**Foundations of Quantum Mechanics**

Prof. Dr. O. Gühne, T. Kraft

*Sheet 9* — SS 2019 — Due: Mon., 17.06.2019

---

### Exercise 24: Popescu-Rohrlich (PR) boxes I (3+5)

Consider a hypothetical box that has a binary input $x$ and binary output $a$, i.e. $x, a \in \{0, 1\}$. Suppose that Alice and Bob both have access to such a box. Alice inputs $x$ into her box and obtains $a$, Bob inputs $y$ into his box and obtains $b$ and the boxes are constructed such, that

$$a \oplus b = xy, \tag{1}$$

where $\oplus$ denotes the addition modulo 2. Suppose Alice has a string of variables $\{x_i\}_{i=1\ldots365}$. Each $x_i$ she associates to a day in her calendar and it is zero if she is busy and one if she is free. Similarly, Bob defines $\{y_i\}_{i=1\ldots365}$. Alice and Bob could meet on the $i^{th}$ day if and only if the product $x_i y_i = 1$. Since Alice is extremely busy there is only one day in her calendar where she is free. Alice wants to find out if they could meet at her free day or not, i.e. if $\sum_i x_i y_i$ is zero or one. To make things simpler, assume that only Alice wants an answer to this question and communication is only possible from Bob to Alice.

a) Describe a classical strategy to decide this question.

b) Assume Alice and Bob have access to a pair of boxes defined above. Find a strategy that decides the question and uses only one bit of communication between Alice and Bob.

### Exercise 25: PR boxes II (5)

Assume Alice has two bits that she wants to communicate to Bob, however she is only allowed to send a single classical bit of information. Clearly, it is not possible for her to communicate two bits of information by just sending one bit.
Things become more interesting if they try to do the following: Alice has her two bits $x_0, x_1$ and she can send a single bit $m$ to Bob. Although Bob cannot recover both bits communicated by Alice he could try to recover only one bit with certainty, but the decision which bit he wants to recover he can make even after Alice has send her single bit $m$. Clearly, this is not possible classically (and also not quantum mechanically), this is called information causality. Surprisingly, the task can be completed if they share a PR box defined above.
Assume Alice inputs $x = x_0 \oplus x_1$ into her part of the PR box and is allowed to send one bit of information to Bob. Describe a strategy in which Bob can succeed in learning one of the bits $x_0$ or $x_1$ with certainty, even if he decides after Alice send her bit which one he wants to learn about.