Kvantumalgoritmusok
A Kvantum Fourier-transzformáció

Mi a Kvantum Fourier-transzformáció?

A **Quantum Fourier Transform (QFT)** a klasszikus diszkrét Fourier-transzformáció kvantumos megfelelője.

Fő célja:

- periódusok felismerése,
- fázisinformáció kinyerése,
- kvantum-interferencia kihasználása.

Mi a Kvantum Fourier-transzformáció?

A **Quantum Fourier Transform (QFT)** a klasszikus diszkrét Fourier-transzformáció kvantumos megfelelője.

Fő célja:

- periódusok felismerése,
- fázisinformáció kinyerése,
- kvantum-interferencia kihasználása.

A QFT számos kvantumalgoritmus alapvető építőköve:

- Shor-algoritmus,
- kvantumos fázisbecslés,
- kvantumos szimuláció,
- kvantumos gépi tanulás.

Diszkrét Fourier-transzformáció

Legyen:

$$(x_0, x_1, \ldots, x_{N-1})$$

egy komplex vektor.

A diszkrét Fourier-transzformáció:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk},$$

ahol

$$\omega_N = e^{2\pi i/N}.$$

Diszkrét Fourier-transzformáció

Legyen:

$$(x_0, x_1, \dots, x_{N-1})$$

egy komplex vektor.

A diszkrét Fourier-transzformáció:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk},$$

ahol

$$\omega_N = e^{2\pi i/N}.$$

A Fourier-transzformáció:

- frekvenciákat azonosít,
- periodicitást tár fel,
- jeleket frekvenciatérbe visz át.

Kvantumállapotok

Egy n-qubites rendszer dimenziója:

$$N = 2^n.$$

Általános kvantumállapot:

$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle,$$

ahol:

- $|x\rangle$ a bázisállapot,
- $a_x \in \mathbb{C}$,
- $$\sum_x |a_x|^2 = 1.$$

A kvantumalgoritmusok az amplitúdókon és fázisokon dolgoznak.

A Kvantum Fourier-transzformáció definíciója

A QFT az alábbi unitér operátor:

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

Ekvivalensen:

$$F_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{xy} |y\rangle.$$

Tulajdonság:

$$F_N^\dagger F_N = I.$$

Tehát a QFT egy **unitér transzformáció**.

A QFT mátrixalakja

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}$$

ahol

$$\omega = e^{2\pi i/N}.$$

Ez a klasszikus Fourier-mátrix kvantumos megfelelője.

1 qubites QFT

Ha:

$$N = 2,$$

akkor:

$$\omega_2 = -1.$$

A QFT:

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Ez pontosan a **Hadamard-kapu**:

$$H = F_2.$$

A Hadamard-kapu tehát a legegyszerűbb Fourier-transzformáció.

2 qubites QFT

$$F_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Példa:

$$F_4|1\rangle = \frac{1}{2}\left(|0\rangle + i|1\rangle - |2\rangle - i|3\rangle\right).$$

A QFT:

- amplitúdókat fázisokká alakít,
- interferenciát hoz létre,
- periodicitást emel ki.

Bináris reprezentáció

Legyen:

$$x = x_1 x_2 \dots x_n$$

az x bináris alakja.

Ekkor:

$$|x_1 x_2 \dots x_n\rangle \mapsto \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \left(|0\rangle + e^{2\pi i \, 0.x_k x_{k+1} \dots x_n} |1\rangle\right).$$

ahol

$$0.x_k x_{k+1} \dots x_n = \frac{x_k}{2} + \frac{x_{k+1}}{2^2} + \cdots .$$

Ez teszi lehetővé a hatékony kvantumáramkör-megvalósítást.

A QFT kvantumáramkör

A QFT felépítése:

- Hadamard-kapuk,
- kontrollált fáziskapuk,
- qubit-cserék.

Komplexitás:

$$O(n^2)$$

Közelítő QFT:

$$O(n \log n)$$

Klasszikus DFT:

$$O(N \log N), \qquad N = 2^n.$$

Ez exponenciális gyorsulást eredményezhet.

Miért talál periódusokat a QFT?

Legyen:

$$f(x + r) = f(x).$$

A kvantumalgoritmus szuperpozíciót készít:

$$\sum_x |x\rangle |f(x)\rangle.$$

Mérés után:

$$\sum_k |x_0 + kr\rangle.$$

QFT alkalmazása:

$$\frac{m}{N} \approx \frac{s}{r}.$$

Az interferencia kiemeli a periódust.

Ez a Shor-algoritmus matematikai alapja.

1. Shor-algoritmus

A QFT legismertebb alkalmazása:

- prímtényezős felbontás,
- perióduskeresés,
- RSA feltörése.

1. Shor-algoritmus

A QFT legismertebb alkalmazása:

- prímtényezős felbontás,
- perióduskeresés,
- RSA feltörése.

Kulcsötlet: A QFT egy klasszikusan nehéz problémát gyakran „perioduskeresési problémává” alakít át, majd ezt a periódust kvantumos interferenciával hatékonyan kimutathatóvá teszi.

2. Kvantumos fázisbecslés

A QFT alapvető szerepet játszik a **Quantum Phase Estimation** algoritmusban.

Feladat:

$$U|u\rangle = e^{2\pi i\phi}|u\rangle.$$

A QFT segítségével meghatározható:

$$\phi.$$

2. Kvantumos fázisbecslés

A QFT alapvető szerepet játszik a **Quantum Phase Estimation** algoritmusban.

Feladat:

$$U|u\rangle = e^{2\pi i\phi}|u\rangle.$$

A QFT segítségével meghatározható:

$$\phi.$$

Alkalmazások:

- kvantumkémia,
- molekulamodellezés,
- sajátérték-problémák.

3. Kvantumos szimuláció

A QFT fontos szerepet játszik:

- Hamilton-operátorok diagonalizálásában,
- energiaszintek meghatározásában,
- kvantumos anyagmodellekben.

Lehetséges alkalmazások:

- gyógyszerkutatás,
- új anyagok,
- katalizátorok.

4. Kvantumos gépi tanulás

A QFT használható:

- spektrális elemzésre,
- feature extraction-re,
- kvantumos kernelmódszerekben.

A terület jelenleg intenzív kutatás alatt áll.

5. Amplitúdóbecslés

A QFT segítségével:

- kvadratikus gyorsulás érhető el,
- Monte Carlo módszerek gyorsíthatók.

Alkalmazások:

- pénzügyi modellezés,
- kockázatelemzés,
- opcióárazás.

Ciklikus eltolások diagonalizálása

Definiáljuk:

$$S|x\rangle = |x + 1 \bmod N\rangle.$$

A Fourier-állapotok:

$$|\tilde{k}\rangle = \frac{1}{\sqrt{N}} \sum_x \omega^{kx} |x\rangle.$$

Ekkor:

$$S|\tilde{k}\rangle = \omega^{-k} |\tilde{k}\rangle.$$

A QFT tehát:

- diagonalizálja az eltolásoperátort,
- frekvenciabázisba visz át.

Mély matematikai kapcsolat

A QFT kapcsolatban áll:

- harmonikus analízissel,
- csoportreprezentáció-elmélettel,
- ciklikus csoportokkal,
- spektrálelmélettel.

Különösen:

$$\mathbb{Z}_N$$

ciklikus csoport Fourier-analízisével.

Összefoglalás

A QFT:

- a kvantumszámítás egyik legfontosabb algoritmikus eszköze,
- periodicitást és fázisinformációt tár fel,
- exponenciális gyorsulást tehet lehetővé.

Fő alkalmazások:

- Shor-algoritmus,
- kvantumos fázisbecslés,
- kvantumos szimuláció,
- kvantumos gépi tanulás,
- amplitúdóbecslés.

A QFT a kvantumalgoritmusok egyik alapvető matematikai építőköve.

Köszönöm a figyelmet!