

# Teorie rozstrzygalne

Łukasz KAMIŃSKI\*

\*Wydział Matematyki, Informatyki  
i Mechaniki, Uniwersytet Warszawski

Od wieków ludzie marzą o narzędziu, które byłoby w stanie odpowiedzieć na każde pytanie. Nie bez powodu wymyślone zostały wyrocznie, magiczne kule. . . czy też sztuczna inteligencja. Intuicja podpowiada jednak, że nawet jeśli którekolwiek z powyższych odpowie na nasze pytanie, to do odpowiedzi powinniśmy podejść z ograniczonym zaufaniem. Czy da się zatem stworzyć narzędzie, które nigdy się nie myli?

Ograniczmy się do pytań matematycznych. Naszym celem jest więc maszyna, która po otrzymaniu matematycznego stwierdzenia odpowiada, czy jest ono prawdziwe, czy też nie. Jeśli założymy, że pytania będą dotyczyły ustalonej struktury matematycznej, zaś stwierdzenia, o których prawdziwość pytamy, będą wyrażone w pewnym formalnym języku, to czy możemy mieć nadzieję na sukces?

## Logika pierwszego rzędu

Stwierdzenia (zdania) będziemy formułować w tzw. *logice pierwszego rzędu*. W uproszczeniu oznacza to, że możemy używać zmiennych (np.  $x, y, \dots$ ), kwantyfikatorów  $\forall, \exists$ , standardowych spójników logicznych  $\wedge, \vee, \neg, \Rightarrow$ , nawiasów oraz symboli funkcyjnych i relacyjnych z pewnego ustalonego wcześniej zbioru, zwanego *sygnaturą*. Na przykład sygnaturą może być  $\{=, +, \cdot\}$ , zaś zdaniem logiki pierwszego rzędu nad tą sygnaturą  $\forall x \exists y (y + y = x)$  lub też  $\forall x \forall y \forall z (x \cdot y = x \cdot z \Rightarrow x + y = x + z)$ . Z drugiej strony, zdanie  $\forall x \in \mathbb{R} \exists y (x \cdot x) \cdot x = y$  nie jest poprawne, i to z kilku powodów: w rozważanej w tym przykładzie sygnaturze nie ma symbolu relacyjnego  $\in \mathbb{R}$  czy też  $\in$ , a ponadto w logice pierwszego rzędu przy kwantyfikatorach nie może stać nic więcej oprócz samych tylko zmiennych. Zajmijmy się więc zdaniem, które są poprawne. Czy zatem  $\forall x \exists y (y + y = x)$  jest zdaniem prawdziwym? To zależy od kontekstu! Przykładowo w zbiorze liczb naturalnych, gdzie  $+$  oraz  $\cdot$  interpretujemy standardowo jako dodawanie i mnożenie, zdanie  $\forall x \exists y (y + y = x)$  nie jest prawdziwe. Jeśli jednak zapytamy o jego prawdziwość w zbiorze liczb rzeczywistych (gdzie  $+$  oraz  $\cdot$  znów interpretujemy standardowo), to poprawna odpowiedź brzmi: prawda. Nasze pytania powinny więc dotyczyć ustalonej *struktury*, czyli zbioru wraz z interpretacjami symboli z sygnatury. *Teorią* struktury nazywamy zbiór wszystkich zdań prawdziwych w tej strukturze. Przykładowo, przez  $\langle \mathbb{N}; +, \cdot, = \rangle$  oznaczamy strukturę liczb naturalnych ze standardowo zdefiniowanymi działaniami  $+$  oraz  $\cdot$ , zaś przez  $Th\langle \mathbb{N}; +, \cdot, = \rangle$  oznaczamy jej teorię. Mówimy, że teoria jest *rozstrzygalna*, jeśli istnieje algorytm, który mając dane na wejściu zdanie logiki pierwszego rzędu, jest w stanie poprawnie odpowiedzieć, czy należy ono do tej teorii.

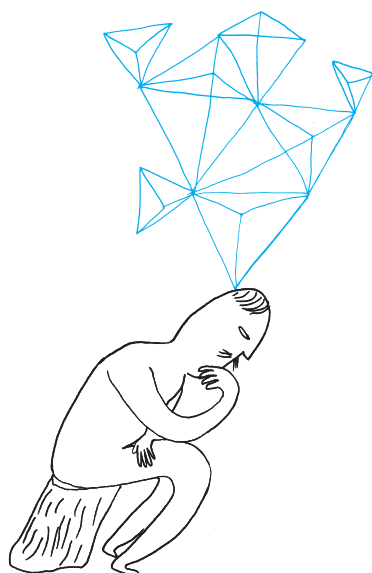
## (Nie)rozstrzygalność w liczbach naturalnych

Pochylmy się nad teorią  $Th\langle \mathbb{N}; +, \cdot, = \rangle$ . Zauważmy, że za pomocą mnożenia można zdefiniować m.in. relację podzielności. Ścisłej rzecz biorąc, można wprowadzić relację  $a|b$ , która jest tak naprawdę skrótem zdania  $\exists c (a \cdot c = b)$ . Mając do dyspozycji relację podzielności, można też napisać formułę  $P(p)$  orzekającą, iż  $p$  jest liczbą pierwszą:  $\forall a \forall b (a \cdot b = p \Rightarrow (a = p \vee b = p) \wedge \neg(a = b))$ . Podobnie dzięki dodawaniu możemy porównywać liczby, bo  $a \leq b$  jest tak naprawdę skrótem zdania  $\exists c (a + c = b)$ . To pozwala już wyrażać naprawdę wiele twierdzeń. Gdyby ktoś skonstruował maszynę potrafiącą rozstrzygać, czy dane zdanie należy do tej teorii, byłby to prawdziwy przełom!

Jednak, jak można się było spodziewać, nie jest tak dobrze! Teoria  $Th\langle \mathbb{N}; +, \cdot, = \rangle$  rozstrzygalna nie jest, co wnioskujemy z jednego ze słynnych twierdzeń Gödla. Czy w takim razie cała nadzieja przepadła? Może po prostu chcieliśmy zbyt wiele? Co by na przykład było, gdyby powstrzymać się od używania mnożenia? Badania nad teorią  $Th\langle \mathbb{N}; +, = \rangle$  prowadził już w 1929 roku Mojżesz Presburger (od jego nazwiska jest ona nazywana arytmetyką Presburgera). Z jego pracy

O teoriach rozstrzygalnych można przeczytać również w nieco starszych wydaniach *Delt*y, np.  $\Delta_{74}^7$ .

Można by chociażby zapytać o prawdziwość zdania:  $\forall_N \exists_p \exists_q (p \geq N \wedge q = p + 2 \wedge P(p) \wedge P(q))$ .



można wywnioskować, że teoria ta jest rozstrzygalna! Załóżmy jednak, że jesteśmy zachłanni i chcemy móc używać jeszcze jakiejś relacji, zachowując przy tym rozstrzygalność. Wiemy już, że rozszerzenie arytmetyki Presburgera o mnożenie to zbyt dużo. Jednak może jeśli ograniczymy się do dorzucenia relacji podzielności  $|$ , to zachowamy rozstrzygalność? Niestety nie. Widzieliśmy już, że mając dodawanie, możemy zdefiniować relację porządku  $\leq$ . Podobnie  $+$  oraz  $|$  pozwalają już zdefiniować mnożenie. Formalnie chcemy umieć zastąpić każde wystąpienie  $c = a \cdot b$  równoważnym zdaniem nieużywającym symbolu mnożenia „ $\cdot$ ”. Zauważmy, że gdybyśmy mogli podnosić do kwadratu, to byłoby łatwo. Istotnie, zdanie  $c = a \cdot b$  jest równoważne zdaniu  $c + c + a^2 + b^2 = (a + b)^2$ . Ale jak zdefiniować na przykład  $a^2$ ? Niech  $x$  będzie najmniejszą liczbą większą od 1, spełniającą  $(a - 1)|(x - 1) \wedge (a + 1)|(x - 1)$ . Wówczas jeśli  $2|a$ , to  $x = a^2$ , zaś jeśli  $2 \nmid a$ , to  $x + x = a^2$  (polecamy zastanowić się nad precyzyjnym uzasadnieniem tego rozumowania). To już wystarcza do stworzenia definicji. Wniosek jest taki, że  $Th(\mathbb{N}; +, |, =)$  nie jest rozstrzygalna, bo nad sygnaturą  $\{+, |, =\}$  jesteśmy w stanie wyrazić to samo co nad sygnaturą  $\{+, \cdot, =\}$ .

Jak widać, nie jest łatwo rozszerzyć arytmetykę Presburgera, zachowując przy tym rozstrzygalność. Istnieją jednak nietrywialne przykłady, jak to zrobić. Jednym z nich jest arytmetyka Semënova, czyli arytmetyka Presburgera z dodatkiem funkcji  $\text{pow}_2(n) = 2^n$ . Zachęcam Czytelnika do pomyślenia nad ciekawymi przykładami zdań w logice pierwszego rzędu nad sygnaturą tej teorii.

### Mnożenie nie takie straszne

Powróćmy do struktury  $(\mathbb{N}; +, \cdot, =)$ . Czy mnożenie samo w sobie jest odpowiedzialne za nierozstrzygalność jej teorii? Wcale nie! Okazuje się, że teoria  $Th(\mathbb{N}; \cdot, =)$  jest rozstrzygalna, co zostało ogłoszone w pracy Thoralfa Skolema, a później w pełni udowodnione przez Andrzeja Mostowskiego. Na część tego pierwszego teorii tę nazywamy arytmetyką Skolema. Podobnie jak wcześniej, zastanówmy się, co można dodać do arytmetyki Skolema, zachowując rozstrzygalność. Oczywiście dodawanie odpada, ale może na przykład relacja porządku  $\leq$ ? Po pierwsze, za pomocą  $\leq$  można zdefiniować funkcję następnik  $\text{succ}(n) = n + 1$  (Czytelniku, sprawdź sam!). Następnie można zdefiniować dodawanie za pomocą tzw. tożsamości Tarskiego:

$$a + b = c \vee c = 0 \iff \text{succ}(ac) \cdot \text{succ}(bc) = \text{succ}(c^2 \text{succ}(ab)).$$

Wynika stąd, że  $Th(\mathbb{N}, \cdot, \leq)$  rozstrzygalna nie jest (bo w przeciwnym wypadku  $Th(\mathbb{N}; +, \cdot, =)$  byłaby rozstrzygalna). Istnieją jednak relacje, które można dorzucić, nie tracąc rozstrzygalności. Przykładem jest relacja  $a \sim b$ , która zachodzi wtedy i tylko wtedy, gdy liczby  $a, b$  mają dokładnie tyle samo dzielników pierwszych, nie wliczając krotności (np.  $20 \sim 6$ ). Fakt ten został udowodniony w 1959 roku przez Salomona Fefermana i Roberta Vaughta.

### Nie tylko liczby naturalne

Jak dotąd przyglądaliśmy się wyłącznie strukturze liczb naturalnych. Rozważmy więc teraz liczby rzeczywiste. W tym miejscu Czytelnik może poczuć się zaskoczony. Alfred Tarski udowodnił, iż struktura  $(\mathbb{R}; +, \cdot, =)$  ma rozstrzygalną teorię! Ma to kilka ciekawych następstw. Przykładowo, twierdzenie to implikuje istnienie algorytmu, który rozstrzyga, czy dane równanie wielomianowe (np.  $x^4 - 3x + 4 = 0$ ) ma rozwiązanie rzeczywiste. Innym zastosowaniem mogą być zadania z geometrii analitycznej, które to da się zakodować jako zdania nad sygnaturą  $\{+, \cdot, =\}$ . Z twierdzeniem Tarskiego jest też związany intrygujący problem otwarty. Nie wiadomo, czy teoria struktury  $(\mathbb{R}; +, \cdot, \exp, =)$  (gdzie  $\exp(x)$  oznacza funkcję  $e^x$ ) jest rozstrzygalna, czy też nie. Można za to udowodnić, że teoria struktury  $(\mathbb{R}; +, \cdot, \sin, =)$  jest nierozstrzygalna.

Na zakończenie dopowiedzmy jeszcze, że teoria  $Th(\mathbb{Q}; +, \cdot, =)$  jest nierozstrzygalna (co zostało udowodnione przez Julię Robinson), a teoria  $Th(\mathbb{C}, +, \cdot, =)$  jest rozstrzygalna (co pozostawiamy jako ćwiczenie). Czytelnikowi pragnącemu dowiedzieć się więcej na opisany tu temat polecamy m.in. artykuł *A Survey of Arithmetical Definability* autorstwa Alexisa Bèsa.

Więcej o zastosowaniach tego twierdzenia pisze Lorenzo Clemente w  $\Delta_{23}^2$ .

Podpowiedź: rozstrzygalność  $Th(\mathbb{C}, +, \cdot, =)$  udowadniamy, korzystając z rozstrzygalności  $Th(\mathbb{R}; +, \cdot, =)$ .