Jan Woleński

Rachunek zdań wcale nie jest taki prosty

Filozofia Nauki 7/3/4, 169-171

1999

Filozofia Nauki
Rok VII, 1999, Nr 3—4(27—28)

Jan Woleński

Rachunek zdań wcale nie jest taki prosty

Satisfiability Problem: Theory and Application **(ed. by D. Du, J. Gu, and P. M. Pardalos), American Mathematical Society, Providence 1997, s: XV + 724**

Rachunek zdań (*PC*) jest najbardziej podstawową teorią logiczną. Uchodzi też za prosty. Istotnie, ma rozmaite pożądane własności. Jest niesprzeczny, pełny (*A* jest tautologią zawsze i tylko wtedy, gdy *A* jest dowodliwe), rozstrzygalny (istnieje procedura wykazywania tautologiczności, która jest wykonalna w skończonej ilości kroków) i Post-zupełny (jeśli *A* jest formułą *PC*, to albo jest tautologią, albo prowadzi do sprzeczności po jej dodaniu do *PC*). Ponadto te wszystkie własności są efektywnie dowodliwe, tj. przy użyciu finitystycznych metod syntaktycznych. Wszelako każdy dobrze wie, iż procedura sprawdzania tautologii przez tabelki zerojedynkowe jest prosta jedynie w wypadku, gdy sprawdzana formuła liczy niewiele zmiennych, przy czym ocena owego „niewiele" zależy od upodobań i cierpliwości. W podręcznikach nie ma przykładów tabelek dla formuł zawierających więcej niż trzy zmienne. Sam dla zabawy, wątpliwej zresztą, rozważałem przypadki z czterema literami. Nie znam z literatury przypadku dla pięciu lub więcej zmiennych.

W istocie rzeczy słowo „skończony" wcale nie przesądza ani o prostocie, ani o łatwości. Zrealizowanie skończonej procedury wymaga czasu i miejsca, ale jak wiele? Na pewno skończonego czasu i skończonej przestrzeni, ale czy można powiedzieć coś więcej? Dopóki nie pojawiły się komputery, sprawa w ogóle nie była rozważana, albowiem nie było ku temu powodów. Od jakichś 25 lat trwają badania nad tzw. problemem spełnialności (problem *SAT*), tj. znajdowaniem algorytmów dla odpowiedzi na następujące pytanie: Jak wiele kroków jest potrzebnych by sprawdzić, czy dana formuła rachunku zdań jest spełnialna czy nie? Formuła *A* jest spełnialna, jeśli istnieje wartościowanie, które jest jej modelem, tj. takie, że wszystkie wartościowane zmienne przybierają wartość prawdy. Podobnie charakteryzuje się problem tautologiczności (problem *TAU*): Jak wiele kroków jest potrzebnych dla okazania, że dana formuła jest tautologią? Rozważa się przy tym nie tabele, ale formy normalne, koniunkcyjne lub alternatywne.

SAT i *TAU* są zwykle wyrażane jako problemy dotyczące czasu potrzebnego maszynie Turinga na stosowne obliczenia. Odróżnia się czas wielomianowy i czas wykładniczy. Czas wielomianowy to taki, którego długość wyraża się wielomianem (podobnie mówi się o przestrzeni wielomianowej), natomiast długość czasu wykładniczego wyraża się funkcją wykładniczą. Różnica jest niebagatelna, gdyż funkcje wykładnicze rosną bardzo szybko. Jeśli jakiś problem wymaga czasu wykładniczego, określany jest jako „oporny". Nie wiadomo, czy *SAT* i *TAU* są oporne czy nie. Przypuszcza się, że nie są. Wiadomo, że *SAT* jest *NP*-zupełny. Symbol *NP* oznacza klasę zbiorów akceptowalnych (rozpoznawalnych) przez maszynę Turinga w wielomianowym czasie niedeterministycznym, natomiast symbol *P* oznacza klasę zbiorów akceptowanych w wielomianowym czasie deterministycznym. Powiada się, że zbiór formuł *PC* jest *NP*-zupełny zawsze i tylko wtedy, gdy *X* należy do *NP* oraz wszystkie inne zbiory będące w *NP* są redukowalne do *X* w deterministycznym czasie wielomianowym, tj. *P*-redukowalne. *SAT* jest *NP*-zupełny. Pociąga to, że P = NP dla *SAT*. Tak więc, jeśli istnieje algorytm dla *SAT* wykonalny w deterministycznym czasie wielomianowym, to wszystkie problemy tyczące się *NP* mają też deterministyczne algorytmy wielomianowe. Jeśli wiadomo, że jakaś kwestia jest oporna, to wiadomo też, iż ma algorytm deterministyczny. Natomiast nie wiadomo, czy *TAU* jest *NP*-zupełny. Jeśli jest, to fakt ten implikuje, że P = NP również dla *TAU*. W ogólności badania nad *SAT* i *TAU* są związane ze złożonością obliczeniową.

Te ogólne wyniki nie przesądzają „wyglądu" stosownych algorytmów. Ich znajdowanie nie jest bynajmniej automatyczne. Powiada się, że zbiory formuł są *NP*-trudne, gdy są *NP*-zupełne. Jak znajdować *P*-algorytmy, tj. rozwiązywać *NP*-trudne problemy? Czy problemy oporne redukują się do trudnych? Ponieważ nie ma automatycznych odpowiedzi, trzeba formułować cząstkowe przypuszczenia. Wiele z nich jest zreferowanych w recenzowanej książce. Trudno się zagłębiać w szczegóły, więc ograniczę się tylko do przytoczenia tematyki poszczególnych artykułów: sposoby znajdowania trudnych klas dla *SAT*, rozmaite algorytmy dla *SAT*, strategie wykorzystujące próbne waluacje dla wybranych zmiennych, względna złożoność niektórych szczególnych przypadków *SAT*, złożoność hierarchiczna i wymiarowość (periodyczna i inna) *NP*-trudnych problemów, analiza przypadków niekorzystnych, tj. zależnych od zbytniej komplikacji odpowiednich postaci normalnych, związki pomiędzy efektywnością poszukiwań algorytmów dla *SAT* i dowodliwością w logice pierwszego rzędu, rozgałęzioność reguł dla *SAT*, dyskretne bazy poszukiwawcze dla *SAT*, strategie aproksymacyjne, strategie wielopłaszczyznowe, algorytmy gałęziowe i obcięte, heurystyki i algorytmy uczące, procedury stochastyczne, podstawowe własności ciał boole'owskich ważne dla *SAT*, rozstrzygalność w czasie wielomianowym w związku z symulacją dla *SAT* poprzez własność Horna, szacowanie progu niespełnialności, rozwiązywanie maksymalnych wersji *SAT*, rozkłady rozwiązań dla koniunkcyjnych formuł normalnych, zastosowanie pochodnych drugiego rzędu w badaniach nad *SAT*, badania lokalne nad *SAT* i problemy projektowania obwodów. Przegląd powyższy wskazuje na kierunki badań i stosowane metody. Wielorakość sposobów jest godna uwagi, bo mamy i badania formalno-logiczne, i probabilistyczne, i techniczne (nawet w sensie inżynierskim).

Co sugeruje filozofowi problem *SAT*? Po pierwsze, że logika czerpie inspiracje z praktyki. To pocieszające, bo znaczy, że logika, nawet na poziomie rachunku zdań, jest teorią otwartą na nowe problemy. I wcale nie prostą, co wyraża tytuł niniejszej recenzji. Po drugie, mówi coś w związku z odwiecznym problemem kryterium prawdy. Od dawna wiadomo, że tzw. klasyczna teoria prawdy nie zmusza nas do przyjęcia żadnego konkretnego kryterium prawdy. Przypuśćmy, że spełnialność (nawet w rachunku zdań) znaczy prawdziwość (klasyczną) w modelu. Jasne jest, że ogólne metalogiczne określenie spełnialności nie sugeruje żadnego konkretnego kryterium prawdy. Pokrótce zreferowane badania przemawiają za tym, że nie może być inaczej. Można tę uwagę przenieść i na teren mocniej związany z pojęciem prawdy w modelu, mianowicie do logiki pierwszego rzędu. Ponieważ rachunek predykatów jest nierozstrzygalny, problem *SAT* nie pojawia się w odniesieniu do tej teorii, bo z góry wiadomo, że badanie spełnialności zbiorów formuł nie sprowadza się do wartościowania zerojedynkowego. Niemniej *NP*-problemy rozważa się i wobec teorii opartych na logice predykatów. Krótko mówiąc, mamy jakieś metalogiczne potwierdzenie starej obserwacji: czym innym jest określenie prawdziwości, a czym innym kryterium prawdy.