

Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai Kar

Hálózati Rendszerek és Szolgáltatások Tanszék

**Kvantumkeresés szimulációja**

Készítették: A tárgy oktatói

E-mail: qount-course@mcl.hu

2023. szeptember 1.

Tartalomjegyzék

[1. Grover-algoritmus szimulációja 3](#_Toc151672027)

[1.1. Ábrák 3](#_Toc151672028)

[2. További fejezetek 3](#_Toc151672029)

[2.1. Ábrák 3](#_Toc151672030)

[2.2. Táblázatok 3](#_Toc151672031)

[2.3. Irodalomjegyzék 4](#_Toc151672032)

[3. Továbblépési lehetőségek 5](#_Toc151672033)

[Irodalomjegyzék 6](#_Toc151672034)

[Rövidítések jegyzéke 7](#_Toc151672035)

[Függelék 8](#_Toc151672036)

# Grover-algoritmus szimulációja

## Grover-algoritmus áttekintése

## Egyszerű Grover algoritmus szimulálása

Először tekintsünk egy klasszikus keresést egy adathalmazban:

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

Itt véletlenszerűen generálunk 10 számot majd ezek között keressük az 1-es értéket, amit átlagban 5,5 keres

Most már tovább léphetünk a kvantumos megközelítésre, ahol a Grover-algoritmust fogjuk használni.

Először létrehozzuk az oracle-t:

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus, diagram látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, képernyő, szoftver látható

Automatikusan generált leírás

Ebben az esetben csak azonos kimenetek lehetnek, vagyis 00 vagy 11.

Ha pedig beszúrunk egy hadamard kaput a controlled z kapu elé, akkor az alábbi hálózat jön létre:

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

Ez pedig a következő állapotvektort generálja:

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

Így végeredményben a következő kimenetek lesznek láthatóak, ahol már két állapot is elő fog fordulni: A 01 és 11 az esetek 50-50%-ában (átlagban).  
A képen szöveg, képernyőkép, képernyő, Diagram látható

Automatikusan generált leírás

## RSA feltörése Grover-algoritmussal

# Shor-algoritmus szimulációja

## 2.1. A Shor-algoritmus

A Shor-algoritmus továbbra is a kvantum-számítástechnika egyik legjelentősebb fejlesztése, mivel kimutatta, hogy a kvantumszámítógépek felhasználhatók a fontos, jelenleg klasszikusan nyomon követhető problémák megoldására. A Shor algoritmusa gyors módot biztosít a nagy számok kvantumszámítógép használatával történő faktorálására, amely a faktorálás nevű probléma. Számos mai kriptorendszer biztonsága azon a feltételezésen alapul, hogy nincs gyors algoritmus a faktoráláshoz. Így a Shor-algoritmus jelentős hatással volt arra, hogyan gondolunk a biztonságra egy kvantum utáni világban.

A Shor-algoritmus hibrid algoritmusként is felfogható. A kvantumszámítógép egy számításilag kemény feladat végrehajtására szolgál, amelyet pontkeresésnek nevezünk. Az időszaki megállapítások eredményeit ezután klasszikusan feldolgozzák a tényezők becsléséhez.

### 2.1.1 Order finding

Alapok:

### 2.1.2 Fázis meghatározás

### 2.1.2 Faktorizálás

A Shor-algoritmus továbbra is a kvantum

## 2.2. Táblázatok

A dokumentumban lévő táblázatok számozottak, mindegyikhez tartozik egy rövid táblázatcím is, a szövegben pedig hivatkozás található az ábrára (pl. A munka eredményét az **Hiba! A hivatkozási forrás nem található.**ban foglaltam össze). Ha tehetjük, ne kézzel írjuk be az táblázatok sorszámát, és a szövegben se kézzel hivatkozzunk a táblázatokra! Mind a LaTeX, mind a Microsoft Office 2010 támogatja az automatikus táblázat-sorszámozást. Utóbbi esetben a *„Hivatkozás”* menü *„Képaláírás beszúrása*” (nem elírás!) menüpontjával tudunk automatikus sorszámot beszúrni, a szövegben pedig a *„Hivatkozás”* menü *„Kereszthivatkozás”* menüpontjával tudunk automatikus hivatkozást beszúrni. LaTeX esetében a \label{ } paranccsal tudunk a táblázatnak hivatkozható címkét létrehozni, és a \ref{ } utasítással tudunk hivatkozni az ábrára. Például: \label{table:test} az ábra beszúrása környezetében, és \ref{table:test} a szövegben, ahol hivatkozunk az ábrára.

## 2.3. Irodalomjegyzék

# Továbblépési lehetőségek

Mutassa be röviden, milyen továbblépési lehetőségek képzelhetőek el.

# Irodalomjegyzék

[1] LINK esetében fel kell tüntetni: *(Utolsó látogatás dátuma: 2020. szeptember 9.)*

[2]

[3]

# Rövidítések jegyzéke

HBR Három betűs rövidítés

QKD Quantum Key Distribution

# Függelék

Opcionális függelék, további anyagokkal