Leszek Pacholski
Uniwersytet Wrocławski

12 lipca 2023 r.

Recenzja rozprawy doktorskiej Complexity of solving equations in finite algebraic structures mgra Piotra Kawałka

W pracy *Satisfiability in multi-valued circuits*, przedstawionej na konferencji Annual ACM/IEEE Symposium on Logic in Computer Science w 2018 roku, promotor rozprawy Paweł M. Idziak oraz promotor pomocniczy Jacek Krzaczkowski przedstawili program systematycznego zbadania złożoności obliczeniowej problemów spełnialności równań w dowolnych algebrach skończonych. Problemy takie są oczywiście w NP. Program postulował sformułowanie i udowodnienie jakiejś wersji twierdzenia o dychotomii podobnego do twierdzenia o dychotomii dla problemu spełnialności więzów (CSP). Ponieważ dodanie do języka algebry definiowanych termów pozwala na wykładnicze skracanie reprezentacji równań, złożoność problemu spełnialności równań w ustalonej algebrze może zależeć od wyboru języka. Dlatego zaproponowali reprezentację wielomianów przy pomocy obwodów i sformułowali problem CSAT(A) - badanie problemu spełnialności dla obwodów, w których bramkami mogą być funkcje z dowolnej algebry skończonej A, a danymi elementy A. Przedstawili częściowe wyniki pozostawiając kilka pytań otwartych.

Program ograniczono do klasy algebr należących do rozmaitości z modularnymi kongruencjami (congruence modular varieties) dla których R. Freese and R. McKenzie (głównie) zbudowali narzędzia (teoria modularnych komutatorów - modular commutator theory oraz teoria kongruencji oswojonych - tame congruence theory) pozwalające na pogłębione badania tych algebr. Klasa ta zawiera znakomitą większość algebr badanych przez matematyków.

Rozprawa Piotra Kawałka poświęcona jest realizacji przedstawionego wyżej programu badawczego i dotyczy złożoności obliczeniowej problemów związanych ze spełnialnością równań w dowolnych algebrach skończonych i spełnialnością sieci nad algebrami skończonymi.

Rozprawa składa się z siedmiu prac

1. Pawel M. Idziak, Piotr Kawałek, Jacek Krzaczkowski, *Expressive Power, Satisfiability and Equivalence of Circuits over Nilpotent Algebras*, Proc. 43rd International Symposium on Mathematical Foundations of Computer Science 2018,
2. Piotr Kawałek, Jacek Krzaczkowski, *Even faster algorithms for CSAT over supernilpotent algebras,* Proc. 45th International Symposium on Mathematical Foundations of Computer Science 2020,
3. Pawel M. Idziak, Piotr Kawałek, Jacek Krzaczkowski, *Intermediate problems in modular circuits satisfiability,* Proc. 35th Annual ACM/IEEE Symposium On Logic in Computer Science 2020,
4. Pawel M. Idziak, Piotr Kawałek, Jacek Krzaczkowski, Armin Weiß, *Equation satisfiability in solvable groups*, Theory of Computing Systems 2022,
5. Pawel M. Idziak, Piotr Kawałek, Jacek Krzaczkowski, *Satisfiability of Circuits and Equations over Finite Malcev Algebras*, Proc. 39th International Symposium on Theoretical Aspects of Computer Science 2022,

6. Pawel M. Idziak, Piotr Kawałek, Jacek Krzaczkowski, Armin Weiß, *Satisfiability problems for finite groups*, Proc. 49th International Colloquium on Automata, Languages, and Programming 2022,
7. Pawel M. Idziak, Piotr Kawałek, Jacek Krzaczkowski, *Complexity of Modular Circuits*, Proc. 37th Annual ACM/IEEE Symposium on Logic in Computer Science 2022,

Prace te są integralną częścią rozprawy. Zostały uzupełnione krótkim autoreferatem omawiającym niektóre rezultaty przedstawione w tych publikacjach. Rozumiem, że zdaniem autora wyniki opisane w autoreferacie są najważniejszymi osiągnięciami rozprawy. Część z nich to przykłady ilustrujące złożoność zadania badawczego i pokazujące, że rozdzielenie problemów trudnych - nie należących do P - od tych dla których istnieją algorytmy wielomianowe nie jest zadaniem prostym. Są też wyniki porządkujące pewne fragmenty teorii. Przytoczę kilka najważniejszych.

W badaniach nad złożonością problemów w klasie NP często przyjmuje się pewną wersję założenia, że NP jest różne od P. W rozprawie rozważa się trzy wersje takich założeń. Hipoteza czasu wykładniczego (ETH) postuluje, że nie ma algorytmów rozwiązujacych problem SAT (spełnialność formuł Boole'a) w czasie podwykładniczym. Zrandomizowana hipoteza czasu wykładniczego (rETH) postuluje, że nia ma takich algorytmów zrandomizowanych. Obwody modularne są uogólnieniem obwodów Boole'a i działają na danych logicznych. Dla każdej bramki obwodu modularnego (MOD_m) z modułem m ustalony jest zbiór liczb naturalnych mniejszych od m i bramka sprawdza, czy reszta modulo m sumy danych do niej wchodzących należy do tego zbioru. CC_h [m] oznacza klasę obwodów głębokości h z modułem m. Hipoteza CDH (constant Degree Hypothesis) zakłada istnienie wykładniczego ograniczenia dolnego na wielkość obwodów modularnych (z bramkami typu (MOD_m) obliczającymi koniunkcję dowolnej arności.

Jednym z rozważanych zagadnień jest problem spełnialności programów w grupach skończonych, badany już od ponad 20 lat. PROGRAMSAT(G) oznacza problem, czy język rozpoznawany przez niejednostajny deterministyczny automat skończony nad ustaloną grupą G jest niepusty. Ładny wynik z pracy [6] mówi, że przy założeniu rETH oraz CDH, PROGRAMSAT(G) można rozwiązać w randomizowanym czasie wielomianowym wtedy i tylko wtedy, gdy istnieje liczba pierwsza i normalna p-podgrupa G_p grupy G taka, że G/G_p jest grupą nilpotentną. Natomiast dla algorytmów deterministycznych, przy założeniu ETH, jeśli G jest grupą rozwiązalną o stopniu nilpotentności $h \geq 3$, to problem spełnialności i problem równoważności wielomianów nad G nie może być rozwiązany w czasie $n^{o(log^{h-2}n)}$.

W pracy [2] zaproponowano algorytmy deterministyczne, szybsze od znanych dotychczas rozwiązujące problem CSAT(A) dla algebr super-nilpotentnych oraz algorytm Monte Carlo rozwiązujący ten problem w czasie liniowym dla algebr nilpotentnych. Wraz z wcześniej znanymi wynikami daje dla to grup skończonych G twierdzenie typu dychotomii - dla każdej grupy skończonej G, jeśli G jest nilpotentna, to istnieje liniowy algorytm Monte Carlo dla CSAT(G), a jeśli nie jest, to CSAT(G) jest NP-zupełny.

Inne, bardzo klasyczne, twierdzenie o dychotomii dotyczy grup symetrii wielokątów regularnych. Przy założeniu rETH problem spełnialności wielomianów w grupie symetrii

wielokąta o m bokach jest rozstrzygalny w randomizowanym czasie wielomianowym wtedy i tylko wtedy, gdy m jest potęgą liczby pierwszej.

Praca [7] dotyczy obwodów modularnych. Jej główne, bardzo eleganckie twierdzenie mówi, że przy założeniu ETH problem spełnialności obwodów CC_h [m] jest w P wtedy i tylko wtedy, gdy h=1 lub m jest potęgą liczby pierwszej.

Rozprawa Piotra Kawałka zawiera wiele interesujących i trudnych wyników. Leży na pograniczu algebry (klasycznej i ogólnej) oraz zaawansowanej teorii złożoności obliczeniowej. Wpisuje się w bardzo modną w ostatnich kilkunastu latach tematykę badań związanych z dychotomią problemów z klasy NP. Doktorant wykazał się, dość unikalną w środowisku informatyków, wiedzą w zakresie algebry oraz dobrym opanowaniem technik dowodowych w teorii złożoności obliczeniowej.

Uważam, że rozprawa Piotra Kawałka z nawiązką spełnia ustawowe i zwyczajowe wymagania stawiane rozprawom doktorskim i wnoszę o dopuszczenie doktoranta do dalszych etapów przewodu doktorskiego.

12.07.2023 Lech Paczolek