Gdańsk, 5 maja 2025

dr hab. inż. Jan Daciuk
Katedra Inteligentnych Systemów Interaktywnych
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska
Ul. Gabriela Narutowicza 11/12
80-233 Gdańsk

RECENZJA ROZPRAWY DOKTORSKIEJ
mgr Jakuba Ruszila
pt. „Synchronization of Finite Automata — Problems and Generalizations"

Podstawa formalna recenzji

Opinię przygotowano w związku z powołaniem na recenzenta uchwałą Rady Dyscypliny Informatyki Technicznej i Telekomunikacji Uniwersytetu Jagiellońskiego z dnia 26 września 2024 roku. Recenzję przygotowano zgodnie z kryteriami stawianymi rozprawom doktorskim w Ustawie — Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2023 r., poz. 742, 1088).

Problematyka i cel rozprawy

Rozprawa doktorska mgr Jakuba Ruszila poświęcona jest problemom znajdowania słów synchronizujących pewien szczególny rodzaj automatów skończonych, w których nie są wyróżnione stan początkowy i stany końcowe. W moim opisie zmuszony jestem przetłumaczyć na język polski pojęcia, z którymi spotykałem się dotąd wyłącznie w języku angielskim, dlatego w przypadkach wątpliwych umieszczam oryginalne nazwy pojęć w języku angielskim w nawiasach. Celem pracy według Autora jest:

1. Zbadanie wpływu rozmiaru alfabetu na długość słów ostrożnie synchronizujących (ang. *carefully synchronizing*), które są odpowiednikami słów synchronizujących dla automatów z częściowo zdefiniowaną funkcją przejść.

2. Wprowadzenie nowej nietrywialnej klasy deterministycznych automatów skończonych z kwadratową górną granicą długości najkrótszego słowa synchronizującego.

3. Rozszerzenie pojęcia automatów z pojedynczym klastrem na automaty z częściowo zdefiniowaną funkcją przejścia, zbadania krańcowych właściwości ich ostrożnie synchronizujących słów i zajęcie się złożonością ustalenia, czy takie automaty posiadają własność ostrożnej synchronizacji.

4. Zbadanie możliwości zaprojektowania asymetrycznego systemu kryptograficznego używającego pojęcia synchronizacji automatów.

Tezy pracy nie zostały wyraźnie przedstawione w jednym miejscu. Można je wywnioskować z analizy podsumowań na końcach niektórych rozdziałów (konkretnie rozdziałów 3 i 4) oraz rozdziału wniosków, który jednak w większej części tekstu odsyła do wyników przedstawionych w poszczególnych rozdziałach. Do wyników pracy należy zaliczyć:

1. Podanie przepisu na automaty z asymptotycznie taką długością co konstrukcja Martyugina, ale ze zmniejszoną liczbą symboli alfabetu.

2. Przedstawienie nowej klasy automatów z zachodzącymi na siebie pętlami i udowodnienie kwadratowej górnej granicy dla ich słów synchronizujących.

3. Rozszerzenie pojęcia automatów skończonych z pojedynczym klastrem na automaty skończone z częściowo zdefiniowaną funkcją przejść. Autor dowodzi, że problem ustalenia, czy taki automat z binarnym alfabetem posiada słowo ostrożnie synchronizujące jest NP-trudny.

4. Szkic zastosowania automatów z częściowo zdefiniowaną funkcją przejść do kryptografii.

Wyniki zostały też opublikowane w następujących artykułach konferencyjnych:

1. J. Ruszil. Some Results Concerning Careful Synchronization of Partial Automata and Subset Synchronization of DFA's. In Pascal Caron and Ludovic Mignot, editors, *Implementation and Application of Automata - 26th International Conference, CIAA 2022, Rouen, France, June 28 - July 1, 2022, Proceedings*, volume 13266 of Lecture Notes in Computer Science, pages 106–115. Springer, 2022.

2. J. Ruszil. Synchronizing Automata with Coinciding Cycles. In Frank Drewes and Mikhail Volkov, editors, *Developments in Language Theory - 27th International Conference, DLT 2023, Umeå, Sweden, June 12-16, 2023, Proceedings*, volume 13911 of Lecture Notes in Computer Science, pages 208–218. Springer, 2023.

3. J. Ruszil. Careful Synchronization of One-Cluster Automata. In Joel D. Day and Florin Manea, editors, *Developments in Language Theory - 28th International Conference, DLT 2024, Göttingen, Germany, August 12-16, 2024, Proceedings*, volume 14791 of Lecture Notes in Computer Science, pages 252–265. Springer, 2024.

Obie konferencje są dobrze znane wśród osób zajmujących się automatami skończonymi i dobrze oceniane. Ministerstwo oceniło je na 70 punktów i zakwalifikowało do właściwej dziedziny. Należy podkreślić, że Jakub Ruszil jest jedynym autorem tych publikacji.

Ocena merytoryczna rozprawy

Rozprawa doktorska mgr Jakuba Ruszila liczy 82 strony, w tym 68 stron tekstu i składa się z siedmiu numerowanych rozdziałów, poprzedzonych podziękowaniami i zakończonym wykazem źródeł. Rozdział 1 wprowadza w tematykę rozprawy, rozdziały 2 do 5 i częściowo 6 zawierają wyniki badań teoretycznych, rozdział 7 zawiera wnioski.

Mgr Jakub Ruszil zajął się głównie problemem znajdowania słów synchronizujących, w tym także dla automatów z częściowo zdefiniowaną funkcją przejść. Badał takie konstrukcje automatów, dla których synchronizacja wymagała słów synchronizujących o zadanych ograniczeniach długości. Rozszerzył znane już problemy na nowe klasy automatów, w szczególności automaty z częściowo zdefiniowaną funkcją przenoszenia, automaty z pojedynczym klastrem, czy automaty z nakładającymi się pętlami.

Prace przeprowadzono zgodnie z metodyką i metodologią badań obowiązującą w informatyce rozumianej jako poddziedzina matematyki. Autor potrafi formalnie definiować problemy, znajdować ich rozwiązania i dokonywać ich dowodów posługując się sprowadzaniem do sprzeczności czy wykazując równoważność danego problemu z innym, znanym problemem. Rozprawa Autora świadczy o właściwej ogólnej wiedzy autora z zakresu matematyki i informatyki, a także o dobrej znajomości zagadnień, którymi się zajmuje w rozprawie.

Przedstawione wyniki mają charakter teoretyczny. Wszystkie twierdzenia i lematy posiadają dowody. Zostały opublikowane w recenzowanych materiałach renomowanych konferencji dotyczących automatów skończonych, a więc zostały poddane ocenie specjalistów w wąskiej dziedzinie, którą zajmuje się Autor. Zastosowana metodologia jest poprawna w matematyce.

Rozdział szósty zawiera propozycję metody szyfrowania i odszyfrowania wiadomości. Jest to tylko szkic, który nie jest jeszcze rozwiązaniem praktycznym. Do jego zastosowania potrzeba wielu analiz. Właściwie taka propozycja powinna być opracowana we współpracy

z osobami zajmującymi się kryptografią lub poddana ocenie przez specjalistów z zakresu kryptografii, na przykład przez zgłoszenie jej do publikacji w czasopiśmie z tej dziedziny.

W przedstawionej rozprawie mgr Ruszil nie wspomina ani słowem o tym, jak doszedł do przedstawionych rozwiązań. Jako informatyk, który nie jest matematykiem, oczekiwałbym, że odbyło się to z wykorzystaniem technik informatycznych. Żmudne rozmyślania nad różnymi konstrukcjami automatów o pożądanych właściwościach można zastąpić i usprawnić pisząc programy, które dokonają takich poszukiwań według zadanych kryteriów, a także zweryfikują ich właściwości. Jeżeli tak rzeczywiście było, to rozprawa powinna zawierać opisy takich programów i odsyłać do repozytorium, z którego można by było je pobrać. Niczego takiego w rozprawie nie znalazłem i czuję się zawiedziony.

Niestety w pracy pojawiają się błędy, które utrudniają jej analizę. Duży stopień jej sformalizowania powoduje, że trudno jest wówczas dociec, co konkretnie na myśli miał autor i do czego dążył. Jest to szczególnie uciążliwe, kiedy błędy w przykładach (lub w definicjach) naruszają powiązania, które te przykłady miały ilustrować.

Praca zawiera tylko trzy algorytmy zdefiniowane formalnie. Algorytm numer 3 jest poprawny. Algorytm numer 2 jest trywialny i umieszczenie go w pracy formalnie jako algorytmu nie było konieczne; do tego wystarczyłby zwykły opis słowny. Natomiast algorytm numer 1 jest niepoprawny. Wiersze numer 4 i 5 powinny być połączone tworząc pojedynczy wiersz. Para stanów określona w wierszu 4 powinna spełniać warunek określony w następnym wierszu. Nie jest to wyłącznie pomyłka redakcyjna — wiersze są numerowane, co w systemie składu tekstu LaTeX, za pomocą którego złożono rozprawę, wymaga jawnego określenia, czy kolejne wiersze tworzą jedno polecenie.

Na następnej stronie rozprawy, stronie numer 17, znajdujemy definicję odwołującą się do izomorfizmu grafów. To pojęcie jest zdefiniowane na następnej stronie. Pojęcia typu permutacji i rzędu permutacji wprowadzone na stronie numer 33 ani nie są zdefiniowane w pracy, ani nie ma w niej odwołania do ich definicji w literaturze. Jest to tym bardziej irytujące, że są to pojęcia spoza teorii automatów.

Lemat numer 2 na stronie 37 nie jest prawdziwy bez dodatkowego założenia, które nie jest jawnie podane. Niestety także dowód wykorzystuje to niejawne założenie, więc nie dostarcza wskazówki, co dokładnie Autor miał na myśli. Ten lemat jest używany dalej w ciągu dowodów, co skutecznie utrudnia ich analizę.

W obserwacji numer 3 na stronie 46 warto było podać, że C jest podzbiorem stanów, $C \subseteq Q$. W dowodzie na następnej stronie czytelnik musi sam się domyślić, że m jest rozmiarem zbioru S, czyli $m = |S|$. Czy nie można było tego podać jawnie?

Na tej samej stronie zaczyna się definicja, która wręcz uniemożliwia dalszą analizę. W ostatnim wierszu strony mamy $\delta_k(c_n, a) = c_1$. W poprzednim wierszu funkcja δ_k jest zdefiniowana dla c_i przy $i < k$. Sugeruje to, że zamiast c_n powinno być tam c_k. Jednak wartość n jest zarówno użyta wcześniej w tej definicji, jak i występuje w lemacie numer 10. Czy zamiast $\frac{n}{2}$ nie można tam było napisać k? Na szczęście definicja opatrzona jest przykładem na rysunku numer 18. Przedstawiony tam automat pozbawiony jest pętli. Bezpośrednio pod rysunkiem definiowany jest zbiór T_k. Litera T jest w nim użyta w trzech różnych znaczeniach, w zależności od czcionki i indeksu. Zbiór jest tworzony w sposób, który algorytmicznie wymagałby trzech poziomów zagnieżdżeń. Można go uprościć pozbywając się jednego z tych poziomów. Opis słowny tego zbioru zupełnie niczego nie wyjaśnia.

W lemacie numer 12 na stronie 52 $n + 3$ powinno moim zdaniem być w rzeczywistości $n+2$, ponieważ ścieżka od $\overline{c}_i^{x_1}$ do $\overline{c}_i^{x_n}$ ma długość $n-1$. Dotyczy to także dalszych rozważań.

Rozdział szósty zaczyna się od bardzo ogólnego, wręcz filozoficznego wprowadzenia do kryptografii. Po nim następuje bezpośrednio nagły przeskok do propozycji nowej metody szyfrowania. Moim zdaniem ten przeskok jest zbyt nagły, a proponowana metoda tajnego przekazania wiadomości powinna być wcześniej naszkicowana słownie, tak aby dać czytelnikowi wskazówkę, do czego zmierza Autor. Analizy nie ułatwia fakt, że automat oznaczony jako „a" z rysunku 20 do przykładu nie wydaje się być ostrożnie synchronizowany za pomocą słowa *aba*. W szczególności, do którego stanu prowadzi funkcja $\delta(3, aba)$? Na stronie 65, w

opisie algorytmu odszyfrowania wiadomości użyty jest symbol u, który nie został wcześniej zdefiniowany. Przypuszczalnie jest tożsamy ze słowem synchronizującym w, ale zarówno w jak i u są użyte obok siebie w tej definicji i w następnych, przy czym u wyłącznie jako $|u|$. Wcześniej to słowo było podane także jako jawny tekst p będący ciągiem etykiet na przejściach pomiędzy automatami składowymi.

Dobór i wykorzystanie literatury

Cytowana literatura liczy 57 pozycji, w większości artykułów w renomowanych czasopismach lub w materiałach renomowanych konferencji naukowych. Odnosi się prawie w całości do automatów skończonych. tylko pięć pozycji traktuje o kryptografii, w tym tylko jeden o zastosowaniu automatów skończonych w kryptografii. Tymczasem literatura na ten szczególny temat jest dużo bogatsza i moim zdaniem powinna być w rozprawie zacytowana przy porównaniu proponowanej metody do innych metod stosujących automaty skończone.

Oprócz pozycji w języku angielskim, Autor cytuje prace w trzech innych językach: francuskim (dwie prace), niemieckim i czeskim.

Sposób formatowania wykazu źródeł jest ogólnie właściwy i wynika bezpośrednio z zastosowanego stylu systemu LaTeX, jednak w niektórych miejscach można spotkać pewne niedociągnięcia:

- w pozycji [1] brakuje roku
- w pozycji [19] brakuje nazwy publikacji i wydawnictwa
- w pozycji [43] brakuje nazwy publikacji

Struktura rozprawy, poprawność językowa i redakcyjna

Ogólna struktura rozprawy jest właściwa i nie odbiega od standardu. Można jednak mieć zastrzeżenia co do wniosków, które powinny być bardziej szczegółowe. Używanie pojęć przed ich zdefiniowaniem (izomorficzność grafów) i dość częste odsyłanie do literatury zamiast opisu konkurencyjnych rozwiązań nie jest dobrą praktyką.

Ze względu na bardzo wysoki stopień sformalizowania rozprawy, powinna ona zawierać słownik pojęć, słownik oznaczeń i skorowidz. Ich brak czyni lekturę pracy mało wygodną i zmusza do częstych poszukiwań, w tym do poszukiwań przed ekranem komputera, który nie zawsze jest w zasięgu czytelnika.

Język pracy nie budzi żadnych zastrzeżeń. W odróżnieniu od np. przykładowych rysunków, Autor szczególnie starannie przyłożył się do korekty tekstu, nie widać też bezpośredniego przenoszenia polskich konstrukcji składniowych lub stałych związków frazeologicznych do angielskiego. Znalazłem jedną literówkę: na stronie 8 „conferene" zamiast „conference". W sformułowaniu twierdzenia numer 11 kolejność fraz nie jest właściwa; zamiast „*constructs in polynomial time the carefully synchronizing automaton* A_ϕ" powinno być „*constructs the carefully synchronizing automaton* A_ϕ *in polynomial time*".

W redakcji pracy także widać dużą staranność, chociaż Autor nie ustrzegł się kilku błędów:

1. Na stronie 27 Autor używa sformułowania „*as presented in this paper*".
2. Na stronie 47 tuż przed punktem 5.1 słowo w' określone jest jako $a^l w(a^{m_1}w)_2^m$ zamiast $a^l w(a^{m_1}w)^{m_2}$
3. Na rysunku 19 na stronie 53 brak etykiety a na przejściach pomiędzy ze stanu r_2 do p_2 i ze stanu r_3 do stanu p_3.
4. Na stronie 55 $e_w(y_{k_1})$ jest powtórzone dwukrotnie zamiast użycia indeksów 2 i 3.

Podsumowanie

Znalezione pracy niedociągnięcia nie przeważają nad jej mocnymi stronami. Stanowi ona niewątpliwie indywidualne i oryginalne rozwiązanie problemu naukowego, stanowi świadectwo dużej wiedzy teoretycznej Kandydata z zakresu matematyki i informatyki w ogólności, a teorii automatów w szczególności, potwierdzone wystąpieniami na czołowych konferencjach z dziedziny teorii automatów. Wnoszę o dopuszczenie rozprawy doktorskiej mgr Jakuba Ruszila do publicznej obrony. Zauważone błędy i przede wszystkim brak towarzyszącego oprogramowania powstrzymują mnie przed zgłoszeniem wniosku o wyróżnienie.