UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Dr. Mónica Benito
https://theorie.physik.uni-konstanz.de/burkard/teaching/19W-QI

Quanteninformationstheorie
Wintersemester 2019/2020- Übungsblatt 13
Ausgabe: 31.1.2020, Abgabe: 7.2.2020, Übungen: 10.2.2020

Aufgabe 42 : Erasure Kanal Kapazität

Durch einem Erasure Kanal wird der Zustand $|0\rangle$ bzw. $|1\rangle$ mit der Wahrscheinlichkeit $1-p$ richtig übertragen und mit der Wahrscheinlichkeit p als gelöscht (*erasure*) markiert (oder bei Charlie abgehört).

a) Argumentieren Sie mithilfe des No-Cloning-Theorems, dass $C(p) = 0$ wenn $p \geq 1/2$. $C(p)$ ist die Kapazität des Kanals.

b) Betrachten Sie den Erasure Kanal 1 mit der Fehlerwahrscheinlichkeit p_1 und $C(p_1) > 0$ und den Erasure Kanal 2 mit der Fehlerwahrscheinlichkeit $p_2 \leq p_1$. Beweisen Sie die Ungleichung

$$C(p_2) \leq 1 - \frac{p_2}{p_1} + \frac{p_2}{p_1} C(p_1)$$

Hinweis: Berechnen Sie die Anzahl der verschlüsselten Qubits, die Bob mit beliebige Güte decodieren kann, wenn Alice $(1 - p_2/p_1)n$ Qubits durch einen perfekt Kanal und $(p_2/p_1)n$ Qubits durch den Kanal 1 übertragt.

c) Beweisen Sie, dass die Kapazität eines Erasure Kanals nach unten begrenzt ist, $C(p) \leq 1 - 2p$.

Aufgabe 43 : Simon Algorithmus (10 Punkte)

Mit Hilfe des Quanten-Simon-Algorithmus lässt sich die Periode einer unbekannte Funktion schneller als mit jeder klassischen Methode berechnen. Gegeben sei ein Orakel, das n-Qubits als Eingabe verwendet um die Funktion $f(a)$ zu berechnen. Diese Funktion ist periodisch unter der bitweisen Addition Modulo 2, das heißt $f(a \oplus b) = f(a) \, \forall \, a$ und für alle andere Werte a unterschiedlich.

a) (2 Punkte) Zeigen Sie, dass die Periode (n-bit Zahl) b durch $b = a_1 \oplus a_2$ bestimmt werden kann, wenn man zwei Werte a_1 and a_2 findet für welche $f(a_1) = f(a_2)$ gilt. Schätzen Sie die Anzahl der notwendigen klassischen Versuche als Funktion von n.

b) (4 Punkte) Der Simon-Algorithmus verlangt als als Startwert ein n-Qubit-Register, welches in einer Überlagerung aller Zustände $|a\rangle$ ist,

$$|r_1\rangle = \frac{1}{2^{n/2}} \sum_{a=0}^{2^n-1} |a\rangle \ .$$

In ein zweites n-Qubit-Register mit jedem Qubit im Zustand $|r_2\rangle = |0\rangle$ werden die Ergebnisse des Orakels geschrieben. Das Orakel führt folgende Abbildung aus:

$$|r_1\rangle \otimes |r_2\rangle = \frac{1}{2^{n/2}} \sum_{a=0}^{2^n-1} |a\rangle \otimes |0\rangle \to \frac{1}{2^{n/2}} \sum_{a=0}^{2^n-1} |a\rangle \otimes |f(a)\rangle \ .$$

Eine Messung wird auf dem zweitem Register in der (Berechungs)-Basis $|a\rangle$ durchgeführt, mit dem Ergebnis $f(a_1)$. Was ist der Zustand des ersten Registers, $|r_1'\rangle$, direkt nach der Messung?
Hinweis: $f(a') = f(a)$ gilt genau dann wenn $a' = a \oplus b$.

c) (4 Punkte) Aus dem Zustand $|r_1'\rangle$ lässt sich noch keine Information über die Periode b bekommen. Zeigen Sie, dass ein Hadamard-Gatter angewendet auf jedes Qubit den Zustand

$$H^{\otimes n}|r_1'\rangle = \frac{1}{2^{(n-1)/2}} \sum_{b\cdot c=0} (-1)^{a_1\cdot c}|c\rangle$$

liefert. Die Summe geht über alle 2^{n-1} Werte von c für welche gilt, $b \cdot c = 0 \mod 2$. Hier ist die Operation $a_1 \cdot c$ das bitweise Skalarprodukt der binären Darstellungen der Zahlen a_1 and c. Schätzen Sie die Anzahl der notwendigen elementaren Operationen , um die Zahl b zu finden.
Hinweise: Ein n-Qubit-Hadamard-Gatter, n-fache Tensorprodukt von 1-Qubit Hadamard-Gattern, kann wie folgt ausgedrückt werden:

$$H^{\otimes n}|a\rangle = \frac{1}{2^{n/2}} \sum_{c=0}^{2^n-1} (-1)^{a\cdot c}|c\rangle$$