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“.

Lösung:

a) Da Alice und Bob immer den gleichen Buchstaben wählen (z.B. immer „c“) erhalten sie immer +1 als Ergebnis, also

$$m_{\text{A:r,B:r}} = m_{\text{A:r,B:s}} = m_{\text{A:s,B:r}} = m_{\text{A:s,B:s}} = 1$$

und damit $S = 1 + 1 + 1 - 1 = 2$.

b) Es ist

$$m_{\text{A:r,B:r}} = 1, \quad m_{\text{A:r,B:s}} = -1, \quad m_{\text{A:s,B:r}} = 1 \quad \text{und} \quad m_{\text{A:s,B:s}} = -1,$$

und damit $S = 1 + (-1) + 1 - (-1) = 2$.

c) In allen Farb-Kombinationen hat man gleich wahrscheinlich Übereinstimmung und nicht-Übereinstimmung, d.h., alle Mittelwerte sind 0 und damit auch $S = 0$.

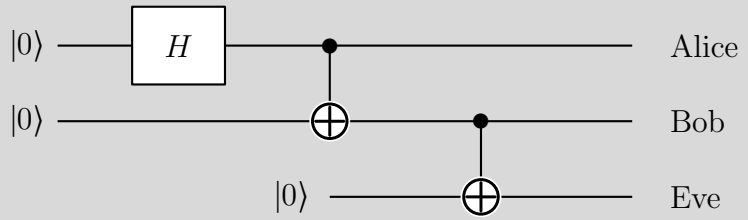
(Eigentlich müsste man hier „Erwartungswert“ statt „Mittelwert“ nehmen; die Mittelwerte approximieren die Erwartungswerte und nähern sich also mit zunehmender Rundenanzahl der Null.)

d) Es gibt viele andere Strategien, z.B., dass Alice stets „c“ und Bob stets „d“ wählt, so dass das Ergebnis stets −1 ist, also $S = (-1) + (-1) + (-1) - (-1) = -2$.

e) Dies entspricht genau der Überprüfung auf Verschränktheit beim E91-Protokoll. Wie im Skript ausgeführt, erhält man $S = 2\sqrt{2} \approx 2.82$.

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. $|-\rangle$?

Lösung:

a) Nach dem Hadamard- und CNOT-Gatter teilen sich Alice und Bob ein Bell-Paar; der gemeinsame Zustand mit Eve ist dann also

$$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \otimes |0\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|000\rangle + |110\rangle\,\big).$$

Durch das zweite CNOT-Gatter wird dies zu

$$\tfrac{1}{\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big).$$

b) Wegen $|0\rangle = \tfrac{1}{\sqrt{2}}\big(\,|+\rangle + |-\rangle\,\big)$ und $|1\rangle = \tfrac{1}{\sqrt{2}}\big(\,|+\rangle - |-\rangle\,\big)$ ist

$$\begin{aligned}
\tfrac{1}{\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big) &= \tfrac{1}{\sqrt{2}}\Big(\tfrac{1}{\sqrt{2}}\big(\,|+\rangle + |-\rangle\,\big) \otimes |00\rangle + \tfrac{1}{\sqrt{2}}\big(\,|+\rangle - |-\rangle\,\big) \otimes |11\rangle\Big) \\
&= \tfrac{1}{2}\big(\,|+00\rangle + |-00\rangle + |+11\rangle - |-11\rangle\,\big) \\
&= \tfrac{1}{2}\Big(\,|+\rangle \otimes \big(\,|00\rangle + |11\rangle\,\big) + |-\rangle \otimes \big(\,|00\rangle - |11\rangle\,\big)\Big).
\end{aligned}$$

Also wird mit gleicher Wahrscheinlichkeit $|+\rangle$ und $|-\rangle$ gemessen.

c) Entsprechend der Rechnung bei b) kollabiert der Zustand beim Messergebnis $|+\rangle$ zu

$$\begin{aligned}
|+\rangle \otimes \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) &= |+\rangle \otimes \tfrac{1}{\sqrt{2}}\Big(\tfrac{1}{\sqrt{2}}\big(\,|+\rangle + |-\rangle\,\big) \otimes |0\rangle + \tfrac{1}{\sqrt{2}}\big(\,|+\rangle - |-\rangle\,\big) \otimes |1\rangle\Big) \\
&= |+\rangle \otimes \tfrac{1}{2}\big(\,|+0\rangle + |-0\rangle + |+1\rangle - |-1\rangle\,\big) \\
&= |+\rangle \otimes \tfrac{1}{2}\Big(\,|+\rangle \otimes \big(\,|0\rangle + |1\rangle\,\big) + |-\rangle \otimes \big(\,|0\rangle - |1\rangle\,\big)\Big).
\end{aligned}$$

Bob erhält also bei einer Messung in der $\{|+\rangle, |-\rangle\}$-Basis gleich wahrscheinlich $|+\rangle$ 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?

Lösung:

Entsprechend Aufgabe 3a) hat man den Zustand $\tfrac{1}{\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big)$.

1. Fall: Alice misst in der Standard-Basis.

   Dann erhält sie mit gleicher Wahrscheinlichkeit $|0\rangle$ bzw. $|1\rangle$, und der Zustand kollabiert zu $|000\rangle$ bzw. $|111\rangle$.

Erhält sie $|0\rangle$, und misst Bob den kollabierten Zustand $|000\rangle$ in einer um $\pm 22.5°$ gedrehten Basis $\{|\phi_0\rangle, |\phi_1\rangle\}$, so erhält er $|\phi_0\rangle$ (also übereinstimmende Messergebnisse) mit der Wahrscheinlichkeit $\cos^2(22.5°)$, unterschiedliche Messergebnisse also mit der Wahrscheinlichkeit $\sin^2(22.5°)$

Entsprechend gilt dies, wenn Alice $|1\rangle$ misst.

Also ist

$$\text{E(A=0° und B=}\pm 22.5°) \;=\; \cos^2(22.5°) - \sin^2(22.5°) \;=\; \tfrac{1}{\sqrt{2}}.$$

2. Fall: Alice misst in der um 45° gedrehten Basis.

Dies entspricht einer Messung in der $\{|+\rangle, |-\rangle\}$-Basis.

Bei dem Messergebnis $|+\rangle$ kollabiert der Zustand wie in Aufgabe 3c) berechnet so, dass sich anschließend Bob und Eve die Qubits eines Bell-Paars $\big(|00\rangle + |11\rangle\big)$ teilen. Dies ist vollständig korreliert in allen Basen, und Messungen bei Bob in allen Basen ergeben gleich wahrscheinlich die beiden möglichen Messergebnisse.

Bei dem Messergebnis $|-\rangle$ kollabiert der Zustand – wie man an der Darstellung in Aufgabe 3b) sehen kann – so, dass sich anschließend Bob und Eve die Qubits eines Bell-Paars $\frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$ teilen. Auch hier ergeben Messungen bei Bob in allen Basen gleich wahrscheinlich die beiden möglichen Messergebnisse, denn wendet man auf das erste Qubit eine Drehung $\left(\begin{smallmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{smallmatrix}\right)$ an, erhält man

$$\begin{aligned}\frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) \;&=\; \frac{1}{\sqrt{2}}\Big(\big(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle\big)\otimes|0\rangle \\ &\qquad - \big(-\sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle\big)\otimes|1\rangle\Big) \\ &=\; \frac{1}{\sqrt{2}}\big(\cos\alpha\,|00\rangle + \sin\alpha\,|10\rangle + \sin\alpha\,|01\rangle - \cos\alpha\,|11\rangle\big),\end{aligned}$$

woran man sieht, dass $|0\rangle$ und $|1\rangle$ im ersten Qubit jeweils mit der Wahrscheinlichkeit $\big(\frac{1}{\sqrt{2}}\big)^2(\cos^2\alpha + \sin^2\alpha) = \frac{1}{2}$ gemessen werden.

Da Bob also bei jedem Winkel alle Ergebnisse gleich wahrscheinlich erhält, ist

$$\text{E(A=45° und B=}\pm 22.5°) \;=\; 0.$$

Insgesamt ist also

$$\begin{aligned}S \;&=\; \text{E(A=0° und B=22.5°)} + \text{E(A=0° und B=}-22.5°) \\ &\qquad + \text{E(A=45° und B=22.5°)} - \text{E(A=45° und B=}-22.5°) \\ &=\; \tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}} + 0 + 0 \;=\; 2\cdot\tfrac{1}{\sqrt{2}} \;=\; \sqrt{2}.\end{aligned}$$

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: 00111010011111000111101011000011010011 10

bei Bob: 00111010011111010111101010100011010011 00

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?

Lösung:

a) Eine Zerlegung in 8er Blöcken führt zu

bei Alice: 00111010 01111100 01111010 11000011 01001110

bei Bob: 00111010 01111101 01111010 10100011 01001100

Die entsprechenden Paritäten sind

bei Alice: 0 1 1 0 0

bei Bob: 0 0 1 0 1

Also werden der zweite und fünfte Block verworfen.

Die resultierenden Bits in 3-erBlöcken sind

bei Alice: 001 110 100 111 101 011 000 011

bei Bob: 001 110 100 111 101 010 100 011

Die entsprechenden XOR-Verknüpfungen ergeben

bei Alice: 1 0 1 1 0 0 0 0

bei Bob: 1 0 1 1 0 1 1 0

b) Die über den öffentlichen Kanal abgegelichene Parität ist dann genau das, was als Schlüssel genutzt wird.

c) Wenn r ein Teiler von k ist, also mit einem s gilt $k = s \cdot r$, dann ist die XOR-Verknüpfung von s Schlüsselbits genau die Parität des entsprechenden Blocks. Wenn Eve den Paritätsabgleich mitgehört hat, kann sie also aus $s-1$ Schlüsselbits das letzte Schlüsselbit berechnen und erhält damit teilweise Kenntnis über den Schlüssel.

   Diesen Informationsgewinn für Eve gibt es auch bei beliebiger Wahl von k und r: Die k-fache XOR-Verknüpfung von Schlüsselbits ist gleich der $(r \cdot k)$-fachen XOR-Verknüpfung der Bits aus nicht verworfenen Blöcken und damit gleich der XOR-Verknüpfung der Parität von r Blöcken.

d) Lässt man in jedem Block *ein* Bit für die Schlüsselbit-Berechnung außer Acht, z.B. dass man für $k = 2$ nur jeweils das zweite Bit eines 2er-Blocks für die Schlüsselbit-Berechnung nutzt, so kann man die oben genannten Nachteile vermeiden.