Podstawy obliczeń kwantowych

Jarosław Miszczak

Instytut Informatyki Teoretycznej i Stosowanej PAN

Instytut Badań Systemowych
Warszawa, 17/12/2016

Obliczenia

Jednym z podstawowych (nieformalnych) założeń współczesnej informatyki jest hipoteza Churcha-Turinga, która określa rodzinę funkcji obliczalnych.

Hipoteza Churcha-Turinga

Dowolne rozsądne obliczenia, mogą być wykonane przez maszynę Turinga.

Hipoteza ta

- nie dotyczy kosztów wykonywanych obliczeń,
- zawiera ukryte założenie, że **rozsądne** obliczenia są wykonywane mechanicznie zgodnie z zasadami fizyki klasycznej.

Obliczenia

- Wszystko wskazuje na to, iż mechanika klasyczne nie jest podstawową teorią opisującą układy fizyczne.
- W chwili obecnej uznaje się, iż taką teorią jest mechanika kwantowa.

Hipoteza Churcha-Turinga-Deutscha

Każdy proces fizyczny może być symulowany przez uniwersalny komputer.

Motywacja
Motywacja techniczna

Prawo Moore'a (1965)

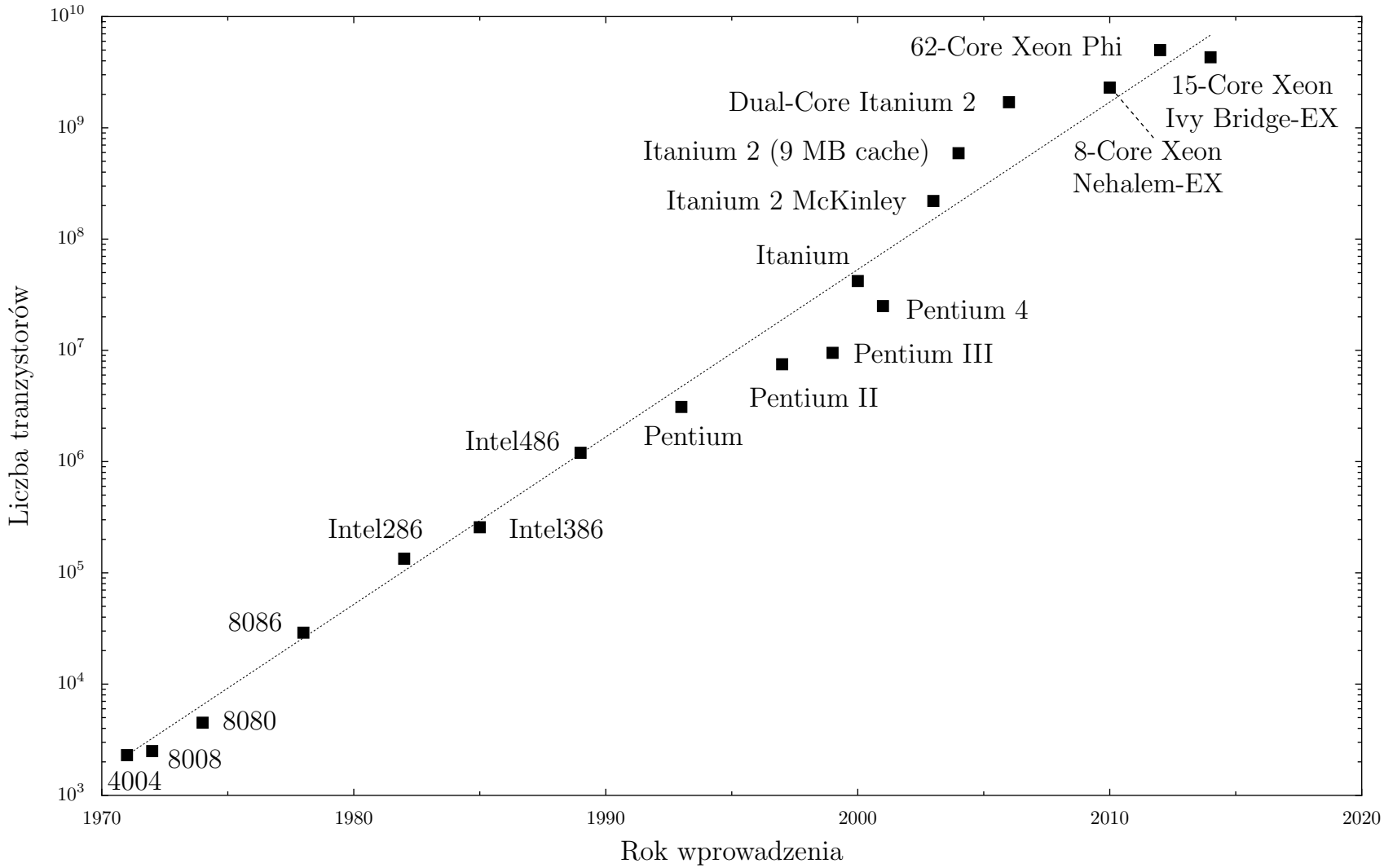
Moc obliczeniowa podwaja się co dwa lata dzięki zwiększeniu **gęstości tranzystorów**.

Prawo Wirtha-Gatesa

Wzrost mocy obliczeniowej jest kompensowany wzrostem **złożoności oprogramowania**.

Motywacja

Motywacja techniczna



Motywacja
Motywacja techniczna

Osborne Executive (1982) oraz iPhone (2007)

Motywacja
Motywacja fizyczna

- Richard Feynmann, 1982 – symulacja układów fizycznych przez komputery klasyczne jest nieefektywna.

(Richard P. Feynman, *Simulating Physics with Computers*, International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982)

Motywacja
Motywacja fizyczna

- Czy maszyna Turinga może wykonać symulacje układów kwantowych efektywnie?
- Czy stan układu kwantowego może być wykorzystany do przechowywania (i przesyłania) dowolnie dużej ilości informacji?

Motywacja
Motywacja kryptograficzna

- W mechanice kwantowej pomiar powoduje, że system ulega zniszczeniu. Czy może być to wykorzystane do zabezpieczenia danych?

Motywacja

- S.J. Wiesner (1970): niepodrabialne pieniądze – podstawa zakazu klonowania i kryptografii kwantowej. S.J. Wiesner, *Conjugate Coding*, SIGACT News, Vol. 15, pp. 78-88 (1983).
- A. Ekert (1991): kryptografia kwantowa (Artur Ekert, *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67: 661–663.)

Stany układu
Zasada liniowości

Liniowość

Pierwszą z zasad przy wprowadzaniu opisu układów w języku mechaniki kwantowej jest **zasada liniowości**. Prowadzi ona do sytuacji w której dwa stany układu kwantowego można dodać i otrzymany w ten sposób obiekt (czyli kombinacja liniowa) jest również poprawnym stanem układu.

Superpozycja stanów

Kombinacja liniowe stanów nazywana jest **superpozycją stanów**.

Stany układu
Zasada liniowości

Aby wykonywać obliczenia ($\equiv$ operować na danych), konieczne jest wprowadzenie reprezentacji danych dostosowanej do modelu obliczeń.

Zasada "zerowego" kwantowania

Przyjmijmy, że $0 \mapsto \binom{1}{0}$ oraz $1 \mapsto \binom{0}{1}$.

Ponieważ $\binom{1}{0}$ i $\binom{0}{1}$ to wektory, więc kwantowy bit może być w stanie

$$x_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad x_0, x_1 \in \mathbb{C},$$

np. $\frac{1}{2}\binom{1}{0} + \frac{i}{2}\binom{0}{1}$.

Stany układu
Notacja Diraca

Notacja Diraca

$|0\rangle \equiv \binom{1}{0}$, $|1\rangle \equiv \binom{0}{1}$

Ponieważ $|0\rangle$ i $|1\rangle$ to wektory, więc kwantowy bit może być w stanie

$$x_0|0\rangle + x_1|1\rangle, \quad x_0, x_1 \in \mathbb{C},$$

np. $\frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle$.

Stany układu
Pomiar

Obserwable

Wyniki pomiaru są określone przez wielkość którą mierzymy.

Stany układu
Pomiar

W naszym przypadku zakładamy, że istnieje wielkość, którą możemy opisać stanami bazowymi. Dla stanu będącego superpozycją postaci

$$\sum_{i=0}^{N-1} a_i |i\rangle$$

pomiar skutkuje wynikiem $|i\rangle$ z prawdopodobieństwem $|a_i|^2$.

Normalizacja

Normalizacja wektorów stanu jest potrzebna do probabilistycznej interpretacji wyników pomiaru.

Układy złożone

Iloczyn Korneckera

Druga zasada dotyczy tworzenia układów złożonych.

Tworzenie układów złożonych

Jeżeli układ jest złożony z dwóch podukładów, to jego stan jest opisany przez **iloczyn tensorowy** przestrzeni reprezentujących podukłady.

Układy złożone
Iloczyn Korneckera

Definicja (Iloczyn tensorowy)

Rozważmy przestrzenie wektorowe V, W i X, oraz odwzorowania ***dwuliniowe*** $f : V \times W \mapsto X$. *Iloczynem tensorowym przestrzeni V i W nazywamy przestrzeń liniową T wraz z odwzorowaniem τ, takim, że odwzorowanie f może być zapisane jako*

$$f = g \circ \tau,$$

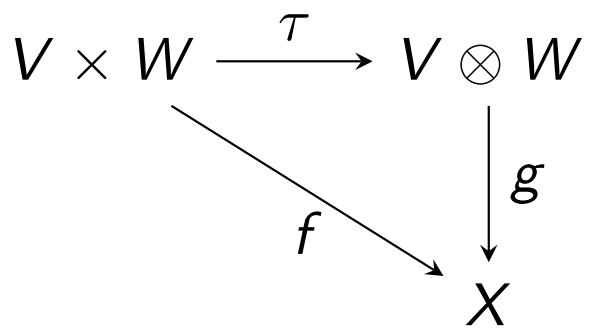
gdzie $g : T \mapsto X$ jest ***liniowe***.

Powyżej zdefiniowaną przestrzeń T oznacza się jako $V \otimes W$.

Układy złożone

Iloczyn Korneckera

Dla dowolnej przestrzeni liniowej X oraz odwzorowania f, poniższy diagram jest przemienny.



Tensory

Tensory to obrazy wektorów bazowych przez odwzorowanie τ.

Układy złożone

Iloczyn Korneckera

W przypadku przestrzeni unitarnych (liniowych z iloczynem skalarnym) powyższa definicja znacznie się upraszcza.

Układy złożone

Iloczyn Korneckera

Definicja (Iloczyn Kroneckera)

Dla dwóch macierzy $A \in \mathbb{M}_{k,l}(\mathbb{C})$ *i* $B \in \mathbb{M}_{m,n}(\mathbb{C})$ *ich iloczynem tensorowym jest macierz*

$$A \otimes B = \begin{pmatrix} \mathbf{a_{11}} b_{11} & \dots & \mathbf{a_{11}} b_{1n} & \dots & a_{1l} b_{11} & \dots & a_{1l} b_{1n} \\ \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ \mathbf{a_{11}} b_{m1} & \dots & \mathbf{a_{11}} b_{mn} & \dots & a_{1l} b_{m1} & \dots & a_{1l} b_{mn} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{k1} b_{11} & \dots & a_{k1} b_{1n} & \dots & a_{kl} b_{11} & \dots & a_{kl} b_{1n} \\ \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ a_{k1} b_{m1} & \dots & a_{k1} b_{mn} & \dots & a_{kl} b_{m1} & \dots & a_{kl} b_{mn} \end{pmatrix}$$

Układy złożone

Iloczyn Korneckera

Zasada "zerowego" kwantowania dla układów złożonych

Jeżeli $(b_0, b_1) \in \{0,1\} \times \{0,1\}$ to przyjmujemy $(b_0, b_1) \mapsto |b_0\rangle \otimes |b_1\rangle$.

W przypadku dwóch **bitów** kwantowych, dozwolone stany to stany bazowe

$$|00\rangle \equiv |0\rangle \otimes |0\rangle,\ |01\rangle \equiv |0\rangle \otimes |1\rangle,\ |10\rangle \equiv |1\rangle \otimes |0\rangle,\ |11\rangle \equiv |1\rangle \otimes |1\rangle$$

oraz ich dowolne kombinacje $x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle$.

Układy złożone
Splątanie

Splątanie jest zasobem

Najważniejszym zasobem dostępnym w kwantowej teorii informacji jest splątanie.

Układy złożone
Splątanie

Rozkład Schmidta

Macierz współczynników rozkładu w bazie

$$\begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix}$$

można zawsze zdiagonalizować unitarnie.

Singular Value Decomposition

Rozkład Schmidta to inna nazwa dla Singular Value Decomposition.

Układy złożone
Splątanie

Stan jest splątany jeżeli po diagonalizacji macierz ma dwa elementy niezerowe, np.

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle).$$

Taki stan nie może być zareprezentowany jako pojedyńczy tensor (rozumiany jako iloczyn tensorowy wektorów bazowych).

Układy złożone
Splątanie

Uogólnienia

Rozkład na wartości singularne nie ma jednoznacznego uogólnienia na macierze 3-modowe. Wiadomo jednak, że w przypadku układów trzech cząstek można wyróżnić dwie nierównoważne klasy stanów splątanych.

Obwody kwantowe

Odwracalność

Trzecią zasadą jest **odwracalność operacji** wykonywanych na stanach (czyli ewolucji układu).

Z fizycznego punktu widzenia wynika ona z zasady zachowania energii – formalizm wektorów stanu zakłada, że nie dochodzi do wypływu informacji z układu (lub równoważnie, że układ jest całkowicie odizolowany).

Bramki kwantowe

Przekłada się to na opis ewolucji układu za pomocą **macierzy unitarnych**, nazywanych **bramkami kwantowymi**.

Obwody kwantowe

- Charles Bennett, 1973 – uniwersalna maszyna Turinga może być zrealizowana w sposób odwracalny.
  (C. H. Bennett, *Logical reversibility of computation*, IBM Journal of Research and Development, vol. 17, no. 6, pp. 525-532 (1973).)

Obwody kwantowe

Obwody odwracalne i zasada Landauera

- Jeżeli nie dochodzi do wymazywania informacji, to proces obliczeniowy może być zrealizowany w sposób odwracalny termodynamicznie.
- W takim procesie nie jest wydzielane ciepło.

Obwody kwantowe

Obwody odwracalne i zasada Landauera

- Rolf Landauer, 1961 – sformułowanie teoretycznego ograniczenia na minimalną energochłonność obliczeń.
- 2012 – pomiar zmiany wydzielania ciepła przy procesie wymazywania informacji. (A. Bérut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, E. Lutz, *Experimental verification of Landauer's principle linking information and thermodynamics*, Nature 483 (7388): 187–190, (2012))

Obwody kwantowe

Obwody odwracalne i zasada Landauera

Zasada Landauera

Każdy nieodwracalnej manipulacji informacją o układzie (np. wymazanie bitu) towarzyszy wzrost entropii.

Do wymazania jednego bitu informacji potrzebna jest co najmniej energia $kT \ln 2$. Daje to 2.75×10^{-24} J w temperaturze pokojowej.

Obwody kwantowe

Przykłady bramek uniwersalnych dla klasycznych obliczeń

- Bramka Fredkina (kontrolowany SWAP)
- Bramka Toffoliego (podwójnie kontrlowany NOT)

Bramki te są **trójbitowe**.

CNOT

W przypadku obliczeń kwantowych do konstrukcji zbioru zupełnego wystarczy dwukubitwa bramka CNOT.

Obwody kwantowe

RESEARCH ARTICLE

QUANTUM MECHANICS

A quantum Fredkin gate

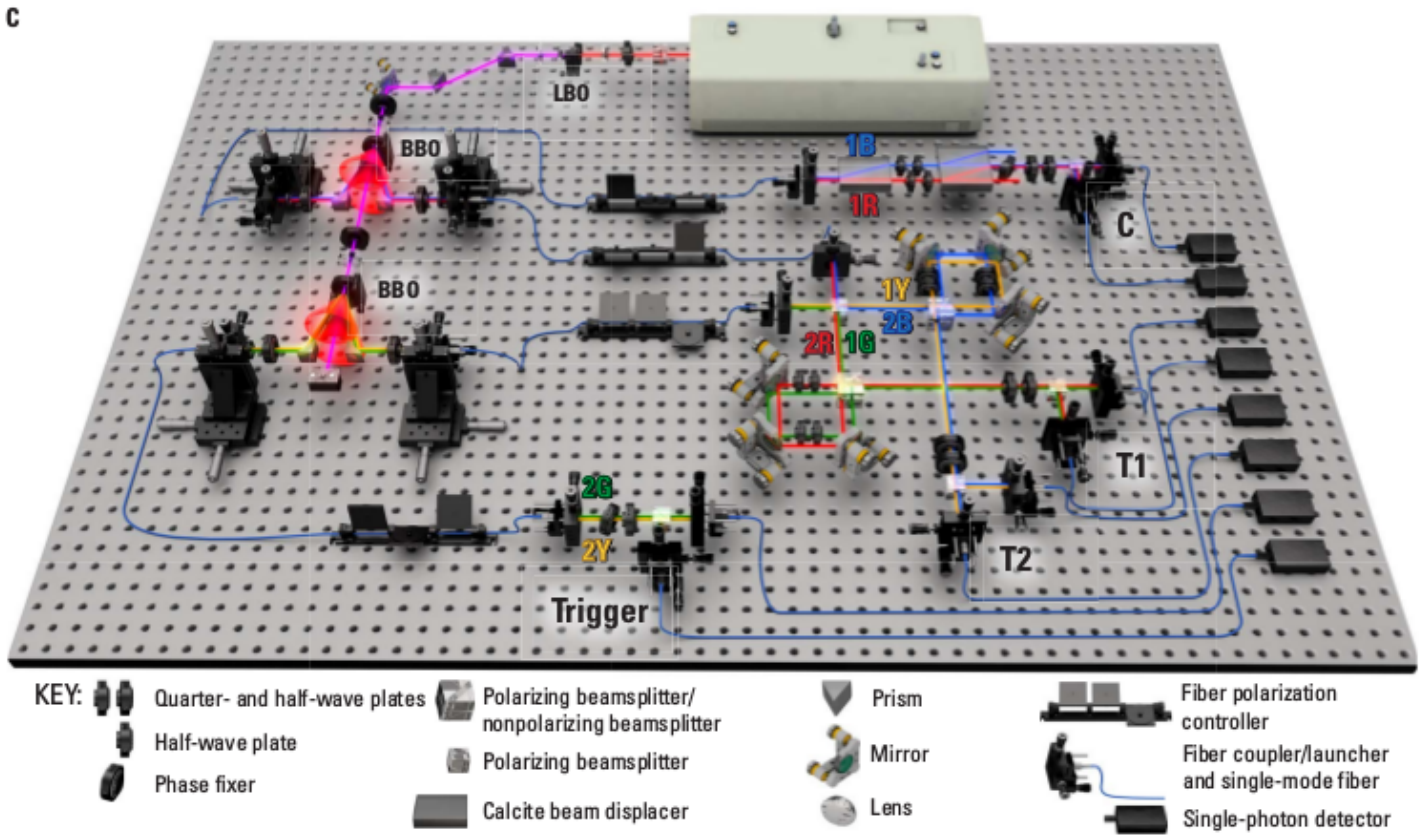
Raj B. Patel,[1]* Joseph Ho,[1] Franck Ferreyrol,[1,2] Timothy C. Ralph,[3] Geoff J. Pryde[1]*

10.1126/sciadv.1501531

Minimizing the resources required to build logic gates into useful processing circuits is key to realizing quantum computers. Although the salient features of a quantum computer have been shown in proof-of-principle experiments, difficulties in scaling quantum systems have made more complex operations intractable. This is exemplified in the classical Fredkin (controlled-SWAP) gate for which, despite theoretical proposals, no quantum analog has been realized. By adding control to the SWAP unitary, we use photonic qubit logic to demonstrate the first quantum Fredkin gate, which promises many applications in quantum information and measurement. We implement example algorithms and generate the highest-fidelity three-photon Greenberger-Horne-Zeilinger states to date. The technique we use allows one to add a control operation to a black-box unitary, something that is impossible in the standard circuit model. Our experiment represents the first use of this technique to control a two-qubit operation and paves the way for larger controlled circuits to be realized efficiently.

(R.B. Patel, J. Ho, F. Ferreyrol, T.C. Ralph and G.J. Pryde, *A quantum Fredkin gate*, Science Advances, 25 Mar 2016, Vol. 2, no. 3, e1501531)

Obwody kwantowe



(R.B. Patel, J. Ho, F. Ferreyrol, T.C. Ralph and G.J. Pryde, *A quantum Fredkin gate*, Science Advances, 25 Mar 2016, Vol. 2, no. 3, e1501531)

Obwody kwantowe
Bramki kwantowe

Zasada "zerowego" kwantowania operacji

Dla zadanej operacji, kwantowym odpowiednikiem jest takie przekształcenie wektorów, które działa odpowiednio na bazie $\{|0\rangle, |1\rangle\}$.

Przykładowo dla operacji negacji kwantowy odpowiednik to

$$Not = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Możliwe jest natomiast wprowadzenie operacji, które nie mają odpowiedników klasycznych, np. operacja Hadamarda

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

która wprowadza superpozycję 0 i 1.

Obwody kwantowe

Bramki kwantowe

Kolejny nieklasyczny przykład to **pierwiastek kwadratowy z negacji** $\sqrt{Not}$, który spełnia własność

$$\sqrt{Not}\sqrt{Not}|x\rangle = Not|x\rangle$$

dla dowolnego wejścia $|x\rangle$.

Oczywiście nic nie stoi na przeszkodzie, żeby zdefiniować pierwiastek dowolnego stopnia z dowolnej macierzy.

Obwody kwantowe

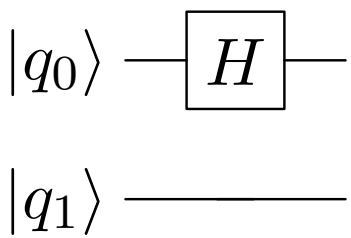
Bogatsze struktura stanów i operacji

W modelu kwantowym zarówno przestrzeń dozwolonych stanów, jak i struktura operacji, są **bogatsze** niż w przypadku modelu klasycznego. Sugeruje to, iż potencjalnie mogą służyć one do wykonywania obliczeń w sposób **bardziej wydajny**.

Obwody kwantowe

Programy kwantowe

Najprostszym sposobem pisania programów kwantowych są *obwody kwantowe*.



Każda linia reprezentuje rejestr (system) kwantowy, a operacje są reprezentowane przez bloki.

Obwody kwantowe

Programowanie to mnożenie macierzy

Program 1: Ustaw płaską superpozycję

W notacji Diraca

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

lub w postaci macierzowej

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}$$

Obwody kwantowe
Programy kwantowe

Bramka *CNOT* (czyli kontrolowana negacja), pozwala na konstrukcję uniwersalnego zbioru bramek.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Jednocześnie pozwala ona na tworzenie stanów splątanych.

Obwody kwantowe

Programy kwantowe

Program 2: Wygeneruj stan splątany

W notacji Diraca

$$CNOT(H \otimes \mathbb{I})|00\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|3\rangle$$

lub w postaci macierzowej

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Obwody kwantowe
Programy kwantowe

Ale można to zrobić prościej korzystając z kwantowego języka programowania (http://tph.tuwien.ac.at/~oemer/qcl.html)

```
qcl> qureg x[2]
qcl> H(x[0])
[2/64] 0.70711 |0> + 0.70711 |1>
qcl> H(x[1])
[2/64] 0.5 |0> + 0.5 |1> + 0.5 |2> + 0.5 |3>
```

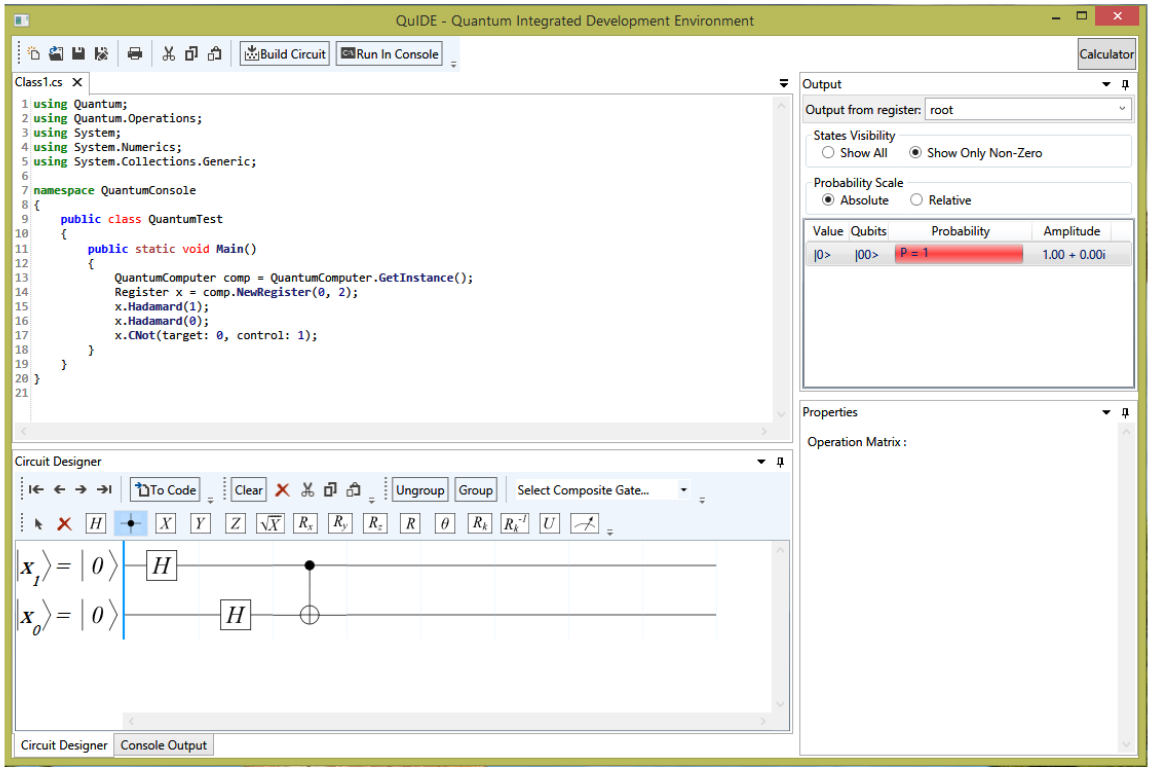
Obwody kwantowe

Programy kwantowe

```
qcl> qureg a[2];
qcl> H(a[0]);
[2/64] 0.70711 |0> + 0.70711 |1>
qcl> dump
: STATE: 2 / 64 qubits allocated, 62 / 64 qubits fr
0.70711 |0> + 0.70711 |1>
qcl> CNOT(a[1],a[0])
[2/64] 0.70711 |0> + 0.70711 |3>
qcl> dump a
: SPECTRUM a: <0,1>
0.5 |0>, 0.5 |3>
```

Obwody kwantowe
Programy kwantowe

Albo wykorzystując środowisko graficzne



(QUIDE, Joanna Patrzyk, Kraków 2014, http://www.quide.eu/)

Algorytmy kwantowe

- Algorytmy kwantowe są tworzone tak, aby wykorzystać superpozycję stanów do obliczania wartość funkcji.
- Dla danej funkcji f, zakładamy, że U_f – bramkę kwantową realizującą f na bazie przestrzeni stanów – można wykonać **efektywnie** na komputerze kwantowym,

$$U_f|x\rangle = |f(x)\rangle.$$

- Aby bramka U_f była unitarna, f musi być **odwracalna**.

Algorytmy kwantowe

Kwantowa równoległość

Bramka U_f może działać na kombinacje liniowe stanów bazowych.

Algorytm Deutscha-Jozsy

- Celem algorytmu Deutscha-Jozsy jest wykazanie, że algorytmy kwantowe są w pewnych przypadkach **lepsze** od algorytmów klasycznych.
- Problem Deutsch-Jozsy jest zaprojektowany tak, żeby być trudnym do wykonania na maszynie klasycznej.
- Złożoność algorytmu jest mierzona liczbą wywołań bramki kwantowej odpowiadającej funkcji.

Algorytm Deutscha-Jozsy

Sformułowanie problemu dla najprostszego przypadku:

- Zadana jest funkcja $f : \{0, 1\} \mapsto \{0, 1\}$.
- Określ czy f jest stała.

Algorytm Deutscha-Jozsy

- Klasycznie żeby określić czy funkcja jest stała musimy znać obie wartości.
- Kwantowo możemy obliczyć obie wartości **jednocześnie** korzystając z superpozycji.

Algorytm Deutscha-Jozsy

Do realizacji algorytmu kluczowa jest możliwość realizacji bramki U_f, która działa zgodnie z zasadą

$$U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle,$$

i jest odwracalną wersją nieodwracalnej funkcji f.

Algorytm Deutscha-Jozsy

Kroki algorytmu

0. Przygotuj stan $|0\rangle|0\rangle$.
1. Wykonaj bramkę $\mathbb{I} \otimes \mathit{Not}$ aby otrzymać $|0\rangle|1\rangle$.
2. Wykonaj bramkę $H \otimes H$.
3. Wykonaj bramkę U_f.
4. Wykonaj bramkę $H \otimes \mathbb{I}$.

Ostatnim etapem jest wykonanie pomiaru.

Algorytm Deutscha-Jozsy

Co lepiej jest rozpisać na tablicy...

Algorytm Deutscha-Jozsy

Wykonanie kroków 1-3 algorytmu daje stan

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle - |1\rangle)$$

lub równoważnie

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \otimes \frac{(-1)^{f(0)}}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Algorytm Deutscha-Jozsy

Po ostatnim kroku otrzymujemy stan

$$\frac{1}{2}\left(1+(-1)^{f(0)\otimes f(1)}\right)|0\rangle + \frac{1}{2}\left(1-(-1)^{f(0)\otimes f(1)}\right)|1\rangle$$

Algorytm Deutscha-Jozsy

- Algorytm jest deterministyczny – po jednym wykonaniu algorytmu znamy odpowiedź.
- Klasyczny algorytm deterministyczny wymaga *dwóch* wywołań funkcji f.

Algorytm Deutscha-Jozsy

Control parameters for the quantum Deutsch algorithm

ŁUKASZ PAWELA

Institute of Theoretical and Applied Informatics
Polish Academy of Sciences
Bałtycka 5, 44-100 Gliwice, Poland

Received 2 November 2011, Revised 21 November 2011, Accepted 5 December 2011

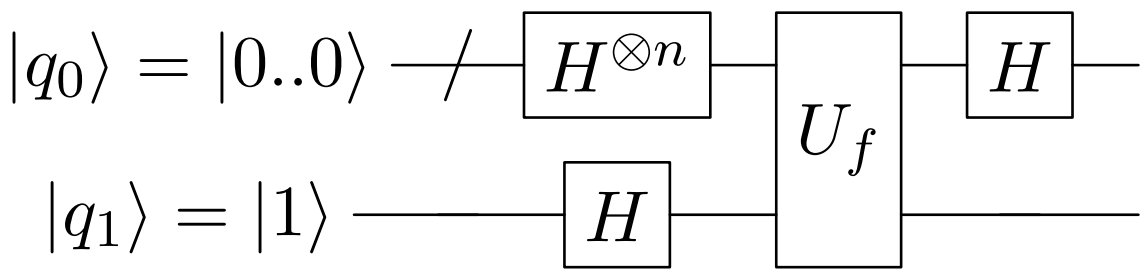
Abstract: An example of two-qubit scenario for finding an optimal control parameters on a spin chain to implement the quantum Deutsch algorithm is provided. Two cases are studied in this paper: two-qubit and three-qubit systems. The latter case is used to study the impact of interaction with an environment on the outcome of the algorithm.

(Ł. Pawela, *Control parameters for the quantum Deutsch algorithm*, Theoretical and Applied Informatics, Vol. 23, no. 3-4, pp. 193-200 (2011))

Algorytm Deutscha-Jozsy

- Algorytm Deutsch-Jozsy może być uogólniony na funkcje $f : \{0,1\}^n \mapsto \{0,1\}$.
- W tym wypadku możliwe jest rozróżnienie między funkcjami *stałymi* i *zbalansowanymi*.
- Klasyczny algorytm wymaga $2^{n-1} + 1$ wywołań funkcji.
- Algorytm kwantowy wymaga *jednego* wywołania U_f.

Algorytm Deutscha-Jozsy



Algorytm Grovera

- Algorytm Grovera pozwala na wyszukanie elementu w zbiorze.
- Wykorzystuje on superpozycję do zapisania informacji o przeszukiwanym zbiorze.
- Algorytm Grovera jest probabilistyczny.

Algorytm Grovera

- Załóżmy, że dysponujemy zbiorem N elementów, z których jeden spełnia pewien warunek.
- Przyjmujemy, że istnieje funkcja f, która przyjmuje wartość 1 tylko na tym elemencie.
- Do konstrukcji algorytmu kwantowego potrzebujemy operacji unitarnej, która odpowiada tej funkcji, U_f,

$$U_f|\omega\rangle = -|\omega\rangle$$

dla $\omega = x^\star$ spełniającego nasz warunek oraz

$$U_f|\omega\rangle = |\omega\rangle$$

dla $\omega \neq x^\star$.

Algorytm Grovera

Kroki algorytmu

- Przygotuj superpozycję $|s\rangle$ wszystkich wyszukiwanych stanów.
- Zastosuj operator U_f.
- Zastosuj operator $U_s = 2|s\rangle\langle s| - \mathbb{I}$
- Powtórz dwa poprzednie kroki około $\frac{\pi}{4}\sqrt{N}$ razy.

Algorytm Grovera

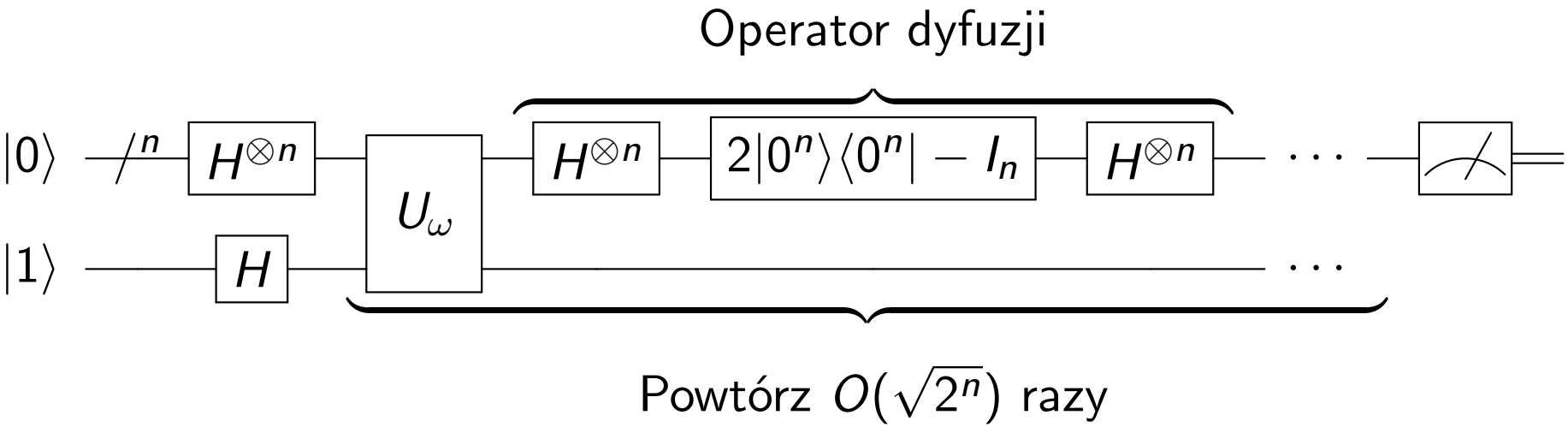
Zobaczmy jak to działa dla jednej iteracji...

Algorytm Grovera

- Proporcja (a właściwie amplituda) stanu $|\omega\rangle$ wzrasta po pierwszej iteracji do $\frac{2}{\sqrt{N}}$.
- Dla $N = 4$ wystarczy jedna iteracja.

Algorytm Grovera

Obwód dla N elementów zapisanych na n qubitach.



Algorytm Grovera

- Algorytm Grover można uogólnić dla kilku zaznaczonych elementów.
- Ponieważ prawdopodobieństwo uzyskania dobrej odpowiedzi rośnie z każdym krokiem, można rozważyć kiedy warto przerwać algorytm.

- Protokoły kwantowe są budowane do *kodowania* i *przesyłania* informacji.
- Oprócz superpozycji stanów, ważna jest tu również możliwość operowania na układach złożonych.

Teleportacja

Transporter działający na statku klasy Galaxy, 2364

Teleportacja

- Teleportacja pozwala na przesłanie stanu kwantowego poprzez wysłanie dwóch bitów.
- Układ, którego stan jest teleportowany, jest niszczony w wyniku działania procedury teleportacji.

Teleportacja służy do przesyłania **stanu** układu.

Teleportacja

- Teleportacja polega przesłaniu stanu między dwoma punktami – lub osobami, np. Alicją i Bobem.
- Zakładamy, że Alicja chce przekazać Bobowi (nieznany) stan $|\psi\rangle_c = a|0\rangle + b|1\rangle$.
- Protokół wymaga, żeby współdzielili jeden ze stanów *splątanych*:

$$|\Phi^+\rangle_{AB} = 1/\sqrt{2}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B),$$
$$|\Phi^-\rangle_{AB} = 1/\sqrt{2}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B),$$
$$|\Psi^+\rangle_{AB} = 1/\sqrt{2}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B),$$
$$|\Psi^-\rangle_{AB} = 1/\sqrt{2}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B).$$

Teleportacja

Przyjmijmy, że Alicja i Bob współdzielą stan

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Zatem stan całego układu to

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B)$$

Teleportacja

Stan całości można zapisać jako

$$
\begin{aligned}
|\Phi^+\rangle_{AB} \otimes |\psi\rangle_C = \quad & \frac{1}{2}|\Phi^+\rangle_{AC} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \\
& + \frac{1}{2}|\Phi^-\rangle_{AC} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \\
& + \frac{1}{2}|\Psi^+\rangle_{AC} \otimes (\beta|0\rangle_B + \alpha|1\rangle_B) \\
& + \frac{1}{2}|\Psi^-\rangle_{AC} \otimes (\beta|0\rangle_B - \alpha|1\rangle_B)
\end{aligned}
$$

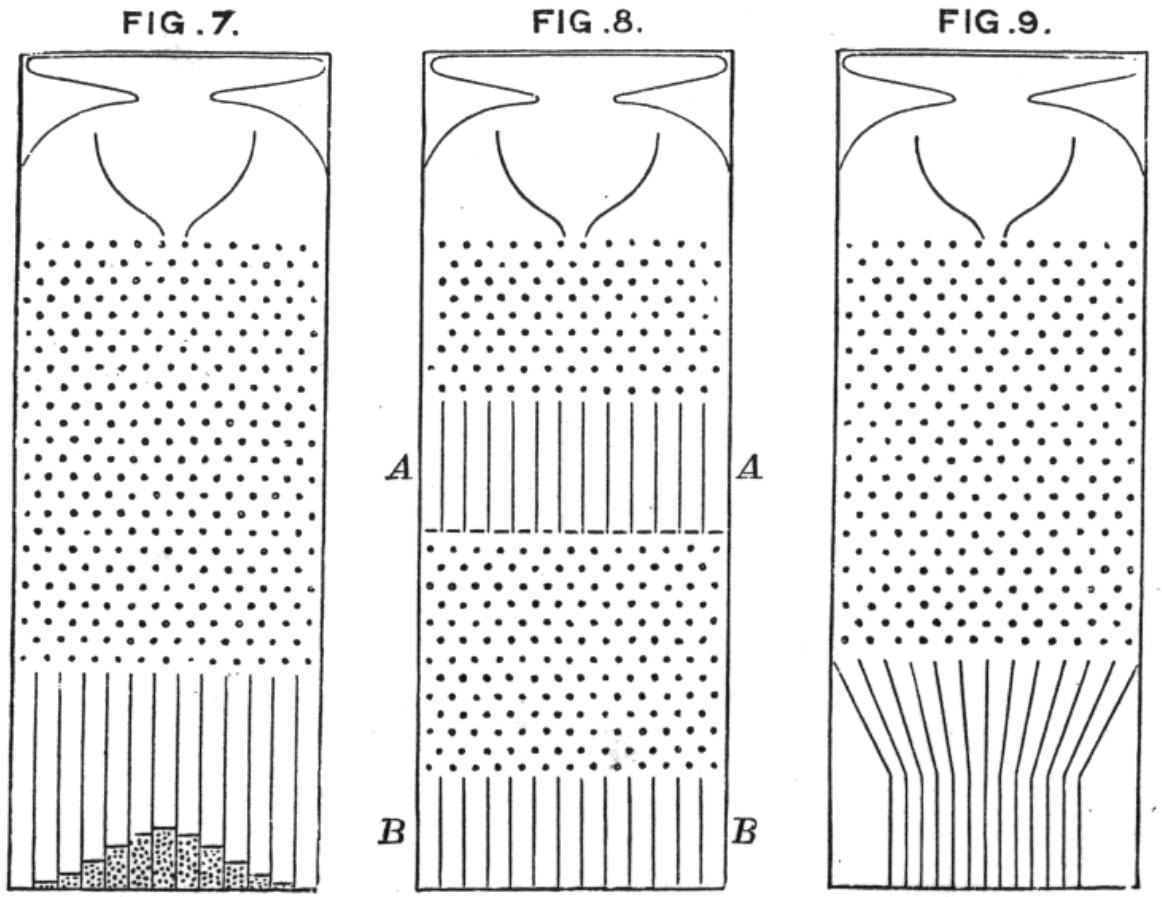
Teleportacja

- Do zakończenia protokołu Alicja musi wysłać Bobowi informację o stanie jej podukładu.
- Możliwych stanów jest 2^2, czyli potrzebne są dwa bity.
- W zależności od otrzymanych danych, Bob wykonuje jedną z operacji.
  - $|\Phi^-\rangle \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
  - $|\Psi^-\rangle \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - $|\Psi^+\rangle \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Teleportacja
Gęste kodowanie

- Protokół gęstego kodowania to odwrotność teleportacji.
- Przesyłając jeden qubit możemy zakodować dwa bity informacji.

Kwantyzacja błądzenia



(F. Galton, Natural Inheritance, Macmillan, 1889, p. 63. See: http://galton.org/)

Kwantyzacja błądzenia

Ewolucja kwantowa musi być liniowa i musi zachowywać prawdopodobieństwa pomiarów – wymaga to użycia do błądzenia operacji unitarnych.
Bezpośredni kwantowy odpowiednik ewolucji na desce Galtona to

$$|x-1\rangle \mapsto \alpha|x-2\rangle + \beta|x\rangle$$
$$|x+1\rangle \mapsto \alpha|x\rangle + \beta|x+2\rangle$$

Stany początkowe są ortogonalne, $\langle x-1|x+1\rangle = 0$.

Kwantowe monety

Do poprawnego zdefiniowania odwracalnej ewolucji potrzebny jest dodatkowy rejestr **monety**.

Kwantyzacja błądzenia

Najprostszy model dyskretnego kwantowego błądzenia z monetą jest opisany operacją

$$U = S(C \otimes \mathbb{I})$$

gdzie S (shift) to operator przesunięcia a C (coin) to operator rzutu monetą. Dla grafu rzędu 2 operator S jest postaci

$$\sum_x |0\rangle\langle 0| \otimes |x-1\rangle\langle x| + |1\rangle\langle 1| \otimes |x+1\rangle\langle x|.$$

Dla przypomnienia

$$CNOT = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes Not.$$

Kwantyzacja błądzenia

Dekodowanie informacji

Końcowym etapem każdej procedury kwantowej jest pomiar – jest on konieczny do odczytania wyniku procedury w sposób użyteczny w świecie klasycznym.

Błądzenie kwantowe vs. kwantowe błądzenie losowe

W błądzeniu kwantowym pomiar jest wykonywany tylko na końcu. W kwantowym błądzeniu losowym pomiar jest wykonywany w każdym kroku.

Błądzenie kwantowe . . .

. . . nie jest losowe – stan układu jest opisany deterministycznie na każdym kroku.

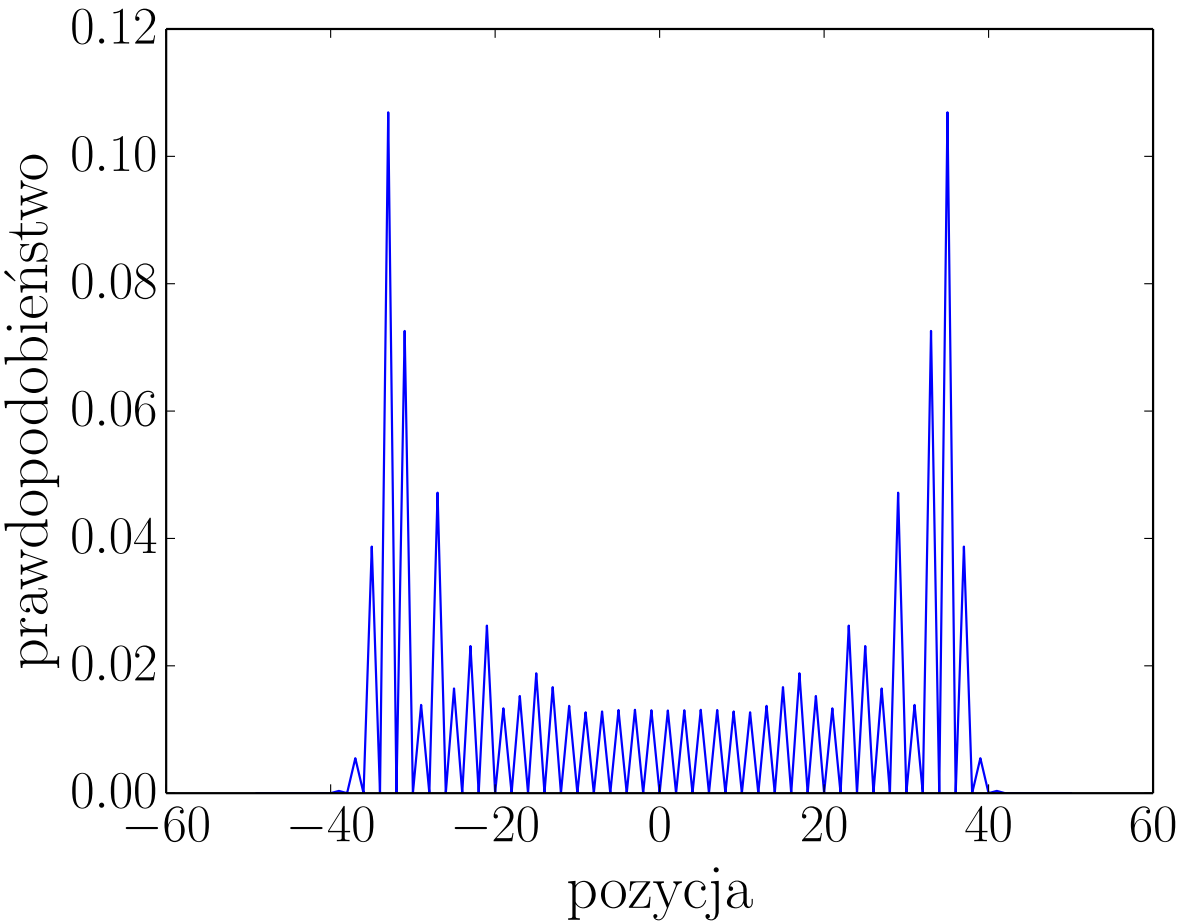
Kwantyzacja błądzenia
Własności

Główną zaletą błądzenia kwantowego jest **szybsze** rozchodzenie się prawdopodobieństwa znalezienia cząstki:

- błądzenie losowe: $\sigma \sim \sqrt{t}$,
- błądzenie kwantowe: $\sigma \sim t$.

Kwantyzacja błądzenia

Własności



Kwantyzacja błądzenia

Własności

Prawdopodobieństwo znalezienia cząstki na pozycji x po t krokach otrzymujemy uśredniając po rejestrze monety

$$P(x,t) = \sum_c |\langle c, x|\phi_t\rangle|^2.$$

Wielkość $P(x,t)$ jest periodyczna dlatego do opisu własności asymptotycznych korzysta się z uśrednionego czasowo rozkładu prawdopodobieństwa (time-averaged limiting distribution)

$$\bar{P}(x,t) = \frac{1}{t}\sum_{s=1}^{t} P(x,s),$$

które dla $t \to \infty$ zbiega do rozkładu granicznego $P(x)$.

Kwantyzacja błądzenia
Własności

Uśredniony rozkład prawdopodobieństwa

Uśredniony rozkład prawdopodobieństwa na pozycji x dla procesu błądzenia z operatorem ewolucji U jest określony formułą

$$P_N(x) = \frac{1}{N} \sum_{t=0}^{N-1} P(x,t),$$

gdzie $P(x,t)$ to prawdopodobieństwo zmierzenia x po t krokach

$$P(x,t) = \sum_{c \in C} |\langle c, x | U^t | \psi_0 \rangle|^2, \tag{1}$$

przy czym $|\psi_0\rangle$ jest dowolnym stanem początkowym.

Kwantyzacja błądzenia
Własności

Graniczny uśredniony rozkład prawdopodobieństwa

Graniczny uśredniony rozkład prawdopodobieństwa na pozyczji x dla dyskretnego procesu błądzenia z operatorem ewolucji U jest dany jako

$$P(x) = \lim_{N\to\infty} P_N(x) = \lim_{N\to\infty} \frac{1}{N} \sum_{t=0}^{N-1} P(x,t), \tag{2}$$

gdzie $P(x,t)$ to rozkład prawdopodobieństwa na pozycji x po t krokach

$$P(x,t) = \sum_{c\in C} |\langle c,x|U^t|\psi_0\rangle|^2, \tag{3}$$

a $|\psi_0\rangle$ to dowolny stan początkowy.

Kwantyzacja błądzenia

Własności

Będziemy teraz chcieli zdefiniować metodę poruszania się po grafie cyklicznym $\mathcal{G} = (V, E)$ z n wierzchołkami.

- $\mathcal{H}_V = \mathbb{C}^n$ reprezentuje przestrzeń pozycji, rozpiętą przez $\{|v\rangle : v \in V\}$,
- $\mathcal{H}_{\mathcal{A}} = \mathbb{C}^2$ przestrzeń monety rozpięta przez dwa wektory,
  - $|0\rangle$ odpowiada kierunkowi “w prawo”,
  - $|1\rangle$ odpowiada kierunkowi “w lewo”,
- zatem cała przestrzeń jest postaci $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_V$.

Błądzenie po cyklu

Dla błądzenia po cyklu operator ewolucji jest zadany wzorem

$$U = S(C \otimes \mathbb{I}_n),$$

gdzie C jest operatorem monety, a S jest operatorem przesunięcia

$$S = |0\rangle\langle 0| \otimes \sum_{i=0}^{n-1} |i+1 \bmod n\rangle\langle i| + |1\rangle\langle 1| \otimes \sum_{i=0}^{n-1} |i-1 \bmod n\rangle\langle i|.$$

gdzie działanie modulo odzwierciedla cykliczność grafu.

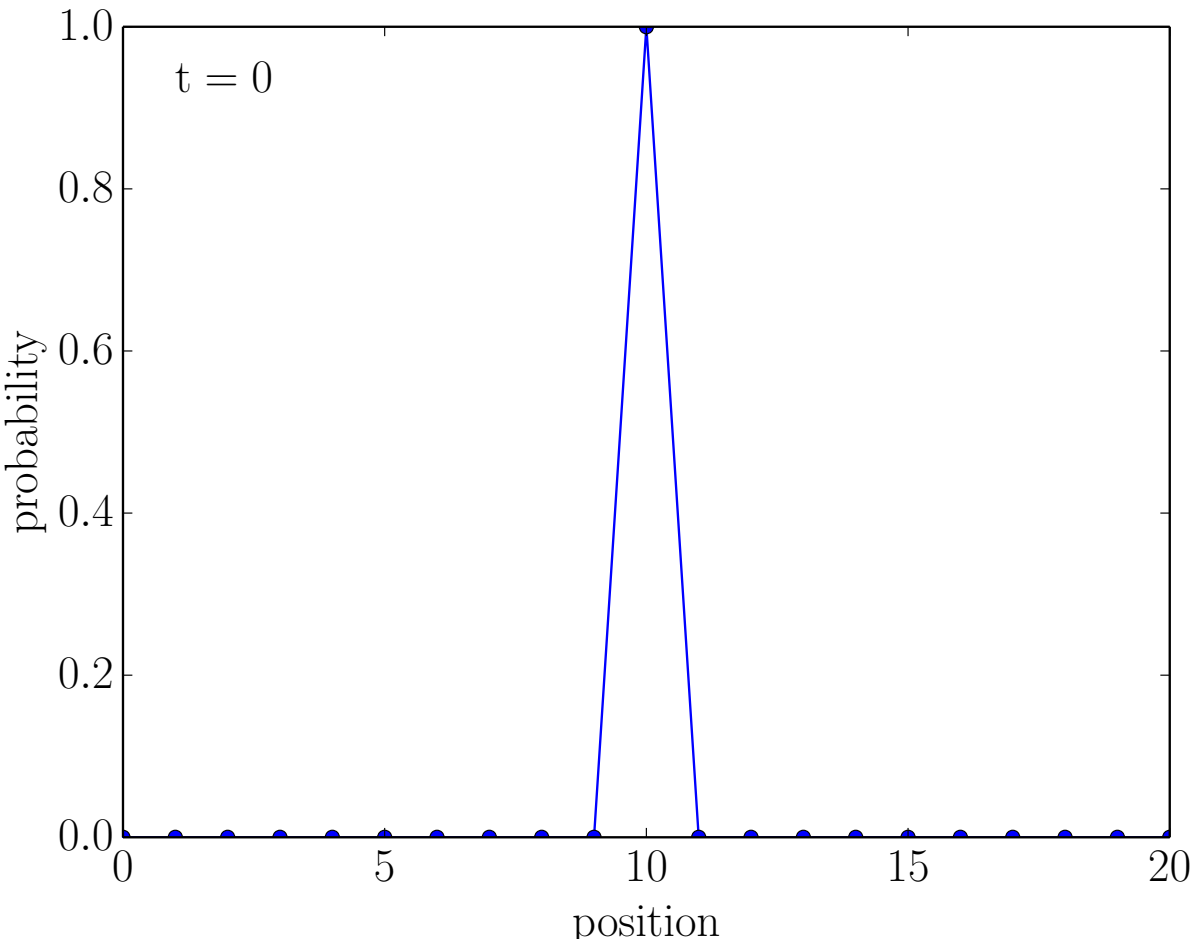
Błądzenie po cyklu
Przykład

Przyjmijmy, że mam cykl z 21 wierzchołkami. Naszym operatorem monety będzie macierz Hadamarda

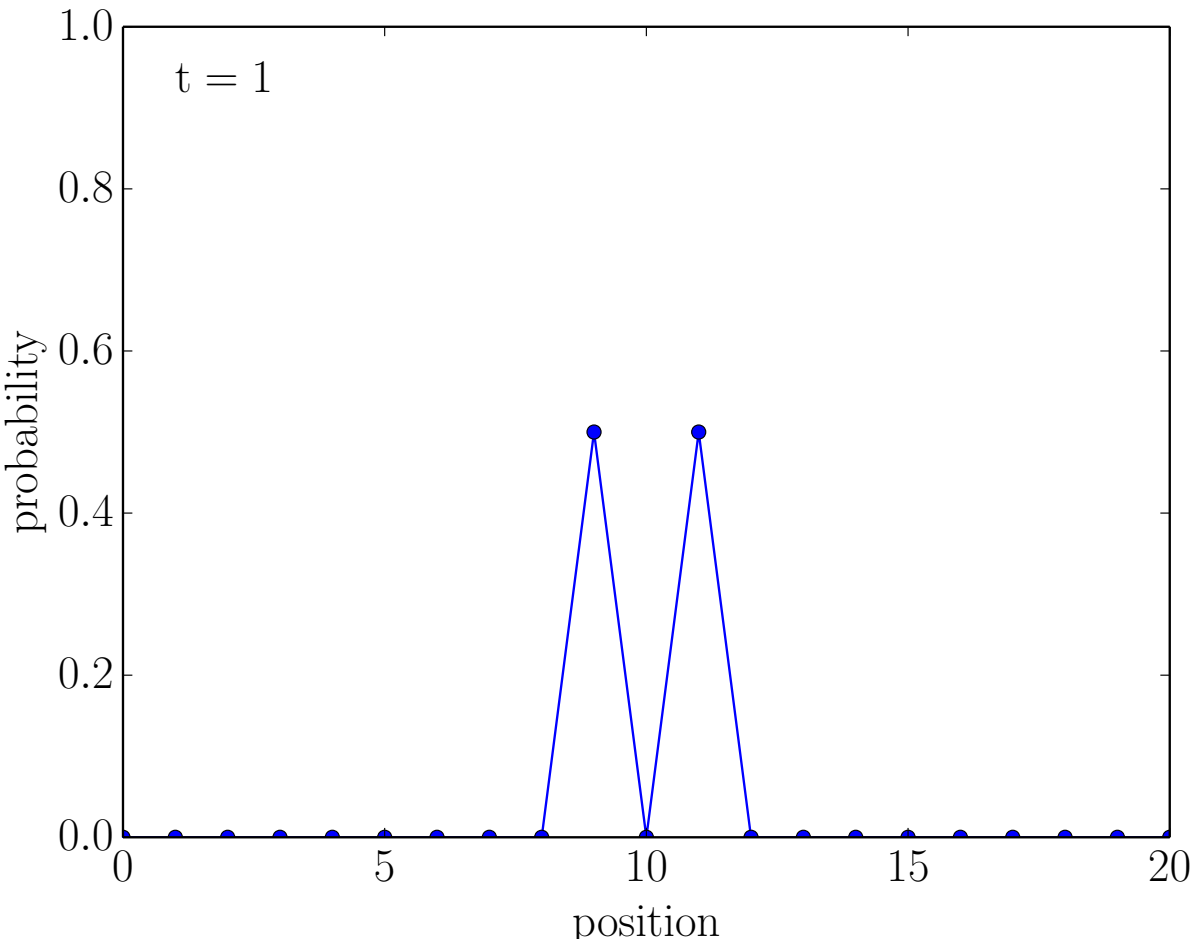
$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

a stan początkowy to $\frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle) \otimes |10\rangle$.

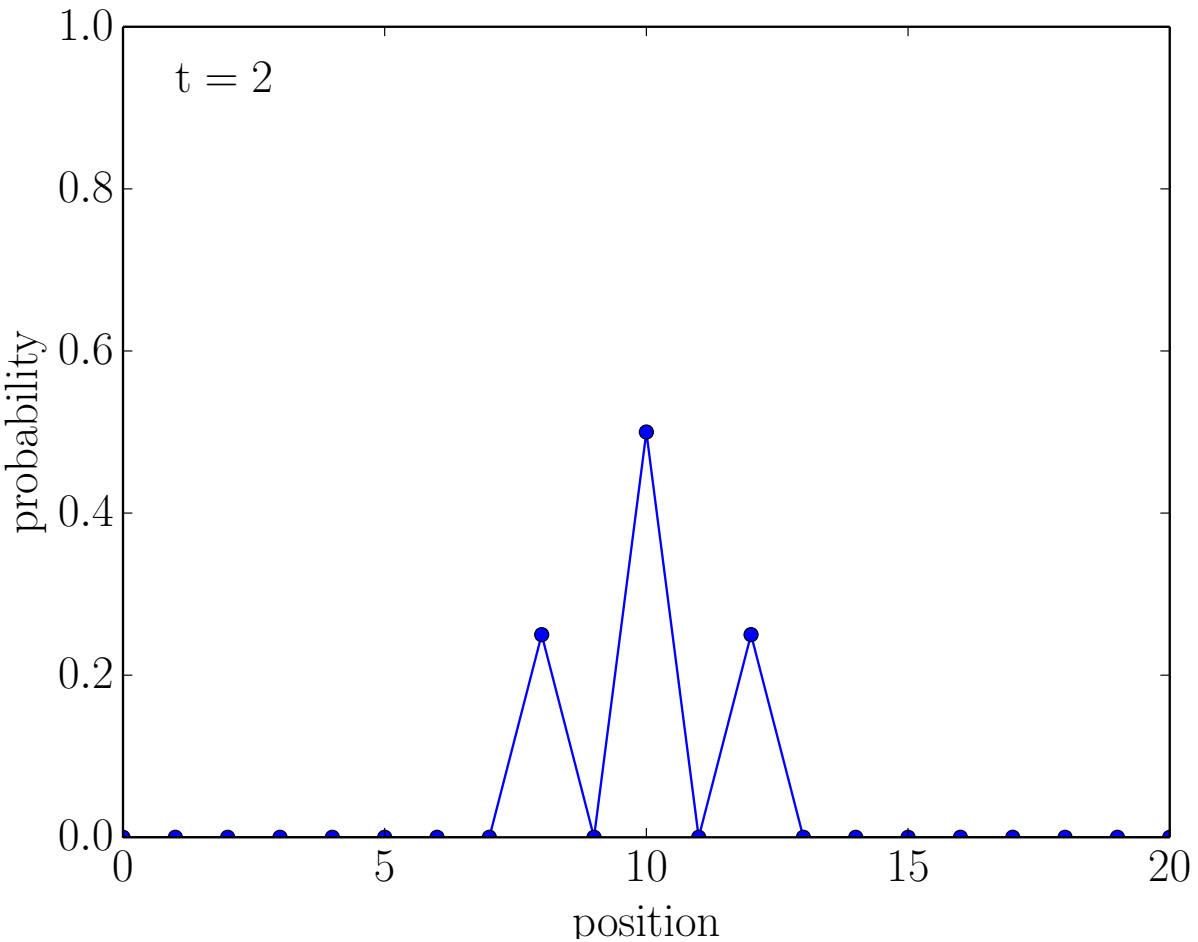
Błądzenie po cyklu
Przykład



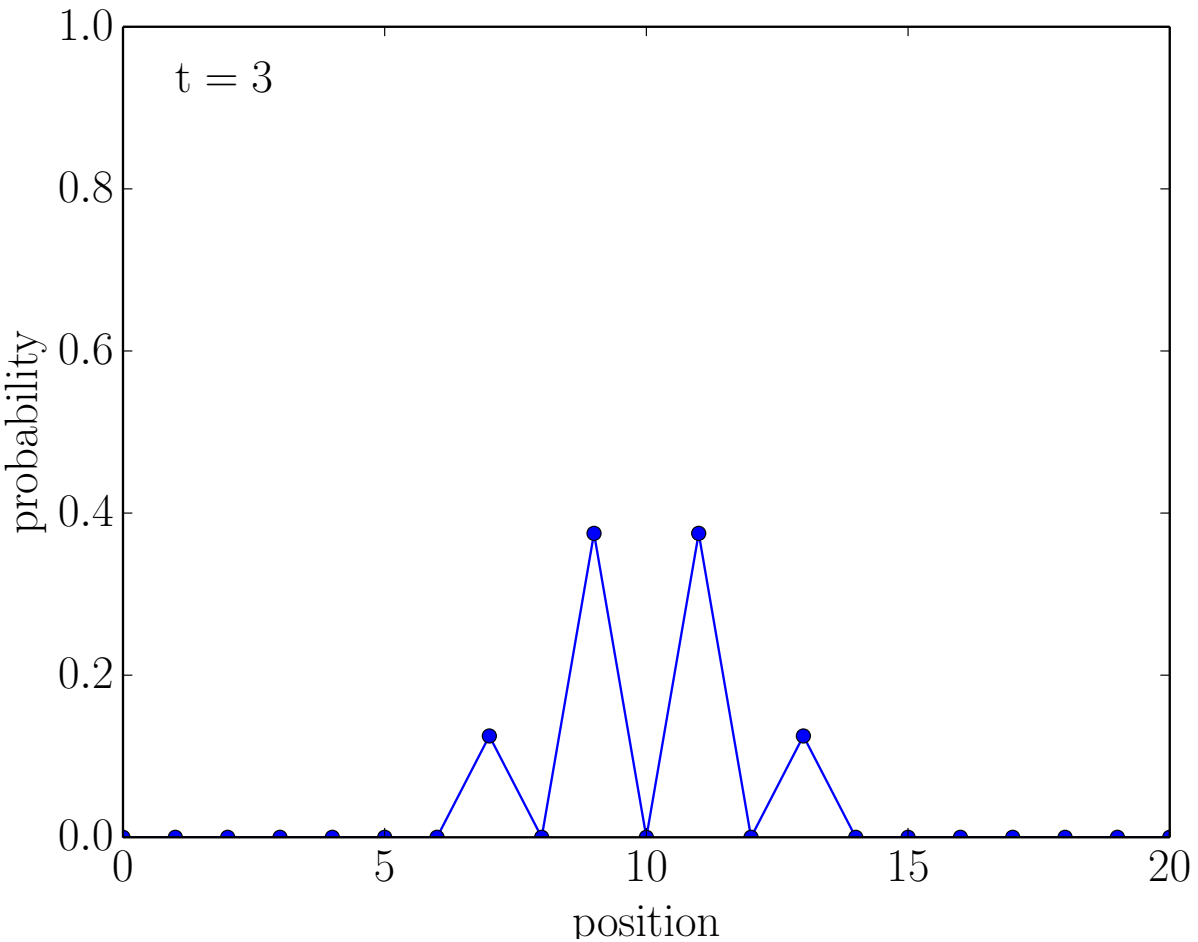
Błądzenie po cyklu
Przykład



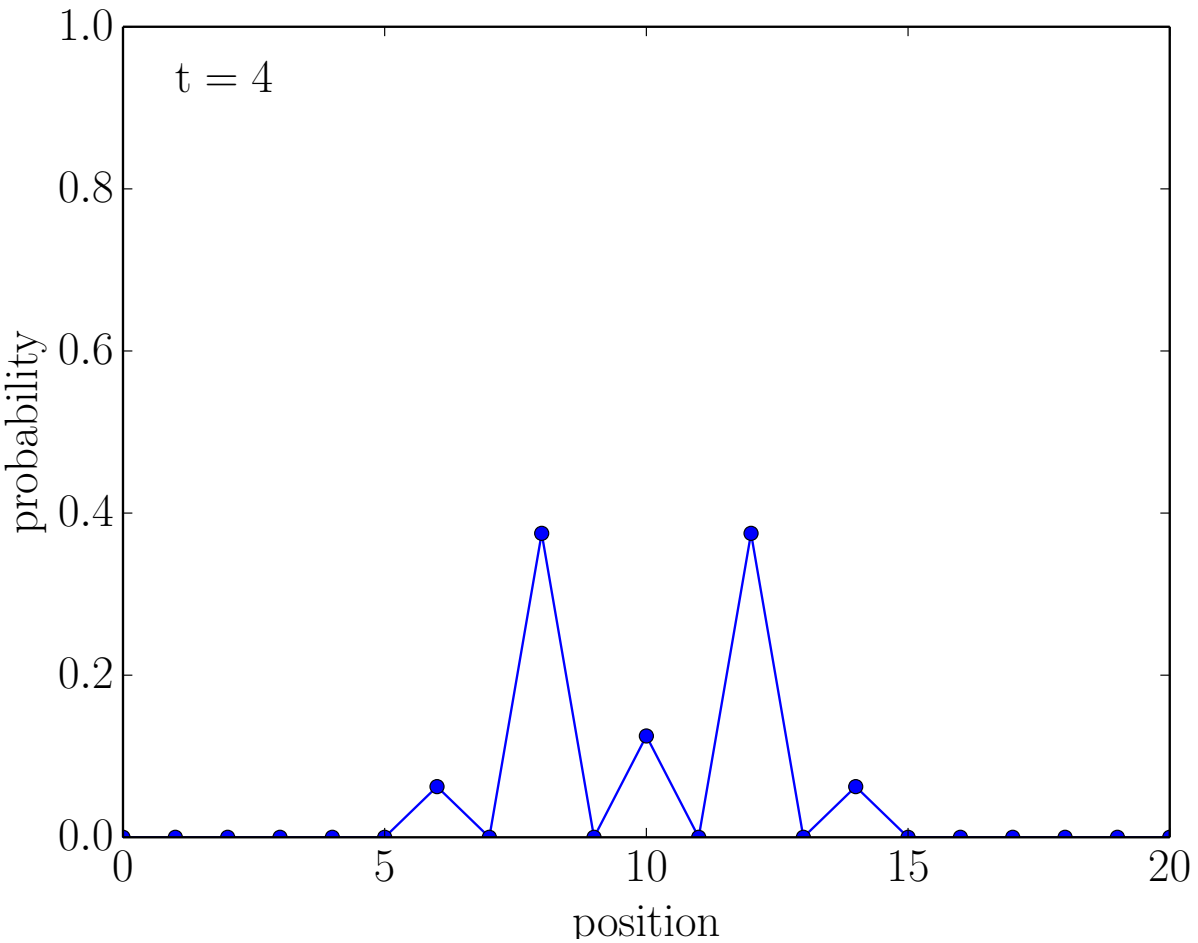
Błądzenie po cyklu
Przykład



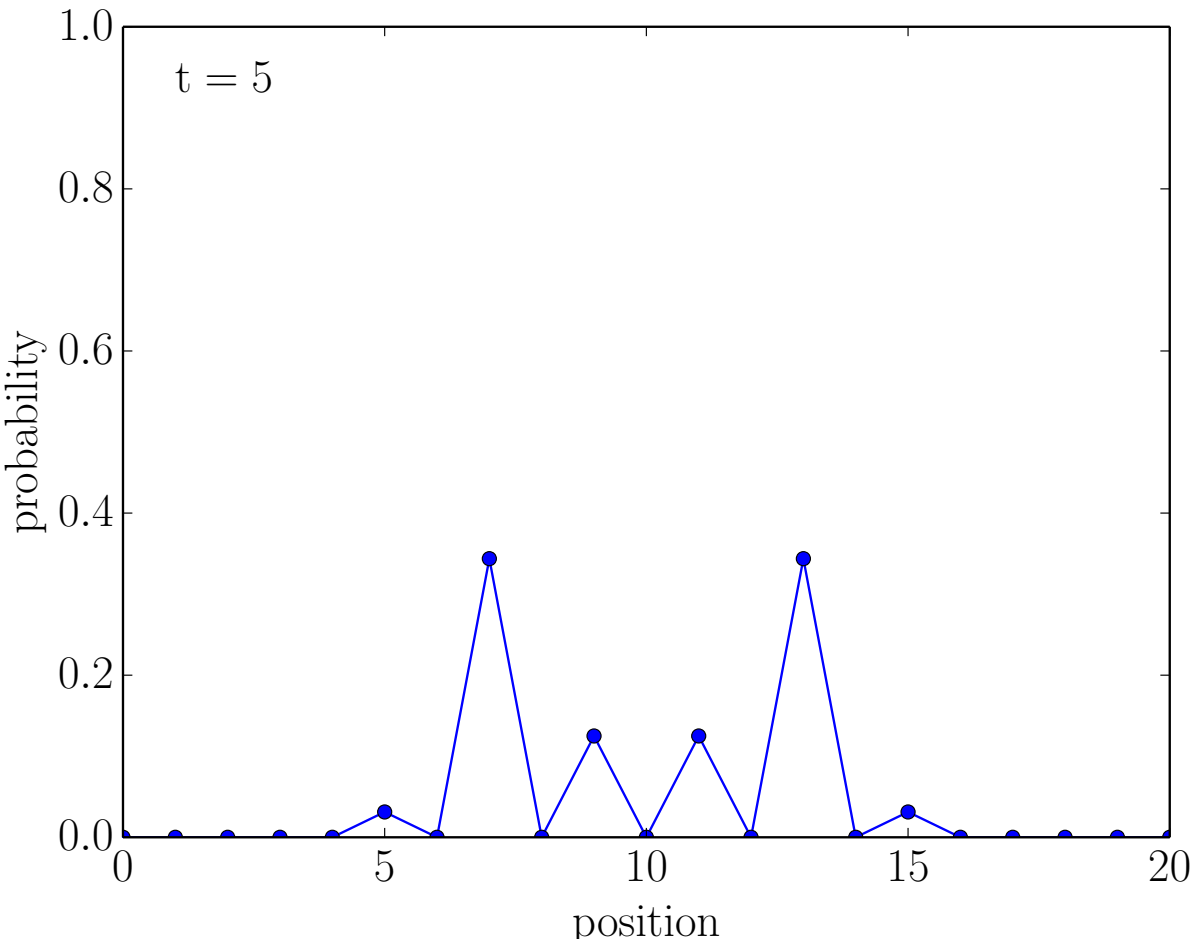
Błądzenie po cyklu
Przykład



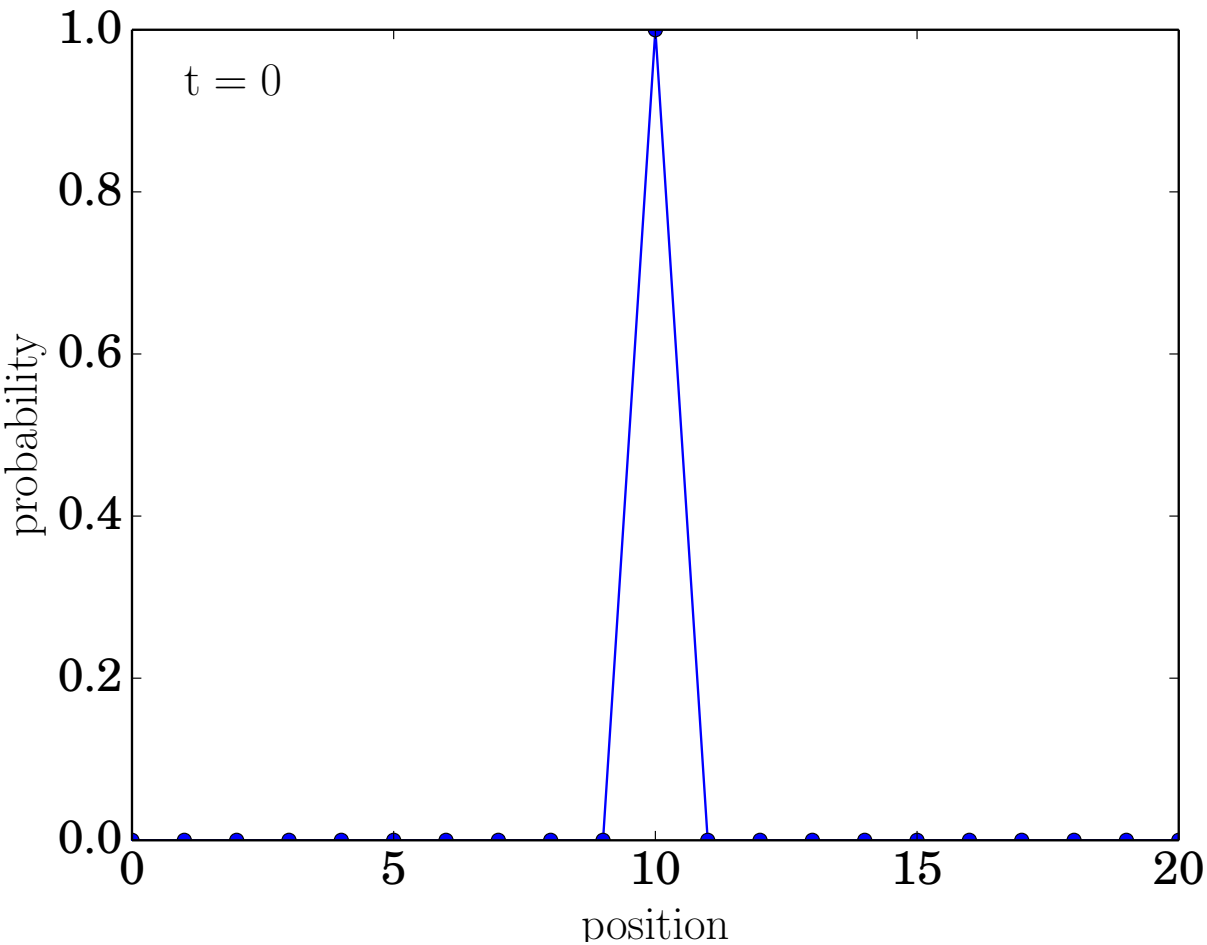
Błądzenie po cyklu
Przykład



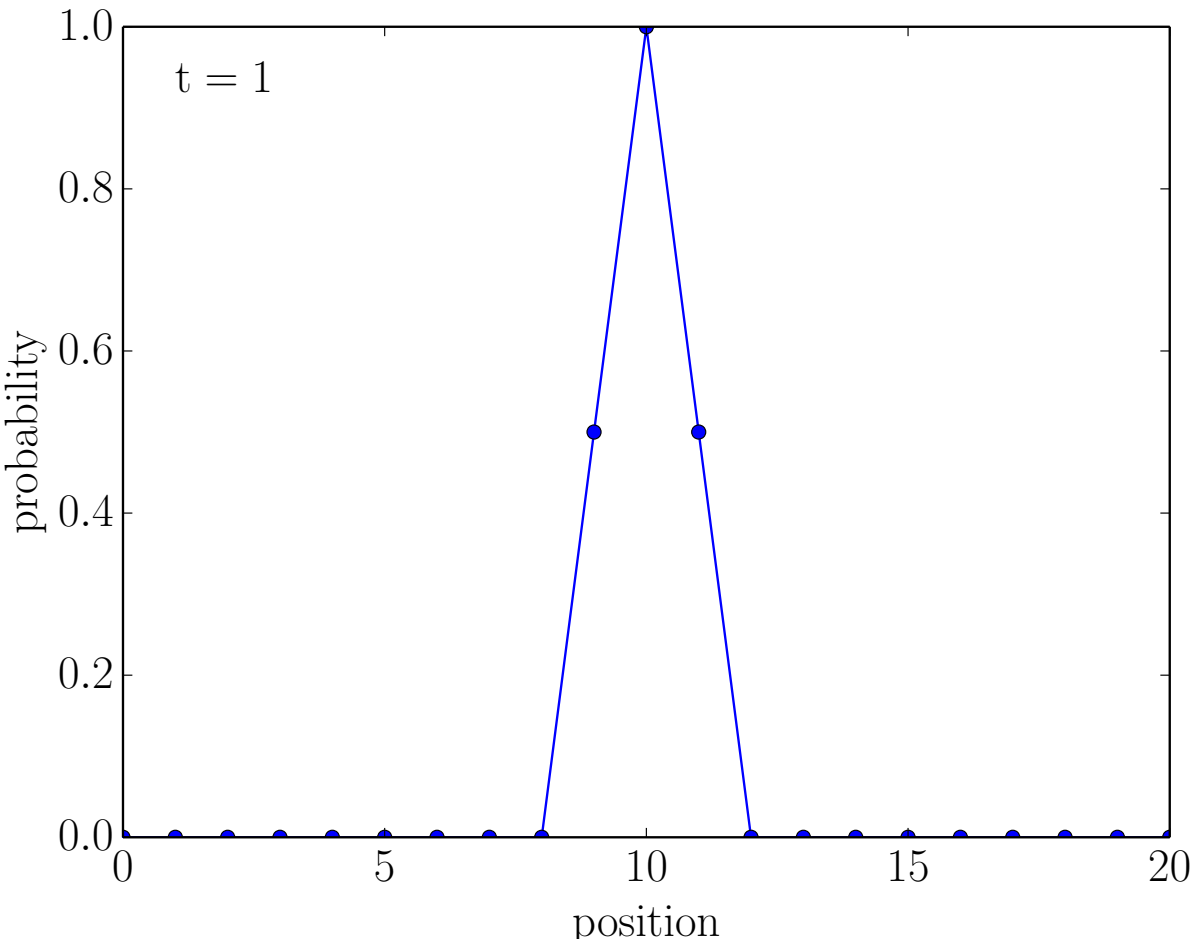
Błądzenie po cyklu
Przykład



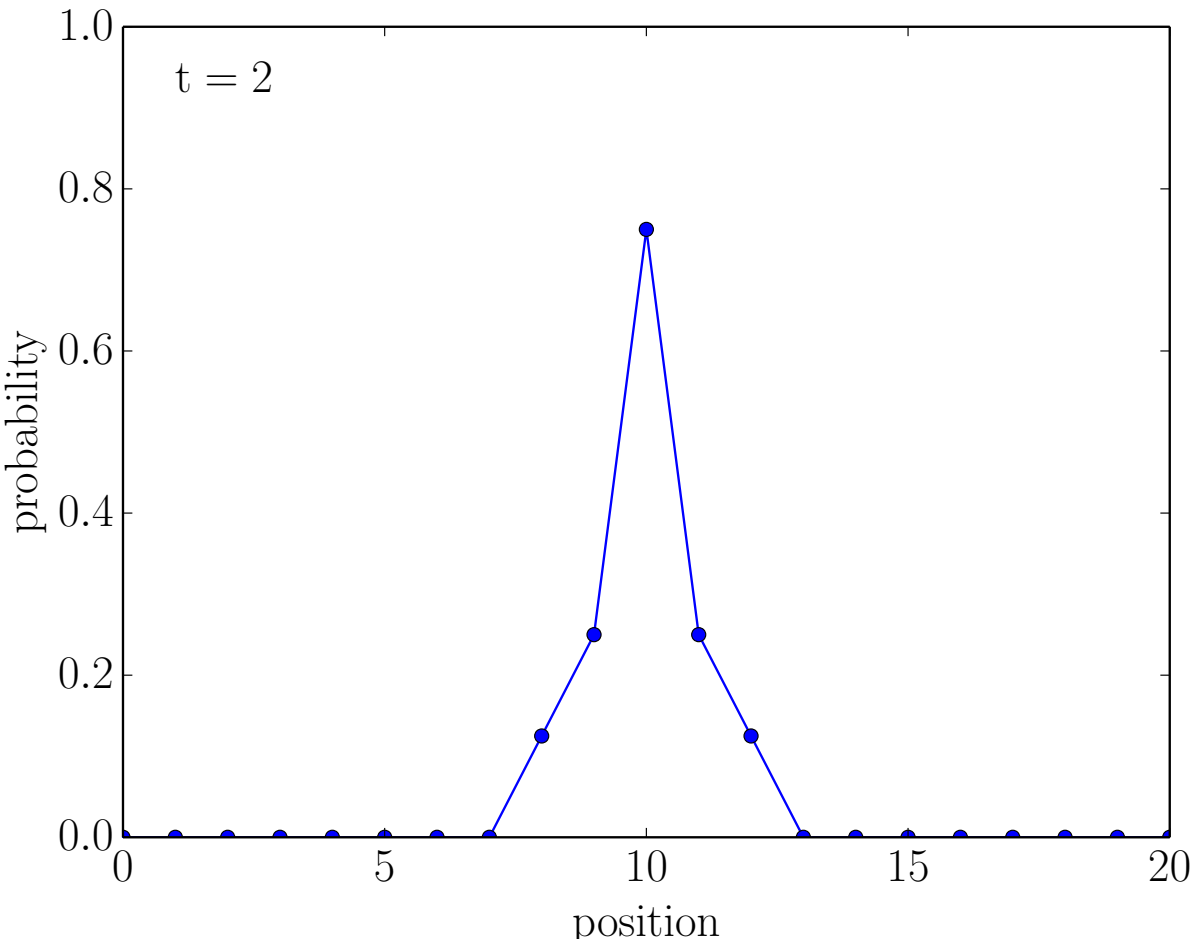
Błądzenie po cyklu
Przykład



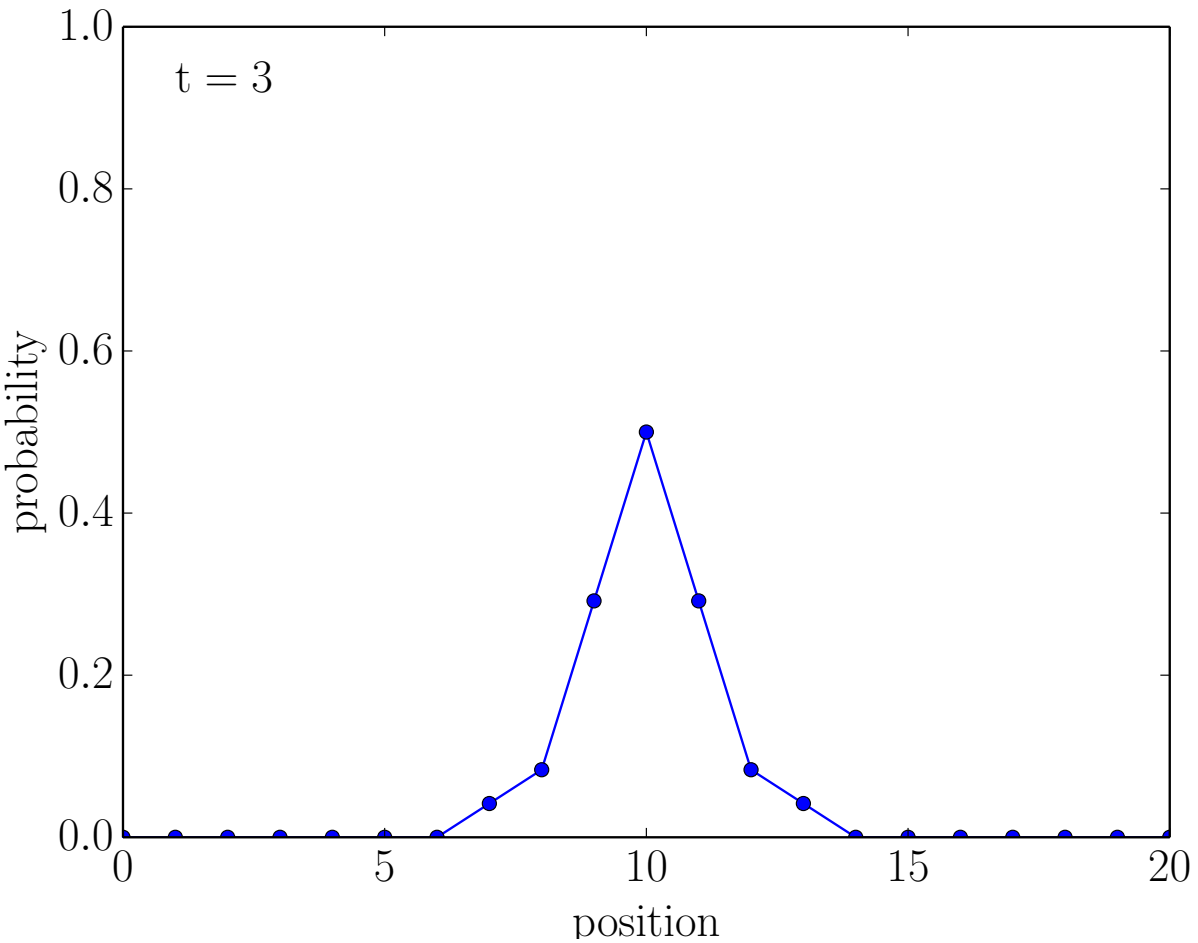
Błądzenie po cyklu
Przykład



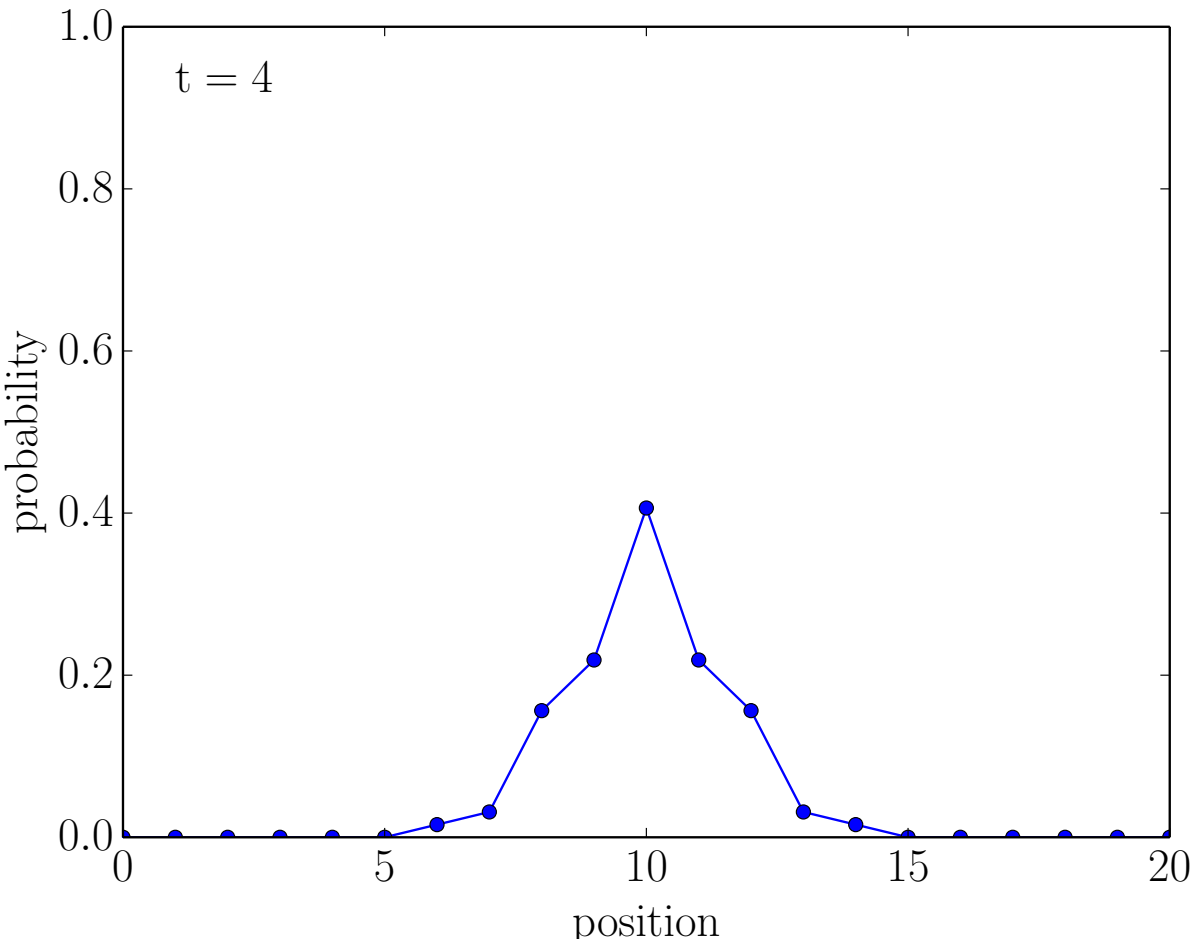
Błądzenie po cyklu
Przykład



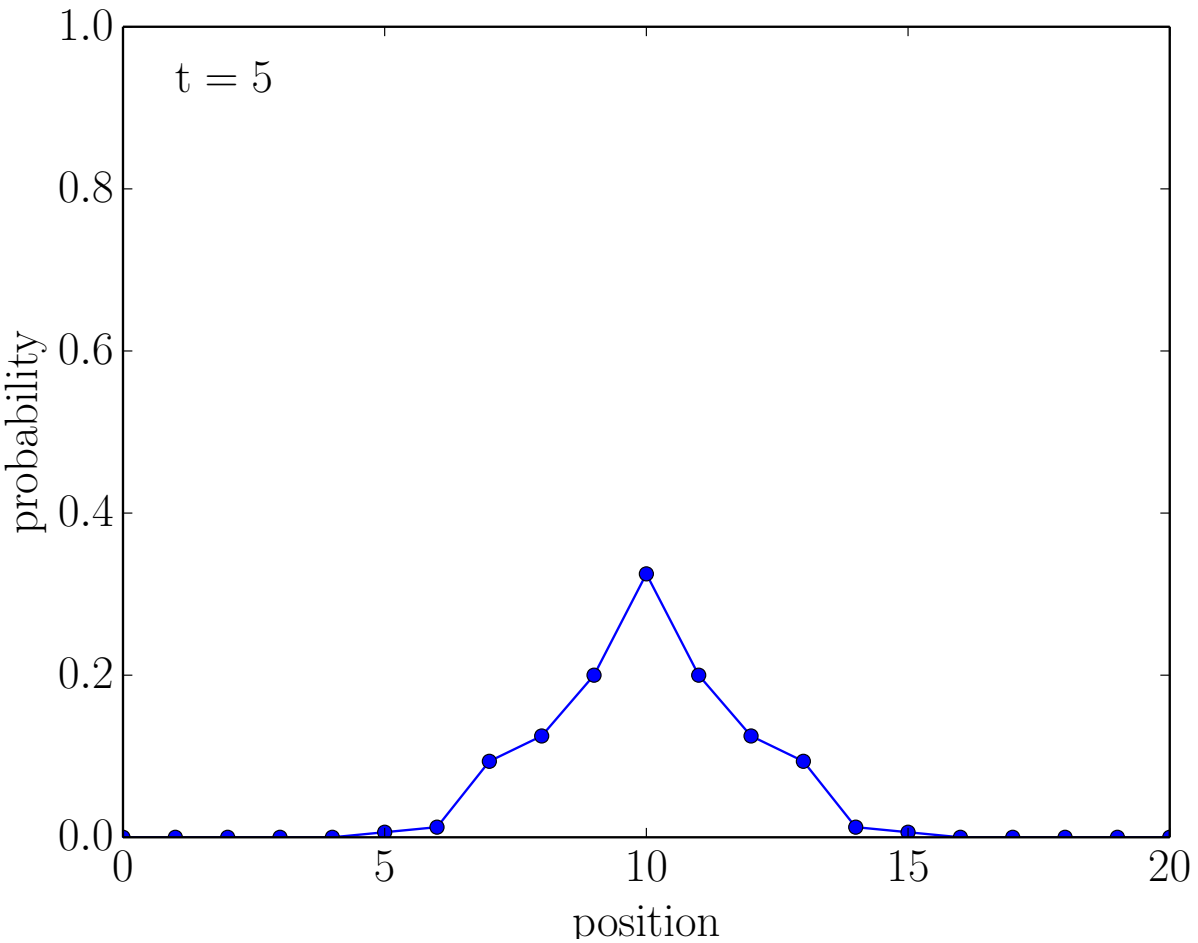
Błądzenie po cyklu
Przykład



Błądzenie po cyklu
Przykład

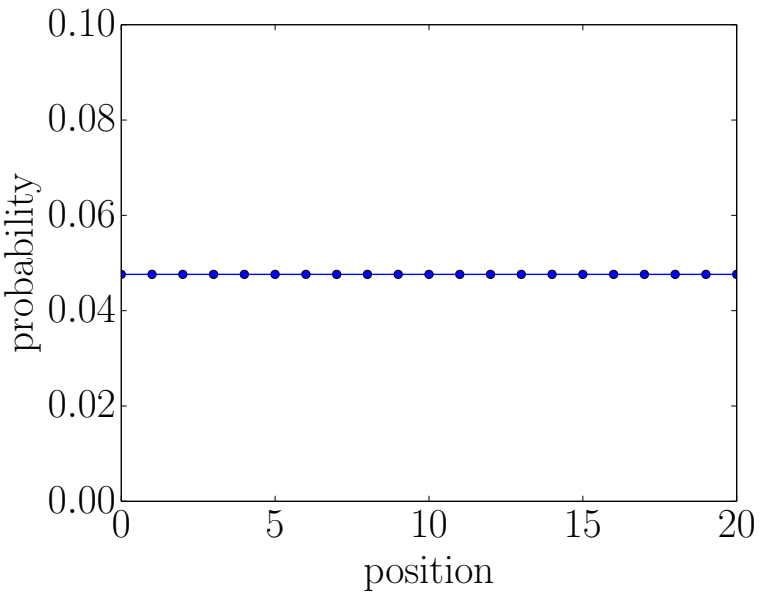


Błądzenie po cyklu
Przykład

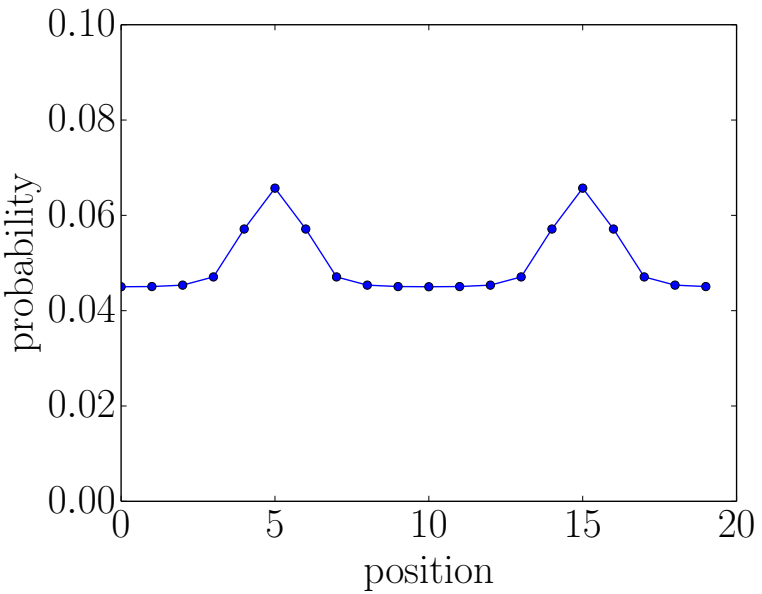


Błądzenie po cyklu
Przykład

Dla cyklu rozkład graniczny jest okresowy lub stały w zależności od parzystości.



21 wierzchołki



20 wierzchołków

Żwawe błądzenie po cyklu

- Topologia cyklu pozwala na wprowadzenie przejść długozasięgowych $\mapsto$ żwawe błądzenie kwantowego.
- Wzbogacenie cyklu od dodatkowe przejścia pozwala na modelowanie zachowania w sieciach złożonych.
- Dodatkowe przejścia mogą modelować grafy skierowanie $\mapsto$ przykład to gra Magnusa i Dereka.

Żwawe błądzenie po cyklu

Żwawe błądzenie kwantowe

Żwawe błądzenie po cyklu z n węzłami i *żwawością* $0 < a \leqslant \lfloor \frac{n}{2} \rfloor$, jest określone przez operator przesunięcia $S^{(n,a)} \in L(\mathbb{C}^3 \otimes \mathbb{C}^n)$ postaci

$$S^{(n,a)} = \sum_{x=0}^{n-1} S_x^{(n,a)}, \tag{4}$$

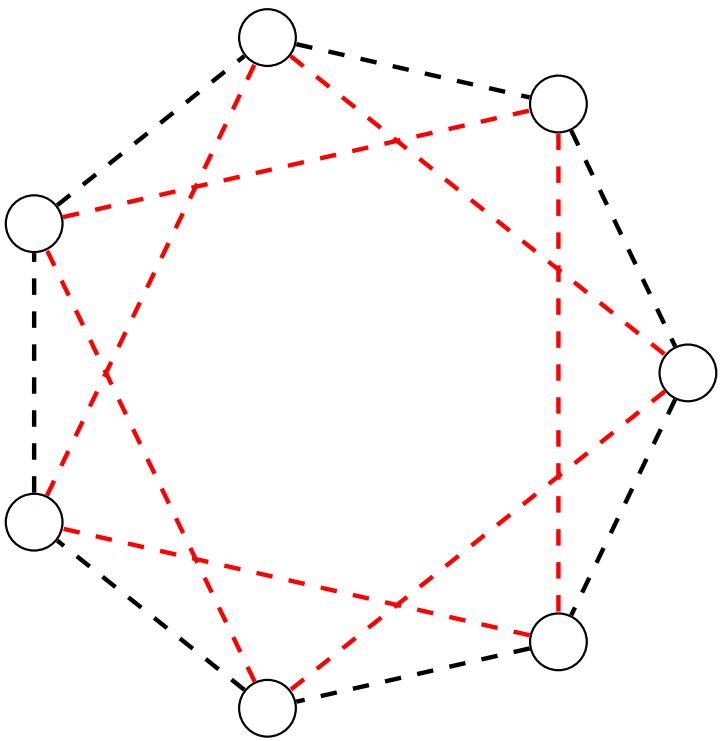
gdzie

$$S_x^{(n,a)} = \sum_{c=0}^{2} |c\rangle\langle c| \otimes |x + \Delta_c \bmod n\rangle\langle x|, \tag{5}$$

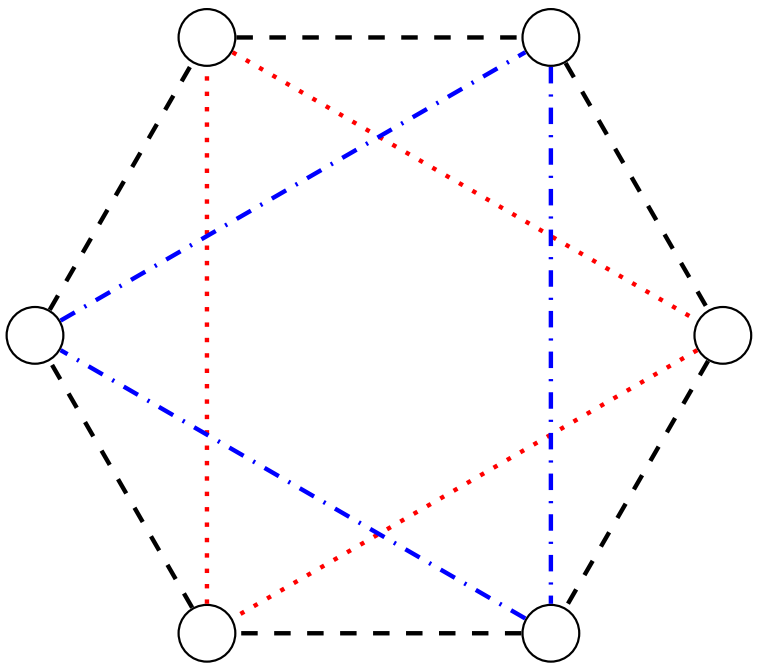
oraz $\Delta_c = \delta_{c,0} - \delta_{c,1} + a\delta_{c,2}$.

Żwawe błądzenie po cyklu

Sieć dla żwawego błądzenia kwantowego z $n = 6$ oraz $n = 7$ węzłów oraz parametrem $a = 2$.



(a) Przypadek aperiodyczny



(b) Przypadek periodyczny

Żwawe błądzenie po cyklu

Periodyczność

Rozważmy żwawe błądzenie po cyklu o n węzłach z parametrem a takim, że $\mathrm{NWD}(n, a) > 1$. Operatorem monety będzie macierz Grovera

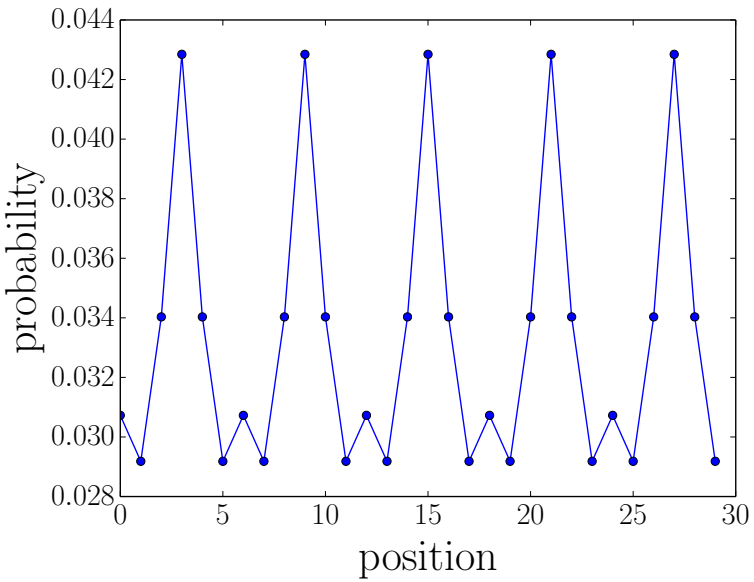
$$G = \frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}. \tag{6}$$

Okresowość rozkładu granicznego

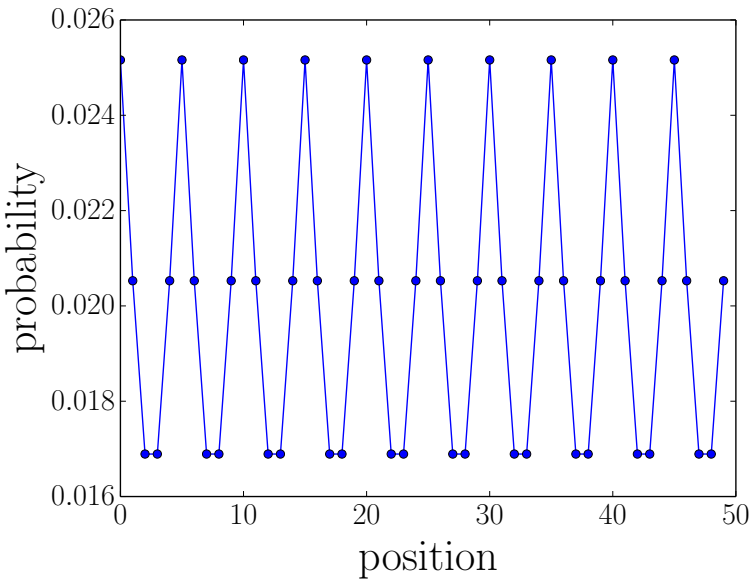
Jeżeli $\mathrm{GCD}(a, n) > 1$ to wówczas graniczny uśredniony po czasie rozkład prawdopodobieństwa jest periodyczny z okresem to $\mathrm{GCD}(a, n)$.

Żwawe błądzenie po cyklu

Periodyczność



$n = 30,\ a = 6$



$n = 50,\ a = 15$

Uśredniony po czasie rozkład prawdopodobieństwa dla żwawego błądzenia na n węzłach, gdzie a jest żwawością błądzenia.

Żwawe błądzenie po cyklu

Żwawość

Model żwawego błądzenia ma też pożądane z punktu widzenia eksploracji grafu własności unikania uwięzienia.
Rozważmy scenariusz w którym mamy dwóch agentów/graczy

- zadaniem pierwszego jest zmaksymalizowanie liczby odwiedzonych węzłów,
- zadaniem drugiego jest ograniczenia działań pierwszego poprzez uwięzienie błądzącej cząstki,
- pierwszy gracz wybiera stan początkowy,
- drugi gracz może w każdej turze wybrać operator monety.

Żwawe błądzenie po cyklu

Żwawość

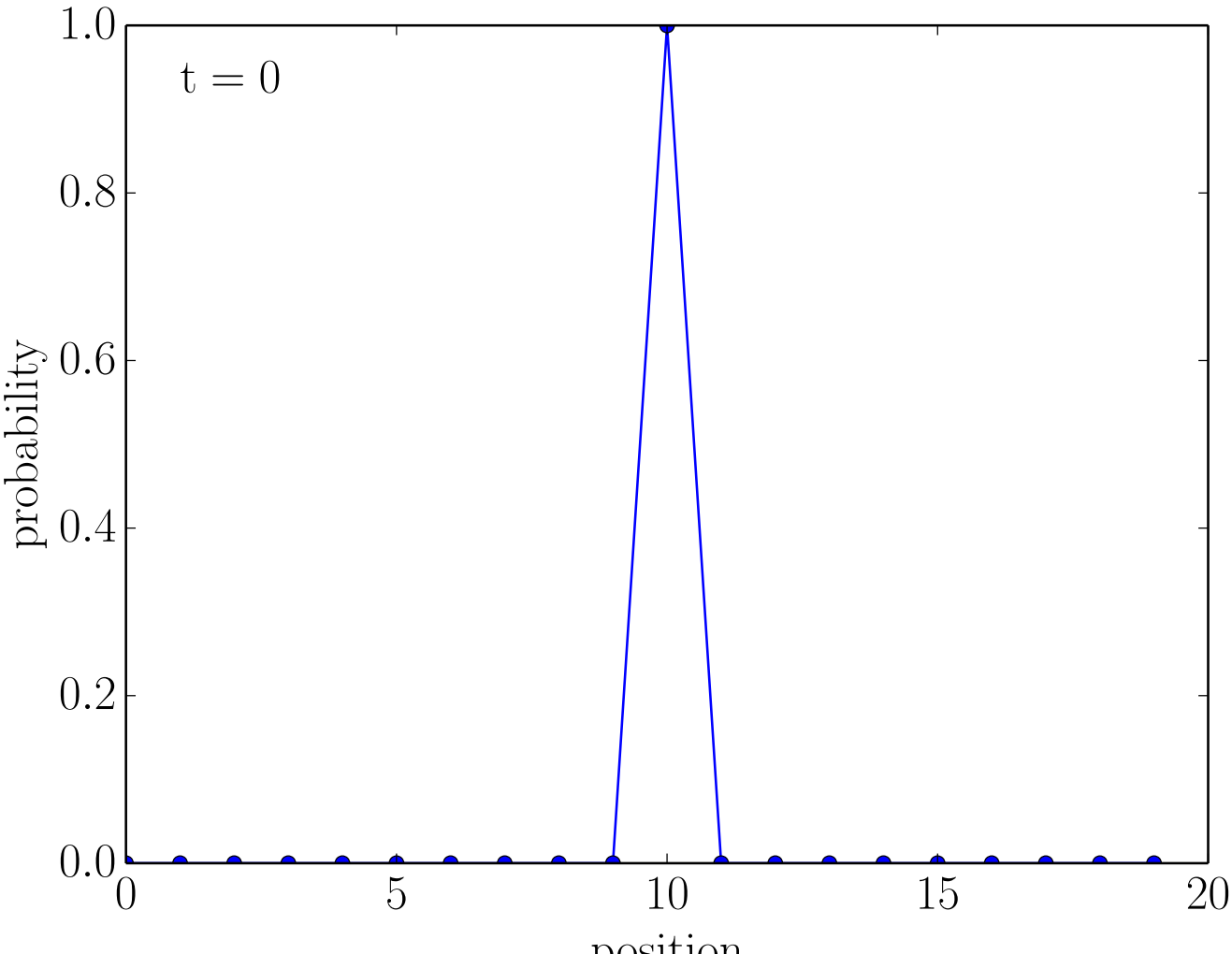
W przypadku błądzenia kwantowego bardzo łatwo jest dobrać monetę, tak aby uniemożliwić eksplorację grafu.

Przyjmijmy $n = 20$ i stan początkowy $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes |10\rangle$. Wystarczy, że drugi gracz wybierze

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{7}$$

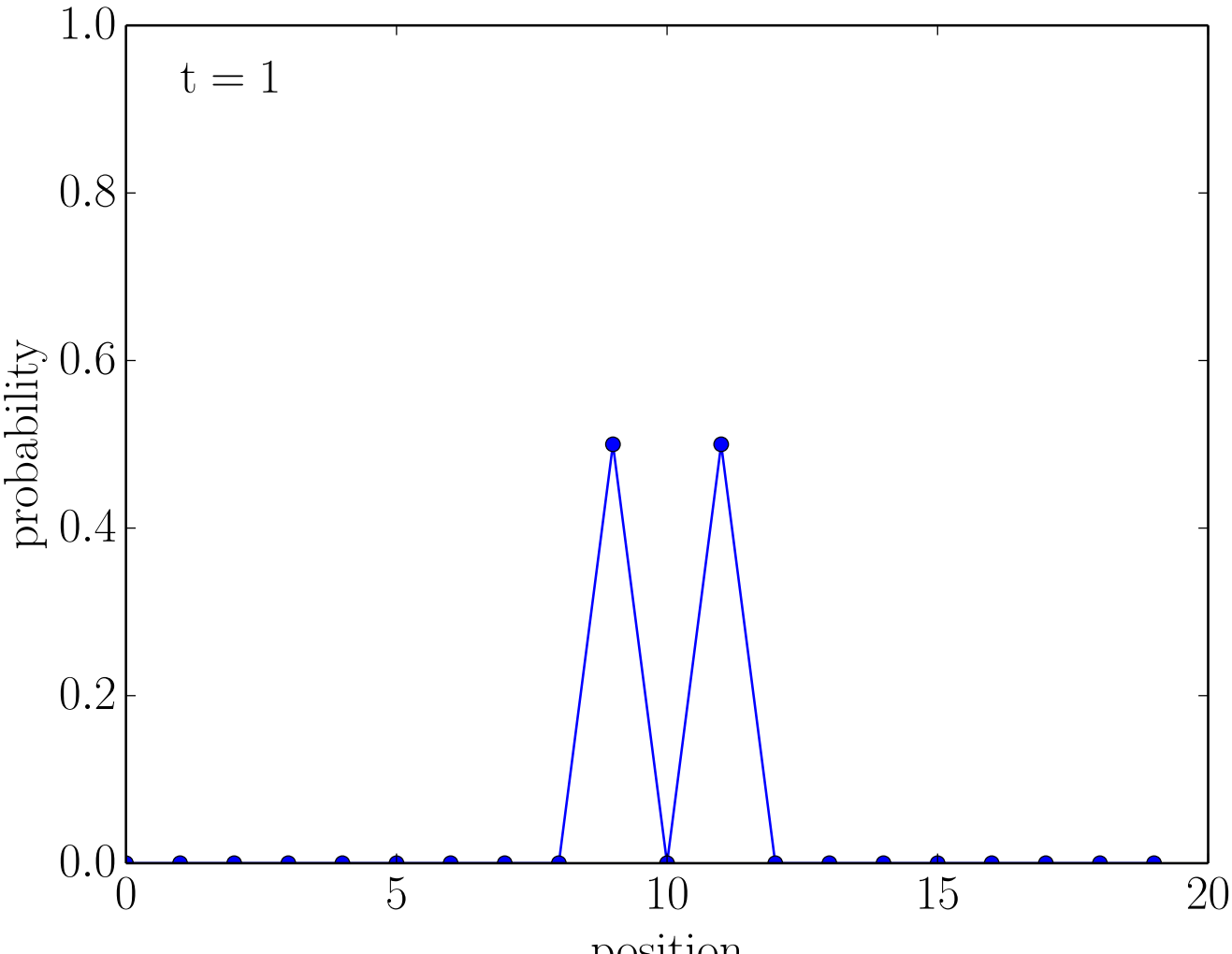
Żwawe błądzenie po cyklu

Żwawość



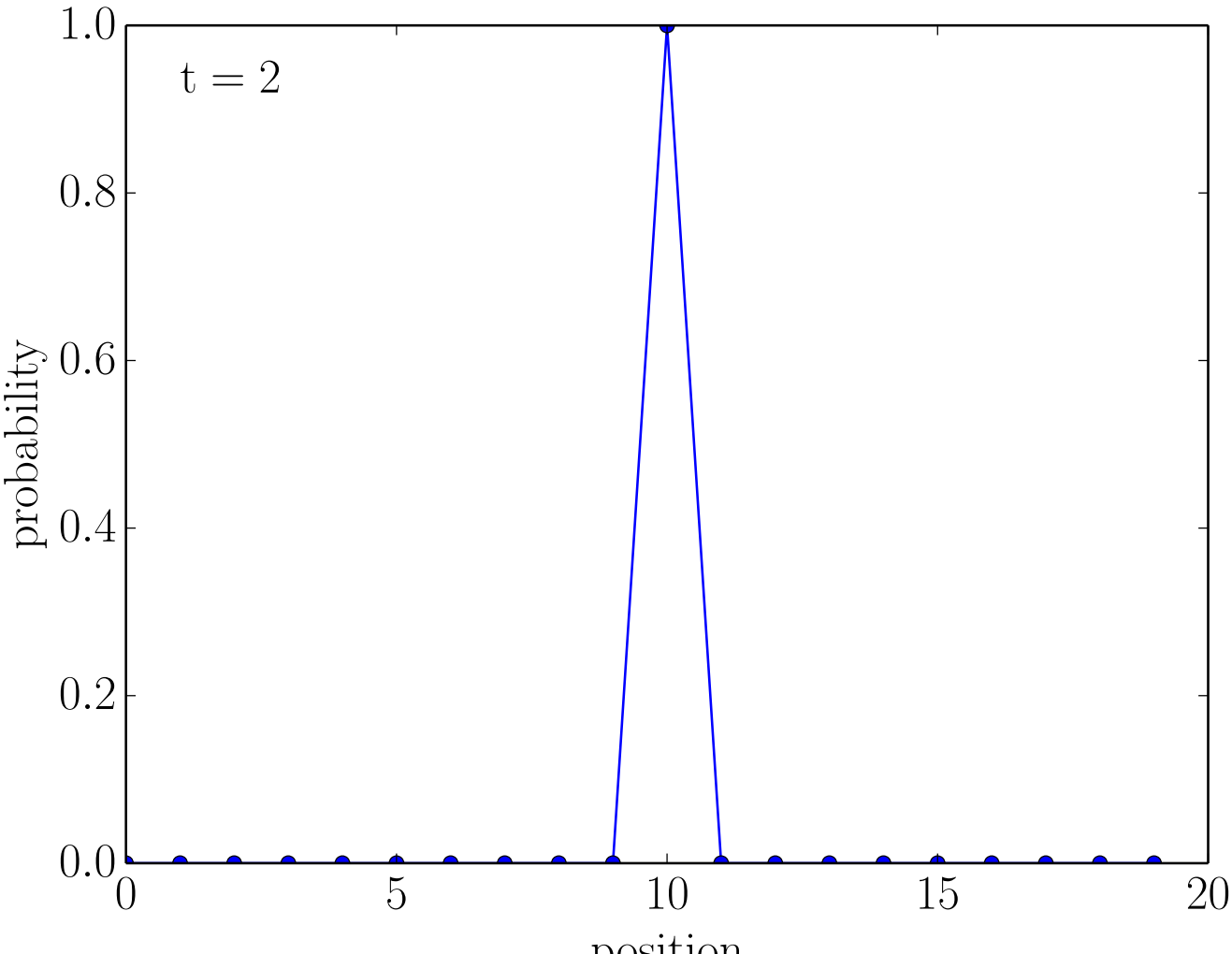
Żwawe błądzenie po cyklu

Żwawość



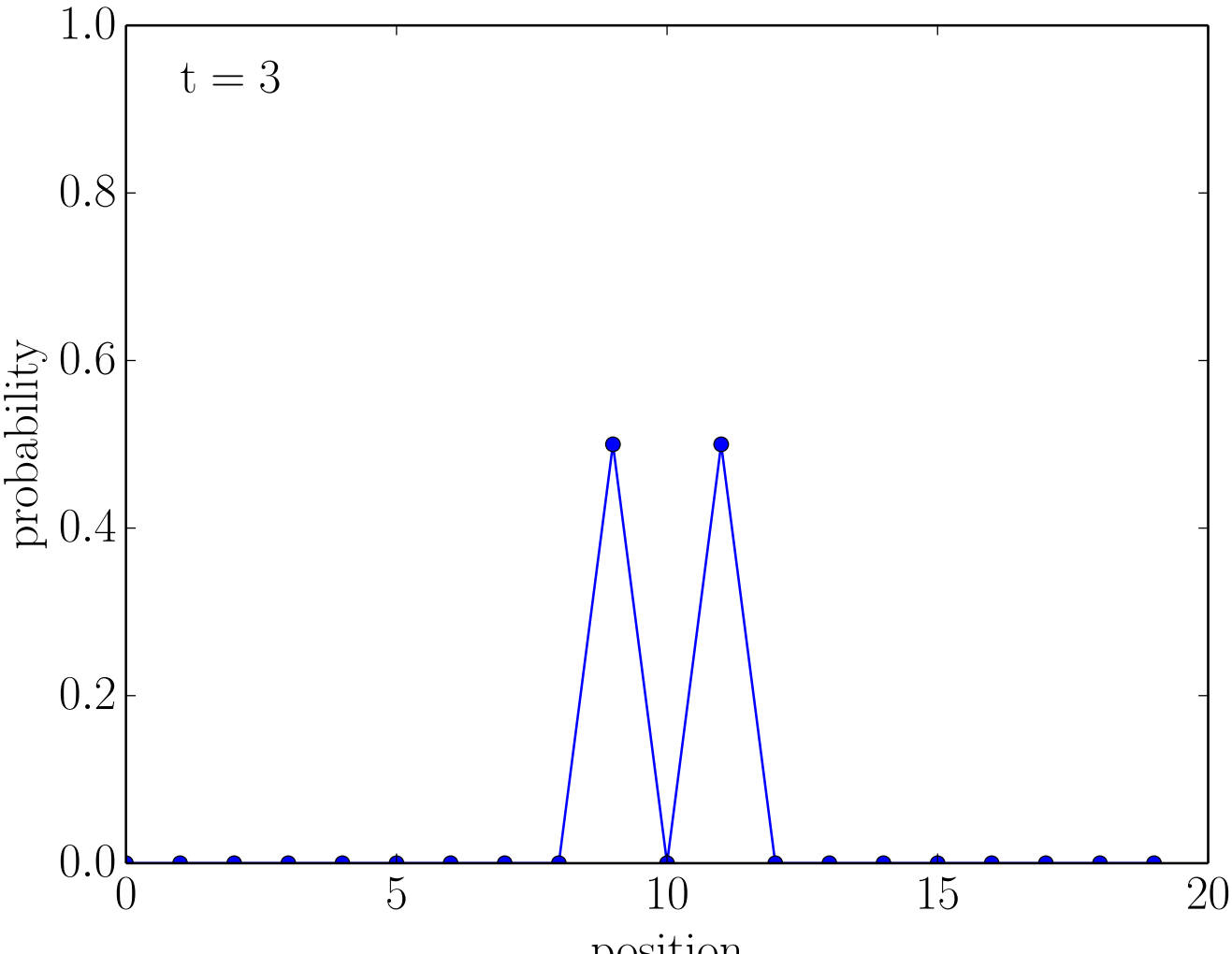
Żwawe błądzenie po cyklu

Żwawość



Żwawe błądzenie po cyklu

Żwawość



Żwawe błądzenie po cyklu

Żwawość

Przez X^{ρ_t} oznaczamy zmienną losową wyniku pomiaru położenia w czasie t.

Żwawość

Przyjmijmy, że proces żwawego błądzenia kwantowego rozpoczynamy w pozycji początkowej $|x_0\rangle$. Jeżeli stan początkowy monety jest wylosowany jako jeden ze stanów bazowych, to dla dowolnej (zależnej od czasu) monety C_t, różnica wartości oczekiwanych położenia $\mathbb{E}(X^{\rho_{t+1}}) - \mathbb{E}(X^{\rho_t})$ jest zawsze dodatnia i równa $\frac{a}{3}$.

Oznacza to, że każdym kroku cząstka przesuwa się średnio o $\frac{a}{3}$.

Podsumowanie

- Główną siła obliczeń kwantowych jest możliwość wykorzystania superpozycji.
- Algorytmy kwantowe muszą być odpowiednio zaprojektowane aby dawać pożądane przyśpieszenie.
- W przypadku protokołów i komunikacji kwantowej najistotniejszą cechą jest splątani – daje on możliwość koordynacji działań.
- Do analizy modeli dyskretnych (np. gier kombinatorycznych) naturalnie pasuje model dyskretnego błądzenia.

Dziękuję za uwagę!