Witold Marciszewski – witold@marciszewski.eu, witmar@calculemus.org

Postęp wiedzy z informatycznego punktu widzenia
Od intuicji do algorytmu, od algorytmu do intuicji

Odczyt na seminarium „Filozoficzne problemy wiedzy”, IFiS PAN, 16 marca 2018.

Streszczenie

Hasło Leibniza **calculemus** wyraził Hilbert w słynnej maksymie na temat wiedzy matematycznej: **Wir müssen wissen, wir werden wissen**.

„Wiedzieć” oznacza tu wiedzę uzyskaną w wyniku dowodu sformalizowanego czyli sprawdzalnego algorytmicznie. Do czasu wyników Gödla, Turinga etc. pojmowano ów postulat w ten sposób, że uzyskałoby się jeden algorytm sprawdzania stosowalny do wszystkich twierdzeń. Miała go dostarczyć logika predykatów. Okazało się to nierealne, co udowodnili Gödel (niezupełność teorii liczb, 1931) i Turing oraz inni (nierozstrzygalność logiki predykatów pierwszego rzędu, 1936). Jest natomiast realne w następującej wersji.

Nie ma jednego algorytmu logicznego, który rozwiązywałby wszystkie problemy matematyczne, ale dla każdego z nieskończonej klasy problemów istnieje algorytm, który go rozwiązuje. Każdy kolejny system dostarcza więcej informacji.

Ten fakt ugruntowany jest w dwóch twierdzeniach, z których ogólniejsze pochodzi od Turinga (1939) z pracy o logikach porządkowych – *ordinal logics*, a doniosłe jego uszczegółowienie i uzupełnienie znajdujemy u Gödla (1936). Oto tekst Turinga.

> The well known theorem of Gödel (1931) shows that every system of logic is in a certain sense incomplete, but at the same time it indicates means whereby from a system L of logic a more complete system L* may be obtained. By repeating the process we get a sequence L, L1 = L*, L2 = L1*, L3 = L2* ,. . . of logics each more complete than the preceding. A logic L_ω may then be constructed in which the provable theorems are the totality of theorems provable with the help of the logics L, L1, L2,...

Gödel ("Über die Länge von Beweisen" 1936) dostarczył przykładu, czym może być taka sekwencja coraz to bliższych zupełności systemów: może to być sekwencja systemów arytmetyki, w której każdy kolejny człon operuje w dowodzeniu logiką wyższego rzędu niż poprzednie.

Z tym uszczegółowieniem łączy się twierdzenie o przyspieszaniu tempa (speedup) dowodzenia przez wydatne skracania dowodów za każdym przejściem do wyższego rzędu.

(1) Formuły teorii niedowodliwe w logice N-tego rzędu są dowodliwe w logice rzędu N+1 lub wyższego. (2) Formuły, które w logice N-go rzędu mają niewykonalnie długie dowody, w którejś z logik wyższego rzędu będą mieć dowody znacząco krótsze, wykonalne w realnie dostępnym czasie.

Konstatacja Gödla pozwala nadać uchwytny sens dość enigmatycznemu pojęciu wyroczni, którym posłużył się Turing, komentując ideę ciągu logik porządkowych.

> Let us suppose that we are supplied with some *unspecified means* of solving number theoretic problems; a kind of *oracle* as it were. We will not go any further into the nature of this oracle than to say that *it cannot be a machine*; with the help of the oracle we could form a new kind of machine (call them *o-machines*), having as one of its fundamental processes that of solving a given number theoretic problem. (s. 13 w pracy 1939, podkreślenia – WM).

Brak określoności (unspecified means) naprawia w pewien sposób gödlowski obraz sekwencji logik coraz wyższego rzędu. Ponieważ ich źródłem jest teoriomnogościowa intuicja coraz wyższego rzędu zbiorów, zdaje się to naprowadzać na taką oto empiryczną interpretację pojęcia wyroczni, że jej werdykty są produktem intelektualnej intuicji matematycznej. Na rzecz zgodności tej interpretacji z intencją Turinga przemawia następujące pojmowanie przez niego intuicji.

> Mathematical reasoning may be regarded rather schematically as the exercise of [...] intuition. [Its] activity consists in making spontaneous judgments which are not the result of conscious trains of reasoning. These judgments are often, but by no means invariably, correct. (s .57).

Niech każdy z wyrazów ciągu L1....Ln... będzie aksjomatycznym systemem arytmetyki wyposażonym w reguły dedukcyjne logiki coraz wyższego rzędu. Są to systemy sformalizowane i dzięki temu do sprawdzania poprawności dowodu mamy stosowny algorytm.

Żeby dokonać formalizacji, nieodzowna jest wyrocznia czyli twórcza intuicja prowadząca do nowych pojęć. Każdy bowiem kolejny rząd logiki wymaga m.in. nowych aksjomatów abstrakcji, definiujących właściwe dla danego rzędu pojęcia zbioru pustego, uniwersalnego, oraz dopełnienia zbioru.

Tak rysuje się droga od intuicji do algorytmu. Kierunek przeciwny doskonale ilustrują dzieje arytmetyki. U pitagorejczyków intuicja co do istnienia liczb niewymiernych nie mogłaby powstać, gdyby nie dysponowali algorytmem potęgowania liczb naturalnych i znajdowania pierwiastka. Dzięki temu, że umieli obliczyć $\sqrt{4}$, stanęli przed pytaniem, ile wynosi $\sqrt{2}$, co ich doprowadziło do intuicji zbioru liczb niewymiernych.

W takim rytmie sprzężeń zwrotnych między intuicją i algorytmem dokonuje się postęp matematyki. A że jest ona lokomotywą dla innych nauk, otrzymujemy obraz postępu wiedzy kreślony barwami zaczerpniętymi z pojęć informatycznych. Pewność więc Hilberta, że dla każdego problemu znajdziemy rozwiązanie natury algorytmicznej jest zasadna, o ile zaimek MY będzie oznaczał nie nasze lub jakieś nieodległe pokolenie, lecz nieskończony potencjalnie ciąg zmierzających do prawdy pokoleń umysłów.