FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

SS 2025
11.06.2025

10. Übungsblatt zur Vorlesung Quanten-Computing

Aufgabe 1

Es wird folgendes Spiel betrachtet:

Alice und Bob sitzen in unterschiedlichen Räumen. Eine Spielrunde besteht darin, dass ihnen eine Farbe (rot oder schwarz) gezeigt wird, und sie daraufhin „c“ oder „d“ sagen sollen. Ob rot oder schwarz gezeigt wird, ist zufällig und bei Alice und Bob unabhängig voneinander. Sagen beide den gleichen Buchstaben („c“ bzw. „d“), so wird das Ergebnis mit +1 bewertet, bei unterschiedlichen Buchstaben wird das Ergebnis mit −1 bewertet.

Es werden viele Runden gespielt und die Mittelwerte $m_{\text{A:r,B:r}}$, $m_{\text{A:r,B:s}}$, $m_{\text{A:s,B:r}}$ und $m_{\text{A:s,B:s}}$ der Punktzahlen bei den vier Kombinationen („beide: rot“, „Alice: rot, Bob: schwarz“, „Alice: schwarz, Bob: rot“, „beide schwarz“) gebildet.

Ziel ist, den Wert

$$S \;=\; m_{\text{A:r,B:r}} + m_{\text{A:r,B:s}} + m_{\text{A:s,B:r}} - m_{\text{A:s,B:s}}$$

zu maximieren.

a) Welchen Wert S erhält man, wenn Alice und Bob stets „c“ wählen?

b) Welchen Wert S erhält man, wenn Alice stets „c“ wählt und Bob stets bei rot „c“ und bei schwarz „d“?

c) Welchen Wert S erhält man, wenn Alice und Bob jeweils gleichverteilt zufällig „c“ und „d“ wählen?

d) Überlegen Sie sich weitere Strategien, und berechnen Sie den entsprechenden Wert für S.

e) Welchen Wert S erhält man, wenn Alice und Bob sich verschränkte Bell-Paare $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ teilen und folgende Strategie nutzen:

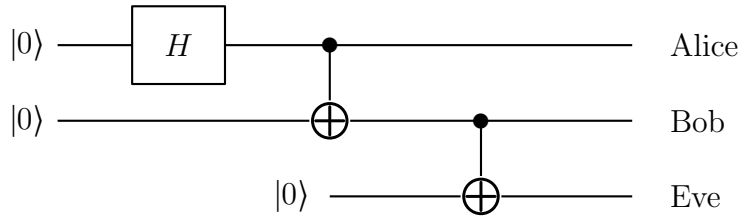
   Wenn Alice die Farbe rot gezeigt wird, misst sie ihr Qubit in der Standard-Basis, bei schwarz in einer um 45° gedrehten Basis. Wenn Bob nach rot gefragt wird, misst er sein Qubit in einer um 22.5° gedrehten Basis, bei schwarz in einer um −22.5° gedrehten Basis. Beim Messergebnis 0 wählen sie „c“, beim Ergebnis 1 „d“.

Aufgabe 2 (mit Qiskit, 4 Punkte)

Modellieren Sie das Spiel von Aufgabe 1 mit der Strategie von e) mit Qiskit und berechnen Sie simulativ den Wert von S.

Aufgabe 3

Entsprechend des Schaltkreises wird ein Bellpaar erzeugt, das an Alice und Bob verteilt wird. Eve hat sich aber mit einer entsprechenden Schaltung eingeklinkt.



a) Welcher Zustand steht am Ausgang der Schaltung?

b) Alice misst in der $\{|+\rangle, |-\rangle\}$-Basis. Mit welcher Wahrscheinlichkeit erhält sie $|+\rangle$ bzw. $|-\rangle$?

c) Wie kollabiert der Zustand, wenn Alice als Messergebnis $|+\rangle$ erhält und mit welcher Wahrscheinlichkeit erhält Bob bei einer anschließenden Messung in der $\{|+\rangle, |-\rangle\}$-Basis $|+\rangle$ bzw. $|-\rangle$?

Aufgabe 4

Betrachtet wird die gleiche Situation wie in Aufgabe 3.

Alice und Bob führen eine Überprüfung auf Verschränkung entsprechend des E91-Protokolls durch. Welchen Wert für S erhalten sie?

Aufgabe 5 (mit Qiskit, 4 Punkte)

Modellieren Sie die Situation von Aufgabe 3 mit Qiskit und berechnen Sie simulativ den Wert von S, den Alice und Bob bei einer Überprüfung auf Verschränkung entsprechend des E91-Protokolls erhalten (vgl. Aufgabe 4).

Aufgabe 6

Alice und Bob haben eine Schlüsselvereinbarung mittels des BB84- oder E91-Protokolls durchgeführt. Nach Elimination der Bits zu ungleichen Basen führen Sie eine Fehlerkorrektur und *privacy amplification* durch, indem sie zu jeweils k aufeinanderfolgenden Bits das Paritätsbit über einen öffentlichen Kanal abgleichen und nur die k-Bit-Blöcke nutzen, bei denen die Parität übereinstimmt; die eigentlichen Schlüsselbits berechnen sie dann durch eine XOR-Verknüpfung von r aufeinanderfolgenden Bits.

a) Wie sieht der Schlüssel konkret aus bei $k = 8$ und $r = 3$ und der Bitfolge (nach Elimination der Bits zu ungleichen Basen)

bei Alice: 00111010011111000111101011000011010011110

bei Bob: 00111010011111010111101010100011010011100

b) Warum ist es nicht sinnvoll $k = 2$ und $r = 2$ zu wählen?

c) Sehen Sie noch andere ungünstige Parameter-Konstellationen?

d) Wie kann man das Protokoll abändern, um die Nachteile, die bei b) oder c) entstehen, zu vermeiden?