

Quantum Information Theory

Exercise sheet 6

Lecture: Prof. Dr. Otfried Gühne Exercise: Costantino Budroni
Lecture: Tuesday, 10-12, Room D 120
Exercise: Monday, 15-17, Room B 107

14. Example of joint entropy

Let $P(A, B)$ be given by:

		B	
		0	1
A	0	1/3	1/3
	1	0	1/3

Find $P(A)$, $P(B)$, $P(A|B)$, $P(B|A)$, $H(A)$, $H(B)$, $H(A, B)$, $H(A|B)$, $H(B|A)$ and $I(A, B)$.

15. Properties of the entropy

- Consider a probability distribution P with $P(a_i) < P(a_j)$ for two indices i and j and a process that makes the distribution more uniform by adding ε to $P(a_i)$ and subtracting it from $P(a_j)$, where $0 < \varepsilon < (P(a_j) - P(a_i))/2$. Show that this process increases the Shannon entropy.
- Show that if $H(B|A) = 0$, then B is a function of A , i. e., for all a with $P(a) > 0$ there is only one possible value of b with $P(a, b) > 0$.

16. Eavesdropping

Consider the BB84 protocol. Eve performs an intercept-and-resend attack on a fraction r of the qubits. Calculate the mutual information $I(A, B)$ between the sifted keys of Alice and Bob.