Komplexitätstheorie

Sommersemester 2019

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 9

Ausgabe: 24.06.2019
Abgabe: 01.07.2019

Auf diesem Blatt können Sie sich 6 Bonuspunkte verdienen.

Aufgabe 9.1 *Quantenkryptographie* (3 + 6 = 9 Punkte)

Alice und Bob wollen einen (klassischen) Schlüssel austauschen und verwenden dazu ein Quanten-Protokoll. Betrachte dazu die folgenden vier 1-Qubit-Zustände aus $\mathbb{C}^2$:

$$|\text{east}\rangle := |0\rangle, \quad |\text{north}\rangle := |1\rangle, \quad |\text{ne}\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \quad \text{und} \quad |\text{nw}\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$$

Wir nennen die von $\{|\text{east}\rangle, |\text{north}\rangle\}$ aufgespannte Basis[1] die +-Basis und $\{|\text{ne}\rangle, |\text{nw}\rangle\}$ die ×-Basis. Für eine Basis $B = \{|b_1\rangle, |b_2\rangle\}$ definiere die Observable $P_B = |b_1\rangle\langle b_1| + |b_2\rangle\langle b_2|$. Das Protokoll läuft wie folgt ab.

- Für $i = 1, \ldots, n$ wiederhole:
  - Alice wirft eine private Münze und wählt mit jeweils gleicher Wahrscheinlichkeit die +-Basis oder die ×-Basis.
  - Alice wirft eine private Münze und wählt mit jeweils gleicher Wahrscheinlichkeit einen der Basisvektoren $|b\rangle$ aus der zuvor gewählten Basis und schickt das Qubit $|q\rangle = |b\rangle$ an Bob.
  - Bob wirft eine private Münze und wählt mit jeweils gleicher Wahrscheinlichkeit die +-Basis oder die ×-Basis und misst das empfangene Qubit $|q\rangle$ in der gewählten Basis.
- Alice veröffentlicht über einen klassischen Kanal, welche Basis sie in Schritt i für $i = 1, \ldots, n$ gewählt hat. Bob tut das gleiche.
- Für alle Schritte i, in denen die Alice' und Bobs Basis nicht übereinstimmen, werden die gesendeten und empfangenen Qubits verworfen. Die verbleibenden Bits bilden den gemeinsamen Schlüssel, wobei wir z. B. $|\text{east}\rangle$ und $|\text{ne}\rangle$ als 0 und $|\text{north}\rangle$ und $|\text{nw}\rangle$ als 1 interpretieren können.

a) Angenommen, Alice und Bob haben in Schritt i dieselbe Basis gewählt, Alice hat das Qubit $|q\rangle$ gesendet und Bobs Messergebnis ist $\hat{q}$. Zeigen Sie: $|q\rangle = |\hat{q}\rangle$ gilt mit Wahrscheinlichkeit 1.

b) Wir betrachten nun einen Angreifer Dave, der Qubits von Alice abfängt. Betrachte einen Schritt i. Dave kennt Alice' Basis nicht, darum wählt sie unabhängig von Alice eine Basis $B = \{|b_1\rangle, |b_2\rangle\}$ und misst darin das von Alice gesendet Qubit $|q\rangle$. Angenommen, die Messung ergab b_1. Durch die Messung kollabiert der Zustand $|q\rangle$ auf den Zustand $|q'\rangle := \frac{|b_1\rangle\langle b_1|q\rangle}{\||b_1\rangle\langle b_1|q\rangle\|} = |b_1\rangle$ (Born-Regel). Dave leitet $|q'\rangle$ an Bob weiter, Alice' ursprüngliche Nachricht $|q\rangle$ ist zerstört.

   Sei $\hat{q}'$ das Messergebnis von Bob. Angenommen, Alice und Bob haben dieselbe Basis gewählt. Zeigen Sie: Egal welche Basis Dave wählt, mit Wahrscheinlichkeit mindestens 1/4 gilt $|q\rangle \neq |\hat{q}'\rangle$.

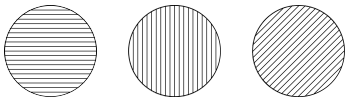
   Fazit: Alice und Bob können ihren gemeinsamen Schlüssel stichprobenartig auf Konsistenz prüfen. Wenn Dave gelauscht hat, werden sie hochwahrscheinlich Abweichungen feststellen.

[1] Wir verwenden hier die Begriffe *Basis* und *Orthonormalbasis* synonym.

Aufgabe 9.2 *Polarisationsfilter und projektive Messungen* (2 + 2 + 5 = 9 Punkte)

Wir schicken linear polarisiertes Licht durch verschiedene Polarisationsfilter. Betrachte drei verschiedene Filter F_h, F_v und F_d:

- Der Filter F_h lässt nur *horizontal* polarisiertes Licht durch.
- Der Filter F_v lässt nur *vertikal* polarisiertes Licht durch.
- Der Filter F_d lässt nur *diagonal* (in nordwest-südost-Richtung) polarisiertes Licht durch.



F_h F_v F_d

Die Polarisationsrichtung modellieren wir durch einen 1-Qubit-Zustand über dem Hilbertraum $\mathbb{C}^2$, wobei der Zustand $|0\rangle$ der horizontalen Polarisation und $|1\rangle$ der vertikalen Polarisation entspricht. Die drei Filter lassen sich dann durch Projektionsoperatoren beschreiben:

$$F_h = |0\rangle\langle 0|, \qquad F_v = |1\rangle\langle 1|, \qquad F_d = \tfrac{1}{2}\Big(|0\rangle + |1\rangle\Big)\Big(\langle 0| + \langle 1|\Big)$$

a) Was passiert, wenn Sie die zwei Filter F_h und F_v übereinander legen? Berechnen Sie F_hF_v und dessen Norm $\|F_hF_v\|$ und interpretieren Sie das Ergebnis.

b) Was passiert, wenn Sie die drei Filter F_h, F_d und F_v übereinander legen? Berechnen Sie $F_hF_dF_v$ und dessen Norm $\|F_hF_dF_v\|$ und interpretieren Sie das Ergebnis.

c) Nehmen Sie an, dass weitere Filter zur Verfügung stehen. Für einen Winkel $\alpha \in [0, \pi/2]$ sei

$$|\alpha\rangle := \cos(\alpha)\,|0\rangle + \sin(\alpha)\,|1\rangle \quad \text{und} \quad F_\alpha := |\alpha\rangle\langle\alpha|.$$

Für $k \in \mathbb{N}$ und alle $j = 0, 1, \ldots, k$ sei $\alpha_j = \frac{j}{k} \cdot \frac{\pi}{2}$. Was passiert, wenn Sie die $k+1$ Filter F_{α_0}, F_{α_1}, …, F_{α_k} übereinander legen? Berechnen Sie $\mathcal{F}_k := \prod_{i=0}^{k} F_{\alpha_i}$ und interpretieren Sie das Ergebnis für den Grenzwert $k \to \infty$.

Hinweis: Bestimmen Sie zunächst $\langle\beta|\gamma\rangle$ für beliebige Winkel $\beta, \gamma \in [0, \pi/2]$. Für kleine x können Sie $\cos(x)$ durch seine Taylorreihe approximieren: $\cos(x) \approx 1 - x^2/2$.

Aufgabe 9.3 *Verschränkte Zustände* (4 + 8 = 12 Punkte)

Wir betrachten das folgende kooperative Spiel: Alice erhält ein zufälliges Bit x, Bob erhält ein zufälliges Bit y. Alice gibt eine Antwort $a = a(x)$, Bob gibt eine Antwort $b = b(y)$. Die beiden gewinnen genau dann, wenn $a \oplus b = x \wedge y$ gilt.

a) Zeigen Sie: Jede deterministische Strategie hat eine Gewinnwahrscheinlichkeit von höchstens 3/4.

Kommentar: Daraus folgt, dass auch jede randomisierte Strategie eine Gewinnwahrscheinlichkeit von höchstens 3/4 besitzt. (Warum?)

Wir wenden uns nun der Quanten-Version des Spiels zu. Alice und Bob tauschen vor dem Spiel den EPR-Zustand $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ aus, Alice bekommt das erste Qubit, Bob das zweite Qubit. Nach Erhalten x und y gehen sie wie folgt vor:

- Wenn $x = 1$, dann dreht Alice das erste Qubit um 22,5° nach links.[2]
- Wenn $y = 1$, dann dreht Bob das zweite Qubit um 22,5° nach rechts.[3]
- Beide messen jeweils ihr Qubit (in der Standardbasis $\{|0\rangle, |1\rangle\}$) und antworten mit dem Messergebnis. (Es spielt keine Rolle, welcher der beiden zuerst misst.)

b) Zeigen Sie: Die Gewinnwahrscheinlichkeit in dem obigen Verfahren beträgt mindestens 4/5.

Hinweis: Unterscheiden Sie die drei Fälle $x + y = 0$, $x + y = 1$, $x + y = 2$ und berechnen Sie jeweils die erwarteten Messergebnisse von Alice und Bob.

[2] Das heißt, sie wendet den Operator $A = (R_{\pi/8} \otimes \mathrm{Id})$ an, wobei R_α der Rotationsoperator um den Winkel α mit $R_\alpha|0\rangle = |\alpha\rangle$ (vgl. Aufgabe 9.2 c) und $R_\alpha|1\rangle = |\pi/2 + \alpha\rangle$ und Id der Identitätsoperator ist.

[3] Das heißt, er wendet den Operator $B = (\mathrm{Id} \otimes R_{-\pi/8})$ an.