Optymalne systemy dowodowe i języki zupełne

Zenon Sadowski (Białystok)

Abstrakcyjnym systemem dowodowym dla rachunku zdań nazywamy dowolną funkcję, która jest obliczalna w czasie wielomianowym i której zbiorem wartości jest $TAUT$ (zbiór tautologii rachunku zdań). Każde słowo w, które ta funkcja przeprowadza na tautologię α jest traktowane jako dowód α.

J. Köbler, J. Messner i J. Torán [1] udowodnili, że istnienie p-optymalnego systemu dowodowego dla rachunku zdań implikuje istnienie języka zupełnego w klasie **UP**. A. Razborov [2] udowodnił, że istnienie optymalnego systemu dowodowego dla rachunku zdań implikuje istnienie rozłącznej **NP**-pary, która jest zupełna w klasie Dis**NP** (rozłącznych **NP**-par).

Motywacją do napisania tej pracy była chęć wyjaśnienia dlaczego w obu tych twierdzeniach implikacje w drugą stronę nie zachodzą. W realizacji tego celu użyteczne okazało się, wprowadzone w pracy, pojęcie semantycznej klasy złożonosci, reprezentowanej w systemie dowodowym dla rachunku zdań. Dla maszyny Turinga będącej odpowiednim modelem obliczeń takiej klasy złożoności istnieje ciąg tautologii rachunku zdań, z których n-ta stwierdza, że maszyna ta spełnia 'promise' tej klasy dla danych wejściowych długości n. Tautologie te posiadają dowody o wielomianowej długości w systemie dowodowym, w którym ta klasa złożoności jest reprezentowalna.

W pracy dowodzimy, że klasa **UP** posiada język zupełny wttw, gdy istnieje system dowodowy dla rachunku zdań, w którym **UP** jest p-reprezentowalna. Z kolei dowodzimy, że p-optymalny (optymalny) system dowodowy dla rachunku zdań istnieje wttw, gdy istnieje system dowodowy dla rachunku zdań, w którym dowolna semantyczna klasa złożoności z warunkiem 'promise' wyrażalnym za pomocą ciągu tautologii, jest p-reprezentowalna (reprezentowalna). Klasa **UP** jest przykładem klasy złożoności, której 'promise' jest wyrażalny za pomocą ciągu tautologii.

Otrzymana charakteryzacja problemu istnienia optymalnego systemu dowodowego jest analogiczna do charakteryzacji tego problemu z wcześniejszej pracy. Zamiast reprezentowalności typu 'uniform' w teorii pierwszego rzędu (arytmetyce) występuje tu jednak reprezentowalność typu 'nonuniform' w systemie dowodowym dla rachunku zdań. Bardzo często w 'proof complexity' system dowodowy dla rachunku zdań jest wersją typu 'nonuniform' teorii pierwszego rzędu.

Literatura

[1] J.Köbler, J.Messner, J.Torán, Optimal proof systems imply complete sets for promise classes, Information and Computation 184 (2003) 71 - 92.

[2] A.Razborov, On provably disjoint NP-pairs, Technical Report 94 - 006, Electronic Colloquium on Computational Complexity, 1994.