Quantum Computing – Lernkontrolle / Test

1.1 Antworten (Musterlösung)

1.) Sie könnten Rechenaufgaben erledigen welche ein klassischer Rechner nicht zu lösen vermag wie.

Datenbanksuche	**klassischer Computer**	**Quantencomputer**	**Quantenalgorithmus**
Formel	~ N / 2	~ √N	
Lösung	**30 Millionen Schritte**	**6000 Schritte**	**Grover**
1024-bit Kryptographie	**klassischer Computer**	**Quantencomputer**	**Quantenalgorithmus**
Formel	~ $\exp(cL^{1/3})$	~ $O(L^3)$	
Lösung	**10^{20} Schritte**	**10^9 Schritte**	**Shor**

2.) David Deutsch gelang 1985 der theoretische Durchbruch, als er eine Turingmaschine modelliere, welche die Gesetzte der Quantenmechanik umsetzt.

3.) Ein klassischer Computer kennt für ein Bit nur die beiden Zustände: 0 oder 1
Ein Quantencomputer rechnet mit dem Quantenbit (Qubit): |0> und |1>

4.) In der Dirac-Notation. $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$.

5.)
a. Greenberger-Horne-Zeilinger-Zustände (kurz: GHZ-Zustände)
b. W-Zustände.

6.) Der Quantencomputer besteht aus einer Reihe von Qubit(Quantenbit),
a. die in einen Anfangszustand versetzt werden können z.B. |0› ,
b. die Information robust speichern,
c. auf die (universelle) Quantengatter anwendbar sind und
d. die gemessen werden können.

7.) Aus dem Ergebnis der Berechnung lässt sich die Eingabe eindeutig berechnen.

8.) Im Jahr 1997 führte Anton Zeilinger erstmals mit Photonen ein Experiment durch welches Quantenzustände mittels einer Zustandsänderung miteinander verschränkter Quante übertrug

9.) a. Ein Quantengatter (engl. Quantum Gate) ist kein technischer Baustein, sondern stellt eine elementare physikalische Manipulation eines oder mehrerer Qubits dar.

b. Logikgatter werden zu einem Schaltnetz verbunden, welche komplexe Operationen wie z.B. die Addition zweier binärer Zahlen durchführt.

10**.) Kategorien :**

- Quanten-Fouriertransformation
- Quanten-Suchalgorithmen
- Quanten-Simulation

11.) 2 Verfahren **:**

Das **BB84-Protokoll**

Es nutzt einzelne Photonen zur Übertragung. Aufgrund des No-Cloning- Theorems können es Angreifer nicht kopieren.

Das **Ekert-Protokoll**

Hier verwenden verschränkte Zustände angewandt.