HHL - Algorithmus

Alfred Nguyen

Fakultät der Informatik
Technische Universität München
85758 Garching, Bavaria

June 2023

Gliederung

Gliederung

Anwendungen

Hauptproblem

- Hauptproblem: gibt keinen vollständigen Vektor aus
- Aber einige Probleme können mit dieser Methode gelöst werden:

Anwendungen

Machine Learning: Least-Square-Fitting

- Datenanpassung mit Least Square Fitting
- durch Berechnung einer Schätzung der inversen Matrix

Analysis of Large Sparse Electrical Networks

- Elektrizitätsnetz vielen verbundenen Komponenten
- geringe Anzahl Verbindungen zwischen den Komponenten
- Berechnung des Widerstands durch approximation von Erwartungswerten

Es wäre wichtig, mehr Anwendungen zu finden, welche den Anforderungen entsprechen.

Anwendung in IT-Security

HHL in der IT-Security

- in erster Linie nur für Lösen von linearen Systemen
- nicht direkt mit IT-Security verbunden
- aber Potenzial als Subroutine angewendet zu werden

Mögliche Anwendungen

- secure multi-party computation
- zero-knowledge proofs
- cryptographic key generation and management
- big data analysis/pattern recognition (für Betrugserkennung)

Variationen

Modifikationen und Optimierung

- QRAM zur Vorbereitung von $|b\rangle$
- kein Ancilla-Bit erforderlich unter bestimmten Voraussetzungen
- Variable time amplitude amplification um condition number κ zu verbessern

Perspektive

- Großer Einfluss im Bereich Quantum Machine Learning
- noch keine bahnbrechenden Anwendungen (wie z.B. Shors Algorithmus zum Brechen von RSA)
- aber viel aktive Forschung um neue Verbesserungen im Algorithmus zu finden
- zeigt deutlichen Fortschritt in der Quantencomputing welt

Was das

Ablauf

1. State Preparation
   - Enkodiere Vektor und Matrix in Quanten Computer
2. Quantum Phase Estimation
   - ermittle Eigenwerte und Eigenvektoren
   - bilde $|b\rangle$ in Eigenbasis A ab
3. Ancilla Bit Rotation - Invertieren der Eigenwerte
4. Inverse Quantum Phase Estimation
5. Messung