Komplexitätstheorie

Sommersemester 2020

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

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 8

Ausgabe: 15.06.2020
Abgabe: 22.06.2020

Die Abgabe erfolgt per E-Mail an Hannes Seiwert (`seiwert@em.uni-frankfurt.de`).

Aufgabe 8.1 *Quantenkryptographie* (4 + 8 = 12 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 $\{|\text{east}\rangle, |\text{north}\rangle\}$ die +-Basis[1] und $\{|\text{ne}\rangle, |\text{nw}\rangle\}$ die ×-Basis. Für eine Basis $B = \{|b_1\rangle, |b_2\rangle\}$ definiere die Observable P_B durch $P_B|b_1\rangle = |b_1\rangle$ und $P_B|b_2\rangle = -|b_2\rangle$. 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 bzw. 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) Betrachte nun einen Angreifer Dave, der Qubits von Alice abfängt. Betrachte einen Schritt i. Dave kennt Alice' Basis nicht, darum wählt er 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 $|q'\rangle := |b_1\rangle$ (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 8.2 *Quantenmechanische endliche Automaten* (12 Punkte)

Sei Σ ein Alphabet. Ein *quantenmechanischer endlicher Automat* (QFA) $A = (\Sigma, Q, \psi_0, F, U, \lambda)$ besitzt

- eine endliche Menge $Q = \{|1\rangle, \ldots, |n\rangle\}$ von Zuständen, die eine ONB des $\mathbb{C}^n$ bilden,
- einen Startzustand $|\psi_0\rangle \in \mathbb{C}^n$,
- eine Menge $F \subseteq Q$ von Endzuständen,
- eine Funktion U, die jeden Buchstaben $a \in \Sigma$ eine *unitäre* $n \times n$-Matrix U_a zuweist,
- und einen Schwellenwert $\lambda \in [0, 1]$.

Für jedes Wort $w = w_1 \ldots w_n \in \Sigma^*$ definiere $U(w) := U_{w_n} \cdot U_{w_{n-1}} \cdot \cdots \cdot U_{w_1}$ und die Akzeptanzwahrscheinlichkeit

$$A(w) := \sum_{f \in F} \left\| \langle f | U(w) \psi_0 \rangle \right\|^2.$$

Die akzeptierte Sprache von A ist $L(A) := \{w \in \Sigma^* : A(w) \geq \lambda\}$. Sei $\varepsilon > 0$. Der QFA A akzeptiert die Sprache $L(A)$ *mit Lücke* ε, wenn $|A(w) - \lambda| \geq \varepsilon$ für alle Wörter $w \in \Sigma^*$ gilt.

Sei p eine Primzahl und $\Sigma = \{a\}$. Betrachte die reguläre Sprache $L_p = \{a^i : i \equiv 0 \bmod p\}$.

Konstruieren Sie einen QFA mit $|Q| = 2$ Zuständen, der L_p mit Lücke $\varepsilon = \Theta(1/p)$ akzeptiert.

Kommentar: Analog zu QFAs lassen sich probabilistische endliche Automaten (PFAs) definieren. Ein PFA besitzt *stochastische* statt unitäre Matrizen, eine Start*verteilung* anstelle eines Startzustandes und berechnet die Akzeptanzwahrscheinlichkeit in der 1-*Norm* anstelle der euklidischen Norm. Man kann zeigen: Jeder PFA, der L_p mit Lücke $\varepsilon > 0$ akzeptiert, besitzt mindestens p Zustände.