

Quantencomputer mit gefangenen Ionen in Penning-Fallen

Von der Phonon-Kopplung dreier Ionen bis zum Shor-Algorithmus
Ein Skript mit vielen Rechenbeispielen für Studierende der Data Science

Christoph Würsch
Institut für Computational Engineering ICE
OST – Ostschweizer Fachhochschule

Version 2 – September 2026

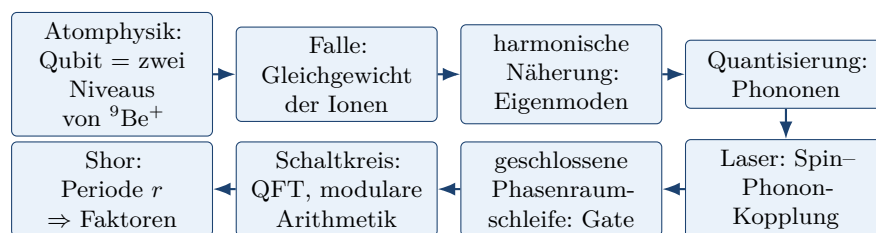
Vorwort

Dieses Skript erklärt, wie ein Quantencomputer mit gefangenen Ionen funktioniert – und zwar am konkreten Beispiel der Technologie, die das Zürcher ETH-Spin-off *ZuriQ* entwickelt: einzelne Beryllium-Ionen (${}^9\text{Be}^+$), die in mikrostrukturierten *Penning-Fallen* über einem Chip schweben, gehalten allein durch statische elektrische Felder und ein starkes Magnetfeld von etwa 3 T [1, 3].

Das Skript richtet sich an Bachelorstudierende der Data Science. Das bedeutet zweierlei. Erstens setze ich keine Quantenmechanik voraus, wohl aber sichere lineare Algebra (Vektoren, Matrizen, Eigenwerte, Singulärwertzerlegung), komplexe Zahlen und etwas Analysis. Zweitens werden Sie überrascht sein, wie viel Ihres Werkzeugkastens Sie hier wiederfinden: Ein Quantenzustand ist ein normierter Vektor, ein Gate eine unitäre Matrix, Verschränkung lässt sich mit dem Rang einer Matrix prüfen, die Eigenmoden einer Ionenkette sind eine Eigenwertzerlegung, die Quanten-Fourier-Transformation ist `numpy.fft.ifft` bis auf einen Faktor, und die Auslese eines Qubits ist ein Klassifikationsproblem mit Poisson-verteilten Merkmalen. Kästen mit der Überschrift *Data-Science-Brille* machen diese Verbindungen explizit.

Der rote Faden

Die zentrale Frage des Skripts lautet: *Wie rechnet man mit schwingenden Ionen?* Die Antwort ist eine Kette von Modellierungsschritten, die wir der Reihe nach durchgehen:



Teil I führt die Sprache der Quanteninformation ein (Qubits, Tensorprodukte, Verschränkung, Gates). Teil II erklärt die Hardware: Was genau *ist* der Quantenzustand eines Beryllium-Ions, wie hält eine Penning-Falle ein Ion fest, und warum ist seine Bewegung quantisiert? Teil III ist das Herzstück: Wir berechnen die Eigenmoden von drei Coulomb-gekoppelten Ionen explizit in der harmonischen Näherung – einmal für eine Kette in einer gemeinsamen Falle und einmal für drei getrennte Mikrofallen, wie bei *ZuriQ* – und zeigen, wie Laserpulse über diese gemeinsamen Schwingungen (Phononen) die Qubits verschränken. Teil IV macht daraus einen Computer: Gate-Zerlegungen, Auslese und Statistik, die Quanten-Fourier-Transformation und schliesslich ausführlich der Shor-Algorithmus zur Faktorisierung ganzer Zahlen.

Wie man dieses Skript liest

- **Rechenbeispiele** sind nummeriert und enthalten echte Zahlen für ${}^9\text{Be}^+$. Alle Zahlen wurden mit den Python-Programmen in Kapitel A nachgerechnet; es lohnt sich, sie selbst auszuführen und zu variieren.
- **Merksätze** fassen das Wesentliche zusammen; **Achtung**-Kästen korrigieren verbreitete Fehlvorstellungen.
- **Übungsaufgaben** mit Lösungen stehen in Kapitel 14.
- Als Konvention verwenden wir $\hbar$ explizit in physikalischen Kapiteln und setzen $\hbar = 1$ nur dort, wo es ausdrücklich gesagt wird. Frequenzen ν in Hz und Kreisfrequenzen $\omega = 2\pi\nu$ in rad/s werden streng unterschieden: „ $\omega = 2\pi \times 2,5 \text{ MHz}$ “ bedeutet $\nu = 2,5 \text{ MHz}$.

Was dieses Skript nicht behauptet

ZuriQ veröffentlicht Architektur und Meilensteine, aber nicht jedes Detail seiner Gate-Protokolle. Die Physik in diesem Skript – Qubit-Niveaus, Fallenfrequenzen, Coulomb-Kopplung, Seitenband- und Mølmer-Sørensen-Gates – ist in der Fachliteratur etabliert und auf die ZuriQ-Plattform übertragbar. Wo wir konkrete Parameter wählen, sind es entweder publizierte Werte (z. B. aus [1]) oder ausdrücklich als Beispielwerte gekennzeichnete Größen.

Inhaltsverzeichnis

Vorwort	i
I Quanteninformation für Data Scientists	1
1 Vom Bit zum Qubit	2
1.1 Zustand als Vektor	2
1.2 Messung: die Bornsche Regel	2
1.3 Globale und relative Phase, Bloch-Kugel	3
1.4 Ein erstes Quantengate und Interferenz	3
1.5 Pauli-Matrizen und Erwartungswerte	4
1.6 Gemischte Zustände (kurz)	4
2 Mehrere Qubits, Tensorprodukt und Verschränkung	5
2.1 Das Tensorprodukt	5
2.2 Verschränkung	5
2.3 Reduzierte Zustände und partielle Spur	6
2.4 Drei Qubits: GHZ und W	7
2.5 Korrelation ist nicht gleich Verschränkung	7
3 Gates: Rechnen durch kontrollierte Zeitentwicklung	8
3.1 Die Schrödinger-Gleichung in einer Zeile	8
3.2 Exponentialfunktionen von Pauli-Matrizen	8
3.3 Zwei-Qubit-Gates	9
3.4 Kohärenz und Fidelity	10
II Die Hardware: Beryllium-Ionen in der Penning-Falle	11
4 Das ${}^9\text{Be}^+$-Ion: Was ist der Quantenzustand wirklich?	12

4.1	Aufbau des Ions	12
4.2	Der Hamiltonoperator des Grundzustands	13
4.3	Das Qubit	14
4.4	Optische Übergänge: Initialisieren und Auslesen	15
4.5	Innerer Zustand versus Bewegung	16
5	Die Penning-Falle	18
5.1	Warum man ein Magnetfeld braucht	18
5.2	Das ideale Quadrupolpotential	18
5.3	Von der Linearisierung zum Eigenwertproblem	20
5.4	Die Mikro-Penning-Falle von ETH und ZuriQ	20
6	Quantisierte Bewegung: Phononen	22
6.1	Der quantenmechanische harmonische Oszillator	22
6.2	Drei Oszillatoren pro Ion in der Penning-Falle	23
6.3	Thermische Zustände	23
6.4	Kohärente Zustände und Verschiebungen	23
III	Phonon-Kopplung und Verschränkung dreier Ionen	25
7	Drei gekoppelte Ionen in harmonischer Näherung	26
7.1	Modell A: drei Ionen in einer linearen Kette	27
7.2	Modell B: drei Ionen in drei Mikrofallen (ZuriQ-artig)	29
7.3	Lamb–Dicke-Parameter: Wie stark spürt ein Laser die Mode?	32
8	Licht koppelt Qubit und Bewegung	34
8.1	Der Wechselwirkungs-Hamiltonoperator	34
8.2	Lamb–Dicke-Näherung: Träger und Seitenbänder	34
8.3	Seitenbandkühlung und Thermometrie	35
8.4	Verschränkung über ein reales Phonon: die Seitenband-Sequenz	36
9	Das geometrische Phasengate: Verschränkung über virtuelle Phononen	38
9.1	Die spinabhängige Kraft	38
9.2	Exakte Lösung mit der Magnus-Entwicklung	39
9.3	Zwei Ionen: das Gate	39
9.4	Drei Ionen und viele Moden: die Kopplungsmatrix J_{ij}	41
9.5	Und in getrennten Mikrofallen?	42

9.6	Die Brücke zur Störungstheorie: virtuelle Phononen	43
IV	Rechnen mit dem Ionen-Quantencomputer	44
10	Vom Schaltkreis zum Laserpuls: Wie man mit Ionen rechnet	45
10.1	Der native Gatesatz	45
10.2	Kompilieren: CNOT und CPhase aus nativen Gates	45
10.3	Ablauf einer Rechnung auf dem Ionen-Chip	46
10.4	Auslese als Klassifikationsproblem	46
10.5	Statistik: Wie viele Shots braucht man?	47
10.6	Konnektivität und Transport	48
11	Die Quanten-Fourier-Transformation	49
11.1	Definition und Verwandtschaft mit der FFT	49
11.2	Die Produktdarstellung	50
11.3	Der Schaltkreis	50
11.4	Aufwand	51
12	Der Shor-Algorithmus	52
12.1	Worum es geht	52
12.2	Werkzeugkasten Zahlentheorie	52
12.3	Von der Faktorisierung zur Periodensuche	53
12.4	Der Quantenteil: Periodensuche	54
12.5	Schritt 5: Kettenbrüche – aus k/Q wird r	57
12.6	Zweite Sicht: Phasenschätzung	58
12.7	Ein vollständig kompilierter Schaltkreis: $N = 15$, $a = 2$	59
12.8	Der vollständige Algorithmus	60
12.9	Was kostet Shor auf echter Hardware?	60
13	Die ZuriQ-Architektur: vom Einzelion zum 2D-Prozessor	61
13.1	Was öffentlich bekannt ist	61
13.2	Paul-Falle und Penning-Mikrofalle im Vergleich	62
13.3	Wie ein Zwei-Qubit-Gate in einem 2D-Array ablaufen kann	62
13.4	Fehlerquellen	62
13.5	Skalierung und Fehlertoleranz	63
14	Übungsaufgaben mit Lösungen	64



A Python-Programme	67
A.1 Drei Ionen: Eigenmoden und Kopplungen	67
A.2 Spin-Phonon-Dynamik und MS-Gate	70
A.3 Shor-Algorithmus	73
A.4 Beryllium-Niveaus	75
B Konstanten und Notation	78
B.1 Konstanten und $^9\text{Be}^+$ -Daten	78
B.2 Notation	78
Literatur	80



Teil I

Quanteninformation für Data Scientists

Kapitel 1

Vom Bit zum Qubit

1.1 Zustand als Vektor

Ein klassisches Bit ist entweder 0 oder 1. Ein probabilistisches Bit (etwa eine Münze, die geworfen, aber noch nicht angesehen wurde) beschreiben wir mit einem Wahrscheinlichkeitsvektor $(p_0, p_1)^T$ mit $p_0, p_1 \geq 0$ und $p_0 + p_1 = 1$. Ein *Qubit* wird ebenfalls durch einen Zweivektor beschrieben – aber seine Einträge sind komplexe *Amplituden*:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \hat{=} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \quad (1.1)$$

Die Schreibweise $|\cdot\rangle$ („Ket“) ist nichts weiter als ein Spaltenvektor; $\langle\psi| = |\psi\rangle^\dagger$ („Bra“) ist der konjugiert-transponierte Zeilenvektor, und $\langle\phi|\psi\rangle$ ist das komplexe Skalarprodukt. Die Rechenbasis ist $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$.

Data-Science-Brille

Vergleichen Sie: Ein Wahrscheinlichkeitsvektor ist in der 1-Norm normiert ($\sum_i p_i = 1$), ein Quantenzustand in der 2-Norm ($\sum_i |c_i|^2 = 1$). Wahrscheinlichkeiten erhält man erst durch Betragsquadrate. Weil Amplituden negativ oder komplex sein können, können sie sich bei der Überlagerung *auslöschen* – das ist Interferenz, und sie ist die eigentliche Ressource des Quantenrechnens.

1.2 Messung: die Bornsche Regel

Misst man ein Qubit in der Rechenbasis, erhält man zufällig 0 oder 1 mit

$$P(0) = |\alpha|^2, \quad P(1) = |\beta|^2. \quad (1.2)$$

Nach der Messung ist der Zustand $|0\rangle$ bzw. $|1\rangle$ („Kollaps“). Eine einzelne Messung liefert also nur ein Bit; um $|\alpha|^2$ zu schätzen, muss man den Versuch viele Male („Shots“) wiederholen. Diese simple Tatsache wird bei Shor entscheidend sein: Man kann nicht „alle 2^n Amplituden auslesen“.

Rechenbeispiel 1.1: Messwahrscheinlichkeiten

Für $|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + i\sqrt{\frac{2}{3}}|1\rangle$ ist $P(0) = \frac{1}{3}$, $P(1) = |i|^2 \cdot \frac{2}{3} = \frac{2}{3}$. Die Phase i ist für diese Messung unsichtbar – aber nicht für eine Messung in einer anderen Basis (siehe Abschnitt 1.4).

1.3 Globale und relative Phase, Bloch-Kugel

Multipliziert man einen Zustand mit $e^{i\gamma}$, ändern sich keine Messwahrscheinlichkeiten; eine *globale* Phase ist physikalisch bedeutungslos. Die *relative* Phase zwischen α und β ist dagegen messbar. Bis auf die globale Phase schreibt man daher jeden Qubit-Zustand als

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle, \quad 0 \leq \theta \leq \pi, \quad 0 \leq \phi < 2\pi, \quad (1.3)$$

also als Punkt auf der Einheitskugel mit Polarwinkel θ und Azimut ϕ – der *Bloch-Kugel* (Abb. 1.1). Der Nordpol ist $|0\rangle$, der Südpol $|1\rangle$, der Äquator enthält die gleichgewichteten Superpositionen

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, \quad |\pm i\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}. \quad (1.4)$$

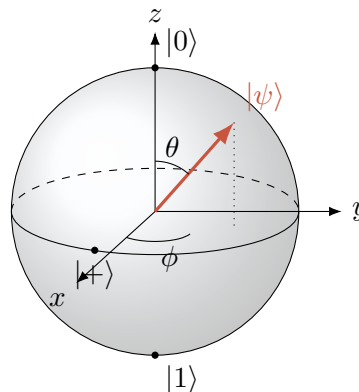


Abbildung 1.1: Bloch-Kugel. Jeder reine Qubit-Zustand ist ein Punkt auf der Oberfläche; Ein-Qubit-Gates sind Drehungen der Kugel.

1.4 Ein erstes Quantengate und Interferenz

Das *Hadamard-Gate*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (1.5)$$

bildet $|0\rangle \mapsto |+\rangle$ und $|1\rangle \mapsto |-\rangle$ ab. Es ist unitär ($H^\dagger H = \mathbb{I}$) und sein eigenes Inverses.

Rechenbeispiel 1.2: Interferenz: zweimal Hadamard

Wir starten in $|0\rangle$. Nach einem Hadamard ist $P(0) = P(1) = \frac{1}{2}$ – scheinbar eine faire Münze. Wendet man ein zweites Hadamard an, erhält man aber nicht wieder „50:50“, sondern

$$H|+\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \frac{1}{2}[(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)] = |0\rangle.$$

Die beiden „Wege“ zu $|1\rangle$ haben die Amplituden $+\frac{1}{2}$ und $-\frac{1}{2}$ und löschen sich aus. Eine klassische Münze, zweimal geworfen, bleibt dagegen fair: Die stochastische Matrix $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ ist idempotent. *Quantenalgorithmen sind so konstruiert, dass sich falsche Antworten auslöschen und richtige verstärken.*

1.5 Pauli-Matrizen und Erwartungswerte

Die drei Pauli-Matrizen

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1.6)$$

sind hermitesch, unitär, quadrieren zu $\mathbb{I}$ und erfüllen $XY = iZ$ (zyklisch). X ist das Quanten-NOT. Der Erwartungswert $\langle Z \rangle = \langle \psi | Z | \psi \rangle = |\alpha|^2 - |\beta|^2 = P(0) - P(1)$ ist die z -Koordinate auf der Bloch-Kugel; allgemein ist der *Bloch-Vektor* $\vec{s} = (\langle X \rangle, \langle Y \rangle, \langle Z \rangle) = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$.

Rechenbeispiel 1.3: Bloch-Vektor bestimmen

Für $|\psi\rangle = \cos \frac{\pi}{8} |0\rangle + e^{i\pi/2} \sin \frac{\pi}{8} |1\rangle$ ist $\theta = \pi/4$, $\phi = \pi/2$, also $\vec{s} = (0, \sin \frac{\pi}{4}, \cos \frac{\pi}{4}) = (0, 0.707, 0.707)$. Messen wir Z mit $S = 1000$ Shots, erwarten wir $P(0) = \cos^2(\pi/8) = 0.854$, also etwa 854 Nullen – mit einer statistischen Unsicherheit von $\sqrt{Sp(1-p)} \approx 11$ Zählereignissen.

1.6 Gemischte Zustände (kurz)

Reale Qubits sind nie perfekt isoliert. Eine statistische Mischung reiner Zustände beschreibt man mit der *Dichtematrix*

$$\rho = \sum_k p_k |\psi_k\rangle \langle \psi_k| = \frac{1}{2}(\mathbb{I} + \vec{s} \cdot \vec{\sigma}), \quad |\vec{s}| \leq 1. \quad (1.7)$$

Reine Zustände liegen auf der Oberfläche ($|\vec{s}| = 1$, $\text{Tr} \rho^2 = 1$), gemischte im Inneren. Dekohärenz (Abschnitt 3.4) lässt den Bloch-Vektor schrumpfen. Wir benötigen Dichtematrizen vor allem in Kapitel 9, um den Zustand der Qubits zu beschreiben, wenn wir die Bewegung der Ionen „wegmitteln“ (partielle Spur).

Kapitel 2

Mehrere Qubits, Tensorprodukt und Verschränkung

2.1 Das Tensorprodukt

Zwei Qubits $|a\rangle = (a_0, a_1)^T$ und $|b\rangle = (b_0, b_1)^T$ bilden gemeinsam den Produktzustand

$$|a\rangle \otimes |b\rangle = \begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{pmatrix} = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle. \quad (2.1)$$

In NumPy ist das `np.kron(a, b)`. Die Basiszustände $|q_1 q_2 \dots q_n\rangle$ werden wie Binärzahlen gelesen: $|101\rangle = |5\rangle$. Ein allgemeiner Zustand von n Qubits ist ein normierter Vektor in $\mathbb{C}^{2^n}$,

$$|\Psi\rangle = \sum_{x=0}^{2^n-1} c_x |x\rangle, \quad \sum_x |c_x|^2 = 1. \quad (2.2)$$

Rechenbeispiel 2.1: Wie gross ist $\mathbb{C}^{2^n}$?

Speichert man jede Amplitude als `complex128` (16 Byte), braucht ein Zustandsvektor von $n = 30$ Qubits $2^{30} \cdot 16 \text{ B} = 16 \text{ GiB}$, für $n = 40$ schon 16 TiB, für $n = 50$ rund 16 PiB. Deshalb lassen sich Quantencomputer mit mehr als etwa 45–50 Qubits im Allgemeinen nicht mehr exakt klassisch simulieren – obwohl jede *Messung* nur n klassische Bits liefert.

Operatoren auf Teilsystemen werden ebenfalls mit $\otimes$ kombiniert: $X_1 \equiv X \otimes \mathbb{I}$ wirkt nur auf Qubit 1, $X_1 X_2 \equiv X \otimes X$ auf beide. Es gilt $(A \otimes B)(|a\rangle \otimes |b\rangle) = A|a\rangle \otimes B|b\rangle$.

2.2 Verschränkung

Merksatz

Ein Zwei-Qubit-Zustand heisst *separabel* (Produktzustand), wenn er sich als $|a\rangle \otimes |b\rangle$ schreiben lässt. Sonst heisst er *verschränkt*.

Das berühmteste Beispiel ist der Bell-Zustand

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (2.3)$$

Angenommen, $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$. Dann wäre $a_0b_1 = 0$ (kein $|01\rangle$), also $a_0 = 0$ oder $b_1 = 0$. Beides widerspricht $a_0b_0 = a_1b_1 = 1/\sqrt{2} \neq 0$. Also ist $|\Phi^+\rangle$ verschränkt. Misst man das erste Qubit, ist das Ergebnis zufällig – aber das zweite Qubit zeigt *immer* dasselbe Ergebnis – und zwar nicht nur in der Z -Basis, sondern auch in der X -Basis (in der Y -Basis sind die Ergebnisse perfekt antikorreliert). Eine klassische Zufallsquelle kann das nicht leisten.

2.2.1 Verschränkung als Rang einer Matrix

Data-Science-Brille: Verschränkung = Rang > 1

Schreiben Sie die vier Amplituden eines Zwei-Qubit-Zustands als 2×2 -Matrix

$$C = \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix} \quad (C = \text{psi.reshape}(2,2)).$$

Ein Produktzustand hat $C = \vec{a}\vec{b}^T$ – eine Matrix vom Rang 1. Der Zustand ist genau dann verschränkt, wenn $\text{rang } C = 2$, d.h. $\det C = c_{00}c_{11} - c_{01}c_{10} \neq 0$. Allgemeiner liefert die Singulärwertzerlegung $C = U\Sigma V^\dagger$ die *Schmidt-Zerlegung*

$$|\Psi\rangle = \sum_k s_k |u_k\rangle \otimes |v_k\rangle, \quad \sum_k s_k^2 = 1,$$

und die Verschränkungsentropie $E = -\sum_k s_k^2 \log_2 s_k^2$ misst, *wie stark* verschränkt ist ($E = 0$: Produkt, $E = 1$: maximal für zwei Qubits). Für Bipartitionen grosser Systeme ist das exakt dasselbe wie eine Niedrigrang-Approximation – die Grundlage von Tensornetzwerk-Simulationen.

Rechenbeispiel 2.2: Verschränkt oder nicht?

- (a) $|\Psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$: $C = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $\det C = 0 \Rightarrow$ Produkt, nämlich $|+\rangle \otimes |+\rangle$.
- (b) $|\Psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$: $\det C = \frac{1}{4}(-1 - 1) = -\frac{1}{2} \neq 0 \Rightarrow$ verschränkt. Die Singulärwerte von C sind $s_{1,2} = 1/\sqrt{2}$, also $E = 1$: maximal verschränkt, obwohl alle vier Amplituden gleich gross sind!
- (c) $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm i|11\rangle)$ – dieser Zustand wird uns beim Mølmer-Sørensen-Gate begegnen (das Vorzeichen hängt von der Konvention ab): $\det C = \pm i/2 \neq 0$, $E = 1$.

2.3 Reduzierte Zustände und partielle Spur

Wie sieht Qubit 1 aus, wenn man Qubit 2 ignoriert? Man bildet die *reduzierte Dichtematrix*

$$\rho_1 = \text{Tr}_2 |\Psi\rangle \langle \Psi| = C C^\dagger. \quad (2.4)$$

Für $|\Phi^+\rangle$ ist $C = \mathbb{I}/\sqrt{2}$ und $\rho_1 = \mathbb{I}/2$: Das einzelne Qubit ist *maximal gemischt*, sein Bloch-Vektor ist null. Die gesamte Information steckt in den Korrelationen. Diese Rechnung wird in Kapitel 9 wichtig: Wenn ein Qubit mit der *Bewegung* eines Ions verschränkt bleibt und wir die Bewegung nicht messen, wird der Qubit-Zustand gemischt – das ist ein Gatefehler.

2.4 Drei Qubits: GHZ und W

Für drei Qubits gibt es zwei wesentlich verschiedene Klassen echter Dreifach-Verschränkung:

$$|\text{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \quad |\text{W}\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}. \quad (2.5)$$

Misst man beim GHZ-Zustand ein Qubit, ist die Verschränkung der beiden anderen zerstört; beim W-Zustand bleibt sie teilweise erhalten. Wir werden in Abschnitt 9.4.3 sehen, dass ein einziger Laserpuls, der alle drei Ionen über ihre gemeinsame Schwerpunktschwingung koppelt, einen GHZ-Zustand erzeugt, während ein Phonon, das zwischen drei Fallen „hüpft“ (Abschnitt 7.2.3), auf natürliche Weise W-artige Überlagerungen erzeugt.

2.5 Korrelation ist nicht gleich Verschränkung

Die klassische Mischung $\rho = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ zeigt perfekte Korrelation in Z , ist aber nicht verschränkt: In der X -Basis verschwindet die Korrelation. Beim Bell-Zustand $|\Phi^+\rangle$ ist dagegen $\langle X_1 X_2 \rangle = \langle Z_1 Z_2 \rangle = 1$.

Begriffe sauber trennen

Eine *Wechselwirkung* ist ein Term im Hamiltonoperator (z.B. $J X_1 X_2$). Eine *Korrelation* ist eine Eigenschaft eines Zustands, z.B. $\langle Z_1 Z_2 \rangle - \langle Z_1 \rangle \langle Z_2 \rangle$. *Verschränkung* ist eine stärkere, genuin quantenmechanische Eigenschaft, die sich nicht durch klassische Mischungen von Produktzuständen erklären lässt. Phononen *vermitteln* eine Wechselwirkung; diese *erzeugt* mit der Zeit Verschränkung.

Kapitel 3

Gates: Rechnen durch kontrollierte Zeitentwicklung

3.1 Die Schrödinger-Gleichung in einer Zeile

Ein abgeschlossenes Quantensystem entwickelt sich gemäss

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H |\psi(t)\rangle, \quad (3.1)$$

wobei der *Hamiltonoperator* H eine hermitesche Matrix ist, deren Eigenwerte die möglichen Energien sind. Für zeitunabhängiges H ist die Lösung

$$|\psi(t)\rangle = U(t) |\psi(0)\rangle, \quad U(t) = \exp\left(-\frac{i}{\hbar} Ht\right), \quad U^\dagger U = \mathbb{I}. \quad (3.2)$$

Merksatz

Ein Quantengate ist keine Box, durch die ein Ion hindurchfliegt. Es ist eine *gezielt eingeschaltete Hamilton-Dynamik* für eine *genau kontrollierte Dauer*: Hamiltonoperator $\xrightarrow{\text{Zeit } t} U = e^{-iHt/\hbar} \rightarrow \text{Gate}$. Bei Ionen wird H durch Laser- oder Mikrowellenfelder mit einstellbarer Frequenz, Phase, Amplitude und Dauer erzeugt.

3.2 Exponentialfunktionen von Pauli-Matrizen

Weil $\sigma^2 = \mathbb{I}$ für jede Pauli-Matrix (und jedes Produkt wie $X \otimes X$), zerfällt die Exponentialreihe in einen geraden und einen ungeraden Teil:

$$e^{-i\varphi\sigma} = \sum_k \frac{(-i\varphi)^k \sigma^k}{k!} = \cos \varphi \mathbb{I} - i \sin \varphi \sigma. \quad (3.3)$$

Das ist die wichtigste Rechenregel dieses Skripts. Damit sind die Drehungen der Bloch-Kugel um die Achse $\mu \in \{x, y, z\}$

$$R_\mu(\theta) = e^{-i\theta\sigma_\mu/2} = \cos \frac{\theta}{2} \mathbb{I} - i \sin \frac{\theta}{2} \sigma_\mu, \quad R_x(\theta) = \begin{pmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}. \quad (3.4)$$

Für eine Drehachse in der Äquatorebene mit Azimut ϕ schreiben wir

$$R_\phi(\theta) = \exp[-i\frac{\theta}{2}(\cos \phi X + \sin \phi Y)]. \quad (3.5)$$

Genau diese Operation erzeugt ein resonanter Laserpuls (Kapitel 8): Die Pulsfläche bestimmt θ , die Laserphase bestimmt ϕ .

Rechenbeispiel 3.1: Rabi-Oszillation und π -Puls

Ein resonantes Feld erzeuge $H = \frac{\hbar\Omega}{2}X$ mit Rabi-Frequenz $\Omega = 2\pi \times 100$ kHz. Aus Gleichungen (3.2) und (3.3) folgt $U(t) = R_x(\Omega t)$ und aus $|0\rangle$ wird

$$|\psi(t)\rangle = \cos \frac{\Omega t}{2} |0\rangle - i \sin \frac{\Omega t}{2} |1\rangle, \quad P_1(t) = \sin^2 \frac{\Omega t}{2} = \frac{1}{2}(1 - \cos \Omega t).$$

Ein π -Puls (vollständige Umkehr $|0\rangle \rightarrow -i|1\rangle$) dauert $t_\pi = \pi/\Omega = 5 \mu\text{s}$, ein $\pi/2$ -Puls (Superposition) $2,5 \mu\text{s}$. Das Hadamard-Gate ist bis auf eine globale Phase $H \doteq R_y(\pi/2)Z$ bzw. $\doteq R_x(\pi)R_y(\pi/2)$ – es ist also kein „eigenes“ physikalisches Gate, sondern eine Folge von Drehungen.

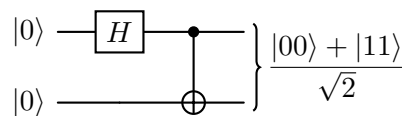
3.3 Zwei-Qubit-Gates

3.3.1 Das CNOT und seine Verwandten

Das *kontrollierte NOT* flippt das Ziel-Qubit, wenn das Kontroll-Qubit $|1\rangle$ ist:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \text{CZ} = \text{diag}(1, 1, 1, -1), \quad \text{CP}(\varphi) = \text{diag}(1, 1, 1, e^{i\varphi}). \quad (3.6)$$

Das kontrollierte Phasengatter $\text{CP}(\varphi)$ ist der Baustein der Quanten-Fourier-Transformation (Kapitel 11). Die klassische Bell-Schaltung erzeugt aus $|00\rangle$ mit einem Hadamard und einem CNOT den Zustand $|\Phi^+\rangle$:



3.3.2 Das Ising-Gate: die natürliche Sprache der Ionen

Ionen-Hardware erzeugt nicht direkt ein CNOT, sondern eine effektive Wechselwirkung der Form $H_{\text{eff}} = \hbar J X_1 X_2$ (Kapitel 9). Nach der Zeit t entsteht das *Ising-* oder *XX-Gate*¹

$$XX(\chi) = e^{-i\chi X_1 X_2} = \cos \chi \mathbb{I} - i \sin \chi X_1 X_2, \quad \chi = Jt. \quad (3.7)$$

¹Oft auch Mølmer-Sørensen-Gate $\text{MS}(\chi)$ genannt.

Rechenbeispiel 3.2: Ein verschränkendes Gate aus einem Hamiltonoperator

Mit Gleichung (3.7) und $\chi = \pi/4$ sowie $X_1 X_2 |00\rangle = |11\rangle$:

$$XX(\frac{\pi}{4}) |00\rangle = \frac{1}{\sqrt{2}}(|00\rangle - i|11\rangle).$$

Das ist maximal verschränkt (Kapitel 2). Beträgt die Kopplung $J = 2\pi \times 1 \text{ kHz}$, dauert das Gate $t_g = \chi/J = \pi/(4J) = 125 \text{ } \mu\text{s}$. Für $\chi = \pi/2$ erhält man $XX(\pi/2) = -iX_1 X_2$: zwei NOTs, keine Verschränkung. Verschränkung ist also eine Frage der *richtigen Gatezeit*.

3.3.3 Universalität

Merksatz

Beliebige Ein-Qubit-Drehungen zusammen mit *einem* verschränkenden Zwei-Qubit-Gate (z. B. CNOT oder $XX(\pi/4)$) sind *universell*: Jede unitäre Operation auf n Qubits lässt sich damit beliebig genau approximieren.

In Abschnitt 10.2 zeigen wir explizit, wie ein CNOT aus einem $XX(\pi/4)$ und vier Ein-Qubit-Drehungen zusammengesetzt wird, und wie man $\text{CP}(\varphi)$ erhält.

3.4 Kohärenz und Fidelity

Reale Qubits verlieren ihre Phaseninformation. Zwei Zeitskalen charakterisieren das:

- T_1 : Zeit, in der ein angeregter Zustand spontan in den Grundzustand zerfällt. Für Hyperfein- oder Zeeman-Qubits in Ionen praktisch unendlich (Stunden bis Jahre).
- T_2 : Zeit, in der die *relative Phase* zufällig wird (Dephasierung). Bei $^9\text{Be}^+$ in 3 T dominiert Magnetfeldrauschen, weil die Qubitfrequenz mit 28 GHz/T vom Feld abhängt (Kapitel 4).

Die Güte eines Gates misst man mit der *Fidelity* $F = |\langle \psi_{\text{ideal}} | \psi_{\text{real}} \rangle|^2$ bzw. $F = \langle \psi_{\text{ideal}} | \rho | \psi_{\text{ideal}} \rangle$ für gemischte Zustände.

Rechenbeispiel 3.3: Fehler multiplizieren sich

Ein Schaltkreis bestehe aus G Gates mit je Fidelity F . Grob ist die Gesamtfidelity $F^G \approx e^{-G(1-F)}$:

F	$G = 100$	$G = 1000$	$G = 10\,000$
0.99	0.366	4×10^{-5}	≈ 0
0.999	0.905	0.368	5×10^{-5}
0.9999	0.990	0.905	0.368

Der Shor-Algorithmus für kryptographisch relevante Zahlen braucht Milliarden von Gates – ohne Quantenfehlerkorrektur (Abschnitt 12.9) ist das aussichtslos.



Teil II

Die Hardware: Beryllium-Ionen in der Penning-Falle

Kapitel 4

Das ${}^9\text{Be}^+$ -Ion: Was ist der Quantenzustand wirklich?

In den Teilen I und IV sprechen wir abstrakt von $|0\rangle$ und $|1\rangle$. Dieses Kapitel beantwortet die Frage, die in populären Darstellungen fast immer übersprungen wird: *Welche physikalischen Zustände eines Beryllium-Ions sind das eigentlich?* Die kurze Antwort lautet: zwei Zeeman-Niveaus des elektronischen Grundzustands, die sich nur in der Orientierung des Elektronenspins relativ zum 3 T-Magnetfeld unterscheiden, während der Kernspin in beiden Zuständen gleich ausgerichtet ist. Die lange Antwort braucht etwas Atomphysik.

4.1 Aufbau des Ions

Beryllium hat die Kernladungszahl $Z = 4$. Das stabile Isotop ${}^9\text{Be}$ hat 4 Protonen und 5 Neutronen. Das einfach positive Ion ${}^9\text{Be}^+$ hat drei Elektronen in der Konfiguration $1s^2 2s$. Die beiden $1s$ -Elektronen bilden eine abgeschlossene Schale mit Gesamtdrehimpuls null; das Ion verhält sich deshalb wie ein „Wasserstoffatom mit einem Valenzelektron“ im $2s$ -Orbital. Es besitzt drei Drehimpulse:

Drehimpuls	Quantenzahl	Wert im Grundzustand $2s^2 S_{1/2}$
Bahndrehimpuls des Valenzelektrons $\mathbf{L}$	L	0 (s -Orbital)
Elektronenspin $\mathbf{S}$	S	$1/2$
elektronischer Gesamtdrehimpuls $\mathbf{J} = \mathbf{L} + \mathbf{S}$	J	$1/2$
Kernspin $\mathbf{I}$	I	$3/2$

Die Termbezeichnung ${}^{2S+1}L_J = {}^2S_{1/2}$ sagt: Dublett ($2S + 1 = 2$), $L = 0$ (Buchstabe S), $J = 1/2$. Der Grundzustand ist also nicht *ein* Zustand, sondern ein Unterraum der Dimension $(2J + 1)(2I + 1) = 2 \cdot 4 = 8$, aufgespannt durch die Produktbasis

$$|m_J, m_I\rangle, \quad m_J \in \{\pm \tfrac{1}{2}\}, \quad m_I \in \{\pm \tfrac{3}{2}, \pm \tfrac{1}{2}\}. \quad (4.1)$$

Welche Linearkombinationen davon Energieeigenzustände sind, hängt vom Magnetfeld ab.

4.2 Der Hamiltonoperator des Grundzustands

Zwei Effekte bestimmen die Energien der acht Zustände:

$$\frac{H}{h} = \underbrace{A \mathbf{I} \cdot \mathbf{J}}_{\text{Hyperfein}} + \underbrace{\frac{\mu_B B}{h} (g_J J_z + g_I I_z)}_{\text{Zeeman}}, \quad (4.2)$$

mit

- der Hyperfeinkonstanten $A = -625,009 \text{ MHz}$ (die Wechselwirkung des Elektronenspins mit dem magnetischen Moment des Kerns; negativ, weil das Kernmoment von ^9Be negativ ist, $\mu_I = -1.1775 \mu_N$),
- dem Elektronen- g -Faktor $g_J = 2.00226$ und $\mu_B/h = 13,996 \text{ GHz/T}$,
- dem (winzigen) Kern- g -Faktor $g_I = -\mu_I/(I\mu_B) = 4.28 \times 10^{-4}$ in der Konvention von Gleichung (4.2).

Gleichung (4.2) ist eine hermitesche 8×8 -Matrix. Man kann sie in wenigen Zeilen Python aufstellen und diagonalisieren (`code/k1_beryllium_niveaus.py`): Die Spinoperatoren $J_{x,y,z}$ (2×2) und $I_{x,y,z}$ (4×4) werden per Kronecker-Produkt kombiniert, $\mathbf{I} \cdot \mathbf{J} = \sum_{\mu} J_{\mu} \otimes I_{\mu}$.

4.2.1 Schwaches Feld: Hyperfeinniveaus $F = 1$ und $F = 2$

Ohne Magnetfeld koppeln $\mathbf{I}$ und $\mathbf{J}$ zum Gesamtdrehimpuls $\mathbf{F} = \mathbf{I} + \mathbf{J}$ mit $F \in \{1, 2\}$. Wegen $\mathbf{I} \cdot \mathbf{J} = \frac{1}{2}[\mathbf{F}^2 - \mathbf{I}^2 - \mathbf{J}^2]$ ist

$$E_F/h = \frac{A}{2} [F(F+1) - I(I+1) - J(J+1)]. \quad (4.3)$$

Rechenbeispiel 4.1: Hyperfeinaufspaltung von $^9\text{Be}^+$

Mit $I(I+1) = \frac{15}{4}$, $J(J+1) = \frac{3}{4}$: $E_{F=2}/h = \frac{A}{2}(6 - \frac{15}{4} - \frac{3}{4}) = \frac{3}{4}A = -468,76 \text{ MHz}$ (fünf-fach entartet), $E_{F=1}/h = \frac{A}{2}(2 - \frac{15}{4} - \frac{3}{4}) = -\frac{5}{4}A = 781,26 \text{ MHz}$ (dreifach entartet). Die Aufspaltung beträgt $2|A| = 1,250 \text{ GHz}$. Wegen $A < 0$ liegt $F = 2$ *unter* $F = 1$ („invertierte“ Hyperfeinstruktur). Die numerische Diagonalisierung bei $B = 0$ reproduziert genau diese Werte.

In Paul-Fallen (Radiofrequenzfallen) mit kleinen Feldern von einigen mT verwendet man häufig Qubits aus $F = 1$ - und $F = 2$ -Zuständen. In der Penning-Falle ist die Situation völlig anders.

4.2.2 Starkes Feld: Paschen–Back–Regime

Die Zeeman-Energie des Elektrons beträgt bei $B = 3 \text{ T}$

$$g_J \mu_B B/h = 2.00226 \times 13,996 \text{ GHz/T} \times 3 \text{ T} = 84,07 \text{ GHz} \gg |A| = 0,625 \text{ GHz}.$$

Der Elektronenspin richtet sich nach dem äusseren Feld aus, nicht mehr nach dem Kern; $\mathbf{I}$ und $\mathbf{J}$ *entkoppeln*. Die Energieeigenzustände sind dann in sehr guter Näherung die Produktzustände

$|m_J, m_I\rangle$, und in erster Ordnung Störungstheorie (nur der Anteil $A I_z J_z$ der Hyperfeinkopplung trägt bei) gilt

$$\frac{E(m_J, m_I)}{h} \approx g_J \frac{\mu_B B}{h} m_J + A m_J m_I + g_I \frac{\mu_B B}{h} m_I. \quad (4.4)$$

Die acht Niveaus bilden zwei Gruppen von je vier, getrennt durch rund 83 GHz (Abb. 4.1). Die numerische Rechnung zeigt, dass die Eigenvektoren bei 3 T zu mehr als 99,99 % aus einem einzigen Produktzustand bestehen.

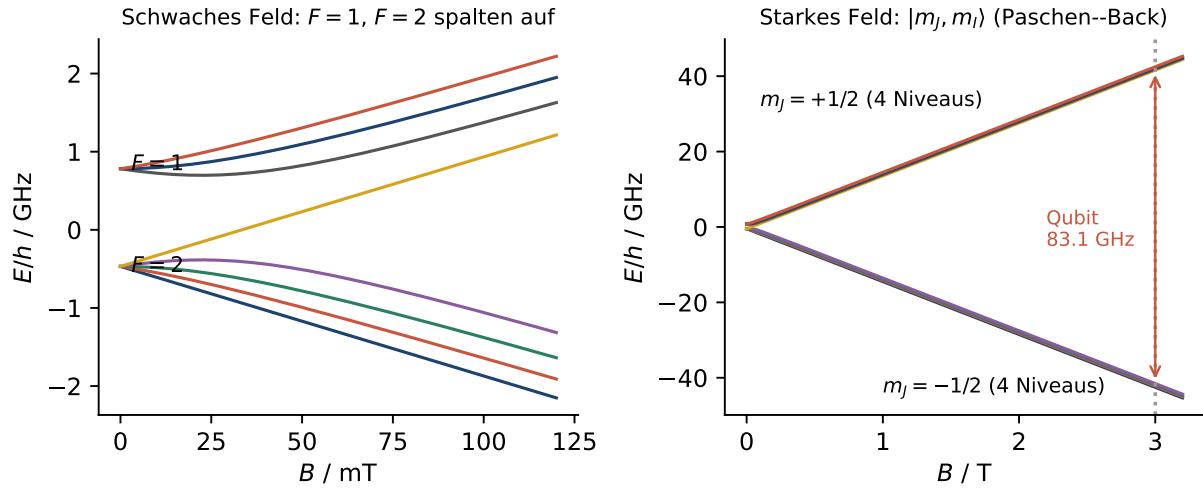


Abbildung 4.1: Exakte Eigenwerte von Gleichung (4.2) („Breit–Rabi-Diagramm“) für den Grundzustand von $^9\text{Be}^+$. Links: Übergang vom Hyperfein-Regime ($F = 1, 2$) ins Paschen–Back-Regime bei einigen zehn mT. Rechts: bei 3 T ist das Spektrum in zwei Gruppen $m_J = \pm \frac{1}{2}$ mit je vier fast parallelen Niveaus (m_I) aufgespalten. Der Pfeil markiert den Qubit-Übergang.

4.3 Das Qubit

ETH und ZuriQ verwenden die beiden Zustände [1]

$$|\uparrow\rangle \equiv \left| m_J = +\frac{1}{2}, m_I = +\frac{3}{2} \right\rangle, \quad |\downarrow\rangle \equiv \left| m_J = -\frac{1}{2}, m_I = +\frac{3}{2} \right\rangle \quad (4.5)$$

Der Kernspin ist in beiden Zuständen gleich (maximal) ausgerichtet; die Qubit-Operation ist ein *reiner Umlapp des Elektronenspins*. Deshalb spricht man von einem *Elektronenspin-Qubit*. Wir identifizieren im ganzen Skript

$$|0\rangle \equiv |\uparrow\rangle \text{ (hell, initialisiert)}, \quad |1\rangle \equiv |\downarrow\rangle \text{ (dunkel)}. \quad (4.6)$$

(Beachten Sie: $|\uparrow\rangle$ ist der energetisch *höhere* Zustand, denn das magnetische Moment des Elektrons ist seinem Spin entgegengerichtet. Die Zuordnung zu 0 und 1 ist Konvention; wir wählen sie so, dass der initialisierte Zustand $|0\rangle$ ist.)

Rechenbeispiel 4.2: Qubitfrequenz bei 3 T

Aus Gleichung (4.4) mit $m_I = +\frac{3}{2}$:

$$E_{\uparrow}/h \approx +\frac{1}{2} \cdot 84.070 + (-0.625) \cdot \frac{1}{2} \cdot \frac{3}{2} + 0.0269 = 41,593 \text{ GHz},$$

$$E_{\downarrow}/h \approx -\frac{1}{2} \cdot 84.070 - (-0.625) \cdot \frac{1}{2} \cdot \frac{3}{2} + 0.0269 = -41,539 \text{ GHz},$$

also $\nu_0 = (E_{\uparrow} - E_{\downarrow})/h \approx g_J \mu_B B/h + A m_I = 84.070 - 0.9375 = 83,13 \text{ GHz}$. Die exakte Diagonalisierung liefert 83,138 GHz (die Differenz ist die zweite Ordnung in $A/(g_J \mu_B B)$). Jain et al. berichten $\nu_0 \simeq 83,2 \text{ GHz}$ [1]; das entspricht nach unserer Rechnung einem Feld von $B = 3,002 \text{ T}$. Zum Vergleich: Die NIST-Penning-Experimente bei 4,46 T verwenden denselben Übergang bei 124 GHz; unser Programm liefert dafür 124,02 GHz.

4.3.1 Die Achillesferse: Magnetfeldempfindlichkeit

Aus Gleichung (4.4) folgt $\partial \nu_0 / \partial B \approx g_J \mu_B / h = 28,02 \text{ GHz/T}$. Das Qubit ist ein exzellentes Magnetometer – und damit empfindlich für jedes Magnetfeldrauschen.

Rechenbeispiel 4.3: Welche Feldstabilität braucht man?

Soll die Qubit-Phase in $\tau = 1 \text{ ms}$ um weniger als 1 rad driften, muss $2\pi \delta \nu \tau < 1$, also $\delta \nu < 159 \text{ Hz}$ sein. Das entspricht $\delta B < 159 \text{ Hz} / (28 \text{ GHz/T}) = 5,7 \text{ nT}$, relativ zu 3 T also $\delta B/B < 2 \times 10^{-9}$. Selbst ein supraleitender Magnet im Dauerstrombetrieb schafft das nicht über lange Zeiten. Deshalb misst man ohne Gegenmassnahmen eine Ramsey-Kohärenzzeit von nur $\approx 1,9 \text{ ms}$; mit einem einzigen Spin-Echo-Puls, der langsame Drifts herausmittelt, steigt sie auf $\approx 240 \text{ ms}$ [1].

4.4 Optische Übergänge: Initialisieren und Auslesen

Neben den acht Grundzustandsniveaus braucht man angeregte Zustände. Der wichtigste ist $2p^2P_{3/2}$, erreichbar mit ultravioletttem Licht der Wellenlänge $\lambda = 313 \text{ nm}$ (Frequenz $c/\lambda \approx 958 \text{ THz}$), mit einer natürlichen Linienbreite $\Gamma = 2\pi \times 19,4 \text{ MHz}$ (Lebensdauer 8,2 ns).

Initialisierung durch optisches Pumpen. Zirkular polarisiertes (σ^+) Licht pumpt den Elektronenspin in $m_J = +\frac{1}{2}$: Ein Ion in $m_J = -\frac{1}{2}$ wird angeregt und zerfällt mit gewisser Wahrscheinlichkeit nach $m_J = +\frac{1}{2}$, von wo es nicht mehr angeregt wird. Im Paschen-Back-Regime ändern optische Übergänge aber in guter Näherung nur m_J , nicht m_I . Um auch den Kernspin in $m_I = +\frac{3}{2}$ zu bringen, braucht es zusätzliche *Rückpump*-Felder, die die schwache Hyperfeinmischung (vor allem im angeregten Zustand) ausnutzen, um m_I schrittweise zu erhöhen. Am Ende sitzt das Ion im „gestreckten“ Zustand $|m_J = +\frac{1}{2}, m_I = +\frac{3}{2}\rangle = |\uparrow\rangle$, aus dem es nicht mehr heraus gepumpt wird. So wird $|0\rangle$ mit hoher Wahrscheinlichkeit präpariert. (Die genaue Pumpsequenz ist experimentabhängig.)

Auslese durch zustandsabhängige Fluoreszenz. Der Laser treibt den Übergang von $|\uparrow\rangle$ in den angeregten Zustand $^2P_{3/2} |m_J = +\frac{3}{2}, m_I = +\frac{3}{2}\rangle$; dieser Zustand kann aus Drehimpulsgründen nur wieder nach $|\uparrow\rangle$ zerfallen. Ein Ion in $|\uparrow\rangle$ streut deshalb Millionen Photonen pro Sekunde

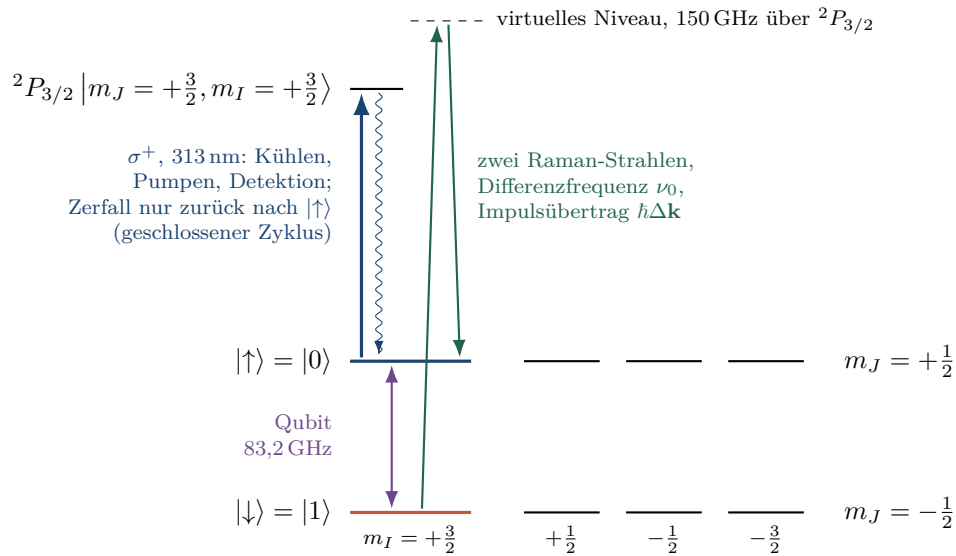


Abbildung 4.2: Vereinfachtes Niveauschema von ${}^9\text{Be}^+$ bei 3 T (nicht massstäblich). Das Qubit besteht aus den beiden Zuständen mit $m_I = +\frac{3}{2}$. Ein zirkular polarisierter Laser treibt den geschlossenen Zyklus $|\uparrow\rangle \leftrightarrow {}^2P_{3/2}$; $|\downarrow\rangle$ ist um 83 GHz verstimmt und bleibt dunkel. Zwei Raman-Strahlen mit Frequenzdifferenz ν_0 treiben den Qubit-Übergang und übertragen dabei einen Impuls $\hbar\Delta\mathbf{k}$ auf das Ion.

(„hell“, ein Ion in $|\downarrow\rangle$ fast keine („dunkel“). Die statistische Behandlung dieser Messung folgt in Abschnitt 10.4.

Qubit-Manipulation. Es gibt zwei Möglichkeiten:

1. *Mikrowellen* bei 83 GHz (Wellenlänge 3,6 mm) treiben den Übergang direkt. Weil die Wellenlänge riesig gegenüber der Bewegungsamplitude des Ions ist, koppeln sie praktisch nicht an die Bewegung (siehe Abschnitt 7.3). Gut für Ein-Qubit-Gates.
2. *Stimulierte Raman-Übergänge* mit zwei phasenstarr gekoppelten 313 nm-Strahlen, die etwa 150 GHz oberhalb von ${}^2P_{3/2}$ verstimmt sind und deren Frequenzdifferenz ν_0 beträgt [1]. Das Ion absorbiert ein Photon aus Strahl 1 und emittiert stimuliert eines in Strahl 2; das virtuelle Niveau wird dabei kaum besetzt. Weil die Wellenvektoren verschieden sind, erhält das Ion einen Impulsübertrag $\hbar\Delta\mathbf{k} = \hbar(\mathbf{k}_1 - \mathbf{k}_2)$. Genau dieser Impulsübertrag koppelt Qubit und Bewegung – die Grundlage aller Zwei-Qubit-Gates (Kapitel 8).

4.5 Innerer Zustand versus Bewegung

Ein Ion hat zwei völlig verschiedene Sorten von Freiheitsgraden:

$$|\text{Ion}\rangle = \underbrace{|\text{innerer Zustand}\rangle}_{|\uparrow\rangle, |\downarrow\rangle} \otimes \underbrace{|\text{Bewegung des Schwerpunkts}\rangle}_{|n_z, n_+, n_-\rangle}. \quad (4.7)$$

Der innere Zustand trägt die Quanteninformation. Die Bewegung des *ganzen Ions* in der Falle ist quantisiert (Kapitel 6); ihre Quanten heissen Phononen. Laser koppeln beide Freiheitsgrade. Die folgende Tabelle ordnet die Energieskalen, mit denen wir es zu tun haben:



Prozess	Grösse	typischer Wert
optischer Übergang ${}^2S_{1/2} \leftrightarrow {}^2P_{3/2}$	c/λ	958 THz
Raman-Verstimmung	$\Delta/2\pi$	150 GHz
Qubit (Elektronenspin im Feld)	ν_0	83,2 GHz
Hyperfeinkopplung	$2 A $	1,25 GHz
Zyklotronbewegung	ν_+	4,4 MHz
axiale Bewegung	ν_z	2,5 MHz
Magnetronbewegung	ν_-	0,71 MHz
Rabi-Frequenzen, Seitenbänder	$\Omega/2\pi, \eta\Omega/2\pi$	1 kHz – 1 MHz
Coulomb-Kopplung zwischen Mikrofallen	$t_{ij}/2\pi$	0,1 kHz – 10 kHz

Diese Hierarchie über zwölf Grössenordnungen ist der Grund, warum man die verschiedenen Freiheitsgrade getrennt modellieren und durch Frequenzwahl gezielt adressieren kann.

Kapitel 5

Die Penning-Falle

5.1 Warum man ein Magnetfeld braucht

Kann man ein Ion allein mit statischen elektrischen Feldern festhalten? Nein. Im ladungsfreien Raum erfüllt das elektrostatische Potential die Laplace-Gleichung $\nabla^2\Phi = 0$. Ein Minimum der potentiellen Energie $q\Phi$ in allen drei Richtungen würde $\partial_x^2\Phi, \partial_y^2\Phi, \partial_z^2\Phi > 0$ verlangen – deren Summe wäre positiv, im Widerspruch zu $\nabla^2\Phi = 0$ (*Earnshaw-Theorem*). Ein statisches Potential hat bestenfalls einen *Sattelpunkt*. Es gibt zwei Auswege:

- **Paul-Falle:** Ein schnell oszillierendes Radiofrequenzfeld (typ. 20 MHz bis 100 MHz, einige 100 V) erzeugt ein zeitgemittelttes effektives Potential. So funktionieren die meisten heutigen Ionen-Quantencomputer.
- **Penning-Falle:** Ein statisches Quadrupolpotential schliesst das Ion entlang einer Achse ein, ein starkes homogenes Magnetfeld entlang derselben Achse zwingt es in der Ebene senkrecht dazu auf Kreisbahnen.

Die Penning-Falle kommt ohne Hochfrequenz aus: keine hohen Wechselspannungen auf dem Chip, keine Verlustleistung durch RF-Ströme und – für ZuriQ entscheidend – keine Einschränkung, wo Fallen entstehen können. Paul-Fallen haben nur entlang einer „RF-Nulllinie“ feldfreie Punkte; in einer Penning-Falle kann man eine Potentialmulde mit statischen Spannungen *überall* über dem Chip formen [2, 1].

5.2 Das ideale Quadrupolpotential

Wir legen das Magnetfeld entlang z , $\mathbf{B} = B\mathbf{e}_z$, und wählen das Potential

$$\Phi(x, y, z) = \frac{V_0}{2d^2} \left(z^2 - \frac{x^2 + y^2}{2} \right). \quad (5.1)$$

Es erfüllt $\nabla^2\Phi = 0$ und ist für ein positives Ion ($qV_0 > 0$) entlang z einschliessend, in der xy -Ebene aber *abstossend*. Die Bewegungsgleichung (Lorentzkraft) lautet

$$m\ddot{\mathbf{r}} = q(-\nabla\Phi + \dot{\mathbf{r}} \times \mathbf{B}). \quad (5.2)$$

5.2.1 Axiale Bewegung

In z -Richtung wirkt keine magnetische Kraft ($\dot{\mathbf{r}} \times \mathbf{B}$ hat keine z -Komponente). Es bleibt ein harmonischer Oszillator:

$$\ddot{z} + \omega_z^2 z = 0, \quad \omega_z^2 = \frac{qV_0}{md^2}. \quad (5.3)$$

5.2.2 Radiale Bewegung

In der Ebene gilt mit der freien Zyklotronfrequenz $\omega_c = qB/m$

$$\ddot{x} = \frac{\omega_z^2}{2}x + \omega_c \dot{y}, \quad \ddot{y} = \frac{\omega_z^2}{2}y - \omega_c \dot{x}. \quad (5.4)$$

Der Trick ist die komplexe Koordinate $w = x + iy$. Dann wird aus zwei gekoppelten Gleichungen eine einzige:

$$\ddot{w} = \frac{\omega_z^2}{2}w - i\omega_c \dot{w}. \quad (5.5)$$

Mit dem Ansatz $w = e^{-i\omega t}$ folgt die quadratische Gleichung $\omega^2 - \omega_c \omega + \frac{1}{2}\omega_z^2 = 0$ mit den Lösungen

$$\omega_{\pm} = \frac{1}{2}(\omega_c \pm \sqrt{\omega_c^2 - 2\omega_z^2}) \quad (5.6)$$

Die radiale Bewegung ist die Überlagerung zweier Kreisbewegungen: der schnellen *modifizierten Zyklotronbewegung* ω_+ und der langsamen *Magnetronbewegung* ω_- (einer $\mathbf{E} \times \mathbf{B}$ -Drift um das Fallenzentrum). Reelle Frequenzen, also Stabilität, verlangen

$$\omega_c^2 > 2\omega_z^2 \iff \nu_z < \nu_c/\sqrt{2}. \quad (5.7)$$

Aus Gleichung (5.6) folgen die nützlichen Identitäten $\omega_+ + \omega_- = \omega_c$, $2\omega_+\omega_- = \omega_z^2$ und $\omega_+^2 + \omega_-^2 = \omega_c^2$ (*Invarianztheorem* von Brown und Gabrielse [5]).

Rechenbeispiel 5.1: Die drei Eigenfrequenzen eines $^9\text{Be}^+$ -Ions bei 3 T

Masse $m = 9.01219 u - m_e = 1,496\,42 \cdot 10^{-26} \text{ kg}$, Ladung $q = e$.

$$\nu_c = \frac{eB}{2\pi m} = \frac{1,602 \cdot 10^{-19} \text{ C} \cdot 3 \text{ T}}{2\pi \cdot 1,496\,4 \cdot 10^{-26} \text{ kg}} = 5,112 \text{ MHz}, \quad \nu_z < \nu_c/\sqrt{2} = 3,615 \text{ MHz}.$$

Mit $\nu_z = 2,5 \text{ MHz}$ (dem Wert aus [1]):

$$\begin{aligned} \nu_{\pm} &= \frac{1}{2}(5,112 \pm \sqrt{5,112^2 - 2 \cdot 2,5^2}) \text{ MHz} = \frac{1}{2}(5,112 \pm 3,692) \text{ MHz} \\ &\Rightarrow \nu_+ = 4,402 \text{ MHz}, \quad \nu_- = 0,710 \text{ MHz}. \end{aligned}$$

Das Experiment misst $\nu_+ \simeq 4,41 \text{ MHz}$ und $\nu_- \simeq 0,71 \text{ MHz}$ [1]. Kontrolle: $\nu_+ + \nu_- = 5,112 \text{ MHz} = \nu_c$ und $2\nu_+\nu_- = 6,25 \text{ MHz}^2 = \nu_z^2$. ✓

Die Magnetronbewegung hat negative Energie

Das Potential ist radial abstossend. Beim Magnetronkreis überwiegt die potentielle Energie: Vergrössert sich der Radius, *sinkt* die Gesamtenergie. Die Bewegung ist daher nur *metastabil*; jede Reibung (etwa durch Laserkühlung) würde den Radius vergrössern, bis das Ion verloren ist. Man kühlt die Magnetronmode deshalb durch Kopplung an eine andere Mode oder mit spezi-

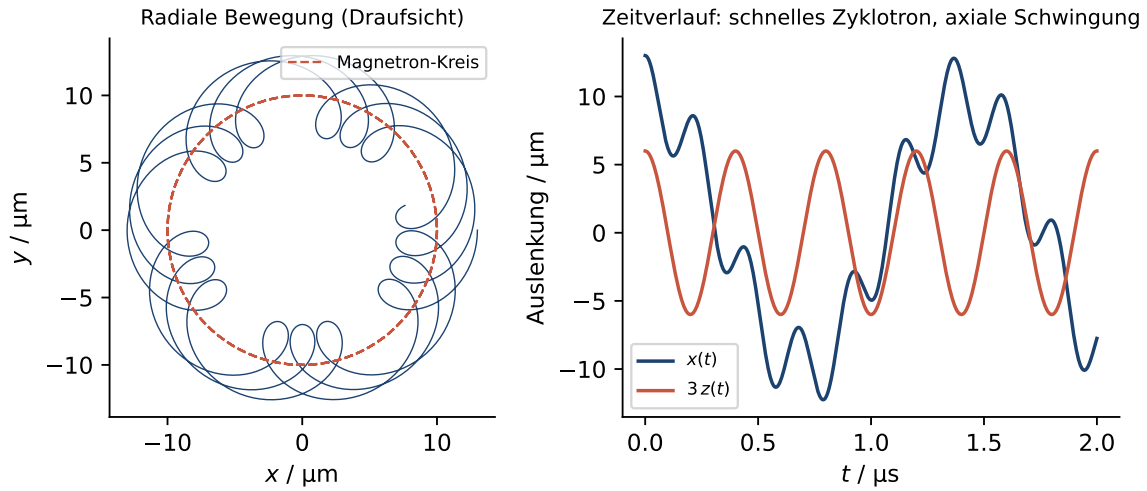


Abbildung 5.1: Numerisch integrierte Bahn eines ${}^9\text{Be}^+$ -Ions bei 3 T, $\nu_z = 2,5\text{ MHz}$ (Magnetronradius $10\text{ }\mu\text{m}$, Zyklotronradius $3\text{ }\mu\text{m}$). Links: In der Draufsicht läuft die schnelle Zyklotronschleife auf dem langsamen Magnetronkreis (Epizykel). Rechts: Zeitverlauf. Programm: `code/k2_penning_falle.py`.

ellen Laserschemata. Quantenmechanisch lautet ihr Hamiltonoperator $H_- = -\hbar\omega_-(a_-^\dagger a_- + \frac{1}{2})$ – mit Minuszeichen. Trotzdem wurde die Magnetronmode in der Mikrofalle auf $\bar{n}_- = 0.03$ gekühlt [1].

5.3 Von der Linearisierung zum Eigenwertproblem

Für spätere Kapitel lohnt es sich, die radiale Bewegung als lineares System zu schreiben. Mit $\mathbf{u} = (x, y)^T$:

$$M\ddot{\mathbf{u}} + G\dot{\mathbf{u}} + K\mathbf{u} = 0, \quad M = m\mathbb{I}, \quad G = qB \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = -\frac{1}{2}m\omega_z^2\mathbb{I}. \quad (5.8)$$

G ist antisymmetrisch (geschwindigkeitsabhängige, keine Arbeit leistende Kraft), K ist *negativ* definit (Sattel). Mit $\mathbf{u} = \mathbf{b}e^{-i\omega t}$ wird daraus das *quadratische* Eigenwertproblem

$$(K - \omega^2 M - i\omega G)\mathbf{b} = 0. \quad (5.9)$$

Numerisch löst man es, indem man $(\mathbf{u}, \dot{\mathbf{u}})$ als Zustandsvektor der Dimension $2 \cdot 2$ nimmt und die Matrix erster Ordnung diagonalisiert; das Programm liefert genau $\nu_\pm$. Für N Ionen in einer Falle wird das zu einem $4N$ -dimensionalen Problem. Die *axialen* Moden (entlang $\mathbf{B}$) sind dagegen frei von Lorentzkraften und führen auf ein gewöhnliches symmetrisches Eigenwertproblem $K\mathbf{b} = m\omega^2\mathbf{b}$ – deshalb verwenden wir sie in Kapitel 7 als Hauptbeispiel.

5.4 Die Mikro-Penning-Falle von ETH und ZuriQ

Statt hyperbolischer Elektroden verwendet die ETH-Gruppe von Jonathan Home einen *planaren*, mikrostrukturierten Chip mit vielen einzeln ansteuerbaren Gleichspannungselektroden in einem 3 T-Feld eines supraleitenden Magneten, bei kryogenen Temperaturen [1]. Die Elektrodenspannungen

formen eine lokale Potentialmulde, in der das Ion $152\text{ }\mu\text{m}$ über der Chipoberfläche gefangen ist (Abb. 5.2).

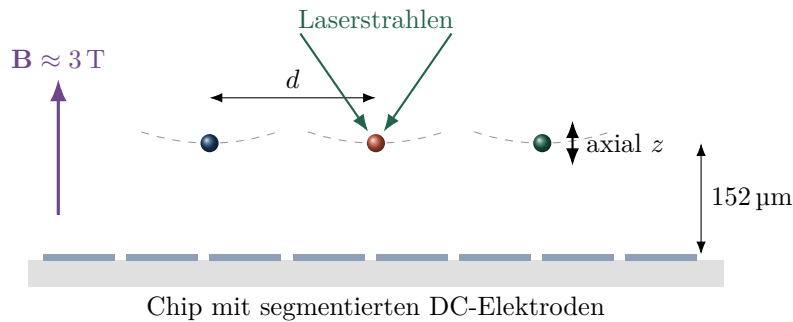


Abbildung 5.2: Schema einer Anordnung einzelner Ionen in Mikro-Penning-Fallen (nicht massstäblich). Jede Fallenposition wird durch die Spannungen der Elektroden darunter bestimmt; durch zeitliche Änderung der Spannungen lässt sich ein Ion in der Ebene transportieren. Das Magnetfeld steht (idealisiert) senkrecht zum Chip; die axiale Bewegung ist die Schwingung senkrecht zur Chipoberfläche.

Zentrale publizierte Resultate [1]:

- volle Quantenkontrolle eines Ions: Ein-Qubit-Gates, Kopplung von Spin und Bewegung, Grundzustandskühlung aller drei Moden auf $\{\bar{n}_+, \bar{n}_-, \bar{n}_z\} = \{0.05, 0.03, 0.007\}$;
- Heizraten $\{\dot{n}_+, \dot{n}_-, \dot{n}_z\} = \{0.49, 3.8, 0.088\}\text{ s}^{-1}$ – sehr klein: Die axiale Mode nimmt im Mittel weniger als ein Phonon in zehn Sekunden auf;
- Transport des Ions in beliebigen Richtungen in der Ebene über dem Chip (in 4 ms zu einer neuen Position), ohne messbare Anregung der Bewegung.

ZuriQ berichtet (Stand Juli 2026), auf dieser Grundlage ein 3×3 -Array aus neun einzeln kontrollierten Ionen in einer nativ zweidimensionalen Anordnung demonstriert zu haben; die Chips werden in Zusammenarbeit mit Infineon industriell gefertigt [3].

Zwei Arten von 2D-Penning-Systemen

Seit Jahrzehnten gibt es Penning-Fallen, in denen hunderte $^9\text{Be}^+$ -Ionen einen gemeinsamen, rotierenden, zweidimensionalen Coulomb-Kristall bilden (NIST, [13]). ZuriQ verfolgt ein anderes Konzept: *einzelne* Ionen in *getrennten* lokalen Potentialmulden, die individuell positioniert werden können und nicht kollektiv rotieren. In beiden Fällen koppelt die Coulomb-Kraft die Bewegungen – aber Gleichgewicht, Modenspektrum, Adressierung und Transport unterscheiden sich. Kapitel 7 behandelt beide Fälle.

Kapitel 6

Quantisierte Bewegung: Phononen

6.1 Der quantenmechanische harmonische Oszillator

Jede Eigenmode der Ionenbewegung ist – in harmonischer Näherung – ein harmonischer Oszillator

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 z^2. \quad (6.1)$$

Quantenmechanisch sind Ort z und Impuls p Operatoren mit $[z, p] = i\hbar$. Man führt den *Vernichter* a und den *Erzeuger* $a^\dagger$ ein:

$$z = z_0 (a + a^\dagger), \quad p = i \frac{\hbar}{2z_0} (a^\dagger - a), \quad z_0 = \sqrt{\frac{\hbar}{2m\omega}}, \quad [a, a^\dagger] = 1. \quad (6.2)$$

Dann ist

$$H = \hbar\omega \left(a^\dagger a + \frac{1}{2} \right), \quad E_n = \hbar\omega \left(n + \frac{1}{2} \right), \quad n = 0, 1, 2, \dots \quad (6.3)$$

Die Eigenzustände $|n\rangle$ (*Fock-Zustände*) sind äquidistant; $a^\dagger a |n\rangle = n |n\rangle$ zählt die Quanten. Ein solches Schwingungsquant einer mechanischen Mode heisst *Phonon*. Die Leiteroperatoren wirken wie

$$a |n\rangle = \sqrt{n} |n-1\rangle, \quad a^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle. \quad (6.4)$$

In einer endlichen Basis $\{|0\rangle, \dots, |n_{\max}-1\rangle\}$ ist a eine Matrix mit $\sqrt{1}, \sqrt{2}, \dots$ auf der oberen Nebendiagonalen – so simulieren wir in Kapitel 9 Qubits und Phononen gemeinsam.

Rechenbeispiel 6.1: Wie gross ist ein Ion im Grundzustand?

Die Ortsunschärfe im Grundzustand ist $\Delta z = z_0$. Für ${}^9\text{Be}^+$ bei $\nu_z = 2,5 \text{ MHz}$:

$$z_0 = \sqrt{\frac{1,0546 \cdot 10^{-34} \text{ Js}}{2 \cdot 1,4964 \cdot 10^{-26} \text{ kg} \cdot 2\pi \cdot 2,5 \cdot 10^6 \text{ s}^{-1}}} = 15,0 \text{ nm}.$$

Das Ion ist also „verschmiert“ über rund 15 nm – etwa zwanzigmal kleiner als die Laserwellenlänge von 313 nm, aber rund 300-mal grösser als ein Atom. Bei $\nu_z = 1 \text{ MHz}$ wird $z_0 = 23,7 \text{ nm}$.

Phonon $\neq$ Teilchen, das zum Ion gehört

Ein Phonon ist ein Energiequant einer *Mode*. Bei einem einzelnen Ion gehört die Mode diesem Ion. Bei mehreren gekoppelten Ionen ist eine Mode eine *kollektive* Bewegung (Kapitel 7); ein Phonon in der Schwerpunktmode „gehört“ allen Ionen gleichzeitig. Genau diese Nichtlokalität macht die Bewegung zum Datenbus zwischen Qubits.

6.2 Drei Oszillatoren pro Ion in der Penning-Falle

Ein Ion in der Penning-Falle hat drei Moden, also

$$H_{\text{mot}} = \hbar\omega_z(a_z^\dagger a_z + \frac{1}{2}) + \hbar\omega_+(a_+^\dagger a_+ + \frac{1}{2}) - \hbar\omega_-(a_-^\dagger a_- + \frac{1}{2}). \quad (6.5)$$

Das Minuszeichen der Magnetronmode (Kapitel 5) bedeutet: Ein zusätzliches Magnetron-Phonon *senkt* die Energie.

6.3 Thermische Zustände

Ist eine Mode im thermischen Gleichgewicht bei Temperatur T , sind die Fock-Zustände geometrisch verteilt:

$$P(n) = \frac{\bar{n}^n}{(\bar{n} + 1)^{n+1}}, \quad \bar{n} = \frac{1}{e^{\hbar\omega/k_B T} - 1}. \quad (6.6)$$

Data-Science-Brille

Gleichung (6.6) ist eine geometrische Verteilung mit Erfolgswahrscheinlichkeit $1/(\bar{n} + 1)$. Die Grundzustandswahrscheinlichkeit ist $P(0) = 1/(\bar{n} + 1)$. Das *Verhältnis* benachbarter Wahrscheinlichkeiten $P(n + 1)/P(n) = \bar{n}/(\bar{n} + 1)$ ist konstant – das nutzt man, um $\bar{n}$ aus Seitenbandmessungen zu schätzen (Abschnitt 8.3).

Rechenbeispiel 6.2: Wie kalt muss es sein?

1. *Kryostat bei 4 K*: $k_B T / (\hbar\omega_z) = 5,52 \cdot 10^{-23} \text{ J} / 1,657 \cdot 10^{-27} \text{ J} \approx 3.3 \times 10^4$. Ohne Laserkühlung schwingt das Ion also mit über 30 000 Phononen.
2. *Doppler-Kühlung* am 313 nm-Übergang erreicht $T_D = \hbar\Gamma/(2k_B) = 0,47 \text{ mK}$. Das ergibt bei 2,5 MHz $\bar{n} \approx 3.4$ – noch zu warm für präzise Gates.
3. *Seitenbandkühlung* (Kapitel 8) entfernt gezielt Phononen: Im Experiment wurde $\bar{n}_z = 0.007$ erreicht [1], also $P(0) = 1/1.007 = 99,3\%$ im Grundzustand.

6.4 Kohärente Zustände und Verschiebungen

Eine konstante Kraft F auf einen Oszillator verschiebt seine Ruhelage. Quantenmechanisch erzeugt eine resonante Kraft aus $|0\rangle$ einen *kohärenten Zustand* $|\alpha\rangle = D(\alpha)|0\rangle$ mit dem Verschiebungsoperator

$$D(\alpha) = \exp(\alpha a^\dagger - \alpha^* a), \quad \langle z \rangle = 2z_0 \text{Re } \alpha, \quad \langle p \rangle = \frac{\hbar}{z_0} \text{Im } \alpha. \quad (6.7)$$

Die komplexe Zahl α ist also ein Punkt im *Phasenraum* (Ort, Impuls). Die wichtigste Eigenschaft für die Gates in Kapitel 9:

$$D(\beta)D(\alpha) = e^{i\text{Im}(\beta\alpha^*)} D(\alpha + \beta). \quad (6.8)$$

Zwei Verschiebungen hintereinander ergeben wieder eine Verschiebung – aber mit einer zusätzlichen *Phase*. Läuft man im Phasenraum eine geschlossene Schleife, kehrt der Oszillator in seinen Ausgangszustand zurück, und es bleibt nur eine Phase übrig, die gleich der doppelten eingeschlossenen Fläche ist. Wenn die Kraft vom Qubit-Zustand abhängt, hängt auch diese Phase vom Qubit-Zustand ab – das ist der ganze Trick des geometrischen Phasengates.



Teil III

Phonon-Kopplung und Verschränkung dreier Ionen

Kapitel 7

Drei gekoppelte Ionen in harmonischer Näherung

Dieses Kapitel ist das mathematische Herzstück. Wir berechnen explizit, wie die Coulomb-Abstossung die Bewegungen dreier Ionen koppelt, welche kollektiven Eigenmoden daraus entstehen und wie diese quantisiert werden. Wir behandeln zwei Modelle:

Modell A Drei Ionen bilden in *einer* Falle eine lineare Kette entlang der Magnetfeldachse. Die Coulomb-Kraft bestimmt dann sowohl die Gleichgewichtslagen als auch die Kopplung. Das ist der Lehrbuchfall (in Penning-Fallen experimentell realisiert [6], in Paul-Fallen der Standard).

Modell B Drei Ionen sitzen in *drei getrennten* Mikro-Penning-Fallen im Abstand d über dem Chip – die Architektur von ZuriQ. Die Gleichgewichtslagen werden von den Elektroden festgelegt; die Coulomb-Kraft ist eine kleine Störung, die die Oszillatoren schwach koppelt.

Beide Modelle folgen demselben Rezept.

Rezept: Normalmoden in sechs Schritten

1. Gesamtpotential $V(\mathbf{r}_1, \dots, \mathbf{r}_N) = \text{Fallenpotential} + \text{Coulomb-Abstossung}$ aufschreiben.
2. Gleichgewicht $\nabla V = 0$ lösen (Kräftegleichgewicht).
3. Um das Gleichgewicht bis zur 2. Ordnung entwickeln (*harmonische Näherung*): $V \approx V_0 + \frac{1}{2} \mathbf{u}^T K \mathbf{u}$ mit der Hesse-Matrix $K_{ij} = \partial^2 V / \partial u_i \partial u_j$.
4. Eigenwertproblem $K \mathbf{b}_n = m \omega_n^2 \mathbf{b}_n$ lösen: Eigenfrequenzen ω_n und Modenvektoren $\mathbf{b}_n$.
5. Normalkoordinaten $Q_n = \mathbf{b}_n^T \mathbf{u}$ einführen: Die Bewegung zerfällt in N *unabhängige* Oszillatoren.
6. Jeden Oszillator quantisieren: $Q_n = z_{0,n}(a_n + a_n^\dagger)$, Phononen der Mode n .

Data-Science-Brille

Schritt 4 ist eine Hauptkomponentenanalyse der Hesse-Matrix: Die Eigenvektoren sind orthogonale „Richtungen“ im Raum der Auslenkungen, die Eigenwerte die Krümmungen (Steifigkeiten) entlang dieser Richtungen. `numpy.linalg.eigh` erledigt das in einer Zeile.

7.1 Modell A: drei Ionen in einer linearen Kette

7.1.1 Potential und Längenskala

Die Ionen sitzen auf der z -Achse bei $z_1 < z_2 < z_3$ in einem harmonischen axialen Potential $\frac{1}{2}m\omega_z^2 z^2$ (Magnetfeld ebenfalls entlang z , also keine Lorentzkraft auf die axiale Bewegung). Mit $k_C = e^2/(4\pi\epsilon_0)$:

$$V = \sum_{i=1}^3 \frac{1}{2} m\omega_z^2 z_i^2 + \sum_{i<j} \frac{k_C}{|z_i - z_j|}. \quad (7.1)$$

Es gibt eine natürliche Längenskala, bei der Fallenkraft und Coulomb-Kraft gleich gross sind:

$$m\omega_z^2 \ell = \frac{k_C}{\ell^2} \implies \ell = \left(\frac{k_C}{m\omega_z^2} \right)^{1/3}. \quad (7.2)$$

Mit dimensionslosen Positionen $u_i = z_i/\ell$ wird $V/(m\omega_z^2 \ell^2) = \sum_i \frac{1}{2} u_i^2 + \sum_{i<j} 1/|u_i - u_j|$. Alle Details der Falle stecken damit in ℓ – die Rechnung gilt für jedes Ion und jede Fallenfrequenz.

Rechenbeispiel 7.1: Längenskala für ${}^9\text{Be}^+$

$k_C = 2,307 \cdot 10^{-28} \text{ J m}$. Bei $\nu_z = 1 \text{ MHz}$: $m\omega_z^2 = 1,4964 \cdot 10^{-26} \text{ kg} \cdot (2\pi \cdot 10^6 \text{ s}^{-1})^2 = 5,908 \cdot 10^{-13} \text{ N/m}$, also $\ell = (3,905 \cdot 10^{-16} \text{ m}^3)^{1/3} = 7,31 \mu\text{m}$. Bei 2,5 MHz wäre $\ell = 3,97 \mu\text{m}$.

7.1.2 Schritt 2: Gleichgewicht

Aus Symmetrie sitzt das mittlere Ion bei $u_2 = 0$, die äusseren bei $u_{1,3} = \mp s$. Auf Ion 3 wirkt die Fallenkraft $-u_3 = -s$ nach innen und die Coulomb-Abstossung von Ion 2 (Abstand s) und Ion 1 (Abstand $2s$) nach aussen:

$$s = \frac{1}{s^2} + \frac{1}{(2s)^2} = \frac{5}{4s^2} \implies s = \left(\frac{5}{4} \right)^{1/3} = 1.0772 \quad (7.3)$$

Für $\nu_z = 1 \text{ MHz}$ sitzen die Ionen also bei $z = -7,87 \mu\text{m}$, 0 , $7,87 \mu\text{m}$. Das Programm `code/k3_drei_ionen_moden.py` findet dasselbe durch numerische Minimierung von V und prüft die Kraftbilanz in SI-Einheiten: Fallenkraft und Coulomb-Kraft betragen je $4,65 \cdot 10^{-18} \text{ N}$.

7.1.3 Schritt 3: Hesse-Matrix

Wir entwickeln $u_i = u_i^{(0)} + \xi_i$. Für den Coulomb-Term eines Paares mit Abstand $r = |u_i - u_j|$ gilt $\partial^2(1/r)/\partial r^2 = 2/r^3$. Damit hat die dimensionslose Hesse-Matrix $A = K/(m\omega_z^2)$ die Einträge

$$A_{ii} = 1 + 2 \sum_{k \neq i} \frac{1}{|u_i - u_k|^3}, \quad A_{ij} = -\frac{2}{|u_i - u_j|^3} \quad (i \neq j). \quad (7.4)$$

Mit $1/s^3 = \frac{4}{5}$ und $1/(2s)^3 = \frac{1}{10}$:

$$A = \begin{pmatrix} 1 + 2(\frac{4}{5} + \frac{1}{10}) & -\frac{8}{5} & -\frac{1}{5} \\ -\frac{8}{5} & 1 + 2(\frac{4}{5} + \frac{4}{5}) & -\frac{8}{5} \\ -\frac{1}{5} & -\frac{8}{5} & 1 + 2(\frac{4}{5} + \frac{1}{10}) \end{pmatrix} = \begin{pmatrix} 2.8 & -1.6 & -0.2 \\ -1.6 & 4.2 & -1.6 \\ -0.2 & -1.6 & 2.8 \end{pmatrix}. \quad (7.5)$$

Beachten Sie: Die Zeilensummen sind alle gleich 1. Das ist kein Zufall – die Coulomb-Kräfte sind innere Kräfte und heben sich bei einer gemeinsamen Verschiebung aller Ionen auf.

7.1.4 Schritt 4: Eigenwerte von Hand, mit Symmetrie

Die Spiegelung P (Ion 1 ↔ Ion 3) vertauscht mit A . Deshalb kann man die Eigenvektoren in spiegelsymmetrische und antisymmetrische aufteilen:

- *Antisymmetrisch*: $\mathbf{b} = (1, 0, -1)^T / \sqrt{2}$. Dann ist $(A\mathbf{b})_1 = (2.8 + 0.2) / \sqrt{2}$, also Eigenwert $\mu = A_{11} - A_{13} = 3$.
- *Symmetrisch*: Im Unterraum mit Basis $\mathbf{e}_s = (1, 0, 1)^T / \sqrt{2}$, $\mathbf{e}_2 = (0, 1, 0)^T$ wird A zur 2×2 -Matrix

$$\begin{pmatrix} A_{11} + A_{13} & \sqrt{2}A_{12} \\ \sqrt{2}A_{12} & A_{22} \end{pmatrix} = \begin{pmatrix} 2.6 & -1.6\sqrt{2} \\ -1.6\sqrt{2} & 4.2 \end{pmatrix}, \quad \text{Spur} = 6.8, \quad \det = 10.92 - 5.12 = 5.8.$$

Die Eigenwerte lösen $\mu^2 - 6.8\mu + 5.8 = 0$, also $\mu = 1$ und $\mu = 5.8 = \frac{29}{5}$.

Damit haben wir alle drei Moden:

$$\begin{array}{llll} \mu_1 = 1, & \omega_1 = \omega_z, & \mathbf{b}_1 = \frac{1}{\sqrt{3}}(1, 1, 1)^T & \text{Schwerpunktmode (COM)} \\ \mu_2 = 3, & \omega_2 = \sqrt{3}\omega_z, & \mathbf{b}_2 = \frac{1}{\sqrt{2}}(1, 0, -1)^T & \text{Streckmode (stretch)} \\ \mu_3 = \frac{29}{5}, & \omega_3 = \sqrt{29/5}\omega_z, & \mathbf{b}_3 = \frac{1}{\sqrt{6}}(1, -2, 1)^T & \text{Knickmode („Egyptian“)} \end{array} \quad (7.6)$$

Rechenbeispiel 7.2: Modenfrequenzen einer ${}^9\text{Be}^+$ -Kette

Bei $\nu_z = 1$ MHz: $\nu_1 = 1,000$ MHz, $\nu_2 = 1,732$ MHz, $\nu_3 = 2,408$ MHz. Kontrolle des Eigenvektors der Knickmode: $A(1, -2, 1)^T = (2.8 + 3.2 - 0.2, -1.6 - 8.4 - 1.6, \dots)^T = (5.8, -11.6, 5.8)^T = 5.8(1, -2, 1)^T$. ✓

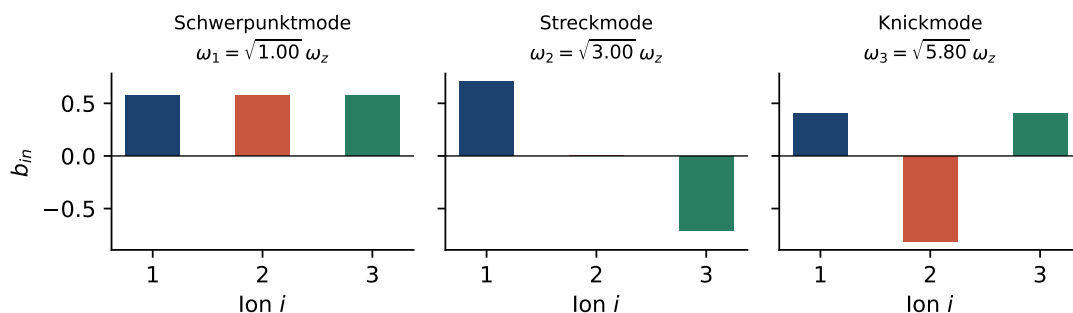


Abbildung 7.1: Modenvektoren b_{in} der drei axialen Moden einer Drei-Ionen-Kette. In der Streckmode steht das mittlere Ion *still* ($b_{22} = 0$) – ein Laser auf Ion 2 kann diese Mode nicht anregen, und über diese Mode koppeln nur die Ionen 1 und 3 (Abschnitt 9.4).

Interpretation

- Die Schwerpunktmode schwingt *exakt* mit ω_z , unabhängig von der Coulomb-Kraft (innere Kräfte bewegen den Schwerpunkt nicht). Sie ist daher empfindlich auf homogene elektrische Störfelder – sie heizt am schnellsten.
- In der Streckmode schwingen die äusseren Ionen gegenphasig, die Feder zwischen ihnen wird gedehnt und gestaucht.

- In der Knickmode schwingt das mittlere Ion gegen die beiden äusseren; das ist die steifste Mode.
- Die Modenvektoren folgen hier aus Symmetrien: Die gemeinsame Verschiebung $(1, 1, 1)$ ist Eigenvektor, weil die Coulomb-Kräfte innere Kräfte sind (gleiche Zeilensummen); die Spiegelsymmetrie trennt die antisymmetrische Mode $(1, 0, -1)$ ab; die dritte Mode ist orthogonal zu beiden. Nur die Eigenwerte hängen von der Coulomb-Physik ab.

7.1.5 Schritt 5: Normalkoordinaten

Fasst man die Modenvektoren als Spalten der orthogonalen Matrix $B = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ zusammen, dann ist $B^T A B = \text{diag}(\mu_1, \mu_2, \mu_3)$. Mit den Normalkoordinaten $\mathbf{Q} = B^T \mathbf{z}$, also

$$Q_1 = \frac{z_1 + z_2 + z_3}{\sqrt{3}}, \quad Q_2 = \frac{z_1 - z_3}{\sqrt{2}}, \quad Q_3 = \frac{z_1 - 2z_2 + z_3}{\sqrt{6}}, \quad (7.7)$$

zerfällt die Energie in drei *ungekoppelte* Oszillatoren:

$$H_{\text{mot}} = \sum_{n=1}^3 \left(\frac{P_n^2}{2m} + \frac{1}{2} m \omega_n^2 Q_n^2 \right). \quad (7.8)$$

7.1.6 Schritt 6: Quantisierung

Jede Normalkoordinate wird wie in Kapitel 6 quantisiert, $Q_n = z_{0,n}(a_n + a_n^\dagger)$ mit $z_{0,n} = \sqrt{\hbar/(2m\omega_n)}$. Zurücktransformiert ist die Auslenkung des einzelnen Ions i

$$\hat{z}_i = \sum_n b_{in} z_{0,n} (a_n + a_n^\dagger) \quad (7.9)$$

Merksatz

Die Auslenkung eines Ions ist eine Überlagerung *aller* Moden, gewichtet mit b_{in} . Umgekehrt spürt jede Mode alle Ionen, an denen sie beteiligt ist. Ein Laser, der an Ion i „zieht“, regt deshalb Phononen an, die auch Ion j spürt: Das ist der *Phononenbus*.

Und die radialen Moden?

In der Ebene senkrecht zu $\mathbf{B}$ kommen die geschwindigkeitsabhängigen Lorentzkräfte hinzu. Für N Ionen erhält man dann $2N$ Zyklotron- und Magnetron-artige Moden aus dem quadratischen Eigenwertproblem von Kapitel 5. Das Rezept bleibt dasselbe, nur Schritt 4 wird zum Eigenwertproblem der $4N \times 4N$ -Matrix erster Ordnung. Wir beschränken uns hier auf die axialen Moden.

7.2 Modell B: drei Ionen in drei Mikrofallen (ZuriQ-artig)

Jetzt sitzt jedes Ion in seiner eigenen Potentialmulde mit gleicher axialer Frequenz ω (senkrecht zum Chip, entlang $\mathbf{B}$). Die Fallenpositionen $\mathbf{R}_i$ in der Chipebene sind durch die Elektroden vorgegeben; die Abstände $d \approx 20 \mu\text{m}$ bis $100 \mu\text{m}$ sind *viel* grösser als die Längenskala ℓ von Modell A.

7.2.1 Coulomb-Kopplung bei Auslenkung senkrecht zur Verbindungslinie

Für zwei Ionen mit Verbindungsvektor $\mathbf{R}$ ($R = |\mathbf{R}|$) gilt allgemein

$$\frac{\partial^2}{\partial R_\alpha \partial R_\beta} \frac{1}{R} = \frac{3R_\alpha R_\beta - R^2 \delta_{\alpha\beta}}{R^5}. \quad (7.10)$$

Liegt $\mathbf{R}$ in der Chipebene und betrachten wir die axiale Auslenkung z senkrecht dazu, ist $R_z = 0$ und damit $\partial_z^2(1/R) = -1/R^3$. Die Coulomb-Energie zweier axial ausgelenkter Ionen im Abstand d ist also

$$V_C \approx \frac{k_C}{d} - \frac{k_C}{2d^3}(z_i - z_j)^2 = \frac{k_C}{d} - \frac{k_C}{2d^3}(z_i^2 + z_j^2) + \frac{k_C}{d^3} z_i z_j. \quad (7.11)$$

Anschaulich: Hebt sich ein Ion aus der Ebene, wird der Abstand *grösser* und die Abstossung kleiner – die Coulomb-Kraft wirkt senkrecht zur Verbindungslinie wie eine *Anti-Feder*. Sie macht jedes Ion etwas „weicher“ (Term $-z_i^2$) und koppelt die Ionen (Term $+z_i z_j$).

7.2.2 Hesse-Matrix

Summiert über alle Paare ergibt sich

$$K = m\omega^2 \mathbb{I} + k_C M, \quad M_{ii} = -\sum_{j \neq i} \frac{1}{d_{ij}^3}, \quad M_{ij} = +\frac{1}{d_{ij}^3}. \quad (7.12)$$

Mit dem kleinen dimensionslosen Parameter

$$\varepsilon = \frac{k_C}{m\omega^2 d^3} \quad (7.13)$$

lautet das Eigenwertproblem $K\mathbf{b} = m\omega_n^2 \mathbf{b}$ mit $\omega_n^2 = \omega^2(1 + \varepsilon\lambda_n)$, wobei λ_n die Eigenwerte der Matrix $d^3 M$ sind.

Linie mit Abstand d . Die übernächsten Nachbarn haben Abstand $2d$ und tragen $1/8$ bei:

$$d^3 M_{\text{Linie}} = \begin{pmatrix} -\frac{9}{8} & 1 & \frac{1}{8} \\ 1 & -2 & 1 \\ \frac{1}{8} & 1 & -\frac{9}{8} \end{pmatrix}, \quad \lambda \in \left\{0, -\frac{5}{4}, -3\right\} \quad (7.14)$$

mit *denselben* Eigenvektoren wie in Modell A: $(1, 1, 1)^T/\sqrt{3}$ zu $\lambda = 0$, $(1, 0, -1)^T/\sqrt{2}$ zu $\lambda = -\frac{5}{4}$, $(1, -2, 1)^T/\sqrt{6}$ zu $\lambda = -3$. (Nachrechnen: $-\frac{9}{8} + 1 + \frac{1}{8} = 0$; $-\frac{9}{8} - \frac{1}{8} = -\frac{5}{4}$; $-\frac{9}{8} - 2 + \frac{1}{8} = -3$.) Translationsinvarianz der Coulomb-Kraft (Zeilensummen null) und Spiegelsymmetrie erzwingen wieder die Modenform – aber die Reihenfolge der Frequenzen ist *umgekehrt*: Die Schwerpunktmode ist jetzt die *höchste*, weil die Anti-Feder die Relativbewegungen weicher macht.

Gleichseitiges Dreieck. Alle Abstände sind gleich, $d^3 M = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$, mit $\lambda = 0$ (COM) und dem *doppelt entarteten* $\lambda = -3$. Jede Überlagerung der beiden Relativmoden ist wieder Eigenmode; die Wahl der Basis ist willkürlich (numpy liefert irgendeine).

Rechenbeispiel 7.3: Modenaufspaltung für drei Mikrofallen

${}^9\text{Be}^+$, $\nu = 2,5 \text{ MHz}$, $d = 30 \mu\text{m}$:

$$\varepsilon = \frac{2,307 \cdot 10^{-28} \text{ J m}}{3,692 \cdot 10^{-12} \text{ N/m} \cdot (30 \cdot 10^{-6} \text{ m})^3} = 2,31 \times 10^{-3}.$$

Wegen $\varepsilon \ll 1$ ist $\omega_n \approx \omega(1 + \frac{1}{2}\varepsilon\lambda_n)$, also $\Delta\nu_n = \frac{1}{2}\varepsilon\lambda_n\nu$:

Mode	λ_n	$\Delta\nu_n$ (Linie)	$\Delta\nu_n$ (Dreieck)
COM (1, 1, 1)	0	0	0
Streck (1, 0, -1)	-5/4	-3,62 kHz	-8,69 kHz
Knick (1, -2, 1)	-3	-8,69 kHz	-8,69 kHz

Die Moden liegen nur wenige kHz auseinander – bei einer Grundfrequenz von 2,5 MHz. Das ist ein wesentlicher Unterschied zu Modell A, wo die Moden um MHz getrennt sind.

7.2.3 Das Bild vom hüpfenden Phonon

Weil die Kopplung so schwach ist, ist ein zweites Bild oft nützlicher: Jedes Ion hat seinen *lokalen* Oszillator a_i , und die Coulomb-Kopplung lässt Phononen von Falle zu Falle hüpfen. Setzt man $z_i = z_0(a_i + a_i^\dagger)$ in den Kopplungsterm $\frac{k_C}{d^3} z_i z_j$ ein und vernachlässigt die schnell oszillierenden Terme $a_i a_j$ und $a_i^\dagger a_j^\dagger$ (*Drehwellennäherung*, gültig für $t_{ij} \ll \omega$), erhält man

$$H_{\text{mot}} = \sum_i \hbar \omega'_i a_i^\dagger a_i + \sum_{i < j} \hbar t_{ij} (a_i^\dagger a_j + a_j^\dagger a_i), \quad t_{ij} = \frac{k_C}{2m\omega d_{ij}^3} \quad (7.15)$$

Das ist formal ein *Tight-Binding-Modell* – dieselbe Mathematik wie für Elektronen in einem Kristall. Die Grösse $\Omega_{\text{ex}} = 2t$ heisst in der Literatur Austauschfrequenz [2].

Rechenbeispiel 7.4: Hüpfrate und Austauschzeit

d	$t/2\pi$	Austauschfrequenz $\Omega_{\text{ex}}/2\pi = 2t/2\pi$	volle Übergabe $\pi/(2t)$
20 μm	9,76 kHz	19,5 kHz	26 μs
30 μm	2,89 kHz	5,79 kHz	86 μs
50 μm	0,62 kHz	1,25 kHz	400 μs
100 μm	0,078 kHz	0,16 kHz	3,2 ms

(${}^9\text{Be}^+$, $\nu = 2,5 \text{ MHz}$.) Die Kopplung fällt mit d^{-3} : doppelter Abstand, achtmal langsamer. Da ZuriQ Ionen transportieren kann (Kapitel 5), lässt sich die Kopplung durch *Zusammenschieben* und *Auseinanderziehen* ein- und ausschalten – oder durch Verstimmen der lokalen Frequenzen ω'_i : Ist $|\omega'_i - \omega'_j| \gg t_{ij}$, findet praktisch kein Austausch statt.

Rechenbeispiel 7.5: Ein Phonon wandert von Ion 1 zu Ion 3

Nur mit nächsten Nachbarn und gleichen lokalen Frequenzen ist der Hopping-Hamiltonoperator im Ein-Phonon-Sektor $H = \hbar t \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ mit Eigenwerten $0, \pm\sqrt{2}\hbar t$. Startet das Phonon bei Ion 1, sind die Amplituden

$$c_1(\tau) = \frac{1}{2}(1 + \cos\sqrt{2}t\tau), \quad c_2(\tau) = -\frac{i}{\sqrt{2}}\sin\sqrt{2}t\tau, \quad c_3(\tau) = \frac{1}{2}(\cos\sqrt{2}t\tau - 1).$$

Bei $\tau^* = \pi/(\sqrt{2}t)$ ist $|c_3| = 1$: *perfekter Zustandstransfer*. Für $d = 30 \mu\text{m}$ ist $\tau^* = 122 \mu\text{s}$. Zwischendurch, bei $\sqrt{2}t\tau = \pi/2$, ist der Zustand $\frac{1}{2}|1_1\rangle - \frac{i}{\sqrt{2}}|1_2\rangle - \frac{1}{2}|1_3\rangle$ – ein einzelnes Phonon, verteilt auf drei Fallen: ein W-artiger verschränkter Zustand der drei Oszillatoren. Mit der vollen Coulomb-Kopplung (übernächste Nachbarn mit $t/8$ und die unterschiedlichen Frequenzverschiebungen ω'_i der inneren und äusseren Falle) sinkt die maximale Transferwahrscheinlichkeit auf 93 % (Abb. 7.2); durch Nachjustieren der lokalen Fallenfrequenzen lässt sich das korrigieren.

Ein Phonon wandert durch drei Mikrofallen ($d = 30 \mu\text{m}$, $\nu = 2.5 \text{ MHz}$)

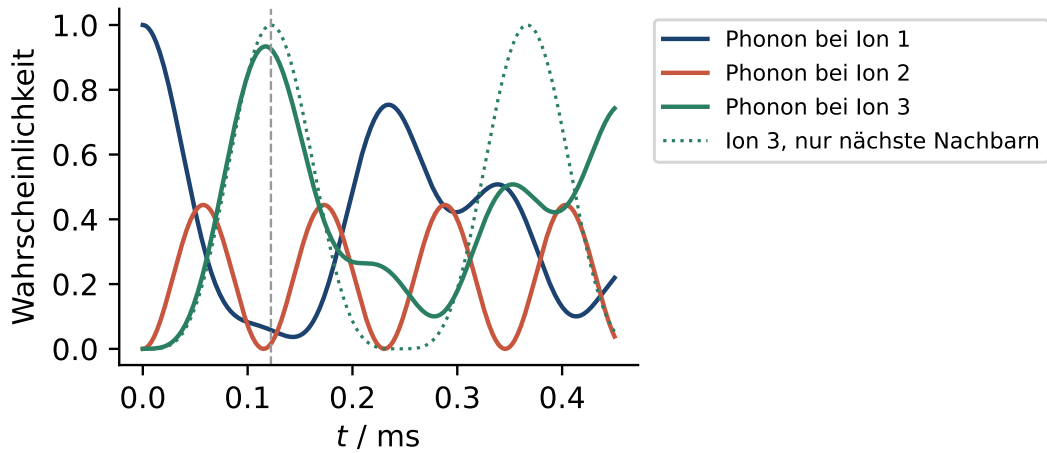


Abbildung 7.2: Wahrscheinlichkeit, das Phonon bei Ion 1, 2 oder 3 zu finden (volle Coulomb-Kopplung in harmonischer Näherung und Drehwellennäherung). Gepunktet: Modell nur mit nächsten Nachbarn, das bei τ^* perfekten Transfer liefert.

7.2.4 Zusammenhang der beiden Bilder

Diagonalisiert man die Hopping-Matrix $(\omega'_i \delta_{ij} + t_{ij})$, erhält man genau die kollektiven Eigenmoden von oben, $b_n = \sum_i c_{in} a_i$. Die beiden Bilder – „lokale Oszillatoren mit Hüpfen“ und „globale Normalmoden“ – sind dieselbe Physik in verschiedenen Basen. Welche Basis zweckmässig ist, hängt davon ab, ob die Kopplung klein (Modell B) oder gross (Modell A) gegenüber den Verstimmungen der Laser ist.

7.3 Lamb–Dicke-Parameter: Wie stark spürt ein Laser die Mode?

Ein Laser mit Wellenvektorübertrag Δk entlang z „sieht“ am Ort von Ion i die Phase $e^{i\Delta k \hat{z}_i}$. Mit Gleichung (7.9) ist

$$\Delta k \hat{z}_i = \sum_n \eta_{in} (a_n + a_n^\dagger), \quad \eta_{in} = \Delta k b_{in} \sqrt{\frac{\hbar}{2m\omega_n}} \quad (7.16)$$

Der *Lamb–Dicke-Parameter* η_{in} ist das Verhältnis der Grundzustandsausdehnung zur reduzierten Wellenlänge, gewichtet mit der Beteiligung des Ions an der Mode.

Rechenbeispiel 7.6: Lamb–Dicke-Parameter der Drei-Ionen-Kette

Zwei Raman-Strahlen bei 313 nm kreuzen sich unter $\theta = 20^\circ$; ihr Differenzwellenvektor $\Delta k = 2k \sin(\theta/2) = 6,97 \cdot 10^6 \text{ m}^{-1}$ zeige entlang z . Bei $\nu_z = 1 \text{ MHz}$ ist $z_0 = 23,7 \text{ nm}$ und $\eta_0 = \Delta k z_0 = 0.165$. Mit $\eta_{in} = \eta_0 b_{in} / \sqrt[4]{\mu_n}$:

	COM ($\nu_1 = 1 \text{ MHz}$)	Streck ($\nu_2 = 1,73 \text{ MHz}$)	Knick ($\nu_3 = 2,41 \text{ MHz}$)
Ion 1	0.095	+0.089	+0.043
Ion 2	0.095	0	−0.087
Ion 3	0.095	−0.089	+0.043

Alle Werte sind $\ll 1$: Wir sind im *Lamb–Dicke-Regime*. (Bei gegenläufigen Strahlen, $\Delta k = 2k$, wäre $\eta_0 \approx 0.95$ – viel zu gross; die Strahlgeometrie ist ein wichtiger Designparameter.)

Rechenbeispiel 7.7: Warum Mikrowellen die Bewegung nicht spüren

Eine Mikrowelle bei 83 GHz hat $k = 2\pi/3,6 \text{ mm} = 1,7 \cdot 10^3 \text{ m}^{-1}$. Mit $z_0 = 15 \text{ nm}$ ist $\eta = 2,6 \cdot 10^{-5}$. Seitenbandprozesse sind damit um den Faktor η unterdrückt: Mikrowellen drehen den Spin, ohne die Bewegung anzufassen. Für Zwei-Qubit-Gates braucht man optische (Raman-)Felder oder starke Magnetfeldgradienten.

Kapitel 8

Licht koppelt Qubit und Bewegung

8.1 Der Wechselwirkungs-Hamiltonoperator

Ein Ion mit Qubit-Frequenz ω_0 in einer Mode mit Frequenz ω (zunächst eine einzige Mode) hat ohne Laser

$$H_0 = \frac{\hbar\omega_0}{2}\sigma_z + \hbar\omega a^\dagger a, \quad \sigma_z = |\uparrow\rangle\langle\uparrow| - |\downarrow\rangle\langle\downarrow|. \quad (8.1)$$

Ein (Raman-)Laserpaar mit Differenzfrequenz ω_L , Phase ϕ und Wellenvektorübertrag Δk fügt

$$H_L = \frac{\hbar\Omega}{2}(\sigma_+ e^{i(\Delta k \hat{z} - \omega_L t + \phi)} + \text{h.c.}), \quad \sigma_+ = |\uparrow\rangle\langle\downarrow| \quad (8.2)$$

hinzu. Das Entscheidende ist der Faktor $e^{i\Delta k \hat{z}}$: Weil $\hat{z} = z_0(a + a^\dagger)$ ein *Operator* ist, enthält der Laserterm Erzeuger und Vernichter von Phononen. Das Licht überträgt Impuls und kann dabei die Bewegung ändern.

Im *Wechselwirkungsbild* bezüglich H_0 (man „dreht mit“, sodass nur noch die langsamen Prozesse übrig bleiben) werden $\sigma_+ \rightarrow \sigma_+ e^{i\omega_0 t}$ und $a \rightarrow a e^{-i\omega t}$. Mit der Verstimmung $\Delta = \omega_L - \omega_0$ und $\eta = \Delta k z_0$:

$$H_I = \frac{\hbar\Omega}{2}\sigma_+ \exp[i\eta(ae^{-i\omega t} + a^\dagger e^{i\omega t})]e^{-i(\Delta t - \phi)} + \text{h.c.} \quad (8.3)$$

8.2 Lamb–Dicke-Näherung: Träger und Seitenbänder

(Eine ausführliche Darstellung dieses Kapitels findet sich im Übersichtsartikel [8].) Für $\eta\sqrt{\langle(a + a^\dagger)^2\rangle} \ll 1$ (Lamb–Dicke-Regime) entwickeln wir die Exponentialfunktion bis zur ersten Ordnung:

$$e^{i\eta(ae^{-i\omega t} + a^\dagger e^{i\omega t})} \approx 1 + i\eta a e^{-i\omega t} + i\eta a^\dagger e^{i\omega t}. \quad (8.4)$$

Jeder der drei Terme wird resonant (zeitunabhängig) für eine andere Laserfrequenz. Behält man nur den resonanten Term (die anderen oszillieren schnell und mitteln sich weg), erhält man:

Laserfrequenz	Name	Hamiltonoperator	Übergang
$\omega_L = \omega_0$	Träger	$\frac{\hbar\Omega}{2}(\sigma_+ e^{i\phi} + \text{h.c.})$	$ \downarrow, n\rangle \leftrightarrow \uparrow, n\rangle$
$\omega_L = \omega_0 - \omega$	rotes Seitenband	$\frac{\hbar\eta\Omega}{2}(\sigma_+ a e^{i\phi'} + \text{h.c.})$	$ \downarrow, n+1\rangle \leftrightarrow \uparrow, n\rangle$
$\omega_L = \omega_0 + \omega$	blaues Seitenband	$\frac{\hbar\eta\Omega}{2}(\sigma_+ a^\dagger e^{i\phi'} + \text{h.c.})$	$ \downarrow, n\rangle \leftrightarrow \uparrow, n+1\rangle$

Dabei ist $\phi' = \phi + \pi/2$ (der Faktor i aus der Entwicklung); im Folgenden wählen wir die Laserphasen so, dass $\phi' = 0$ bzw. $\phi = 0$. Das rote Seitenband ist das *Jaynes–Cummings*-Modell der Quantenoptik, das blaue sein „Anti“-Gegenstück. Energetisch ist das anschaulich: Beim roten Seitenband fehlt dem Laser die Energie $\hbar\omega$, um den Spin anzuheben – er holt sie sich aus der Bewegung und vernichtet ein Phonon.

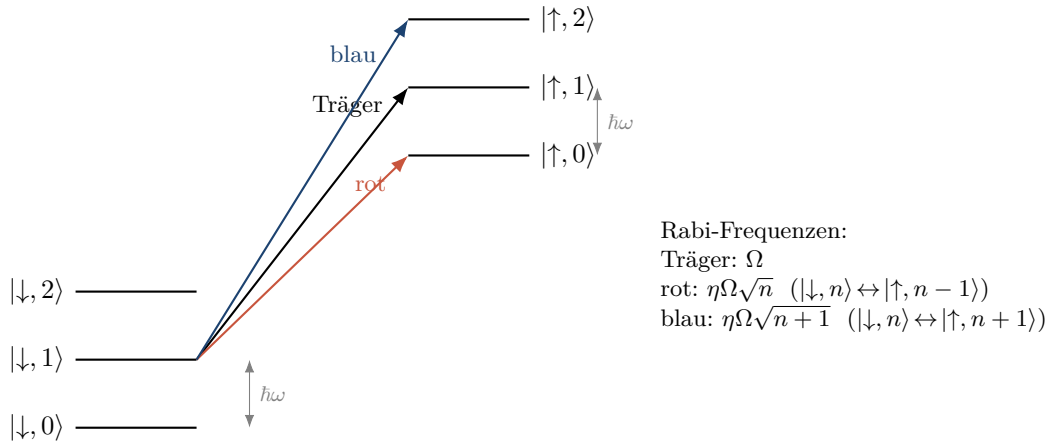


Abbildung 8.1: Leiter der Zustände $|\text{Spin}, n\rangle$, gezeigt für den Startzustand $|\downarrow, 1\rangle$. Träger, rotes und blaues Seitenband koppeln ihn an verschiedene Partner; die Seitenbandkopplungen hängen über $\sqrt{n}$ bzw. $\sqrt{n+1}$ von der Phononenzahl ab.

Da $a^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle$, ist die Rabi-Frequenz des blauen Seitenbands zwischen $|\downarrow, n\rangle$ und $|\uparrow, n+1\rangle$ gleich $\eta\Omega\sqrt{n+1}$, die des roten Seitenbands zwischen $|\downarrow, n\rangle$ und $|\uparrow, n-1\rangle$ gleich $\eta\Omega\sqrt{n}$.

Rechenbeispiel 8.1: Pulsdauern

$\Omega = 2\pi \times 100 \text{ kHz}$, $\eta = 0.1$. Träger- π -Puls: $\pi/\Omega = 5 \mu\text{s}$. Blauer π -Puls $|\downarrow, 0\rangle \rightarrow |\uparrow, 1\rangle$: $\pi/(\eta\Omega) = 50 \mu\text{s}$. Roter π -Puls $|\downarrow, 1\rangle \rightarrow |\uparrow, 0\rangle$ ebenfalls $50 \mu\text{s}$, aber für $|\downarrow, 2\rangle \rightarrow |\uparrow, 1\rangle$ nur $50 \mu\text{s}/\sqrt{2} = 35 \mu\text{s}$. Seitenbänder sind um den Faktor η langsamer und *abhängig von n* – das ist eine Fehlerquelle, wenn die Mode nicht im Grundzustand ist.

8.3 Seitenbandkühlung und Thermometrie

Kühlen. Man treibt einen Seitenbandübergang, der ein Phonon vernichtet, und pumpt anschließend optisch in den Ausgangszustand zurück (ohne n zu ändern). Da bei $^9\text{Be}^+$ in der Penning-Falle das optische Pumpen nach $|\uparrow\rangle$ führt (Kapitel 4), verwendet man den Übergang $|\uparrow, n\rangle \rightarrow |\downarrow, n-1\rangle$ – nach unserer Tabelle ist das das *blaue* Seitenband (sein Term $\sigma_- a$), denn der Spin verliert dabei die Energie $\hbar\omega_0$ und die Bewegung $\hbar\omega$. Danach pumpt man zurück nach $|\uparrow\rangle$. Jeder Zyklus entfernt ein Phonon. Im Zustand $|\uparrow, 0\rangle$ gibt es keinen Partner $|\downarrow, -1\rangle$ mehr – der Prozess stoppt. (In Lehrbüchern, in denen man in den energetisch *unteren* Zustand pumpt, ist es entsprechend das rote Seitenband.) So erreicht man $\bar{n} \approx 0.01$.

Messen der Temperatur. Man präpariert $|\uparrow\rangle$ und treibt kurz eines der beiden Seitenbänder. Das phononenvernichtende blaue Seitenband $|\uparrow, n\rangle \rightarrow |\downarrow, n-1\rangle$ hat die Stärke $\propto \sqrt{n}$ und wirkt nicht auf $n = 0$; das phononenerzeugende rote Seitenband $|\uparrow, n\rangle \rightarrow |\downarrow, n+1\rangle$ hat die Stärke $\propto \sqrt{n+1}$. Für einen thermischen Zustand gilt dann das berühmte Verhältnis der Anregungswahr-

scheinlichkeiten

$$\frac{P_{\downarrow}^{\text{blau}}}{P_{\downarrow}^{\text{rot}}} = \frac{\bar{n}}{\bar{n} + 1}. \quad (8.5)$$

(Beweis: Das Verhältnis der Wahrscheinlichkeiten benachbarter Fock-Zustände ist konstant, Gleichung (6.6). Startet man – wie in vielen Lehrbüchern – im unteren Zustand $|\downarrow\rangle$, vertauschen sich die Rollen von rot und blau.)

Rechenbeispiel 8.2: Temperaturschätzung

Nach Seitenbandkühlung misst man nach je $S = 2000$ Shots 21-mal „dunkel“ (also $|\downarrow\rangle$) beim blauen und 940-mal beim roten Seitenband. Dann ist $R = 21/940 = 0.0223$ und $\bar{n} = R/(1 - R) = 0.023$. Die Poisson-Unsicherheit der kleinen Zählrate ($\sqrt{21} \approx 4.6$) dominiert: $\bar{n} = 0.023 \pm 0.005$.

8.4 Verschränkung über ein reales Phonon: die Seitenband-Sequenz

Jetzt können wir die zentrale Frage erstmals beantworten: *Wie verschränkt ein Phonon zwei Ionen?* Die folgende Sequenz geht auf die Idee von Cirac und Zoller zurück [9]. Wir betrachten Ion 1 und Ion 2 der Drei-Ionen-Kette und ihre gemeinsame Schwerpunktmode (COM, $b_{11} = b_{21} = 1/\sqrt{3}$), die in den Grundzustand gekühlt ist. Beide Qubits sind in $|0\rangle = |\uparrow\rangle$ initialisiert.

Rechenbeispiel 8.3: Zwei Ionen über die Schwerpunktmode verschränken

Start: $|\psi_0\rangle = |\uparrow\uparrow\rangle |n=0\rangle$.

Schritt 1: roter $\pi/2$ -Puls auf Ion 1. Das rote Seitenband koppelt $|\uparrow, 0\rangle \leftrightarrow |\downarrow, 1\rangle$. Ein halber Rabi-Zyklus erzeugt eine Überlagerung:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} (|\uparrow\uparrow\rangle |0\rangle - i |\downarrow\uparrow\rangle |1\rangle).$$

Ion 1 ist jetzt mit der *Bewegung* verschränkt: „Spin unten“ gehört zu „ein Phonon“.

Schritt 2: blauer π -Puls auf Ion 2. Das blaue Seitenband koppelt $|\downarrow, n\rangle \leftrightarrow |\uparrow, n+1\rangle$. Im ersten Term ist Ion 2 in $|\uparrow, 0\rangle$; ein Partner $|\downarrow, -1\rangle$ existiert nicht, also passiert nichts. Im zweiten Term ist Ion 2 in $|\uparrow, 1\rangle$, und der π -Puls bringt es nach $-i |\downarrow, 0\rangle$:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} (|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle) \otimes |0\rangle.$$

Ergebnis: Das Phonon ist verschwunden, die Bewegung wieder im Grundzustand – und die beiden Qubits sind maximal verschränkt, $|\psi_2\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$. Die numerische Simulation (code/k4_spin_phonon.py) bestätigt Amplituden $+0.7071$ und -0.7071 .

Merksatz

Das Phonon dient als *Quantenbus*: Die Information „Ion 1 hat geflippt“ wird kohärent in die gemeinsame Bewegung geschrieben und von Ion 2 wieder ausgelesen. Weil das Phonon zu *beiden* Ionen gehört, ist das möglich, obwohl die Laser die Ionen einzeln adressieren und die Ionen $8\text{ }\mu\text{m}$ voneinander entfernt sind.

Wahl der Mode wählt die Partner. Benutzt man statt der COM-Mode die Streckmode, kann man Ion 1 und Ion 3 verschränken, während Ion 2 (mit $b_{22} = 0$) die Mode gar nicht anregen kann. Die Rabi-Frequenz des Seitenbands an Ion i ist $\eta_{in}\Omega$; aus der Tabelle in Abschnitt 7.3 liest man ab, wie schnell welches Ion an welche Mode koppelt.

Grenzen. Die Seitenband-Sequenz braucht (i) Einzelionenadressierung, (ii) Grundzustandskühlung, weil die Seitenband-Rabi-Frequenzen von n abhängen, und (iii) ist während des Gates die Quanteninformation zeitweise im Phonon gespeichert, das durch Heizen zerstört werden kann. Das Cirac-Zoller-CNOT-Gate [9] ergänzt diese Idee um ein Hilfsniveau und liefert ein vollständiges CNOT. Robuster ist das Gate des nächsten Kapitels, das die Mode nur *virtuell* anregt und von der Phononenzahl unabhängig ist.

Kapitel 9

Das geometrische Phasengate: Verschränkung über virtuelle Phononen

Die Seitenband-Sequenz aus Abschnitt 8.4 verlangt, dass die Mode exakt im Grundzustand ist. Mølmer und Sørensen [10] (und unabhängig Milburn sowie Solano et al.) fanden ein Gate, das *unabhängig* vom Bewegungszustand funktioniert. Es ist heute das Standard-Zwei-Qubit-Gate fast aller Ionen-Quantencomputer; mit genau diesem Gate wurden am NIST bereits im Jahr 2000 vier ${}^9\text{Be}^+$ -Ionen verschränkt [11]. In Penning-Kristallen mit hunderten ${}^9\text{Be}^+$ -Ionen erzeugt dieselbe Physik – als spinabhängige optische Dipolkraft auf die axialen Moden – programmierbare Ising-Wechselwirkungen [13].

9.1 Die spinabhängige Kraft

Man beleuchtet die Ionen gleichzeitig mit einem rot verstimmten und einem blau verstimmten Seitenband-Feld, beide um δ von der Mode entfernt:

$$\omega_L^{\text{rot}} = \omega_0 - (\omega - \delta), \quad \omega_L^{\text{blau}} = \omega_0 + (\omega - \delta).$$

Die beiden Felder sind also um $\mu = \omega - \delta$ vom Träger entfernt. Addiert man die beiden Seitenband-Hamiltonoperatoren aus Kapitel 8 (jetzt nicht exakt resonant, daher mit Zeitabhängigkeit $e^{\pm i\delta t}$) und wählt die Phasen symmetrisch, so wird aus $\sigma_+ a + \sigma_+ a^\dagger + \text{h.c.}$ das Produkt $(\sigma_+ + \sigma_-)(\dots) = \sigma_x(\dots)$:

$$H_I(t) = \hbar \sum_i g_i \sigma_x^{(i)} (a e^{-i\delta t} + a^\dagger e^{i\delta t}), \quad g_i = \frac{\eta_i \Omega_i}{2} \quad (9.1)$$

Das ist eine *Kraft* auf den Oszillator (linear in $a + a^\dagger$, also in $\hat{z}$), deren *Vorzeichen vom Qubit abhängt*: Für den σ_x -Eigenzustand $|+\rangle$ zieht sie in die eine, für $|-\rangle$ in die andere Richtung, und sie rotiert mit der Verstimmung δ .

9.2 Exakte Lösung mit der Magnus-Entwicklung

Für zeitabhängige Hamiltonoperatoren ist $U(t) = \mathcal{T} \exp \left[-\frac{i}{\hbar} \int H dt \right]$ (zeitgeordnet). Die Magnus-Entwicklung schreibt $U = \exp(\Omega_1 + \Omega_2 + \dots)$ mit

$$\Omega_1 = -\frac{i}{\hbar} \int_0^t H(t_1) dt_1, \quad \Omega_2 = -\frac{1}{2\hbar^2} \int_0^t dt_1 \int_0^{t_1} dt_2 [H(t_1), H(t_2)]. \quad (9.2)$$

Mit $S \equiv \sum_i g_i \sigma_x^{(i)}$ ist $H_I/\hbar = S(ae^{-i\delta t} + a^\dagger e^{i\delta t})$.

Erste Ordnung: spinabhängige Verschiebung.

$$\Omega_1 = S(\alpha(t)a^\dagger - \alpha^*(t)a), \quad \alpha(t) = \frac{1}{\delta}(1 - e^{i\delta t}). \quad (9.3)$$

e^{Ω_1} ist ein Verschiebungsoperator $D(s\alpha(t))$, wobei s der Eigenwert von S ist. Im Phasenraum läuft der Oszillator auf einem *Kreis* mit Mittelpunkt s/δ und Radius $|s|/\delta$ (Abb. 9.1, rechts), und bei $t = 2\pi K/\delta$ ($K = 1, 2, \dots$) ist $\alpha = 0$: Die Bewegung ist *zurück am Ausgangspunkt*, egal wo dieser war.

Zweite Ordnung: die geometrische Phase. Der Kommutator ist wegen $[a, a^\dagger] = 1$ eine Zahl mal S^2 :

$$[H(t_1), H(t_2)]/\hbar^2 = S^2(e^{-i\delta(t_1-t_2)} - e^{i\delta(t_1-t_2)}) = -2i S^2 \sin \delta(t_1 - t_2).$$

Integrieren liefert

$$\Omega_2 = i S^2 \left(\frac{t}{\delta} - \frac{\sin \delta t}{\delta^2} \right). \quad (9.4)$$

Alle höheren Magnus-Terme verschwinden, weil $[\Omega_2, H] = 0$ (S^2 vertauscht mit S). Die Lösung ist also *exakt*

$$U(t) = D(S\alpha(t)) \exp \left[i S^2 \left(\frac{t}{\delta} - \frac{\sin \delta t}{\delta^2} \right) \right] \quad (9.5)$$

9.3 Zwei Ionen: das Gate

Für zwei Ionen mit $g_1 = g_2 = g$ ist $S = g(X_1 + X_2)$ und $S^2 = g^2(2\mathbb{I} + 2X_1X_2)$. Bei $t_g = 2\pi K/\delta$ ist die Verschiebung null und es bleibt, bis auf eine globale Phase,

$$U(t_g) \doteq \exp \left[+i \frac{4\pi K g^2}{\delta^2} X_1 X_2 \right] = XX(-\chi), \quad \chi = \frac{4\pi K g^2}{\delta^2}. \quad (9.6)$$

Für ein maximal verschränkendes Gate braucht man $\chi = \pi/4$, also

$$\delta = 4g\sqrt{K}, \quad t_g = \frac{2\pi K}{\delta} = \frac{\pi\sqrt{K}}{2g} \quad (9.7)$$

und aus $|00\rangle$ wird $\frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$ (das Vorzeichen von i hängt von der Konvention für δ ab; vgl. Abschnitt 3.3.2).

Das Phasenraumbild: Fläche wird zu Phase

Die Operatoren $X_1 + X_2$ haben die Eigenwerte $+2$ (für $|++\rangle$), 0 (für $|+-\rangle, |-+\rangle$) und -2 (für $|--\rangle$).

- Für $|++\rangle$ und $|--\rangle$ wird der Oszillator kräftig herumgeschoben und läuft eine Kreisbahn mit Fläche $\pi(2g/\delta)^2$. Die erworbene Phase ist die doppelte Fläche: $2\pi \cdot 4g^2/\delta^2$.
- Für $|+-\rangle$ und $|-+\rangle$ heben sich die Kräfte auf; keine Bewegung, keine Phase.

Die *relative* Phase zwischen diesen Fällen ist das Gate. Weil nur die *Fläche* zählt, nicht der Startpunkt im Phasenraum, ist das Gate unabhängig vom Anfangszustand der Mode – auch für thermische Zustände! Die Mode wird dabei nur „virtuell“ angeregt: Am Ende des Gates ist sie exakt im Ausgangszustand.

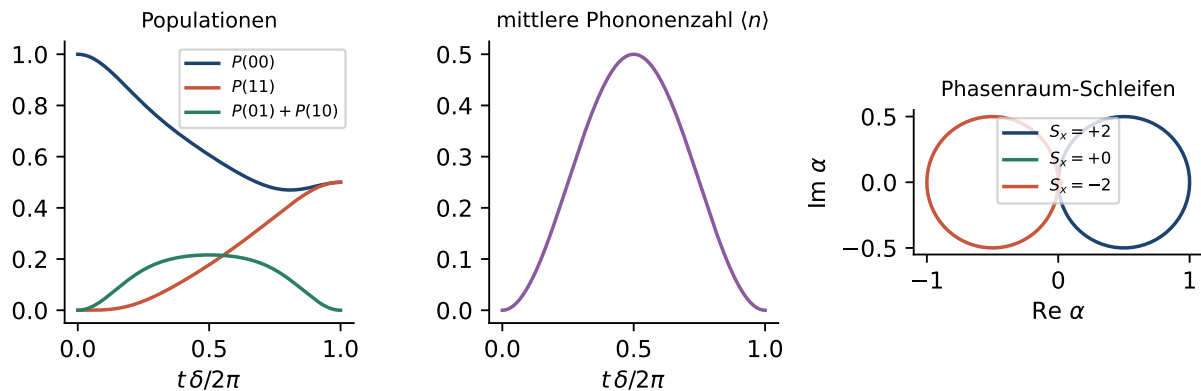


Abbildung 9.1: Numerische Simulation (code/k4_spin_phonon.py) des Gates Gleichung (9.1) für zwei Ionen, $\delta = 4g$, Start in $|00\rangle |n=0\rangle$. Links: Nach $t_g = 2\pi/\delta$ ist $P(00) = P(11) = \frac{1}{2}$. Mitte: Die mittlere Phononenzahl steigt während des Gates auf 0.5 und kehrt exakt auf 0 zurück. Rechts: Phasenraumbahnen $\alpha_s(t)$ für die drei Eigenwerte von $X_1 + X_2$.

Rechenbeispiel 9.1: Das Gate in Zahlen (Drei-Ionen-Kette, zwei Ionen über COM)

Mit $\eta_{i1} = 0.095$ (Abschnitt 7.3) und $\Omega = 2\pi \times 52,6 \text{ kHz}$ ist $g = \eta\Omega/2 = 2\pi \times 2,5 \text{ kHz}$. Die Bedingung Gleichung (9.7) mit $K = 1$ verlangt $\delta = 4g = 2\pi \times 10 \text{ kHz}$, und das Gate dauert $t_g = 2\pi/\delta = 100 \mu\text{s}$. Zum Vergleich: Die Kohärenzzeit mit Spin-Echo beträgt 240 ms (Kapitel 4), die axiale Heizrate $\dot{n} = 0.09 \text{ s}^{-1}$ bringt während des Gates im Mittel 10^{-5} Phononen – vernachlässigbar.

Rechenbeispiel 9.2: Die Simulation im Detail

Die Simulation verwendet eine abgeschnittene Fock-Basis mit $n_{\max} = 20$ (Zustandsraum $2 \times 2 \times 20 = 80$) und integriert die Schrödinger-Gleichung mit `scipy.integrate.solve_ivp`. Resultate:

Situation	Bell-Fidelity	Reinheit $\text{Tr } \rho^2$ der Qubits
ideal, Start in $n_0 = 0$	1.000000	1.00000
Start in $n_0 = 1$ bzw. $n_0 = 3$	1.000000	1.00000
Gatezeit 2 % zu lang	0.998	0.996
Gatezeit 5 % zu lang	0.988	0.976

Die Unabhängigkeit von n_0 ist exakt. Ist die Gatezeit falsch, schliesst sich die Schleife nicht: Die Qubits bleiben mit der Bewegung verschränkt, und nach Ausspuren der Bewegung ist ihr

Zustand *gemischt* (Reinheit < 1) – vgl. Kapitel 2.

9.4 Drei Ionen und viele Moden: die Kopplungsmatrix J_{ij}

9.4.1 Die allgemeine Formel

Beleuchtet man alle Ionen und berücksichtigt alle Moden n , wird aus Gleichung (9.1)

$$H_I = \hbar \sum_{i,n} g_{in} \sigma_x^{(i)} (a_n e^{-i\delta_n t} + \text{h.c.}), \quad g_{in} = \frac{\eta_{in} \Omega_i}{2}, \quad \delta_n = \omega_n - \mu,$$

wobei μ der gemeinsame Abstand der beiden Seitenbandfelder vom Träger ist (für eine einzelne Mode ist das genau $\mu = \omega - \delta$ aus Gleichung (9.1)). Die Moden sind unabhängig, und dieselbe Magnus-Rechnung ergibt im Mittel (für lange Zeiten bzw. nach Schliessen aller Schleifen) eine effektive Ising-Wechselwirkung

$$H_{\text{eff}} = \hbar \sum_{i < j} J_{ij} X_i X_j, \quad J_{ij} = \Omega_i \Omega_j \sum_n \eta_{in} \eta_{jn} \frac{\omega_n}{\mu^2 - \omega_n^2} \quad (9.8)$$

Das ist die Standardformel der Ionenphysik [12, 14]. Nahe einer Mode ($\mu \approx \omega_n$) ist $\omega_n/(\mu^2 - \omega_n^2) \approx 1/(2(\mu - \omega_n)) = -1/(2\delta_n)$, und man erhält $J_{ij} \approx -\sum_n 2g_{in}g_{jn}/\delta_n$ – für zwei Ionen und eine Mode also $J = -2g^2/\delta$, in Übereinstimmung mit $U(t_g) = e^{-iJt_g X_1 X_2} = XX(-\chi)$ aus dem vorigen Abschnitt. In Matrixschreibweise mit $W = \text{diag}(\omega_n/(\mu^2 - \omega_n^2))$, der Matrix $\eta = (\eta_{in})$ und gleichen $\Omega_i = \Omega$:

$$J = \Omega^2 \eta W \eta^T. \quad (9.9)$$

Merksatz

Die Geometrie und Coulomb-Physik (Kapitel 7) bestimmen die Modenvektoren b_{in} und Frequenzen ω_n ; die Laser bestimmen Ω und μ und damit W . Durch die Wahl von μ *programmiert* man die Wechselwirkungsmatrix J .

9.4.2 Rechenbeispiel: die Drei-Ionen-Kette

Rechenbeispiel 9.3: Wie die Laserfrequenz die Kopplungspartner auswählt

Parameter aus Abschnitt 7.3 ($\nu_z = 1$ MHz), $\Omega = 2\pi \times 50$ kHz. Die Tabelle zeigt $J_{ij}/2\pi$ in Hz (code/k3_drei_ionen_moden.py):

Verstimmung μ	J_{12}	J_{13}	J_{23}
10 kHz über COM (ν_1)	1134	1144	1134
10 kHz über Streckmode (ν_2)	19	−973	19
10 kHz über Knickmode (ν_3)	−466	228	−466
weit weg (3 MHz)	−4.3	0.7	−4.3

Interpretation mit den Produkten $b_{in}b_{jn}$:

- Nahe COM dominiert $b_{i1}b_{j1} = \frac{1}{3}$ für alle Paare: gleichmässige „alle-mit-allen“-Kopplung.
- Nahe Streckmode dominiert $b_{12}b_{32} = -\frac{1}{2}$, während $b_{12}b_{22} = 0$: Praktisch nur Ion 1 und Ion 3 wechselwirken – über den Kopf des mittleren Ions hinweg.
- Nahe Knickmode: $b_{13}b_{23} = -\frac{1}{3}$, $b_{13}b_{33} = +\frac{1}{6}$ – Vorzeichen und Stärke wechseln.

- *Weit weg* tragen alle Moden bei, mit Vorzeichen, die sich teilweise aufheben; es bleibt eine schwache, mit dem Abstand abfallende Kopplung (in grossen Kristallen näherungsweise $J_{ij} \propto |i - j|^{-\alpha}$).

Die „Reichweite“ der Kopplung ist also nicht einfach „je näher, desto stärker“; sie entsteht aus der *Interferenz* aller Modenbeiträge.

9.4.3 Drei Ionen verschränken: der GHZ-Zustand

Beleuchtet man alle drei Ionen gleich stark nahe der COM-Mode, ist $g_{i1} = g$ für alle i und $S = g(X_1 + X_2 + X_3)$. Wieder gilt Gleichung (9.5), jetzt mit $S^2 = g^2(3 + 2 \sum_{i < j} X_i X_j)$. Mit $\delta = 4g$ und $t_g = 2\pi/\delta$ entsteht die paarweise Phase $\chi = \pi/4$ für *alle drei Paare gleichzeitig*. Die Simulation liefert aus $|000\rangle$

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle),$$

einen verschränkten Zustand, der in einer gedrehten Basis ein GHZ-Zustand ist. Eine anschliessende globale Drehung $R_x(\pi/2)^{\otimes 3} = \exp(-i\frac{\pi}{4} \sum_i X_i)$ macht daraus

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + i|111\rangle). \quad (9.10)$$

(Für eine gerade Ionenanzahl entsteht der GHZ-Zustand direkt; für ungerade braucht es die zusätzliche Drehung [10].) Ein einziger Puls verschränkt also alle Ionen, die die Mode teilen – ein Vorteil gegenüber Architekturen mit nur nächsten-Nachbar-Kopplung.

9.5 Und in getrennten Mikrofallen?

In Modell B (ZuriQ-artig) sind die Moden nur um wenige kHz aufgespalten (Abschnitt 7.2.2). Für zwei Fallen gibt es eine COM-Mode ($b = (1, 1)/\sqrt{2}$) und eine Relativmode ($b = (1, -1)/\sqrt{2}$) mit $\Delta\nu = -\varepsilon\nu$. In Gleichung (9.8) tragen beide mit entgegengesetztem Vorzeichen bei; ist μ weit von beiden entfernt, heben sie sich fast auf. Man muss daher nahe an *einer* Mode arbeiten, und zwar mit einer Verstimmung, die vergleichbar mit der Modenaufspaltung ist.

Rechenbeispiel 9.4: Zwei Ionen in Mikrofallen

$^9\text{Be}^+$, $\nu = 2,5$ MHz, Raman-Geometrie wie oben ($\eta_0 = 0.104$), $\Omega = 2\pi \times 50$ kHz, μ oberhalb der COM-Mode (`code/k3b_zwei_mikrofallen_gate.py`). Die Kopplung an die COM-Mode ist $g = \eta\Omega/2 = 2\pi \times 1,85$ kHz; die effektive Beschreibung mit J_{12} ist nur gültig, wenn die Verstimmung $|\delta| \gtrsim 4g \approx 2\pi \times 7,4$ kHz ist (dann schliessen sich die Schleifen mehrfach während des Gates). Gatezeit für $\chi = J_{12}t_g = \pi/4$ und Zahl K der Phasenraumschleifen der COM-Mode:

	$d = 30 \mu\text{m}$ ($\Delta\nu = 5,8$ kHz)			$d = 50 \mu\text{m}$ ($\Delta\nu = 1,25$ kHz)		
$\mu - \omega_{\text{COM}}$	$J_{12}/2\pi$	t_g	K	$J_{12}/2\pi$	t_g	K
10 kHz	249 Hz	0,50 ms	5	75 Hz	1,7 ms	17
20 kHz	76 Hz	1,6 ms	33	20 Hz	6,3 ms	126
50 kHz	13,9 Hz	9,0 ms	451	3,3 Hz	38 ms	1920
100 kHz	3,6 Hz	35 ms	3489	0,8 Hz	155 ms	15472

Fern der Moden fällt J_{12} wie $\Delta\nu/\delta^2$, weil sich die Beiträge der beiden Moden fast aufheben. Weil $J \propto \Omega^2$, verkürzt ein zehnmal stärkerer Laser die Gatezeit um den Faktor 100 (bei entsprechend grösserem $|\delta|$). Weitere Wege zu schnellen Gates sind (i) kleine Abstände durch

Zusammenschieben der Ionen vor dem Gate und (ii) Pulse mit Verstimmungen im Bereich der Modenaufspaltung, deren Phasenraumbahnen für *beide* Moden gleichzeitig schliessen. Jain et al. [2] diskutieren zudem Gates über die radialen Moden, die in Mikro-Penning-Fallen besonders grosse Nullpunktsbewegungen haben können.

9.6 Die Brücke zur Störungstheorie: virtuelle Phononen

Man kann J_{ij} auch ohne Magnus-Entwicklung verstehen. Ist die Verstimmung δ gross gegen die Kopplung g , wird die Mode nur *virtuell* angeregt. Eine Schrieffer–Wolff-Transformation e^S mit $[H_0, S] = -V$ eliminiert den Spin–Phonon-Term V in erster Ordnung und hinterlässt

$$H_{\text{eff}} \approx H_0 + \frac{1}{2}[S, V]. \quad (9.11)$$

Weil V linear in Spin und Phonon ist, ist $[S, V]$ quadratisch in den Spins und unabhängig von der Phononenzahl: Das ist $\sum J_{ij} X_i X_j$. Das Bild: Ion i emittiert ein virtuelles Phonon, Ion j absorbiert es – analog zum Austausch virtueller Photonen, der die Coulomb-Kraft vermittelt.

Zusammenfassung: Wie Phononen Qubits verschränken

1. Die Coulomb-Kraft koppelt die Bewegungen; in harmonischer Näherung entstehen kollektive Eigenmoden $\mathbf{b}_n$.
2. Ein Laser mit Impulsübertrag koppelt jedes Qubit an jede Mode, mit Stärke $\eta_{in} \propto b_{in}$.
3. Eine spinabhängige Kraft schiebt die Mode im Phasenraum im Kreis; die Fläche hängt von der *Summe* der Spins ab.
4. Nach geschlossener Schleife ist die Bewegung unverändert, aber die Qubits haben eine zustandsabhängige Phase $\propto X_i X_j$ erworben: ein verschränkendes Gate.



Teil IV

Rechnen mit dem Ionen-Quantencomputer

Kapitel 10

Vom Schaltkreis zum Laserpuls: Wie man mit Ionen rechnet

10.1 Der native Gatesatz

Ein Quantenprogramm wird als Schaltkreis aus abstrakten Gates geschrieben (H, CNOT, CP, ...). Die Hardware kann aber nur ihre *nativen* Operationen ausführen. Für Ionen sind das:

Gate	Physik	typische Dauer
$R_\phi(\theta) = e^{-i\frac{\theta}{2}(\cos\phi X + \sin\phi Y)}$	resonanter Raman- oder Mikrowellenpuls	1 μ s bis 10 μ s
$R_z(\theta)$	<i>virtuell</i> : Phase aller folgenden Pulse verschieben	0 s
$XX(\chi) = e^{-i\chi X_i X_j}$	Mølmer-Sørensen-Gate (Kapitel 9)	10 μ s bis 200 μ s
Messung in Z	zustandsabhängige Fluoreszenz	0,1 ms bis 1 ms

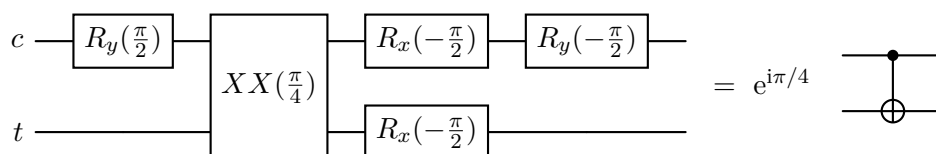
Warum R_z nichts kostet

Eine Drehung um z ändert nur die relative Phase zwischen $|0\rangle$ und $|1\rangle$. Da alle weiteren Pulse relativ zur Laserphase definiert sind, kann man statt das Qubit zu drehen einfach das *Bezugssystem* drehen, d. h. die Phase ϕ aller späteren Pulse auf diesem Qubit um θ verschieben. Das ist reine Buchhaltung in der Steuersoftware.

10.2 Kompilieren: CNOT und CPhase aus nativen Gates

Rechenbeispiel 10.1: CNOT aus einem Mølmer-Sørensen-Gate

Eine systematische Suche über Vorzeichen (`code/k5_gates_qft_messung.py`) findet, in zeitlicher Reihenfolge von links nach rechts (c : Kontrolle, t : Ziel):



Als Matrixprodukt (rechts wirkt zuerst): $\text{CNOT} = e^{-i\pi/4} [R_y(-\frac{\pi}{2}) \otimes \mathbb{I}] [R_x(-\frac{\pi}{2}) \otimes R_x(-\frac{\pi}{2})] XX(\frac{\pi}{4}) [R_y(\frac{\pi}{2}) \otimes \mathbb{I}]$. Ein CNOT kostet also *ein* MS-Gate und vier Ein-Qubit-Pulse

[16]. Übung: Prüfen Sie die Gleichung mit NumPy für alle vier Basiszustände.

Rechenbeispiel 10.2: Kontrollierte Phase aus ZZ

Für die QFT brauchen wir $CP(\varphi) = \text{diag}(1, 1, 1, e^{i\varphi})$. Der Trick: Der Projektor auf $|11\rangle$ ist $|11\rangle\langle 11| = \frac{1}{4}(\mathbb{I} - Z_1)(\mathbb{I} - Z_2) = \frac{1}{4}(\mathbb{I} - Z_1 - Z_2 + Z_1Z_2)$. Da alle Terme vertauschen,

$$CP(\varphi) = e^{i\varphi|11\rangle\langle 11|} = e^{i\varphi/4} e^{-i\frac{\varphi}{4}Z_1} e^{-i\frac{\varphi}{4}Z_2} e^{+i\frac{\varphi}{4}Z_1Z_2} = e^{i\varphi/4} R_z(\frac{\varphi}{2}) \otimes R_z(\frac{\varphi}{2}) \cdot ZZ(-\frac{\varphi}{4}).$$

Und $ZZ(\chi) = (H \otimes H) XX(\chi) (H \otimes H)$, weil $HXH = Z$. Ergebnis: Eine kontrollierte Phase kostet ein MS-Gate mit Winkel $\chi = -\varphi/4$ (statt $\pi/4$ beim CNOT) plus Ein-Qubit-Gates, von denen die R_z virtuell sind. Für die QFT mit $\varphi = \pi/2, \pi/4, \dots$ braucht man also MS-Gates mit *kleineren* Winkeln – also kürzere Pulse oder schwächere Laser.

10.3 Ablauf einer Rechnung auf dem Ionen-Chip

Eine einzelne Ausführung (*Shot*) eines Quantenprogramms besteht aus:

1. **Doppler-Kühlung** (~ 1 ms) auf $\bar{n} \approx 3$.
2. **Seitenbandkühlung** (einige ms) aller relevanten Moden auf $\bar{n} \lesssim 0.05$.
3. **Optisches Pumpen** aller Qubits nach $|0\rangle = |\uparrow\rangle$.
4. **Transport** (bei ZuriQ): Ionen an die Positionen fahren, an denen sie wechselwirken sollen.
5. **Gatesequenz**: Pulsfolge aus $R_\phi(\theta)$, $XX(\chi)$ und virtuellen R_z .
6. **Auslese**: Fluoreszenzdetektion jedes Ions mit Kamera oder Photomultiplier.

Dann wiederholt man das Ganze S -mal und erhält ein Histogramm der Bitstrings. Das Ergebnis eines Quantencomputers ist immer eine *Stichprobe* aus der Verteilung $P(x) = |c_x|^2$.

10.4 Auslese als Klassifikationsproblem

Während der Detektionszeit zählt man die Photonen n eines Ions. Die Zahl ist Poisson-verteilt: im hellen Zustand $|\uparrow\rangle$ mit Mittelwert λ_b , im dunklen Zustand $|\downarrow\rangle$ mit kleinem Untergrund λ_d (Streulicht, Dunkelzählrate). Man entscheidet mit einer Schwelle n_{th} : „hell“, falls $n \geq n_{\text{th}}$.

Rechenbeispiel 10.3: Optimale Schwelle

$\lambda_b = 12$, $\lambda_d = 0.3$ (Abb. 10.1). Fehlerwahrscheinlichkeiten $\epsilon_d = P(n \geq n_{\text{th}} \mid \text{dunkel})$ und $\epsilon_b = P(n < n_{\text{th}} \mid \text{hell})$:

n_{th}	ϵ_d	ϵ_b	Mittel
1	2.6×10^{-1}	6.1×10^{-6}	1.3×10^{-1}
2	3.7×10^{-2}	8.0×10^{-5}	1.9×10^{-2}
3	3.6×10^{-3}	5.2×10^{-4}	2.1×10^{-3}
4	2.7×10^{-4}	2.3×10^{-3}	1.3×10^{-3}
5	1.6×10^{-5}	7.6×10^{-3}	3.8×10^{-3}

Die optimale Schwelle ist $n_{\text{th}} = 4$ mit einer mittleren Auslesefidelity von 99,87 %. Das ist ein Bayes-Klassifikator mit gleichen Priors und eindimensionalem Merkmal. In der Praxis begrenzen zusätzlich *Depumping*-Prozesse während der Detektion (ein helles Ion wird durch nicht-resonante Streuung dunkel) die Fidelity.

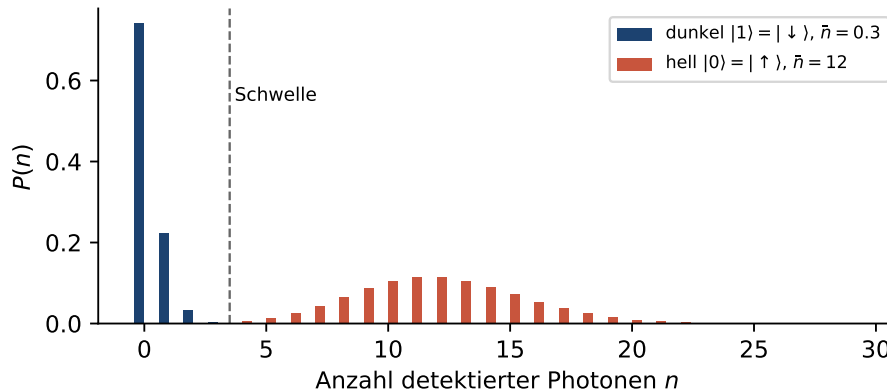


Abbildung 10.1: Photonenzahl-Verteilungen eines hellen und eines dunklen Ions und optimale Schwelle.

Data-Science-Brille: Ausleseentfaltung mit der Konfusionsmatrix

Die Auslesefehler bilden eine Konfusionsmatrix $C = \begin{pmatrix} 1-\epsilon_b & \epsilon_d \\ \epsilon_b & 1-\epsilon_d \end{pmatrix}$, die wahre Verteilung $\vec{p}$ in die beobachtete $\vec{p}_{\text{obs}} = C\vec{p}$ abbildet. Kennt man C aus Kalibrationsmessungen, schätzt man $\vec{p} = C^{-1}\vec{p}_{\text{obs}}$. Beispiel: $\epsilon_b = 0.02$, $\epsilon_d = 0.01$, beobachtet $P_{\text{obs}}(0) = 0.50$. Dann $P(0) = (0.50 - \epsilon_d)/(1 - \epsilon_b - \epsilon_d) = 0.49/0.97 = 0.505$. Für n Qubits ist C eine $2^n \times 2^n$ -Matrix (bei unabhängigen Fehlern das Kronecker-Produkt der Einzelmatrizen).

10.5 Statistik: Wie viele Shots braucht man?

Jede Wahrscheinlichkeit wird aus S Bernoulli-Versuchen geschätzt; die Standardabweichung ist

$$\sigma_{\hat{p}} = \sqrt{\frac{p(1-p)}{S}} \leq \frac{1}{2\sqrt{S}}. \quad (10.1)$$

Rechenbeispiel 10.4: Shot-Budget

Für eine Genauigkeit von ± 0.01 bei $p \approx 0.5$ braucht man $S = p(1-p)/\sigma^2 = 2500$ Shots, für ± 0.001 schon 250 000. Bei rund 10 ms pro Shot (Kühlen dominiert) sind das 25 s bzw. 42 min. Die Präzision wächst nur mit $\sqrt{S}$ – ein Grund, warum Quantenalgorithmen so gebaut werden, dass die Antwort mit *hoher* Wahrscheinlichkeit in wenigen Messergebnissen konzentriert ist (wie bei Shor).

Rechenbeispiel 10.5: Fidelity eines Bell-Zustands aus Korrelationen schätzen

Die Dichtematrix des Zielzustands $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$ hat die Pauli-Zerlegung $|\Psi\rangle\langle\Psi| = \frac{1}{4}(\mathbb{I} + X_1Y_2 + Y_1X_2 + Z_1Z_2)$ (nachrechnen!). Also ist die Fidelity eines gemessenen Zustands ρ

$$F = \text{Tr}(\rho|\Psi\rangle\langle\Psi|) = \frac{1}{4}(1 + \langle XY \rangle + \langle YX \rangle + \langle ZZ \rangle).$$

Man misst drei Korrelatoren (dafür dreht man vor der Messung in die X - bzw. Y -Basis). Beispielmesswerte $\langle ZZ \rangle = 0.98$, $\langle XY \rangle = 0.95$, $\langle YX \rangle = 0.96$ ergeben $F = 0.9725$. Mit je $S = 1000$ Shots ist die Unsicherheit jedes Korrelators etwa $\sqrt{(1 - \langle \cdot \rangle^2)/S} \approx 0.01$, also $\sigma_F \approx \frac{1}{4}\sqrt{3} \cdot 0.01 \approx 0.004$.

10.6 Konnektivität und Transport

In einer linearen Paul-Kette können alle Ionen über gemeinsame Moden gekoppelt werden, aber mit wachsender Ionenanzahl rücken die Moden zusammen und die Gates werden langsamer. Die QCCD-Architektur (*quantum charge-coupled device*) teilt die Ionen deshalb in kleine Gruppen und transportiert sie zwischen Zonen. In Paul-Fallen braucht Transport in 2D jedoch Kreuzungen (*junctions*), an denen das RF-Feld Störungen verursacht. In der Penning-Mikrofalle entfällt dieses Problem: Ionen lassen sich in *jeder* Richtung über den Chip bewegen [1, 3]. Für einen Schaltkreis bedeutet das: Zwei Qubits, die ein Gate ausführen sollen, werden zusammengefahren (grosses $t_{ij} \propto d^{-3}$), gekoppelt und wieder getrennt.

Kapitel 11

Die Quanten-Fourier-Transformation

11.1 Definition und Verwandtschaft mit der FFT

Für ein Register aus n Qubits, $Q = 2^n$, ist die Quanten-Fourier-Transformation die unitäre Abbildung

$$\text{QFT}_Q |x\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} e^{2\pi i x k / Q} |k\rangle, \quad (\text{QFT}_Q)_{kx} = \frac{\omega^{xk}}{\sqrt{Q}}, \quad \omega = e^{2\pi i / Q}. \quad (11.1)$$

Auf einen allgemeinen Zustand $\sum_x c_x |x\rangle$ wirkt sie wie die diskrete Fourier-Transformation der Amplituden.

Data-Science-Brille: QFT = ifft

NumPy definiert $\text{fft}(c)_k = \sum_x c_x e^{-2\pi i x k / Q}$ und $\text{ifft}(c)_k = \frac{1}{Q} \sum_x c_x e^{+2\pi i x k / Q}$. Die QFT hat das Vorzeichen der inversen Transformation und die unitäre Normierung, also

$$\text{QFT}_Q \vec{c} = \sqrt{Q} \cdot \text{numpy.fft.ifft}(\vec{c}).$$

Das Programm `code/k5_gates_qft_messung.py` prüft das. Der Unterschied liegt nicht in der Mathematik, sondern im Zugriff: Die FFT liefert alle Q Koeffizienten; die QFT erzeugt einen Zustand, aus dem eine Messung nur *einen* Index k zieht, mit Wahrscheinlichkeit $|\tilde{c}_k|^2$. Die QFT beschleunigt daher nicht „die Fourier-Analyse Ihrer Daten“, sondern ist nur dann nützlich, wenn die Antwort in wenigen dominanten Frequenzen steckt – wie bei der Periodensuche.

Rechenbeispiel 11.1: Die 4×4 -QFT

Für $n = 2$, $Q = 4$, $\omega = i$:

$$\text{QFT}_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Angewandt auf den periodischen Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)$ (Periode 2) ergibt sich $\frac{1}{2\sqrt{2}}[(1+1)|0\rangle + (1-1)|1\rangle + (1+1)|2\rangle + (1-1)|3\rangle] = \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)$: Die Amplituden bei $k = 1, 3$ löschen sich aus, übrig bleiben die Vielfachen von $Q/r = 2$.

11.2 Die Produktdarstellung

Der Schlüssel zu einem effizienten Schaltkreis ist die Binärdarstellung. Wir schreiben $x = x_{n-1} \dots x_1 x_0$ ($x = \sum_j x_j 2^j$) und verwenden Binärbrüche $0.x_j x_{j-1} \dots x_0 = x_j/2 + x_{j-1}/4 + \dots$. Mit $k = \sum_l k_l 2^l$ zerfällt die Phase:

$$e^{2\pi i x k / 2^n} = \prod_{l=0}^{n-1} e^{2\pi i x k_l 2^l / 2^n},$$

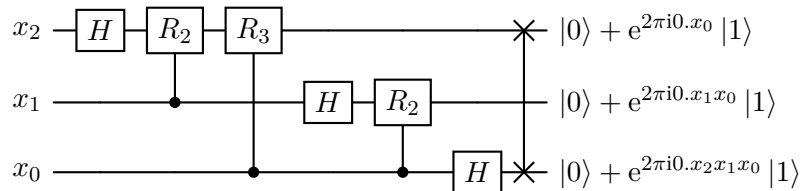
und weil ganzzahlige Anteile von $x 2^l / 2^n$ keinen Beitrag liefern, bleibt für das Bit k_l nur der gebrochene Anteil $0.x_{n-1-l} \dots x_0$. Damit faktorisiert die QFT eines Basiszustands:

$$\text{QFT} |x\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i 0.x_0} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0.x_1 x_0} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i 0.x_{n-1} \dots x_0} |1\rangle) \quad (11.2)$$

(das linke Qubit ist das höchstwertige Ausgangsbit k_{n-1}). Die QFT eines Basiszustands ist also ein *Produktzustand* – sie kodiert die Zahl x in den Phasen der einzelnen Qubits.

11.3 Der Schaltkreis

Jeder Faktor in Gleichung (11.2) lässt sich mit einem Hadamard (liefert $|0\rangle + e^{2\pi i 0.x_j} |1\rangle$) und kontrollierten Phasen $R_m = \text{diag}(1, e^{2\pi i / 2^m})$ von den niedrigeren Bits erzeugen. Für drei Qubits (Eingang $|x_2 x_1 x_0\rangle$):



Nach dem Hadamard auf x_2 und den kontrollierten Rotationen R_2 (Phase $\pi/2$, kontrolliert von x_1) und R_3 (Phase $\pi/4$, von x_0) trägt die oberste Leitung $|0\rangle + e^{2\pi i 0.x_2 x_1 x_0} |1\rangle$; entsprechend die anderen. Der SWAP am Ende stellt die Bitreihenfolge von Gleichung (11.2) her. Das Programm bestätigt: Der Schaltkreis ist für $n = 3$ und $n = 4$ bis auf Rundung gleich der QFT-Matrix.

Rechenbeispiel 11.2: $\text{QFT}_8 |5\rangle$ explizit

$5 = 101_2$, also $x_2 = 1, x_1 = 0, x_0 = 1$. Die drei Binärbrüche sind $0.x_0 = 0.1_2 = \frac{1}{2}$, $0.x_1 x_0 = 0.01_2 = \frac{1}{4}$, $0.x_2 x_1 x_0 = 0.101_2 = \frac{5}{8}$:

$$\text{QFT}_8 |5\rangle = \frac{1}{\sqrt{8}} (|0\rangle - |1\rangle) \otimes (|0\rangle + i |1\rangle) \otimes (|0\rangle + e^{5\pi i / 4} |1\rangle).$$

Ausmultipliziert sind die acht Amplituden $\frac{1}{\sqrt{8}} e^{2\pi i \cdot 5k/8}$, $k = 0, \dots, 7$:

$$\sqrt{8} \text{QFT}_8 |5\rangle = \left(1, -\frac{1+i}{\sqrt{2}}, i, \frac{1-i}{\sqrt{2}}, -1, \frac{1+i}{\sqrt{2}}, -i, \frac{-1+i}{\sqrt{2}} \right)^T.$$

Alle acht Amplituden haben Betrag $1/\sqrt{8}$: Eine Messung direkt nach der QFT eines Basiszustands liefert völlig zufällige Ergebnisse. Die Information steckt in den Phasen – sichtbar wird sie erst durch Interferenz mit anderen Termen, wie im Shor-Algorithmus.

11.4 Aufwand

Die n -Qubit-QFT braucht n Hadamards, $n(n-1)/2$ kontrollierte Phasen und $\lfloor n/2 \rfloor$ SWAPs, also $O(n^2)$ Gates. Die klassische FFT auf 2^n Werten braucht $O(n2^n)$ Operationen:

n	H	CP	klassische FFT $\sim n2^n$
3	3	3	24
10	10	45	1.0×10^4
20	20	190	2.1×10^7
50	50	1225	5.6×10^{16}

Die Rotationen R_m mit grossem m haben winzige Winkel $2\pi/2^m$; lässt man alle mit $m > \log_2 n + O(1)$ weg (*approximative QFT*), sinkt der Aufwand auf $O(n \log n)$ bei vernachlässigbarem Fehler.

Auf der Ionen-Hardware. Jedes $CP(\varphi)$ wird nach Abschnitt 10.2 zu einem MS-Gate mit $\chi = -\varphi/4$ plus Ein-Qubit-Pulsen. Die 3-Qubit-QFT braucht also drei MS-Gates (Winkel $\pi/8, \pi/16, \pi/8$) und die SWAP-Operation, die man auf Ionen oft gar nicht ausführt: Man benennt die Qubits einfach um – oder transportiert die Ionen physisch, was in der Penning-Mikrofalle besonders natürlich ist.

Kapitel 12

Der Shor-Algorithmus

12.1 Worum es geht

Gegeben ist eine zusammengesetzte ganze Zahl N , etwa das Produkt zweier grosser Primzahlen. Gesucht sind ihre Faktoren. Die besten bekannten klassischen Algorithmen (das Zahlkörpersieb) brauchen eine Laufzeit, die in der Stellenzahl $n = \log_2 N$ *subexponentiell*, aber schneller als jedes Polynom wächst, etwa $\exp(c n^{1/3} (\log n)^{2/3})$. Peter Shor zeigte 1994 [18], dass ein Quantencomputer das Problem in *polynomieller* Zeit, grob $O(n^3)$ Gates, löst.

Rechenbeispiel 12.1: Warum Faktorisieren wichtig ist: RSA im Kleinen

Wähle $p = 3$, $q = 11$, also $N = 33$ und $\varphi(N) = (p - 1)(q - 1) = 20$. Öffentlicher Exponent $e = 3$ (teilerfremd zu 20), privater Exponent $d = 7$, denn $3 \cdot 7 = 21 \equiv 1 \pmod{20}$.

- Verschlüsseln der Nachricht $m = 4$: $c = m^e \bmod N = 4^3 \bmod 33 = 64 \bmod 33 = 31$.
- Entschlüsseln: $c^d \bmod N = 31^7 \bmod 33$. Mit $31 \equiv -2$: $(-2)^7 = -128 \equiv -128 + 4 \cdot 33 = 4$.
✓

Jeder kennt $(N, e) = (33, 3)$. Wer $N = 3 \cdot 11$ faktorisieren kann, berechnet $\varphi(N)$ und daraus d – und kann mitlesen. Bei RSA-2048 hat N rund 617 Dezimalstellen.

Der Algorithmus besteht aus einem klassischen Rahmen und einem einzigen Quantenunterprogramm, der *Periodensuche*. Wir gehen beides Schritt für Schritt durch.

12.2 Werkzeugkasten Zahlentheorie

12.2.1 Modulare Arithmetik

$a \equiv b \pmod{N}$ heisst: N teilt $a - b$. Man rechnet mit Resten: $17 \bmod 5 = 2$, $(7 \cdot 8) \bmod 15 = 56 \bmod 15 = 11$.

12.2.2 Grösster gemeinsamer Teiler: der Euklidische Algorithmus

$\text{ggT}(a, b)$ berechnet man durch wiederholte Division mit Rest, $\text{ggT}(a, b) = \text{ggT}(b, a \bmod b)$, in $O(\log \min(a, b))$ Schritten – klassisch schnell.

Rechenbeispiel 12.2: Euklid

ggT(21, 9): $21 = 2 \cdot 9 + 3$, $9 = 3 \cdot 3 + 0 \Rightarrow \text{ggT} = 3$.

ggT(1071, 462): $1071 = 2 \cdot 462 + 147$, $462 = 3 \cdot 147 + 21$, $147 = 7 \cdot 21 + 0 \Rightarrow \text{ggT} = 21$.

12.2.3 Die Ordnung

Für a mit $\text{ggT}(a, N) = 1$ ist die *Ordnung* $r = \text{ord}_N(a)$ die kleinste positive Zahl mit

$$a^r \equiv 1 \pmod{N}. \quad (12.1)$$

Die Funktion $f(x) = a^x \bmod N$ ist dann periodisch mit Periode r : $f(x+r) = a^x a^r \bmod N = f(x)$. Nach dem Satz von Euler teilt r die Zahl $\varphi(N)$; insbesondere ist $r < N$.

12.2.4 Schnelles Potenzieren

$a^x \bmod N$ für grosse x berechnet man durch wiederholtes Quadrieren:

Rechenbeispiel 12.3: Square-and-Multiply

$2^{13} \bmod 21$ mit $13 = 1101_2 = 8 + 4 + 1$: $2^1 = 2$, $2^2 = 4$, $2^4 = 16$, $2^8 = 16^2 = 256 \equiv 4 \pmod{21}$.

Also $2^{13} = 2^8 \cdot 2^4 \cdot 2^1 \equiv 4 \cdot 16 \cdot 2 = 128 \equiv 2 \pmod{21}$. (Kontrolle: $2^{13} = 8192 = 390 \cdot 21 + 2$.)

Man braucht nur $O(\log x)$ Multiplikationen. *Genau diese Zerlegung in Potenzen a^{2^j} verwendet auch der Quantenschaltkreis.*

12.3 Von der Faktorisierung zur Periodensuche**Satz (Reduktion)**

Sei N ungerade, keine Primzahlpotenz, $\text{ggT}(a, N) = 1$ und $r = \text{ord}_N(a)$. Ist r gerade und $a^{r/2} \not\equiv -1 \pmod{N}$, dann sind

$$p = \text{ggT}(a^{r/2} - 1, N), \quad q = \text{ggT}(a^{r/2} + 1, N)$$

nichttriviale Teiler von N .

Beweis. Aus $a^r \equiv 1$ folgt $N \mid a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$. N teilt nicht $a^{r/2} - 1$, sonst wäre schon $a^{r/2} \equiv 1$ und r nicht minimal. N teilt nicht $a^{r/2} + 1$, das ist die Voraussetzung $a^{r/2} \not\equiv -1$. N teilt also das Produkt, aber keinen der Faktoren – folglich müssen die Primfaktoren von N auf beide Faktoren verteilt sein, und beide ggT sind echte Teiler. $\square$

Rechenbeispiel 12.4: Alle Basen für $N = 15$

a	r	$a^{r/2} \bmod 15$	$\text{ggT}(a^{r/2} - 1, 15)$	$\text{ggT}(a^{r/2} + 1, 15)$	Ergebnis
2	4	4	3	5	✓
4	2	4	3	5	✓
7	4	4	3	5	✓
8	4	4	3	5	✓
11	2	11	5	3	✓
13	4	4	3	5	✓
14	2	14	–	–	× ($14 \equiv -1$)

Die Basen 3, 5, 6, 9, 10, 12 haben schon $\text{ggT}(a, 15) > 1$ – Glückstreffer ohne Quantencomputer. Von den sieben teilerfremden Basen funktionieren sechs.

Rechenbeispiel 12.5: $N = 21$: auch Misserfolge

Für $a = 2$: $2^1, \dots, 2^6 \equiv 2, 4, 8, 16, 11, 1$, also $r = 6$, $2^3 = 8$, $\text{ggT}(7, 21) = 7$, $\text{ggT}(9, 21) = 3$. ✓
Für $a = 4$: $r = 3$ ungerade ×. Für $a = 5$: $r = 6$, aber $5^3 = 125 \equiv 20 \equiv -1$ ×. Insgesamt sind 6 der 11 teilerfremden Basen erfolgreich.

Allgemein gilt: Hat N genau m verschiedene ungerade Primfaktoren, dann ist ein zufällig gewähltes teilerfremdes a mit Wahrscheinlichkeit mindestens $1 - 2^{1-m}$ erfolgreich [17]; für $N = pq$ also mindestens $\frac{1}{2}$. Nach wenigen Versuchen hat man einen Faktor.

Achtung

Bis hierhin ist keine Quantenmechanik im Spiel. Das Einzige, was klassisch schwer ist, ist die *Ordnung* r . Für N mit hunderten Stellen ist r typischerweise astronomisch gross, und die Folge $a^x \bmod N$ sieht zufällig aus.

12.4 Der Quantenteil: Periodensuche

12.4.1 Register und Grössen

Man verwendet zwei Register:

- ein *Eingangsregister* mit t Qubits für $x \in \{0, \dots, Q - 1\}$, $Q = 2^t$ mit $N^2 \leq Q < 2N^2$;
- ein *Arbeitsregister* mit $L = \lceil \log_2 N \rceil$ Qubits für die Werte $f(x)$.

Für $N = 15$: $N^2 = 225$, also $Q = 256$, $t = 8$, $L = 4$. Für $N = 21$: $N^2 = 441$, $Q = 512$, $t = 9$, $L = 5$.

12.4.2 Schritt 1: gleichmässige Superposition

Hadamards auf alle t Eingangsqubits:

$$H^{\otimes t} |0\rangle^{\otimes t} |0\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle. \quad (12.2)$$

12.4.3 Schritt 2: modulare Exponentiation

Ein reversibler Schaltkreis $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$ berechnet f auf allen Komponenten gleichzeitig:

$$|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |a^x \bmod N\rangle. \quad (12.3)$$

Für $N = 15$, $a = 2$: $|\psi_2\rangle \propto |0\rangle |1\rangle + |1\rangle |2\rangle + |2\rangle |4\rangle + |3\rangle |8\rangle + |4\rangle |1\rangle + |5\rangle |2\rangle + \dots$ Die Register sind jetzt verschränkt, und die Periodizität $r = 4$ steckt in der Struktur des Zustands.

Quantenparallelismus ist nicht genug

Gleichung (12.3) enthält alle Q Funktionswerte. Misst man jetzt, erhält man aber nur ein zufälliges Paar $(x, f(x))$ – nicht mehr als eine klassische Auswertung. Der Trick besteht darin, die globale Eigenschaft „Periodizität“ durch Interferenz in wenige wahrscheinliche Messergebnisse zu übersetzen.

12.4.4 Schritt 3 (gedanklich): Messen des Arbeitsregisters

Wir können uns vorstellen, das Arbeitsregister zu messen (das ändert die Statistik des Eingangsregisters nicht – *Prinzip der aufgeschobenen Messung*). Erhält man den Wert $y_0 = f(x_0)$, bleiben im Eingangsregister nur die x mit $f(x) = y_0$, also $x = x_0, x_0 + r, x_0 + 2r, \dots$:

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |x_0 + jr\rangle, \quad M \approx Q/r. \quad (12.4)$$

Rechenbeispiel 12.6: Der Zweig $f(x) = 1$

Für $N = 15$, $a = 2$, $Q = 256$ und $y_0 = 1$: $x \in \{0, 4, 8, \dots, 252\}$, also $M = 64$. Für $N = 21$, $a = 2$, $Q = 512$, $y_0 = 1$: $x \in \{0, 6, 12, \dots, 510\}$, also $M = 86$. Beachten Sie: $512/6 = 85.33$ ist keine ganze Zahl – dieser Fall ist der realistische.

Messen wir das Eingangsregister jetzt direkt, erhalten wir ein zufälliges $x_0 + jr$; wegen des unbekannten, zufälligen Offsets x_0 nützt das nichts. Deshalb:

12.4.5 Schritt 4: QFT und Interferenz

Anwenden der QFT auf Gleichung (12.4):

$$\text{QFT } |\psi_3\rangle = \sum_{k=0}^{Q-1} A(k) |k\rangle, \quad A(k) = \frac{e^{2\pi i k x_0 / Q}}{\sqrt{MQ}} \sum_{j=0}^{M-1} e^{2\pi i k r j / Q}. \quad (12.5)$$

Der Offset x_0 steckt nur noch in einer Phase vor der Summe – er fällt aus $|A(k)|^2$ heraus! Die Summe ist eine geometrische Reihe in $z = e^{2\pi i k r / Q}$:

$$\sum_{j=0}^{M-1} z^j = \frac{1 - z^M}{1 - z} \quad \Rightarrow \quad P(k) = |A(k)|^2 = \frac{1}{MQ} \frac{\sin^2(\pi k r M / Q)}{\sin^2(\pi k r / Q)} \quad (12.6)$$

(mit $|1 - e^{i\theta}| = 2|\sin(\theta/2)|$). Das ist ein *Fejér-Kern* – dieselbe Funktion wie das Beugungsmuster eines optischen Gitters mit M Spalten. Er hat scharfe Maxima, wenn kr/Q ganzzahlig ist:

$$\frac{k}{Q} \approx \frac{s}{r}, \quad s = 0, 1, \dots, r-1 \quad (12.7)$$

Zeigerbild der Interferenz

Jeder Summand z^j ist ein Einheitszeiger in der komplexen Ebene, jeder um den Winkel $2\pi kr/Q$ gegen den vorigen gedreht. Passt dieser Winkel zu einem Vielfachen von 2π , zeigen alle M Zeiger in dieselbe Richtung, und die Summe hat Länge M (konstruktive Interferenz). Sonst laufen die Zeiger im Kreis und die Summe bleibt klein (Abb. 12.1).

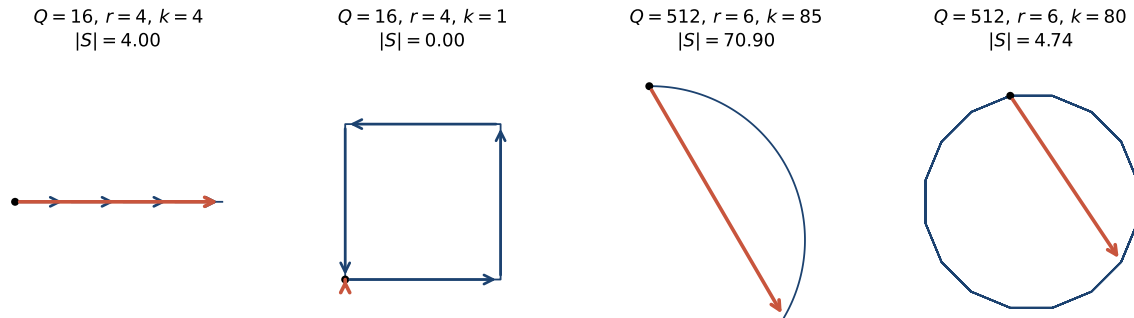


Abbildung 12.1: Die Summe $S = \sum_j z^j$ als Kette von Zeigern (schwarzer Punkt: Ursprung, roter Pfeil: Summe). Links: $Q = 16$, $r = 4$, $M = 4$. Für $k = 4$ sind alle Zeiger parallel, $|S| = 4$; für $k = 1$ schliessen sie ein Quadrat, $|S| = 0$. Rechts: $Q = 512$, $r = 6$, $M = 86$. Für $k = 85 \approx 512/6$ krümmt sich die Kette nur leicht, $|S| = 70.9$ (von maximal 86); für $k = 80$ läuft sie im Kreis, $|S| = 4.7$.

Rechenbeispiel 12.7: Der perfekte Fall: r teilt Q

$Q = 16$, $r = 4$, $M = 4$. Für $k = 4$: $z = e^{2\pi i \cdot 16/16} = 1$, $S = 4$. Für $k = 1$: $z = e^{2\pi i \cdot 4/16} = i$, $S = 1 + i - 1 - i = 0$. Allgemein gilt für $r \mid Q$: $P(k) = 1/r$ genau für $k \in \{0, Q/r, 2Q/r, \dots\}$ und sonst exakt null. Für $N = 15$, $a = 2$, $Q = 256$ liefert die Simulation $P(0) = P(64) = P(128) = P(192) = 0.25$ (Abb. 12.2, oben).

Rechenbeispiel 12.8: Der realistische Fall: $N = 21$, $r = 6$

Jetzt ist $Q/r = 85.33$ keine ganze Zahl. Die Peaks liegen bei den ganzen Zahlen nahe 85.33 s . Die exakte Verteilung (`code/k6_shor.py`, über alle Zweige y_0 summiert):

k	$P(k)$	k/Q	nächster Bruch s/r	Kandidat für r
0	0.1667	0.00000	0/1	– (nutzlos)
85	0.1140	0.16602	1/6	6
86	0.0285	0.16797	1/6	6
171	0.1140	0.33398	1/3	3 (nur ein Teiler von r)
256	0.1667	0.50000	1/2	2 (nur ein Teiler von r)
341	0.1140	0.66602	2/3	3
427	0.1140	0.83398	5/6	6

Für den Zweig $y_0 = 1$ mit $M = 86$ ergibt Gleichung (12.6) $P(85) = 0.114$, $P(86) = 0.028$ und für $k = 80$ (zwischen den Peaks) nur $P(80) = 0.0005$.

Wie wahrscheinlich ist ein guter Peak? Sei k die ganze Zahl, die sQ/r am nächsten liegt, also $|k - sQ/r| \leq \frac{1}{2}$. Mit $\theta = \pi(kr/Q - s)$ ist $|\theta| \leq \pi r/(2Q)$, und Gleichung (12.6) wird zu

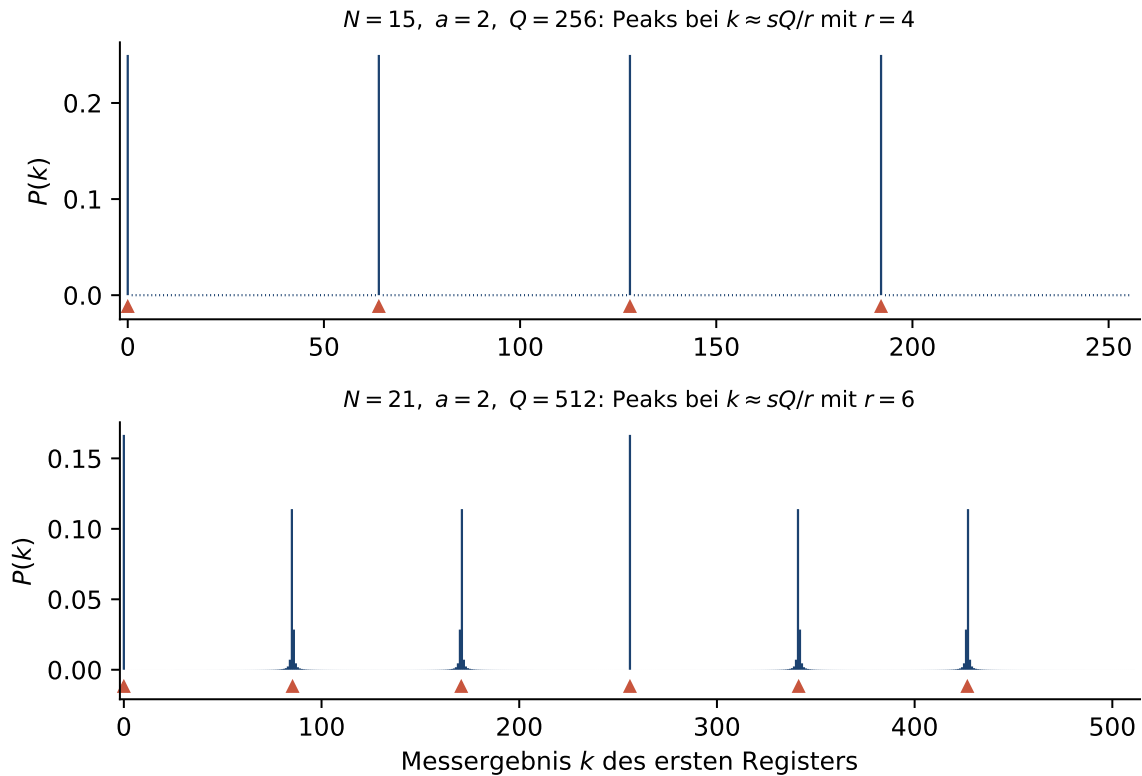


Abbildung 12.2: Exakte Messverteilung des Eingangsregisters nach der QFT. Die Dreiecke markieren sQ/r . Oben ($r = 4$ teilt $Q = 256$): vier scharfe Linien. Unten ($r = 6$): Peaks mit Nachbarn, weil sQ/r nicht ganzzahlig ist.

$P(k) = \sin^2(M\theta)/(MQ \sin^2 \theta)$. Wegen $M \approx Q/r$ ist $|M\theta| \leq \pi/2$; mit $\sin x \geq 2x/\pi$ für $|x| \leq \pi/2$ und $\sin^2 \theta \leq \theta^2$ folgt

$$P(k) \geq \frac{1}{MQ} \cdot \frac{4M^2\theta^2/\pi^2}{\theta^2} = \frac{4M}{\pi^2 Q} \approx \frac{4}{\pi^2} \cdot \frac{1}{r} \approx \frac{0.405}{r}. \quad (12.8)$$

Summiert über alle s trifft man also mit Wahrscheinlichkeit $\geq 40\%$ einen Wert nahe einem sQ/r . (Für $N = 21$: $0.114 \geq 0.405/6 = 0.068$. ✓)

12.5 Schritt 5: Kettenbrüche – aus k/Q wird r

Wir kennen k und Q und wissen $|k/Q - s/r| \leq 1/(2Q)$. Gesucht ist ein Bruch s/r mit $r < N$. Da $Q \geq N^2$, ist $1/(2Q) \leq 1/(2N^2) < 1/(2r^2)$, und ein Satz von Legendre garantiert:

Merksatz

Gilt $|x - s/r| < 1/(2r^2)$, dann ist s/r ein *Näherungsbruch* der Kettenbruchentwicklung von x .

Die Kettenbruchentwicklung ist der Euklidische Algorithmus in anderer Verpackung:

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} \equiv [a_0; a_1, a_2, a_3, \dots],$$

wobei die a_i die ganzzahligen Anteile der wiederholten Kehrwerte sind. Die Näherungsbrüche p_i/q_i (Abbruch nach a_i) folgen rekursiv aus $p_i = a_i p_{i-1} + p_{i-2}$, $q_i = a_i q_{i-1} + q_{i-2}$ mit $p_{-1} = 1$, $q_{-1} = 0$, $p_{-2} = 0$, $q_{-2} = 1$.

Rechenbeispiel 12.9: $85/512$ entwickeln

$$\frac{85}{512} = 0 + \frac{1}{512/85}, \quad 512 = 6 \cdot 85 + 2 \Rightarrow \frac{512}{85} = 6 + \frac{2}{85},$$

$$\frac{85}{2} = 42 + \frac{1}{2}, \quad \frac{2}{1} = 2.$$

Also $\frac{85}{512} = [0; 6, 42, 2]$ mit den Näherungsbrüchen

$$\frac{0}{1}, \quad \frac{1}{6}, \quad \frac{42}{253}, \quad \frac{85}{512}.$$

Der letzte Näherungsbruch mit Nenner $< N = 21$ ist $\frac{1}{6} \Rightarrow$ Kandidat $r = 6$. Test: $2^6 = 64 = 3 \cdot 21 + 1 \equiv 1$. ✓

Für $k = 427$: $\frac{427}{512} = [0; 1, 5, 42, 2]$, Näherungsbrüche $0, 1, \frac{5}{6}, \dots \Rightarrow r = 6$. ✓

Für $k = 171$: $\frac{171}{512} = [0; 2, 1, 170]$, Näherungsbrüche $0, \frac{1}{2}, \frac{1}{3}, \dots \Rightarrow$ Kandidat 3, aber $2^3 = 8 \not\equiv 1$.

Der Grund: $s = 2$ und $r = 6$ haben den gemeinsamen Teiler 2, gekürzt ergibt $2/6 = 1/3$.

Was tun bei gekürzten Brüchen? Man testet kleine Vielfache des Kandidaten ($2 \cdot 3 = 6$ funktioniert) oder wiederholt den Quantenteil und nimmt das kleinste gemeinsame Vielfache zweier Kandidaten ($\text{kgV}(3, 2) = 6$). Für $N = 21$, $a = 2$ liefert der Kettenbruch in einem einzigen Durchlauf mit Wahrscheinlichkeit 0.32 direkt $r = 6$; mit dem kgV zweier Läufe steigt die Erfolgswahrscheinlichkeit deutlich. Da ein Lauf polynomiell kostet, genügen wenige Wiederholungen.

12.6 Zweite Sicht: Phasenschätzung

Die meisten modernen Darstellungen (und Experimente) formulieren Shor als *Phasenschätzung*. Der unitäre Operator

$$U_a |y\rangle = |ay \bmod N\rangle \quad (12.9)$$

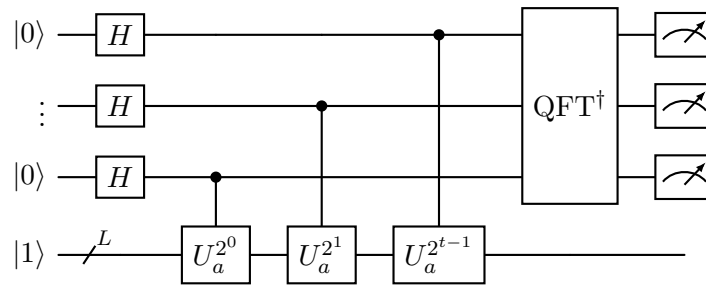
permutiert die Zahlen $1, a, a^2, \dots, a^{r-1}$ zyklisch. Seine Eigenzustände sind die „Fourier-Moden“ dieses Zyklus:

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{m=0}^{r-1} e^{-2\pi i s m / r} |a^m \bmod N\rangle, \quad U_a |u_s\rangle = e^{2\pi i s / r} |u_s\rangle. \quad (12.10)$$

Rechenbeispiel 12.10: Eigenzustände für $N = 15$, $a = 2$

$|u_s\rangle = \frac{1}{2}(|1\rangle + e^{-i\pi s/2}|2\rangle + e^{-i\pi s}|4\rangle + e^{-3i\pi s/2}|8\rangle)$. Anwenden von U_2 verschiebt $|1\rangle \rightarrow |2\rangle \rightarrow |4\rangle \rightarrow |8\rangle \rightarrow |1\rangle$; man kann den Faktor $e^{2\pi i s/4}$ ausklammern und erhält wieder $|u_s\rangle$. Die Eigenwerte sind $1, i, -1, -i$.

Entscheidend: $\frac{1}{\sqrt{r}} \sum_s |u_s\rangle = |1\rangle$. Das leicht präparierbare $|1\rangle$ ist eine gleichgewichtete Überlagerung aller Eigenzustände. Die Phasenschätzung mit t Kontrollqubits wendet kontrolliert $U_a^{2^0}, U_a^{2^1}, \dots, U_a^{2^{t-1}}$ an (genau die Potenzen des Square-and-Multiply!), was per *Phase-Kickback* die Phase s/r ins Kontrollregister schreibt; die inverse QFT liest sie als $k/Q \approx s/r$ aus:



Nach dem Kickback ist das Kontrollregister im Zustand $\frac{1}{\sqrt{Q}} \sum_x e^{2\pi i x s/r} |x\rangle$, also (mit unserer Konvention) $\text{QFT} |k\rangle$ mit $k = sQ/r$; zum Auslesen braucht es daher die *inverse* QFT. Verwendet man stattdessen die QFT, misst man $k/Q \approx (r - s)/r$ – für die Bestimmung von r ebenso brauchbar; die Verteilung $P(k)$ ist symmetrisch unter $k \rightarrow Q - k$. Beide Sichten liefern dieselbe Verteilung $P(k)$.

12.7 Ein vollständig kompilierter Schaltkreis: $N = 15$, $a = 2$

Für $N = 15$ ist die modulare Multiplikation besonders einfach. Schreibt man $y \in \{1, \dots, 14\}$ mit vier Bits, dann ist

$$2y \bmod 15 = \text{zyklische Rotation der vier Bits um eine Stelle nach links}, \quad (12.11)$$

denn $2y$ schiebt alle Bits nach links, und ein herausfallendes Bit mit Wert $16 \equiv 1$ erscheint rechts wieder.

Rechenbeispiel 12.11: Multiplikation als Bitrotation

$1 = 0001 \rightarrow 0010 = 2$, $2 \rightarrow 0100 = 4$, $4 \rightarrow 1000 = 8$, $8 = 1000 \rightarrow 0001 = 1$, $7 = 0111 \rightarrow 1110 = 14$ ($2 \cdot 7 = 14$ ✓), $3 = 0011 \rightarrow 0110 = 6$ ✓.

Eine zyklische Rotation von vier Bits sind drei SWAPs, ein *kontrolliertes* U_2 also drei kontrollierte SWAPs (Fredkin-Gates). $U_2^2 = U_4$ ist eine Rotation um zwei Stellen (zwei SWAPs: Bit $3 \leftrightarrow 1$, $2 \leftrightarrow 0$), und $U_2^4 = U_{16} = U_1 = \mathbb{I}$: Alle weiteren kontrollierten Potenzen U^{2^j} mit $j \geq 2$ sind die Identität und entfallen! Von den acht Kontrollqubits wirken nur zwei. Die gatenaehe Simulation (`code/k6_shor.py`: Zustandsvektor der Dimension 2^{12} , kontrollierte Rotationen, QFT) liefert exakt

$$P(0) = P(64) = P(128) = P(192) = 0.25.$$

Mit dem Kettenbruch ergeben $k = 64$ und $k = 192$ direkt $r = 4$, $k = 128$ ergibt $r = 2$ (Teiler) und $k = 0$ nichts: Erfolg in 50 % der Läufe, mit kgV-Trick mehr.

Vorsicht bei „Faktorisierungsrekorden“

Das obige Beispiel ist lehrreich, aber auch ein Warnsignal: Wer beim Kompilieren schon weiss, dass $U^4 = \mathbb{I}$, hat die Periode bereits benutzt. Viele frühe Demonstrationen haben Schaltkreise mit Kenntnis der Lösung vereinfacht [21]. Ehrlich ist ein Schaltkreis nur, wenn er für ein beliebiges a ohne Kenntnis von r konstruiert wird. Das Innsbrucker Experiment mit fünf Kalzium-Ionen [20] hat Shor für $N = 15$ in einer skalierbaren Form realisiert, bei der ein Kontrollqubit nach Messung und Reset wiederverwendet wird („Kitaev-Shor“).

12.8 Der vollständige Algorithmus

1. Ist N gerade oder eine Primzahlpotenz p^k ? Dann klassisch lösen.
2. Wähle zufällig $a \in \{2, \dots, N-1\}$. Ist $g = \text{ggT}(a, N) > 1$: fertig, g ist ein Faktor.
3. **Quantencomputer:** Periodensuche für $f(x) = a^x \bmod N$ mit $Q \geq N^2$; Messergebnis k .
4. Kettenbruch von $k/Q \Rightarrow$ Kandidat r ; prüfe $a^r \equiv 1 \pmod{N}$ (sonst kleine Vielfache oder neuer Lauf).
5. Ist r ungerade oder $a^{r/2} \equiv -1 \pmod{N}$: zurück zu 2.
6. Gib $\text{ggT}(a^{r/2} \pm 1, N)$ aus.

12.9 Was kostet Shor auf echter Hardware?

Qubits. Das Eingangsregister kann man mit dem Kitaev-Trick auf ein einziges, wiederverwendetes Qubit reduzieren; die modulare Arithmetik braucht Hilfsqubits. Ein bekannter Schaltkreis kommt mit $2n + 3$ logischen Qubits aus [19].

Gates. Die modulare Exponentiation ist der Löwenanteil: rund $2n$ kontrollierte modulare Multiplikationen (eine pro Kontrollqubit, da $Q \approx N^2$) zu je $O(n^2)$ Gates, also $O(n^3)$ – gegenüber $O(n^2)$ für die QFT. Für RSA-2048 ($n = 2048$) sind das Milliarden logischer Operationen.

Fehlerkorrektur. Nach Abschnitt 3.4 ist das ohne Quantenfehlerkorrektur unmöglich. Man kodiert jedes *logische* Qubit in viele *physikalische*. Die Ressourcenschätzungen sind in den letzten Jahren stark gefallen: 2019 schätzten Gidney und Ekerå rund 20 Millionen verrauschte Qubits und 8 h Laufzeit [22]; 2025 zeigte Gidney, dass weniger als eine Million verrauschter Qubits in weniger als einer Woche genügen würden – unter Annahme einer Gatefehlerrate von 0,1 % und eines Fehlerkorrekturzyklus von 1 μs auf einem quadratischen Gitter mit nächsten-Nachbar-Kopplung [23]. Ionen sind langsamer (Gates im 10 μs bis 100 μs -Bereich), haben aber höhere Fidelities und flexiblere Konnektivität; welche Architektur gewinnt, ist offen.

Der tiefere Punkt

Der Quantencomputer berechnet nicht alle $a^x \bmod N$ und liest sie aus. Er erzeugt eine Superposition, prägt ihr durch modulare Exponentiation die Periodizität auf, und die QFT verwandelt diese globale Eigenschaft durch Interferenz in Messwahrscheinlichkeiten, die bei $k/Q \approx s/r$ konzentriert sind. Der klassische Kettenbruch liest r ab, und ein ggT liefert die Faktoren:

Superposition $\rightarrow$ mod. Exponentiation $\rightarrow$ QFT $\rightarrow$ Interferenz
 $\rightarrow$ Messwert $k \rightarrow$ Kettenbruch $\rightarrow r \rightarrow \text{ggT} \rightarrow p, q$.

Kapitel 13

Die ZuriQ-Architektur: vom Einzelion zum 2D-Prozessor

13.1 Was öffentlich bekannt ist

ZuriQ ist ein Spin-off der ETH Zürich, das eng mit der Gruppe von Jonathan Home (Trapped Ion Quantum Information, TIQI) zusammenarbeitet. Öffentlich dokumentiert sind (Stand September 2026):

- **Physikalische Grundlage:** mikrofabrizierte Penning-Fallen mit statischen elektrischen Feldern in einem homogenen Magnetfeld von 3 T; volle Quantenkontrolle eines ${}^9\text{Be}^+$ -Ions (Spin und Bewegung), Grundzustandskühlung aller drei Moden und Transport des Ions in beliebigen Richtungen über dem Chip [1].
- **Konzept:** nativ zweidimensionale Anordnungen einzelner Ionen ohne RF-Felder und ohne Kreuzungsstrukturen; Ionen sollen sich frei in alle Richtungen bewegen lassen, auch dreidimensional [2, 3].
- **Stand:** ein 3×3 -Array aus neun individuell kontrollierten Ionen; Chips in Zusammenarbeit mit Infineon industriell gefertigt; Ziel sind hunderte Qubits pro Chip [3].
- **Fehlertoleranz:** öffentliche Arbeiten zur Planung fehlertoleranter Architekturen für die Mikro-Penning-Plattform [4].

13.2 Paul-Falle und Penning-Mikrofalle im Vergleich

	Paul-Falle (RF)	Penning-Mikrofalle
Einschluss	RF-Feld, zeitgemitteltes Pseudopotential	statisches $\mathbf{E}$ + homogenes $\mathbf{B}$ (3 T)
Mögliche Fallenorte	nur entlang RF-Nulllinien	überall über dem Chip
Transport in 2D	braucht Kreuzungen (Junctions)	frei in jeder Richtung
Leistung auf Chip	RF-Verluste, hohe Spannungen	nur DC-Spannungen
Qubit (bei Be^+)	Hyperfeinqubit, oft feldunempfindlich wählbar	Elektronenspin, 28 GHz/T feldempfindlich
Radiale Bewegung	zwei Oszillatoren mit positiver Energie	Zyklotron + Magnetron (negative Energie)
Infrastruktur	Standardvakuum/-kryostat	supraleitender Magnet, Kryostat

Die Penning-Mikrofalle tauscht also die RF-Probleme gegen die Anforderungen eines starken, sehr stabilen Magnetfelds. Die Feldempfindlichkeit des Qubits wird durch dynamische Entkopplung (Spin-Echo) und die Stabilität supraleitender Magnete beherrschbar (Kapitel 4).

13.3 Wie ein Zwei-Qubit-Gate in einem 2D-Array ablaufen kann

Aus den Kapiteln 7 und 9 lässt sich ein plausibler Ablauf ableiten (ohne unveröffentlichte Implementierungsdetails zu behaupten):

1. Die beiden beteiligten Ionen werden durch Umprogrammieren der Elektrodenspannungen zusammengefahren. Wegen $t_{ij} \propto d^{-3}$ steigt die Coulomb-Kopplung beim Halbieren des Abstands um den Faktor 8.
2. Die lokalen axialen Frequenzen werden gleich eingestellt, sodass die Moden hybridisieren (COM- und Relativmode, Abschnitt 7.2.2).
3. Ein spinabhängiger Kraftpuls (Raman-Strahlen) erzeugt $XX(\chi)$ über diese Moden, mit Verstimmungen und Pulsformen, die die Phasenraumschleifen *beider* Moden schliessen.
4. Die Ionen werden wieder getrennt; andere Ionenpaare im Array können parallel dasselbe tun.

Alternativ können auch die radialen (Zyklotron-/Magnetron-)Moden als Bus dienen, deren Kopplung und Nullpunktsbewegung in der Penning-Falle besondere Eigenschaften haben [2].

13.4 Fehlerquellen

Motionales Heizen. Elektrische Feldfluktuationen an der Chipoberfläche erhöhen die Phononenzahl. Die gemessene axiale Heizrate von 0.088 s^{-1} bei $152 \mu\text{m}$ Abstand [1] ist sehr klein; näher an der Oberfläche (für stärkere Kopplung) steigt sie typischerweise stark an. Ein Zielkonflikt: kleiner Abstand zwischen Ionen erfordert oft auch kleinere Abstände zur Oberfläche.

Modenfrequenzrauschen. Schwankt ω_n , schliesst sich die Phasenraumschleife nicht exakt; es bleibt Spin-Bewegungs-Verschränkung (Kapitel 9, Tabelle zur Gatezeit).

Magnetfeldrauschen. 28 GHz/T Empfindlichkeit: Dephasierung ohne Echo auf der ms-Skala.

Laser. Spontane Streuung aus dem virtuellen Niveau (daher 150 GHz Verstimmung), Intensitäts- und Phasenrauschen, Übersprechen auf Nachbarionen.

Auslese. Depumping und Untergrund (Abschnitt 10.4).

13.5 Skalierung und Fehlertoleranz

Für grosse Algorithmen wie Shor braucht man logische Qubits, z. B. in einem Oberflächencode, der auf einem *zweidimensionalen* Gitter mit nächsten-Nachbar-Wechselwirkungen arbeitet. Eine nativ zweidimensionale Ionenanordnung mit rekonfigurierbaren Positionen passt gut zu solchen Codes: Syndrom-Messungen erfordern viele parallele Zwei-Qubit-Gates zwischen benachbarten Daten- und Hilfsqubits. Ob Penning-Mikrofallen die nötigen Fidelities (deutlich über 99,9%), Taktraten und Qubitzahlen erreichen, ist Gegenstand aktueller Forschung und Entwicklung.

Die ganze Kette in einem Bild

$$\begin{array}{ccccc}
 \underbrace{|\uparrow\rangle, |\downarrow\rangle}_{\text{Elektronenspin in 3 T}} & \xrightarrow{\text{Laser}} & \underbrace{\eta_{in} \propto b_{in}}_{\text{Spin-Phonon}} & \xleftarrow{\text{Coulomb}} & \underbrace{K\mathbf{b}_n = m\omega_n^2\mathbf{b}_n}_{\text{Eigenmoden}} \\
 \Rightarrow & \underbrace{J_{ij} = \Omega^2 \sum_n \eta_{in} \eta_{jn} \frac{\omega_n}{\mu^2 - \omega_n^2}}_{\text{Gate } XX(\chi)} & \Rightarrow & \underbrace{\text{QFT, } a^x \bmod N}_{\text{Shor}} & \Rightarrow p, q
 \end{array}$$

Kapitel 14

Übungsaufgaben mit Lösungen

Teil I: Quanteninformation

Aufgabe 1 (Bloch-Vektor). Bestimmen Sie $\langle X \rangle, \langle Y \rangle, \langle Z \rangle$ für $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/3}|1\rangle)$.

Lösung. $\theta = \pi/2, \phi = \pi/3: \vec{s} = (\cos \frac{\pi}{3}, \sin \frac{\pi}{3}, 0) = (0.5, 0.866, 0)$. □

Aufgabe 2 (Rotation). Zeigen Sie $R_x(\pi)|0\rangle = -i|1\rangle$ und $R_x(2\pi) = -\mathbb{I}$. Warum ist das Minuszeichen physikalisch harmlos – und wann nicht?

Lösung. Aus $R_x(\theta) = \cos \frac{\theta}{2} \mathbb{I} - i \sin \frac{\theta}{2} X$ folgt $R_x(\pi) = -iX$ und $R_x(2\pi) = -\mathbb{I}$. Global ist -1 eine unbeobachtbare Phase. Wird die Drehung aber *kontrolliert* ausgeführt (nur wenn ein anderes Qubit $|1\rangle$ ist), wird aus der globalen eine relative Phase – dann ist sie messbar. □

Aufgabe 3 (Verschränkungstest). Für welche φ ist $|\Psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + e^{i\varphi}|11\rangle)$ verschränkt? Für welches φ maximal?

Lösung. $\det C = \frac{1}{4}(e^{i\varphi} - 1)$ verschwindet nur für $\varphi = 0$. Die Singulärwerte von $C = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & e^{i\varphi} \end{pmatrix}$ sind gleich (maximale Verschränkung), wenn $C \propto$ unitär, d. h. die Spalten orthogonal sind: $1 + e^{i\varphi} = 0$, also $\varphi = \pi$ (das ist CZ $|++\rangle$). □

Aufgabe 4 (Ising-Gate). Berechnen Sie $XX(\chi)|01\rangle$. Für welches χ entsteht ein maximal verschränkter Zustand?

Lösung. $XX(\chi)|01\rangle = \cos \chi |01\rangle - i \sin \chi |10\rangle$; maximal verschränkt für $\chi = \pi/4$ (gleiche Beträge), z. B. $\frac{1}{\sqrt{2}}(|01\rangle - i|10\rangle)$. □

Teil II: Hardware

Aufgabe 5 (Hyperfeinaufspaltung allgemein). Zeigen Sie, dass für $J = \frac{1}{2}$ die Hyperfeinaufspaltung $E_{F=I+1/2} - E_{F=I-1/2} = hA(I + \frac{1}{2})$ ist, und werten Sie für ${}^9\text{Be}^+$ aus.

Lösung. $\frac{A}{2}[(I + \frac{1}{2})(I + \frac{3}{2}) - (I - \frac{1}{2})(I + \frac{1}{2})] = \frac{A}{2}(I + \frac{1}{2}) \cdot 2 = A(I + \frac{1}{2})$. Für $I = \frac{3}{2}$: $2A = -1,250 \text{ GHz}$; das Minus bedeutet, dass $F = 2$ unten liegt. □

Aufgabe 6 (Qubitfrequenz bei anderem Feld). Schätzen Sie die Qubitfrequenz bei $B = 2,5 \text{ T}$ mit Gleichung (4.4).

Lösung. $\nu_0 \approx 28.025 \text{ GHz/T} \cdot 2.5 \text{ T} - 0.9375 \text{ GHz} = 69,13 \text{ GHz}$. Die exakte Diagonalisierung liefert 69,127 GHz. $\square$

Aufgabe 7 (Penning-Frequenzen). Berechnen Sie $\nu_{\pm}$ für $^9\text{Be}^+$ bei 3 T und $\nu_z = 3 \text{ MHz}$. Ist die Falle stabil? Was passiert bei $\nu_z = 3,7 \text{ MHz}$?

Lösung. $\nu_c = 5,112 \text{ MHz}$, $\sqrt{\nu_c^2 - 2\nu_z^2} = \sqrt{26.13 - 18} = 2,852 \text{ MHz}$, also $\nu_+ = 3,982 \text{ MHz}$, $\nu_- = 1,130 \text{ MHz}$; Kontrolle $2\nu_+\nu_- = 9.00 = \nu_z^2$. Stabil, da $3 < 3.615$. Bei 3,7 MHz wird der Radikand negativ: Die radiale Bewegung wächst exponentiell, das Ion geht verloren. $\square$

Aufgabe 8 (Thermische Besetzung). Wie gross ist die Wahrscheinlichkeit, eine Mode mit $\bar{n} = 0.05$ im Grundzustand zu finden, und wie gross, zwei oder mehr Phononen zu finden?

Lösung. $P(0) = 1/1.05 = 0.952$, $P(1) = 0.05/1.05^2 = 0.045$, also $P(n \geq 2) = 1 - 0.952 - 0.045 = 0.0023$. $\square$

Teil III: Phononen-Kopplung

Aufgabe 9 (Zwei Ionen in einer Kette). Berechnen Sie Gleichgewichtsabstand und Eigenmoden von zwei Ionen in einem axialen Potential.

Lösung. Kräftegleichgewicht $u = 1/(2u)^2 \Rightarrow u^3 = \frac{1}{4}$, Abstand $2u = 2 \cdot 4^{-1/3} \ell = 2^{1/3} \ell = 1.26 \ell$. Mit $1/(2u)^3 = \frac{1}{2}$: $A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, Eigenwerte 1 (COM, $(1, 1)/\sqrt{2}$) und 3 (Streckmode, $(1, -1)/\sqrt{2}$). Die Streckmode schwingt mit $\sqrt{3}\omega_z$ – wie bei drei Ionen! $\square$

Aufgabe 10 (Zwei Mikrofallen). Zwei $^9\text{Be}^+$ -Ionen in Mikrofallen mit $\nu = 2,5 \text{ MHz}$ haben den Abstand $d = 40 \mu\text{m}$. Berechnen Sie ε , die Frequenz der Relativmode und die Hüpfrate t .

Lösung. $\varepsilon = 2.314 \times 10^{-3} \cdot (30/40)^3 = 9.76 \times 10^{-4}$. Mit $d^3 M = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ (Eigenwerte 0, -2) ist $\omega_{\text{rel}} = \omega\sqrt{1 - 2\varepsilon}$, also $\Delta\nu \approx -\varepsilon\nu = -2,44 \text{ kHz}$. $t/2\pi = \varepsilon\nu/2 = 1,22 \text{ kHz}$, Austauschzeit $\pi/(2t) = 0,20 \text{ ms}$. $\square$

Aufgabe 11 (Lamb–Dicke–Regime). Wie gross ist η für ein einzelnes Ion bei 2,5 MHz, wenn die Raman-Strahlen senkrecht zueinander stehen und $\Delta\mathbf{k}$ entlang z liegt? Ist die Lamb–Dicke–Näherung gut?

Lösung. $\Delta k = \sqrt{2}k = \sqrt{2} \cdot 2\pi/313 \text{ nm} = 2,84 \cdot 10^7 \text{ m}^{-1}$, $z_0 = 15,0 \text{ nm}$, also $\eta = 0.43$. Das ist zu gross: Terme zweiter Ordnung ($\eta^2 \approx 0.18$) sind nicht vernachlässigbar. Kleinere Strahlwinkel oder höhere Fallenfrequenzen helfen. $\square$

Aufgabe 12 (Mode wählt Partner). Sie wollen in der Drei-Ionen-Kette nur Ion 1 und Ion 3 verschränken, ohne Ion 2 zu adressieren oder zu verschieben. Welche Mode verwenden Sie, und warum funktioniert das auch, wenn alle drei Ionen beleuchtet werden?

Lösung. Die Streckmode $\mathbf{b}_2 = (1, 0, -1)/\sqrt{2}$: Weil $b_{22} = 0$, ist $\eta_{22} = 0$; Ion 2 koppelt nicht an diese Mode. Nahe ω_2 dominiert in Gleichung (9.8) der Term $\propto b_{12}b_{32}$, und die Tabelle in Abschnitt 9.4.2 zeigt $|J_{13}| \approx 50|J_{12}|$. $\square$

Aufgabe 13 (Seitenband-Sequenz). Wiederholen Sie Abschnitt 8.4, aber mit einem blauen $\pi/2$ -Puls auf Ion 1 und Start in $|\downarrow\rangle|0\rangle$. Welchen Puls brauchen Sie auf Ion 2?

Lösung. Blau $\pi/2$ auf Ion 1: $\frac{1}{\sqrt{2}}(|\downarrow\downarrow\rangle|0\rangle - i|\uparrow\downarrow\rangle|1\rangle)$. Auf Ion 2 braucht man jetzt ein rotes π -Puls: Im ersten Term hat $|\downarrow, 0\rangle$ keinen roten Partner ($|\uparrow, -1\rangle$), im zweiten wird $|\downarrow, 1\rangle \rightarrow -i|\uparrow, 0\rangle$.

Ergebnis: $\frac{1}{\sqrt{2}}(|\downarrow\downarrow\rangle - |\uparrow\uparrow\rangle)|0\rangle$. □

Aufgabe 14 (MS-Gate mit zwei Schleifen). Wie gross müssen δ und t_g für ein $XX(\pi/4)$ -Gate mit $K = 2$ Schleifen bei $g = 2\pi \times 2,5$ kHz sein? Warum könnte man $K = 2$ wählen?

Lösung. $\delta = 4g\sqrt{2} = 2\pi \times 14,1$ kHz, $t_g = \pi\sqrt{2}/(2g) = 141$ μ s. Grösseres δ bedeutet kleinere Phasenraumkreise (weniger Anregung der Mode, weniger Empfindlichkeit gegen Heizen und andere Moden), bezahlt mit längerer Gatezeit. □

Teil IV: Algorithmen

Aufgabe 15 (QFT von Hand). Berechnen Sie $\text{QFT}_4|1\rangle$ und $\text{QFT}_4|2\rangle$. Welche der beiden Ausgaben ist ein Produktzustand?

Lösung. $\text{QFT}_4|1\rangle = \frac{1}{2}(|0\rangle + i|1\rangle - |2\rangle - i|3\rangle) = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle + i|1\rangle)$; $\text{QFT}_4|2\rangle = \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$. Beide – die QFT eines Basiszustands ist immer ein Produktzustand (Gleichung (11.2)). □

Aufgabe 16 (CZ aus MS). Zeigen Sie mit Abschnitt 10.2: CZ braucht ein MS-Gate mit $|\chi| = \pi/4$, also ist CZ genauso „teuer“ wie ein CNOT.

Lösung. $\text{CZ} = \text{CP}(\pi)$, also $\chi = -\pi/4$. Und $\text{CNOT} = (\mathbb{I} \otimes H) \text{CZ} (\mathbb{I} \otimes H)$. □

Aufgabe 17 (Shor für $N = 35$). Wählen Sie $a = 2$. Bestimmen Sie r , prüfen Sie die Bedingungen und berechnen Sie die Faktoren. Wie gross muss Q sein?

Lösung. $2^1, \dots, 2^{12} \bmod 35 = 2, 4, 8, 16, 32, 29, 23, 11, 22, 9, 18, 1$, also $r = 12$. $2^6 \bmod 35 = 29 \neq 34$. $\text{ggT}(28, 35) = 7$, $\text{ggT}(30, 35) = 5$. $\checkmark N^2 = 1225 \leq Q = 2048 < 2450$, also $t = 11$ Eingangsqubits und $L = 6$ Arbeitsqubits. □

Aufgabe 18 (Kettenbruch). Beim Lauf für $N = 21$, $a = 2$, $Q = 512$ wird $k = 341$ gemessen. Welches r liefert der Kettenbruch, und wie geht es weiter?

Lösung. $\frac{341}{512} = [0; 1, 1, 1, 170]$ mit Näherungsbrüchen $0, 1, \frac{1}{2}, \frac{2}{3}, \dots \Rightarrow$ Kandidat $r = 3$. Test: $2^3 = 8 \neq 1$. Nächstes Vielfaches: $r = 6$, $2^6 = 64 \equiv 1$. $\checkmark$ (Hier war $s/r = 4/6$ zu $2/3$ gekürzt.) □

Aufgabe 19 (Auslese). $\lambda_b = 8$, $\lambda_d = 0.5$, Schwelle $n_{\text{th}} = 2$. Berechnen Sie beide Fehlerwahrscheinlichkeiten. Würden Sie die Schwelle verschieben?

Lösung. $\epsilon_d = 1 - e^{-0.5}(1 + 0.5) = 0.090$, $\epsilon_b = e^{-8}(1 + 8) = 0.0030$. Der Dunkelfehler dominiert; eine höhere Schwelle ($n_{\text{th}} = 3$) balanciert besser: $\epsilon_d = 0.014$, $\epsilon_b = 0.014$. □

Aufgabe 20 (Fehlerbudget). Ein Algorithmus braucht 5000 Zwei-Qubit-Gates. Welche Gatefidelity ist nötig, damit das Ergebnis in mindestens 50 % der Läufe fehlerfrei ist?

Lösung. $F^{5000} \geq 0.5 \Rightarrow F \geq 0.5^{1/5000} = e^{-\ln 2/5000} \approx 1 - 1.39 \times 10^{-4}$, also $F \geq 99,986$ %. □

Anhang A

Python-Programme

Alle Zahlen und Abbildungen dieses Skripts wurden mit den folgenden Programmen erzeugt (Python 3, NumPy, SciPy, Matplotlib). Sie liegen im Unterordner `code/` und werden aus diesem Ordner gestartet, z. B. `python k3_drei_ionen_moden.py`. Die Abbildungen landen in `figures/`.

Datei	Inhalt
<code>konstanten.py</code>	Naturkonstanten, Daten von $^9\text{Be}^+$, Plot-Stil
<code>k1_beryllium_niveaus.py</code>	8×8 -Hyperfein-Zeeman-Hamiltonoperator, Qubitfrequenz (Kapitel 4)
<code>k2_penning_falle.py</code>	Eigenfrequenzen, Bahnkurve, quadratisches Eigenwertproblem (Kapitel 5)
<code>k3_drei_ionen_moden.py</code>	Modelle A und B, Hopping, Lamb-Dicke, J_{ij} (Kapitel 7 und 9)
<code>k3b_zwei_mikrofallen_gate.py</code>	J_{12} für zwei Mikrofallen (Kapitel 9)
<code>k4_spin_phonon.py</code>	Seitenband-Sequenz, MS-Gate für 2 und 3 Ionen (Kapitel 8 und 9)
<code>k5_gates_qft_messung.py</code>	CNOT/CP-Kompilation, QFT, Auslesestatistik (Kapitel 10 und 11)
<code>k6_shor.py</code>	Ordnungen, Verteilungen, Kettenbrüche, gatenae Simulation (Kapitel 12)

A.1 Drei Ionen: Eigenmoden und Kopplungen

```
1  """Kapitel 'Drei gekoppelte Ionen': Gleichgewicht, Hesse-Matrix, Eigenmoden.
2  Modell A: drei Ionen als lineare Kette entlang der Magnetfeldachse einer Falle.
3  Modell B: drei Ionen in drei getrennten Mikro-Penning-Fallen (ZuriQ-artig)."""
4  import numpy as np
5  from scipy.optimize import minimize
6  from konstanten import *
7
8  np.set_printoptions(precision=5, suppress=True)
9
10 # ----- Modell A
11 def potential_dimlos(u):
12     """ $V/(m \omega_z^2 l^2) = \sum_i u_i^2/2 + \sum_{\{i < j\}} 1/|u_i - u_j|$ """
13     V = 0.5 * np.sum(u**2)
14     for i in range(len(u)):
15         for j in range(i + 1, len(u)):
16             V += 1.0 / abs(u[i] - u[j])
```

```

17     return V
18
19 def hesse_dimlos(u):
20     N = len(u)
21     A = np.zeros((N, N))
22     for i in range(N):
23         for j in range(N):
24             if i == j:
25                 A[i, i] = 1 + 2 * sum(1 / abs(u[i] - u[k])**3 for k in range(N) if k != i)
26             else:
27                 A[i, j] = -2 / abs(u[i] - u[j])**3
28     return A
29
30 def modell_A(nu_z=1.0e6, verbose=True):
31     res = minimize(potential_dimlos, x0=[-1.0, 0.1, 1.2], tol=1e-14)
32     u0 = np.sort(res.x)
33     A = hesse_dimlos(u0)
34     mu, b = np.linalg.eigh(A)
35     wz = 2 * np.pi * nu_z
36     l = (k_C / (m_Be * wz**2))**(1 / 3)
37     if verbose:
38         print("=== Modell A: lineare Kette, nu_z = %.2f MHz ===" % (nu_z / 1e6))
39         print("Gleichgewicht u0 =", u0, " analytisch (5/4)^(1/3) =", (5 / 4)**(1 / 3))
40         print("Längenskala l = %.3f um, Positionen =" % (l * 1e6), u0 * l * 1e6, "um")
41         print("Hesse-Matrix A =\n", A)
42         print("Eigenwerte mu =", mu, " (erwartet 1, 3, 29/5 = 5.8)")
43         print("Frequenzen nu_n = sqrt(mu) nu_z =", np.sqrt(mu) * nu_z / 1e6, "MHz")
44         print("Eigenvektoren (Spalten):\n", b * np.sign(b[0]))
45         # SI-Kontrolle: Coulombkraft = Fallenkraft
46         F_C = k_C * (1 / (u0[2] - u0[1])**2 + 1 / (u0[2] - u0[0])**2) / l**2
47         print("Kraftbilanz äusseres Ion: F_Falle = %.4e N, F_Coulomb = %.4e N" % (m_Be * wz**2
48             * u0[2] * l, F_C))
49     return u0, A, mu, b * np.sign(b[0]), l
50
51 # ----- Modell B
52 def modell_B(pos, nu=2.5e6, verbose=True, name=""):
53     """pos: (N,2)-Array der Fallenpositionen in der Chipebene (m).
54     Axiale Moden (senkrecht zur Ebene, entlang B)."""
55     N = len(pos)
56     w = 2 * np.pi * nu
57     K = m_Be * w**2 * np.eye(N)
58     for i in range(N):
59         for j in range(N):
60             if i != j:
61                 d = np.linalg.norm(pos[i] - pos[j])
62                 K[i, j] += k_C / d**3 # d^2 V / dz_i dz_j
63                 K[i, i] -= k_C / d**3 # d^2 V / dz_i^2 (Anti-Feder)
64     lam, b = np.linalg.eigh(K / m_Be)
65     wn = np.sqrt(lam)
66     if verbose:
67         dmin = min(np.linalg.norm(pos[i] - pos[j]) for i in range(N) for j in range(i + 1, N))
68         eps = k_C / (m_Be * w**2 * dmin**3)
69         print(f"=== Modell B ({name}): nu = {nu/1e6} MHz, d = {dmin*1e6:.1f} um, eps = {eps:.4
70             e} ===")
71         print("K/(k_C/d^3) - (m w^2 d^3/k_C) 1 =\n", (K - m_Be * w**2 * np.eye(N)) / (k_C /
72             dmin**3))
73         print("Modenfrequenzen - nu [kHz]:", (wn / 2 / np.pi - nu) / 1e3)
74         print("Eigenvektoren (Spalten, nach aufsteigender Frequenz):\n", b * np.sign(b[0] + 1e
75             -12))
76     return wn, b, K

```

```
74 def hopping(d, nu=2.5e6):
75     w = 2 * np.pi * nu
76     return k_C / (2 * m_Be * w * d**3) # rad/s
77
78 if __name__ == "__main__":
79     u0, A, mu, bA, l = modell_A()
80     uA2, AA2, muA2, bA2, lA2 = modell_A(nu_z=2.5e6, verbose=False)
81     print("Längenskala bei 2.5 MHz: %.3f um, Abstand = %.3f um" % (lA2 * 1e6, (uA2[2] - uA2
82         [1]) * lA2 * 1e6))
83
84     d = 30e-6
85     line = np.array([-d, 0], [0, 0], [d, 0])
86     tri = d * np.array([0, 0], [1, 0], [0.5, np.sqrt(3) / 2])
87     wnL, bL, KL = modell_B(line, name="Linie")
88     wnT, bT, KT = modell_B(tri, name="Dreieck")
89     for dd in [20e-6, 30e-6, 50e-6, 100e-6]:
90         t = hopping(dd)
91         print(f"d = {dd*1e6:5.0f} um : t/2pi = {t/2/np.pi:8.1f} Hz, Swap-Zeit pi/(2t) = {np.pi
92             / (2*t)*1e3:.3f} ms,"
93             f" f = 0omega_ex=2t: {2*t/2/np.pi/1e3:.3f} kHz")
94
95     # Phononen-Hüpfen im Einteilchen-Sektor (RWA): H/hbar = Diagonal + t_ij
96     plt = style()
97     w = 2 * np.pi * 2.5e6
98     Hc = (KL / m_Be - w**2 * np.eye(3)) / (2 * w) # effektive Kopplungsmatrix (rad/s), RWA
99     print("RWA-Hopping-Matrix Linie / (2pi Hz):\n", Hc / 2 / np.pi)
100     ts = np.linspace(0, 0.45e-3, 800)
101     ev, V = np.linalg.eigh(Hc)
102     psi0 = np.array([1, 0, 0], dtype=complex)
103     P = np.array([np.abs(V @ (np.exp(-1j * ev * t) * (V.conj().T @ psi0)))*2 for t in ts])
104     # nur nächste Nachbarn
105     t1 = hopping(d)
106     Hnn = t1 * np.array([0, 1, 0], [1, 0, 1], [0, 1, 0])
107     ev2, V2 = np.linalg.eigh(Hnn)
108     P2 = np.array([np.abs(V2 @ (np.exp(-1j * ev2 * t) * (V2.conj().T @ psi0)))*2 for t in ts
109         ])
110     tstar = np.pi / (np.sqrt(2) * t1)
111     print(f"Perfekter Transfer 1->3 (nur NN) bei t* = pi/(sqrt2 t) = {tstar*1e3:.4f} ms")
112     print(f"Mit übernächsten Nachbarn: max P3 = {P[:,2].max():.4f} bei t = {ts[P[:,2].argmax()
113         ]*1e3:.4f} ms")
114     fig, ax = plt.subplots(figsize=(5.2, 2.6))
115     for i, c in enumerate(["#1c4270", "#c8553d", "#2a7f62"]):
116         ax.plot(ts * 1e3, P[:, i], color=c, label=f"Phonon bei Ion {i+1}")
117     ax.plot(ts * 1e3, P2[:, 2], color="#2a7f62", ls=":", lw=1.1, label="Ion 3, nur nächste
118         Nachbarn")
119     ax.axvline(tstar * 1e3, color="0.6", ls="--", lw=0.8)
120     ax.set_xlabel("$t$ / ms"); ax.set_ylabel("Wahrscheinlichkeit")
121     ax.set_title("Ein Phonon wandert durch drei Mikrofallen ($d=30$ μm, $\\nu=2.5$ MHz)",
122         fontsize=9)
123     ax.legend(loc="upper left", bbox_to_anchor=(1.01, 1.0), fontsize=7.5)
124     fig.tight_layout(); fig.savefig(f"{FIG}/phonon_hopping.pdf")
125
126     # Modenbild für Modell A
127     fig, axs = plt.subplots(1, 3, figsize=(7.0, 2.2), sharey=True)
128     names = ["Schwerpunktmode", "Streckmode", "Knickmode"]
129     for n in range(3):
130         axs[n].bar([1, 2, 3], bA[:, n], color=["#1c4270", "#c8553d", "#2a7f62"], width=0.5)
131         axs[n].axhline(0, color="k", lw=0.6)
132         axs[n].set_xticks([1, 2, 3]); axs[n].set_xlabel("Ion $i$")
133         axs[n].set_title(f"{names[n]}\n$\\omega_{n+1}=\\sqrt{{{\\mu[n]:.2f}}}\n$, $\\omega_z$",
134             fontsize=8.5)
```

```
128     axs[0].set_ylabel("$b_{i n}$")
129     fig.tight_layout(); fig.savefig(f"{FIG}/moden_3ionen.pdf")
130
131     # Lamb-Dicke-Parameter Modell A (nu_z = 1 MHz), Strahlwinkel 20 Grad
132     wz = 2 * np.pi * 1e6
133     theta = np.deg2rad(20)
134     dk = 2 * (2 * np.pi / lam_D) * np.sin(theta / 2)
135     z0 = np.sqrt(hbar / (2 * m_Be * wz))
136     eta0 = dk * z0
137     wn = np.sqrt(mu) * wz
138     eta = eta0 * bA / np.sqrt(np.sqrt(mu))[None, :]
139     print(f"dk = {dk:.4e} 1/m, z0 = {z0*1e9:.2f} nm, eta0 = {eta0:.4f}")
140     print("eta_in (Zeilen Ion, Spalten Mode):\n", eta)
141     # Zum Vergleich 90-Grad-Geometrie
142     print("eta0 bei dk = sqrt2 k:", np.sqrt(2) * 2 * np.pi / lam_D * z0)
143
144     # Effektive Kopplung J_ij = Omega^2 sum_n eta_in eta_jn w_n / (mu^2 - w_n^2)
145     Om = 2 * np.pi * 50e3
146     for label, muL in [("knapp über COM (+10 kHz)", wn[0] + 2 * np.pi * 10e3),
147                       ("knapp über Streckmode (+10 kHz)", wn[1] + 2 * np.pi * 10e3),
148                       ("knapp über Knickmode (+10 kHz)", wn[2] + 2 * np.pi * 10e3),
149                       ("weit über allen Moden (3 MHz)", 2 * np.pi * 3.0e6)]:
150         J = Om**2 * (eta * (wn / (muL**2 - wn**2))[None, :]) @ eta.T
151         np.fill_diagonal(J, 0)
152         print(f"J/(2pi Hz), mu {label}:\n", J / 2 / np.pi)
153     # Zerlegung für J_13 in Modenbeiträge
154     print("b_1n b_3n =", bA[0] * bA[2], " b_1n b_2n =", bA[0] * bA[1])
```

A.2 Spin-Phonon-Dynamik und MS-Gate

```
1  """Kapitel 'Verschränkung über Phononen': numerische Simulation
2  (a) Seitenband-Sequenz (Cirac-Zoller-Idee): Qubit -> Phonon -> Qubit
3  (b) Mølmer-Sørensen-/Geometrisches-Phasen-Gate für 2 und 3 Ionen
4  Basis pro Ion: Index 0 = |up> = |0> (hell, initialisiert), Index 1 = |down> = |1>."""
5  import numpy as np
6  from scipy.linalg import expm
7  from scipy.integrate import solve_ivp
8  from konstanten import style, FIG
9
10 np.set_printoptions(precision=4, suppress=True)
11 I2 = np.eye(2)
12 X = np.array([[0, 1], [1, 0]], complex)
13 Y = np.array([[0, -1j], [1j, 0]])
14 Z = np.diag([1.0, -1.0]).astype(complex)
15 sp = np.array([[0, 1], [0, 0]], complex) # sigma_+ = |up><down|
16 sm = sp.T.copy()
17
18 def kron(*ops):
19     out = np.array([[1.0 + 0j]])
20     for o in ops:
21         out = np.kron(out, o)
22     return out
23
24 def boson(nmax):
25     a = np.diag(np.sqrt(np.arange(1, nmax)), 1).astype(complex)
26     return a, a.conj().T
27
28 # ----- (a)
```

```
29 def seitenband_sequenz(nmax=6):
30     a, ad = boson(nmax)
31     Im = np.eye(nmax)
32     # Resonante Seitenband-Hamiltonoperatoren (Wechselwirkungsbild, hbar = 1, Rabi = 1)
33     def H_rot(ion): # rotes Seitenband |down,n+1> <-> |up,n> : sigma_+ a + h.c.
34         s = [I2, I2]; s[ion] = sp
35         op = kron(*s, a)
36         return op + op.conj().T
37     def H_blau(ion): # blaues Seitenband |down,n> <-> |up,n+1> : sigma_+ a^dag + h.c.
38         s = [I2, I2]; s[ion] = sp
39         op = kron(*s, ad)
40         return op + op.conj().T
41     def puls(H, flaeche): # Pulsfläche theta = Omega_sb * t, U = exp(-i theta/2 * H)
42         return expm(-0.5j * flaeche * H)
43     psi = np.zeros(4 * nmax, complex); psi[0] = 1 # |up up, n=0>
44     def show(psi, titel):
45         print(titel)
46         for k in np.nonzero(np.abs(psi) > 1e-9)[0]:
47             s1, rest = divmod(k, 2 * nmax); s2, n = divmod(rest, nmax)
48             print(f" {psi[k]:+.4f} |{'ud'[s1]}{'ud'[s2]}, n={n}>")
49     show(psi, "Start:")
50     psi = puls(H_rot(0), np.pi / 2) @ psi; show(psi, "nach rotem pi/2-Puls auf Ion 1:")
51     psi = puls(H_blau(1), np.pi) @ psi; show(psi, "nach blauem pi-Puls auf Ion 2:")
52     return psi
53
54 # ----- (b)
55 def ms_simulation(Nion=2, g=1.0, K=1, nmax=20, n0=0, tfac=1.0, npts=400):
56     """H_I(t) = g * S_x (a e^{-i d t} + a^dag e^{i d t}), d = 4 g sqrt(K) (2 Ionen)."""
57     delta = 4 * g * np.sqrt(K) if Nion == 2 else 4 * g * np.sqrt(K)
58     a, ad = boson(nmax)
59     Sx = sum(kron(*[X if j == i else I2 for j in range(Nion)]) for i in range(Nion))
60     Is = np.eye(2*Nion)
61     A = np.kron(Sx, a); Ad = np.kron(Sx, ad)
62     def rhs(t, psi):
63         return -1j * g * ((A * np.exp(-1j * delta * t) + Ad * np.exp(1j * delta * t)) @ psi)
64     psi0 = np.zeros(2*Nion * nmax, complex); psi0[n0] = 1 # |0...0> (x) |n0>
65     T = tfac * 2 * np.pi * K / delta
66     ts = np.linspace(0, T, npts)
67     sol = solve_ivp(rhs, (0, T), psi0, t_eval=ts, rtol=1e-10, atol=1e-12)
68     return ts, sol.y, delta, nmax
69
70 def reduziere_spins(psi, Nion, nmax):
71     M = psi.reshape(2*Nion, nmax)
72     return M @ M.conj().T # reduzierte Dichtematrix der Spins
73
74 if __name__ == "__main__":
75     seitenband_sequenz()
76
77     # Analytische Erwartung
78     U = expm(-1j * np.pi / 4 * kron(X, X))
79     print("exp(-i pi/4 XX)|00> =", U[:, 0])
80
81     plt = style()
82     ts, Y_, delta, nmax = ms_simulation(Nion=2)
83     a, ad = boson(nmax)
84     nop = np.kron(np.eye(4), ad @ a)
85     P = []; nbar = []
86     for k in range(len(ts)):
87         rho = reduziere_spins(Y_[k], 2, nmax)
88         P.append(np.real(np.diag(rho))); nbar.append(np.real(Y_[k].conj() @ nop @ Y_[k])
89     )
```

```

89 P = np.array(P)
90 rho_end = reduziere_spins(Y[:, -1], 2, nmax)
91 print("Endzustand Spin-Dichtematrix (2 Ionen):\n", rho_end)
92 for target, nm in [(1, 0, 0, 1j), "(|00>+i|11>)/sqrt(2)", ((1, 0, 0, -1j), "(|00>-i|11>)/sqrt(2))]:
93     v = np.array(target) / np.sqrt(2)
94     print(f"Fidelity mit {nm}: {np.real(v.conj() @ rho_end @ v):.6f}")
95 print(f"<n> (t_g) = {nbar[-1]:.2e}, max <n> = {max(nbar):.3f}")
96
97 fig, ax = plt.subplots(1, 3, figsize=(7.4, 2.6))
98 tt = ts * delta / (2 * np.pi)
99 ax[0].plot(tt, P[:, 0], label="$P(00)$"); ax[0].plot(tt, P[:, 3], label="$P(11)$")
100 ax[0].plot(tt, P[:, 1] + P[:, 2], label="$P(01)+P(10)$")
101 ax[0].set_xlabel("$t\\,\\,\\delta/2\\pi$"); ax[0].legend(fontsize=7); ax[0].set_title("Populationen", fontsize=9)
102 ax[1].plot(tt, nbar, color="#8a5a9e"); ax[1].set_xlabel("$t\\,\\,\\delta/2\\pi$")
103 ax[1].set_title("mittlere Phononenzahl $\\langle n \\rangle$", fontsize=9)
104 # Phasenraum: alpha_s(t) = s g/delta (1 - e^{i delta t})
105 g = 1.0; t1 = np.linspace(0, 2 * np.pi / delta, 200)
106 for s, c in [(2, "#1c4270"), (0, "#2a7f62"), (-2, "#c8553d")]:
107     al = s * g / delta * (1 - np.exp(1j * delta * t1))
108     ax[2].plot(al.real, al.imag, color=c, label=f"$S_x={s:d}$")
109     ax[2].plot(al.real[0], al.imag[0], "o", color=c, ms=3)
110 ax[2].set_aspect("equal"); ax[2].set_xlabel("Re $\\alpha$"); ax[2].set_ylabel("Im $\\alpha$")
111 ax[2].legend(fontsize=7, loc="upper center"); ax[2].set_title("Phasenraum-Schleifen", fontsize=9)
112 fig.tight_layout(); fig.savefig(f"{FIG}/ms_gate.pdf")
113
114 # Unabhängigkeit vom Anfangs-Phononenzustand
115 for n0 in [0, 1, 3]:
116     ts2, Y2, _, nm = ms_simulation(Nion=2, n0=n0, nmax=30, npts=3)
117     rho = reduziere_spins(Y2[:, -1], 2, nm)
118     v = np.array([1, 0, 0, 1j]) / np.sqrt(2)
119     print(f"Start mit n0 = {n0}: Bell-Fidelity = {np.real(v.conj() @ rho @ v):.6f}")
120 # Fehlschliessen der Schleife: Gatezeit 2% zu lang
121 for tf in [1.0, 1.02, 1.05]:
122     ts3, Y3, _, nm = ms_simulation(Nion=2, tfac=tf, npts=3)
123     rho = reduziere_spins(Y3[:, -1], 2, nm)
124     v = np.array([1, 0, 0, 1j]) / np.sqrt(2)
125     print(f"Gatezeit x {tf}: Fidelity = {np.real(v.conj() @ rho @ v):.5f}, Reinheit Tr rho^2 = {np.real(np.trace(rho@rho)):.5f}")
126
127 # Drei Ionen über die Schwerpunktmode: g gleich für alle, delta = 4 g
128 ts4, Y4, _, nm = ms_simulation(Nion=3, npts=3)
129 rho3 = reduziere_spins(Y4[:, -1], 3, nm)
130 w, v = np.linalg.eigh(rho3)
131 print("3 Ionen: grösster Eigenwert von rho =", w[-1])
132 vec = v[:, -1] * np.exp(-1j * np.angle(v[0, -1]))
133 print("3 Ionen: Zustand (Basis 000..111):", vec)
134 Ua = expm(-1j * np.pi / 4 * (kron(X, X, I2) + kron(X, I2, X) + kron(I2, X, X)))
135 print("exp(-i pi/4 sum X_i X_j) |000> =", Ua[:, 0])
136 Ub = expm(+1j * np.pi / 4 * (kron(X, X, I2) + kron(X, I2, X) + kron(I2, X, X)))
137 print("exp(+i pi/4 sum X_i X_j) |000> =", Ub[:, 0] * np.exp(-1j * np.angle(Ub[0, 0])))
138 # Für ungerade Ionenzahl: zusätzliche globale Rotation R_x(pi/2) = exp(-i pi/4 S_x) ergibt GHZ
139 Sx3 = kron(X, I2, I2) + kron(I2, X, I2) + kron(I2, I2, X)
140 ghz = expm(-1j * np.pi / 4 * Sx3) @ Ub[:, 0]
141 ghz = ghz * np.exp(-1j * np.angle(ghz[0]))
142 print("R_x(pi/2)^{x3} * MS |000> =", ghz)

```

A.3 Shor-Algorithmus

```
1  """Kapitel 'Shor-Algorithmus': Zahlentheorie, exakte Messverteilungen,
2  Kettenbrüche und eine gatenae Simulation der Phasenschätzung für N = 15."""
3  from math import gcd
4  from fractions import Fraction
5  import numpy as np
6  from konstanten import style, FIG
7
8  def ordnung(a, N):
9      r, y = 1, a % N
10     while y != 1:
11         y = (y * a) % N; r += 1
12     return r
13
14 def euklid(a, b, verbose=False):
15     while b:
16         if verbose: print(f" {a} = {a//b}*{b} + {a%b}")
17         a, b = b, a % b
18     return a
19
20 def kettenbruch(num, den):
21     """Koeffizienten [a0; a1, a2, ...] und Näherungsbrüche von num/den."""
22     koef, konv = [], []
23     p0, q0, p1, q1 = 0, 1, 1, 0
24     n, d = num, den
25     while d:
26         a = n // d; koef.append(a)
27         p0, p1 = p1, a * p1 + p0
28         q0, q1 = q1, a * q1 + q0
29         konv.append(Fraction(p1, q1))
30         n, d = d, n - a * d
31     return koef, konv
32
33 def verteilung(N, a, Q):
34     """Exakte Wahrscheinlichkeit P(k) nach QFT des ersten Registers
35     (zweites Register implizit gemessen/verfolgt)."""
36     x = np.arange(Q)
37     f = np.array([pow(a, int(xx), N) for xx in x])
38     P = np.zeros(Q)
39     for y in np.unique(f):
40         amp = np.zeros(Q, complex); amp[f == y] = 1.0
41         # QFT:  $A(k) = 1/Q \sum_x e^{2\pi i x k / Q}$  ... (1/sqrt Q für Zustand, 1/sqrt Q für QFT)
42         A = np.fft.ifft(amp) * Q / Q # =  $(1/Q) \sum_x amp_x e^{+2\pi i x k / Q}$ 
43         P += np.abs(A)**2
44     return P
45
46 def r_aus_messung(k, Q, N):
47     if k == 0: return None
48     _, konv = kettenbruch(k, Q)
49     kand = [c.denominator for c in konv if c.denominator < N]
50     return kand[-1] if kand else None
51
52 if __name__ == "__main__":
53     print("Euklid gcd(9, 21):"); print(" ->", euklid(21, 9, verbose=True))
54     print("Euklid gcd(63, 1071)... Beispiel:", euklid(1071, 462, verbose=True))
55     for N in [15, 21, 35]:
56         print(f"\n=== N = {N} ===")
57         ok_count, tot = 0, 0
58         for a in range(2, N):
```

```

59     if gcd(a, N) != 1:
60         print(f" a={a:2d}: gcd(a,N)={gcd(a,N)} -> Faktor sofort (Glück)"); continue
61     r = ordnung(a, N); tot += 1
62     if r % 2 == 0 and pow(a, r // 2, N) != N - 1:
63         p, q = gcd(pow(a, r // 2) - 1, N), gcd(pow(a, r // 2) + 1, N)
64         ok_count += 1
65         print(f" a={a:2d}: r={r:2d}, a^(r/2) mod N = {pow(a,r//2,N):2d}, gcds = {p}, {q}
           ok")
66     else:
67         why = "r ungerade" if r % 2 else "a^(r/2) = -1 mod N"
68         print(f" a={a:2d}: r={r:2d} -- ({why})")
69     print(f" Erfolgsquote über teilerfremde a: {ok_count}/{tot} = {ok_count/tot:.3f}")
70
71     # Exakte Verteilungen
72     plt = style()
73     fig, ax = plt.subplots(2, 1, figsize=(6.6, 4.6))
74     for i, (N, a, Q) in enumerate([(15, 2, 256), (21, 2, 512)]):
75         P = verteilung(N, a, Q)
76         r = ordnung(a, N)
77         print(f"\nN={N}, a={a}, Q={Q}, r={r}: Summe P = {P.sum():.6f}")
78         top = np.argsort(P)[: -1][:14]
79         for k in sorted(top):
80             rc = r_aus_messung(k, Q, N)
81             _, konv = kettenbruch(k, Q)
82             print(f" k={k:3d} P={P[k]:.4f} k/Q={k/Q:.5f} Näherungsbrüche={ [str(c) for c in
               konv] } -> r-Kandidat {rc}")
83
84         # Erfolgswahrscheinlichkeit, dass der Kettenbruch direkt r liefert
85         ps = sum(P[k] for k in range(Q) if r_aus_messung(k, Q, N) == r)
86         print(f" P(Kettenbruch liefert direkt r={r}) = {ps:.4f}")
87         ax[i].vlines(np.arange(Q), 0, P, lw=0.9, color="#1c4270")
88         for s in range(r):
89             ax[i].plot(s * Q / r, -0.012, "^", color="#c8553d", ms=4, clip_on=False)
90             ax[i].set_xlim(-2, Q + 2); ax[i].set_ylabel("$P(k)$")
91             ax[i].set_title(f"$N={N}, \\\ a={a}, \\\ Q={Q}$: Peaks bei $k\\approx sQ/r$ mit $r={r}$",
               fontsize=9)
92         ax[1].set_xlabel("Messergebnis $k$ des ersten Registers")
93         fig.tight_layout(); fig.savefig(f"{FIG}/shor_verteilung.pdf")
94
95     # Zweig y = 1 für N = 21
96     Q, N, a = 512, 21, 2
97     xs = [x for x in range(Q) if pow(a, x, N) == 1]
98     M = len(xs)
99     print(f"\nN=21: Zweig f(x)=1 enthält M={M} Werte x = {xs[:4]} ... {xs[-1]}")
100    for k in [0, 85, 171, 256, 80]:
101        S = sum(np.exp(2j * np.pi * k * x / Q) for x in xs)
102        print(f" k={k:3d}: |S|^2/(M Q) = {abs(S)**2/(M*Q):.5f}")
103        print(f"4/pi^2 = {4/np.pi**2:.4f}")
104
105    # Phasenzeiger-Abbildung
106    fig, axs = plt.subplots(1, 4, figsize=(7.6, 2.3))
107    cases = [(16, 4, 4, 4, "$Q=16, \\\ r=4, \\\ k=4$"), (16, 4, 4, 1, "$Q=16, \\\ r=4, \\\ k=1$"),
      (512, 6, 86, 85, "$Q=512, \\\ r=6, \\\ k=85$"), (512, 6, 86, 80, "$Q=512, \\\ r=6, \\\ k=80$")]
108    for axx, (Q, r, M, k, tit) in zip(axs, cases):
109        z = np.exp(2j * np.pi * k * r * np.arange(M) / Q)
110        c = np.concatenate([ [0], np.cumsum(z) ])
111        axx.plot(c.real, c.imag, "-", lw=0.8, color="#1c4270")
112        if M <= 8:
113            for j in range(M):
114                axx.annotate("", xy=(c[j+1].real, c[j+1].imag), xytext=(c[j].real, c[j].imag),
                  arrowprops=dict(arrowstyle="->", color="#1c4270", lw=1.2))

```

```

116     axx.annotate("", xy=(c[-1].real, c[-1].imag), xytext=(0, 0),
117                 arrowprops=dict(arrowstyle="→", color="#c8553d", lw=1.6))
118     axx.set_aspect("equal"); axx.set_title(tit + f"\n$|S|={abs(c[-1]):.2f}$", fontsize=8)
119     axx.set_xticks([]); axx.set_yticks([])
120     for sp in axx.spines.values(): sp.set_visible(False)
121     xr = [c.real.min(), c.real.max()]; yr = [c.imag.min(), c.imag.max()]
122     span = max(xr[1] - xr[0], yr[1] - yr[0], 1.0) * 0.6 + 0.3
123     cx, cy = np.mean(xr), np.mean(yr)
124     axx.set_xlim(cx - span, cx + span); axx.set_ylim(cy - span, cy + span)
125     axx.plot([0], [0], "o", color="k", ms=2.5)
126     fig.tight_layout(); fig.savefig(f"{FIG}/phasoren.pdf")
127
128     # Gatenae Simulation der Phasenschätzung, N=15, a=2, t=8 Zählqubits, 4 Arbeitsqubits
129     t, w = 8, 4
130     dim = 2**(t + w)
131     psi = np.zeros((2**t, 2**w), complex)
132     psi[:, 1] = 1 / np.sqrt(2**t) # H(x)t |0>, Arbeitsregister |1> = |0001>
133     def mult_rot(y, s): # Multiplikation mit 2s mod 15 = zyklische Bitrotation um s
134         if y == 15 or y == 0: return y
135         return ((y << s) | (y >> (4 - s))) & 0xF if s % 4 else y
136     for j in range(t): # kontrolliertes U(2j): U = mal 2 mod 15
137         s = (2**j) % 4 # 2(2j) mod 15 = Rotation um 2j mod 4
138         for x in range(2**t):
139             if (x >> j) & 1:
140                 row = psi[x].copy(); new = np.zeros_like(row)
141                 for y in range(16): new[mult_rot(y, s)] += row[y]
142                 psi[x] = new
143     # QFT auf erstem Register (Konvention wie im Text: e{+2 pi i x k / Q})
144     Qm = 2**t
145     j, k = np.meshgrid(np.arange(Qm), np.arange(Qm))
146     F = np.exp(2j * np.pi * j * k / Qm) / np.sqrt(Qm)
147     psi = F @ psi
148     Pk = np.sum(np.abs(psi)**2, axis=1)
149     print("\nGatenae Simulation N=15: Wahrscheinlichkeiten > 1e-6:",
150           {int(k): round(float(p), 4) for k, p in enumerate(Pk) if p > 1e-6})
151     # Tabelle der Multiplikation mit 2 mod 15 als Bitrotation
152     for y in [1, 2, 4, 8, 3, 7]:
153         print(f" y={y:2d}={y:04b} -> 2y mod 15 = {(2*y)%15:2d} = {(2*y)%15:04b}, Rotation: {
            mult_rot(y, 1):04b}")

```

A.4 Beryllium-Niveaus

```

1  """Kapitel 'Was ist das Qubit?': Hyperfein- und Zeeman-Struktur des
2  9Be+-Grundzustands 2S1/2 (J = 1/2, I = 3/2) durch exakte Diagonalisierung
3  der 8x8-Matrix H = A I.J + muB B (gJ Jz + gI Iz)."""
4  import numpy as np
5  from konstanten import *
6
7  def spin_ops(s):
8      """Spinoperatoren (Sx, Sy, Sz) für Spin s in der Basis m = s, s-1, ..., -s."""
9      m = np.arange(s, -s - 1, -1)
10     d = len(m)
11     Sz = np.diag(m)
12     Sp = np.zeros((d, d))
13     for k in range(1, d):
14         Sp[k - 1, k] = np.sqrt(s * (s + 1) - m[k] * (m[k] + 1))
15     Sx = (Sp + Sp.T) / 2
16     Sy = (Sp - Sp.T) / 2j

```

```
17     return Sx, Sy, Sz, m
18
19 Jx, Jy, Jz, mJ = spin_ops(0.5)
20 Ix, Iy, Iz, mI = spin_ops(1.5)
21 IJ = np.kron(Jx, Ix) + np.kron(Jy, Iy) + np.kron(Jz, Iz)
22 labels = [(a, b) for a in mJ for b in mI] # Produktbasis |mJ, mI>
23
24 def H_hz(B):
25     """Hamiltonoperator in Hz (E/h)."""
26     return A_hfs * IJ + muB * B / h * (gJ * np.kron(Jz, np.eye(4)) + gI * np.kron(np.eye(2),
27                                         Iz))
28
29 def niveaus(B):
30     E, V = np.linalg.eigh(H_hz(B))
31     # Zuordnung zu |mJ, mI> über den grössten Überlapp (gilt im Hochfeld)
32     idx = [int(np.argmax(np.abs(V[:, k])**2)) for k in range(8)]
33     return E, V, idx
34
35 if __name__ == "__main__":
36     print(f"gI = {gI:.4e}, muB/h = {muB/h/1e9:.4f} GHz/T")
37     print(f"Nullfeld-Hyperfeinaufspaltung 2|A| = {2*abs(A_hfs)/1e9:.6f} GHz")
38     for B in [0.0, 1e-4, 0.01, 3.0]:
39         E, V, idx = niveaus(B)
40         print(f"\nB = {B} T")
41         for k in range(8):
42             print(f" E/h = {E[k]/1e9:+10.5f} GHz dominanter Zustand |mJ,mI> = {labels[idx[k]]}
43             "
44             f" Gewicht {np.abs(V[idx[k],k])**2:.5f}")
45     # Qubitfrequenz |mJ=+1/2,mI=3/2> <-> |mJ=-1/2,mI=3/2> als Funktion von B
46     def f_qubit(B):
47         E, V, idx = niveaus(B)
48         up = E[idx.index(labels.index((0.5, 1.5)))]
49         dn = E[idx.index(labels.index((-0.5, 1.5)))]
50         return up - dn
51     for B in [2.9, 3.0, 3.002, 4.4588]:
52         f = f_qubit(B)
53         dfdB = (f_qubit(B + 1e-6) - f_qubit(B - 1e-6)) / 2e-6
54         print(f"B = {B:.4f} T : f_Qubit = {f/1e9:.4f} GHz, df/dB = {dfdB/1e9:.4f} GHz/T")
55     # B-Feld für f = 83.2 GHz (Jain et al. 2024)
56     from scipy.optimize import brentq
57     B83 = brentq(lambda B: f_qubit(B) - 83.2e9, 2.5, 3.5)
58     print(f"f_Qubit = 83.2 GHz <=> B = {B83:.4f} T")
59     # Näherung Paschen-Back
60     B = 3.0
61     approx = gJ * muB * B / h + A_hfs * 1.5
62     print(f"Paschen-Back-Näherung bei 3 T: {approx/1e9:.4f} GHz")
63     # Feldstabilität
64     print(f"Frequenzverschiebung bei dB/B = 1e-6 (3 T): {28.0e9*3e-6/1e3:.1f} kHz")
65
66     # Abbildung Breit-Rabi
67     plt = style()
68     Bs = np.linspace(0, 0.12, 400)
69     Es = np.array([np.linalg.eigvalsh(H_hz(b)) for b in Bs]) / 1e9
70     fig, ax = plt.subplots(1, 2, figsize=(7.2, 3.1))
71     for k in range(8):
72         ax[0].plot(Bs * 1e3, Es[:, k], lw=1.3)
73     ax[0].set_xlabel("$B$ / mT"); ax[0].set_ylabel("$E/h$ / GHz")
74     ax[0].set_title("Schwachtes Feld: $F=1$, $F=2$ spalten auf", fontsize=9)
75     ax[0].text(3, 0.75, "$F=1$", fontsize=9); ax[0].text(3, -0.55, "$F=2$", fontsize=9)
76     Bs2 = np.linspace(0, 3.2, 300)
77     Es2 = np.array([np.linalg.eigvalsh(H_hz(b)) for b in Bs2]) / 1e9
```

```
76     for k in range(8):
77         ax[1].plot(Bs2, Es2[:, k], lw=1.3)
78     ax[1].axvline(3.0, color="0.6", ls=":")
79     ax[1].set_xlabel("$B$ / T"); ax[1].set_ylabel("$E/h$ / GHz")
80     ax[1].set_title("Starkes Feld: $|m_J, m_I\rangle$ (Paschen--Back)", fontsize=9)
81     ax[1].annotate("$m_J=+1/2$ (4 Niveaus)", (0.1, 32), fontsize=8.5)
82     ax[1].annotate("$m_J=-1/2$ (4 Niveaus)", (1.0, -44), fontsize=8.5)
83     ax[1].annotate("", xy=(3.0, 41.6), xytext=(3.0, -41.5), arrowprops=dict(arrowstyle="<->",
84         color="#c8553d"))
84     ax[1].annotate("Qubit\n83.1 GHz", (2.2, -5), fontsize=8, color="#c8553d")
85     fig.tight_layout()
86     fig.savefig(f"{FIG}/breit_rabi.pdf")
87     print("Abbildung breit_rabi.pdf geschrieben")
```

Anhang B

Konstanten und Notation

B.1 Konstanten und $^9\text{Be}^+$ -Daten

Grösse	Symbol	Wert
reduzierte Planck-Konstante	$\hbar$	$1,054\,572 \cdot 10^{-34} \text{ J s}$
Elementarladung	e	$1,602\,177 \cdot 10^{-19} \text{ C}$
Coulomb-Konstante	$k_C = e^2/4\pi\epsilon_0$	$2,307 \cdot 10^{-28} \text{ J m}$
Bohrsches Magneton	$\mu_B/\hbar$	$13,996 \text{ GHz/T}$
Masse $^9\text{Be}^+$	m	$1,496\,42 \cdot 10^{-26} \text{ kg}$
Kernspin	I	$3/2$
Hyperfeinkonstante	A	$-625,009 \text{ MHz}$
Elektronen- g -Faktor	g_J	2.00226
Wellenlänge $^2S_{1/2} \leftrightarrow ^2P_{3/2}$	λ	$313,1 \text{ nm}$
Linienbreite	$\Gamma/2\pi$	$19,4 \text{ MHz}$
Qubitfrequenz bei 3 T	ν_0	$83,2 \text{ GHz}$
Feldempfindlichkeit	$\partial\nu_0/\partial B$	$28,0 \text{ GHz/T}$
Zyklotronfrequenz bei 3 T	ν_c	$5,112 \text{ MHz}$

B.2 Notation

Symbol	Bedeutung
$ 0\rangle \equiv \uparrow\rangle, 1\rangle \equiv \downarrow\rangle$	Qubit-Zustände $ m_J = \pm\frac{1}{2}, m_I = +\frac{3}{2}\rangle$
X, Y, Z	Pauli-Operatoren ($= \sigma_x, \sigma_y, \sigma_z$)
$R_\mu(\theta), XX(\chi)$	Rotation, Ising-/MS-Gate $e^{-i\chi X_i X_j}$
$\omega_z, \omega_\pm, \omega_c$	axiale, Zyklotron-/Magnetron-, freie Zyklotronfrequenz
ℓ	Längenskala der Ionenkette $(k_C/m\omega_z^2)^{1/3}$
d, ε	Fallenabstand, Kopplungsparameter $k_C/(m\omega^2 d^3)$
b_{in}	Beteiligung von Ion i an Mode n
$a_n, a_n^\dagger$	Vernichter/Erzeuger der Mode n
$z_{0,n}$	Grundzustandsausdehnung $\sqrt{\hbar/2m\omega_n}$
t_{ij}	Phononen-Hüpftrate zwischen Fallen i und j
η_{in}	Lamb-Dicke-Parameter
Ω, g_{in}	Rabi-Frequenz, Spin-Phonon-Kopplung $\eta_{in}\Omega/2$

μ, δ_n	Verstimmung der Seitenbandfelder, Verstimmung zur Mode n
J_{ij}	effektive Spin–Spin-Kopplung
N	(Kap. 12) zu faktorisierende Zahl
a, r	Basis, Ordnung von a modulo N
$Q = 2^t, k$	Grösse des Eingangsregisters, Messergebnis

Literaturverzeichnis

- [1] S. Jain et al. (Gruppe J. P. Home, ETH Zürich), *Penning micro-trap for quantum computing*, Nature **627**, 510–514 (2024); arXiv:2308.07672.
- [2] S. Jain, J. Alonso, M. Grau, J. P. Home, *Scalable arrays of micro-Penning traps for quantum computing and simulation*, Phys. Rev. X **10**, 031027 (2020).
- [3] ZuriQ, *ZuriQ raises \$25.5 million to scale new groundbreaking 2D quantum architecture*, Pressemitteilung, 28. Juli 2026, <https://zuriq.com/fundraise/zuriq-raises-25-5-million/>.
- [4] ZuriQ, *Planning for Fault-Tolerance with QC Design*, 4. September 2025, <https://zuriq.com/error-correction/planning-for-fault-tolerance-with-qc-design/>.
- [5] L. S. Brown, G. Gabrielse, *Geonium theory: Physics of a single electron or ion in a Penning trap*, Rev. Mod. Phys. **58**, 233 (1986).
- [6] S. Mavadia, J. F. Goodwin, G. Stutter, S. Bharadia, D. R. Crick, D. M. Segal, R. C. Thompson, *Control of the conformations of ion Coulomb crystals in a Penning trap*, Nat. Commun. **4**, 2571 (2013).
- [7] D. F. V. James, *Quantum dynamics of cold trapped ions with application to quantum computation*, Appl. Phys. B **66**, 181 (1998).
- [8] D. Leibfried, R. Blatt, C. Monroe, D. Wineland, *Quantum dynamics of single trapped ions*, Rev. Mod. Phys. **75**, 281 (2003).
- [9] J. I. Cirac, P. Zoller, *Quantum computations with cold trapped ions*, Phys. Rev. Lett. **74**, 4091 (1995).
- [10] K. Mølmer, A. Sørensen, *Multiparticle entanglement of hot trapped ions*, Phys. Rev. Lett. **82**, 1835 (1999).
- [11] C. A. Sackett et al., *Experimental entanglement of four particles*, Nature **404**, 256 (2000).
- [12] K. Kim et al., *Entanglement and tunable spin-spin couplings between trapped ions using multiple transverse modes*, Phys. Rev. Lett. **103**, 120502 (2009).
- [13] J. G. Bohnet et al., *Quantum spin dynamics and entanglement generation with hundreds of trapped ions*, Science **352**, 1297 (2016).
- [14] C. Monroe et al., *Programmable quantum simulations of spin systems with trapped ions*, Rev. Mod. Phys. **93**, 025001 (2021).
- [15] C.-C. J. Wang, A. C. Keith, J. K. Freericks, *Phonon-mediated quantum spin simulator employing a planar ionic crystal in a Penning trap*, Phys. Rev. A **87**, 013422 (2013).
- [16] D. Maslov, *Basic circuit compilation techniques for an ion-trap quantum machine*, New J. Phys. **19**, 023035 (2017).
- [17] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press (2010).

- [18] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26**, 1484 (1997); Konferenzversion FOCS 1994.
- [19] S. Beauregard, *Circuit for Shor's algorithm using $2n+3$ qubits*, Quantum Inf. Comput. **3**, 175 (2003).
- [20] T. Monz et al., *Realization of a scalable Shor algorithm*, Science **351**, 1068 (2016).
- [21] J. A. Smolin, G. Smith, A. Vargo, *Oversimplifying quantum factoring*, Nature **499**, 163 (2013).
- [22] C. Gidney, M. Ekerå, *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*, Quantum **5**, 433 (2021); arXiv:1905.09749 (2019).
- [23] C. Gidney, *How to factor 2048 bit RSA integers with less than a million noisy qubits*, arXiv:2505.15917 (2025).