Wprowadzenie do obliczeń kwantowych

Zbigniew Puchała

Instytut Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk

2024

Zagadnienia wstępne, fizyka mikroświata, efekty kwantowe

Mechanika kwantowa

- Mechanika kwantowa opisuje zachowania bardzo małych cząstek fizycznych, czyli np.:
  - fotonów,
  - elektronów,
  - *kwantowych bitów* – **kubitów**.
- W mikroświecie obowiązują prawa, które różnią się od tych znanych z fizyki klasycznej.
- Zjawiska kluczowe:
  - superpozycja,
  - splątanie,
  - tunelowanie kwantowe.

Efekty kwantowe

- **Superpozycja**:
  - Obiekt kwantowy może *istnieć w wielu stanach jednocześnie*.
  - Przykład: Kubit jako kombinacja stanów $|0\rangle$ i $|1\rangle$:

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

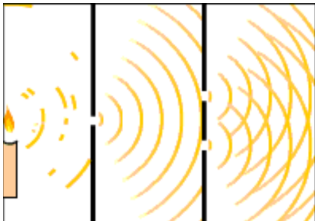
    gdzie $|\alpha|^2 + |\beta|^2 = 1$.
- **Splątanie**:
  - Stan dwóch (lub więcej) cząstek jest wspólny, nawet jeśli są przestrzennie oddzielone.
  - Przykład: Stan Bella:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

- **Tunelowanie kwantowe**:
  - Cząstka może „przeskoczyć" przez barierę potencjału, która klasycznie byłaby nieprzekraczalna.

Eksperymenty w fizyce kwantowej

- **Eksperyment podwójnej szczeliny** (Younga):
  - Cząstki (np. elektrony) przechodzą przez dwie szczeliny i tworzą na ekranie wzór interferencyjny.
  - Dowód na falowo-korpuskularną naturę cząstek.



Rysunek: źródło: Wikipedia, autor: Mpfiz

Eksperymenty w fizyce kwantowej

- **Splątanie kwantowe**:
  - Doświadczenia Aspecta potwierdziły nielokalność splątanych cząstek.
- **Zasada nieoznaczoności Heisenberga**:
  - Nie można jednocześnie dokładnie zmierzyć położenia i pędu cząstki.
  - Matematycznie: $\Delta x \cdot \Delta p \geqslant \frac{\hbar}{2}$.

Zastosowania efektów kwantowych

- **Obliczenia kwantowe**:
  - Algorytm Shora (rozkład na czynniki pierwsze),
  - Algorytm Grovera (przeszukiwanie baz danych).
- **Kryptografia kwantowa**:
  - Bezpieczne przesyłanie informacji dzięki splątaniu.
- **Symulacje kwantowe**:
  - Modelowanie układów chemicznych i biologicznych.

Ewolucja układu w czasie. Równanie Schroedingera

Ewolucja układu kwantowego

- W mechanice kwantowej układ opisujemy za pomocą **funkcji falowej** $\psi(t)$:

$$|\psi(t)\rangle = \text{stan układu w chwili } t.$$

- Funkcja falowa zawiera pełną informację o układzie, np. prawdopodobieństwo znalezienia cząstki w danym miejscu.
- Ewolucja układu w czasie jest **deterministyczna** i opisana równaniem Schrödingera:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle ,$$

gdzie $\hat{H}$ to operator Hamiltona, reprezentujący energię układu.

- Idea: Równanie Schrödingera określa, jak stan układu zmienia się w czasie pod wpływem oddziaływań.

Kluczowe aspekty ewolucji w czasie

- **Liniowość równania**:
  - Ewolucja funkcji falowej jest **liniowa**, co oznacza, że kombinacja stanów początkowych pozostaje kombinacją w czasie.
- **Jednostajność ewolucji**:
  - Całkowita energia układu ($\hat{H}$) pozostaje stała w czasie.
- **Superpozycja stanów**:
  - Jeśli układ początkowo jest w stanie superpozycji, ewoluuje jako superpozycja.
- **Przykład**: Prosty oscylator kwantowy.
  - Ruch jest cykliczny i determinowany przez operator Hamiltona.
- **Związek z obserwacją**:
  - Ewolucja opisana równaniem Schrödingera trwa do momentu dokonania pomiaru.

Stany kwantowe i superpozycja stanów – definicje i przykłady

Kubit

Elementarnym obiektem w informatyce kwantowej jest kubit, który jest najprostszym układem kwantowym. Stan kubitu (zdefiniowany poniżej) opisuje wektor o dwóch elementach zespolonych.
W celu opisania stanu kubitu zwyczajowo wybieramy bazę obliczeniową

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Wówczas dowolny stan $|\psi\rangle$ kubitu tworzy liniową kombinację wektorów bazowych

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

z $|\alpha|^2 + |\beta|^2 = 1$ oraz $\alpha, \beta \in \mathbb{C}$.

Opis stanu kubitu

- Liczby α i β są zespolone. Do ich zapisania potrzebujemy czterech liczb rzeczywistych.
- Warunek normalizacji:

$$|\alpha|^2 + |\beta|^2 = 1$$

pozwala wyeliminować jedną z tych liczb.

- Wynika z tego, że dowolny stan kubitu można opisać za pomocą **trzech liczb rzeczywistych**.
- Ogólna postać stanu kubitu:

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

gdzie $\gamma, \theta, \phi \in \mathbb{R}$.

Znaczenie fazy globalnej

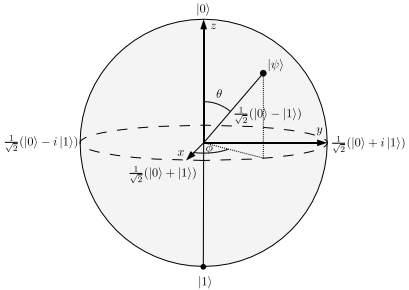
- Współczynnik $e^{i\gamma}$ to tzw. **faza globalna**.
- Faza globalna nie wpływa na fizyczne własności stanu kubitu, dlatego możemy przyjąć $\gamma = 0$.
- W efekcie stan kubitu przyjmuje prostszą postać:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\,.$$

- Stany różniące się fazą globalną są fizycznie identyczne.

Sfera Blocha

- Liczby θ i ϕ mogą być traktowane jako współrzędne punktu na **sferze Blocha**.
- Sfera Blocha to trójwymiarowa sfera o promieniu 1.
- Współrzędne na sferze Blocha:
  θ (długość łuku od bieguna północnego do punktu na sferze), ϕ (kąt azymutalny).
- Sfera Blocha umożliwia intuicyjną wizualizację stanu kubitu i operacji kwantowych.



Definicja stanu kwantowego

- **Stan kwantowy** w mechanice kwantowej to wektor w przestrzeni Hilberta:

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix}.$$

- W bazie obliczeniowej można go zapisać jako:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{n-1} |n-1\rangle .$$

- Każde $\alpha_i \in \mathbb{C}$ (liczby zespolone) spełnia warunek normalizacji:

$$\||\psi\rangle\| = \sqrt{|\alpha_0|^2 + |\alpha_1|^2 + \ldots + |\alpha_{n-1}|^2} = 1.$$

Amplitudy prawdopodobieństwa

- Współczynniki α_i w stanie $|\psi\rangle$ nazywamy **amplitudami prawdopodobieństwa**.
- Jeśli $\alpha_i = 1$, układ kwantowy znajduje się w stanie odpowiadającym tej amplitudzie:

$$\alpha_0 = 1 \implies |\psi\rangle = |0\rangle\,.$$

- Jeżeli więcej niż jedna amplituda jest niezerowa, mówimy o **superpozycji stanów**.
- Przykład:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|2\rangle\,.$$

Stan jest w superpozycji $|0\rangle$ i $|2\rangle$.

Właściwości bazy obliczeniowej

- Baza obliczeniowa składa się z wektorów $|0\rangle, |1\rangle, \ldots, |n-1\rangle$.
- Jest **ortonormalna**, co oznacza:

$$\langle i|j\rangle = \begin{cases} 1 & \text{dla } i = j, \\ 0 & \text{dla } i \neq j. \end{cases}$$

- Norma euklidesowa stanu w bazie obliczeniowej wynosi 1:

$$\||\psi\rangle\| = \sqrt{\sum_{i=0}^{n-1} |\alpha_i|^2}.$$

Wprowadzenie do pomiarów kwantowych

Pomiar kwantowy:

- Łącznik między światem kwantowym a klasycznym.
- Jedyny sposób zdobycia informacji o układzie kwantowym.
- **Nieodwracalność:** pomiar bezpowrotnie zmienia stan kwantowy.

Opis matematyczny:

$$\mathcal{P} = \{\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_{n-1}\}$$

Warunek zupełności:

$$\mathbf{P}_0 + \mathbf{P}_1 + \ldots + \mathbf{P}_{n-1} = \mathbf{I}$$

Pomiar rzutowy

Cechy pomiaru rzutowego:

- Macierze są rzutami ortogonalnymi:

$$\mathbf{P}_i^2 = \mathbf{P}_i$$

- Dla różnych indeksów $i \neq j$:

$$\mathbf{P}_i \mathbf{P}_j = \mathbf{0}$$

Działanie pomiaru kwantowego

Przebieg pomiaru:

- Dany jest stan $|\psi\rangle$ i zbiór macierzy pomiaru $\mathcal{P}$.
- Wynik i uzyskujemy z prawdopodobieństwem:

$$p_i = \|\mathbf{P}_i |\psi\rangle\|^2$$

- Po pomiarze stan zmienia się na:

$$|\psi_i\rangle = \frac{\mathbf{P}_i |\psi\rangle}{\|\mathbf{P}_i |\psi\rangle\|}$$

Przykład pomiaru 1

Pomiar dla jednego kubitu:

$$\mathbf{P}_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\mathbf{P}_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Stan początkowy: $|\psi\rangle = \sqrt{0.7}\,|0\rangle + \sqrt{0.3}i\,|1\rangle$ **Prawdopodobieństwa:**

$$p_0 = 0.7, \quad p_1 = 0.3$$

Przykład pomiaru 2

Pomiar w innej bazie:

$$\mathbf{Q}_{-i} = |-_i\rangle\langle -_i| = \frac{1}{2}\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}$$

$$\mathbf{Q}_{+i} = |+_i\rangle\langle +_i| = \frac{1}{2}\begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}$$

Prawdopodobieństwa:

$$p_{-i} \approx 0.958, \quad p_{+i} \approx 0.042$$

Szeregowanie pomiarów

Szeregowanie:

- Kolejny pomiar tego samego operatora daje ten sam wynik.
- Wynik po drugim pomiarze:

$$p_i' = 1, \quad \forall i$$

Wnioski: Po pierwszym pomiarze stan zostaje „utrwalony" w zmierzonym wyniku.

Pomiar częściowy

Pomiar częściowy:

- Wykonujemy pomiar tylko na części układu.
- Przykład dla stanu dwukubitowego:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Po pomiarze pierwszego kubitu:

$$p_{0?} = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

Wprowadzenie do Bramek Kwantowych

- **Definicja**: Bramka kwantowa to operacja unitarna na jednym lub więcej kubitach.
- **Właściwości**:
  - **Unitarność**: $U^\dagger U = I$
  - **Odwracalność**: Każda bramka ma odwrotną operację.
- Operacje są reprezentowane przez macierze kwadratowe.

Podstawowe Bramki Kwantowe

- **Bramka Pauli-X** (*NOT*):

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- **Bramka Pauli-Y**:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

- **Bramka Pauli-Z**:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Bramki na jednym kubicie

- **Bramka Hadamarda (H)**:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Służy do wprowadzania superpozycji.
- Przykład działania: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Bramki na dwóch kubitach

- **Bramka CNOT** (Controlled-NOT):

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Używana do tworzenia splątania.
- Przykład działania: $CNOT(|10\rangle) = |11\rangle$

Odwrotność Bram

- Dla każdej bramki kwantowej U istnieje odwrotność $U^\dagger$.
- Przykład: Bramki Pauliego są samoodwrotne:

$$X^\dagger = X, \quad Y^\dagger = Y, \quad Z^\dagger = Z$$

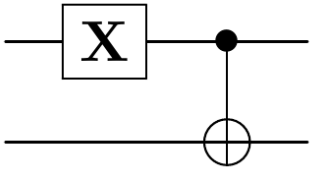
- Bramki zachowują normę stanu kwantowego: $|\psi'|^2 = |\psi|^2$

Zastosowanie Bramek Kwantowych

- Budowanie algorytmów kwantowych, np.:
  - Algorytm Grovera
  - Algorytm Shora
- Realizacja operacji logicznych na kubitach.
- Tworzenie splątanych stanów kwantowych.

Podsumowanie

- Bramki kwantowe to podstawowe elementy algorytmów kwantowych.
- Właściwości unitarności i odwracalności są kluczowe.
- Operacje mogą być realizowane na jednym lub wielu kubitach.



Rysunek: Graficzna reprezentacja operacji $\mathbf{CNOT}_1^2(\mathbf{X} \otimes \mathbf{I})$

Obwody Kwantowe

- Obwód kwantowy to graficzna reprezentacja działania bramek kwantowych.
- Każda linia w obwodzie oznacza pojedynczy kubit.
- Bramka nakładana na jeden lub więcej kubitów jest przedstawiana jako symbol na linii kubitu.
- Czas w obwodzie biegnie od lewej do prawej.

Tworzenie stanu splątanego ze stanu separowalnego

- Startujemy od stanu separowalnego:

$$|\psi_{t=1}\rangle = |0\rangle \otimes |0\rangle$$

- Nakładamy bramkę Hadamarda na pierwszy kubit:

$$|\psi_{t=2}\rangle = (\mathbf{H} \otimes \mathbf{I})\,|\psi_{t=1}\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \otimes |0\rangle$$

- Otrzymujemy:

$$|\psi_{t=2}\rangle = \frac{1}{\sqrt{2}}\,(|00\rangle + |10\rangle)$$

Nakładanie bramki CNOT

- Nakładamy bramkę $\mathbf{CNOT}_1^2$, gdzie pierwszy kubit jest kontrolującym, a drugi docelowym:

$$|\psi_{t=3}\rangle = \mathbf{CNOT}_1^2 |\psi_{t=2}\rangle$$

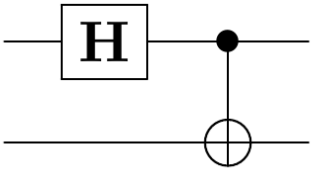
- Wynik:

$$|\psi_{t=3}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

- Otrzymany stan to stan Bella $|\Phi^+\rangle$.

Obwód Kwantowy

Obwód kwantowy realizujący tę operację wygląda następująco:



- Bramki są nakładane od lewej do prawej.
- $\mathbf{H}$ to bramka Hadamarda.
- $\mathbf{CNOT}$ realizuje splątanie.

Podsumowanie

- Obwody kwantowe umożliwiają graficzne przedstawienie operacji na kubitach.
- Proces tworzenia stanu splątanego składa się z:
  - Nakładania bramki Hadamarda.
  - Zastosowania bramki CNOT.
- Otrzymany stan $|\Phi^+\rangle$ jest przykładem stanu Bella.

Stany Wielosystemowe

Dwa kubity

Dwa kubity

- Operacją matematyczną łączącą dwa stany kwantowe jest **iloczyn Kroneckera**.
- Dla dwóch kubitów $|\psi\rangle$ i $|\phi\rangle$:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad |\phi\rangle = \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$$

- Ich łączny stan to:

$$|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix}$$

Interpretacja iloczynu Kroneckera

- Łączny stan można zapisać jako:

$$|\psi\phi\rangle = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle$$

- Zapis skrócony:

$$|\psi\phi\rangle = \alpha\gamma\,|0\rangle + \alpha\delta\,|1\rangle + \beta\gamma\,|2\rangle + \beta\delta\,|3\rangle$$

- Etykiety 00, 01, 10, 11 odpowiadają liczbom binarnym.

Stan Bella

- Rozważmy stan:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle)$$

- Wtedy współczynniki $c_0 = c_3 = \frac{1}{\sqrt{2}}$, $c_1 = c_2 = 0$.
- Nie istnieją takie $\alpha, \beta, \gamma, \delta$, które spełniają:

$$\alpha\gamma = c_0, \quad \alpha\delta = c_1, \quad \beta\gamma = c_2, \quad \beta\delta = c_3$$

- Wniosek: stan $\left|\Phi^+\right\rangle$ nie jest iloczynem Kroneckera.

Splątanie kwantowe

Definicja splątania

- Stan $|\phi\rangle$ jest **splątany**, jeśli nie można go zapisać jako $|\psi_1\rangle \otimes |\psi_2\rangle$.
- Stan Bella $|\Phi^+\rangle$ jest przykładem stanu splątanego.
- Stan jest **separowalny**, jeśli istnieją $|\psi_1\rangle$ i $|\psi_2\rangle$ takie, że $|\phi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

Splątanie wielu układów

- Stan (produktowy) n kubitów opisujemy jako:

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

- Przykłady stanów splątanych:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Własności stanów splątanych

- Splątane stany wykazują zjawiska nieintuicyjne, np. zdalne oddziaływanie.
- Nawet po oddaleniu splątane cząstki pozostają związane.
- Kluczowe w zastosowaniach takich jak teleportacja kwantowa i kryptografia.

Podsumowanie

- Iloczyn Kroneckera łączy stany kwantowe wielu układów.
- Splątanie kwantowe jest kluczowym zjawiskiem w mechanice kwantowej.
- Stany Bella i GHZ mają istotne znaczenie w informatyce kwantowej.

Informacja Klasyczna i Kwantowa

Wprowadzenie

- Informacja klasyczna i kwantowa różnią się, ale ich matematyczny opis jest zaskakująco podobny.
- Zrozumienie informacji kwantowej wymaga znajomości informacji klasycznej.
- Informacja klasyczna jest punktem odniesienia do badania kwantowej informacji.
- Porównania między nimi pomagają zrozumieć bardziej złożone zagadnienia kwantowe.

Stany Klasyczne

Stany Klasyczne i Rozkłady Prawdopodobieństwa

- System klasyczny przechowuje informację w **stanach klasycznych**, np.:
  - Bit: 0 lub 1.
  - Bajt: ciąg 8 bitów, $2^8 = 256$ możliwych stanów.
- Ważne jest określenie **alfabetu** możliwych stanów układu.
- Stany mogą być deterministyczne lub probabilistyczne.

Przykład: Stan Probabilistyczny

- Przykład: Zaszumione łącze transmitujące bit:
  - Dla wysłanego 0: $P(\text{OUT} = 0) = \frac{5}{6}$, $P(\text{OUT} = 1) = \frac{1}{6}$.
  - Dla wysłanego 1: $P(\text{OUT} = 0) = \frac{1}{4}$, $P(\text{OUT} = 1) = \frac{3}{4}$.
- Stan odbiorcy przy wysłanym 0 zapisujemy wektorowo:

$$\begin{bmatrix} \frac{5}{6} \\ \frac{1}{6} \end{bmatrix}$$

- Wektor odpowiada prawdopodobieństwom stanów układu.

Stan Probabilistyczny - Definicja Ogólna

- Stan probabilistyczny to wektor o długości n, gdzie:
  - n - liczba możliwych stanów układu.
  - Współrzędne są rzeczywiste, nieujemne i sumują się do 1:

$$\sum_{i=1}^{n} p_i = 1.$$

- Porządek możliwych stanów musi być ustalony i konsekwentnie stosowany.

Operacje Klasyczne

Macierze Kolumnowo-Stochastyczne

- Operacje na stanach probabilistycznych są opisane przez macierze kolumnowo-stochastyczne:
  - Każda kolumna to wektor probabilistyczny.
  - Wartości są nieujemne, a sumy w kolumnach wynoszą 1.
- Przykład macierzy dla dwóch stanów:

$$M = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} \end{bmatrix}$$

- Działanie na wektorze stanu:

$$\mathbf{p}' = M \cdot \mathbf{p}.$$

Podsumowanie

- Informacja klasyczna opiera się na stanach deterministycznych lub probabilistycznych.
- Stany probabilistyczne opisujemy wektorami, a operacje - macierzami stochastycznymi.
- Matematyczny opis informacji klasycznej stanowi podstawę dla zrozumienia informacji kwantowej.

Informacja Kwantowa

Wprowadzenie

- Informacja kwantowa jest rozszerzeniem pojęcia informacji klasycznej.
- Opiera się na prawach mechaniki kwantowej, takich jak superpozycja i splątanie.
- Kluczowe różnice w stosunku do informacji klasycznej:
  - Stany kwantowe nie są deterministyczne ani czysto probabilistyczne.
  - Możliwość kodowania informacji w superpozycji stanów.
  - Istnienie stanów splątanych, których nie można rozdzielić na indywidualne układy.

Qubit

Qubit - Podstawowa jednostka informacji kwantowej

- Klasyczna jednostka: **bit** (0 lub 1).
- Kwantowa jednostka: **qubit**, który może być w stanie:

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

- α i β są zespolonymi amplitudami prawdopodobieństwa.
- Qubit można interpretować jako punkt na sferze Blocha:
  - Superpozycja stanów $|0\rangle$ i $|1\rangle$.
  - Pomiar prowadzi do kolapsu do jednego ze stanów z określonym prawdopodobieństwem.

Operacje na Qubitach

- Operacje na stanach kwantowych są opisane macierzami jednostkowymi.
- Przykłady bramek kwantowych:
  - Bramka Hadamarda (H):
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$
  - Bramka Pauli-X (odpowiednik NOT):
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$
- Operacje wieloqubitowe, np. bramka CNOT (kontrolowane NOT).

Splątanie Kwantowe

Splątanie Kwantowe

- Stan dwóch qubitów jest **splątany**, jeśli nie można go zapisać jako:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,.$$

- Przykład: stan Bella $\left|\Phi^+\right\rangle$:

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

- Splątanie prowadzi do korelacji, które nie mają klasycznego odpowiednika.
- Kluczowe znaczenie w:
  - Kryptografii kwantowej.
  - Teleportacji kwantowej.
  - Algorytmach kwantowych.

Stany Wielosystemowe

- Łączenie układów opisuje **iloczyn tensorowy**:

$$|\psi\rangle \otimes |\phi\rangle \,.$$

- Dla dwóch qubitów:

$$|\psi\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle), \quad |\phi\rangle = (\gamma\,|0\rangle + \delta\,|1\rangle),$$

$$|\psi\phi\rangle = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle \,.$$

- Stany splątane są szczególnym przypadkiem stanów wielosystemowych.

Porównanie Informacji

Porównanie Informacji Klasycznej i Kwantowej

Informacja Klasyczna	**Informacja Kwantowa**
Bit: 0 lub 1	Qubit: superpozycja $\alpha\|0\rangle + \beta\|1\rangle$
Deterministyczne lub probabilistyczne	Superpozycja i splątanie
Operacje logiczne (AND, OR, NOT)	Operacje kwantowe (Hadamard, CNOT)
Brak korelacji nielokalnych	Splątanie kwantowe

Podsumowanie

- Informacja kwantowa rozszerza pojęcie informacji klasycznej.
- Superpozycja i splątanie są fundamentami informacji kwantowej.
- Matematyczne narzędzia, takie jak iloczyn tensorowy i macierze jednostkowe, odgrywają kluczową rolę.
- Zastosowania: algorytmy kwantowe, kryptografia, teleportacja.

Twierdzenie o Zakazie Klonowania

Wprowadzenie

- **Twierdzenie o Zakazie Klonowania (No-Cloning Theorem):** W mechanice kwantowej niemożliwe jest stworzenie dokładnej kopii nieznanego stanu kwantowego.
- Twierdzenie to wynika z podstawowych zasad mechaniki kwantowej:
  - Liniowość operacji kwantowych.
  - Jednostkowość przekształceń.
- Ma fundamentalne znaczenie w teorii informacji kwantowej:
  - Chroni prywatność informacji w kryptografii kwantowej.
  - Ogranicza zdolności obliczeń i komunikacji kwantowej.

Sformułowanie matematyczne

Sformułowanie matematyczne

- Rozważmy stan kwantowy $|\psi\rangle$, który chcemy skopiować:

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

- Klonowanie wymagałoby istnienia operacji jednostkowej U, takiej że:

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle\,,$$

gdzie $|e\rangle$ to stan początkowy urządzenia pomocniczego.

- Dla dwóch różnych stanów $|\psi\rangle$ i $|\phi\rangle$ musiałoby być:

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle\,,$$

$$U(|\phi\rangle \otimes |e\rangle) = |\phi\rangle \otimes |\phi\rangle\,.$$

Dowód Twierdzenia

Dowód Twierdzenia

- Dla dwóch różnych stanów $|\psi\rangle$ i $|\phi\rangle$:

$$\langle\psi|\phi\rangle = c, \quad |c| < 1.$$

- Po operacji klonowania:

$$\langle\psi\psi|\phi\phi\rangle = (\langle\psi|\phi\rangle)^2 = c^2.$$

- Jednakże operacja unitarna U zachowuje normę:

$$|\langle\psi|\phi\rangle| = |\langle\psi\psi|\phi\phi\rangle|,$$

co prowadzi do sprzeczności, gdy $|c| < 1$.

- Wniosek: Nie istnieje unitarna operacja U, która realizuje klonowanie.

Konsekwencje

Konsekwencje Twierdzenia

- **Kryptografia kwantowa:**
  - No-Cloning Theorem zapewnia bezpieczeństwo protokołów takich jak BB84.
- **Teleportacja kwantowa:**
  - Informacja kwantowa może być przenoszona, ale nie kopiowana.
- **Obliczenia kwantowe:**
  - Klonowanie stanów wejściowych jest niemożliwe, co wpływa na algorytmy i operacje.
- **Fizyka kwantowa:**
  - Ograniczenia dotyczące manipulacji stanami kwantowymi wynikają z fundamentalnych zasad teorii.

Porównanie z Klonowaniem Klasycznym

Porównanie z Klonowaniem Klasycznym

Klonowanie Klasyczne	**Klonowanie Kwantowe**
Można kopiować dowolny stan bitu	Nie można kopiować nieznanego stanu qubitu
Bez ograniczeń fizycznych	Ograniczenia wynikają z liniowości
Deterministyczne	Statystyczne (tylko dla pewnych przypadków)

Podsumowanie

Podsumowanie

- Twierdzenie o zakazie klonowania jest jednym z fundamentów mechaniki kwantowej.
- Wykazuje ograniczenia w manipulacji informacją kwantową.
- Ma szerokie zastosowanie w kryptografii, komunikacji i obliczeniach kwantowych.

Teleportacja kwantowa

Wprowadzenie

- Teleportacja kwantowa to proces przesyłania nieznanego stanu kwantowego przy użyciu:
  - stanu splątanego (zasób kwantowy),
  - komunikacji klasycznej.
- Kluczowe osoby:
  - Brett: jego kubit jest w nieznanym stanie $|\psi\rangle$,
  - Alice: próbuje przesłać stan kubitu Bretta,
  - Robert: odbiorca stanu kwantowego.
- W teleportacji klasyczna informacja nie wystarcza do odtworzenia stanu.

Stan początkowy

Stan początkowy układu

- Nieznany stan kubitu Bretta:
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,.$$
- Alice i Robert współdzielą stan splątany Bella:
$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$
- Stan początkowy trzech kubitów:
$$|\psi_{t=0}\rangle = |\psi\rangle \otimes \left|\Phi^+\right\rangle.$$
- Po podstawieniu:
$$|\psi_{t=0}\rangle = \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right).$$

Operacja CNOT

Nakładanie bramki CNOT

- Alice nakłada bramkę $\mathbf{CNOT}_1^2$ na kubity Bretta (1) i swoje (2).
- Zmienia to stan układu na:

$$|\psi_{t=1}\rangle = (\mathbf{CNOT}_1^2 \otimes \mathbf{I})\,|\psi_{t=0}\rangle\,.$$

- Wynik:

$$|\psi_{t=1}\rangle = \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle\right).$$

Bramka Hadamarda

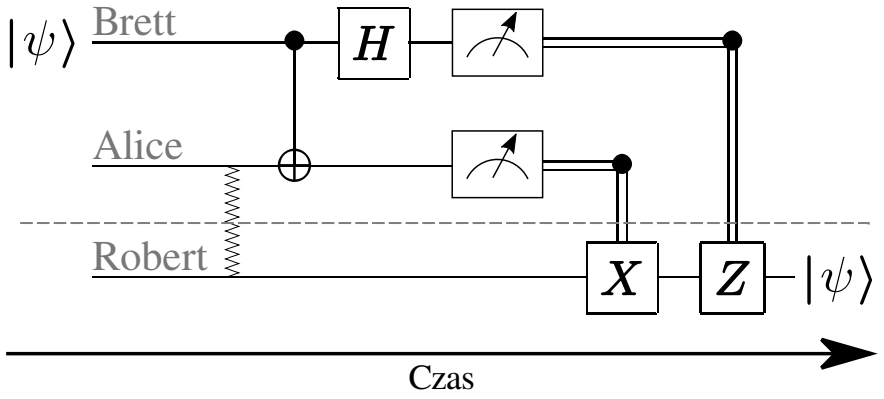
Nakładanie bramki Hadamarda

- Alice nakłada bramkę Hadamarda na kubit Bretta (1):

$$|\psi_{t=2}\rangle = (\mathbf{H} \otimes \mathbf{I} \otimes \mathbf{I})\,|\psi_{t=1}\rangle\,.$$

- Po operacji Hadamarda stan układu wynosi:

$$|\psi_{t=2}\rangle = \frac{1}{2}(\alpha\,|000\rangle + \alpha\,|100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|010\rangle + \beta\,|001\rangle - \beta\,|110\rangle - \beta\,|101\rangle).$$



Rysunek: Obwód teleportacji kwantowej. Linie poziome oznaczają kubity. Pionowa linia zygzakowata oznacza stan splątany. Linie podwójne oznaczają klasyczne bity. Pozioma linia przerywana oddziela układy Bretta i Alice od układu Roberta.

Pomiar i wyniki

Pomiar kubitów Alice

- Alice wykonuje pomiar dwóch pierwszych kubitów, który daje jeden z czterech wyników z równym prawdopodobieństwem.
- Wyniki i stany Roberta:
  - Wynik 00:
  $$|\psi_R\rangle = |\psi\rangle\,.$$
  - Wynik 01:
  $$|\psi_R\rangle = \mathbf{Z}\,|\psi\rangle\,.$$
  - Wynik 10:
  $$|\psi_R\rangle = \mathbf{X}\,|\psi\rangle\,.$$
  - Wynik 11:
  $$|\psi_R\rangle = \mathbf{XZ}\,|\psi\rangle\,.$$

Korekcja stanu Roberta

Korekcja stanu Roberta

- Alice przesyła wynik pomiaru do Roberta za pomocą kanału klasycznego.
- Robert stosuje odpowiednie bramki na swoim kubicie:
  - Dla wyniku 00: brak operacji.
  - Dla wyniku 01: $\mathbf{Z}$.
  - Dla wyniku 10: $\mathbf{X}$.
  - Dla wyniku 11: $\mathbf{XZ}$.
- Po korekcji stan kubitu Roberta wynosi:

$$|\psi_R\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,.$$

Podsumowanie

Podsumowanie protokołu teleportacji

- Teleportacja kwantowa umożliwia przesyłanie stanu kwantowego przy użyciu:
  - stanu splątanego Bella,
  - klasycznego kanału komunikacyjnego.
- Proces obejmuje:
  1. Wykonanie operacji kwantowych (CNOT, Hadamard),
  2. Pomiar częściowy,
  3. Przesłanie wyniku pomiaru klasycznie,
  4. Korekcję stanu odbiorcy.
- Teleportacja nie wymaga fizycznego przesyłania nośnika kwantowego.

Kryptografia

Problem: Bezpieczna transmisja bitów

- Dwie osoby (Alicja i Bob) chcą przesłać tajną informację w formie ciągu bitów.
- Informacja nie powinna zostać przechwycona przez osoby trzecie (np. Ewa).
- Klasyczne szyfrowanie opiera się na algorytmach, których bezpieczeństwo nie jest gwarantowane.
- Potrzebne: metoda całkowicie bezpiecznego przesyłu informacji.

Szyfr Vernama

Czym jest szyfr Vernama?

- Alicja i Bob współdzielą losowy klucz (ciąg bitów).
- Aleksandria szyfruje wiadomość, wykonując operację XOR między bitami wiadomości i klucza.
- Centrum deszyfruje wiadomość, ponownie stosując operację XOR z kluczem.
- Operacja XOR: wynik 1, gdy argumenty są różne, 0 w przeciwnym razie.

Tabela XOR

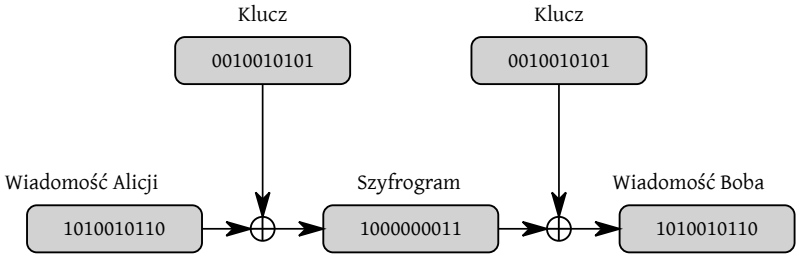
we_1	we_2	wy
0	0	0
0	1	1
1	0	1
1	1	0

Tabela: Tabela działania operacji XOR

Schemat działania szyfru Vernama

- Oznaczenia:
  - Wiadomość: $a_1, a_2, \ldots, a_n$
  - Klucz: $k_1, k_2, \ldots, k_n$
  - Szyfrogram: $s_1, s_2, \ldots, s_n$
  - Otrzymana wiadomość: $b_1, b_2, \ldots, b_n$
- Wzory:
  - Szyfrowanie: $s_i = \mathrm{XOR}(a_i, k_i)$
  - Deszyfrowanie: $b_i = \mathrm{XOR}(s_i, k_i)$

Przykład działania szyfru Vernama



Rysunek: Symbol $\oplus$ oznacza operację XOR.

Zalety szyfru Vernama

- Gwarantuje całkowite bezpieczeństwo pod warunkiem, że:
  - Klucz jest losowy.
  - Klucz jest znany tylko nadawcy i odbiorcy.
- Szyfrogram wygląda jak losowy ciąg bitów dla osoby trzeciej (Ewy).

Protokół BB84

Problem z szyfrem Vernama

- Wymaga klucza tak długiego jak wiadomość, który musi być:
  - Całkowicie losowy,
  - Bezpiecznie przesłany między nadawcą a odbiorcą.
- Rozwiązanie: **Protokół BB84** (Bennett i Brassard, 1984).

Podstawy protokołu BB84

Stany i pomiary kwantowe

- Cztery stany kubitowe:

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

- Dwa typy pomiarów:

$$\mathcal{P} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}, \quad \mathcal{Q} = \{|+\rangle\langle +|, |-\rangle\langle -|\}$$

Zależność wyników pomiaru od stanu

Stan	Pomiar	Wynik
$\|0\rangle$	$\mathcal{P}$	0
$\|1\rangle$	$\mathcal{P}$	1
$\|+\rangle$	$\mathcal{Q}$	$+$
$\|-\rangle$	$\mathcal{Q}$	-
$\|0\rangle$	$\mathcal{Q}$	$+/-$, $p_+ = p_- = \frac{1}{2}$
$\|1\rangle$	$\mathcal{Q}$	$+/-$, $p_+ = p_- = \frac{1}{2}$
$\|+\rangle$	$\mathcal{P}$	$0/1$, $p_0 = p_1 = \frac{1}{2}$
$\|-\rangle$	$\mathcal{P}$	$0/1$, $p_0 = p_1 = \frac{1}{2}$

Tabela: Zależność wyniku pomiaru od stanu i pomiaru.

Kroki protokołu

Opis kroków

1. Alicja wysyła losowe kubity.
2. Bob wybiera losowo rodzaj pomiaru ($\mathcal{P}$ lub $\mathcal{Q}$).
3. Bob zapisuje wyniki i rodzaje pomiarów.
4. Bob ujawnia rodzaje pomiarów.
5. Alicja informuje, które pomiary były dopasowane.
6. Kubity są dzielone na dwie grupy:
   - Dopasowane do pomiarów,
   - Niedopasowane (odrzucane).

Tworzenie klucza

- Jeśli nie wykryto błędów, z dopasowanych kubitów tworzony jest klucz.
- Porównanie losowego podzbioru kubitów pozwala wykryć podsłuch.

Przykład działania protokołu

Przykład bez podsłuchu

A_1	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
C_1	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{Q}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$	$\mathcal{P}$
bit	0	1	1				1		0			0		1				1	0	0

Tabela: Przykład realizacji protokołu bez podsłuchu.

Podsłuch w protokole BB84

- Alice przechwytuje kubity, wykonuje pomiary i wysyła zmienione kubity.
- Zmiany stanów są wykrywane przez porównanie wyników.
- Zmodyfikowane kubity są odrzucane.