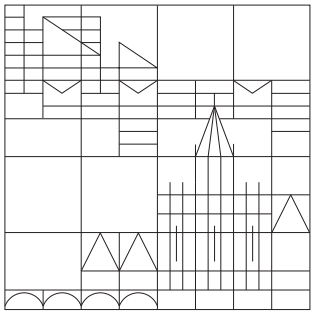
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Dr. Mónica Benito
http://theorie.physik.uni-konstanz.de/burkard/teaching/18S-QI



Quanteninformationstheorie
Sommersemester 2018 - Übungsblatt 3
Ausgabe: 15.5.2018, Abgabe: 22.5.2018, Übungen: 24./25.5.2018

Aufgabe 10: Dichtematrix und Quanteninformation

a) Geben Sie die Dichtematrix ρ für den Zustand $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$ an.

b) Finden Sie die Dichtematrizen der Systeme A und B aus den partiellen Spuren $\rho_A = \mathrm{Tr}_B \rho$ und $\rho_B = \mathrm{Tr}_A \rho$.

Hinweis: Die partielle Spur der Dichtematrix des zusammengesetzten Systems $\rho \equiv \rho_{AB}$ bezüglich des Teilsystems B ist durch die reduzierte Dichtematrix ρ_A gegeben, mit den Komponenten $(\rho_A)_{i,j} = \sum_k \rho_{ik,jk}$. Die Summe läuft über die zum Teilsystem B gehörenden Indizes.

c) Berechnen Sie die von Von-Neumann-Entropien $S(\rho_A)$, $S(\rho_B)$ und $S(\rho)$. Vergleichen Sie $S(\rho)$ mit $S(\rho_A)$ bzw. $S(\rho_B)$. Stellen Sie Ihr Ergebnis der allgemeinen Regel für die (klassische) Shannon-Entropie gegenüber.

d) Führen Sie die Schritte a)-c) für einen Zustand der Form $|\psi'\rangle = |\phi\rangle_A |\chi\rangle_B$ durch. Wo gibt es Unterschiede und woran liegen diese?

e) Eine Dichtematrix beschreibe den Zustand von 2 Qubits. Die partiell transponierte Dichtematrix bekommt man, wenn man die Dichtematrix nur bezüglich eines Teilsystems transponiert. Wenn wir das zweite Teilsystem zum Transponieren auswählen, bedeutet dies die folgende Transformation für die Dichtematrix ρ in der Basis $\{|0\rangle_A |0\rangle_B, |0\rangle_A |1\rangle_B, |1\rangle_A |0\rangle_B, |1\rangle_A |1\rangle_B\}$: $\rho_{12} \leftrightarrows \rho_{21}$, $\rho_{14} \leftrightarrows \rho_{23}$, $\rho_{32} \leftrightarrows \rho_{41}$ und $\rho_{34} \leftrightarrows \rho_{43}$. Finden Sie die partiell transponierten Dichtematrizen für die Zustände $|\psi\rangle$ und $|\psi'\rangle$. Was ist der wichtige Unterschied zwischen diesen beiden Operatoren?

Hinweis: Stellen Sie fest, ob die partiell transponierten Dichtematrizen positiv semidefinit sind, z. B. indem Sie überprüfen, ob diese Operatoren nur Eigenwerte ≥ 0 haben.

Aufgabe 11 : Boolean functions (2 Punkte)

a) Schreiben Sie die Function XOR in disjunktiver Normalform.

b) Schreiben Sie die Abbildung

$$(x, y, z) \to (x + y, x + y + z) \bmod 2$$

in disjunktiver Normalform.

Aufgabe 12: RSA-Protokoll (4 Punkte)

Alice würde es gern allen ermöglichen, ihr verschlüsselte Information zu senden, die nur sie entschlüsseln kann. Dafür nimmt sie zwei grosse Primzahlen p und q und berechnet das Produkt $N = p\,q$. Alice wählt ausserdem einen Kodierungsexponenten e, der folgende Bedingung erfüllt:

$$\mathrm{ggT}(e, (p-1)(q-1)) = 1.$$

ggT bezeichnet den grössten gemeinsamen Teiler. Der öffentliche Schlüssel ist damit (N, e). Um den geheimen Schlüssel zu bekommen, findet Alice den Dekodierungsexponenten aus der folgenden Gleichung:

$$e\,d = 1 \mod [(p-1)(q-1)]. \tag{1}$$

Damit ist der geheime Schlüssel (d, p, q). Die verschlüsselte Nachricht ist nun $c = m^e \mod N$, wobei m die Nachricht ist, und $m < N$ erfüllt sein muss. Die Entschlüsselung erfolgt nach der Formel $m = c^d \mod N$.

a) (2 Punkte) Benutzen Sie das Euler-Theorem, zusammen mit der Gleichung (1) und den algebraischen Eigenschaften des Modulus, um sich zu vergewissern, dass $c^d \mod N = m$. Das Euler-Theorem besagt, dass für beliebige Primzahlen p und q und eine natürliche Zahl m gilt

$$m^{(p-1)(q-1)} = 1 \mod p\,q, \quad \text{falls} \quad \mathrm{ggT}(m, p\,q) = 1; \tag{2}$$
$$m^{q-1} = 1 \mod q, \quad \text{falls} \quad \mathrm{ggT}(m, q) = 1. \tag{3}$$

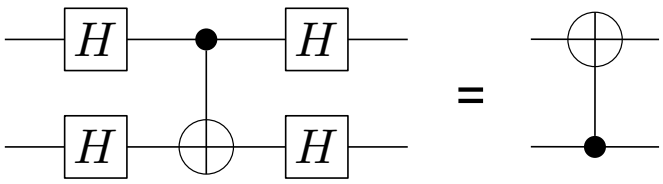
Die folgende Eigenschaft des Modulus ist ebenfalls nützlich:

$$x^s \mod N = (x \mod N)^s \mod N. \tag{4}$$

b) (2 Punkte) Benutzen Sie das in a) beschriebene RSA-Protokoll um eine Nachricht zu verschlüsseln und wieder zu entschlüsseln. Nehmen Sie z.B. $p = 7$, $q = 11$ und $e = 37$. In diesem Fall ist dann $d = 13$. Nehmen Sie $m = 2$ und finden Sie die verschlüsselte Nachricht c und daraus m wieder. Die Rechnung kann man mit einem normalen Taschenrechner durchführen, wenn man die Eigenschaft (4) benutzt.

Aufgabe 13 : CNOT- und Hadamard-Gatter (2 Punkte)

Zeigen Sie, dass die Rolle von *control*- und *target*-Qubit für das CNOT-Gatter durch den folgenden Quantenschaltkreis vertauscht werden kann:



H bezeichnet hierbei das *Hadamard*-Gatter.