Nr rejestracyjny: 2022/45/B/ST6/02229; Kierownik projektu: dr Jacek Krzaczkowski

Problemy spełnialności i równoważności dla skończonych algebr

Jacek Krzaczkowski

Od czasów starożytnych rozwiązywanie równań było jednym z najważniejszych problemów matematyki i było rozważane od samych początków tego co dzisiaj nazywamy informatyką. Jednym ze znaczących przykładów jest słynny 10. problem Hilberta, to jest pytanie czy istnieje algorytm stwierdzający czy równanie wielomianów o współczynnikach całkowitoliczbowych ma rozwiązanie, w którym wartości niewiadomych są liczbami całkowitymi. Problem został rozwiązany przez J. Matijasiewicz w 1970 r. Okazało się, że nie istnieje algorytm sprawdzający czy wielomian ma rozwiązanie w liczbach całkowitych. Dzisiaj, trudność rozwiązywania równań nad skończonymi strukturami algebraicznymi zapewnia bezpieczeństwo kryptografii klucza publicznego. Inaczej niż w przypadku wyników uzyskanych przej Matijasiewicza, algorytm może stwierdzić czy dane równanie nad skończoną strukturą algebraiczną ma rozwiązanie. Wystarczy sprawdzić wszystkie potencjalne rozwiązania (wartości niewiadomych). Taki prymitywny algorytm do rozwiązania równania z n niewiadomymi nad strukturą o k elementach wykona liczbę kroków proporcjonalną do k^n. Z drugiej strony, dla niektórych struktur potrafimy rozwiązywać równania dużo szybciej np.: jeżeli jedyną operacją występującą w równaniu jest dodawania modulo liczba pierwsza p, wtedy łatwo jest stwierdzić czy równanie ma rozwiązanie ze zbioru $\{0, 1, \ldots, p-1\}$ (w tym przypadku wszystko co musi zrobić algorytm to redukcja wyrazów podobnych i sprawdzenie czy równanie nie jest trywialnie sprzeczne).

Głównym celem projektu jest scharakteryzowanie dla których struktur algebraicznych kilka problemów obliczeniowych związanych z rozwiązywaniem równań może być rozwiązanych przez efektywny algorytm (to jest działający w tak zwanym czasie wielomianowym). Rozważane problemy są jednego z trzech typów. Dla danego równania nad ustaloną strukturą algebraiczną pytamy czy:

- to równanie ma rozwiązanie,
- to równanie ma rozwiązanie, w którym wartości niewiadomych należą do otrzymanych razem z równaniem list (potencjalnie różnych dla różnych niewiadomych),
- równanie jest spełnione przez wszystkie wartości niewiadomych.

Wielomiany są w matematyce typowym sposobem opisu operacji struktur algebraicznych. W wielu dziedzinach informatyki używamy w tej roli sieci/obwodów czyli prostego modelu obliczeń, w którym otrzymane na wejściu wartości są przetwarzane przez ciąg bramek, z których każda liczy funkcję z ustalonego zbioru. Dla wszystkich rodzajów problemów wymienionych powyżej rozważamy dwie wersje. Jedną, w której rozważamy równania wielomianów i drugą, w której rozważamy równania sieci. Sieci często umożliwiają opisanie funkcji w krótszy sposób niż wielomiany. Dzieje się tak dlatego, że wynik obliczeń jednej bramki może być użyty jako dane wejściowe wielu innych bramek (w przypadku wielomianów aby użyć wielokrotnie wartości jakiegoś wyrażenia musimy je wstawić w każde miejsce, w którym chcemy tej wartości użyć). Stąd rozwiązywanie równań sieci (i inne podobne problemy) może być trudniejsze niż ten sam problem dla równań wielomianów.

Automaty i języki przez nie rozpoznawane to jedne z najpowszechniej rozważanych problemów w informatyce teoretycznej. Interesujemy się automatem NUDFA (ang. non-uniform deterministic finite automaton) pewną modyfikacją skończonych automatów deterministycznych. Automat NUDFA można zdefiniować przy pomocy trzech elementów: skończonej struktury algebraicznej (pierwotnie dowolnej półgrupy), termu/wielomianu oraz tak zwanego programu. Rozważamy następujące pytanie

- Jaka jest złożoność obliczeniowa problemu, w którym pytamy czy język rozpoznawany przez automat NUDFA nad ustaloną skończoną strukturą algebraiczną nie jest pusty?

Okazało się, że sprawdzanie czy język rozpoznawany przez automat NUDFA nie jest pusty jest blisko związane z problemem spełnialności równań i zamierzamy rozważać te problemy razem.

Będziemy rozważać wymienione powyżej problemy dla różnych klas struktur algebraicznych. Nasze badania rozpoczniemy od grup. Następnie zamierzamy rozważyć struktury algebraiczne z tak zwanych rozmaitości kongruencyjnie modularnych, dużej klasy „dobrze" zachowujących się struktur zawierającej między innymi grupy, pierścienie, kraty i większość popularnych struktur algebraicznych z ważnym wyjątkiem półgrup. Na koniec wyjdziemy poza rozmaitości kongruencyjnie modularne i sprawdzimy co jesteśmy w stanie powiedzieć o złożoności obliczeniowej rozważanych problemów w ogólnym przypadku.