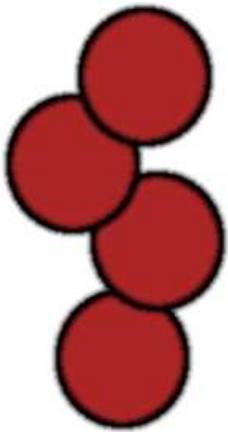


Klasyczne i kwantowe podejście do teorii automatów i języków formalnych

mgr inż. Olga Siedlecka

olga.siedlecka@icis.pcz.pl

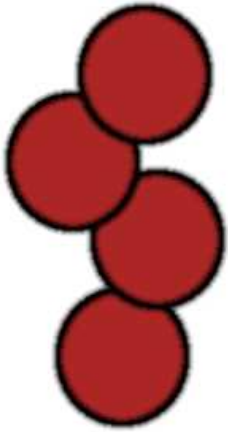
Zakład Informatyki Stosowanej i Inżynierii Oprogramowania
Instytut Informatyki Teoretycznej i Stosowanej
Politechnika Częstochowska



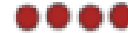
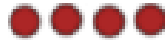
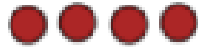
Plan seminarium



- Wstęp
- Definicje pomocnicze
- Klasyczna teoria automatów i języków formalnych
 - Symbol, alfabet, słowo, język
 - Automaty i ich odmiany
 - Algorytm minimalizacji automatu
- Kwantowa teoria automatów
 - Definicja automatu kwantowego
 - Kwantowe języki



Wstęp



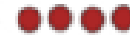
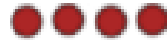
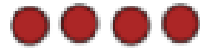
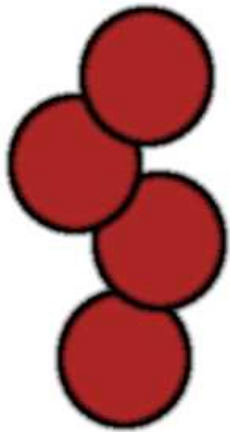
Zastosowanie automatów klasycznych.



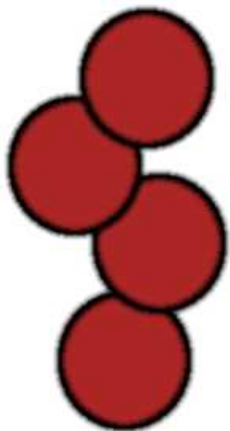
Nowe modele obliczeń.



Kwantowy model obliczeń.



Definicje pomocnicze



Przestrzeń Hilberta



Przestrzeń Hilberta - jest:



liniowa,



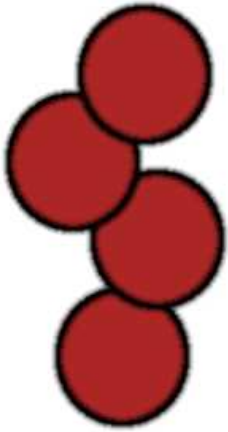
unormowana,



zupełna,



unitarna.



Macierz unitarna

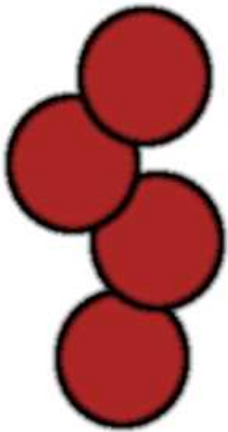


Macierzą unitarną nazywamy macierz kwadratową zespoloną U o rozmiarze $n \times n$ spełniającą własność:

$$U^*U = UU^* = I, \quad (1)$$

gdzie I jest macierzą jednostkową $n \times n$, a U^* oznacza macierz sprzężoną transponowaną (sprzężenie hermitowskie). Zauważmy, że własność ta oznacza, że macierz U posiada macierz odwrotną U^{-1} równą sprzężeniu hermitowskiemu jej samej, czyli:

$$U^* = U^{-1}. \quad (2)$$



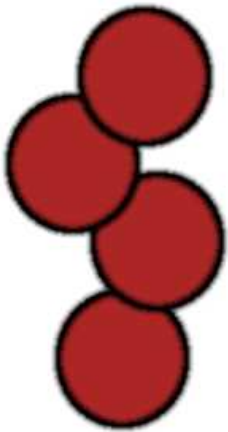
Mechanika kwantowa [1]



- W mechanice kwantowej stan n -poziomowego układu jest reprezentowany przez wektor jednostkowy w n -wymiarowej zespolonej przestrzeni wektorowej H_n , którą nazywamy **przestrzenią stanów** układu. Wybierzmy w przestrzeni stanów H_n bazę ortonormalną $\{|\mathbf{x}_1\rangle, |\mathbf{x}_2\rangle, \dots, |\mathbf{x}_n\rangle\}$. Wektory bazowe $|\mathbf{x}_i\rangle$ nazywamy **stanami bazowymi**.
- Dowolny stan układu kwantowego można przedstawić w postaci **superpozycji** stanów bazowych:

$$\alpha_1|\mathbf{x}_1\rangle + \alpha_2|\mathbf{x}_2\rangle + \dots + \alpha_n|\mathbf{x}_n\rangle \quad (3)$$

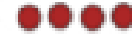
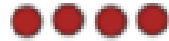
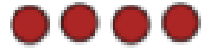
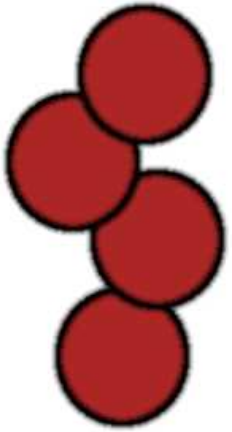
gdzie α_i są liczbami zespolonymi nazywanymi **amplitudami prawdopodobieństwa** względem wybranej bazy.



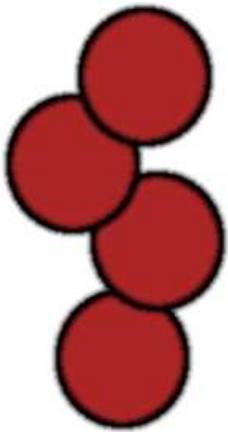
Mechanika kwantowa [2]



- Warunek unormowania wektora stanu wymaga, by spełniały one równanie $|\alpha_1|^2 + |\alpha_2|^2 + \dots + |\alpha_n|^2 = 1$. Prawdopodobieństwo zaobserwowania własności x_i wynosi $|\alpha_i|^2$.
- Jeżeli dwa układy kwantowe są opisywane za pomocą przestrzeni stanów H_n i H_m , to przestrzeń stanów układu złożonego opisana jest przez iloczyn tensorowy $H_n \otimes H_m$.
- Ewolucja czasowa układów kwantowych jest opisana za pomocą macierzy unitarnych.



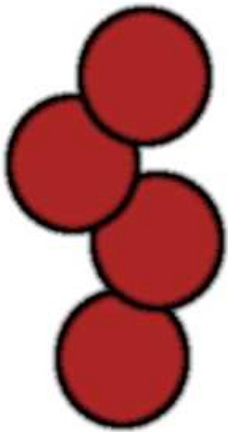
Klasyczna teoria automatów i języków formalnych



Symbol, alfabet, słowo [1]



- **Symbol** - pojęcie niedefiniowane (inaczej: litera, znak)
- **Alfabet** - skończony, niepusty zbiór symboli. Np.:
 - $\Sigma_1 = \{0, 1\}$ - alfabet binarny,
 - $\Sigma_2 = \{a, b, c, \dots, z\}$ - alfabet łaciński (małych liter)
- **Słowo**(łańcuch) - skończona sekwencja symboli z danego alfabetu. Np.: słowo 011101 jest słowem z alfabetu binarnego. Słowo puste (nie zawierające symboli) oznaczamy ε . Przez długość słowa rozumiemy liczbę pozycji w tym słowie i oznaczamy: $|w|$, np.: $|011101| = 6$ i $|\varepsilon| = 0$.



Symbol, alfabet, słowo [2]

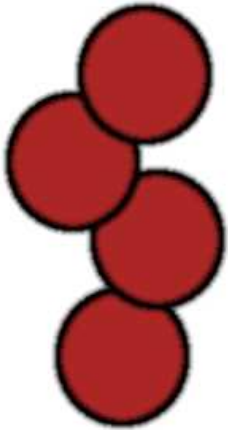


- **Konkatenacja słów** - niech $x = a_1a_2 \dots a_n$ i $y = b_1b_2 \dots b_m$ będą słowami, o długościach odpowiednio n i m , wtedy słowo $xy = a_1a_2 \dots a_nb_1b_2 \dots b_m$ o długości $n + m$ stanowi ich konkatenację.
- **Notacja potęgowa** - Jeżeli Σ jest alfabetem, wtedy Σ^k oznacza zbiór wszystkich słów o długości k , o symbolach z tego alfabetu. Zatem:

$$\Sigma = \{0, 1\}, \quad \Sigma^0 = \{\epsilon\}, \quad \Sigma^1 = \{0, 1\}, \quad \Sigma^2 = \{00, 01, 10, 11\} \dots \quad (4)$$

- Zbiór wszystkich słów nad alfabetem Σ oznaczamy Σ^* , zaś zbiór wszystkich niepustych słów Σ^+ . Np.:

$$\Sigma = \{0, 1\}, \quad \Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \dots, \quad \Sigma^* = \Sigma^+ \cup \{\epsilon\}. \quad (5)$$



Język



Język - Niech Σ będzie alfabetem, zaś Σ^* zbiorem wszystkich słów nad tym alfabetem, wtedy dowolny jego podzbiór $L \subseteq \Sigma^*$ nazywamy językiem nad alfabetem Σ . Np.: język polski nad alfabetem polskim, język C++, czy inne języki programowania nad alfabetem zawierającym znaki ASCII itp.

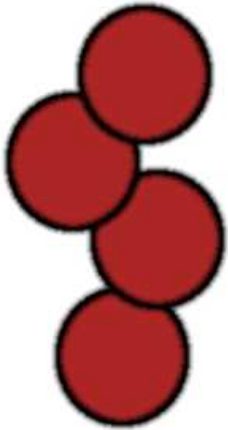
$$L_0 = \emptyset \quad (6)$$

$$L_1 = \{\epsilon\} \quad (7)$$

$$L_2 = \Sigma^* \quad (8)$$

$$L_3 = \{\epsilon, 0, 001, 0001\} \quad (9)$$

$$L_4 = \{0, 01, 011, 0111, \dots\} \quad (10)$$



Niedeterministyczny automat skończony

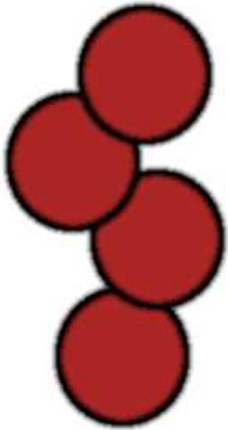


- **Niedeterministycznym automatem skończonym** - nazywamy piątkę

$$NFA = \{Q, \Sigma, \delta, q_0, F\}, \quad (11)$$

gdzie:

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



Deterministyczny automat skończony

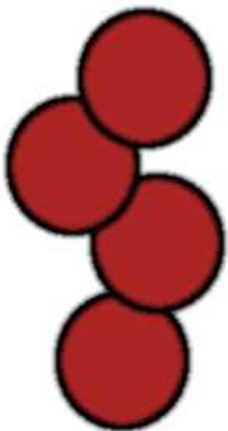


- **Deterministycznym automatem skończonym** - nazywamy piątkę

$$DFA = \{Q, \Sigma, \delta, q_0, F\}, \quad (12)$$

gdzie:

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



Przykład NFA



Przykład niedeterministycznego automatu skończonego:

$NFA = \{Q, \Sigma, \delta, q, F\}$, gdzie:

$Q = \{q_0, q_1, q_2\}$ - skończony zbiór stanów,

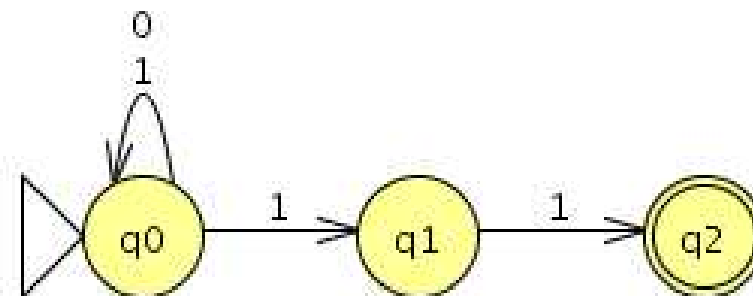
$\Sigma = \{0, 1\}$ - alfabet wejściowy,

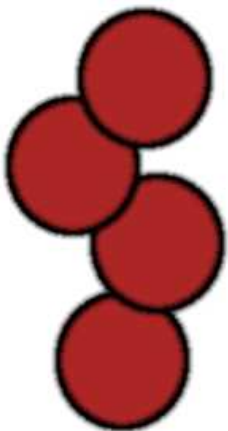
$q = q_0$ - stan początkowy,

$F = \{q_2\}$ - zbiór stanów końcowych (akceptowalnych)

δ - funkcja przejść:

$Q \setminus \Sigma$	0	1
q_0	$\{q_0\}$	$\{q_0, q_1\}$
q_1	$\emptyset$	$\{q_2\}$
q_2	$\emptyset$	$\emptyset$





Przykład DFA



Przykład deterministycznego automatu skończonego:

$DFA = \{Q, \Sigma, \delta, q, F\}$, gdzie:

$Q = \{q_0, q_1, q_2, q_3\}$ - skończony zbiór stanów,

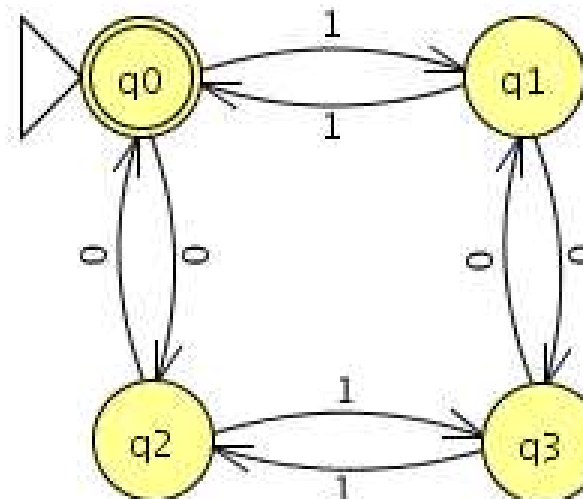
$\Sigma = \{0, 1\}$ - alfabet wejściowy,

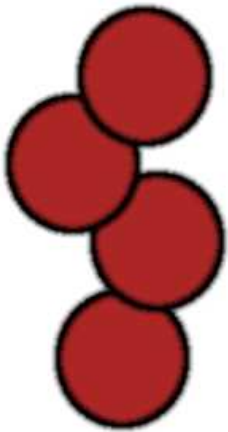
$q = q_0$ - stan początkowy,

$F = \{q_0\}$ - zbiór stanów końcowych (akceptowalnych)

δ - funkcja przejść:

$Q \setminus \Sigma$	0	1
q_0	q_2	q_1
q_1	q_3	q_0
q_2	q_0	q_3
q_3	q_1	q_2





Język akceptowany przez FA



- Jeżeli $NFA = \{Q, \Sigma, \delta, q_0, F\}$ jest niedeterministycznym automatem skończonym, to:

$$L(A) = \{w \in \Sigma^* : \hat{\delta}(q_0, w) \cap F \neq \emptyset\} \quad (13)$$

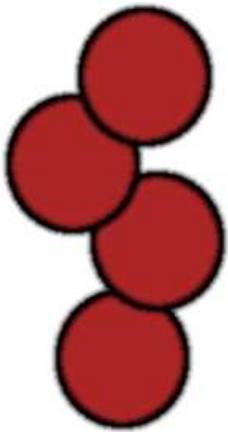
jest językiem akceptowanym przez ten automat.

- Jeżeli $DFA = \{Q, \Sigma, \delta, q_0, F\}$ jest deterministycznym automatem skończonym, to:

$$L(A) = \{w \in \Sigma^* : \hat{\delta}(q_0, w) \in F\} \quad (14)$$

jest językiem akceptowanym przez ten automat.

- Język akceptowany przez automat skończony jest regularny.



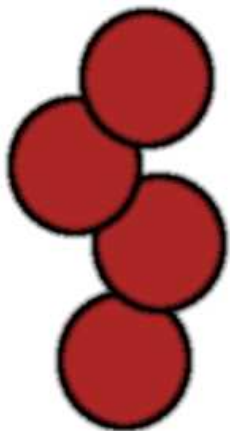
Minimalizacja DFA [1]



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

Algorytm minimalizacji deterministycznego automatu skończonego polega na:

- wyeliminowaniu stanów nieosiągalnych,
- złączeniu stanów nierozróżnialnych.



Minimalizacja DFA [2]



Dla automatu: $DFA = \{Q, \Sigma, \delta, q_0, F\}$

$Q = \{A, B, C, D, E, F, G\}$ - skończony zbiór stanów,

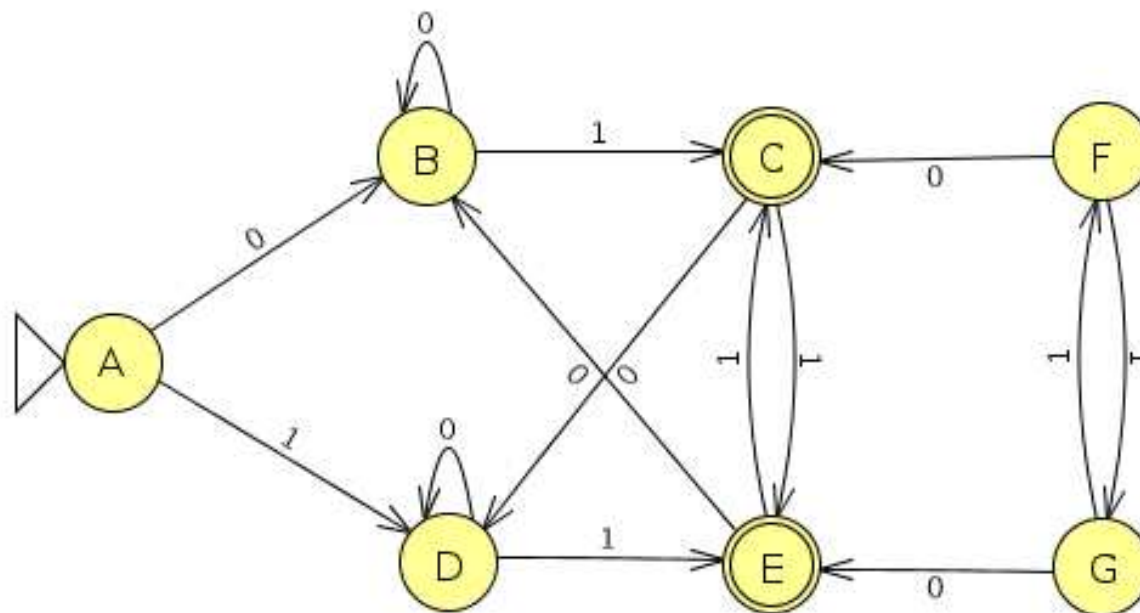
$\Sigma = \{0, 1\}$ - zbiór symboli terminalnych (alfabet wejściowy),

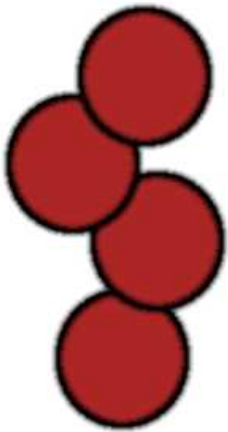
$q_0 = A$ - stan początkowy,

$F = \{C, E\}$ - zbiór stanów końcowych (akceptowalnych)

δ - funkcja przejść:

$Q \setminus \Sigma$	0	1
A	B	D
B	B	C
C	D	B
D	D	E
E	B	C
F	C	G
G	E	F

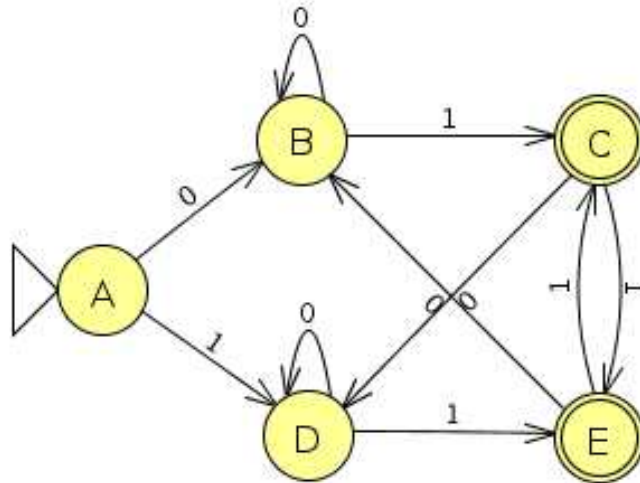




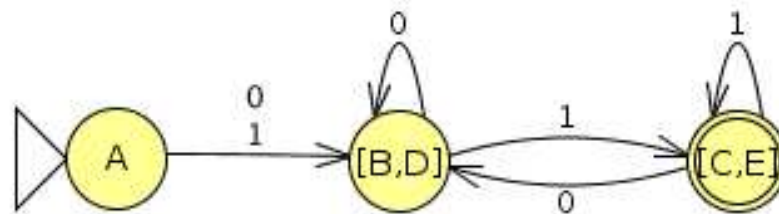
Minimalizacja DFA [3]

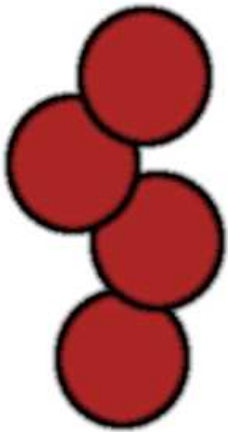


- Wyeliminowanie stanów nieosiągalnych:



- Złączenie stanów nierozróżnialnych:





Automat ze stosem



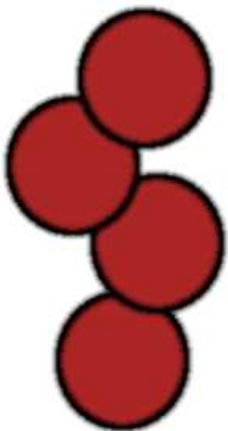
● **Automatem ze stosem** - nazywamy

$$PDA = \{Q, \Sigma, \Gamma, \delta, q_0, Z_0, F\}, \quad (15)$$

gdzie:

- Q - skończony zbiór stanów, $\#Q < \infty$,
- Σ - alfabet wejściowy,
- Γ - skończony zbiór symboli stosowych,
- δ - funkcja przejść $\delta : Q \times (\Sigma \cup \{\epsilon\}) \times \Gamma \mapsto Q \times \Gamma^*$,
- $q_0 \in Q$ - stan początkowy,
- $Z_0 \in \Gamma$ - symbol początkowy stosu,
- $F \subseteq Q$ - zbiór stanów końcowych (akceptowalnych).

● Języki akceptowane przez PDA nazywamy bezkontekstowymi.

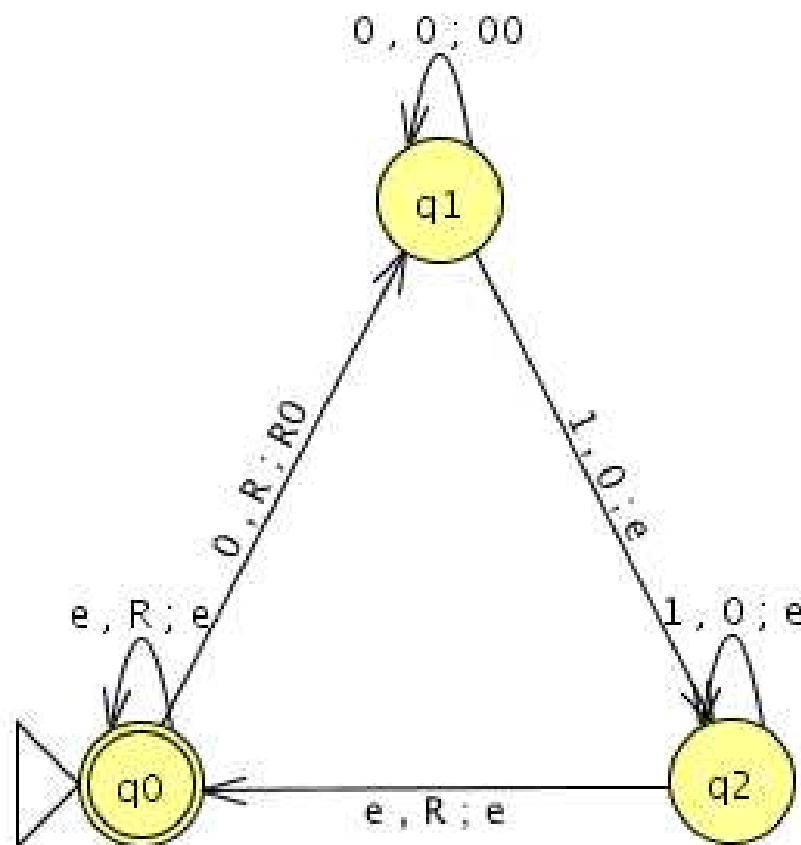


Przykład PDA

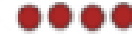
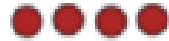
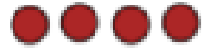
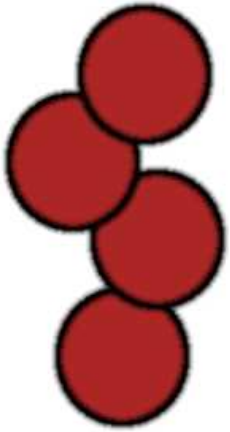


Przykład automatu ze stosem:

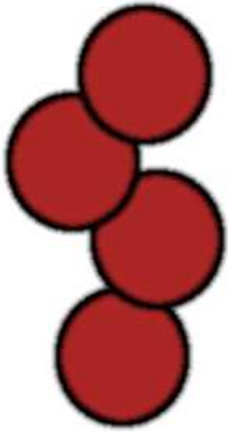
$$PDA = \{\{q_0, q_1, q_2\}, \{0, 1\}, \{R, 0\}, \delta, q_0, R, \{q_0\}\}$$



stan	symbol	stos	stan	stos
q_0	0	R	q_1	R0
q_1	0	0	q_1	00
q_1	1	0	q_2	ϵ
q_2	1	0	q_2	ϵ
q_2	ϵ	R	q_0	ϵ
q_0	ϵ	R	q_0	ϵ



Kwantowa teoria automatów i języków formalnych

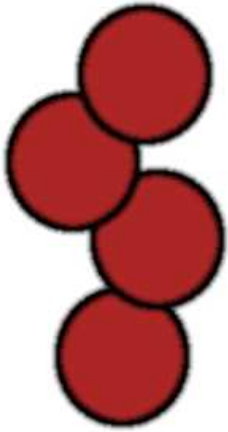


Automat kwantowy



1997 rok - definicja kwantowych automatów:

- Cris Moore, James Crutchfield
- Attila Kondacs, John Watrous



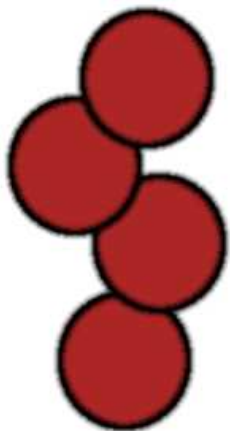
Język kwantowy



Z perspektywy Moore'a i Crutchfield'a:

- **Język kwantowy** określa jakie jest prawdopodobieństwo zaobserwowania danego słowa:

$$QL : \Sigma^* \mapsto [1, 0]. \quad (16)$$



Automat kwantowy

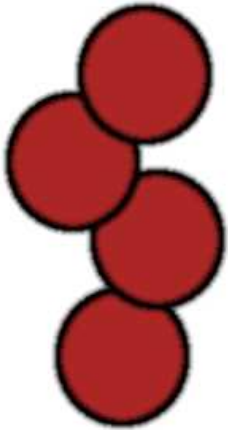


● Kwantowy automat definiujemy jako:

$$QA = \{H, \Sigma, U_\sigma, \langle s_0 |, F, P\}, \quad (17)$$

gdzie:

- H - przestrzeń Hilberta,
- Σ - alfabet wejściowy,
- U_σ - unitarna macierz przejść $U_\sigma : H \mapsto H$ dla każdego symbolu $\sigma \in \Sigma$,
- $\langle s_0 | \in H$ - stan początkowy, spełniający warunek $||s_0||^2 = 1$,
- $F \subseteq H$ - podprzestrzeń stanów akceptowalnych.
- P - operator $P : H \mapsto F$



Język kwantowy akceptowany przez QA

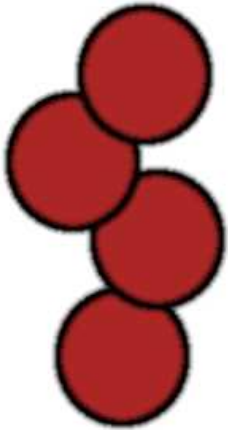


Jeżeli unitarna macierz przejść dla całego słowa U_w będzie równa:

$$U_w = U_{w_1} U_{w_2} \dots U_{w_{|w|}} \quad (18)$$

wtedy język akceptowany przez kwantowy automat jest funkcją:

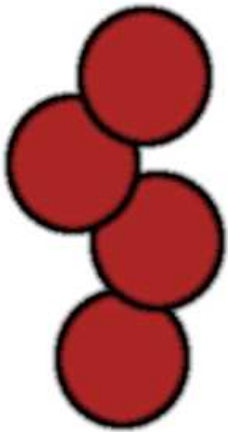
$$f_{QA}(w) = ||s_0 U_w P||^2. \quad (19)$$



QFA, QRL



Kwantowy automat skończony, to automat w którym H , s_0 i U_σ mają skończony wymiar n . Kwantowy język akceptowany przez kwantowy automat skończony nazywamy kwantowym językiem regularnym.



2QFA [1]



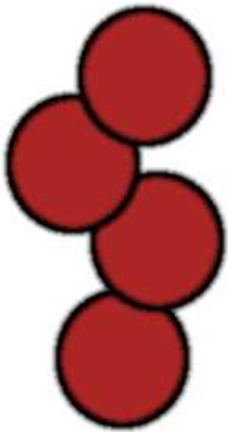
Z perspektywy Kondacs'a i Watrous'a:

- Dwukierunkowy skończony automat kwantowy definiujemy jako:

$$2QFA = \{Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej}\}, \quad (20)$$

gdzie:

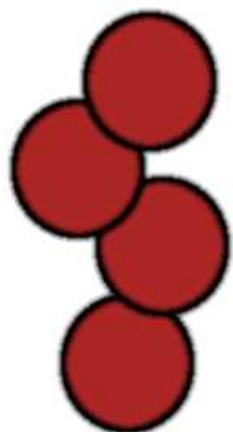
- Q - skończony zbiór stanów,
- Σ - alfabet wejściowy,
- δ - funkcja przejść,
- $q_0 \in Q$ - stan początkowy,
- $Q_{acc} \subset Q$ - zbiór stanów akceptowalnych,
- $Q_{rej} \subset Q$ - zbiór stanów odrzucających.



2QFA [2]

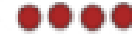
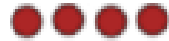
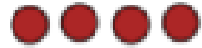
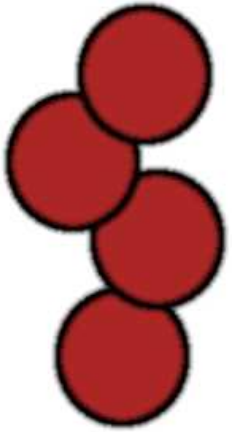


- Definiujemy także $Q_{non} = Q \setminus (Q_{acc} \cup Q_{rej})$ - stanów nie będących końcowymi, oraz symbole ℓ i $\wp$ oznaczające lewy i prawy koniec słowa wejściowego, stąd alfabet na którym operuje automat ma postać $\Gamma = \Sigma \cup \{\ell, \wp\}$.
- Funkcja przejść jest odwzorowaniem: $\delta : Q \times \Gamma \times Q \times \{-1, 0, 1\} \mapsto \mathbb{C}$.

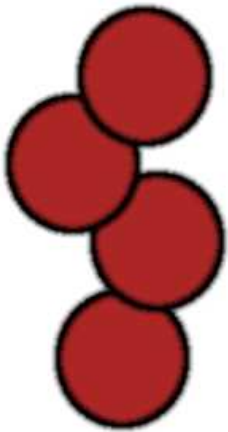


Cel





Dziękuję za uwagę i proszę o pytania.



Źródła



- M. Hirvensalo, *Algorytmy kwantowe*, Wydawnictwa Szkolne i Pedagogiczne S.A., Warszawa 2004
- J. E. Hopcroft, R. Motwani, J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, second edition, Addison-Wesley, 2001
- J. Majewski, *Teoria automatów i języków formalnych, teoria kompilacji*, wykłady: <http://home.agh.edu.pl/~tekomp/>
- C. Moore, J.P. Crutchfield, *Quantum Automata and Quantum Grammars*, Theoretical Computer Science, Vol. 237, No. 1–2, pp. 275–306, 2000
- A. Kondacs, J. Watrous, *On the Power of Quantum Finite State Automata*, Proceedings of the 38th Annual Symposium on Foundations of Computer Science, pp. 66–75, 1997