewa. Niech v będzie interpretacją niesioną prze b. Wówczas:*

(i) *jeżeli α występuje w b, to $v(\alpha) = 1$,*

(ii) *jeżeli $\neg\alpha$ występuje w b, to $v(\alpha) = 0$.*

Dowód. Dowód przebiega przez indukcję z uwagi na stopień skomplikowania formuły α. Jeżeli α jest zmienną zdaniową, wynik zachodzi na mocy definicji. Ze złożonych przypadków rozważmy dwa: taki, w którym α ma postać $\beta \wedge \gamma$, i taki, w którym α to $\neg\beta$.

Załóżmy, że $\beta \wedge \gamma$ występuje w b. Ponieważ drzewo jest dojrzałe, reguła dla $\wedge$ została w b zastosowana. Zatem zarówno β, jak i γ są w tej gałęzi. Na mocy założenia indukcyjnego $v(\beta) = = v(\gamma) = 1$ i stąd $v(\beta \wedge \gamma) = 1$, jak wymagamy. Dalej, załóżmy, że w gałęzi b występuje $\neg(\beta \wedge \gamma)$. Ponieważ zastosowano do niej regułę dla zanegowej koniunkcji, zatem albo $\neg\beta$, albo $\neg\gamma$ są w naszej gałęzi. Na mocy założenia indukcyjnego albo $v(\beta) = 0$, albo $v(\gamma) = 0$. W każdym wypadku $v(\gamma) = 0$, jak wymagamy.

Rozważmy przypadek negacji. Załóżmy, że $\neg\beta$ występuje w b. Wówczas, ponieważ wynik zachodzi dla β, więc $v(\beta) = 0$, a stąd $v(\neg\beta) = 1$. Jeżeli w gałęzi b występuje $\neg\neg\beta$, wówczas jest w niej także β na mocy prawa podwójnej negacji. Na mocy założenia indukcyjnego $v(\beta) = 1$, a wiec $v(\neg\beta) = 0$. □

Twierdzenie 6. *Dla skończonego X, jeżeli $X \models \alpha$, to $X \vdash \alpha$.*

Dowód. Dowód przeprowadzimy przez kontrapozycję. Załóżmy, że $X \nvdash \alpha$. Wykażemy, że $X \not\models \alpha$.

Rozważmy dojrzałe drzewo dla $X \vdash \alpha$ i wybierzmy pewną żywą gałąź. Interpretacja niesiona przez tę gałąź, na mocy lematu o pełności, czyni wszystkie formuły z X prawdziwymi, a α – fałszem. Zatem $X \not\models \alpha$. □

3. Drzewa modalne

Wchodzimy niniejszym na teren *logiki modalnej*. Głównym przedmiotem naszego zainteresowania będzie podstawowa logika modalna K (od Kripkego).

Aletyczna logika modalna dotyczy *trybów* (sposobów), w jakich zadania mogą być prawdziwe/ fałszywe, w szczególności możliwości i konieczności.

Semantyka dla logik modalnych, którą zaprezentujemy, korzysta z pojęcia *możliwego świata*. Od lat toczy się dyskusja na temat tego, czym właściwie są światy możliwe. Nam wystarczą pewne podstawowe intuicje. Łatwo wyobrazić sobie, że sprawy mogłyby potoczyć się inaczej, a rzeczy – być inne. Tym, co sobie w takich wypadkach wyobrażamy, jest inna sytuacja, pewien możliwy świat. Oczywiście świat aktualny jest także światem możliwym, choć oprócz niego istnieje mnóstwo innych.

Kolejne intuicyjne pojęcie, jakie leży u podstaw semantyki możliwych światów, to *możliwość względna*. Otóż, pewne stany rzeczy są możliwe względem pewnych sytuacji (światów), a względem innych – nie. Biorąc na przykład pod uwagę chwilę obecną, możliwe jest, że za tydzień będę jadł kolację z Nicole Kidman w Sydney. Ale biorąc pod uwagę sytuację podobną do obecnej z tą różnicą, że zachodzi za 6 dni i 23 godziny, wspólna kolacja z Nicole Kidman nie będzie już możliwa. Tyle intuicji.

Alfabet języka zdaniowej logiki modalnej jest wzbogaceniem alfabetu logiki klasycznej o dwa spójniki: $\Box$ (pudełko) i $\Diamond$ (diament). $\Box\alpha$ czytamy jako „(jest) konieczne (koniecznie prawdziwe), że α", a $\Diamond\alpha$ – jako „(jest) możliwe (możliwie prawdziwe), że α". Gramatyka jest poszerzeniem klasycznej o regułę: jeżeli α jest formułą, to formułami są także $\Box\alpha$, $\Diamond\alpha$.

Interpretacją stosowną dla tego języka będzie trójka uporządkowana postaci $\langle W, R, v\rangle$. W jest dowolnym niepustym zbiorem przedmiotów, które bierzemy za światy możliwe. $R \subseteq W \times W$ jest binarną relacją na zbiorze możliwych światów. Zatem, gdy $w_1, w_2 \in W$, R może, ale nie musi je wiązać. Jeśli wiąże $(w_1 R w_2)$, mówimy, że świat w_2 jest *osiągalny* ze świata w_1. Intuicyjnie, R jest relacją względnej możliwości, czyli to, że $w_1 R w_2$, znaczy, iż ze względu na w_1 sytuacja w_2 jest możliwa. I w końcu, v jest funkcją przypisującą wartość prawdziwościową (1 lub 0) każdej parze złożonej ze świata w i zmiennej zdaniowej p ($v_w(p) = 1$ lub $v_w(p) = 0$). Nieformalnie odczytujemy to jako „p jest prawdziwe (odpowiednio: fałszywe) w możliwym świecie w"[3].

Funkcję v daną w interpretacji łatwo rozszerzyć na cały język, tzn. sprawić, by przypisywała pewną wartość prawdziwościową każdej formule. Robimy to rekursywnie za pomocą szeregu warunków. Warunki dla spójników prawdziwościowych są takie same jak dla logiki klasycznej, z wyjątkiem relatywizacji względem światów. Zatem dla $\neg$, $\wedge$ i $\vee$ warunki te przybiorą następującą postać. Dla dowolnego $w \in W$:

$$v_w(\neg\alpha) = \begin{cases} 1, & \text{gdy } v_w(\alpha) = 0, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

$$v_w(\alpha \wedge \beta) = \begin{cases} 1, & \text{gdy } v_w(\alpha) = v_w(\beta) = 1, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

$$v_w(\alpha \vee \beta) = \begin{cases} 1, & \text{gdy } v_w(\alpha) = 1 \text{ lub } v_w(\beta) = 1, \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

[3] Możemy nieco upakować notację, co zazwyczaj się robi. Para $\mathcal{F} = \langle W, R\rangle$ będzie stanowiła całość nazywaną *modalną ramą Kripkego*, a nasza interpretacja, nazywa też *modelem na ramie* $\mathcal{F}$, przybierze postać $\mathfrak{M} = \langle \mathcal{F}, v\rangle$.

Innymi słowy, możliwe światy nie odgrywają żadnej roli w określaniu warunków prawdziwościowych dla spójników niemodalnych.

Są natomiast istotne w określaniu warunków prawdziwościowych dla spójników modalnych. Dla dowolnego $w \in W$:

$$v_w(\Diamond\alpha) = \begin{cases} 1, & \text{gdy dla pewnego } w' \in W \text{ takiego, że } wRw', v_{w'}(\alpha) = 1, \\ 0 & \text{w przeciwnym wypadku,} \end{cases}$$

$$v_w(\Box\alpha) = \begin{cases} 1, & \text{gdy dla każdego } w' \in W \text{ takiego, że } wRw', v_{w'}(\alpha) = 1, \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

Swobodnie mówiąc, „możliwe, że α" jest prawdziwe w świecie w, jeżeli α jest prawdziwe w *pewnym* świecie możliwym ze względu na w. Z kolei, „konieczne, że α" jest prawdziwe w świecie w, gdy α jest prawdziwe w *każdym* świecie możliwym ze względu na w.

Zauważmy, że jeśli z w nie jest osiągalny żaden świat, to każda formuła postaci $\Diamond\alpha$ jest w w fałszywa, bo jeżeli z w nie jest osiągalne nic, to tym bardziej świat w którym α jest prawdziwe. Z drugiej strony w omawianym wypadku w świecie w będzie prawdziwe wszystko kształtu $\Box\alpha$, bo jeśli z w nie jest osiągalny żaden świat, to (trywialnie) we wszystkich światach osiągalnych z w formuła α jest prawdziwa.

Pojęcia wynikania logicznego i prawdy logicznej dla logiki modalnej K definiujemy następująco:

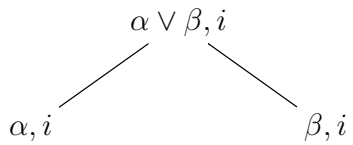
$X \models \alpha$, gdy dla każdej interpretacji $\langle W, R, v\rangle$ i każdego $w \in W$:
jeżeli $v_w(\beta) = 1$ dla każdego $\beta \in X$, to $v_w(\alpha) = 1$,
$\models \alpha$, gdy $\varnothing \models \alpha$, tj. dla każdej interpretacji $\langle W, R, v\rangle$ i każdego $w \in W$, $v_w(\alpha) = 1$.

Drzewa dla K budujemy w sposób bardzo podobny do przypadku logiki klasycznej, z kilkoma modyfikacjami:

(i) W każdym węźle drzewa widnieje albo formuła z pewna liczbą naturalną (α, i), albo układ postaci irj, gdzie i, j to liczby naturalne. Intuicyjnie, różne liczby wskazują na różne światy możliwe. α, i znaczy, że α jest prawdziwa w świecie i, a irj – że świat j jest osiągalny ze świata i.

(ii) Lista początkowa drzewa składa się z $\alpha, 0$ dla każdej przesłanki α (jeśli jakieś istnieją) i $\neg\beta, 0$, gdzie β jest wnioskiem.

(iii) Reguły dla spójników prawdziwościowych pozostają w mocy, z tą różnicą, że liczbę przy formule dziedziczą jej bezpośredni następcy. Tak na przykład reguła dla alternatywy będzie miała postać:



(iv) Reguły dla spójników modalnych są następujące:

$$\begin{array}{cc} \Box\alpha, i \quad irj & \neg\Box\alpha, i \\ \Big| & \Big| \\ \alpha, j & \Diamond\neg\alpha, i \end{array} \qquad \begin{array}{cc} \Diamond\alpha, i & \neg\Diamond\alpha, i \\ \Big| & \Big| \\ irj \quad \alpha, j & \Box\neg\alpha, i \end{array}$$

W regule dla $\Box$ (górna lewa) oba z napisów nad pionową linią muszą być obecne w gałęzi, aby formuła miała zastosowanie; stosuje się ją przy tym dla *każdego* takiego j. W regule dla $\Diamond$ (dolna lewa) liczba j musi być *nowa*, tj. nie może występować gdziekolwiek w gałęzi powyżej.

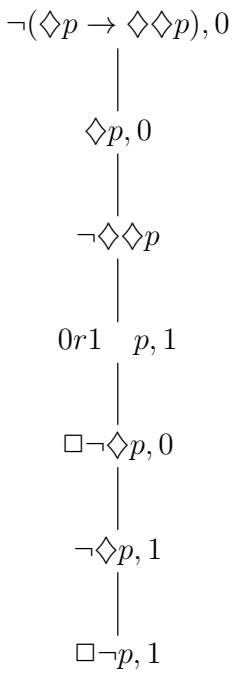
(v) Gałąź usycha wtedy i tylko wtedy, gdy dla pewnej formuły α i liczby naturalnej i zarówno α, i, jak i $\neg\alpha, i$ występują w gałęzi. (W obu przypadkach musi być to samo i).

Oto przykład drzewa wykazującego, że $\vdash \Box\alpha \to \Box(\beta \to \alpha)$.

$$\begin{array}{c} \neg(\Box\alpha \to \Box(\beta \to \alpha)), 0 \\ \Big| \\ \Box\alpha, 0 \\ \Big| \\ \neg\Box(\beta \to \alpha), 0 \\ \Big| \\ \Diamond\neg(\beta \to \alpha), 0 \\ \Big| \\ 0r1 \quad \neg(\beta \to \alpha), 1 \\ \Big| \\ \beta, 1 \\ \Big| \\ \neg\alpha, 1 \\ \Big| \\ \alpha, 1\dagger \end{array}$$

Praktyka wskazuje, że gdy „doptasza" się węzły, by zaznaczyć, że mamy je z głowy, nie powinno się nigdy odznaczać węzłów z formułą postaci $\Box\alpha$, gdyż może się zdarzyć, iż będziemy musieli w pewnej późniejszej fazie znowu ich użyć.

Drzew, oczywiście, możemy też używać do budowania kontrmodeli. Pokażemy, jak przy ich pomocy wykazać, iż $\nvdash \Diamond p \to \Diamond\Diamond p$, i skonstruować stosowny kontrmodel.



Kontrmodel może być łatwo odczytany z żywej gałęzi. Dla każdej liczby i występującej w gałęzi istnieje świat w_i. w_iRw_j, gdy irj występuje w gałęzi. Dla każdej zmienne zdaniowej, jeżeli p, i jest w gałęzi, to $v_{w_i}(p) = 1$, jeżeli natomiast w gałęzi jest $\neg p, i$, to $v_{w_i}(p) = 0$ (jeśli nie zachodzi żadne z nich, to $v_{w_i}(p)$ może być dowolne).

Nasz kontrmodel będzie prosty: $W = \{w_0, w_1\}$, w_0Rw_1 i $v_{w_1}(p) = 1$. Używając warunków prawdziwości, możemy bezpośrednio sprawdzić, że ta interpretacja działa – poprzednik rozważanej implikacji jest w niej prawdziwy, a następnik – fałszywy. Ponieważ p jest prawdziwe w w_1, a w_1 jest osiągalny z w_0, zatem w tym ostatnim prawdziwe jest $\Diamond p$. Ponieważ z w_1 nic nie jest osiągalne, każda formuła postaci $\Diamond\alpha$ będzie w nim fałszywa, a zatem i $\Diamond\Diamond p$. Nasza interpretacja falsyfikuje daną implikację.

Istnieje wiele systemów logiki modalnej. Najważniejszą klasą logik modalnych jest klasa logik *normalnych*[4]. Podstawową modalną logiką normalną jest omówiona wyżej logika K. Inne logiki normalne otrzymujemy, nakładając dodatkowe ograniczenia na relację osiągalności R. Ważniejsze

[4] Modalne logiki *nienormalne* to takie, które w W oprócz światów normalnych mają też światy *nienormalne* – wszystko w nich jest możliwe i nic nie jest konieczne. Logiki tego typu są słabsze niż K.

z tych restrykcji to:

ρ zwrotność – dla każdego w: wRw,

σ symetryczność – dla każdych w_1, w_2: jeżeli w_1Rw_2, to w_2Rw_1,

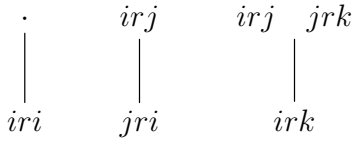
τ przechodniość – dla każdych w_1, w_2, w_3: jeżeli w_1Rw_2 i w_2Rw_3, to w_1Rw_2.

Interpretację, której R spełnia warunek ρ, nazwiemy *ρ-interpretacją*. Jako K_ρ oznaczymy logikę definiowaną w terminach zachowania prawdziwości we wszystkich światach wszystkich ρ--interpretacji. Wynikanie $\models_{K_\rho}$ definiujemy następująco: $X \models_{K_\rho} \alpha$ wtedy i tylko wtedy, gdy dla każdego $w \in W$, jeżeli $v_w(\beta) = 1$ dla każdego $\beta \in X$, to $v_w(\alpha) = 1$. Podobnie dla σ i τ.

Warunki ograniczające R mogą być łączone. Historycznie rzecz ujmując, systemy K_ρ, $K_{\rho\sigma}$, $K_{\rho\tau}$ i $K_{\rho\sigma\tau}$ znane są jako T, B, $S4$ i $S5$ odpowiednio.

Drzewa dla K łatwo adaptuje się do innych systemów. Robimy to za pomocą dodatkowych reguł, które wprowadzają do gałęzi informacje o r. Ponieważ informacje te są brane pod uwagę przy zastosowaniach reguły dla $\Box$, w efekcie rośnie liczba zastosowań tejże reguły.

Reguły dla ρ, σ i τ to odpowiednio:



Reguła dla ρ mówi, że jeżeli i jest liczbą naturalną z drzewa, to wpisujemy iri. Stosuje się ją od razu do świata 0 z listy początkowej i zawsze po wprowadzeniu nowej liczby naturalnej. Dwie pozostałe reguły są jasne.

W systemach „złożonych" stosowanie reguł komplikuje się, więc dla wygody dobrze przyjąć ułatwiającą procedurę. Nowe światy normalnie wprowadzamy przy pomocy $\diamondsuit$-reguły. Stosujemy ją jako pierwszą. Potem ustalamy wszystko o r, co powinno być dodane, i dodajemy to. Na koniec stosujemy $\Box$-regułę, gdy tylko nowe fakty o r tego wymagają.

Zamkniemy sekcję uwagą o systemie $K_{\rho\sigma\tau}$, znanym jako $S5$. Okazuje sie, że przy takim złożeniu warunków nałożonych na R wszystko jest osiągalne ze wszystkiego – dla każdego w_1, w_2, w_1Rw_2. Wówczas R przestaje się w interpretacji całkowicie liczyć; interpretacja przybiera postać $\langle W, v\rangle$, a warunek prawdziwości dla $\Box$ upraszcza się do: $v_w(\Box\alpha) = 1$ wtedy i tylko wtedy, gdy dla każdego $w' \in W$, $v_w(\alpha) = 1$, i podobnie dla $\diamondsuit$.

Drzewa stają się wtedy nadzwyczaj proste: nigdy nie wspomina się r. Stosując $\diamondsuit$-regułę do $\diamondsuit\alpha, i$, dostajemy nowy węzeł postaci α, j (gdzie j jest nowe); natomiast stosując $\Box$-regułę do $\Box\alpha, i$, dodajemy do gałęzi α, j dla każdego j.

W przypadku drzew dla wszystkich wspomnianych logik modalnych, stanowią one trafną i pełną procedurę dedukcyjną względem odpowiadających sobie semantyk.

4. Drzewa intuicjonistyczne

Logika intuicjonistyczna pierwotnie wyrosła z pewnej filozoficznej wizji matematyki zwanej *intuicjonizmem*.

Faktem jest, że potrafimy zrozumieć nieograniczoną ilość nigdy wcześniej nie słyszanych zdań. Nasuwa się pytanie: jak to możliwe? Jedna z koncepcji mówi, że rozumiemy zdania, gdyż rozumiemy ich części składowe oraz sposób złożenia; znaczenie zdania określane jest przez znaczenie jego części oraz gramatyczną konstrukcję, która je składa w całość. Zjawisko to określa się jako *składalność*.

Ortodoksyjnym poglądem, przypisywanym Fregemu, jest twierdzenie, że znaczenie zdania dane jest przez warunki, w których jest ono prawdziwe, czyli jego *warunki prawdziwości*. Dalej, na mocy składalności, warunki prawdziwości zdania muszą być dane w terminach warunków prawdziwości jego komponentów. Dla przykładu $\neg\alpha$ jest prawdziwe wtedy i tylko wtedy, gdy α nie jest prawdziwe, $\alpha \wedge \beta$ jest prawdziwe wtedy i tylko wtedy, gdy α jest prawdziwe i β jest prawdziwe itp.

Prawdę z kolei traktuje się zazwyczaj jako pewien szczególny związek między językiem a rzeczywistością pozajęzykową. Zdanie „Nicole Kidman ma męża" jest prawdziwe na mocy pewnego obiektywnego stanu rzeczy. Ale wielu uważa pojęcie obiektywnej, pozajęzykowej rzeczywistości za bardzo problematyczne – dla matematyki w szczególności.

Jaka pozajęzykowa rzeczywistość miałaby odpowiadać prawdom rodzaju $2+3 = 5$? Niektórzy (*realiści*) sugerują, że istnieją obiektywnie przedmioty matematyczne takie jak liczba 3 czy 5. Inni zaprzeczają temu poglądowi. Wśród nich są intuicjoniści, którzy odrzucili zwyczajową koncepcję prawdy w odniesieniu do matematyki z tego właśnie powodu.

Jak zatem w takim przypadku określane jest znaczenie zdania? Według intuicjonistów znaczenie zdania dane jest nie przez warunki, w których jest ono prawdziwe, przy czym prawdziwość pojmuje się jako związek z zewnętrzną rzeczywistością, ale przez warunki, w których jest *dowiedzione*, czyli *warunki dowodliwości*, przy czym dowód jest pewną mentalną konstrukcją specjalnego rodzaju.

Przyjrzyjmy się temu bliżej. Załóżmy, że wiemy, co liczy się jako dowód najprostszych formuł (zmiennych zdaniowych). Wówczas warunki dowiedlności dla formuł zbudowanych przy użyciu spójników zdaniowych będą następujące:

- dowodem $\alpha \wedge \beta$ jest para złożona z dowodu α i dowodu β,
- dowodem $\alpha \vee \beta$ jest dowód α lub dowód β,
- dowodem $\neg\alpha$ jest dowód, że nie ma dowodu α,
- dowodem $\alpha \to \beta$ jest konstrukcja przekształcająca dowolny dowód α w dowód β.

Zauważmy, że warunki te nie gwarantują zachodzenia wielu standardowych praw logicznych – w szczególności prawa wyłączonego środka: $\alpha \vee \neg\alpha$. Na przykład: niech α będzie *hipotezą bliźniaczych liczb pierwszych* (istnieje nieskończona liczba par liczb pierwszych, takich że druga z pary

jest większa o 2 od pierwszej, jak 3 i 5, 11 i 13, 29 i 33). Jest to hipoteza obecnie nierozstrzygnięta. Na dzisiaj nie istnieje dowód α, nie istnieje też dowód, że nie ma dowodu α. Zatem nie istnieje dowód $\alpha \vee \neg\alpha$, co za tym idzie, prawo to jest nie do zaakceptowania. Jak widać, intuicjonizm generuje całkiem inną logikę.

Aby lepiej zrozumieć logikę intuicjonistyczną, przyjrzyjmy się odpowiadającej jej semantycd możliwych światów, która lepiej oddaje powyższe idee.

Intuicjonistyczna interpretacja stosowna dla języka tej logiki to trójka uporządkowana postaci $\langle W, R, v\rangle$, podobna do interpretacji normalnej logiki modalnej $K_{\rho\tau}$ (czyli R jest zwrotna i przechodnia), z tą różnicą, że nałożony jest na nią jeszcze jeden warunek, mianowicie dla każdej zmiennej zdaniowej p:

$$\text{Dla każdego } w \in W, \text{ jeżeli } v_w(p) = 1, \text{ a } wRw', \text{ to } v_{w'}(p) = 1.$$

Warunek ten nazywany jest *warunkiem dziedziczenia*.

Przyporządkowanie wartości logicznych formułom molekularnym jest dane przez następujące warunki:

$$\begin{aligned}
v_w(\alpha \wedge \beta) = 1 \quad &\text{wtedy i tylko wtedy, gdy} \quad v_w(\alpha) = v_w(\beta) = 1,\\
v_w(\alpha \vee \beta) = 1 \quad &\text{wtedy i tylko wtedy, gdy} \quad v_w(\alpha) = 1 \text{ lub } v_w(\beta) = 1,\\
v_w(\neg\alpha) = 1 \quad &\text{wtedy i tylko wtedy, gdy} \quad \text{dla każdego } w' \text{ takiego, że } wRw', v_{w'}(\alpha) = 0,\\
v_w(\alpha \to \beta) = 1 \quad &\text{wtedy i tylko wtedy, gdy} \quad \text{dla każdego } w' \text{ takiego, że } wRw',\\
&\qquad\qquad\qquad\qquad\quad \text{albo } v_{w'}(\alpha) = 0, \text{ albo } v_{w'}(\beta) = 1.
\end{aligned}$$

Zauważmy, że nasze $\neg\alpha$ jest tym samym, co $\Box\neg\alpha$, a nasze $\alpha \to \beta$ – tym samym, co $\Box(\alpha \to \beta)$.

Przy tak zadanych warunkach prawdziwościowych warunek dziedziczenia zachodzi nie tylko dla zmiennych zdaniowych, ale dla wszystkich formuł.

Zastanówmy się, w jaki sposób powyższa interpretacja oddaje wyrażone uprzednio nieformalne idee. Myślmy o światach jako o stanach wiedzy w danym czasie; mówiąc swobodnie, prawdziwe w nich jest to, co zostało na tę chwilę udowodnione. w_1Rw_2 znaczy, że stan wiedzy w_2 jest możliwym rozszerzeniem w_1, otrzymanym przez odkrycie pewnej liczby (być może 0) nowych dowodów. Przy takim rozumieniu R musi być zwrotna i przechodnia. Warunek dziedziczenia także jest jasny: jeśli coś zostało dowiedzione, to pozostaje dowiedzione, czegokolwiek innego byśmy nie dowiedli.

W obliczu warunków dowodliwości, rekursywne warunki powyżej wydają się naturalne. $\alpha \wedge \beta$ jest dowiedzione w danej chwili wtedy i tylko wtedy, gdy α jest dowiedzione w tej chwili i β jest dowiedzione w tej chwili; $\alpha \vee \beta$ jest dowiedzione w danej chwili wtedy i tylko wtedy, gdy α jest dowiedzione w tej chwili lub β jest dowiedzione w tej chwili. Jeżeli $\neg\alpha$ jest dowiedzione w danym czasie, to mamy dowód, że nie ma dowodu α. Zatem α nie będzie dowiedzione w żadnej z chwil późniejszych. Jeżeli $\neg\alpha$ nie jest dowiedzione w danej chwili, to przynajmniej możliwe jest, że dowód α kiedyś się pojawi, więc α będzie prawdziwe w pewnej chwili w przyszłości. W końcu, jeżeli $\alpha \to \beta$ jest dowiedzione w danym czasie, to dysponujemy konstrukcją, która dowolny dowód α przekształca w dowód β. Zatem w każdej przyszłej chwili albo nie ma dowodu

α, albo, jeśli jest, to daje nam dowód β. Jeżeli $\alpha \to \beta$ nie jest dowiedzione w danej chwili, to jest co najmniej możliwe, że w pewnej chwili w przyszłości α zostanie dowiedzione, a β – nie, tj. α będzie prawdziwe w tym czasie, a β – nie.

Pojęcie wynikania logicznego ($\models_I$) definiujemy w zwyczajny sposób jako zachowanie prawdy we wszystkich światach wszystkich interpretacji.

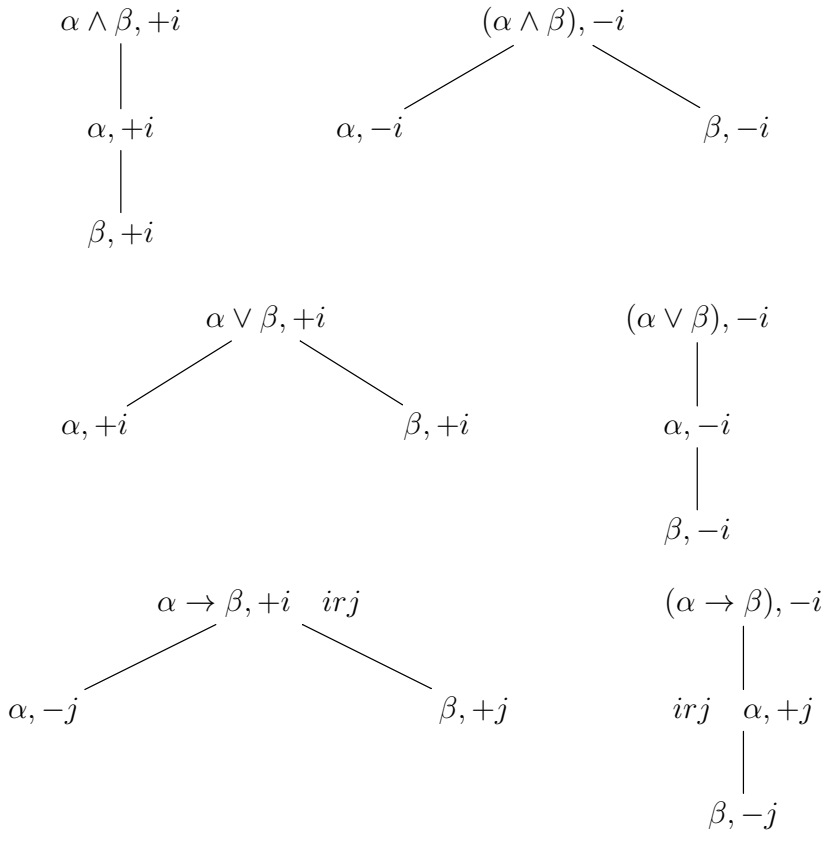
Drzewa dla logiki intuicjonistycznej uzyskujemy, dokonując pewnych modyfikacji w drzewach modalnych:

(i) Węzeł drzewa będzie miał teraz postać $\alpha, +i$ lub $\alpha, -i$. Intuicyjnie, pierwsze mówi, że α jest prawdziwe w świecie i, drugie – że α jest w i fałszywe. Dla logik modalnych fałszywość α w i była wskazywana przez $\neg\alpha, i$. Teraz musi być inaczej, bo α może być fałszywe w danym świecie, nawet jeśli $\neg\alpha$ nie jest tam prawdziwe.

(ii) Lista początkowa drzewa składa się z $\alpha, +0$ dla każdej przesłanki (jeśli są jakieś) oraz $\beta, -0$, gdzie β jest wnioskiem.

(iii) Gałąź usycha, gdy występują w niej węzły postaci $\alpha, +i$ i $\alpha, -i$.

(iv) Reguły dla spójników są następujące:



$$\dfrac{\neg\alpha, +i \quad irj}{\alpha, -j} \qquad \dfrac{\neg\alpha, -i}{irj \quad \alpha, +j} \qquad \dfrac{p, +i \quad irj}{p, +j}$$

Reguły dla $\wedge$ i $\vee$ są jasne. Pierwsza reguła dla $\to$ i $\neg$ stosuje się do każdego j w gałęzi. W drugiej – w obu przypadkach – j jest nowe. Reguły te łatwiej zapamiętać, gdy uświadomimy sobie, że $\alpha \to \beta$ to $\Box(\alpha \to \beta)$, natomiast $\neg\alpha$ to $\Box\neg\alpha$. Zauważmy, że nigdy nie możemy „odptaszyć" węzła postaci $\alpha \to \beta, +i$ lub $\neg\alpha, +i$, ponieważ być może będziemy musieli do nich wrócić i zastosować ponownie stosowną regułę, gdy tylko pojawi się napis postaci irj. Ostatnia reguła ma zastosowanie wyłącznie do zmiennych zdaniowych i każdego j (różnego od i). Regułę tę wymusza warunek dziedziczenia. Zauważmy, że nie ma analogicznej reguły dla $p, -i$.

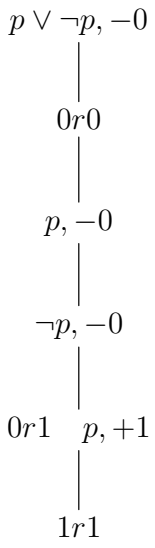
(v) Mamy też reguły dla ρ i τ, jako wymagane przez warunek zwrotności i przechodniości R.

Rozważmy drzewo wykazujące, że $\vdash_I p \to \neg\neg p$.

$$\begin{array}{c} p \to \neg\neg p, -0 \\ | \\ 0r0 \\ | \\ 0r1 \quad p, +1 \\ | \\ \neg\neg p, -1 \\ | \\ 1r1 \\ | \\ 1r2 \quad \neg p, +2 \\ | \\ 2r2 \\ | \\ 0r2 \\ | \\ p, -2 \\ | \\ p, +2\dagger \end{array}$$

Węzły 3 i 4 otrzymujemy z 1 dzięki zastosowaniu reguły dla fałszywej $\rightarrow$; 6 – stosując do 4 regułę dla fałszywej $\neg$; 9 – aplikując do 6 i 7 regułę dla prawdziwej $\neg$, a 10 – działając na 3 regułą dziedziczenia (wobec $1r2$). Węzły 2, 5, 7, 8 są efektem zastosowania reguł dla zwrotności i przechodniości.

Poniższe drzewo zademonstruje nam, że $\nvdash_I p \vee \neg p$, oraz pomoże konstruować kontrmodel.



Węzły 3 i 4 dostajemy, stosując do 1 regułę dla fałszywej $\rightarrow$; 5 – stosując do 4 regułę dla fałszywej $\neg$, a 2 i 6 – na mocy reguły dla zwrotności.

Kontrmodel odczytujemy z żywej gałęzi dojrzałego drzewa w następujący sposób. Światy i relacja osiągalności są takie, jakie wyznacza gałąź. Jeżeli węzeł postaci $p, +i$ występuje w gałęzi, to p traktujemy jako prawdziwe w świecie w_i, w przeciwnym wypadku p jest w w_i fałszywe. (W szczególności, gdy w gałęzi jest węzeł postaci $p, -i$, to ustalamy, że p jest w w_i fałszywe).

Z naszego drzewa odczytujemy:

$$W = \{w_0, w_1\},$$

$$w_0 R w_0,$$

$$w_1 R w_1,$$

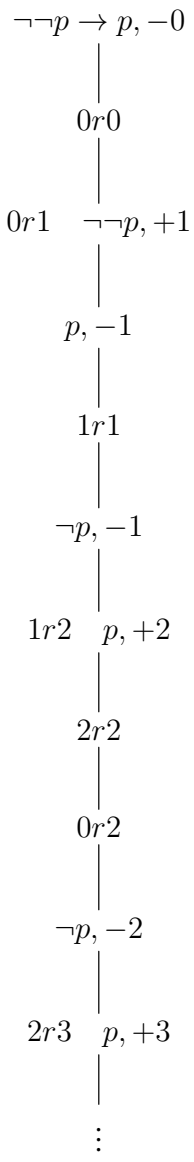
$$w_0 R w_1,$$

$$v_{w_0}(p) = 0,$$

$$v_{w_1}(p) = 1.$$

p jest w w_1 fałszywe; ponieważ w_0 jest osiągalne z w_1, a w w_1 p jest prawdziwe, zatem w w_0 fałszywe musi być $\neg p$. A zatem w w_0 fałszywe jest $p \vee \neg p$.

Żywe drzewo dla logiki intuicjonistycznej może być nieskończone. Ilustruje to poniższy przykład dla $\nvdash_I \neg\neg p \to p$:



Kiedykolwiek wprowadzamy nowy świat i, trzeci węzeł (i przechodniość) wymagają, by wpisać $\neg p, -i$. To z kolei zmusza nas do wprowadzenia kolejnego nowego świata j takiego, że irj i $p, +j$ itd.

W takich wypadkach wygodniej konstruować kontrmodele bezpośrednio. Dla $\neg\neg p \to p$ następujący będzie odpowiedni: $W = \{w_0, w_1\}$, w_0Rw_0, w_1Rw_1, w_0Rw_1, $v_{w_0}(p) = 0$, $v_{w_1}(p) = 1$. Ponieważ p jest prawdziwe w w_1, więc $\neg p$ jest fałszywe w w_0 i w_1. Zatem $\neg\neg p$ jest prawdziwe w w_0. A ponieważ p jest tam fałszywe, więc $\neg\neg p \to p$ jest w w_0 fałszywe.

Zaprezentowane drzewa są trafną i pełną procedurą dedukcyjną względem opisanej semantyki.

5. Drzewa relewantne

Wielu logików tautologie rodzaju $\vdash (p \wedge \neg p) \rightarrow q$ traktuje z wyjątkową niechęcią ze względu na brak związku między poprzednikiem a następnikiem. To rozczarowanie doprowadziło do powstania rodziny logik *relewantnych*, które biorą pod uwagę zaniedbywane dotąd związki istotności. Choć w ogólności semantyki dla logik relewantnych są dość skomplikowane, semantyka dla *pociągania pierwszego stopnia* (*PPS*) – systemu, w którym rozważa się tylko formuły postaci $\alpha \rightarrow \beta$, gdzie α i β nie zawierają implikacji – da się przedstawić w zaskakująco prostej formie.

W klasycznej logice zdań interpretacja to funkcja ze zbioru formuł w wartości logiczne 1 i 0. W ujęciu takim przyjmuje się, że każda formuła jest albo prawdziwa, albo fałszywa; nigdy natomiast ani prawdziwa, ani fałszywa czy prawdziwa i fałszywa zarazem.

Istnieją poważne powody, by wątpić w to założenie[5]. Jeśli żywi się takie wątpliwości, to naturalnym jest traktować interpretację nie jako funkcję, lecz jako relację między formułami a wartościami prawdziwościowymi. A zatem formuła może się wiązać z 1, może z 0, może z oboma, albo z żadnym.

Zauważmy, że istotne jest byśmy wyraźnie rozróżniali między fałszywością w interpretacji a niebyciem prawdziwym w interpretacji. (Takiej różnicy nie ma w logice klasyczniej). Fakt, że formuła jest fałszywa (wiąże się z 0), nie znaczy, że jest nieprawdziwa (może przecież wiązać się z 1). Z kolei fakt, że formuła jest nieprawdziwa (nie wiąże się z 1), nie przesądza, że jest fałszywa (bo może nie wiązać się też z 0).

W PPS interpretacja to relacja v między zmiennymi zdaniowymi a wartościami 1 i 0 ($v \subseteq Z \times \{1, 0\}$, gdzie Z to zbiór zmiennych zdaniowych). $pv1$ znaczy, że p wiąże się z 1, natomiast $pv0$ – że p wiąże się z 0.

Daną w ten sposób interpretację v rozszerzamy do relacji między *wszystkimi* formułami a wartościami prawdziwościowymi przy pomocy następujących warunków:

$$
\begin{array}{lll}
\alpha \wedge \beta v1 & \text{wtedy i tylko wtedy, gdy} & \alpha v1 \text{ i } \beta v1, \\
\alpha \wedge \beta v0 & \text{wtedy i tylko wtedy, gdy} & \alpha v0 \text{ lub } \beta v0, \\
 & & \\
\alpha \vee \beta v1 & \text{wtedy i tylko wtedy, gdy} & \alpha v1 \text{ lub } \beta v1, \\
\alpha \vee \beta v0 & \text{wtedy i tylko wtedy, gdy} & \alpha v0 \text{ i } \beta v0, \\
 & & \\
\neg \alpha v1 & \text{wtedy i tylko wtedy, gdy} & \alpha v0, \\
\neg \alpha v0 & \text{wtedy i tylko wtedy, gdy} & \alpha v1.
\end{array}
$$

Zauważmy, że są to w zasadzie warunki prawdziwościowe jak dla logiki klasycznej, pozbawione tylko założenia, że podział na prawdę i fałsz jest rozłączny i wyczerpujący. Zatem koniunkcja jest prawdziwa w interpretacji, gdy oba jej człony są w niej prawdziwe, jest fałszywa – jeśli przynajmniej jeden z członów jest fałszywy itp.

[5] Chodzi tu o *zlepki prawdziwościowe* – formuły zarazem prawdziwe i fałszywe (np. sprzeczne prawa czy paradoksalne formuły samoodnoszące się), a także o *luki prawdziwościowe* – zdania ani prawdziwe, ani fałszywe (np. formuły z defektem denotacyjnym czy przygodne zdania o przyszłości).

Aby zobaczyć, jak te warunki działają, rozważmy formułę $\neg p \wedge (q \vee r)$. Niech $pv1$, $pv0$, $qv1$ i $rv0$, a v nie wiąże żadnych innych zmiennych z wartościami prawdziwościowymi. Ponieważ p jest prawdziwe, zatem $\neg p$ jest fałszywe; a ponieważ p jest fałszywe, więc $\neg p$ jest prawdziwe. Zatem $\neg p$ jest zarazem prawdziwe i fałszywe. Ponieważ q jest prawdziwe, $q \vee r$ jest także prawdziwe, a ponieważ q nie jest fałszywe, więc $q \vee r$ też nie będzie fałszywe. Zatem $q \vee r$ jest po prostu prawdziwe. Wówczas $\neg p \wedge (q \vee r)$ jest prawdziwe, bo oba człony są prawdziwe, i jest też fałszywe, bo pierwszy człon jest fałszywy. Ostatecznie: $\neg p \wedge (q \vee r)v1$ i $\neg p \wedge (q \vee r)v0$.

Wynikanie logiczne dla PPS definiujemy, jak zazwyczaj, w kategoriach zachowywania prawdy:

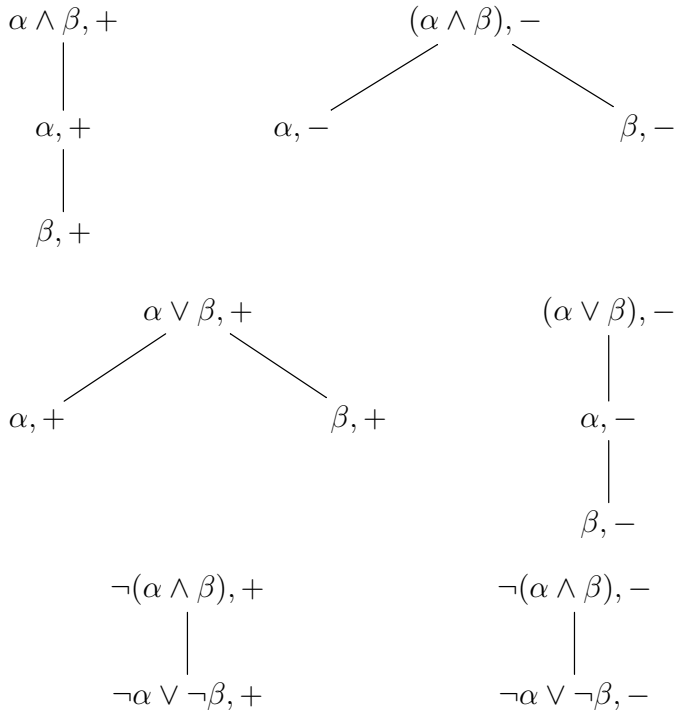
$$\begin{array}{rll} X \models \alpha & \text{wtedy i tylko wtedy, gdy} & \text{dla każdej interpretacji } v\text{:} \\ & & \text{jeżeli } \beta v1 \text{ dla każdego } \beta \in X\text{, to } \alpha v1, \\ \models \alpha & \text{wtedy i tylko wtedy, gdy} & \varnothing \models \alpha\text{, tj. dla każdej } v\text{, } \alpha v1. \end{array}$$

Drzewa dla PPS otrzymujemy, modyfikując przypadek klasyczny w następujący sposób:

(i) Każdy węzeł drzewa ma teraz postać $\alpha, +$ lub $\alpha, -$. Intuicyjnie, $\alpha, +$ znaczy, że α jest prawdziwe, a $\alpha, -$ znaczy, że α nie jest prawdziwe . Tak jak w logice intuicjonistycznej, $\neg\alpha, +$ nie znaczy tego samego, co $\alpha, -$.

(ii) Lista początkowa składa się z $\alpha, +$ dla każdej z przesłanek (jeśli są jakieś) oraz $\beta, -$, gdzie β jest wnioskiem.

(iii) Reguły konstrukcyjne drzew dla PPS są następujące:



$$\begin{array}{c} \neg(\alpha \vee \beta), + \\ | \\ \neg\alpha \wedge \neg\beta, + \\ \neg\neg\alpha, + \\ | \\ \alpha, + \end{array} \qquad \begin{array}{c} \neg(\alpha \vee \beta), - \\ | \\ \neg\alpha \wedge \neg\beta, - \\ \neg\neg\alpha, - \\ | \\ \alpha, - \end{array}$$

Dwie pierwsze reguły są jasne: jeżeli $\alpha \wedge \beta$ jest prawdziwe, to prawdziwe są α i β; jeśli $\alpha \wedge \beta$ nie jest prawdziwe, to nie jest prawdziwy jeden z jej członów. Podobnie w przypadku reguły dla alternatywy. Pozostałe reguły też są łatwe do zapamiętania, bo $\neg(\alpha \wedge \beta)$ i $\neg\alpha \vee \neg\beta$ mają w PPS te same wartości prawdziwościowe, podobnie zresztą jak $\neg(\alpha \vee \beta)$ i $\neg\alpha \wedge \neg\beta$ oraz $\neg\neg\alpha$ i α.

(iv) Gałąź drzewa usycha, jeśli zawiera węzły postaci $\alpha, +$ i $\alpha, -$.

Rozważmy proste drzewo wykazujące, iż $\alpha \vdash \alpha \vee \beta$.

$$\begin{array}{cc} \alpha, + & \alpha \vee \beta, - \\ & | \\ & \alpha, - \\ & | \\ & \beta, -\dagger \end{array}$$

Zastosowaliśmy powyżej tylko regułę dla nieprawdziwej alternatywy względem wniosku z korzenia.

Poniższe drzewo zademonstruje, że PPS nie jest logiką *wybuchową*, czyli nie zachodzi w niej prawo przepełnienia $p \wedge \neg p \nvdash_{\text{PPS}} q$.

$$\begin{array}{cc} p \wedge \neg p, + & q, - \\ & | \\ & p, + \\ & | \\ & \neg p, + \end{array}$$

Kontrmodel odczytujemy z żywej gałęzi dojrzałego drzewa w prosty sposób. Dla każdej zmiennej zdaniowej p: jeżeli jest w tej gałęzi węzeł postaci $p, +$, kładziemy $pv1$; jeżeli jest tam węzeł kształtu $\neg p, +$, kładziemy $pv0$. Żadne inne fakty dotyczące v nie zachodzą.

W naszym wypadku interpretacja v niesiona przez żywą gałąź jest taka, że $pv1$ i $pv0$. Łatwo sprawdzić, że v czyni przesłankę prawdziwą, a wniosek nieprawdziwym.

Metoda drzew dla PPS jest trafną i pełną procedurą dowodową ze względu na przedstawioną wyżej semantykę.

6. Podsumowanie

Przeprowadzony powyżej przegląd zastosowań techniki drzew sematycznych pokazuje, jak użytecznym, plastycznym i wygodnym są narzędziem.

Od strony praktycznej drzewa pozwalają bardzo sprawnie testować dedukowalność, czego nie można powiedzieć o systemach aksjomatycznych. Każda formuła, którą dodajemy do gałęzi, pochodzi od formuły już tam istniejącej. Zazwyczaj mamy wybór formuły, do której będziemy aplikowanić odpowiednią dla niej regułę, ale zawsze liczba takich możliwych wyborów jest skończona. W systemie aksjomatycznym, zwykle wyposażonym w regułę odrywania, aby wyprowadzić β, musimy znaleźć takie α, że α oraz $\alpha \rightarrow \beta$ są wyprowadzalne. Kandydatów na takie α jest nieskończenie wiele. Jeśli budując drzewa, dokonujemy mądrych wyborów, nie tylko się nam udaje (jeśli jest szansa powodzenia), ale z reguły dzieje się tak z łatwością. Stąd drzewa są jakby stworzone do poszukiwania dedukcji. Natomiast o tym, jak upraszczają metateoretyczne dowody pełności i trafności, przekonaliśmy się na przykładzie logiki klasycznej.

Drzewa będą z pewnością wzrastać dla wielu innych logik, zapewne dlatego, że o wiele łatwiej jest nimi operować niż aparatami teoriodowodowymi w innych formalizacjach.

Literatura

[1] D. Bostock, *Intermediate Logic*, Oxford University Press, Oxford 1997.

[2] A. D'Agostino, D. M. Gabbay, R. Hähnle, J. Possega (eds.), *Handbook of Taleau Methods*, Kluwer Academic Publishers, Dordrecht 1999.

[3] C. Howson, *Logic with Trees*, Routledge, London 1996.

[4] G. Priest, *An Introduction to Non-Classical Logic*, Cambridge University Press, Cambridge 2001.

[5] G. Restall, *Logic. An Introduction*, Routledge, New York 2006.

On substructural weakenings of classical logic

Andrzej Wroński

Special features of substructural logics are best seen through their Gentzen-style formalizations. The classical calculus **LK** of Gentzen uses so called *sequents* which are expressions of the form $\Gamma \vdash \Delta$ where Γ and Δ are finite (possibly empty) lists (i.e. sequences) of formulas of the considered language and the symbol $\vdash$ denotes the relation of logical consequence. The intended interpretation of $\Gamma \vdash \Delta$ is the following: *the disjunction of the whole list Δ is a logical consequence of the conjunction of the whole list Γ*. The conjunction and disjunction of an empty list are understood as sentential constants: *verum* and *falsum*, respectively. Here, we shall modify axioms and inference rules of **LK** in an inessential way in order to make explicit each structural rule to be used.

The *axioms* of **LK** are all sequents of the form:

$$\Delta \vdash \Delta\,, \quad \text{where } \Delta \text{ is a nonempty list.}$$

The *structural inference rules* of **LK** are the following:

$$\frac{\Gamma_1, \alpha, \alpha, \Gamma_2 \vdash \Delta}{\Gamma_1, \alpha, \Gamma_2 \vdash \Delta}\ \textit{contraction left} \qquad \frac{\Gamma \vdash \Delta_1, \alpha, \alpha, \Delta_2}{\Gamma \vdash \Delta_1, \alpha, \Delta_2}\ \textit{contraction right}$$

$$\frac{\Gamma_1, \alpha, \beta, \Gamma_2 \vdash \Delta}{\Gamma_1, \beta, \alpha, \Gamma_2 \vdash \Delta}\ \textit{exchange left} \qquad \frac{\Gamma \vdash \Delta_1, \alpha, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \beta, \alpha, \Delta_2}\ \textit{exchange right}$$

$$\frac{\Gamma_1, \Gamma_2 \vdash \Delta}{\Gamma_1, \alpha, \Gamma_2 \vdash \Delta}\ \textit{weakening left} \qquad \frac{\Gamma \vdash \Delta_1, \Delta_2}{\Gamma \vdash \Delta_1, \alpha, \Delta_2}\ \textit{weakening right}$$

prof. dr hab. Andrzej Wroński
andrzej.wronski@uj.edu.pl
Instytut Filozofii
Uniwersytet Jagielloński

Roughly speaking, *contraction*, *exchange* and *weakening* facilitate treating any list of formulas in a sequent as if it were a set – multiple occurrences of a given formula in a list can be reduced to a single occurrence and additionally, commuting or repeating formulas occurring in a list is allowed.

The *logical inference rules* of **LK** are simple, elegant and well known:

$$\frac{\Gamma \vdash \Delta, \alpha}{\neg\alpha, \Gamma \vdash \Delta}\ (\neg\ \textit{left}) \qquad \frac{\alpha, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg\alpha}\ (\neg\ \textit{right})$$

$$\frac{\alpha, \beta, \Gamma \vdash \Delta}{\alpha \wedge \beta, \Gamma \vdash \Delta}\ (\wedge\ \textit{left}) \qquad \frac{\Gamma_1 \vdash \Delta_1, \alpha \qquad \Gamma_2 \vdash \Delta_2, \beta}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, \alpha \wedge \beta}\ (\wedge\ \textit{right})$$

$$\frac{\alpha, \Gamma_1 \vdash \Delta_1 \qquad \beta, \Gamma_2 \vdash \Delta_2}{\alpha \vee \beta, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\vee\ \textit{left}) \qquad \frac{\Gamma \vdash \Delta, \alpha, \beta}{\Gamma \vdash \Delta, \alpha \vee \beta}\ (\vee\ \textit{right})$$

$$\frac{\Gamma_1 \vdash \Delta_1, \alpha \qquad \beta, \Gamma_2 \vdash \Delta_2}{\alpha \to \beta, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\to\ \textit{left}) \qquad \frac{\alpha, \Gamma \vdash \Delta, \beta}{\Gamma \vdash \Delta, \alpha \to \beta}\ (\to\ \textit{right})$$

$$\frac{\alpha(t), \Gamma \vdash \Delta}{\forall_x\, \alpha, \Gamma \vdash \Delta}\ (\forall\ \textit{left}) \qquad \frac{\Gamma \vdash \Delta, \alpha(x)}{\Gamma \vdash \Delta, \forall_y\, \alpha(y)}\ [\forall\ \textit{right}]$$

$$\frac{\alpha(x), \Gamma \vdash \Delta}{\exists_y\, \alpha(y), \Gamma \vdash \Delta}\ [\exists\ \textit{left}] \qquad \frac{\Gamma \vdash \Delta, \alpha(t)}{\Gamma \vdash \Delta, \exists_x\, \alpha}\ (\exists\ \textit{right})$$

Formal systems appropriate for substructural logics are obtained by tampering with structural rules of ordinary Gentzen systems. Thus, Gentzen-style calculi without the weakening rule correspond to so called *relevant logics*, where sequents with superfluous premises or a redundant information in conclusion sell badly (see [1, 2]).

If we remove weakening and contraction leaving only the rule of exchange then the resulting system will be a version of so called *linear logic* of Girard (see [3]), which is of interest to logicians as well as computer scientists.

The lack of the contraction rule causes a sort of *resource-sensitivity* – it matters how many times a given premise occurs in a sequent. Thus, in a contractionless logic we are no longer allowed to treat the list of premises of a sequent as if it were a set. However, if the rule of exchange is present then the list of premises still can be treated as a multiset of formulas.

A good source of knowledge on various algebraic aspects of substructural logic is a new book

of N. Galatos, P. Jipsen, T. Kowalski and H. Ono [4].

The following remarkable fact has been noted in 1960 by Hao Wang:

Theorem 1. *The first-order system* **LK** *with the contraction rule removed becomes decidable* (see p. 4 in H. Wang [5] or p. 228 in [6]).

Note a sharp contrast with a famous result of A. Church [7], that the first order logic in a language with any predicate symbol which is more then unary must be undecidable.

There is, however, a price to pay for resource-sensitivity and decidability of contractionless logic – the common idempotence laws for $\wedge$ and $\vee$ do not hold because the sequents: $\alpha \vdash \alpha \wedge \alpha$ and $\alpha \vee \alpha \vdash \alpha$ are unprovable.

An algebraic counterpart of the classical propositional logic is the well known variety of Boolean algebras. In the case of contractionless logic, the appropriate structure is an intriguing class of all algebras $\mathfrak{A} = \langle A, \odot, \oplus, ^{\perp}, \mathbf{0}, \mathbf{1}\rangle$ satisfying the following conditions:

(A1)	$x \odot y = y \odot x$	(B1)	$x \oplus y = y \oplus x$
(A2)	$x \odot (y \odot z) = (x \odot y) \odot z$	(B2)	$x \oplus (y \oplus z) = (x \oplus y) \oplus z$
(A3)	$x \odot \mathbf{1} = x$	(B3)	$x \oplus \mathbf{0} = x$
(A4)	$x \odot \mathbf{0} = \mathbf{0}$	(B4)	$x \oplus \mathbf{1} = \mathbf{1}$
(A5)	$x \odot x^{\perp} = \mathbf{0}$	(B5)	$x \oplus x^{\perp} = \mathbf{1}$
(A6)	$(x \odot y)^{\perp} = (x^{\perp} \oplus y^{\perp})$	(B6)	$(x \oplus y)^{\perp} = (x^{\perp} \odot y^{\perp})$
(C1)	$x^{\perp\perp} = x$		
(C2)	if $x \odot y = \mathbf{0}$ and $x \oplus y = \mathbf{1}$	then	$x = y^{\perp}$
(C3)	if $x \oplus y = \mathbf{1}$ and $y^{\perp} \oplus z = \mathbf{1}$	then	$x \oplus z = \mathbf{1}$

The above class of algebras was isolated by V. N. Grišin in [8], where it was characterized in a different manner. The present characterization has been chosen because of its outstanding simplicity and clear connections with Boolean algebras. It is easy to verify that any Grišin algebra can be partially ordered by the relation $\leq$ defined in a familiar way: $x \leq y$ iff $x^{\perp} \oplus y = \mathbf{1}$, and the following conditions hold:

(D1) $x \odot (y \oplus z) \leq (x \odot y) \oplus z$

(D2) If $v \leq x$ and $w \leq y$ then $v \odot w \leq x \odot y$ and $v \oplus w \leq x \oplus y$

Since 1983 we know that the class of Grišin algebras is not closed under homomorphic images (see Krzystek [9]) and thus, it is not a variety. Now the question arises how to characterize the smallest variety containing all Grišin algebras and we have a problem:

Problem 2. *Axiomatize the set of all identities of Grišin algebras. Is it finitely axiomatizable?*

To simplify our problem even more let us observe that instead of Grišin algebras, one can consider term-equivalent structures of type $\langle 2, 0\rangle$. For any Grišin algebra $\mathfrak{A} = \langle A, \odot, \oplus, ^{\perp}, \mathbf{0}, \mathbf{1}\rangle$ we put $\overline{\mathfrak{A}} = \langle A, \rightarrow, \mathbf{0}\rangle$, where $a \rightarrow b := a^{\perp} \oplus b$, for $a, b \in A$. The operation $\rightarrow$ is an algebraic counterpart of the implication connective of contractionless logic in terms of which one can recover operations of the Grišin algebra $\mathfrak{A}$ putting for $a, b \in A$:

$$a^{\perp} := a \rightarrow \mathbf{0}, \;\; a \oplus b := a^{\perp} \rightarrow b, \;\; a \odot b := (a \rightarrow b^{\perp})^{\perp} \text{ and } \mathbf{1} := \mathbf{0} \rightarrow \mathbf{0}$$

Using the abbreviation $\mathbf{1} := \mathbf{0} \to \mathbf{0}$ one can characterize Grišin algebras in terms of $\to$ and $\mathbf{0}$ in the following simple manner:

Fact 3. *A structure $\mathfrak{A} = \langle A, \to, \mathbf{0}\rangle$ is a term-equivalent form of a Grišin algebra iff the following conditions hold:*

(B) $(x \to y) \to ((z \to x) \to (z \to y)) = \mathbf{1}$

(C) $x \to (y \to z) = y \to (x \to z)$

(K) $x \to (y \to x) = \mathbf{1}$

(Z_1) $(x \to \mathbf{0}) \to \mathbf{0} = x$

(Z_2) $\mathbf{0} \to x = \mathbf{1}$

(!!) *If* $x \to y = \mathbf{1} = y \to x$ *then* $x = y$

We are particularly interested in the quasivariety generated by purely implicational reducts of Grišin algebras which can be characterized as the class of all structures $\langle A, \to, \mathbf{1}\rangle$ satisfying the conditions (B),(C),(K) and (!!) above. This is the well known class of so called BCK-algebras, whose enigmatic name is justified by the fact that implicational terms in the defining equations are types of the combinators B, C and K dictated by the Curry-Howard correspondence (see [10, 11]). Now our problem can be reformulated as follows:

Problem 4. *Axiomatize the set all identities of* BCK*-algebras. Is it finitely axiomatizable?*

Note that BCK-algebras verify the identities from the following list:

(1) $\mathbf{1} \to x = x$,

(2) $x \to (y \to z) = ((x \to (y \to z)) \to z) \to z$.

(3) $x \to (y \to z) = y \to (x \to z)$.

Moreover, we can generalize (2) and (3) in the following manner:

(4) $x_0 \to (x_1 \to (\cdots (x_n \to z) \cdots)) = ((x_0 \to (x_1 \to (\cdots (x_n \to z) \cdots))) \to z) \to z$,

(5) $x_0 \to (x_1 \to (\cdots (x_n \to z) \cdots)) = x_{f_0} \to (x_{f_1} \to (\cdots (x_{f_n} \to z) \cdots))$, for any permutation f of $\{0, \ldots, n\}$.

The identity (5) allows us to treat antecedents of the operation $\to$ as a multiset and thus, the expression of the form $\Gamma \to b$ can be safely used to abbreviate any expression of the form

$$a_0 \to (a_1 \to (\cdots (a_n \to b) \cdots))$$

where Γ is a multiset of all antecedents $a_0, \ldots, a_n$. Now, the identity (4) can be written simply as:

$$\Gamma \to z = ((\Gamma \to z) \to z) \to z.$$

Let us consider a certain variety $\mathbb{H}$ – to be further thought of as a possible candidate for $\mathsf{H}(\mathrm{BCK})$. We define $\mathbb{H}$ as the variety determined by the following identities:

(i) $(x \to y) \to ((z \to x) \to (z \to y)) = \mathbf{1}$,

(ii) $x \to \mathbf{1} = \mathbf{1}$,

(iii) $\mathbf{1} \to x = x$,

(iv) $x \to (y \to z) = y \to (x \to z)$,

(v) $x \to (y \to z) = ((x \to (y \to z)) \to z) \to z$.

Note that the defining identities of $\mathbb{H}$ hold in BCK-algebras which means that $\mathbb{H} \supseteq \mathsf{H}(\mathrm{BCK})$. Moreover, an easy induction proves that the important generalized BCK-identities (4) and (5) hold in $\mathbb{H}$ and we have the following:

Fact 5. $\mathbb{H}$ *and* BCK *verify the same identities of the form:* $\varphi = \mathbf{1}$.

Indeed, let v be a one-to-one mapping of variables occurring in a term φ into the set of free generators of an algebra $\mathfrak{F} = \langle F, \to_{\mathfrak{F}}, \mathbf{1}_{\mathfrak{F}} \rangle$ being a free member of $\mathbb{H}$. Define a relation

$$\eta := \left\{ \langle a, b \rangle \in F^2 \ : \ a \to_{\mathfrak{F}} b = \mathbf{1}_{\mathfrak{F}} = b \to_{\mathfrak{F}} a \right\}$$

and observe that $\eta \in \mathsf{Cg}(\mathfrak{F}),\ \mathfrak{F}/\eta \in \mathrm{BCK},\ \mathbf{1}_{\mathfrak{F}}/\eta = \{\mathbf{1}_{\mathfrak{F}}\}$. Now, supposing that $\mathfrak{F}/\eta \models \varphi = \mathbf{1}$ one gets that $v(\varphi)/\eta = \mathbf{1}_{\mathfrak{F}}/\eta$ and finally $v(\varphi) = \mathbf{1}_{\mathfrak{F}}$ which clearly means that $\mathbb{H} \models \varphi = \mathbf{1}$.

The fact above implies that the result of Nagayama [12] concerning BCK-identities carries over to the variety $\mathbb{H}$ i.e. we have:

Fact 6. *If* $\mathbb{H} \models \Gamma \to x = \Delta \to y$ *where* $x,\ y$ *are distinct variables then*

$$\mathbb{H} \models \Gamma \to x = \mathbf{1} = \Delta \to y.$$

Thus, all what is needed to solve our problem by proving that $\mathbb{H} = \mathsf{H}(\mathrm{BCK})$ is a verification of the following:

Conjecture 7. *If* $\mathbb{H} \models (\Gamma \to x) \to (\Delta \to x) = \mathbf{1} = (\Delta \to x) \to (\Gamma \to x)$ *then*

$$\mathbb{H} \models \Gamma \to x = \Delta \to x.$$

References

[1] A. R. Anderson, N. D. Belnap, *Entailment: The Logic of Relevance and Necessity* Volume I, Princeton University Press, Princeton 1975.

[2] A. R. Anderson, N. D. Belnap, J. M. Dunn, *Entailment: The Logic of Relevance and Necessity* Volume II, Princeton University Press, Princeton 1992.

[3] J.-Y. Girard, *Linear Logic*, "Theoretical Computer Science", 50 (1987), p. 1–102.

[4] N. Galatos, P. Jipsen, T. Kowalski, H. Ono, *Residuated Lattices: An Algebraic Glimpse at Substructural Logics*, Elsevier 2007.

[5] H. Wang, *Toward Mechanical Mathematics*, "IBM journal for research and development", 4 (1960), p. 2–22.

[6] H. Wang, *A Survey of Mathematical Logic*, Science Press and North-Holland Publishing, Peking and Amsterdam 1963.

[7] A. Church, *A note on Entscheidungsproblem*, "The Journal of Symbolic Logic", 1 (1936), p. 40–41.

[8] V. N. Grišin, *On algebraic semantics for logic without the contraction rule*, Moskva 1976.

[9] P. S. Krzystek, *O algebrach pre-Boole'owskich*, Uniwersytet Jagielloński 1983.

[10] H. B. Curry, R. Feys, *Combinatory Logic*, vol. I, North-Holland, Amsterdam 1958.

[11] W. Howard, *The formulae-as-types notion of construction*, Academic Press, Boston 1980.

[12] M. Nagayama, *On a property of BCK-identities*, "Studia Logica", 53 (1994), p. 227–234.

Zbiory rozmyte i logika rozmyta

Hanna Zdanowicz

Streszczenie. Logika rozmyta jest uogólnieniem klasycznej logiki dwuwartościowej i jest ściśle powiązana z teorią zbiorów rozmytych. W przypadku logiki rozmytej pomiędzy stanami 1 (prawda) i 0 (fałsz) znajdują się stany pośrednie określające stopień przynależności do zbioru. Taki sposób rozumowania zbliżony jest do naturalnego sposobu myślenia i może być stosowany, gdy mamy do czynienia z nieprecyzyjnymi warunkami lub niejednoznaczną odpowiedzią. Logika rozmyta znalazła szereg zastosowań w inżynierii i ekonomii, w szczególności do oceny klientów bankowych.

1. Zbiory rozmyte i logika rozmyta

W klasycznym podejściu do logiki występują dwa możliwe stany: prawda lub fałsz i każdemu zdaniu logicznemu przypisuje się jedną z tych dwóch wartości. Dzięki zastosowaniu logiki rozmytej możliwe jest wprowadzenie wartości ułamkowych, rozmycie granic między stanami prawda-fałsz oraz określenie stanów takich jak „częściowo prawda" lub „prawie fałsz". Z zagadnieniem logiki rozmytej nieodłącznie wiąże się zagadnienie zbiorów rozmytych.

Teoria zbiorów rozmytych została wprowadzona w 1965 r. przez Lotfi A. Zadeha jako uogólnienie klasycznej teorii zbiorów. Cechą charakterystyczną zbioru rozmytego jest fukcja przynależności, określająca, w jakim stopniu rozważany element należy do zbioru.

Definicja 1. *Zbiorem rozmytym* A w niepustej przestrzeni X nazywamy zbiór

$$\{(x, \mu_A(x)) : x \in X)\},$$

gdzie A jest zbiorem i $\mu_A \colon A \to [0, 1]$ jest funkcją przynależności do zbioru A.

Definicja 2. Dla każdego $x \in A$ wielkość $\mu_A(x)$ nazywa się *stopniem przynależności elementu* x *do zbioru rozmytego* (A, μ_A).

Hanna Zdanowicz
hania.z@poczta.fm
studentka matematyki, informatyki i ekonometrii
Uniwersytet Łódzki

Definicja 3. Niech $x \in A$. Wówczas mówimy, że

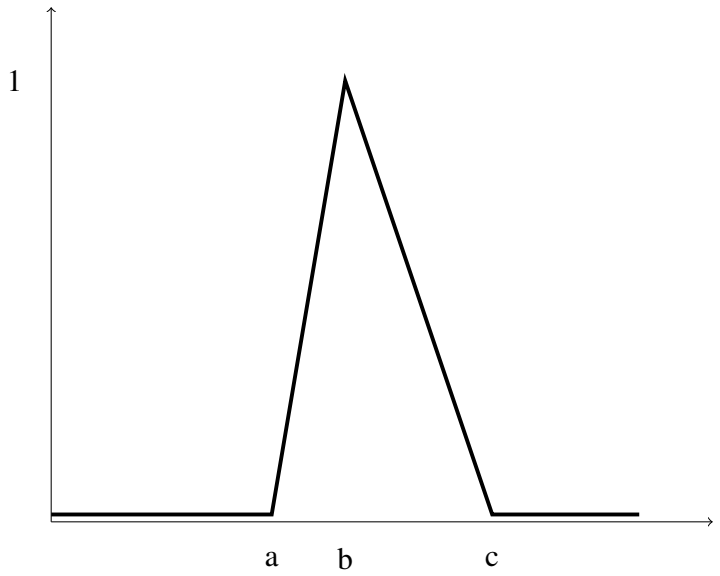
- x *nie należy do* A, jeśli $\mu_A(x) = 0$,
- x *całkowicie należy do* A, jeśli $\mu_A(x) = 1$,
- x *częściowo należy do* A, jeśli $0 < \mu_A(x) < 1$.

Funkcje przynależności mogą mieć różne postaci. Najczęściej stosowane są funkcje trójkątne, trapezowe i S-funkcje, których nazwy pochodzą od kształtu wykresu funkcji.

Funkcje trójkątne definiowane są przy pomocy trzech parametrów a, b, c, przy czym $a < b < c$, i opisane są ogólnym wzorem

$$\mu_A(x) = \begin{cases} 0, & \text{gdy } x < a, \\ \frac{x-a}{b-a}, & \text{gdy } a \leq x < b, \\ \frac{c-x}{c-b}, & \text{gdy } b \leq x < c, \\ 0, & \text{gdy } x \geq c. \end{cases}$$

Rysunek 1. Trójkątna funkcja przynależności

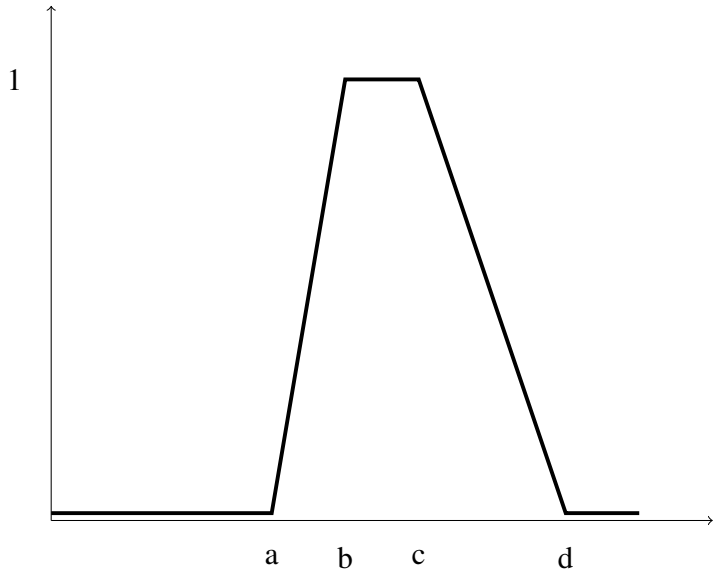


Źródło: Opracowanie własne.

Funkcje trapezowe definiowane są przy pomocy czterech parametrów a, b, c, d, przy czym $a < b < c < d$, i opisane są ogólnym wzorem

$$\mu_A(x) = \begin{cases} 0, & \text{gdy } x < a, \\ \frac{x-a}{b-a}, & \text{gdy } a \leq x < b, \\ 1, & \text{gdy } b \leq x < c, \\ \frac{d-x}{d-c}, & \text{gdy } c \leq x < d, \\ 0, & \text{gdy } x \geq d. \end{cases}$$

Rysunek 2. Trapezowa funkcja przynależności



Źródło: Opracowanie własne.

S-funkcja (albo funkcja klasy S) opisana jest dwoma parametrami a, b, przy czym $a < b$, i jest postaci

$$\mu_A(x) = \begin{cases} 0, & \text{gdy } x < a, \\ 2\left(\frac{x-a}{b-a}\right)^2, & \text{gdy } a \leq x < \frac{b-a}{2}, \\ 1 - 2\left(\frac{x-a}{b-a}\right)^2, & \text{gdy } \frac{b-a}{2} \leq x < b, \\ 1, & \text{gdy } x \geq b. \end{cases}$$

Przykład 4. Niech X będzie zbiorem wszystkich ludzi. Rozważmy podzbiór osób wysokich. W przypadku klasycznego podejścia należałoby okreslić graniczny wzrost, powyżej którego osoby można określić jako wysokie. Załóżmy, że ten graniczny wzrost został ustalony na poziomie 180 cm. Wobec tego każda z osób ze zbioru X, która ma powyżej 180 cm wzrostu, jest określana

jako wysoka. Co jednak z osobą, która mierzy 1,79 cm? Zgodnie z przyjętym kryterium musi zostać ona zakwalifikowana jako osoba niska, jednak intuicyjnie wydaje się, że bliżej jej do zbioru osób wysokich niż niskich. W tym przypadku z pomocą przychodzi teoria zbiorów rozmytych. Niech $w(x)$ oznacza wzrost osoby x.

Rozważmy funkcję przynależności postaci

$$\mu_A(x) = \begin{cases} 0, & \text{gdy } w(x) < 170, \\ \frac{w(x)-170}{20}, & \text{gdy } 170 \leq w(x) < 190, \\ 1, & \text{gdy } w(x) \geq 190. \end{cases}$$

Dla tak zdefiniowanej funkcji przynależności można okreslić stopień przynależności poszczególnych osób do zbioru osób wysokich. Takie przyporządkowanie przedstawione jest w poniższej tablicy.

Tablica 1. Przynależność do zbioru osób wysokich

wzrost	stopień przynależności
160	0
180	0,5
190	1
165	0
175	0,25
195	1
185	0,75

Źródło: opracowanie własne.

Natomiast graficznie opisaną powyżej fukcję przynależności można przedstawić tak jak na rysunku 3.

Analogicznie można rozważać rozmyte zbiory osób młodych lub bogatych, ale także można w ten sposób wyodrębnić zbiór liczb „równych około 10” (rysunek 4).

Podobnie jak dla klasycznej teorii zbiorów, w przypadku zbiorów rozmytych można mówić o sumie zbiorów, ich iloczynie oraz dopełnieniu zbioru, jednakże te operacje są bardziej skomplikowane.

Definicja 5. Funkcję T dwóch zmiennych

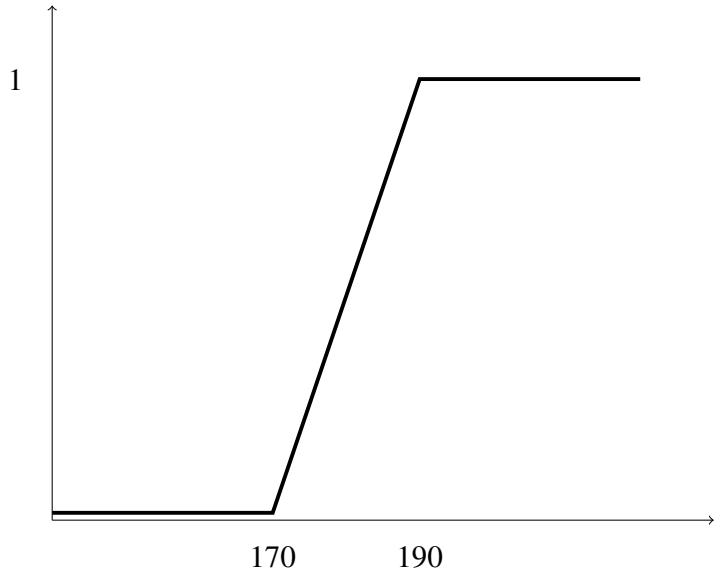
$$T\colon [0,1] \times [0,1] \to [0,1]$$

nazywamy *T-normą*, jeżeli:

(i) jest nierosnąca względem obu argumentów:

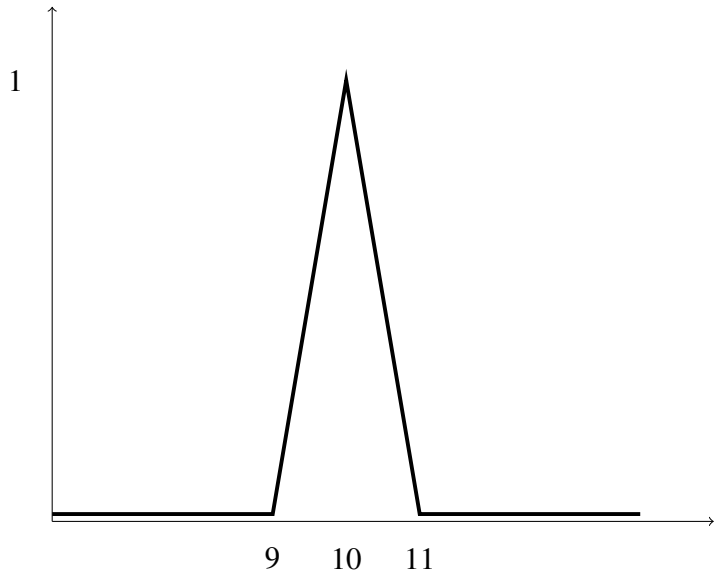
$$T(a,c) \leq T(b,d) \quad \text{dla } a \leq b \text{ i } c \leq d,$$

Rysunek 3. Funkcja przynależności do zbioru osób wysokich



Źródło: Opracowanie własne.

Rysunek 4. Funkcja przynależności do zbioru liczb równych około 10



Źródło: Opracowanie własne.

(ii) spełnia warunek przemienności:

$$T(a,b) = T(b,a),$$

(iii) spełnia warunek łączności:

$$T(T(a,b),c) = T(a,T(b,c)),$$

(iv) spełnia warunki brzegowe:

$$T(a,0) = 0, \quad T(a,1) = a,$$

gdzie $a, b, c, d \in [0,1]$.

Przykładowe T-normy przedstawione są w poniższej tablicy.

Tablica 2. Przykładowe T-normy

Nazwa	Wzór $\mu_{A\cap B}(x)$
minimum	$\min(\mu_A(x), \mu_B(x))$
iloczyn	$\mu_A(x) \cdot \mu_B(x)$
iloczyn Hamachera	$\dfrac{\mu_A(x) \cdot \mu_B(x)}{\mu_A(x) + \mu_B(x) - \mu_A(x) \cdot \mu_B(x)}$
iloczyn Einsteina	$\dfrac{\mu_A(x) \cdot \mu_B(x)}{2 - (\mu_A(x) + \mu_B(x) - \mu_A(x) \cdot \mu_B(x))}$
iloczyn drastyczny	$\begin{cases} \min(\mu_A(x), \mu_B(x)), & \text{gdy } \max(\mu_A(x), \mu_B(x)) = 1 \\ 0 & \text{w przeciwnym wypadku} \end{cases}$
ograniczona różnica	$\max(0, \mu_A(x) + \mu_B(x) - 1)$

Definicja 6. Funkcję S dwóch zmiennych

$$S\colon [0,1] \times [0,1] \to [0,1]$$

nazywamy *S-normą*, jeżeli:

(i) jest nierosnąca względem obu argumentów:

$$S(a,c) \leq S(b,d) \quad \text{dla } a \leq b \text{ i } c \leq d,$$

(ii) spełnia warunek przemienności:

$$S(a,b) = S(b,a),$$

(iii) spełnia warunek łączności:

$$S(S(a,b),c) = S(a,S(b,c)),$$

(iv) spełnia warunki brzegowe:

$$S(a,0) = a, \quad S(a,1) = 1,$$

gdzie $a, b, c, d \in [0,1]$.

Przykładowe S-normy przedstawione są w poniższej tablicy.

Tablica 3. Przykładowe S-normy

Nazwa	Wzór $\mu_{A\cup B}(x)$
maksimum	$\max(\mu_A(x), \mu_B(x))$
suma algebraiczna	$\mu_A(x) + \mu_B(x) - \mu_A(x) \cdot \mu_B(x)$
suma Hamachera	$\dfrac{\mu_A(x) + \mu_B(x) - 2\mu_A(x) \cdot \mu_B(x)}{1 - \mu_A(x) \cdot \mu_B(x)}$
suma Einsteina	$\dfrac{\mu_A(x) + \mu_B(x)}{1 + \mu_A(x) \cdot \mu_B(x)}$
suma drastyczna	$\begin{cases} \max(\mu_A(x), \mu_B(x)), & \text{gdy } \min(\mu_A(x), \mu_B(x)) = 0 \\ 0 & \text{w przeciwnym wypadku} \end{cases}$
suma ograniczona	$\min(1, \mu_A(x) + \mu_B(x))$

Dla tak określonych T-norm oraz S-norm można zdefiniować iloczyn oraz sumę zbiorów rozmytych.

Definicja 7. *Iloczynem* $A \cap B$ zbiorów rozmytych A i B w niepustej przestrzeni X nazywamy zbiór uporządkowanych par

$$\{(x, \mu_{A\cap B}(x)) \colon x \in X)\},$$

gdzie funkcja przynależności do zbioru $A \cap B$ dana jest wzorem

$$\mu_{A\cap B}(x) = T(\mu_A(x), \mu_B(x))$$

i T jest T-normą.

Sumą $A \cap B$ zbiorów rozmytych A i B w niepustej przestrzeni X nazywamy zbiór uporządkowanych par

$$\{(x, \mu_{A\cup B}(x)) \colon x \in X)\},$$

gdzie funkcja przynależności do zbioru $A \cup B$ dana jest wzorem

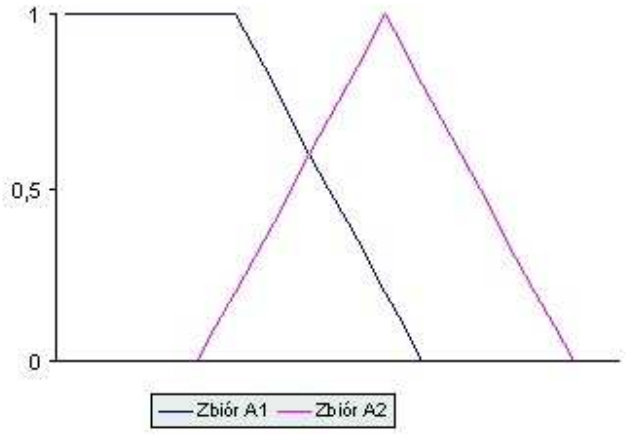
$$\mu_{A\cup B}(x) = S(\mu_A(x), \mu_B(x))$$

i S jest S-normą.

Rozpatrzmy następujący przykład.

Przykład 8. Rozważmy zbiory rozmyte przedstawione na poniższym rysunku.

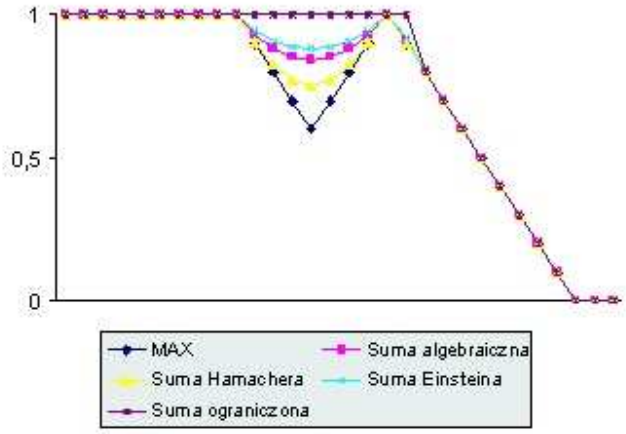
Rysunek 5. Przykładowe zbiory rozmyte A_1, A_2.



Źródło: `www.isep.pw.edu.pl/ZakladNapedu/dyplomy/fuzzy/podstawy_FL.htm`.

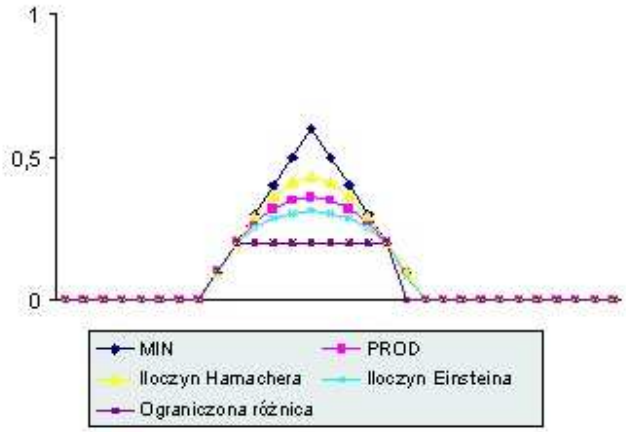
Sumy i iloczyny zbiorów A_1 oraz A_2 znajdują się na rysunkach 6 oraz 7.

Rysunek 6. Suma zbiorów A_1 i A_2.



Źródło: `www.isep.pw.edu.pl/ZakladNapedu/dyplomy/fuzzy/podstawy_FL.htm`.

Rysunek 7. Iloczyn zbiorów rozmytych A_1 i A_2.



Źródło: `www.isep.pw.edu.pl/ZakladNapedu/dyplomy/fuzzy/podstawy_FL.htm`.

Oprócz sumy i iloczynu, można również rozważać dopełnienia zbiorów rozmytych.

Definicja 9. Dopełnieniem zbioru rozmytego A w przestrzeni X nazywamy zbiór rozmyty A' o funkcji przynależności danej wzorem

$$\mu_{A'} = 1 - \mu_A.$$

2. Zastosowanie w bankowości

Metoda k-średnich jest jedną z metod analizy skupień wykorzystywanych do pozyskiwania wiedzy, a dokładniej do eksploracji danych. Cechą charakterystyczną tej metody jest wybór liczby zgrupowań przed rozpoczęciem procedury przydzielania obiektów do skupień. Początkowo obiekty są losowo przydzialane do skupień, a następnie w trakcie postępowania iteracyjnego są przenoszone między skupieniami tak, aby wariancja wewnątrz tych skupień była jak najmniejsza.

W przypadku rozmytej metody k-średnich, podobnie jak poprzednio, liczbę skupień określa się na początku postępowania, jednak po zakończeniu procesu iteracyjnego nie dostajemy rozłącznych zbiorów obiektów, lecz dla każdego obiektu określone stopnie przynależności do poszczególnych zgrupowań.

Rozmyta metoda k-średnich umożliwia podział i porównywanie klientów z uwzględnieniem niepewności czy niedokładności wystepującej w przypadku tego zagadnienia. W tym rozumowaniu badamy, w jakim stopniu klienci należą do poszczególnych klas, a nie – jak w przypadku zwykłej metody k-średnich – czy należą do określonej klasy.

Przed rozpoczęciem procedury wyznaczania skupień należy wskazać liczbę skupień c, do których będziemy przyporządkowywać klientów, a także tzw. wykładnik m, $m > 1$, który określa

stopień rozmytości wyników skupiania. Dla wartości m bliskich 1 rezultaty są zbliżone do tych otrzymanych przy pomocy zwykłej metody k-średnich, natomiast dla $m \to \infty$ wartości stopni przynależności do skupień przyjmują wartości bliskie $\frac{1}{c}$.

Załóżmy, że badamy K obiektów x_k, $k = 1, \ldots, K$, przy czym każdy z nich ma N cech o wartościach $x_{k,n}$, $n = 1, \ldots, N$. Procedura postepowania jest procedurą iteracyjną i składa się z następujących czterech kroków:

(i) Podać początkowe wartości stopni przynależności $\mu_{i,k}$ k-tego obiektu (w tym przypadku klienta) do i-tego skupienia, $i = 1, \ldots, c$, $k = 1, \ldots, K$, przy czym musi zachodzić

$$\sum_{i=1}^{c} \mu_{i,k} = 1$$

oraz $\mu_{i,k} \in [0, 1]$ dla każdych $i = 1, \ldots, c$, $k = 1, \ldots, K$.

(ii) Obliczyć centra skupień v_i, $i = 1, \ldots, c$ z uwzględnieniem wartości $\mu_{i,k}$:

$$v_i = \frac{\sum_{k=1}^{K} (\mu_{i,k})^m \times x + k}{\sum_{k=1}^{K} (\mu_{i,k})^m}.$$

(iii) Obliczyć nowych wartości stopni przynależności $\mu_{i,k}^{\text{nowe}}$, $i = 1, \ldots, c$, $k = 1, \ldots, K$, uwzględniając centra skupień wyznaczone w poprzednim kroku:

$$\mu_{i,k}^{\text{nowe}} = \frac{1}{\sum_{j}^{c} = 1 \left(\frac{\|v_i - x_k\|}{\|v_j - x_k\|} \right)^{\frac{2}{m-1}}},$$

gdzie $\| \cdot \|$ oznacza odległość euklidesową.

(iv) Jeżeli $\| \mu^{\text{nowe}} - \mu \| > \varepsilon$, gdzie ε jest ustalonym współczynnikiem zbieżności, przyjąć $\mu = \mu^{\text{nowe}}$ i przejść do kroku 2.

Stosując opisaną metodę, można przeprowadzić analizę klientów banku charakteryzowanych za pomocą cech takich jak wiek, dochód, depozyt, kredyt czy zysk. Wyznaczone w trakcie postępowania centra skupień mogą być traktowane jako profile klientów banku, np. klienci czterdziestoletni, o wysokich zarobkach i dużych depozytach, biorący dość wysokie kredyty oraz przynoszący bankowi średnie zarobki. Następnie, analizując uzyskane stopnie przynależności kientów do poszczególnych skupień, można wyciągać wnioski co to tego, czy klienci należą do tych skupień w sposób zdecydowany, z dużym stopniem przynależności (np. większym od 0,9), czy charakteryzują się dużą rozmytością. Wnioski wyciągnięte z przeprowadonego badania pozwalają także dokonywać analizy profili nowych klientów i efektywniejsze nimi zarządzanie.

Zastosowanie rozmytej metody k-średnich pozwala na uniknięcie przyporządkowywania klientów do poszczególnych skupień „na siłę" do jednego skupienia, co może powodować utratę znacznej części informacji o kliencie, zwłaszcza w przypadku osób, które leżą niejako na obrzeżu skupienia.

Opisana metoda k-średnich nie jest jednak pozbawiona wad. Wymaga ona arbitralnego określenia pewnych parametrów, np. liczby skupień, na które chcemy podzielić obiekty, czy miary odległości. Zmieniając te parametry, można uzyskać różne rezultaty, jednak podstawowe wnioski powinny być takie same. Jedynym sposobem eliminacji tej wady jest dokonywanie eksperymentów i na ich podstawie utworzenie najlepszego dla danego zastosowania podziału.

Literatura

[1] L. Bolc, J. Cytowski, P. Stacewicz, *O logice i wnioskowaniu rozmytym*, Warszawa 1996.

[2] M. Lasek, *Data mining: zastosowania w analizach i ocenach klientów bankowych*, Warszawa 2002.

[3] `www.isep.pw.edu.pl/ZakladNapedu/dyplomy/fuzzy/podstawy_FL.htm`.