

Inhaltsverzeichnis

1	Mathematische Grundlagen	3
1.1	Hilberträume	3
1.2	Automorphismen	8
1.3	Diskrete Wahrscheinlichkeitsräume	10
2	Multi-q-Bits und Funktionen	12
2.1	q-Bits und Multi-q-Bits	12
2.2	Gates	15
2.3	n-stellige Boolesche Funktionen	17
2.4	Messungen	19
2.5	q-Algorithmen	20
	Literaturverzeichnis	24

Kapitel 1

Mathematische Grundlagen

1.1 Hilberträume

Ausgangspunkt der Betrachtungen dieses Abschnitts sind die Begriffe „Gruppe“, „Körper“ und „Vektorraum“, die wir kurz rekapitulieren.

Definition 1.1 ((abelsche) Gruppe) Eine nichtleere Menge G zusammen mit einer Verknüpfung $\otimes : G \times G \rightarrow G$ wird als Gruppe $(G, \otimes)$ bezeichnet, falls die folgenden Bedingungen erfüllt sind:

(G1) Für alle $a, b, c \in G$ gilt das Assoziativgesetz:

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c.$$

(G2) Es gibt ein $e \in G$ (neutrales Element genannt) mit den folgenden Eigenschaften:

1. $e \otimes a = a \otimes e = a$ für alle $a \in G$.
2. Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a \otimes a' = a' \otimes a = e$.
(a' heißt inverses Element von a)

Gilt zudem das Kommutativgesetz

$$a \otimes b = b \otimes a$$

für alle $a, b \in G$, so heißt die Gruppe $(G, \otimes)$ abelsch.

Es ist einfach zu zeigen, dass das neutrale Element in einer Gruppe immer eindeutig ist.

Der nun zu definierende Begriff „Körper“ baut unmittelbar auf dem Gruppenbegriff auf.

Definition 1.2 (Körper) Eine nichtleere Menge $\mathbb{K}$ zusammen mit zwei Verknüpfungen

$$\begin{aligned}\oplus &: \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}, \\ \odot &: \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}\end{aligned}$$

wird als Körper $(\mathbb{K}, \oplus, \odot)$ bezeichnet, falls die folgenden Bedingungen erfüllt sind:

- (K1) $(\mathbb{K}, \oplus)$ ist eine abelsche Gruppe.
- (K2) $(\mathbb{K} \setminus \{0\}, \odot)$ ist eine abelsche Gruppe, wobei 0 das neutrale Element bezüglich $\oplus$ bezeichnet.
- (K3) Für alle $a, b, c \in \mathbb{K}$ gilt das Distributivgesetz:

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c).$$

Da in einem Körper $(\mathbb{K}, \oplus, \odot)$ für alle $a, b, c \in \mathbb{K}$ gilt:

$$a \odot c = a \odot (0 \oplus c) = (a \odot 0) \oplus (a \odot c),$$

folgt für alle $a \in \mathbb{K}$ aus der Eindeutigkeit des neutralen Elements bezüglich $\oplus$:

$$a \odot 0 = 0.$$

Daher muß in (K2) das neutrale Element bezüglich $\oplus$ ausgeschlossen werden (ansonsten hätte dieses neutrale Element bezüglich $\odot$ kein inverses Element).

Beispiele:

- Die rationalen Zahlen $(\mathbb{Q}, +, \cdot)$ und die reellen Zahlen $(\mathbb{R}, +, \cdot)$ sind Körper.
- Die Menge $\mathbb{C} := \mathbb{R}^2 := \{(a, b); a, b \in \mathbb{R}\}$ bildet mit den Verknüpfungen

$$\begin{aligned}+ &: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}, (a, b) + (a', b') = (a + a', b + b'), \\ \cdot &: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}, (a, b) \cdot (a', b') = (aa' - bb', ab' + a'b)\end{aligned}$$

einen Körper $(\mathbb{C}, +, \cdot)$.

Definiert man in diesem Körper $i := (0, 1)$ (i heißt imaginäre Einheit), so kann man die komplexen Zahlen folgendermaßen darstellen:

$$(a, b) = (a, 0) + (0, b) = a + bi,$$

da die Menge $\{(a, 0); a \in \mathbb{R}\}$ die Menge der reellen Zahlen repräsentiert. Ferner ergibt sich $i^2 = -1$. Für eine komplexe Zahl $z = (a, b) = a + bi$ heißt die reelle Zahl a Realteil von z und die reelle Zahl b heißt Imaginärteil von z .

Die komplexe Zahl $\bar{z} := (a, -b) = a - bi$ wird als die zu z konjugiert komplexe Zahl bezeichnet. Ferner führt man durch $|z| := \sqrt{a^2 + b^2}$ den Betrag von z ein. Gilt $|z| = 1$ für eine komplexe Zahl z , so gibt es ein eindeutiges $\phi \in [0, 2\pi[$ mit

$$z = \cos(\phi) + \sin(\phi)i =: e^{i\phi}.$$

Somit kann jede beliebige komplexe Zahl z in Polarkoordinaten $z = |z| \cdot e^{i\phi}$ dargestellt werden.

In den verschiedensten Teilgebieten der Mathematik betrachtet man immer wieder Mengen, deren Elemente einerseits durch eine Addition verknüpft sind, andererseits mit einem Zahlenfaktor multipliziert werden können. Solche Mengen werden wir im folgenden als Vektorräume bezeichnen.

Definition 1.3 (Vektorraum) Sei $(\mathbb{K}, \oplus, \odot)$ ein Körper. Eine nichtleere Menge V zusammen mit zwei Verknüpfungen

$$\begin{aligned} \dot{+} &: V \times V \rightarrow V, \\ * &: \mathbb{K} \times V \rightarrow V \end{aligned}$$

wird als Vektorraum $(V, \dot{+}, *)$ über $\mathbb{K}$ bezeichnet, falls die folgenden Bedingungen erfüllt sind:

(V1) $(V, \dot{+})$ ist eine abelsche Gruppe.

(V2) Für alle $\lambda, \mu \in \mathbb{K}$ und $v, w \in V$ gilt:

$$\begin{aligned} (\lambda \oplus \mu) * v &= (\lambda * v) \dot{+} (\mu * v) \\ \lambda * (v \dot{+} w) &= (\lambda * v) \dot{+} (\lambda * w) \\ \lambda * (\mu * v) &= (\lambda \odot \mu) * v \\ 1 * v &= v, \end{aligned}$$

wobei 1 das neutrale Element von $\mathbb{K}$ bezüglich $\odot$ bezeichnet.

Beispiele:

- Sei $(\mathbb{K}, \oplus, \odot)$ ein Körper, so ist für jedes $n \in \mathbb{N}$ die Menge

$$\mathbb{K}^n := \{(x_1, \dots, x_n); x_i \in \mathbb{K}, i = 1, \dots, n\}$$

mit den Verknüpfungen

$$\begin{aligned} \dot{+} &: \mathbb{K}^n \times \mathbb{K}^n \rightarrow \mathbb{K}^n, (x_1, \dots, x_n) \dot{+} (y_1, \dots, y_n) = (x_1 \oplus y_1, \dots, x_n \oplus y_n) \\ * &: \mathbb{K} \times \mathbb{K}^n \rightarrow \mathbb{K}^n, \lambda * (x_1, \dots, x_n) = (\lambda \odot x_1, \dots, \lambda \odot x_n) \end{aligned}$$

ein Vektorraum über $\mathbb{K}$.

- Der Körper $(\mathbb{C}, +, \cdot)$ ist durch

$$+ : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}, z + w = z + w$$

$$* : \mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}, \lambda * (a + bi) = (\lambda \cdot a) + (\lambda \cdot b)i$$

ein Vektorraum über $\mathbb{R}$.

Da Vektorräume insbesondere in der Geometrie eine wichtige Rolle spielen, sucht man nach Möglichkeiten, um die Länge von Vektoren (also von Elementen eines Vektorraumes) und den Winkel zwischen Vektoren messen zu können. Dies führt für $\mathbb{K} = \mathbb{R}$ beziehungsweise $\mathbb{K} = \mathbb{C}$ auf den Begriff des Skalarprodukts.

Definition 1.4 (Skalarprodukt, Norm, Winkel, Prähilbertraum) Sei $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ und $(V, +, *)$ ein Vektorraum über $\mathbb{K}$. Eine Abbildung

$$\langle \bullet, \bullet \rangle : V \times V \rightarrow \mathbb{K}, \quad (u, v) \mapsto \langle u, v \rangle$$

heißt Skalarprodukt, falls für alle $u, v, w \in V$ und alle $\lambda \in \mathbb{K}$ gilt:

$$(\text{SP1}) \quad \langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle,$$

$$(\text{SP2}) \quad \langle \lambda * u, v \rangle = \lambda \cdot \langle u, v \rangle,$$

$$(\text{SP3}) \quad \langle u, v \rangle = \overline{\langle v, u \rangle},$$

$$(\text{SP4}) \quad \langle u, u \rangle > 0 \text{ für alle } u \neq \vec{0} \text{ (}\vec{0} \text{ ist neutrales Element bezüglich } \oplus \text{)}.$$

Die Abbildung

$$\| \bullet \| : V \rightarrow \mathbb{R}_0^+, u \mapsto \sqrt[+]{\langle u, u \rangle}$$

heißt Norm und $\|u\|$ wird als Länge von u bezeichnet. Für zwei Vektoren $u, v \in V$ mit $\|u\| > 0$ und $\|v\| > 0$ wird mit $\theta \in [0, \pi]$ gegeben durch

$$\cos(\theta) = \frac{\operatorname{Re}(\langle u, v \rangle)}{\|u\| \cdot \|v\|}$$

der Winkel zwischen u und v festgelegt.

Ist $\theta = \frac{\pi}{2}$ (also $\langle u, v \rangle = 0$), so heißen u und v orthogonal.

Ein Vektorraum $(V, +, *, \langle \bullet, \bullet \rangle)$ über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ zusammen mit einem Skalarprodukt $\langle \bullet, \bullet \rangle$ heißt Prähilbertraum.

Beispiele:

- Für den Vektorraum $(\mathbb{R}^n, +, *)$, $n \in \mathbb{N}$, über $\mathbb{R}$ ist durch

$$\langle \bullet, \bullet \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}, \quad (u, v) \mapsto \sum_{i=1}^n u_i v_i$$

ein Skalarprodukt definiert.

- Für den Vektorraum $(\mathbb{C}^n, \dot{+}, *)$, $n \in \mathbb{N}$, über $\mathbb{C}$ ist durch

$$\langle \bullet, \bullet \rangle : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}, \quad (u, v) \mapsto \sum_{i=1}^n u_i \overline{v_i}$$

ein Skalarprodukt definiert.

Betrachten wir eine spezielle Folge $\{q_i\}_{i \in \mathbb{N}}$ rationaler Zahlen, die folgendermaßen definiert ist: Ausgehend von der irrationalen Zahl $\sqrt{2} = 1.414213\dots$ ergibt sich q_i durch Abhacken der Dezimaldarstellung von $\sqrt{2}$ nach der i -ten Stelle. Also gilt:

$$q_1 = 1 \quad q_2 = 1.4 \quad q_3 = 1.41 \quad q_4 = 1.414 \quad \text{usw.}$$

Offensichtlich gilt:

$$\lim_{i \rightarrow \infty} |q_i - \sqrt{2}| = 0$$

und somit konvergiert die Folge $\{q_i\}_{i \in \mathbb{N}}$ rationaler Zahlen gegen eine irrationale Zahl $\sqrt{2} \notin \mathbb{Q}$.

Allgemein heißt eine Folge $\{v_i\}_{i \in \mathbb{N}}$ von Vektoren eines Prähilbertraumes $(V, \dot{+}, *, \langle \bullet, \bullet \rangle)$ Cauchy-Folge, falls es zu jedem $\epsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt mit

$$\|v_n - v_m\| < \epsilon \quad \text{für alle } n, m > n_0 \quad (\text{Cauchy-Kriterium}),$$

wobei „ $v_n - v_m$ “ eine Abkürzung für „ $v_n \dot{+} (-v_m)$ “ darstellt und $-v_m$ das inverse Element von v_m bezüglich $\dot{+}$ bezeichnet. Jede konvergente Folge ist eine Cauchy-Folge. Ein Prähilbertraum heißt Hilbertraum, falls jede Cauchy-Folge gegen ein Element des Raumes konvergiert.

Beispiele:

- Sei $C[a, b]$ die Menge aller stetigen Funktionen $f : [a, b] \rightarrow \mathbb{R}$ und sei $\mathbb{K} = \mathbb{R}$. Mit den Verknüpfungen

$$\begin{aligned} \dot{+} & : C[a, b] \times C[a, b] \rightarrow C[a, b], \quad (f \dot{+} g)(x) := f(x) + g(x) \\ * & : \mathbb{R} \times C[a, b] \rightarrow C[a, b], \quad (\lambda * f)(x) := \lambda \cdot f(x) \end{aligned}$$

ist $(C[a, b], \dot{+}, *)$ ein Vektorraum über $\mathbb{R}$.

Durch

$$\langle \bullet, \bullet \rangle : C[a, b] \times C[a, b] \rightarrow \mathbb{R}, \quad (f, g) \mapsto \int_a^b f(x)g(x)dx$$

wird $(C[a, b], \dot{+}, *, \langle \bullet, \bullet \rangle)$ ein Prähilbertraum.

- Der Vektorraum $(\mathbb{R}^n, \dot{+}, *)$, $n \in \mathbb{N}$, über $\mathbb{R}$ ist mit dem Skalarprodukt

$$\langle \bullet, \bullet \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}, \quad (u, v) \mapsto \sum_{i=1}^n u_i v_i$$

ein Hilbertraum.

Aus der Geometrie ist der Begriff der linearen Unabhängigkeit von Vektoren geläufig. Diesen Begriff können wir nun auf allgemeine Vektorräume übertragen.

Definition 1.5 (linear (un)abhängig) Sei $(V, \dot{+}, *)$ ein Vektorraum über $\mathbb{K}$. Eine Menge $v_1, \dots, v_k \in V$ von Vektoren heißt linear unabhängig, falls für $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ aus der Gleichung

$$(\lambda_1 * v_1) \dot{+} \dots \dot{+} (\lambda_k * v_k) = \vec{0} \quad (\vec{0} \text{ ist neutrales Element bezüglich } \dot{+})$$

folgt:

$$\lambda_1 = \dots = \lambda_k = 0 \quad (0 \text{ ist neutrales Element bezüglich } \oplus).$$

Ansonsten heißen die Vektoren $v_1, \dots, v_k$ linear abhängig.

Wichtig sind nun Vektorräume, für die es eine maximale Anzahl linear unabhängiger Vektoren gibt.

Definition 1.6 (Dimension, (orthonormale) Basis) Sei $(V, \dot{+}, *)$ ein Vektorraum über $\mathbb{K}$ und sei $\{v_1, \dots, v_d\}$, $d \in \mathbb{N}$, eine Menge linear unabhängiger Vektoren aus V mit

$$V = \{(\lambda_1 * v_1) \dot{+} \dots \dot{+} (\lambda_d * v_d); \lambda_1, \dots, \lambda_d \in \mathbb{K}\},$$

so heißt die natürliche Zahl d die Dimension von V und die Menge $\{v_1, \dots, v_d\}$ wird als Basis von V bezeichnet. Ist V ein Prähilbertraum mit

$$\langle v_i, v_j \rangle = \begin{cases} 0 & \text{falls } i \neq j \\ 1 & \text{falls } i = j \end{cases}, \quad i, j = 1, \dots, d,$$

so heißt $\{v_1, \dots, v_d\}$ orthonormale Basis von V .

Beispiele:

- Für $\mathbb{R}^n$ über $\mathbb{R}$ mit dem bereits betrachteten Skalarprodukt ist die Dimension gleich n und $\{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$ ist eine orthonormale Basis.
- Für $\mathbb{C}^n$ über $\mathbb{R}$ ist die Dimension gleich $2n$ und

$$\{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1), (i, 0, \dots, 0), \dots, (0, \dots, 0, i)\}$$

ist eine Basis.

1.2 Automorphismen

In diesem Abschnitt betrachten wir lineare Abbildungen, die einen Vektorraum auf sich selbst abbilden.

Definition 1.7 (lineare Abbildung, Automorphismus) Sei $(V, \dot{+}, *)$ ein Vektorraum über $\mathbb{K}$ und sei $f : V \rightarrow V$ eine Abbildung mit

$$(LA1) \quad f(u \dot{+} v) = f(u) \dot{+} f(v) \quad \text{für alle } u, v \in V,$$

$$(LA2) \quad f(\lambda * u) = \lambda * f(u) \quad \text{für alle } u \in V, \lambda \in \mathbb{K},$$

so heißt die Abbildung f linear. Ist zudem f bijektiv, so wird f als Automorphismus bezeichnet.

Es gibt eine wichtige Verbindung zwischen Automorphismen und Matrizen, die wir im folgenden skizzieren.

Sei $(V, \dot{+}, *)$ ein Vektorraum über $\mathbb{K}$ der Dimension $d \in \mathbb{N}$ und sei $\{v_1, \dots, v_d\}$ eine Basis von V , so kann jeder Vektor $v \in V$ wegen der Darstellung

$$v = (\lambda_1 * v_1) \dot{+} \dots \dot{+} (\lambda_d * v_d)$$

durch $(\lambda_1, \dots, \lambda_d) \in \mathbb{K}^d$ repräsentiert werden. Sei nun $f : V \rightarrow V$ eine lineare Abbildung, so gilt:

$$f((\lambda_1 * v_1) \dot{+} \dots \dot{+} (\lambda_d * v_d)) = (\lambda_1 * f(v_1)) \dot{+} \dots \dot{+} (\lambda_d * f(v_d)).$$

Stellen wir nun die Vektoren $f(v_1), \dots, f(v_d)$ wieder mit

$$f(v_i) = (\mu_{1,i} * v_1) \dot{+} \dots \dot{+} (\mu_{d,i} * v_d), \quad i = 1, \dots, d$$

durch $(\mu_{1,1}, \dots, \mu_{1,d}), \dots, (\mu_{d,1}, \dots, \mu_{d,d}) \in \mathbb{K}^d$ dar, so können wir die lineare Abbildung f durch die Matrix

$$\mathbf{M}_f = \begin{pmatrix} \mu_{1,1} & \cdots & \mu_{1,d} \\ \vdots & \ddots & \vdots \\ \mu_{d,1} & \cdots & \mu_{d,d} \end{pmatrix} \in \mathbb{K}^{d,d}$$

repräsentieren. Diese Darstellung hängt natürlich von der Wahl der Basis ab. Für

$$\begin{aligned} v &= (\lambda_1 * v_1) \dot{+} \dots \dot{+} (\lambda_d * v_d) \\ f(v_1) &= (\mu_{1,1} * v_1) \dot{+} \dots \dot{+} (\mu_{d,1} * v_d) \\ &\vdots \\ f(v_d) &= (\mu_{1,d} * v_1) \dot{+} \dots \dot{+} (\mu_{d,d} * v_d) \end{aligned}$$

gilt dann:

$$f(v) = (\alpha_1 * v_1) \dot{+} \dots \dot{+} (\alpha_d * v_d)$$

mit:

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} = \begin{pmatrix} \mu_{1,1} & \cdots & \mu_{1,d} \\ \vdots & \ddots & \vdots \\ \mu_{d,1} & \cdots & \mu_{d,d} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix}.$$

Ist f ein Automorphismus, so ist $\mathbf{M}_f$ regulär.

1.3 Diskrete Wahrscheinlichkeitsräume

In der Wahrscheinlichkeitstheorie werden Methoden zur Beschreibung und Analyse von Zufallsexperimenten (Experimente mit nicht vorhersehbarem Ausgang) bereitgestellt. Der umgangssprachliche Begriff 'Zufallsexperiment' wird durch den Begriff 'Wahrscheinlichkeitsraum' mathematisch präzisiert. Wir benötigen für das Folgende nur diskrete Wahrscheinlichkeitsräume und definieren daher:

Definition 1.8 (diskreter Wahrscheinlichkeitsraum) Sei Ω eine nichtleere Menge mit endlich vielen Elementen, $\mathcal{P}(\Omega)$ die Menge aller Teilmengen von Ω (Potenzmenge) und $P : \mathcal{P}(\Omega) \rightarrow \mathbb{R}$ eine Abbildung mit:

(M1) $P(A) \geq 0$ für alle $A \in \mathcal{P}(\Omega)$

(M2) $P(\emptyset) = 0, \quad P(\Omega) = 1$

(M3) Für jede Folge $A_1, A_2, \dots, A_n, n \in \mathbb{N}$, paarweise disjunkter Mengen mit $A_i \in \mathcal{P}(\Omega), n \in \mathbb{N}$, gilt:

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i),$$

so wird $(\Omega, \mathcal{P}(\Omega), P)$ als diskreter Wahrscheinlichkeitsraum bezeichnet. Die Punkte $\omega \in \Omega$ heißen Ergebnisse, die Mengen $A \in \mathcal{P}(\Omega)$ Ereignisse. Die Funktion P wird als Wahrscheinlichkeitsmaß bezeichnet. Für alle Ereignisse A wird $P(A)$ die Wahrscheinlichkeit von A genannt.

Wir werden im folgenden davon ausgehen, daß ein Zufallsexperiment durch einen diskreten Wahrscheinlichkeitsraum $(\Omega, \mathcal{P}(\Omega), P)$ gegeben ist. Die Elemente der Menge $\Omega = \{\omega_1, \dots, \omega_m\}$ stellen die möglichen Ergebnisse des Zufallsexperimentes dar. Das Wahrscheinlichkeitsmaß P ist durch

$$p_j := P(\{\omega_j\}), \quad j = 1, \dots, m$$

eindeutig festgelegt.

Beispiele:

- **Gleichverteilung und Laplace-Experiment**

Ist

$$p_j = \frac{1}{m}, \quad \text{für } j = 1, \dots, m,$$

so wird dieses Wahrscheinlichkeitsmaß Gleichverteilung genannt. Ein Zufallsexperiment, das durch einen Wahrscheinlichkeitsraum mit Gleichverteilung repräsentiert wird, heißt nach P. S. de Laplace (1749-1827) Laplace-Experiment.

- **Binomial-Verteilung und Bernoulli-Experiment**

Wählt man $p \in \mathbb{R}$, $0 < p < 1$, und $\Omega = \{0, 1, 2, \dots, s\}$, $s \in \mathbb{N}$, so wird (mit $\binom{s}{j} := \frac{s!}{(s-j)!j!}$) das durch

$$p_j = \binom{s}{j} p^j (1-p)^{s-j} \text{ für } j = 0, \dots, s$$

gegebene Wahrscheinlichkeitsmaß Binomial-Verteilung $B(s, p)$ mit Parameter s, p genannt. Ein Zufallsexperiment, das durch einen Wahrscheinlichkeitsraum mit Binomial-Verteilung mit Parameter s, p repräsentiert wird, heißt nach J. Bernoulli (1654-1705) Bernoulli-Experiment mit Parameter s, p . Ein Bernoulli-Experiment kann folgendermaßen interpretiert werden: Man betrachtet ein Zufallsexperiment, bei dem es nur zwei mögliche Ergebnisse gibt, nämlich mit Wahrscheinlichkeit p das Ergebnis 'T' (Treffer) und mit Wahrscheinlichkeit $(1-p)$ das Ergebnis 'N' (Niete). Dieses Experiment führen wir s -mal durch, ohne daß sich die Ergebnisse gegenseitig beeinflussen. Die Wahrscheinlichkeit, daß nach diesen s Versuchen genau j Treffer auftreten, ist gegeben durch $\binom{s}{j} p^j (1-p)^{s-j}$, $0 \leq j \leq s$, $s \in \mathbb{N}$. Somit wird die s -malige Durchführung unseres Experimentes durch ein Bernoulli-Experiment beschrieben.

Sind für $m \in \mathbb{N}$ genau m nichtnegative reelle Zahlen $p_1, \dots, p_m$ mit

$$\sum_{i=1}^m p_i = 1$$

gegeben, so repräsentieren diese m reellen Zahlen ein Wahrscheinlichkeitsmaß P auf der Potenzmenge einer Menge Ω mit m Elementen.

Kapitel 2

Multi-q-Bits und Funktionen

2.1 q-Bits und Multi-q-Bits

Im Rahmen der klassischen Informationstheorie wird eine Variable $x \in B$ mit $|B| = 2$ als Bit bezeichnet. Häufig fasst man mehrere Bits zu einem Symbol $y \in B^n, n \in \mathbb{N}$, zusammen. Solch ein Symbol könnte man als Multi-Bit bezeichnen. Dieses Multi-Bit kann dann 2^n verschiedene Werte annehmen.

In der Quanteninformationstheorie betrachtet man einen Hilbertraum $\mathcal{H}$ der Dimension $d = 2$ über $\mathbb{C}$ mit Skalarprodukt $\langle \bullet, \bullet \rangle_{\mathcal{H}}$. Sei nun $\{v_1, v_2\}$ eine orthonormale Basis von $\mathcal{H}$, so wird die Menge

$$\mathcal{S}_{\mathcal{H}}^1 := \{v = (\lambda_1 * v_1) + (\lambda_2 * v_2); \lambda_1, \lambda_2 \in \mathbb{C} \text{ und } \langle v, v \rangle_{\mathcal{H}} = 1\}$$

als Sphäre von $\mathcal{H}$ bezeichnet. Es gilt für $v = (\lambda_1 * v_1) + (\lambda_2 * v_2) \in \mathcal{S}_{\mathcal{H}}^1$ wegen $\langle v, v \rangle_{\mathcal{H}} = 1$:

$$\lambda_1 \overline{\lambda_1} + \lambda_2 \overline{\lambda_2} = 1$$

($\lambda_1 \overline{\lambda_1}$ und $\lambda_2 \overline{\lambda_2}$ sind nichtnegative reelle Zahlen). In welchem Zusammenhang stehen nun klassische Bits und die Sphäre $\mathcal{S}_{\mathcal{H}}^1$? Dazu wählen wir einen Vektor $v \in \mathcal{S}_{\mathcal{H}}^1$ repräsentiert durch $(\lambda_1, \lambda_2) \in \{(z_1, z_2) \in \mathbb{C}^2; z_1 \overline{z_1} + z_2 \overline{z_2} = 1\}$ und interpretieren die Größe $\lambda_1 \overline{\lambda_1}$ als Wahrscheinlichkeit dafür, dass $v = v_1$ gilt, und die Größe $\lambda_2 \overline{\lambda_2}$ als Wahrscheinlichkeit dafür, dass $v = v_2$ gilt. Jeder Vektor $v \in \mathcal{S}_{\mathcal{H}}^1$ repräsentiert somit ein „unscharfes Bit“ mit $B = \Omega = \{v_1, v_2\}$ und $p_1 = P(\{v_1\}) = \lambda_1 \overline{\lambda_1}$ sowie $p_2 = P(\{v_2\}) = \lambda_2 \overline{\lambda_2}$.

Definition 2.1 (q-Bit) Sei $\mathcal{H}$ ein Hilbertraum der Dimension $d = 2$ über $\mathbb{C}$ und sei $\{v_1, v_2\}$ eine orthonormale Basis von $\mathcal{H}$, so wird jeder Vektor

$$v \in \mathcal{S}_{\mathcal{H}}^1 = \{(\lambda_1 * v_1) + (\lambda_2 * v_2); \lambda_1, \lambda_2 \in \mathbb{C} \text{ und } \lambda_1 \overline{\lambda_1} + \lambda_2 \overline{\lambda_2} = 1\}$$

als q-Bit bezeichnet.

Ein q-Bit (Abkürzung für Quanten-Bit) impliziert somit ein Wahrscheinlichkeitsmaß

auf der Potenzmenge einer zweielementigen Menge. Der Übergang von klassischen Bits zu „unscharfen“ q-Bits wird physikalisch durch die Unschärferelation von Heisenberg begründet; dabei werden die Grenzen der physikalischen Meßbarkeit wahrscheinlichkeits-theoretisch beschrieben und die Elemente der Sphäre $\mathcal{S}_{\mathcal{H}}^1$ entsprechen den reinen Zuständen eines quantentheoretischen Systems.

An dieser Stelle erscheint es wichtig, den Zusammenhang zwischen einem Bit und einem q-Bit klarzustellen. Ein Bit kann immer zwei verschiedene Werte annehmen, in unserem Kontext die Werte v_1 oder v_2 ; sobald ein Bit festgelegt ist, ist diese Festlegung unmittelbar erkennbar. Auch ein q-Bit kann im Prinzip nur zwei verschiedene Werte annehmen, die in den Basiselementen $\{v_1, v_2\}$ von $\mathcal{H}$ festgelegt sind. Allerdings ist der entsprechende Wert (also v_1 oder v_2) nicht unmittelbar erkennbar, sondern nur in Form einer Wahrscheinlichkeitsverteilung auf $\{v_1, v_2\}$ repräsentiert durch $(\lambda_1, \lambda_2) \in \{(z_1, z_2) \in \mathbb{C}^2; z_1 \bar{z}_1 + z_2 \bar{z}_2 = 1\}$. Um nun ein q-Bit zu einer Entscheidung zwischen v_1 und v_2 zu zwingen, muss man eine „Messung“ durchführen (cf. Abschnitt 2.4). Dieser Messung entspricht wahrscheinlichkeits-theoretisch eine Durchführung eines Zufallsexperimentes mit den möglichen Ereignissen $\Omega = \{v_1, v_2\}$ gemäß der Verteilung repräsentiert durch (λ_1, λ_2) . Interessant ist nun, dass sich die zu einem q-Bit gehörige Wahrscheinlichkeitsverteilung nach einer Messung des q-Bits verändert. Dies entspricht der physikalischen Beobachtung, dass eine Messung das betrachtete Szenario verändert. Wir werden in Abschnitt 2.4 darauf zurückkommen.

Völlig analog zum Weg vom klassischen Bit zum q-Bit gehen wir nun den Weg vom Symbol $y \in B^n$, $n \in \mathbb{N}$, zum Multi-q-Bit. Da $y \in B^n$ genau 2^n verschiedene Werte annehmen kann, benötigen wir nun einen Hilbertraum der Dimension $d = 2^n$, der für den Spezialfall $n = 1$ gerade den Hilbertraum $\mathcal{H}$ liefert. Sei also $\mathcal{H}$ unser bereits betrachteter Hilbertraum der Dimension $d = 2$ über $\mathbb{C}$ mit der orthonormalen Basis $\{v_1, v_2\}$ und dem Skalarprodukt $\langle \bullet, \bullet \rangle_{\mathcal{H}}$, so führen wir nun den folgenden Vektorraum über $\mathbb{C}$ ein:

$$\mathcal{H}^{\otimes n} := \{(u_1, \dots, u_{2^{(n-1)}}); u_i \in \mathcal{H}, i = 1, \dots, 2^{(n-1)}\},$$

wobei die in $\mathcal{H}$ definierten Verknüpfungen $\dot{+}$ und $*$ nun komponentenweise durchgeführt werden und so zu den entsprechenden Verknüpfungen auf $\mathcal{H}^{\otimes n}$ werden. Durch

$$\langle \bullet, \bullet \rangle_{\mathcal{H}^{\otimes n}} : \mathcal{H}^{\otimes n} \times \mathcal{H}^{\otimes n} \rightarrow \mathbb{C} \quad (u, w) \mapsto \sum_{i=1}^{2^{(n-1)}} \langle u_i, w_i \rangle_{\mathcal{H}}$$

wird $\mathcal{H}^{\otimes n}$ zu einem Hilbertraum über $\mathbb{C}$ mit der orthonormalen Basis

$$\{e_1, \dots, e_{2^n}\} = \{(v_1, \vec{0}, \dots, \vec{0}), \dots, (\vec{0}, \dots, \vec{0}, v_1), (v_2, \vec{0}, \dots, \vec{0}), \dots, (\vec{0}, \dots, \vec{0}, v_2)\},$$

wobei $\vec{0}$ das neutrale Element in $\mathcal{H}$ bezüglich $\dot{+}$ bezeichnet.

Mit der Sphäre

$$\mathcal{S}_{\mathcal{H}^{\otimes n}}^1 := \{e = (\lambda_1 * e_1) \dot{+} \dots \dot{+} (\lambda_{2^n} * e_{2^n}); \lambda_1, \dots, \lambda_{2^n} \in \mathbb{C} \text{ und } \langle e, e \rangle_{\mathcal{H}^{\otimes n}} = 1\}$$

können wir nun mit

$$\langle e, e \rangle_{\mathcal{H}^{\otimes n}} = \lambda_1 \bar{\lambda}_1 + \dots + \lambda_{2^n} \bar{\lambda}_{2^n}$$

Multi-q-Bits definieren.

Definition 2.2 (Multi-q-Bit) Seien $\mathcal{H}$ ein Hilbertraum der Dimension $d = 2$ über $\mathbb{C}$ mit dem Skalarprodukt $\langle \bullet, \bullet \rangle_{\mathcal{H}}$, $\{v_1, v_2\}$ eine orthonormale Basis von $\mathcal{H}$ und $n \in \mathbb{N}$. Sei ferner

$$\mathcal{H}^{\otimes n} := \{(u_1, \dots, u_{2^{(n-1)}}); u_i \in \mathcal{H}, i = 1, \dots, 2^{(n-1)}\},$$

so wird jeder Vektor

$$e \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 = \{(\lambda_1 * e_1) \dot{+}, \dots, \dot{+} (\lambda_{2^n} * e_{2^n}); \lambda_1, \dots, \lambda_{2^n} \in \mathbb{C} \text{ und } \lambda_1 \overline{\lambda_1} + \dots + \lambda_{2^n} \overline{\lambda_{2^n}} = 1\}$$

als Multi-q-Bit bezeichnet, wobei

$$\{e_1, \dots, e_{2^n}\} = \{(v_1, \vec{0}, \dots, \vec{0}), \dots, (\vec{0}, \dots, \vec{0}, v_1), (v_2, \vec{0}, \dots, \vec{0}), \dots, (\vec{0}, \dots, \vec{0}, v_2)\}$$

eine orthonormale Basis bezüglich des Skalarproduktes

$$\langle \bullet, \bullet \rangle_{\mathcal{H}^{\otimes n}} : \mathcal{H}^{\otimes n} \times \mathcal{H}^{\otimes n} \rightarrow \mathbb{C} \quad (u, w) \mapsto \sum_{i=1}^{2^{(n-1)}} \langle u_i, w_i \rangle_{\mathcal{H}}$$

darstellt.

Ein Multi-q-Bit impliziert somit ein Wahrscheinlichkeitsmaß auf der Potenzmenge der Menge

$$\Omega = \{e_1, \dots, e_{2^n}\}.$$

Dieses Wahrscheinlichkeitsmaß ist gegeben durch

$$p_i = P(\{e_i\}) = \lambda_i \overline{\lambda_i}, \quad i = 1, \dots, 2^n,$$

und ist die quantentheoretische Version eines Symbols $y \in \{v_1, v_2\}^n$.

Es gibt nun sehr viele Möglichkeiten, durch eine bijektive Abbildung

$$\zeta : \{v_1, v_2\}^n \rightarrow \{e_1, \dots, e_{2^n}\}$$

jedem Symbol $y \in \{v_1, v_2\}^n$ ein Basiselement e_i zuzuordnen. Wir wollen nun eine Abbildung ζ festlegen. Ersetzt man dazu v_1 durch die Zahl „0“ und v_2 durch die Zahl „1“, so ist jedem $y \in \{v_1, v_2\}^n$ durch Interpretation als Binärzahl eine natürliche Zahl

$$n(y) \in \{0, \dots, 2^n - 1\}$$

etwa folgendermaßen zugeordnet:

$$y = (v_{i_1}, \dots, v_{i_n}) \mapsto n(y) = \sum_{j=1}^n (i_j - 1) 2^{j-1}, \quad i_j \in \{1, 2\}.$$

Wir wählen für ζ :

$$\zeta : \{v_1, v_2\}^n \rightarrow \{e_1, \dots, e_{2^n}\}, \quad y \mapsto e_{n(y)+1}.$$

Beispiel: $n = 3$

Symbol $y \in \{v_1, v_2\}^3$	$n(y)$	Basiselement
(v_1, v_1, v_1)	$000 \hat{=} 0$	e_1
(v_2, v_1, v_1)	$100 \hat{=} 1$	e_2
(v_1, v_2, v_1)	$010 \hat{=} 2$	e_3
(v_2, v_2, v_1)	$110 \hat{=} 3$	e_4
(v_1, v_1, v_2)	$001 \hat{=} 4$	e_5
(v_2, v_1, v_2)	$101 \hat{=} 5$	e_6
(v_1, v_2, v_2)	$011 \hat{=} 6$	e_7
(v_2, v_2, v_2)	$111 \hat{=} 7$	e_8

2.2 Gates

In diesem Abschnitt soll festgelegt werden, wie Abbildungen $F : \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \rightarrow \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$ aussehen dürfen, die jedem Multi-q-Bit $e \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$ wieder ein Multi-q-Bit $F(e)$ zuordnen. Da jedes Multi-q-Bit e insbesondere Element eines Hilbertraumes $\mathcal{H}^{\otimes n}$ ist, legen wir zunächst fest, dass nur Automorphismen $F : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$ in Frage kommen. Somit können wir, da ja $\{e_1, \dots, e_{2^n}\}$ als Basis gewählt wurde, unsere möglichen Kandidaten durch die Menge aller regulären $2^n \times 2^n$ -Matrizen über $\mathbb{C}$ repräsentieren. Allerdings fehlt uns noch die Einschränkung, dass die Sphäre wieder auf die Sphäre abgebildet werden muss. Diejenigen Matrizen, die genau diese Eigenschaft erfüllen, werden als unitäre Matrizen bezeichnet.

Definition 2.3 (unitäre Matrix) Eine Matrix $\mathbf{M} = (m_{ij}) \in \mathbb{C}^{k,k}$, $k \in \mathbb{N}$, heißt unitär, falls mit $\mathbf{M}^* := (m_{ij}^*) \in \mathbb{C}^{k,k}$, $m_{ij}^* = \overline{m_{ji}}$, $i, j \in \{1, \dots, k\}$, gilt:

$$\mathbf{M}\mathbf{M}^* = \mathbf{E} \quad (\mathbf{E} \text{ bezeichnet die Einheitsmatrix}).$$

Offensichtlich ist wegen $\mathbf{M}^{-1} = \mathbf{M}^*$ jede unitäre Matrix regulär. Ferner gilt für $\lambda \in \{z \in \mathbb{C}^k; z_1 \overline{z_1} + \dots + z_k \overline{z_k} = 1\}$:

$$(\mathbf{M}\lambda)_1 \overline{(\mathbf{M}\lambda)_1} + \dots + (\mathbf{M}\lambda)_k \overline{(\mathbf{M}\lambda)_k} = 1.$$

Um die Notation nicht unnötig kompliziert zu gestalten, unterscheiden wir im allgemeinen bei Vektoren $x \in \mathbb{K}^n$ nicht zwischen der Zeilendarstellung

$$x = (x_1, \dots, x_n)$$

und der Spaltendarstellung

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Beispiele:

- Jede Diagonalmatrix, deren Diagonalelemente die Länge 1 haben, ist unitär.
- Jede reelle symmetrische Matrix, deren Eigenwerte die Werte ± 1 annehmen, ist unitär.
- Jede Matrix, deren Zeilen eine orthonormale Basis des $\mathbb{C}^k$ bilden, ist unitär.

Eine eben beschriebene Abbildung F , die - repräsentiert durch eine unitäre Matrix M_F - einem Multi-q-Bit $e \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$ wieder ein Multi-q-Bit $F(e) \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$ zuordnet, wird als Gate bezeichnet.

Beispiele:

- *NOT*-Gate:
Sei $b \in \{v_1, v_2\}$ ein Bit, so wird durch $NOT : \{v_1, v_2\} \rightarrow \{v_1, v_2\}$, $v_1 \mapsto v_2$ und $v_2 \mapsto v_1$ die logische Verneinung definiert. Ist nun $\{v_1, v_2\}$ die Basis eines Hilbertraumes $\mathcal{H}$, so kann man die Funktion NOT bezüglich dieser Basis durch die Matrix

$$M_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

darstellen. Diese Matrix ist unitär und kann direkt zur Definition einer *NOT*-Operation auf q-Bits verwendet werden:

$$F_{NOT} : \mathcal{S}_{\mathcal{H}}^1 \rightarrow \mathcal{S}_{\mathcal{H}}^1 \quad (\lambda_1, \lambda_2) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}$$

($F_{NOT}((\lambda_1, \lambda_2))$ als Spaltenvektor notiert).

Offensichtlich werden die Wahrscheinlichkeiten für die Ergebnisse $\{v_1\}$ und $\{v_2\}$ durch F_{NOT} gerade vertauscht.

- Hadamard-Gate:
Hadamard-Gates haben die Aufgabe, Multi-q-Bits, die eine Gleichverteilung implizieren (also $P(\{e_i\}) = \frac{1}{2^n}$, $i = 1, \dots, 2^n$) dadurch zu generieren, dass man dieses Gate auf Basiselemente anwendet. Bezüglich der Basis $\{e_1, \dots, e_{2^n}\}$ erhält man die unitären Matrizen:

$$n = 1 : \quad \mathbf{M}_{\mathbf{Ha},1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$n = 2 : \quad \mathbf{M}_{\mathbf{Ha},2} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

$$n = k + 1 : \quad \mathbf{M}_{\mathbf{Ha},k+1} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{M}_{\mathbf{Ha},k} & \mathbf{M}_{\mathbf{Ha},k} \\ \mathbf{M}_{\mathbf{Ha},k} & -\mathbf{M}_{\mathbf{Ha},k} \end{pmatrix}.$$

Offensichtlich werden für die Konstruktion der Hadamard-Matrizen Walsh-Funktionen herangezogen, die in der digitalen Nachrichtenübertragung insbesondere bei CDMA-Verfahren eine wichtige Rolle spielen.

Der Hintereinanderausführung von Gates entspricht die Matrixmultiplikation unitärer Matrizen. Für zwei Gates

$$F_1 : \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \rightarrow \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \text{ und } F_2 : \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \rightarrow \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$$

und den entsprechenden unitären Matrizen $\mathbf{M}_{F_1}$ und $\mathbf{M}_{F_2}$ gilt somit für $F : \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \rightarrow \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$, $e \mapsto F_2(F_1(e))$:

$$\mathbf{M}_F = \mathbf{M}_{F_2} \mathbf{M}_{F_1}.$$

Neben Gates gibt es noch eine zweite Art von Funktionen $F : \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \rightarrow \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$, die verwendet werden dürfen, nämlich die im Abschnitt 2.4 zu betrachtenden Messungen.

2.3 n-stellige Boolesche Funktionen

Seien $\mathcal{H}$ ein zweidimensionaler Hilbertraum mit orthonormalen Basis $\{v_1, v_2\}$ und $B : \{v_1, v_2\}^n \rightarrow \{v_1, v_2\}^m$, $m, n \in \mathbb{N}$, eine n-stellige Boolesche Funktion. Diese Funktion läßt sich mit $v_1 \hat{+} v_1 := v_1$, $v_1 \hat{+} v_2 = v_2 \hat{+} v_1 := v_2$ und $v_2 \hat{+} v_2 := v_1$ und mit

$$\begin{aligned} \tilde{B} : \{v_1, v_2\}^{n+m} &\rightarrow \{v_1, v_2\}^{n+m} \\ (b_1, \dots, b_n, b_{n+1}, \dots, b_{n+m}) &\mapsto (b_1, \dots, b_n, b_{n+1} \hat{+} B(b_1, \dots, b_n)_1, \dots, \\ &\quad b_{n+m} \hat{+} B(b_1, \dots, b_n)_m) \end{aligned}$$

wegen

$$\tilde{B}(b_1, \dots, b_n, v_1, \dots, v_1) = (b_1, \dots, b_n, B(b_1, \dots, b_n)_1, \dots, B(b_1, \dots, b_n)_m)$$

durch die Funktion $\tilde{B}$ repräsentieren. Der Vorteil der Darstellung $\tilde{B}$ für B liegt nun darin, dass $\tilde{B}$ sofort auf ein Multi-q-Bit verallgemeinert werden kann. Betrachten wir dazu ein Beispiel mit $n = 2$ und $m = 1$:

$$B : \{v_1, v_2\}^2 \rightarrow \{v_1, v_2\}, \quad (b_1, b_2) \mapsto b_1 \dot{+} b_2.$$

Nun repräsentieren wir wie bisher die Menge $\{v_1, v_2\}^3$ durch die orthonormale Basis $\{e_1, \dots, e_8\}$ des $\mathcal{H}^{\otimes 3}$. Für $\tilde{B}$ gilt dann:

$$\begin{aligned} \tilde{B}(e_1 \hat{=} (v_1, v_1, v_1)) &= (v_1, v_1, v_1) \hat{=} e_1 \\ \tilde{B}(e_2 \hat{=} (v_2, v_1, v_1)) &= (v_2, v_1, v_2) \hat{=} e_6 \\ \tilde{B}(e_3 \hat{=} (v_1, v_2, v_1)) &= (v_1, v_2, v_2) \hat{=} e_7 \\ \tilde{B}(e_4 \hat{=} (v_2, v_2, v_1)) &= (v_2, v_2, v_1) \hat{=} e_4 \\ \tilde{B}(e_5 \hat{=} (v_1, v_1, v_2)) &= (v_1, v_1, v_2) \hat{=} e_5 \\ \tilde{B}(e_6 \hat{=} (v_2, v_1, v_2)) &= (v_2, v_1, v_1) \hat{=} e_2 \\ \tilde{B}(e_7 \hat{=} (v_1, v_2, v_2)) &= (v_1, v_2, v_1) \hat{=} e_3 \\ \tilde{B}(e_8 \hat{=} (v_2, v_2, v_2)) &= (v_2, v_2, v_2) \hat{=} e_8 \end{aligned}$$

und als Gate bezüglich der gewählten Basis:

$$M_{\tilde{B}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Jede n-stellige Boolsche Funktion B kann über die Darstellung mit $\tilde{B}$ und nach Auszeichnung einer Basis des $\mathcal{H}^{\otimes (n+m)}$ durch ein Gate (also eine unitäre Matrix) dargestellt werden.

Stellen wir uns nun die Frage, was passiert, wenn wir in obigem Beispiel das Gate $M_{\tilde{B}}$ nicht auf einen Einheitsvektor, sondern auf ein allgemeines Multi-q-Bit anwenden. Dazu betrachten wir das Multi-q-Bit (in Spaltennotation)

$$e = \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \hat{=} \frac{1}{2}(e_1 \dot{+} e_2 \dot{+} e_3 \dot{+} e_4).$$

Die Vektoren e_1, e_2, e_3, e_4 repräsentieren gerade die Tripel (v_i, v_j, v_1) mit $i, j \in \{1, 2\}$. Somit erhält man für diese Vektoren als dritte Komponente von $\tilde{B}(v_i, v_j, v_1)$:

$$\tilde{B}(v_i, v_j, v_1) = (v_i, v_j, \mathbf{B}(\mathbf{v}_i, \mathbf{v}_j)).$$

Wendet man nun das Multi-q-Bit e auf das Gate $\mathbf{M}_{\tilde{B}}$ an, so ergibt sich:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \\ 0 \\ 1/2 \\ 1/2 \\ 0 \end{pmatrix} \hat{=} \frac{1}{2}(e_1 + e_4 + e_6 + e_7).$$

Somit erhält man durch Anwendung eines speziellen Multi-q-Bits e die simultane Berechnung aller möglichen Funktionswerte von B :

$$\begin{aligned} e_1 &\hat{=} (v_1, v_1, v_1) \implies B(v_1, v_1) = v_1, \\ e_4 &\hat{=} (v_2, v_2, v_1) \implies B(v_2, v_2) = v_1, \\ e_6 &\hat{=} (v_2, v_1, v_2) \implies B(v_2, v_1) = v_2, \\ e_7 &\hat{=} (v_1, v_2, v_2) \implies B(v_1, v_2) = v_2. \end{aligned}$$

Diesen Effekt nennt man Quanten-Parallelität. Die Funktion $\tilde{B}$ ist eine quantentheoretische Black-Box; das heißt, von der Funktion $\tilde{B}$ steht nur die Wirkung $\mathbf{M}_{\tilde{B}}e$ auf $e \in \mathcal{S}_{\mathcal{H}^{\otimes(n+m)}}^1$ zur Verfügung und jede Multiplikation $\mathbf{M}_{\tilde{B}}e$ wird als eine Funktionsauswertung gezählt. Gesucht ist ein Quantencomputer, der $\mathbf{M}_{\tilde{B}}e$ mit dem gleichen Aufwand berechnet wie ein klassischer Rechner eine Auswertung von B .

2.4 Messungen

Wie bereits in Abschnitt 2.1 angedeutet, kann ein Multi-q-Bit $e \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$ im Prinzip nur 2^n verschiedene Werte $\{e_1, \dots, e_{2^n}\}$ annehmen. Allerdings ist der Wert eines Multi-q-Bits e nicht unmittelbar erkennbar, sondern nur die durch

$$e = (\lambda_1, \dots, \lambda_{2^n}) \in \{(z_1, \dots, z_{2^n}) \in \mathbb{C}^{2^n}; \sum_{i=1}^{2^n} z_i \bar{z}_i = 1\}$$

gegebene Wahrscheinlichkeitsverteilung auf $\mathcal{P}(\Omega)$ mit $\Omega = \{e_1, \dots, e_{2^n}\}$.

Eine Vorrichtung zur Messung eines Multi-q-Bits e entspricht nun einer Partitionierung $E_1, \dots, E_k \subseteq \Omega$ von Ω . (also: $E_i \cap E_j = \emptyset$ für $i \neq j$ und $\bigcup_{j=1}^k E_j = \{e_1, \dots, e_{2^n}\}$). Die Mengen $E_1, \dots, E_k$ repräsentieren die möglichen Ergebnisse der Messung. Ein Ergebnis $E_i = \{e_{i_1}, \dots, e_{i_m}\}$ erhält man mit Wahrscheinlichkeit

$$P(E_i) = \sum_{j=1}^m \lambda_{i_j} \bar{\lambda}_{i_j} \quad i_j \in \{1, \dots, 2^n\}.$$

Analog zur Quantenphysik, bei der jede Messung eine Veränderung des zu betrachtenden Systems bedeutet, verändert die Messung eines Multi-q-Bits e das Multi-q-Bit selbst. In unserem Fall wird das Multi-q-Bit e aus wahrscheinlichkeitstheoretischer Sicht stark verändert, denn $e = (\lambda_1, \dots, \lambda_{2^n}) \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1$ geht durch eine Messung mit Ergebnis $E_i = \{e_{i_1}, \dots, e_{i_m}\}$ über in das Multi-q-Bit

$$\epsilon = (\mu_1, \dots, \mu_{2^n}) \in \mathcal{S}_{\mathcal{H}^{\otimes n}}^1 \text{ mit } \mu_k = \begin{cases} 0 & \text{falls } k \notin \{i_1, \dots, i_m\} \\ \frac{\lambda_k}{\sqrt{\sum_{j=1}^m \lambda_{i_j} \overline{\lambda_{i_j}}}} & \text{falls } k \in \{i_1, \dots, i_m\} \end{cases} .$$

Wie kann man nun eine Messung auf dem Rechner simulieren? Dazu zerlegt man das Einheitsintervall $[0, 1]$ in 2^n Teile der Form:

$$I_1 = [0, \lambda_1 \overline{\lambda_1}] , I_2 =]\lambda_1 \overline{\lambda_1}, \lambda_1 \overline{\lambda_1} + \lambda_2 \overline{\lambda_2}] , \dots , I_{2^n} = \left] \sum_{i=1}^{2^n-1} \lambda_i \overline{\lambda_i}, 1 \right] ,$$

wobei $]a, b] = \emptyset$, falls $a \geq b$. Nun generiert man mit Hilfe eines Pseudozufallszahlengenerators eine Realisierung ρ einer $[0, 1]$ -Gleichverteilung. Diese Zahl ρ ist Element genau eines Intervalls I_k der obigen Zerlegung. Somit erhält man diejenige Menge E_l als Ergebnis der Messung, für die gilt: $e_k \in E_l$.

2.5 q-Algorithmen

Ein q-Algorithmus besteht nach Wahl eines geeigneten Hilbertraumes und nach Wahl einer orthonormierten Basis (wir verwenden die bisherigen Bezeichnungen) im wesentlichen aus der sequentiellen Anwendung von Gates (repräsentiert durch unitäre Matrizen) und Messungen auf Basiselemente (repräsentiert durch Einheitsvektoren) oder auf im q-Algorithmus bereits berechnete Multi-q-Bits. Lediglich das Ergebnis von Messungen kommt als nach außen sichtbares Resultat eines q-Algorithmus' in Frage.

Als Beispiel betrachten wir einen q-Algorithmus zur Lösung des folgenden Problems: Gegeben ist eine Boolesche Funktion

$$B : \{v_1, v_2\}^n \rightarrow \{v_1, v_2\},$$

von der wir a priori wissen, dass B entweder konstant ist (also alle Funktionswerte gleich v_1 oder alle Funktionswerte gleich v_2) oder ausgeglichen ist (also 2^{n-1} Funktionswerte gleich v_1 und 2^{n-1} Funktionswerte gleich v_2). Um nun zu entscheiden, welche Eigenschaft B hat, sind normalerweise die Auswertungen von mindestens zwei und höchstens $2^{n-1} + 1$ Funktionswerten erforderlich. Wir entwickeln nun unter Verwendung der zu B gehörigen Funktion $\tilde{B}$ einen q-Algorithmus, der diese Frage mit nur einer Auswertung von $\tilde{B}$, zwei Hadamard-Gates und einer Messung entscheidet. Zunächst wenden wir den $(2^n + 1)$ -ten Einheitsvektor (entspricht dem

Basisvektor e_{2^n+1}) auf das Hadamard-Gate an:

$$x_1 = \mathbf{M}_{\text{Ha}, n+1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow (2^n + 1)\text{-te Komponente} .$$

Als Ergebnis erhalten wir einen Vektor x_1 , dessen erste 2^n Komponenten aus dem Wert $\frac{1}{\sqrt{2^{n+1}}}$ bestehen und dessen letzte 2^n Komponenten aus dem Wert $-\frac{1}{\sqrt{2^{n+1}}}$ bestehen. Alle positiven Komponenten von x_1 repräsentieren genau die Basisvektoren, die den Tupeln $(v_{i_1}, \dots, v_{i_n}, \mathbf{v}_1)$ zugeordnet sind. Alle negativen Komponenten von x_1 repräsentieren genau die Basisvektoren, die den Tupeln $(v_{i_1}, \dots, v_{i_n}, \mathbf{v}_2)$ zugeordnet sind. Ist nun die Funktion B ausgeglichen, so ergibt sich für

$$x_2 = \mathbf{M}_{\tilde{B}} x_1,$$

dass genau die Hälfte der ersten 2^n Komponenten von x_2 den Wert $\frac{1}{\sqrt{2^{n+1}}}$ und genau die Hälfte der ersten 2^n Komponenten von x_2 den Wert $-\frac{1}{\sqrt{2^{n+1}}}$ besitzen. Gleiches gilt für die zweiten 2^n Komponenten von x_2 . Wendet man also auf x_2 das Hadamard-Gate an:

$$x_3 = \mathbf{M}_{\text{Ha}, n+1} x_2,$$

so ist die $(2^n + 1)$ -te Komponente von x_3 gleich Null.
Ist die Funktion B konstant, so ergibt sich für

$$x_2 = \mathbf{M}_{\tilde{B}} x_1,$$

dass für $B \equiv v_1$ genau die ersten 2^n Komponenten von x_2 den Wert $\frac{1}{\sqrt{2^{n+1}}}$ und die genau die zweiten 2^n Komponenten von x_2 den Wert $-\frac{1}{\sqrt{2^{n+1}}}$ besitzen. Für $B \equiv v_2$ ist es genau umgekehrt. Wendet man also auf dieses x_2 das Hadamard-Gate an:

$$x_3 = \mathbf{M}_{\text{Ha}, n+1} x_2,$$

so ist die $(2^n + 1)$ -te Komponente von x_3 gleich 1 (für $B \equiv v_1$) oder gleich -1 (für $B \equiv v_2$). Eine Messung des Multi-q-Bits x_3 mit den möglichen Messergebnissen $E_1 = \{e_{2^n+1}\}$ und $E_2 = \{e_1, \dots, e_{2^n}, e_{2^n+2}, \dots, e_{2^{n+1}}\}$ ergibt die gewünschte Entscheidung.

Im folgenden wollen wir den eben betrachteten, nach D. Deutsch und R. Josza benannten q-Algorithmus kurz analysieren. Führt man die angegebenen Operationen auf einem klassischen Computer aus, so ist offensichtlich, dass sich im Aufwand durch die etwas ungewöhnliche Formulierung der Funktion B durch $\tilde{B}$ und durch die Verwendung von Multi-q-Bits nichts verbessert. Setzt man allerdings voraus, dass durch einen Quanten-Computer die Matrixmultiplikation $\mathbf{M}_{\tilde{B}}e$ für jedes Multi-q-Bit e mit gleichem Aufwand zu leisten ist, wie eine Auswertung der

Funktion B nach heutigem Standard, so ist die Komplexitätsreduktion gewaltig. Multipliziert man die Matrix $M_{\tilde{B}}$ nur mit Einheitsvektoren, so entspricht eine solche Multiplikation gerade der Auswertung der Funktion B im klassischen Sinne. Wie könnte man nun die Ideen eines q-Algorithmus' verwenden, um auf einem klassischen Rechner zu einer Komplexitätsreduktion zu kommen? Zunächst dürfen wir nur Einheitsvektoren (entsprechen den Basiselementen) auf die einzelnen Gates anwenden. Ein Multi-q-Bit e kann man nun durch einen Einheitsvektor ersetzen, indem man das zu e gehörige Zufallsexperiment durchführt und dann e durch das Ergebnis dieses Zufallsexperimentes ersetzt. Wendet man diese Vorgehensweise auf den obigen Algorithmus an, so führt man zunächst ein Zufallsexperiment $(\{e_1, \dots, e_{2^n}\}, \mathcal{P}(\{e_1, \dots, e_{2^n}\}), P(e_i) = \frac{1}{2^n})$ (im Rechner, cf. Abschnitt 2.4) durch (entspricht der Wirkung des ersten Hadamard-Gates). Das zum Ergebnis $e^{(j)}$ dieses Zufallsexperiments gehörige Tupel $(v_{i_1}, \dots, v_{i_n})$ setzt man in die Funktion B ein (entspricht im q-Algorithmus der Multiplikation $M_{\tilde{B}}e$). Dieses Verfahren wird nun so lange wiederholt, bis sich entweder verschiedene Funktionswerte einstellen oder bis eine gewählte maximale Anzahl m von gleichen Funktionswerten mit m Versuchen errechnet wurde. Im ersten Fall ist die Entscheidung klar, da B ausgeglichen sein muss; im zweiten Fall entscheidet man sich dafür, dass B konstant ist (dieser Entscheidungsfindung entspricht im q-Algorithmus die Wirkung des zweiten Hadamard-Gates). Ist nun B trotzdem ausgeglichen, so ist die Wahrscheinlichkeit dafür gleich $(1/2)^m$. Will man nun die Wahrscheinlichkeit, sich falsch zu entscheiden (also B wird für konstant gehalten obwohl B ausgeglichen ist) unter eine vorgegebene Fehlerwahrscheinlichkeit α drücken, so muss man die Anzahl m der notwendigen Funktionsauswertungen gemäß folgender Ungleichung wählen:

$$m \geq \frac{\ln(\alpha)}{\ln(2)}.$$

Für $m \geq 24$ sind sechs Richtige im Lotto mit einem Tipp (6 aus 49) wahrscheinlicher als eine Fehlentscheidung über B . Die Anzahl m ist für jedes feste α unabhängig von der Dimension n des Problems (beziehungsweise der Dimension 2^{n+1} des Hilbertraums). Diese Dimensionsunabhängigkeit wird vom q-Algorithmus vererbt, der ja nur eine Auswertung von $M_{\tilde{B}}$ für eine sichere Entscheidung benötigt.

Nicht jeder q-Algorithmus führt automatisch zu einem klassischen stochastischen Algorithmus mit optimaler Komplexität. Als Beispiel betrachten wir den Suchalgorithmus von L. Grover; dabei gehen wir nur auf die wesentlichen Ideen ein. Gegeben sei eine unstrukturierte Datenbank mit 2^n Einträgen. Gesucht ist ein spezieller Eintrag in dieser Datenbank (zum Beispiel die Person zu einer speziellen Telefonnummer mit Hilfe des Telefonbuchs). Wir repräsentieren die 2^n Einträge der Datenbank durch die orthonormale Basis $\{e_1, \dots, e_{2^n}\}$ unseres Hilbertraumes $\mathcal{H}^{\otimes n}$ und den gesuchten Eintrag bezeichnen wir mit e_j . Um nun zu entscheiden, ob ein Eintrag e_i der gesuchte Eintrag ist, steht im klassischen Fall eine binäre Funktion f definiert auf der Menge aller Einträge der Datenbank zur Verfügung. Bezüglich unserer Multi-q-Bits wird diese Funktion durch eine unitäre Diagonalmatrix M repräsentiert, deren j -tes Diagonalelement gleich -1 ist, während alle übrigen Diagonalelemente gleich Eins sind. Die Matrix M ist eine quantentheoretische Black-Box. Neben diesem Gate

benötigen wir noch das Gate

$$\mathbf{P} = \frac{1}{2^n} \begin{pmatrix} (2 - 2^n) & 2 & \cdots & 2 \\ 2 & (2 - 2^n) & 2 & \vdots \\ 2 & 2 & \ddots & 2 \\ 2 & \cdots & 2 & (2 - 2^n) \end{pmatrix}.$$

Der Algorithmus von Grover besteht aus der iterativen Anwendung des Gates $\mathbf{PM}$:

$$x_1 := \begin{pmatrix} \frac{1}{\sqrt{2^n}} \\ \vdots \\ \frac{1}{\sqrt{2^n}} \end{pmatrix}, \quad x_i = \mathbf{PM}x_{i-1}, \quad i = 2, \dots, K.$$

Wählt man nun K in der Größenordnung $\frac{4}{\pi}\sqrt{2^n}$, so kann man zeigen, dass die j -te Komponente von x_K , die ja gerade den gesuchten Eintrag in der Datenbank repräsentiert, eine große Wahrscheinlichkeit darstellt. Nach etwa $\sqrt{2^n}$ Funktionsauswertungen erhält man somit ein Multi-q-Bit, dessen Messung mit $E_i = \{e_i\}$, $i = 1, \dots, 2^n$, mit großer Wahrscheinlichkeit den gesuchten Eintrag liefert. Für $n = K = 2$ erhält man:

$$x_2 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \longleftarrow (j)\text{-te Komponente}.$$

Versucht man, diesen q-Algorithmus durch Anwendung stochastisch gewählter Einheitsvektoren auf $\mathbf{PM}$ auf einen klassischen Rechner zu übertragen, so zeigt sich, dass der resultierende stochastische Algorithmus im allgemeinen schlechter ist als die übliche stochastische Methode, die im Mittel $\frac{2^n+1}{2}$ Versuche benötigt.

Literaturverzeichnis

A. K. Ekert, R. Jozsa, *Quantum computation and Shor's algorithm*. Rev. Mod. Phys. **68**, pp. 733-753, 1996.

H. S. Green, *Information Theory and Quantum Physics*. Springer Verlag, 2000.

M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

L. Grover, *A fast quantum algorithm for database search*. ACM Symp. on Theory of Computation, pp. 212-219, Philadelphia 1997.