Dr hab. Wit Foryś Kraków, 24.03.2025

Recenzja rozprawy doktorskiej

Synchronization of Finite Automata – Problems and Generalizations

Autor: **mgr Jakub Ruszil**

Formalną podstawą opracowania recenzji stanowi uchwała Rady Dyscypliny Informatyki Technicznej i Telekomunikacji Uniwersytetu Jagiellońskiego z dnia 26.09.2024. Promotorem rozprawy jest profesor dr hab. Adam Roman, a promotorem pomocniczym dr Jakub Zygadło. Rozprawa mieści się w dziedzinie nauk technicznych, w dyscyplinie informatyka techniczna i telekomunikacja.

Rozprawa napisana jest w języku angielskim. Ze względu na brak jednoznacznego nazewnictwa w języku polskim związanego z pojęciem synchronizowalności automatu przyjmuję, na użytek tej recenzji, iż „carefully synchronized word" to słowo c-synchronizujące, A 'carefully sunchronized automaton" to automat c-synchronizowalny.

Rozprawa doktorska zatytułowana „Synchronization of Finite Automata – Problems and Generalizations", której autorem jest Pan mgr Jakub Ruszil składa się z 7 rozdziałów i liczy 81 stron. Dwa pierwsze rozdziały stanowią wprowadzenie do problemu synchronizacji i różnych jego aspektów, zawierając również motywację tego rodzaju badań. Autor określa zamierzone cele rozprawy oraz przedstawia jej strukturę. Rezultaty Autora zawarte są w rozdziałach 3, 4, 5 i 6. Rozprawę kończy rozdział 7 zawierający podsumowanie i wnioski. Rezultaty prezentowane w pracy (rozdziały: 3,4 i 5) były prezentowane na międzynarodowych konferencjach oraz opublikowane w materiałach pokonferencyjnych w serii LNCS Proceedings.

Merytoryczną część rozprawy otwiera rozdział 3. Autor wykorzystując konstrukcję ciągu automatów o n stanach zaproponowaną przez P. Martyugina w pracy
P.V. Martyugin, Careful Synchronization of Partial Automata with Restricted Alphabets, Proceedings LNCS, 2013,
redukuje liczność alfabetu nad którym określone są te automaty, zachowując długość słowa c-synchronizującego ustalonego przez P. Martyugina. Następnie Autor rozważa rodzinę automatów określoną nad alfabetem o ustalonej liczności, w której każdy odpowiada określonemu podziałowi liczby n (n jest liczbą stanów automatu). Rezultaty wpisują się we wcześniejsze prace z tej tematyki, na przykład:
de Bondt, M., Don, H. M., & Zantema, H. Lower bounds for synchronizing word lengths in partial automata, International Journal of Foundations of Computer Science, 30(1), 2019.
Brakuje porównania uzyskanych rezultatów z rozprawy z zastanymi, na przykład z cytowaną powyżej pracą.
Usuwając z określonych automatów litery „c" (wraz z odpowiednimi przejściami) Autor formułuje Wniosek 2, który dotyczy automatów DFA synchronizowanych do podzbioru stanów S. Tu również brak odniesienia uzyskanego rezultatu do znanych wcześniej wyników.

W rozdziale 4 Autor rozważa deterministyczne automaty skończone z nakładającymi się cyklami. Definicja umieszczona na stronie 35 prowadzi do wątpliwości związanych z Obserwacją 2. Jeśli mianowicie przyjmiemy, że automat składa się z pełnego cyklu na zbiorze Q={1,…..,n} określonego przez literę a, oraz z cyklu (k,k+1) określonego przez literę b, to tak określony automat jest deterministyczny o nakładających się cyklach – zgodnie z definicją ze strony 35 (przecięcie A_a i S_b daje zbiór {k,k+1}, który dla litery a generuje ścieżkę k → k+1, a dla litery b ścieżkę k→k+1→k. Czy cykl jest ścieżką? Skierowaną ścieżką? Określenia przytoczone na stronie 16 i 17 nie rozstrzygają tego problemu. Być może problem wynika z nieprecyzyjnej definicji, być może Obserwacja 2 nie jest prawdziwa, być może należy dodać jakieś założenia.

Nieprawdziwy jest Lemat 2. Wystarczy ustalić dowolny, niepusty zbiór Z oraz przyjąć A_1=…..=A_k = Z i wtedy dla każdego podciągu B_1, ,,,,,, B_l warunek pustego przecięcia zbiorów B_i oraz B_j nie jest spełniony.

Lemat ten wykorzystany jest w dowodzie Lematu 5. Lemat 5 wykorzystywany jest w Lemacie 6. W konsekwencji powstaje wątpliwość co do poprawności dowodu Twierdzenia 6 i ewentualnej jego prawdziwości.

Wniosek 3 umieszczony na stronie 44 orzeka, że każdy automat z nakładającymi się cyklami ma własność synchronizacji. W świetle Twierdzenia 6 oznacza to, że dla automatu z nakładającymi się cyklami istnieje litera x oraz stany p,q, takie że p.x=q,x. Automat z nakładającymi się cyklami podany przez Autora na stronie 36 nie spełnia tego ostatniego warunku.

Wskazane problemy związane z rezultatami tego rozdziału powinny być przez Doktoranta wyjaśnione podczas obrony.

Rozdział kończy wynik dotyczący dolnego ograniczenia długości najkrótszego słowa synchronizującego w rodzinie automatów nakładającymi się cyklami, który jest bezpośrednim wykorzystaniem wyniku dla automatu V_5 (Rystsova) z pracy
F.Gonze, V.V. Gusev, R.M. Jungers, B. Gerencser, M.V. Volkov, On the Interplay Between Cerny and Babai's Conjectures, Int.Journal Found. Comput. Sci., 30, 2019

Znów brakuje tutaj porównania uzyskanych rezultatów z rozprawy z zastanymi, na przykład z zawartymi w pracy D. Stonera dla rodziny automatów F(p,k).
D. Stoner, On the Minimal Reset Words of Synchronizing Automata, MIT, Research Science Institute, July 30, 2014

W rozdziale 5 Autor rozważa problem c-synchronizacji dla automatów 1-klastrowych. Autor określa rodzinę jedno-klastrowych częściowych automatów i uzyskuje wykładnicze oszacowanie na najkrótsze słowo c-synchronizujące przy wykładniczo rosnącym rozmiarze alfabetu. Udowadnia także, iż rozstrzygniecie czy dany jedno klastrowy automat jest c-synchronizowalny jest NP trudne, nawet przy ograniczeniu rozważań do 2 elementowego alfabetu.
Problem synchronizacji (zwykłej) dla tej klasy automatów, określonej około roku 2010 przez M.- P. Bell, był rozważany wcześniej, a wyniki ustalone, na przykład w pracy
M-P. Béal, M.V. Berlinkov, D. Perrin,. A quadratic upper bound on the size of a synchronizing word in one-cluster automata. Intern. Journal of Foundations of Computer Science, 22, 2011.
Brakuje w rozprawie odniesienia się do rezultatów zawartych w powyższej pracy.

W rozdziale 6 podana jest propozycja kryptosystemu asymetrycznego działającego w oparciu o c-synchronizowalność. Propozycja ta jest na tyle ogólna, że trudno się obiektywnie do niej ustosunkować. Aby cokolwiek powiedzieć na temat tej propozycji, aby ją ocenić, czy też wskazać jakieś sugestie dalszego rozwoju należy przeprowadzić choćby standardowe testy NIST.

Oceniając rozprawę z punktu widzenia matematyka muszę stwierdzić, że, niestety, brakuje jej tzw. rygoru matematycznego. Czyta się ją w związku z tym ciężko. Definicje przedstawiane są opisowo i nieprecyzyjnie, co w rezultacie prowadzi do pewnych niejednoznaczności w interpretacji tez Autora oraz wielokrotnie wymusza konieczność szukania bardziej precyzyjnych określeń w literaturze. Pewne pojęcia czy obiekty matematyczne wprowadzane są z pominięciem koniecznych informacji na przykład o oznaczeniach. Permanentnie Autor definiując zbiory potrzebne do prowadzenia rozważań pomija zakresy warunków (funkcji zdaniowych) okreslających te zbiory. Lematy i twierdzenia częstokroć formułowane są bez odpowiednich założeń.

Gdyby była to rozprawa doktorska w dziedzinie nauk ścisłych (dyscyplina: matematyka lub informatyka) sugerowałbym jej istotną korektę. Ponieważ jednak Autor broni rozprawę w dziedzinie nauk inżynieryjno-technicznych przychylam się do dopuszczenia go do dalszych etapów postępowania. Równocześnie podkreślam, że oczekuję od Autora rozprawy wyjaśnień dotyczących wskazanych w recenzji błędów w rozprawie i ich konsekwencji.

Reasumując, stwierdzam, że recenzowana rozprawa doktorska Pana mgr Jakuba Ruszila pod tytułem Synchronization of Finite Automata – Problems and Generalizations" spełnia wymagania zawarte w ustawie z dnia 14 marca 2003 roku (wraz z późniejszymi zmianami) "O stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (Dz.U. Nr 65, poz. 595)" i stawiam wniosek o przyjęcie przedłożonej rozprawy doktorskiej i dopuszczenie mgr Jakuba Ruszila do dalszych etapów postępowania o nadanie stopnia doktora w dyscyplinie: informatyka techniczna i telekomunikacja.