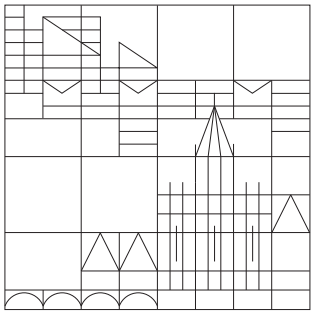
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Marko Rancic
http://theorie.physik.uni-konstanz.de/burkard/teaching/14S-QI



Quanteninformationstheorie
Sommersemester 2014 - Übungsblatt 3
Ausgabe: 13.05.2014, Abgabe: 20.05.2014, Übungen: 22./23.05.2014

Aufgabe 13: Dichtematrix und Quanteninformation (schriftlich)

a) (1 Punkt) 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) (2 Punkte) Finden Sie die Dichtematrizen der Systeme A und B aus den partiellen Spuren $\rho_A = \mathrm{Tr}_B \rho$ und $\rho_B = \mathrm{Tr}_A \rho$.

c) (2 Punkte) 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) (2 Punkte) 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) (2 Punkte) 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 sind, z. B. indem Sie überprüfen, ob diese Operatoren nur Eigenwerte ≥ 0 haben.

Aufgabe 14: Hamiltonoperator und Quantengatter

Betrachten Sie den folgenden Hamiltonoperator für ein Qubit,

$$H = i\hbar\omega(|0\rangle\langle 1| - |1\rangle\langle 0|),$$

der auf einem Hilbert-Raum von orthogonalen Zuständen $\{|0\rangle, |1\rangle\}$ wirkt, wobei ω reell ist.

i) Überprüfen Sie, ob H selbstadjungiert ist.

ii) Finden Sie die Eigenwerte und die entsprechenden normierten Eigenzustände von H.

iii) Finden Sie die unitäre Matrix

$$U(t) = \exp(-iHt/\hbar).$$

Zu welchen Zeiten t wirkt $U(t)$ wie ein NOT-Operator:

$$U(t)\,|0\rangle \to |1\rangle\,, \qquad U(t)\,|1\rangle \to |0\rangle?$$

iv) Berechnen Sie $U(t = \pi/4\omega)$ und $(U(t = \pi/4\omega))^2$.

Aufgabe 15: RSA-Protokoll

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) Benutzen Sie das Lagrange-Theorem, zusammen mit der Gleichung (1) und den algebraischen Eigenschaften des Modulus, um sich zu vergewissern, dass $c^d = m$. Das Lagrange-Theorem besagt, dass für ein $x \in \{1, ..., p\,q-1\}$ mit $\mathrm{ggT}(p\,q-1, x) = 1$ die folgende Beziehung erfüllt ist,

$$x^{(p-1)(q-1)} = 1 \mod p\,q, \tag{2}$$

falls p und q Primzahlen sind. Die folgende Eigenschaft des Modulus ist ebenfalls nützlich:

$$x^s \mod N = (x \mod N)^s \mod N. \tag{3}$$

b) 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 (3) benutzt.