Algorytmy kwantowe

Zbigniew Puchała

Instytut Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk

2024

Algorytm Shora

Wprowadzenie

- Algorytm Shora to kwantowy algorytm umożliwiający faktoryzację liczby N.
- Opracowany przez Petera Shora w 1994 roku.
- Stanowi zagrożenie dla kryptosystemów opartych na RSA.

Znaczenie problemu faktoryzacji

- RSA opiera się na trudności faktoryzacji dużych liczb.
- Algorytm Shora umożliwia szybkie odtworzenie klucza prywatnego.
- Klucz publiczny: $N = p \cdot q$, gdzie p, q są liczbami pierwszymi.

Czas działania algorytmu

- Algorytm działa w czasie $O((\log N)^3)$.
- Pamięć: $O(\log N)$.
- Klasyczne algorytmy faktoryzacji są wykładnicze.

Struktura algorytmu

1. Część klasyczna: Redukcja problemu do znajdowania okresu.
2. Część kwantowa: Znalezienie okresu funkcji.

Klasyczna redukcja

Klasyczna redukcja problemu

Aby zredukować problem faktoryzacji:

- Wybieramy N, nieparzystą liczbę złożoną.
- Problem faktoryzacji N sprowadzamy do znalezienia dwóch liczb p i q takich, że:

$$N = p \cdot q, \quad p, q > 1.$$

- Powtarzamy procedurę, aż znajdziemy wyłącznie liczby pierwsze.

Kluczowe obserwacje

- Za pomocą algorytmu Euklidesa możemy szybko obliczyć $\mathrm{nwd}(a, b)$.
- Sprawdzamy efektywnie, czy N jest liczbą parzystą:

  Jeśli N jest parzysta, to 2 jest czynnikiem.

- Jeśli N nie jest potęgą liczby pierwszej:
  - Stosujemy algorytm kwantowy do znajdowania rzędu r.

Znalezienie rzędu

Definicja rzędu liczby

- Dla liczby a, rząd r modulo N to najmniejsza liczba $r > 0$, dla której:

$$a^r \equiv 1 \pmod{N}.$$

- Jeśli znamy r, możemy znaleźć czynniki N za pomocą:

$$N \mid (a^{r/2} - 1)(a^{r/2} + 1).$$

Podejście kwantowe: Znalezienie r

- Algorytm kwantowy wykorzystuje interferencję kwantową i transformację Fouriera.
- Jeśli r jest parzyste, możemy zapisać:

$$N \mid (a^{r/2} - 1)(a^{r/2} + 1).$$

- Obliczamy:

$$d = \mathrm{nwd}(N, a^{r/2} - 1) \quad \text{lub} \quad d = \mathrm{nwd}(N, a^{r/2} + 1).$$

Szczegóły redukcji klasycznej

1. Wybieramy losowo a z przedziału $2 \leqslant a < N$.
2. Obliczamy $\mathrm{nwd}(a, N)$:
   - Jeśli $\mathrm{nwd}(a, N) > 1$, znaleziono czynnik.
3. Znajdujemy rząd r:
$$a^r \equiv 1 \pmod{N}.$$
4. Wyznaczamy czynniki za pomocą nwd:
$$d = \mathrm{nwd}(N, a^{r/2} - 1).$$

Kwantowy podproblem

Transformacja Fouriera i znajdowanie okresu

- Kwantowa transformacja Fouriera (QFT) identyfikuje okres funkcji $f(k) = a^k \mod N$.
- Wynik QFT zawiera szczyty odpowiadające wielokrotnościom r, czyli okresowi funkcji.
- Pomiar na końcu obliczeń pozwala na wyznaczenie r z wysokim prawdopodobieństwem.

Przykład faktoryzacji

Dla $N = 15$:

- Wybieramy $a = 7$.
- Obliczamy r za pomocą QFT: $r = 4$.
- Wyznaczamy czynniki:

$$d_1 = \text{nwd}(15, 7^{4/2} - 1) = \text{nwd}(15, 48) = 3,$$

$$d_2 = \text{nwd}(15, 7^{4/2} + 1) = \text{nwd}(15, 50) = 5.$$

Przegląd podproblemu kwantowego

- Podproblem kwantowy składa się z dwóch etapów:
  1. Kwantowe oszacowanie fazy (QPE): Koduje informacje o r.
  2. Algorytm ułamków łańcuchowych: Wyciąga r z wyników pomiarów.
- Układ kwantowy wykorzystuje dwa rejestry:
  - Pierwszy rejestr: $2n$ kubitów dla odpowiedniej dokładności.
  - Drugi rejestr: n kubitów dla operacji modulo.

Struktura układu kwantowego

Układ kwantowy: Rejestry i stany

- Układ operuje na dwóch rejestrach:
  - Pierwszy rejestr: $2n$ kubitów, inicjalizowany jako $|0\rangle^{\otimes 2n}$.
  - Drugi rejestr: n kubitów, inicjalizowany jako $|1\rangle$.
- Stan początkowy układu:
$$|0\rangle^{\otimes 2n} \otimes |1\rangle.$$
- Operator U reprezentuje mnożenie modulo N i działa na drugim rejestrze.

Część klasyczna

1. Wylosowanie liczby $a < N$.
2. Obliczenie $NWD(a, N)$:
   - Jeśli $NWD(a, N) \neq 1$, zakończ – znaleziono dzielnik.
   - W przeciwnym razie przejdź dalej.
3. Znalezienie okresu r, gdzie $f(x) = a^x \mod N$.

Znalezienie okresu r

- Jeśli r jest nieparzyste, wróć do początku.
- Jeśli $a^{r/2} \equiv -1 \mod N$, wróć do początku.
- Faktoryzacja: $NWD(a^{r/2} \pm 1, N)$.

Część kwantowa: Znalezienie okresu funkcji

1. Przygotowanie rejestrów kwantowych.
2. Implementacja funkcji $f(x) = a^x \mod N$.
3. Zastosowanie kwantowej transformaty Fouriera (QFT).
4. Pomiar i analiza wyników.

Przykład działania algorytmu

- Dla $N = 15$, $a = 7$.
- Znaleziono $r = 4$.
- Faktoryzacja: $NWD(7^2 - 1, 15) = 3$, $NWD(7^2 + 1, 15) = 5$.

Wyzwania implementacyjne

- Precyzyjna implementacja QFT.
- Optymalizacja liczby kubitów i bramek kwantowych.
- Błędy i dekoherencja w systemach kwantowych.

Zastosowania

- Złamanie kryptosystemów RSA.
- Rozwój kryptografii postkwantowej.
- Badania nad właściwościami grup i funkcji okresowych.

Zagrożenia dla bezpieczeństwa

- Możliwość łamania szyfrowania klucza publicznego.
- Konieczność opracowania nowych standardów kryptograficznych.

Podsumowanie

- Algorytm Shora to jeden z najważniejszych algorytmów kwantowych.
- Jego potencjalne zastosowania zmieniają przyszłość kryptografii.
- Wymaga zaawansowanego sprzętu kwantowego do praktycznego zastosowania.

Źródła

- P. Shor, „Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, 1994.

Transformacja Fouriera

Wprowadzenie

- Transformacja Fouriera to fundamentalne narzędzie w analizie funkcji.
- Quantum Fourier Transform (QFT) adaptuje klasyczną transformację Fouriera do obliczeń kwantowych.
- Zastosowania:
  - Algorytm znajdowania okresu (period-finding).
  - Algorytm Shora do faktoryzacji liczb.
- QFT nad Z_N jest kluczowym elementem tych algorytmów.

Transformacja Fouriera dla funkcji

Transformacja Fouriera nad Z_N

Definicja

Dla funkcji $g : Z_N \to \mathbb{C}$, transformacja Fouriera nad Z_N jest zdefiniowana jako:

$$\hat{g}(\gamma) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} g(x) e^{-2\pi i \gamma x / N}$$

- $x, \gamma \in Z_N$: zmienne w grupie modulo N.
- $\hat{g}(\gamma)$: współczynniki Fouriera.

Odwrotna transformacja Fouriera

$$g(x) = \frac{1}{\sqrt{N}} \sum_{\gamma=0}^{N-1} \hat{g}(\gamma) e^{2\pi i \gamma x / N}$$

Właściwości QFT

- **Liniowość:** Transformacja Fouriera zachowuje liniowość funkcji.
- **Ortogonalność:** Wynikowe funkcje bazowe $e^{-2\pi i \gamma x/N}$ są ortogonalne.
- **Unitarność:** QFT jest realizowana jako macierz unitarna.
- **Efektywność:** QFT można zaimplementować na komputerze kwantowym w czasie $O(n^2)$, gdzie $n = \log_2 N$.

Implementacja QFT

Obwód kwantowy dla QFT

- Wejście: Stan kwantowy $|x\rangle$, gdzie $x \in \{0, 1, \ldots, N-1\}$.
- Wyjście:

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{\gamma=0}^{N-1} e^{-2\pi i \gamma x / N} |\gamma\rangle$$

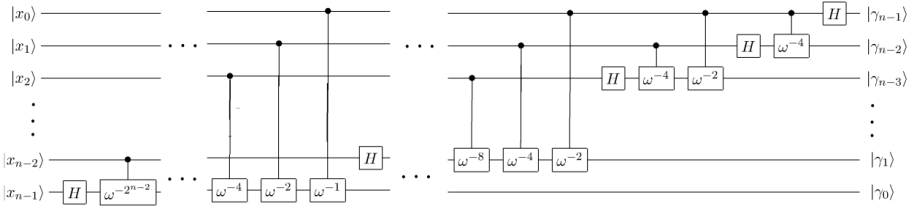
- Obwód wykorzystuje:
  - Bramki Hadamarda (H).
  - Bramki przesunięcia fazowego (R_k):

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{pmatrix}$$

  - Bramki kontrolowane (Controlled-Phase).

Schemat obwodu

- Realizacja obwodu dla $n = \log_2 N$ qubitów:
  1. Na każdym qubicie zastosuj Hadamarda (H).
  2. Dodaj kontrolowane przesunięcia fazowe R_k w zależności od niższych bitów.
  3. Na koniec odwróć kolejność qubitów.
- Całkowity koszt: $O(n^2)$ bramek kwantowych.



Podsumowanie

Podsumowanie

- QFT nad Z_N adaptuje klasyczną transformację Fouriera do obliczeń kwantowych.
- Kluczowe etapy:
  - Definicja transformacji dla funkcji.
  - Efektywna implementacja na komputerze kwantowym.
- Zastosowania w algorytmach:
  - Znajdowanie okresów.
  - Faktoryzacja liczb.

Dalsze kroki

Analiza efektywności QFT w praktycznych zastosowaniach.

Znajdowanie okresu funkcji

Definicja problemu znajdowania okresów

Problem znajdowania okresów

Dana jest funkcja $f : Z_N \to X$, dla której:

- $f(x) = f(x + s)$ dla pewnego $s \in Z_N \setminus \{0\}$,
- Wszystkie inne wartości $f(x)$ są różne.

Cel

Znaleźć okres s, korzystając z dostępu do funkcji f poprzez orakulum:

$$O_f(|x\rangle|b\rangle) = |x\rangle|b \oplus f(x)\rangle.$$

Znaczenie problemu

- Rozwiązanie problemu znajdowania okresów to kluczowy element algorytmu Shora do faktoryzacji liczb.
- Klasyczne rozwiązanie jest wydajne tylko dla $N = 2^n$, wymaga $O(\log N)$ prób.
- Algorytm kwantowy generalizuje problem na dowolne N, nie zakładając, że s dzieli N.

Algorytm kwantowy

Kroki algorytmu

1. Przygotuj stan kwantowy:
$$\frac{1}{\sqrt{N}} \sum_{x \in Z_N} |x\rangle.$$
2. Zaaplikuj orakulum O_f:
$$\frac{1}{\sqrt{N}} \sum_{x \in Z_N} |x\rangle |f(x)\rangle.$$
3. Zmierz rejestr odpowiadający wartościom $f(x)$. Stan zmienia się na:
$$\frac{1}{\sqrt{s}} \sum_{x \in H} |x\rangle,$$
gdzie $H = \{0, s, 2s, \dots\}$ to grupa generowana przez s.
4. Zastosuj transformację Fouriera nad Z_N (QFT).
5. Zmierz stan kwantowy i zapisz wynik γ.

Opis matematyczny

Transformacja Fouriera

QFT przekształca stan:

$$\frac{1}{\sqrt{N}} \sum_{x \in H} |x\rangle$$

na:

$$\sum_{\gamma \in Z_N} \hat{g}(\gamma)|\gamma\rangle,$$

gdzie $\hat{g}(\gamma)$ to współczynniki Fouriera dla funkcji $h(x) = 1_H(x)$.

Prawdopodobieństwo

Po pomiarze otrzymujemy $\gamma \in H$ z prawdopodobieństwem:

$$P(\gamma) = s \cdot |\hat{g}(\gamma)|^2.$$

Analiza wyników

Znajdowanie okresu s

- Wynik pomiaru γ spełnia $\gamma \cdot s = 0 \mod N$.
- Powtarzając algorytm wielokrotnie, otrzymujemy zbiór wartości $\{\gamma_1, \gamma_2, \dots\}$.
- Wykorzystując algorytm Euklidesa, obliczamy NWD(γ_i, N), aby wyznaczyć s.

Złożoność

Algorytm wymaga $O(n^2)$ bramek oraz wielokrotnych pomiarów.

Podsumowanie

Podsumowanie

- Algorytm kwantowy znajduje okres s poprzez zastosowanie QFT i wielokrotne pomiary.
- Wyniki są wykorzystywane w algorytmie Shora do faktoryzacji liczb.
- Znaczenie:
  - Eksponencjalne przyspieszenie względem algorytmów klasycznych.
  - Kluczowy krok w rozwoju obliczeń kwantowych.

Dalsze kroki

Implementacja praktyczna i analiza algorytmu Shora.

Wprowadzenie

Wprowadzenie do problemu znajdowania okresu

- Problem: Znalezienie okresu funkcji $f : \mathbb{Z}_N \to$ kolory.
- Warunek: Istnieje s, takie że $f(x+s) = f(x)$ dla wszystkich $x \in \mathbb{Z}_N$.
- Wniosek: $s \mid N$ (okres dzieli N).
- Klasyczne podejście działa, ale komputer kwantowy jest bardziej efektywny:
  - Wykorzystuje superpozycję i interferencję.
  - Redukuje liczbę operacji wymaganych do znalezienia okresu.

Złożoność algorytmów liczbowych

Podstawowe operacje liczbowe w czasie wielomianowym

- Mnożenie liczb $P \cdot Q$ - czas wielomianowy ($O(n^2)$ dla klasycznych metod).
- Dzielenie z resztą: $\lfloor P/Q \rfloor$ i $P \mod Q$ - czas wielomianowy.
- Potęgowanie modularne $P^Q \mod R$ - czas wielomianowy:
  - Algorytm szybkiego potęgowania (iteracyjne podnoszenie do kwadratu).
- Algorytm Euklidesa do znajdowania NWD - czas wielomianowy.
- Testowanie pierwszości:
  - Miller-Rabin (randomizowany, $O(n^2 \log n)$).
  - AKS (deterministyczny, $O(n^6)$).
- Faktoryzacja liczb: klasyczne algorytmy są eksponencjalne.

Algorytm Shora

Etapy algorytmu Shora

1. Faktoryzacja $\leqslant$ Znajdowanie rzędu:
   - Redukcja problemu faktoryzacji do znajdowania rzędu (klasyczna redukcja).
   - Wykorzystanie własności $A^s \equiv 1 \mod M$.
2. Znajdowanie rzędu $\approx$ Znajdowanie okresu:
   - Algorytm kwantowy wykorzystujący superpozycję i transformację Fouriera.
3. Rozpoznawanie ułamków prostych (klasyczne obliczenia za pomocą rozwinięć ułamków ciągłych).

Znajdowanie rzędu i jego znaczenie

- Rząd s elementu $A \mod M$ to najmniejsza liczba całkowita spełniająca $A^s \equiv 1 \mod M$.
- Znajdowanie rzędu pozwala na wyznaczenie okresu funkcji wykładniczej $f(x) = A^x \mod M$.
- Kluczowe znaczenie w algorytmie Shora: faktoryzacja liczb zredukowana do znajdowania rzędu.
- Powiązanie z teorią grup: s dzieli $\varphi(M)$, gdzie φ to funkcja Eulera.

Definicja problemu znajdowania rzędu

- Dane: A, M (liczby n-bitowe), gdzie NWD$(A, M) = 1$.
- Cel: Znalezienie najmniejszego $s \geqslant 1$, takiego że $A^s \equiv 1 \mod M$.
- Właściwości:
  - $s \mid \varphi(M)$ (funkcja Eulera).
  - $\varphi(M)$ to rząd grupy multiplikatywnej $\mathbb{Z}_M^*$.
  - s jest porządkiem multiplikatywnym elementu $A \mod M$.

Redukcja faktoryzacji do znajdowania rzędu

Przekształcenie problemu

- Cel: Znalezienie nietrywialnego pierwiastka kwadratowego $1 \mod M$.
- Postępowanie:
  1. Wybierz losowe $A \in \mathbb{Z}_M^*$.
  2. Znajdź rząd s liczby A (algorytm kwantowy).
  3. Jeśli s jest parzyste, oblicz $r \equiv A^{s/2} \mod M$.
  4. Jeśli $r \not\equiv \pm 1 \mod M$, to NWD$(M, r-1)$ daje dzielnik M.
  5. Powtarzaj, jeśli warunki nie są spełnione.
- Gwarancja sukcesu: dla liczb złożonych z co najmniej dwóch czynników pierwszych sukces występuje z prawdopodobieństwem co najmniej $1/2$ (pojedyncze próby).

Znaczenie sukcesu znajdowania rzędu

- Algorytm Shora działa z wysokim prawdopodobieństwem sukcesu dzięki losowemu wyborowi A.
- Jeśli nie uda się znaleźć s w jednej próbie, proces można powtórzyć wielokrotnie.
- W przypadku specyficznych M, inne metody (np. testowanie pierwiastków) mogą być wykorzystane w połączeniu z algorytmem.

Kwantowy algorytm znajdowania rzędu

Główne kroki algorytmu

1. Przygotowanie stanu kwantowego:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle,$$

   gdzie $f(x) = A^x \mod M$.
2. Pomiar drugiego rejestru - kolapsuje do superpozycji preobrazu losowego $f(x)$.
3. Zastosowanie kwantowej transformacji Fouriera (QFT):

$$|\psi\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{\gamma=0}^{N-1} e^{2\pi i \gamma x / N} |\gamma\rangle.$$

4. Pomiar γ - losowa wielokrotność N/s.
5. Wyznaczenie s za pomocą analizy wyników pomiarów.

Kwantowa transformacja Fouriera

- Kluczowy element algorytmu Shora.
- Definicja: QFT na N elementach przekształca $|x\rangle$ w:

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k x / N} |k\rangle.$$

- Złożoność obliczeniowa: $O(n^2)$ dla n-bitowych liczb.
- Wykorzystanie w znajdowaniu okresu: identyfikacja wielokrotności N/s - z wykorzystaniem ułamków łańcuchowych.

Eliminacja błędów

- Wielokrotne uruchamianie algorytmu pozwala wyeliminować błędne wyniki.
- Z prawdopodobieństwem $1/\text{poly}(n)$ licznik k i mianownik s są względnie pierwsze.
- Powtarzanie eksperymentu pozwala zwiększyć precyzję.

Podsumowanie

Podsumowanie

- Algorytm Shora pozwala na efektywne rozkładanie liczb na czynniki pierwsze.
- Kluczowe kroki:
  1. Redukcja faktoryzacji do znajdowania rzędu.
  2. Kwantowe znajdowanie rzędu za pomocą QFT.
  3. Analiza ułamków ciągłych do odzyskania okresu.
- Zastosowania:
  - Kryptografia (np. RSA).
  - Problemy teoretyczne w matematyce i informatyce.

Algorytm Deutsch-Jozsa

Dlaczego algorytm Deutsch-Jozsa?

- Pierwszy algorytm, który pokazał przewagę obliczeniową komputerów kwantowych.
- Rozwiązuje problem rozróżniania funkcji typu:
  - **Stała**: $f(x) = c$, gdzie $c \in \{0, 1\}$ dla wszystkich x.
  - **Zrównoważona**: $f(x) = 0$ dla połowy wartości x i $f(x) = 1$ dla drugiej połowy.
- Klasycznie wymaga $2^{n-1} + 1$ wywołań funkcji. Kwantowo tylko jednego.

Podstawy kwantowe

Superpozycja

- Kluczowa różnica między obliczeniami klasycznymi a kwantowymi:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |\alpha|^2 + |\beta|^2 = 1$$

- Superpozycja pozwala reprezentować wszystkie możliwe stany równocześnie.
- Przykład dla dwóch kubitów:

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

Interferencja kwantowa

- Interferencja pozwala wzmacniać pożądane stany i eliminować inne.
- Wykorzystuje różnicę faz między amplitudami stanów.
- Przykład operacji Hadamarda dla jednego kubitu:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Opis algorytmu Deutsch-Jozsa

Założenia problemu

- Dana funkcja $f : \{0,1\}^n \to \{0,1\}$.
- Gwarancja: $f(x)$ jest albo stała, albo zrównoważona.
- Celem jest określenie rodzaju funkcji w możliwie najmniejszej liczbie wywołań.

Kroki algorytmu Deutsch-Jozsa

1. Przygotowanie stanu początkowego:

$$|\psi_0\rangle = |0^n\rangle\,|1\rangle$$

2. Nałożenie superpozycji za pomocą bramek Hadamarda:

$$H^{\otimes(n+1)}\,|\psi_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle\,(|0\rangle - |1\rangle)$$

3. Implementacja orakulum:

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

Działanie orakulum

- Orakulum U_f zmienia stan na:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right)$$

- Informacja o $f(x)$ jest zakodowana w fazach stanów kwantowych.

Interferencja i pomiar

- Kolejne bramki Hadamarda na pierwszych n kubitach:

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$$

- Po operacji mamy stan:

$$|\psi_3\rangle = \sum_{z \in \{0,1\}^n} \alpha_z |z\rangle \left(|0\rangle - |1\rangle\right)$$

gdzie $\alpha_z = \sum_{x \in \{0,1\}^n} \frac{1}{2^{n+1}} (-1)^{x \cdot z + f(x)}$.

- Wynik pomiaru:
  - Jeśli $f(x)$ jest stała: wszystkie amplitudy poza $|0^n\rangle$ kasują się.
  - Jeśli $f(x)$ jest zrównoważona: amplituda $|0^n\rangle$ wynosi 0.

Przykład działania

Przykład dla $n = 2$

- Funkcja $f(x)$:
  - Stała: $f(00) = f(01) = f(10) = f(11) = 0$
  - Zrównoważona: $f(00) = 0, f(01) = 1, f(10) = 0, f(11) = 1$
- Wynik dla stałej: $|\psi_3\rangle = \frac{1}{\sqrt{2}} |00\rangle (|0\rangle - |1\rangle)$.
- Wynik dla zrównoważonej: $|\psi_3\rangle \perp |00\rangle (|0\rangle - |1\rangle)$.

Podsumowanie

Podsumowanie

- Algorytm Deutsch-Jozsa pokazuje przewagę obliczeniową dzięki superpozycji i interferencji.
- Redukcja liczby wywołań orakulum z $O(2^n)$ do $O(1)$.
- Stanowi podstawę dla bardziej zaawansowanych algorytmów kwantowych.

Algorytm Grovera

Wprowadzenie

- Algorytm Grovera został opracowany przez Lova Grovera w 1996 roku.
- Umożliwia rozwiązanie problemu wyszukiwania niestrukturalnego z kwadratowym przyspieszeniem względem algorytmów klasycznych.
- Jest jednym z kluczowych algorytmów ilustrujących potencjał obliczeń kwantowych.
- Oparty na zjawiskach superpozycji i interferencji.

Problem wyszukiwania niestrukturalnego

Definicja problemu

Problem wyszukiwania niestrukturalnego

Dane:

- Zbiór $X = \{x_1, x_2, \ldots, x_N\}$.
- Funkcja $f : X \to \{0, 1\}$.

Cel: Znaleźć $x^* \in X$, takie że $f(x^*) = 1$.

- Problem jest niestrukturalny, ponieważ brak jest informacji o organizacji danych.
- Klasyczne algorytmy wymagają $O(N)$ zapytań w najgorszym przypadku.

Podejście klasyczne vs kwantowe

Porównanie podejść

Klasyczne podejście

- Korzysta z deterministycznych lub losowych algorytmów.
- Złożoność: $\Theta(N)$ zapytań w najgorszym przypadku.

Podejście kwantowe

- Wykorzystuje mechanikę kwantową: superpozycję i interferencję.
- Redukuje liczbę zapytań do $\Theta(\sqrt{N})$.

Oracle kwantowy

Oracle kwantowy

- Oracle oznacza elementy spełniające warunek $f(x^*) = 1$.
- Realizowany jako bramka kwantowa O_f:

$$O_f|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Powoduje zmianę znaku amplitudy stanu x^*, gdy $f(x^*) = 1$.

Implementacja oracla

- Możliwa z użyciem klasycznych bramek logicznych w układzie kwantowym.
- Wymaga dodatkowych qubitów pomocniczych do zachowania unitarności.

Operator dyfuzji Grovera

Operator dyfuzji

- Operator dyfuzji wzmacnia amplitudę stanu x^*.
- Definicja:

$$D = 2|\psi\rangle\langle\psi| - I,$$

gdzie $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$.

Wizualizacja działania

- Odbicie amplitud wokół średniej μ:

$$\alpha_x \to 2\mu - \alpha_x.$$

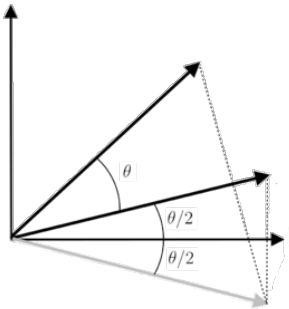
- Powtarzanie procesu zwiększa amplitudę x^*.

Algorytm Grovera

Etapy algorytmu

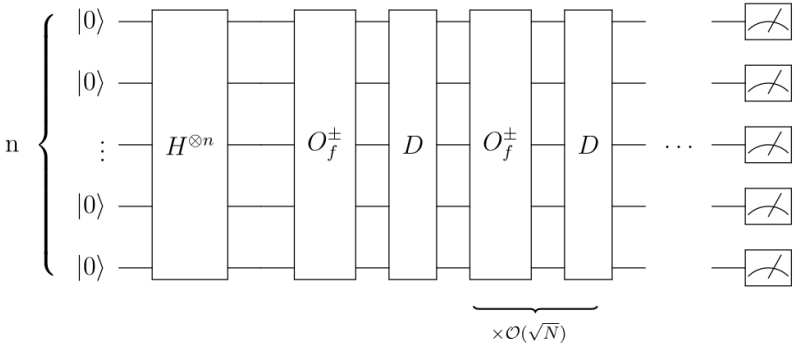
1. Inicjalizacja:
   - Przygotowanie superpozycji: $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ za pomocą bramek Hadamarda.
2. Oracle: Oznaczenie stanu docelowego x^*.
3. Operator dyfuzji: Wzmocnienie amplitudy x^*.
4. Powtórzenie kroków 2 i 3 $\lceil \pi/4\sqrt{N} \rceil$ razy.
5. Pomiar: Odczytanie stanu x^*.

Etapy algorytmu



1. Oracle: Oznaczenie stanu docelowego x^*.
2. Operator dyfuzji: Wzmocnienie amplitudy x^*.

Schemat algorytmu



- $H^{\otimes n}$ - Bramka Hadamarda.
- O_f - Oracle.
- D - Operator dyfuzji.

Analiza matematyczna

Wzmocnienie amplitudy

- Po t iteracjach amplituda x^* wynosi:

$$\alpha^{(t)} = \sin\left((2t+1)\theta\right),$$

  gdzie $\sin\theta = \frac{1}{\sqrt{N}}$.
- Maksymalizacja amplitudy po około $t = \lceil \pi/4\sqrt{N} \rceil$ iteracjach.

Złożoność obliczeniowa

- Liczba zapytań: $O(\sqrt{N})$.
- Liczba bramek kwantowych: $O(\sqrt{N}\log N)$.
- Prawdopodobieństwo sukcesu: Możemy zwiększyć, powtarzając proces.

Podsumowanie

Podsumowanie

- Algorytm Grovera oferuje kwadratowe przyspieszenie w porównaniu do metod klasycznych.
- Kluczowe zastosowania:
  - Wyszukiwanie w bazach danych.
  - Rozwiązywanie problemów kombinatorycznych.
- Demonstruje siłę superpozycji i interferencji w obliczeniach kwantowych.

Twierdzenie kodowania źródła Shannona

Wprowadzenie

- Twierdzenie kodowania źródła Shannona jest kluczowym wynikiem teorii informacji.
- Opisuje minimalną liczbę bitów potrzebnych do bezstratnego zakodowania informacji.
- Zostało wprowadzone przez Claude'a Shannona w 1948 roku.
- Stanowi podstawę dla kompresji danych.

Definicja

Twierdzenie Shannona

Średnia długość kodu L wymagana do zakodowania źródła informacji X nie może być mniejsza niż entropia źródła $H(X)$:

$$L \geqslant H(X)$$

gdzie:

- $H(X)$ - entropia źródła, mierzona w bitach na symbol.

- Entropia wyraża średnią ilość informacji dostarczaną przez symbol źródła.
- Kodowanie osiągające $L = H(X)$ jest optymalne.

Entropia źródła

Definicja entropii

Entropia źródła X o wartościach $x_1, x_2, \ldots, x_n$ z prawdopodobieństwami $p_1, p_2, \ldots, p_n$ jest zdefiniowana jako:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

- Wyższa entropia oznacza większą niepewność i większą ilość informacji.
- Przykład: Entropia rzutu monetą o równych szansach wynosi $H = 1$ bit.

Kodowanie bezstratne

- Kodowanie źródła polega na przypisywaniu krótszych kodów częstszym symbolom.
- Przykład: Kod Huffmana generuje optymalne bezstratne kody.
- Zasada:
  - Długość kodu $L(x_i)$ dla symbolu x_i jest proporcjonalna do $-\log_2 p_i$.
- Średnia długość kodu: $L = \sum_{i=1}^{n} p_i L(x_i)$.

Zastosowania

- Kompresja danych:
  - Algorytmy takie jak ZIP, JPEG, MP3 opierają się na zasadach twierdzenia.
- Projektowanie protokołów komunikacyjnych:
  - Efektywne przesyłanie danych przez ograniczone kanały.
- Analiza źródeł informacji:
  - Pomiar redundancji i struktury danych.

Ograniczenia twierdzenia

- Zakłada, że źródło jest stacjonarne i ergodyczne:
  - W praktyce dane mogą mieć zmienne prawdopodobieństwa symboli.
- Nie uwzględnia strat związanych z kodowaniem stratnym (np. w JPEG).
- Twierdzenie dotyczy tylko kodowania bezstratnego.

Przykład: Rzut monetą

- Założenia:
  - Moneta jest symetryczna ($p_1 = p_2 = 0.5$).
- Entropia:

$$H(X) = -(0.5 \log_2 0.5 + 0.5 \log_2 0.5) = 1 \text{ bit}$$

- Interpretacja:
  - Każdy rzut niesie dokładnie 1 bit informacji.

Podsumowanie

- Twierdzenie Shannona opisuje fundamentalne granice kompresji bezstratnej.
- Minimalna długość kodu zależy od entropii źródła.
- Zastosowanie w praktycznych systemach kompresji i transmisji danych.
- Umożliwia efektywne zarządzanie informacją w różnych dziedzinach.

Stany Kwantowe i Macierz Gęstości

Stany kwantowe

- Stan kwantowy opisuje pełną informację o układzie w mechanice kwantowej.
- Reprezentowany jako wektor w przestrzeni Hilberta $|\psi\rangle$.
- Wektory są znormalizowane:

$$\langle\psi|\psi\rangle = 1$$

- Stan czysty: opisywany przez jeden wektor $|\psi\rangle$.
- Stan mieszany: kombinacja statystyczna stanów czystych.

Qubit

- Qubit to najprostszy układ kwantowy:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{gdzie} \quad |\alpha|^2 + |\beta|^2 = 1$$

- Współczynniki α i β mogą być zespolone.
- Ogólna reprezentacja z użyciem parametrów kuli Blocha:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

- Parametry:
  - $\theta \in [0, \pi]$
  - $\phi \in [0, 2\pi)$

Macierz gęstości

- Opisuje zarówno stany czyste, jak i mieszane.
- Definicja:

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$$

  - p_k – prawdopodobieństwo stanu $|\psi_k\rangle$.
- Właściwości:
  - Hermitowska: $\rho = \rho^\dagger$
  - Ślad równy 1: $\mathrm{Tr}(\rho) = 1$
  - Dodatnio określona: $\langle\phi|\rho|\phi\rangle \geqslant 0$ dla dowolnego $|\phi\rangle$.

Przykłady macierzy gęstości

- Stan czysty:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

- Stan mieszany:

$$\rho = p_1|0\rangle\langle 0| + p_2|1\rangle\langle 1|$$

$$\rho = \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix}, \quad p_1 + p_2 = 1$$

Sfera Blocha

- Graficzna reprezentacja stanów qubitu.
- Stan czysty $|\psi\rangle$: punkt na powierzchni sfery Blocha.
- Stan mieszany: wektor Blocha $\boldsymbol{n}$ wewnątrz sfery.

$$\rho = \frac{1}{2}(I + \boldsymbol{n} \cdot \boldsymbol{\sigma})$$

  - $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ – macierze Pauliego.
  - $\boldsymbol{n}$: wektor Blocha.
- Długość $|\boldsymbol{n}| \leqslant 1$:
  - $|\boldsymbol{n}| = 1$: stan czysty.
  - $|\boldsymbol{n}| < 1$: stan mieszany.

Podsumowanie

- Stany kwantowe:
  - Czyste: wektor w przestrzeni Hilberta.
  - Mieszane: kombinacja statystyczna stanów czystych.
- Macierz gęstości:
  - Uniwersalny opis stanów kwantowych.
  - Kluczowe właściwości: hermitowskość, dodatniość, śladowość.
- Sfera Blocha:
  - Geometria qubitów.
  - Wizualizacja stanów czystych i mieszanych.

Kwantowa Teoria Informacji

Wprowadzenie

- Kwantowa teoria informacji rozszerza klasyczne pojęcia teorii informacji na układy kwantowe.
- Wykorzystuje unikalne właściwości mechaniki kwantowej:
  - Superpozycję stanów
  - Splątanie kwantowe
- Analizuje przesyłanie, przetwarzanie i przechowywanie informacji w systemach kwantowych.

Kwantowa kompresja

- Problem: Jak najlepiej zakodować stany kwantowe, aby minimalizować wymaganą przestrzeń Hilberta?
- Kluczowa idea:
  - Średnia długość kodowania kwantowego jest ograniczona przez entropię von Neumanna $S(\rho)$.
  - $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$, gdzie ρ to macierz gęstości opisująca stan kwantowy.
- Wniosek: Możemy bezstratnie skompresować n kopii stanu kwantowego ρ do $nS(\rho)$ qubitów, jeśli n jest duże.

Przykład kwantowej kompresji

- Rozważmy stan kwantowy o macierzy gęstości:

$$\rho = \begin{bmatrix} 0.7 & 0 \\ 0 & 0.3 \end{bmatrix}$$

- Entropia von Neumanna:

$$S(\rho) = -0.7 \log_2 0.7 - 0.3 \log_2 0.3 \approx 0.881 \text{ bitów}$$

- Dla $n = 1000$:
  - Możemy bezstratnie zakodować te stany w $1000 \times 0.881 \approx 881$ qubitach.

Entropie kwantowe

- Entropia von Neumanna:

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho)$$

- Interpretacja:
  - Mierzy ilość niepewności (lub mieszaniny) stanu kwantowego.
  - Stan czysty: $S(\rho) = 0$
  - Stan maksymalnie mieszany: $S(\rho) = \log_2 d$, gdzie d to wymiar przestrzeni Hilberta.
- Względna entropia kwantowa:

$$S(\rho||\sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma)$$

  - Miara odległości między dwoma stanami kwantowymi ρ i σ.

Twierdzenie Holevo

Treść twierdzenia

Ilość informacji klasycznej I, którą można wydobyć z układu kwantowego, jest ograniczona przez entropię Holevo:

$$\chi = S(\rho) - \sum_i p_i S(\rho_i)$$

gdzie $\rho = \sum_i p_i \rho_i$.

- Informacja Holevo χ określa maksymalną ilość klasycznej informacji dostępnej w stanach kwantowych.
- Ograniczenie fundamentalne dla komunikacji kwantowej.

Przykład zastosowania twierdzenia Holevo

- Rozważmy zbiór stanów:

$$\rho_1 = |0\rangle\langle 0|, \quad \rho_2 = |1\rangle\langle 1|, \quad \rho = \frac{1}{2}(\rho_1 + \rho_2)$$

- Entropia von Neumanna:

$$S(\rho) = 1 \text{ bit}$$

- Entropia średnia:

$$\sum_i p_i S(\rho_i) = 0 \text{ bitów}$$

- Entropia Holevo:

$$\chi = S(\rho) - \sum_i p_i S(\rho_i) = 1 - 0 = 1 \text{ bit}$$

- Interpretacja: Możemy wydobyć maksymalnie 1 bit informacji z układu.

Kwantowe kody dostępu swobodnego (QRAC)

- QRAC umożliwiają przechowywanie n bitów informacji w $m < n$ qubitach, zapewniając probabilistyczny dostęp do danych.
- Kluczowa cecha: Możliwość odczytania jednego z zapisanych bitów z dużym prawdopodobieństwem.
- Przykład: 2-bitowy QRAC
  - Dane: $x_1, x_2 \in \{0, 1\}$.
  - Kodowanie w stanie kwantowym $|\psi_{x_1 x_2}\rangle$.
  - Odczyt: Z prawdopodobieństwem $\approx 85\%$ poprawnie odczytujemy x_1 lub x_2.

Podsumowanie

- Kwantowa teoria informacji wprowadza nowe możliwości przetwarzania informacji.
- Kluczowe pojęcia:
  - Kwantowa kompresja – efektywne wykorzystanie przestrzeni Hilberta.
  - Entropie kwantowe – miary niepewności i mieszaniny stanów.
  - Twierdzenie Holevo – ograniczenia w przesyłaniu informacji klasycznej przez układy kwantowe.
  - QRAC – probabilistyczne kody dostępu.
- Zastosowania w kryptografii, komunikacji i obliczeniach kwantowych.

Kompresja Schumachera

Wprowadzenie

- Kompresja Schumachera to kwantowy odpowiednik klasycznego kodowania Shannona.
- Redukuje liczbę qubitów potrzebnych do przesyłania stanu kwantowego.
- Kluczowe wnioski wynikają z typowości kwantowej i entropii von Neumanna.

Matematyczne podstawy

- **Entropia von Neumanna**: $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$
- Stan kwantowy: $\rho = \sum p(x)|\psi_x\rangle\langle\psi_x|$
- Wskaźnik kompresji: $R_\infty = S(\rho)$

Projekcja na typową podprzestrzeń

- Typowość: większość stanów kwantowych można wyrazić w typowej podprzestrzeni.
- Projekcja: $P_T =$ typowa podprzestrzeń o wymiarze $2^{nS(\rho)}$.
- Kluczowe: pozwala na wierną rekonstrukcję stanu.

Wierna kompresja

- Wzór: $n = Rm$, gdzie R to stopień kompresji.
- Warunek wierności: $\tilde{F} > 1 - \epsilon$
- Kompresja Schumachera minimalizuje zasoby qubitowe.

Znaczenie praktyczne

- Zastosowania:
  - Optymalizacja komunikacji kwantowej.
  - Minimalizacja zasobów w obliczeniach kwantowych.
- Redukcja liczby qubitów bez utraty informacji.

Podsumowanie

- Kompresja Schumachera to fundament kwantowej teorii informacji.
- Umożliwia efektywne kodowanie stanów kwantowych.
- Kluczowa rola w technologii kwantowej przyszłości.

Kwantowa Korekcja Błędów

Wprowadzenie

- Szumy w komunikacji i obliczeniach kwantowych prowadzą do błędów.
- Korekcja błędów pozwala na ochronę informacji kwantowej.
- Inspiracja: klasyczna korekcja błędów (np. redundancja 3-bitowa).
- Wyzwaniem jest nieprzeszkadzanie w delikatnej superpozycji stanów kwantowych.

Szumy i błędy kwantowe

- Główne źródła błędów:
  - Interakcje z otoczeniem (dekoherencja).
  - Niedoskonałości w implementacji fizycznej.
- Typy błędów:
  - Bit-flip (X): $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$.
  - Phase-flip (Z): $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$.
  - Depolaryzacja: miesza wszystkie stany z równymi prawdopodobieństwami.

Korekcja błędów w mechanice kwantowej

- Celem jest detekcja i korekta błędów kwantowych bez niszczenia stanu.
- Przykład klasyczny: redundancja 3-bitowa:

$$0 \to 000,$$
$$1 \to 111.$$

- W przypadku błędu: $|000\rangle \to |100\rangle$, można zidentyfikować pozycję i skorygować.

Kodowanie dla bit-flip

- Kodowanie chroniące przed błędem bit-flip:

$$|0\rangle \to |000\rangle,$$
$$|1\rangle \to |111\rangle.$$

- Detekcja błędów za pomocą pomiarów stabilizatorów:

$$S_1 = Z_1 Z_2,$$
$$S_2 = Z_2 Z_3.$$

- Wyniki pomiarów wskazują na pozycję błędu.

Kodowanie dla phase-flip

- Błąd typu phase-flip:

$$|0\rangle \to |0\rangle,$$
$$|1\rangle \to -|1\rangle.$$

- Kodowanie chroniące przed błędem phase-flip:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \to \alpha|++\rangle + \beta|--\rangle,$$

gdzie $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ i $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Korekcja obu typów błędów

- Kodowanie chroniące przed bit-flip i phase-flip:

$$|0\rangle \to \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle).$$

- Proces korekcji:
  1. Wykrycie błędów za pomocą stabilizatorów.
  2. Aplikacja operatora naprawiającego na podstawie wyników pomiarów.

Kanał depolaryzujący

- Opis matematyczny:

$$\Lambda(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z).$$

- Reprezentacja operatorów Krausa:

$$K_0 = \sqrt{1-p}I,$$
$$K_1 = \sqrt{\frac{p}{3}}X,$$
$$K_2 = \sqrt{\frac{p}{3}}Y,$$
$$K_3 = \sqrt{\frac{p}{3}}Z.$$

- Depolaryzacja miesza stan z szumem z prawdopodobieństwem p.

Twierdzenie o korekcji błędów

- Warunki poprawnej korekcji błędów:

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij},$$

  gdzie E_a i E_b to operatory błędów.
- Interpretacja:
  - Korekcja działa, gdy błędy są rozróżnialne w przestrzeni kodowej.

Kod Shora

- Chroni przed bit-flip i phase-flip poprzez 9 qubitów.
- Kodowanie:

$$|0\rangle \to \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle),$$
$$|1\rangle \to \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle).$$

- Proces naprawy:
  1. Detekcja błędów przy użyciu stabilizatorów.
  2. Korekta za pomocą odpowiednich operatorów.

Znaczenie praktyczne

- Ochrona informacji w komunikacji kwantowej.
- Stabilność obliczeń kwantowych w obliczu szumów.
- Wyzwania implementacyjne:
  - Realizacja fizyczna kodów.
  - Minimalizacja zasobów.

Podsumowanie

- Korekcja błędów jest kluczowym elementem technologii kwantowej.
- Opracowanie efektywnych kodów pozwala na niezawodne przetwarzanie informacji.
- Przykłady kodów: bit-flip, phase-flip, kod Shora.
- Wciąż trwają badania nad optymalizacją zasobów.