

Metody minimalizacji automatów kwantowych

mgr inż. Olga Siedlecka

olga.siedlecka@icis.pcz.pl

Instytut Informatyki Teoretycznej i Stosowanej
Politechnika Częstochowska

18 września 2008 roku



Plan prezentacji

- Wprowadzenie
- Cel pracy
- Plan pracy
- Automaty skończone
- Minimalizacja jednokierunkowego skończonego automatu kwantowego
- Minimalizacja dwukierunkowego skończonego automatu kwantowego
- Wyniki
- Podsumowanie

Wprowadzenie

- Historia komputerów kwantowych
- Technologie fizycznej realizacji komputera kwantowego
- Rozwój teorii obliczeń kwantowych
- Automaty skończone
- Związek automatów niedeterministycznych, probabilistycznych i kwantowych
- Problem minimalizacji automatów skończonych

Cel i zakres pracy

- Usystematyzowanie i ujednolicenie istniejących definicji automatów kwantowych
- Zdefiniowanie relacji bisymulacji i nierozróżnialności dla zbiorów stanów reaktywnego skończonego automatu probabilistycznego, jednokierunkowego skończonego automatu kwantowego oraz dwukierunkowego skończonego automatu kwantowego
- Minimalizacja automatów kwantowych wykorzystując metody klasyczne:
 - odrzucanie stanów nieosiągalnych, tj. stanów dla których prawdopodobieństwo osiągnięcia wynosi zero
 - łączenie stanów nierozróżnialnych (z wykorzystaniem relacji nierozróżnialności)
- Zbudowanie algorytmu minimalizacji dla wyżej wymienionych typów automatów

Plan pracy

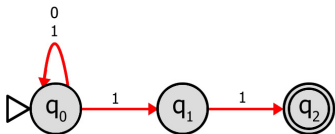
- Wprowadzenie
- Wybrane zagadnienia z teorii informacji kwantowej
- Wybrane zagadnienia z teorii automatów skończonych
- Minimalizacja automatów kwantowych
- Podsumowanie
- Bibliografia
- Streszczenie w języku angielskim
- Dodatki

Niedeterministyczny automat skończony

Definicja NFA

Niedeterministycznym automatem skończonym - nazywamy piątkę $NFA = (Q, \Sigma, \delta, q_0, F)$, gdzie:

- Q - skończony zbiór stanów, $\#Q < \infty$,
- Σ - alfabet wejściowy,
- δ - funkcja przejść $\delta : Q \times (\Sigma \cup \{\epsilon\}) \mapsto 2^Q$,
- $q_0 \in Q$ - stan początkowy,
- $F \subseteq Q$ - zbiór stanów końcowych (akceptujących).



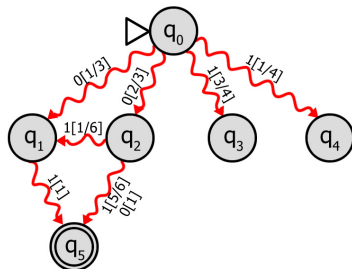
Reaktywny automat probabilistyczny

Definicja PA

Skończony reaktywny automat probabilistyczny - to piątka

$PA = (Q, \Sigma, \delta, q_0, F)$, w której:

- Q - skończony zbiór stanów,
 $\#Q < \infty$,
- Σ - alfabet wejściowy,
- δ - funkcja prawdopodobieństwa przejść $\delta : Q \times \{\Sigma \cup \{\epsilon\}\} \mapsto \mathcal{D}(Q)$.
- $q_0 \in Q$ - stan początkowy,
- $F \subseteq Q$ - zbiór stanów końcowych (akceptujących).



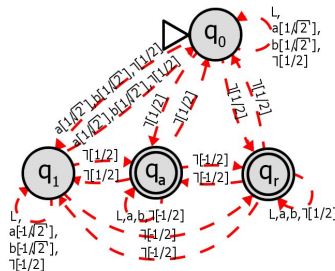
Jednokierunkowy automat kwantowy

Definicja 1QFA

Jednokierunkowy automat kwantowy to szóstka

$1QFA = (Q, \Sigma, \delta, q_0, Q_a, Q_r)$, w której:

- Q - skończony zbiór stanów,
- Σ - alfabet wejściowy,
- δ - funkcja przejść $\delta : Q \times \Gamma \times Q \mapsto \mathbb{C}$,
- $q_0 \in Q$ - stan początkowy,
- $Q_a \subset Q$ - zbiór stanów końcowych, akceptujących,
- $Q_r \subset Q$ - zbiór stanów końcowych, odrzucających.



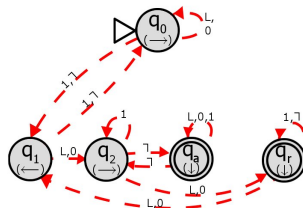
Dwukierunkowy automat kwantowy

Definicja 2QFA

Dwukierunkowy automat kwantowy

to krotka $1QFA = (Q, \Sigma, \delta, D, q_0, Q_a, Q_r)$,
w której:

- Q - skończony zbiór stanów,
- Σ - alfabet wejściowy,
- δ - funkcja przejść
 $\delta : Q \times \Gamma \times Q \times D \mapsto \mathbb{C}$,
- D - zbiór kierunków przesunięcia głowicy po taśmie $\{\leftarrow, \downarrow, \rightarrow\}$,
 pomocniczo $\mathcal{D} : Q \mapsto \{\leftarrow, \downarrow, \rightarrow\}$,
- $q_0 \in Q$ - stan początkowy,
- $Q_a \subset Q$ - zbiór stanów końcowych, akceptujących,
- $Q_r \subset Q$ - zbiór stanów końcowych, odrzucających.



Relacja równoważności

Definicja

Niech dany będzie dowolny jednokierunkowy skończony automat kwantowy $1QFA = (Q, \Sigma, q_0, \delta, Q_a, Q_r)$. Przy zadanym alfabecie taśmy Γ , dla $\sigma \in \Gamma$, V_σ będzie unitarnym operatorem w przestrzeni Hilberta $l_2(Q)$ - $V_\sigma(|q\rangle) = \sum_{q' \in Q} \delta(q, \sigma, q')|q'\rangle$. Dla danego V_σ zdefiniowane będzie v_σ równe odpowiednio: $v_\sigma[Q] = \sum_{q' \in Q} |\delta(q, \sigma, q')|^2$, $v_\sigma[S] = \sum_{q' \in S} |\delta(q, \sigma, q')|^2$, (suma kwadratów wartości bezwzględnych amplitud), gdzie $S \subseteq Q$.

Definicja

Niech R będzie relacją równoważności na zbiorze S , A dowolnym zbiorem, zaś $V_1, V_2 \in l_2(S)$ będą unitarnymi operatorami odpowiadającymi przekształceniom układów kwantowych. Wówczas:

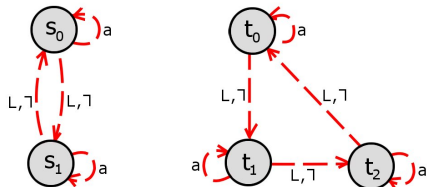
$$V_1 \equiv_{R,A} V_2 \iff \forall C \in S/R, \forall a \in A : v_{1a}[C] = v_{2a}[C]. \quad (1)$$

Relacja bisymulacji

Definicja

Niech $1QFA_1 = (S, \Sigma, \delta)$ i $1QFA_2 = (T, \Sigma, \delta)$ będą dwoma skończonymi jednokierunkowymi automatami kwantowymi, wtedy istnieje **relacja silnej bisymulacji** $R \subseteq S \times T$, jeżeli dla wszystkich par $(s, t) \in R$ i dla wszystkich $\sigma \in \Sigma$ spełniony jest warunek:

- jeżeli $V1_\sigma(|s\rangle) = \sum_{s' \in S} \delta(s, \sigma, s')|s'\rangle$ wtedy istnieje $V2_\sigma(|t\rangle) = \sum_{t' \in T} \delta(t, \sigma, t')|t'\rangle$ takie, że $V1 \equiv_{R, \Sigma} V2$.



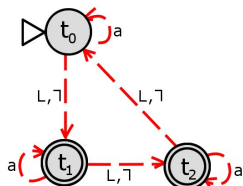
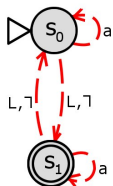
Relacja nierozróżnialności I

Definicja

Niech $1QFA_1 = (S, \Sigma, \delta, s_0, S_a, S_r)$ i $1QFA_2 = (T, \Sigma, \delta, t_0, T_a, T_r)$ będą dwoma skończonymi jednokierunkowymi automatai kwantowymi, gdzie zbiory: $S_n = S \setminus (S_a \cup S_r)$ i $T_n = T \setminus (T_a \cup T_r)$ zawierają stany niewstrzymujące, wtedy istnieje **relacja nierozróżnialności** $N \subseteq S \times T$, jeżeli dla wszystkich par $(s, t) \in N$ i dla wszystkich $\sigma \in \Sigma$ spełnione są warunki:

- $(s, t) \in N^0$, wtedy i tylko wtedy, gdy $(s \in S_a \wedge t \in T_a) \vee (s \in S_r \wedge t \in T_r) \vee (s \in S_n \wedge t \in T_n)$,
- $(s, t) \in N^k$, wtedy i tylko wtedy, gdy $(s, t) \in N^{k-1}$ oraz
 - jeżeli $V1_\sigma(|s\rangle) = \sum_{s' \in S} \delta(s, \sigma, s')|s'\rangle$ wtedy istnieje $V2_\sigma(|t\rangle) = \sum_{t' \in T} \delta(t, \sigma, t')|t'\rangle$ takie, że $V1 \equiv_{R, \Sigma} V2$.

Relacja nierozróżnialności II



Automat ilorazowy

Twierdzenie

Relacja nierozróżnialności N jest kongruencją w zbiorze stanów automatu $1QFA = (Q, \Sigma, \delta, q_0, Q_a, Q_r)$ względem odpowiadającej mu funkcji przejść δ .

Twierdzenie

Ponieważ relacja nierozróżnialności N na zbiorze stanów automatu $1QFA = (Q, \Sigma, \delta, q_0, Q_a, Q_r)$ względem jego funkcji przejść jest kongruencją, to istnieje automat ilorazowy

$1QFA/N = (Q/N, \Sigma, \delta/N, [q_0]_N, Q_{a/N}, Q_{r/N})$ będący minimalnym automatem skończonym akceptującym ten sam język L_{1QFA} , co automat wejściowy (gdzie dla $\delta/N([q]_N, \sigma, [q']_N)$ jest określony operator $V1$, dla $[\delta(q, \sigma, q')]_N$ jest określony operator $V2$ i ma miejsce $V1 \equiv_{R, \Sigma} V2$).

Minimalizacja 1QFA

Definicja

Automat skończony nazywa się minimalnym jeżeli wszystkie stany tego automatu są parami nierównoważne względem relacji nierozróżnialności.

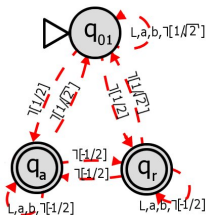
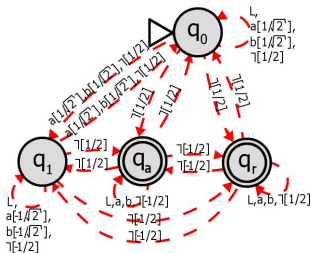
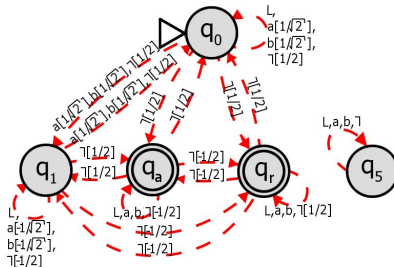
Twierdzenie

Automat A rozpoznający język L jest automatem **minimalnym**, gdy nie istnieje automat o mniejszej liczbie stanów rozpoznający L

Minimalizacja kwantowego automatu skończonego składa się z:

- wyeliminowania stanów nieosiągalnych (po wyjściu ze stanu początkowego),
- złączenia stanów nierozróżnialnych.

Przykład minimalizacji 1QFA

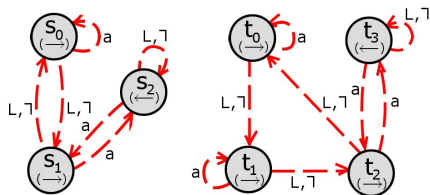


Relacja bisymulacji

Definicja

Niech $2QFA_1 = (S, \Sigma, \delta, \mathcal{D})$ i $2QFA_2 = (T, \Sigma, \delta, \mathcal{D})$ będą dwoma skończonymi dwukierunkowymi automatami kwantowymi ($\mathcal{D}$ jest funkcją określającą kierunek przesunięcia po taśmie dla danego stanu), wtedy istnieje **relacja silnej bisymulacji** $R \subseteq S \times T$, jeżeli dla wszystkich par $(s, t) \in R$ i dla wszystkich $\sigma \in \Sigma$ spełnione jest:

- jeżeli $V1_\sigma(|s\rangle) = \sum_{s' \in S} \delta(s, \sigma, s', d)|s'\rangle$ wtedy istnieje $V2_\sigma(|t\rangle) = \sum_{t' \in T} \delta(t, \sigma, t', d)|t'\rangle$ takie, że $V1 \equiv_{R, \Sigma} V2$ i $\mathcal{D}(s) = \mathcal{D}(t)$.



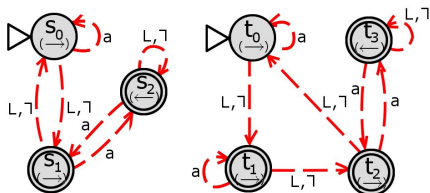
Relacja nierozróżnialności I

Definicja

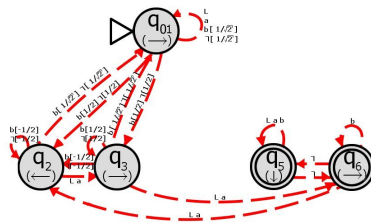
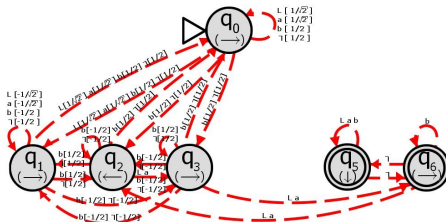
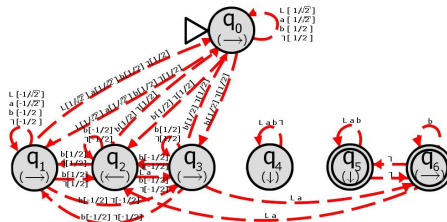
Niech $2QFA_1 = (S, \Sigma, \delta, \mathcal{D}, s_0, S_a, S_r)$ i $2QFA_2 = (T, \Sigma, \delta, \mathcal{D}, t_0, T_a, T_r)$ będą dwoma skończonymi dwukierunkowymi automatai kwantowymi, zbiory $S_n = S \setminus (S_a \cup S_r)$ i $T_n = T \setminus (T_a \cup T_r)$ zawierają stany niewstrzymujące, wtedy istnieje **relacja nierozróżnialności** $N \subseteq S \times T$, jeżeli dla wszystkich par $(s, t) \in N$ i dla wszystkich $\sigma \in \Sigma$ spełnione są warunki:

- $(s, t) \in N^0$, wtedy i tylko wtedy, gdy $(s \in S_a \wedge t \in T_a) \vee (s \in S_r \wedge t \in T_r) \vee (s \in S_n \wedge t \in T_n)$,
- $(s, t) \in N^k$, wtedy i tylko wtedy, gdy $(s, t) \in N^{k-1}$ oraz
 - jeżeli $V1_\sigma(|s\rangle) = \sum_{s' \in S} \delta(s, \sigma, s', d) |s'\rangle$ wtedy istnieje $V2_\sigma(|t\rangle) = \sum_{t' \in T} \delta(t, \sigma, t', d) |t'\rangle$ takie, że $V1 \equiv_{R, \Sigma} V2$ i $\mathcal{D}(s) = \mathcal{D}(t)$.

Relacja nierozróżnialności II



Minimalizacja 2QFA



Wyniki I

- Zestawienie, usystematyzowanie i ujednolicenie wiedzy na temat istniejących typów automatów kwantowych, poparte przykładami
- Zdefiniowanie relacji nierozróżnialności jako relacji kongruencji dla reaktywnego probabilistycznego automatu skończonego PA, dowód istnienia automatu ilorazowego jako automatu minimalnego
- Zdefiniowanie relacji bisymulacji oraz relacji nierozróżnialności jako relacji kongruencji dla jednokierunkowego skończonego automatu kwantowego 1QFA, dowód istnienia automatu ilorazowego jako automatu minimalnego
- Zdefiniowanie relacji bisymulacji, oraz relacji nierozróżnialności jako relacji kongruencji dla dwukierunkowego skończonego automatu kwantowego 2QFA, dowód istnienia automatu ilorazowego jako automatu minimalnego

Wyniki II

- Opracowanie metod minimalizacji PA, 1QFA, 2QFA wraz z algorytmami:
 - wykluczenia stanów nieosiągalnych – o złożoności $O(|\Sigma|n^2)$ ($|\Sigma|$ – liczba symboli w alfabecie, n – liczba stanów w automacie)
 - złączenia stanów nierozróżnialnych – o złożoności $O(|\Sigma|n^3)$
- dla każdego z algorytmów dowiedziono poprawności, przeanalizowano czas działania i podano przykłady
- Wyniki pracy opublikowano w czasopismach i materiałach konferencyjnych: [3], [1], [4], [2], [5]

Podsumowanie

- Zastosowanie metod minimalizacji
- Dalsze kierunki badań:
 - Opracowanie algorytmów o mniejszej złożoności
 - Opracowanie algorytmów dla pozostałych typów automatów kwantowych
 - Minimalizacja poprzez ograniczenie przestrzeni stanów
 - Symulacja automatów kwantowych przez probabilistyczne
 - Języki akceptowane przez automaty kwantowe

Publikacje I



KRYVYI, S., MATVEYEVA, L., LUKIANOVA, E., AND SIEDLECKA, O.

Ontologiczne spojrzenie na teorię automatów.

In *Proc. of 13-th International Conference KDS-2007 (Knowledge-Dialog-Solution)* (Sofia, 2007), vol. 2, pp. 427-436.



KRYVYI, S., MATVEYEVA, L., LUKIANOVA, E., AND SIEDLECKA, O.

Ontology view on automata theory.

International Journal Information Theories and Applications 15, 4 (2008), 337-344.



SIEDLECKA, O.

A brief overview of quantum computing theory.

Computing, Multimedia and Intelligent Techniques 2, 1 (2006), 35-44.



SIEDLECKA, O.

Algorytm minimalizacji jednokierunkowego, skończonego automatu kwantowego.

In *FCCS 2008, 4th Polish and International PD Forum-Conference on Computer Science* (2008).
CD-ROM.



SIEDLECKA, O.

Minimization of reactive probabilistic automata.

In *International Book Series Information Science and Computing - Algorithmic and Mathematical Foundations of the Artificial Intelligence* (2008), no. 1, ITNEA, pp. 75-80.

Odpowiedzi na pytania recenzentów I

dr hab. inż. Domański, prof. P.Cz

- Różnice w opisach pozycji literaturowych pojawiły się w związku ze stosowaniem latex'a do edycji pracy i tzw. bibtex'a do bibliografii, który posiada różne style. Ten który wybrałam (ACM) różnie oznacza artykuły, książki, czy materiały konferencyjne. Pozycja literaturowa 48 jest e-printem i nie zwróciłam uwagi, że dla tego typu publikacji wybrany styl nie określa formatowania.
- Pozycja 35, czyli praca Einstein'a Podolskiego i Rosena z 1935 roku jest dostępna w Internecie w postaci skanu artykułu.

Odpowiedzi na pytania recenzentów II

prof. dr hab. Jakub Rembieliński

- W podrozdziale 5.7 podaje dwa przykłady języków akceptowanych przez dwukierunkowy automat kwantowy, oraz przykład języka przez niego odrzucanego. Zwróciłam uwagę szczególnie na ten typ automatu, ponieważ akceptuje niektóre języki bezkontekstowe. Języki kwantowe oraz ich umiejscowienie w hierarchii jest obszerną dziedziną badań, której możnaby poświęcić cały doktorat, dlatego pozostawiam ten temat jako interesujący plan dalszych badań.
- Dla każdego typu automatu będzie istniała odrębnie zdefiniowana relacja równoważności, którą w wypadku omawianych automatów nazwałam relacją nierozróżnialności. Każda taka relacja będzie się musiała różnić definicją, bo różne będą własności różnych typów automatów, np. jeżeli jeden będzie miał tylko wejście, a drugi wejście i wyjście, jeden będzie reaktywny, a drugi generatywny itp. Poza tym



Odpowiedzi na pytania recenzentów III

istnieje jeszcze metoda minimalizacji nie korzystająca z relacji równoważności (Brzozowskiego).

- Podrozdział o tytule homomorfizm automatów skończonych (nie kwantowych) faktycznie zawiera odnośniki do niepublikowanych wykładów prof. Kryvyi'a, co jest niewystarczające, przepraszam za niedopatrzenie. Jednakże twierdzenia dotyczące równoważności stanów, epimorfizmu, homomorfizmu, izomorfizmu automatów skończonych, to twierdzenia powszechnie występujące, także w podręcznikach akademickich, często wraz z dowodami. Biorąc pod uwagę doświadczenia, by nie zamieszczać nie swoich, powszechnie znanych dowodów, chciałam uniknąć tego typu zastrzeżeń. Powinnam była dodać odnośniki także do innych pozycji literaturowych.

Odpowiedzi na pytania recenzentów IV

- Z twierdzenia 4.1.17 wynika, że nigdy dwa stany nie będą równoważne jeżeli jeden z nich należy do stanów akceptujących, a drugi do pozostałych. Często w literaturze taki stan rzeczy pozostawiony jest w domyśle, stąd i taka naleciałość u mnie. Faktycznie w definicji 4.1.37 można było to podkreślić.
- Relacje kongruencji mogą być zdefiniowane na wiele różnych sposobów, praca była wielokrotnie przeredagowywana, poszerzana i przycinana, najprawdopodobniej, w którymś momencie nie zauważyłam, że pozostawiłam dwie definicje.
- Znów wina przycinania i poszerzania, początkowo istniały jeszcze dodatkowe podrozdziały, które zostały uznane za zbyt podręcznikowe, stąd to co poprzednio było lematem, powinno być określone jako definicja.
- Błędy językowe prawdopodobnie wynikają ze zbyt dosłownego tłumaczenia przeze mnie prac anglojęzycznych.

Odpowiedzi na pytania recenzentów V

- Nastąpił błąd edytorski w obu wypadkach bibliografia powinna się odnosić do pozycji 53.