

ESTEBAN A. MARTINEZ

QUANTUM COMPUTATION AND QUANTUM SIMULATION
WITH A TRAPPED-ION QUANTUM COMPUTER

QUANTUM COMPUTATION AND QUANTUM SIMULATION WITH A TRAPPED-ION QUANTUM COMPUTER

ESTEBAN A. MARTINEZ

A dissertation submitted to the Faculty of Mathematics,
Computer Science and Physics of the University of Innsbruck,
in partial fulfillment of the requirements for the degree of
Doctor of Natural Science (Doctor rerum naturalium).

Carried out under the supervision of Prof. Rainer Blatt at the
Quantum Optics and Spectroscopy Group.



Institute for Experimental Physics
University of Innsbruck

December 2016

ABSTRACT

The field of experimental quantum information processing is already at the stage where few-qubit quantum computers are available, such as the one in our laboratory, consisting of a string of $^{40}\text{Ca}^+$ ions confined in a macroscopic linear Paul trap. In this work, improvements to the experimental setup are shown, followed by recent experiments. A new software for compiling quantum algorithms into experimental pulse sequences is described, that improves on previously existing tools. Then, a new laser setup for Raman cooling is shown. These tools are applied to experiments exploring two research lines: quantum computation and quantum simulations. The first experiment reported is a scalable implementation of Shor's algorithm for integer factoring, paradigmatic for quantum computation. The second experiment is a quantum simulation of quantum electrodynamics, as a particular case of lattice gauge theories, which are fundamental for high-energy physics. Here it is experimentally demonstrated how these theories can be efficiently simulated on a quantum computer.

ZUSAMMENFASSUNG

Im Forschungsgebiet der experimentellen Quanteninformationsverarbeitung sind bereits Quantenrechner mit wenigen Qubits verfügbar. In unserem Labor haben wir einen Quanteninformationsprozessor, der mit einzelnen gefangenen $^{40}\text{Ca}^+$ Ionen in einer makroskopischen Paulfalle rechnet. Diese Dissertation befasst sich mit Beiträgen zum experimentellen Aufbau und kürzlich durchgeführten Experimenten. Es wird eine neue Software zum Übersetzen von Quantenalgorithmen in experimentelle Pulssequenzen beschrieben, die auf einer bereit verfügbaren Methode aufbaut und diese verbessert. Dann wird ein neuer Laseraufbau vorgezeigt, der zur Laserkühlung an einem Ramanübergang verwendet wird. Die Nützlichkeit dieser Erweiterungen wird anhand von Experimenten zu Quantenalgorithmen und Quantensimulation demonstriert. Das erste Experiment ist eine skalierbare Implementierung des Shor-Algorithmus zur Faktorisierung ganzer Zahlen, ein Musterbeispiel für die Leistungsfähigkeit eines Quantenrechners. Weiters wird eine Quantensimulation der Quantenelektrodynamik als Beispiel für eine Gittereichfeldtheorie demonstriert. Solche Theorien sind ein wesentlicher Grundbaustein der Hochenergiephysik. In dieser Arbeit wird experimentell bewiesen, wie sie mithilfe eines Quantenrechners effizient simuliert werden können.

ACKNOWLEDGMENTS

First and foremost I would like to thank my advisor, Prof. Rainer Blatt, who gave a theorist the opportunity to try his hand at lab work and become an experimentalist. To whatever extent this succeeded is certainly because of his guidance, support and the encouraging work environment that he cultivates.

The experiments that I show in this thesis are the result of much hard work by many people. Thanks to my LinTrap lab and office mates Thomas Monz, Philipp Schindler, Daniel Nigg and Alexander Erhard for their patience, companionship and good humor. Flying brains, Graukas tasting sessions and cups of mate at 2 AM to finish state tomographies have made the work a lot more enjoyable.

Working in this research group has been a privilege, and it is hard to name all the people I have learnt from. Among them I would like to thank: Senior scientists Mike Chwalla, Yves Colombe, Markus Henrich, Ben Lanyon, Tracy Northup and Christian Roos, who have always been willing to lend a hand and share their experience. Matthias Brandl and Muir Kumph for patient advice on electronics. Cornelius Hempel and Klemens Schüppert for their help with server administration. The administrative staff Patricia, Renate, Karin and Michaela for making our daily work much easier, and the staff at the electronic and mechanical workshops for their valuable assistance.

Most of the results shown here are the fruit of close collaborations between experiment and theory. It has been fundamental to have great theorists close by to provide exciting ideas, plan experiments and interpret results. Among them, I would like to thank Marcello Dalmonte, Christine Muschik and Prof. Peter Zoller for the collaboration on the gauge theory simulations, and Markus Müller and Prof. Miguel Ángel Martín-Delgado on the color code project (and tapas in Madrid).

Academic matters aside, I would also like to thank the many colleagues and friends who have made me feel welcome in Innsbruck and were German and Tyrolean teachers, skiing, snowboarding, mountain biking and climbing coaches, fellow cooks, chess opponents, musical partners and brunch companions. I cannot really name all the people who helped make the time outside the lab that much nicer without forgetting anyone, but I am happy to have met many great people here.

My last but not least thanks go to my parents. It is owing to their effort, encouragement and support that I was able to come to Innsbruck to carry out this work.

CONTENTS

1	INTRODUCTION	1
2	QUANTUM INFORMATION WITH TRAPPED IONS	5
2.1	Quantum information	5
2.2	Quantum computing	8
2.3	The $^{40}\text{Ca}^+$ qubit	10
2.4	Experimental toolbox	12
2.5	Digital quantum simulation	14
3	SHOR'S ALGORITHM	17
3.1	The quantum Fourier transform	17
3.2	Order-finding	19
3.3	Shor's algorithm	22
4	SIMULATING LATTICE GAUGE THEORIES	25
4.1	The Schwinger model	26
4.2	Lattice gauge theories	28
4.2.1	Dirac fermions on a lattice	29
4.2.2	Coupling to gauge fields	30
4.3	Spin models	32
4.3.1	Mapping fermions to spins	32
4.3.2	Mapping gauge fields to spins	33
4.3.3	Encoding gauge fields into long-range interactions	33
5	COMPILING QUANTUM ALGORITHMS	37
5.1	Compilation of local unitaries	38
5.2	Compilation of general unitaries	41
5.2.1	Compilation in layers	42
5.2.2	Numerical optimization	44
5.2.3	Compilation of isometries	47
5.2.4	Compensation of systematic errors	49
6	A LASER SETUP FOR RAMAN COOLING	51
6.1	Raman cooling	51
6.2	Optical setup	54
6.3	Experimental implementation of Raman cooling	56
7	REALIZATION OF A SCALABLE SHOR ALGORITHM	61
7.1	Requirements for a scalable implementation	61
7.2	Experimental implementation	65
7.3	Results	68

8	SIMULATION OF A WILSON MODEL	71
8.1	Introduction	71
8.2	Encoding of the Schwinger model	72
8.3	Implementation of the encoded Schwinger model	74
8.3.1	Long-range interactions	77
8.3.2	Nearest neighbor terms	78
8.3.3	Single-particle terms	79
8.4	Measurement and postselection	79
8.5	Experimental results	80
8.6	Experimental errors	84
8.7	Finite size effects	85
9	SIMULATION OF A QUANTUM LINK MODEL	87
9.1	The Schwinger model	87
9.2	Experimental implementation and results	90
10	SUMMARY AND OUTLOOK	93
A	APPENDIX TO THE QUANTUM COMPILER	95
A.1	Compiling local unitaries	95
A.1.1	Finding basis changes	95
A.1.2	Writing a unitary as a product of two equatorial rotations	95
A.1.3	Unitaries up to a collective Z rotation	96
A.1.4	Unitaries up to independent Z rotations	98
B	APPENDIX TO SHOR'S ALGORITHM	101
B.1	Pulse sequence optimisation	101
B.2	Controlled-SWAP	101
B.3	Four-Target Controlled-NOT	102
B.4	Two-Target Controlled-NOT	102
B.5	Controlled Quantum Modular Multipliers	103
	PUBLICATIONS	105
	BIBLIOGRAPHY	107
	INDEX	117

LIST OF FIGURES

Figure 1	Moore's law.	2	
Figure 2	The Bloch sphere representation.	7	
Figure 3	A quantum circuit with controlled gates and measurements at the end.	9	
Figure 4	Quantum circuit representation for the CNOT gate.	10	
Figure 5	A string of four ions trapped in our linear Paul trap.	11	
Figure 6	$^{40}\text{Ca}^+$ electronic level scheme.	11	
Figure 7	Beam configuration in our experimental setup.	12	
Figure 8	Electronic level manifold of $^{40}\text{Ca}^+$ with Zeeman splitting.	14	
Figure 9	Stroboscopic implementation of a time evolution.	15	
Figure 10	Implementation of the inverse quantum Fourier transform (QFT [†]) on 3 qubits.	19	
Figure 11	Kitaev's version of the QFT.	20	
Figure 12	The order-finding algorithm.	21	
Figure 13	Order-finding with Kitaev's QFT.	22	
Figure 14	Behavior of the electric field lines in classical electromagnetism.	27	
Figure 15	The string breaking mechanism.	28	
Figure 16	Definition of the lattice.	29	
Figure 17	Elimination of the gauge fields using Gauss' law.	35	
Figure 18	Pulse sequence to perform a projective measurement on the $\{X, Y, Z\}$ bases.	39	
Figure 19	Decomposition of a Toffoli gate.	42	
Figure 20	Sequence with layers of local and entangling gates applied consecutively.	43	
Figure 21	Average time required to find the global optimum.	46	
Figure 22	Optimal number of entangling gates needed to compile random Clifford operations.	47	
Figure 23	Compilation of an isometry.	49	
Figure 24	State fidelity for a Toffoli gate applied on the 8 canonical input states.	50	
Figure 25	Level scheme for sideband cooling.	52	
Figure 26	Three-level Λ system.	53	
Figure 27	Spatial arrangement of the three Raman cooling beams.	53	

Figure 28	Optical setup for producing and tuning the Raman cooling light.	54
Figure 29	Offset lock scheme for stabilizing the Raman cooling laser to an already locked laser.	55
Figure 30	Error signal after conversion of the beat frequency to voltage.	55
Figure 31	Excitation spectrum of the Raman transition $4^2S_{1/2}(m = -1/2)$ to $4^2S_{1/2}(m = +1/2)$.	57
Figure 32	Exponential decays of the $4^2S_{1/2}(m = -1/2)$ population.	58
Figure 33	Frequency scan around the Raman cooling transition.	59
Figure 34	Rabi flops on the blue sideband of the qubit transition.	59
Figure 35	Quantum circuits of Shor's algorithm for factoring 15.	62
Figure 36	Experimentally obtained truth table of the controlled 2 mod 15 multiplier	63
Figure 37	Setup for performing conditional operations depending on the state of the ions.	66
Figure 38	In-sequence photon-count histogram.	67
Figure 39	Results and correct order-assign probability for the different implementations to factor 15.	68
Figure 40	Encoding fermions in Wilson's lattice gauge theories into spins.	73
Figure 41	Effective long-range interactions emerging from the elimination of the gauge fields.	74
Figure 42	Time-discretization scheme for the digital quantum simulation of our model.	74
Figure 43	Implementation of the long-range interactions by means of Mølmer-Sørensen (MS) gates.	75
Figure 44	Experimental pulse sequence for the Wilson model simulation.	76
Figure 45	Time evolution of the particle number density v .	81
Figure 46	Time evolution of the vacuum persistence amplitude and entanglement.	83
Figure 47	Comparison of the evolutions of the particle number density $v(t)$ and the rate function $\lambda(t)$.	84
Figure 48	Evolution of the particle number density v and the logarithmic negativity E_n for different system sizes N .	86
Figure 49	Encoding of the fermions and gauge fields for a quantum link model (QLM).	88
Figure 50	The two physical states of our minimal QLM.	89

Figure 51	Excitation of the e^-e^+ state as a function of time.	89
Figure 52	Pulse sequence for the experimental implementation of the QLM simulation.	90
Figure 53	Time evolution of the QLM simulation for different masses.	91
Figure 54	Observed evolution parameters as a function of the mass.	92
Figure 55	QLM with periodic boundary conditions.	92
Figure 56	Controlled modular multipliers.	104

LIST OF TABLES

Table 1	Controlled SWAP operation	102
Table 2	Four-target controlled NOT	102

LIST OF ALGORITHMS

Figure 1	Quantum order-finding	21
Figure 2	Shor's algorithm	23

LIST OF ACRONYMS

AMO	atomic, molecular and optical physics
AOM	acousto-optic modulator
CCD	charge coupled device
CNOT	controlled-NOT
DC	direct current
DFT	discrete Fourier transform
ELI	Extreme Light Infrastructure

- FET field-effect transistor
- LGT lattice gauge theory
- MS Mølmer-Sørensen
- PDH Pound-Drever-Hall
- PID Proportional-Integral-Differential
- QC quantum computer
- QCD quantum chromodynamics
- QED quantum electrodynamics
- QFT quantum Fourier transform
- QLM quantum link model
- RF radio-frequency
- RSA Rivest-Shamir-Adleman
- S/H sample and hold
- SBC sideband cooling
- SSO squared statistical overlap
- WM Wilson model
- XCELS Exawatt Center for Extreme Light Studies

INTRODUCTION

“Begin at the beginning,” the King said, very gravely, “and go on till you come to the end: then stop.”

—Lewis Carroll, *Alice in Wonderland* [1]

Quantum mechanics has revolutionized science and technology in the twentieth century, enabling applications such as semiconductor devices, lasers and superconducting materials. However, these developments all rely on the *bulk* manipulation of large ensembles of quantum mechanical systems. As E. Schrödinger put it in 1952: “We never experiment with just one electron or atom or (small) molecule. In thought experiments we sometimes assume that we do; this invariably entails ridiculous consequences. . . we are not experimenting with single particles, any more than we can raise Ichthyosauria in the zoo.” [2] Only seven years later, R. Feynman offered a different perspective: “The principles of physics, as far as I can see, do not speak against the possibility of maneuvering things atom by atom. It is not an attempt to violate any laws; it is something in principle that can be done, but has not been done because we are too big.” [3]

Thanks to the advances in experimental quantum optics towards the end of the twentieth century, we can now confidently say that we can, indeed, maneuver things atom by atom. We now have full experimental control of the individual quantum states of trapped atoms or ions, together with the ability to engineer interactions between them [4]. This allows us to encode and manipulate *quantum information*, much in the way that classical computers process classical information. We already have, in effect, small-scale *quantum computers* in the laboratory [5]. What can we achieve with this new technology?

In this thesis, some of the possibilities offered by a small-scale trapped-ion quantum computer are explored. One promising road to follow with quantum technology is to perform computational tasks that are not feasible for classical computers. It is the case for many important problems that the computational resources required to solve them grow exponentially with the problem size. Despite the technological progress of the semiconductor industry, the progress of transistor speed and miniaturization is slowing down and might plateau in the near future (see Figure 1). This means that simply employing more classical computational power will not be sustainable in the future, and thus a radically new approach is needed. Quantum mechanics offers a way around this obstacle, since quantum systems are intrinsically richer than classical ones. Several algorithms have been

proposed that take advantage of quantum mechanical phenomena like *superposition* or *entanglement* for performing tasks more efficiently than classical computers [6]. In this thesis a paradigmatic example is discussed, Shor’s algorithm for integer factoring [7], which we have implemented for the first time in a scalable way.

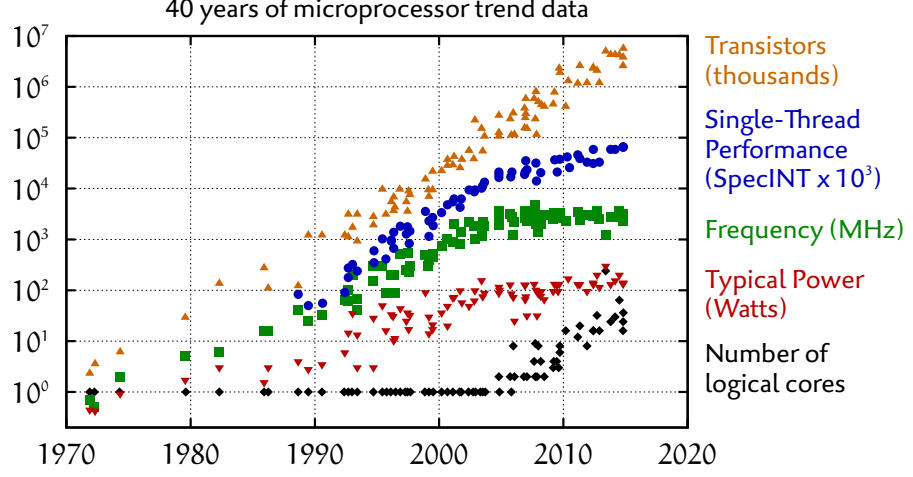


Figure 1: Evolution of microprocessors since the 1970’s. The data shows an exponential growth until the year 2000 (Moore’s law) and a slow-down since then. Credit K. Rupp¹.

The second avenue of research that is presented here is to exploit quantum computers to investigate the fundamental laws of nature. Interactions between the elementary constituents of matter are described by so-called *gauge theories* [8, 9]. However, computing the real-time dynamics in gauge theories is a notorious challenge for classical computational methods. This is so because the processing time and memory requirements increase exponentially with the system size. In the spirit of Feynman’s vision of a quantum simulator [10, 11], this has recently stimulated theoretical effort to devise schemes for simulating such theories on engineered quantum devices. Such simulations can solve these problems efficiently, that is, the required simulation time and simulator size scale polynomially with the system size [12]. In this thesis, the first experimental demonstration of a digital quantum simulation of a lattice gauge theory is reported. More specifically, quantum electrodynamics in one spatial dimension (the Schwinger model) [13, 14] is investigated.

The structure of this thesis is as follows: In Chapter 2, the fundamentals of quantum information processing using trapped $^{40}\text{Ca}^+$ ions are introduced. In Chapter 3, Shor’s algorithm is presented as a paradigmatic application of quantum computing, as well as the experimental requirements for its scalable implementation. In Chapter 4, two

¹ Original data up to the year 2010 collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten. New plot and data collected for 2010–2015 by K. Rupp. Adapted from: <https://www.karlrupp.net/2015/06/40-years-of-microprocessor-trend-data/>.

frameworks for quantum simulation of gauge theories are introduced: quantum link models and Wilson models. In Chapter 5, a tool to enable the implementation of quantum algorithms or simulations is described, consisting of software for compilation of quantum unitaries into experimentally available pulse sequences. In Chapter 6, a technical improvement to the existing experimental setup is presented: a new laser setup for Raman cooling. In Chapter 7, an experimental implementation of Shor's algorithm is described. In Chapters 8 and 9 the implementation of two different approaches to quantum simulation of lattice gauge theories is shown. Finally, in Chapter 10 the contents of this work are summarized and an outlook towards future advances is given.

By any objective standard, the theory of computational complexity ranks as one of the greatest intellectual achievements of humankind – along with fire, the wheel, and computability theory.

—Scott Aaronson, Quantum Computing Since Democritus [15]

Quantum mechanics has not only revolutionized the foundations of physics, but also changed the way we understand information and computation. Quantum systems are richer than classical ones: they can store more information and offer additional resources that can be used for computation. For this reason, in the past few decades strong theoretical and experimental efforts have focused on realizing a *quantum computer*: a device that can perform computation making direct use of quantum-mechanical phenomena. To achieve this, we must use a physical system that offers both robustness against external disturbances and a high degree of control. Trapped ions fulfill these requirements, and therefore are a promising platform for quantum computation. Since the appearance of the landmark work by I. Cirac and P. Zoller [16] describing the implementation of logic gates using trapped-ion qubits, many experimental advances have been made in this field [4, 5, 17, 18]. Nowadays, small-scale quantum information processors based on trapped ions are available in the laboratory.

In this chapter, some basic concepts in the field of quantum information processing are introduced. In Section 2.1 quantum computers are introduced, together with the criteria that they must fulfill so as to be useful. In Section 2.3, it is shown how to implement a quantum computer with trapped ions. In Section 2.4, the experimental toolbox that is available in our trapped-ion system is described. Finally, in Section 2.5 it is shown how this toolbox can be used to perform digital quantum simulations of physical systems.

QUANTUM INFORMATION

The basic unit of information in modern digital computing is the *bit*, which can have only one of two values; let us call these 0 and 1. A bit can be implemented by any physical system with two possible states, for example, two stable voltages of a flip-flop circuit or two magnetization directions. By analogy, a quantum system which can be in two possible states, which we call $|0\rangle$ and $|1\rangle$, is called a *qubit* (quantum bit) [6, 19]. The key distinction from classical bits is the fact

that the state of a qubit is not necessarily either $|0\rangle$ or $|1\rangle$, but can be a *superposition* of both. In quantum mechanics, the state of an *isolated* physical system is described by a vector in the space of all possible states, called a *Hilbert space* [6]. The most general state of a qubit is described by a vector $|\psi\rangle$ that is a linear combination of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

Suppose the state of a quantum system is not completely known, namely, we might only know that it is in certain states $\{|\psi_i\rangle\}$ with probabilities p_i . In this case, the state can be described using the *density matrix* formalism [6]. The density matrix ρ is an operator defined by:

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|. \quad (2)$$

The notation $|\psi_i\rangle \langle\psi_i|$ corresponds to an operator that maps the state $|\psi_i\rangle$ to $|\psi_i\rangle$, and maps every state orthogonal to $|\psi_i\rangle$ to 0. The density matrix of a system completely describes its state and allows us to calculate any quantities of interest. For instance, the expectation value of any observable A , represented by a Hermitian matrix, can be calculated as:

$$\langle A \rangle = \text{tr}(A\rho). \quad (3)$$

In the case that the system is described by a single quantum state $|\psi_i\rangle$, with probability $p_i = 1$, we call its state *pure*. Mathematically, this corresponds to the condition [6]:

$$\text{tr } \rho^2 = 1. \quad (4)$$

On the contrary, if a system is in a mixture of several quantum states, we say it is in a *mixed* state. The most general density matrix of a qubit can be written as:

$$\rho = \frac{1}{2}(\mathbb{1} + r_x \sigma_x + r_y \sigma_y + r_z \sigma_z), \quad (5)$$

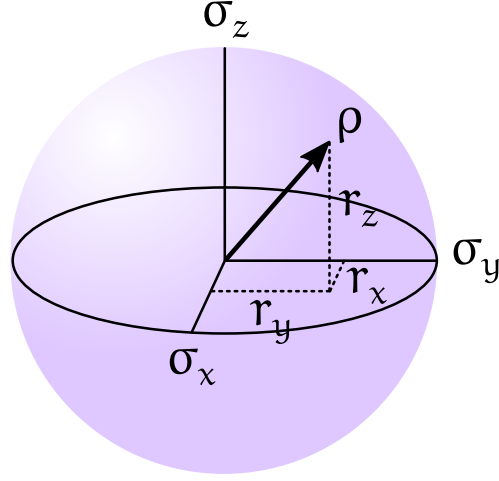


Figure 2: The Bloch sphere is a convenient representation of the state of a qubit, in this case described by the density matrix $\rho = (\mathbb{1} + r_x \sigma_x + r_y \sigma_y + r_z \sigma_z)/2$.

where $\mathbb{1}$ is the 2×2 identity matrix, $\sigma_{x,y,z}$ are the *Pauli matrices*:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (6)$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad (7)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (8)$$

and $\mathbf{r} = (r_x, r_y, r_z)$ is a real vector with $\|\mathbf{r}\| \leq 1$. In this way, the state of a qubit as a density matrix corresponds to a vector $\mathbf{r}$. This has a convenient pictorial representation in terms of the *Bloch sphere*, as shown in Figure 2. The basis states $|0\rangle$ and $|1\rangle$ lie on the south and north poles of the Bloch sphere, respectively. Pure states lie on the surface of the sphere, and mixed states in its interior.

If we are dealing with a composite system made of N qubits, its possible states are spanned by the products of all possible states of each individual qubit. For instance, the state of an isolated two-qubit system can be written as:

$$\rho = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle, \quad (9)$$

where the first and second numbers in each state vector correspond to the states of qubit 1 and 2, respectively, and $\sum |\alpha_i|^2 = 1$. As opposed to classical systems, it may not be possible to describe the state of a quantum system by simply describing the state of each of its components. If the state $|\psi\rangle$ of a quantum system can be separated as

$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_N\rangle$, we say that the state is *separable*. If this is not the case, then it is *entangled*.

Entanglement is of great theoretical and experimental interest, since it is a characteristic feature of quantum systems and cannot be described classically. It can be quantified in different ways; in Chapter 8 we use a measure known as the *logarithmic negativity* [20], which we proceed to define. Let us consider a system with state ρ , divided into subsystems A and B, such that:

$$\rho = \sum_{ijkl} p_{kl}^{ij} |i\rangle\langle j| \otimes |k\rangle\langle l|. \quad (10)$$

The *partial transpose* of the density matrix ρ with respect to subsystem A is defined as:

$$\rho^{T_B} = \sum_{ijkl} p_{kl}^{ij} |j\rangle\langle i| \otimes |k\rangle\langle l|. \quad (11)$$

The logarithmic negativity E_n quantifies how much entanglement there is between the subsystems A and B, and is defined as:

$$E_N(\rho) = \log_2 \|\rho^{T_A}\|_1, \quad (12)$$

where $\|X\|_1 = \text{Tr}|X| = \text{Tr}\sqrt{X^\dagger X}$ is the *trace norm*, or the sum of the singular values of the operator X .

QUANTUM COMPUTING

A *quantum computer* is a device that can store and manipulate quantum information. These manipulations are performed as a sequence of *quantum gates*, which are operations that take a quantum state as an input and produce a quantum state as output. Formally, a quantum gate is a unitary operator U which maps state vectors to state vectors:

$$U |\psi_{\text{input}}\rangle = |\psi_{\text{output}}\rangle, \quad (13)$$

where U is a matrix such that the inverse operation U^{-1} is given by:

$$U^{-1} = U^\dagger = (U^T)^*. \quad (14)$$

A unitary operation cannot map two different input states $|\psi_1\rangle$ and $|\psi_2\rangle$ to the same output state, so quantum information cannot be lost. This implies that quantum operations are *reversible* [6].

A *universal quantum computer* is a quantum device able to implement arbitrary unitary operations, or at least to approximate them to arbitrary accuracy. However, in any specific implementation of a quantum computer, only a certain set of operations is available. There-

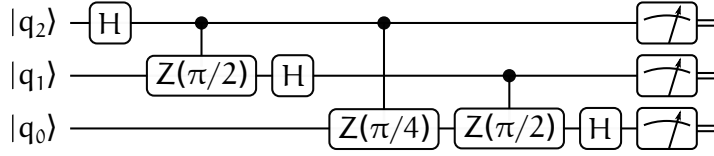


Figure 3: A quantum circuit with controlled gates and measurements at the end.

fore, it is necessary to decompose the desired unitary operation as a sequence of these available quantum gates. A set of quantum gates is known as *universal* if it is possible to approximate any unitary quantum operation to an arbitrary accuracy with a sequence of these gates.

A universal set of gates requires both *local* operations, which can be expressed as the product of single-qubit operations, and *multi-qubit* operations, which implement interactions between the qubits and can produce entanglement. An example of a single-qubit operation is the *Hadamard gate*, which creates a superposition state on a qubit starting from a basis state, and is represented by the unitary matrix:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (15)$$

A frequently used two-qubit operation is the CNOT gate, which flips a *target* qubit conditionally on the state of a *control* qubit, as described by the unitary matrix:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (16)$$

A canonical universal set of gates [6] consists of single-qubit operations plus CNOT gates. Other universal sets of gates can be used to implement quantum operations, such as the set described in Section 2.4.

Quantum algorithms, namely, sequences of quantum unitaries, are usually visually depicted as *quantum circuits* [21], as shown in Figure 3. Each qubit is depicted by a single straight line, with its initial state to the left. The quantum algorithm is represented from left to right, with each quantum gate depicted as a box. Conditional quantum gates are represented by a dot on the control qubit and a vertical line connecting it to the gate, as depicted in Figure 4 for the CNOT gate.

The key criteria for a successful implementation of a quantum computer, as listed by D. DiVincenzo [22], are:

1. A scalable physical system with well characterized qubits.

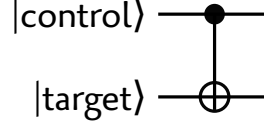


Figure 4: Quantum circuit representation for the CNOT gate.

2. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000\dots\rangle$.
3. Long relevant decoherence times, much longer than the gate operation time.
4. A “universal” set of gates.
5. A qubit-specific measurement capability.
6. The ability to interconvert stationary and flying qubits.
7. The ability to faithfully transmit flying qubits between specified locations.

THE $^{40}\text{Ca}^+$ QUBIT

Here and in the rest of this work, all experimental implementations are based on qubits encoded in the electronic degrees of freedom of trapped ions. The use of trapped ions for quantum computing is by now a standard technique, and has already been described extensively in the literature [4, 5, 17, 18]. Our implementation of a quantum information processor is based on trapped $^{40}\text{Ca}^+$ ions in a linear Paul trap, as depicted in Figure 5. This system has already been described in detail in [23], so it will be only briefly reviewed. The relevant electronic level scheme for $^{40}\text{Ca}^+$ is shown in Figure 6. The $3^2\text{D}_{5/2}$ level has a lifetime of 1.045 s [24] before decaying to the ground state $4^2\text{S}_{1/2}$, which is much longer than typical gate durations (on the order of μs) [18]. Moreover, the $3^2\text{D}_{5/2}$ to $4^2\text{S}_{1/2}$ transition has a wavelength of 729 nm, which means it can be conveniently manipulated using laser pulses in the optical regime.

Ions in a Paul trap are subject to effective harmonic trapping potentials (*secular* potentials) along the axial and radial directions. An ion crystal trapped in these potentials has motional modes which can be cooled down close to their ground state and coherently manipulated by means of laser pulses [17]. An ion can absorb a photon that is blue- or red-detuned from the electronic transition by the secular frequency of a motional mode. This process excites the electronic transition of the ion and creates or destroys, respectively, a single excitation of the mode (a *phonon*). In this way, the motional degrees of freedom of the ions can be entangled with their electronic degrees of freedom, thus acting as a “bus” for the transfer of quantum information. There exist

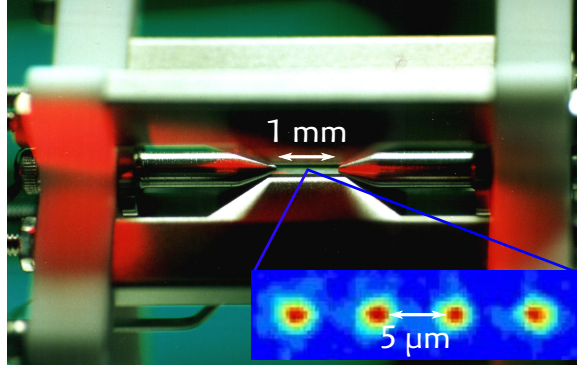


Figure 5: A string of four ions trapped in our linear Paul trap.

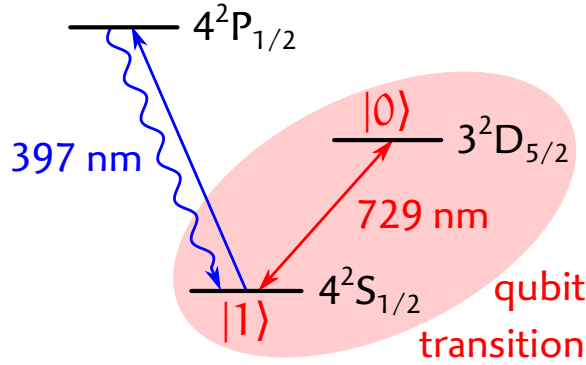


Figure 6: $^{40}\text{Ca}^+$ electronic level scheme.

several protocols that use the common motional modes to implement entangling gates between the ions. In Section 2.4 the scheme that is employed in this work, the so-called MS gate, is described.

Without going into further detail, let us see how trapped ions fulfill the DiVincenzo criteria and thus make a good candidate for a qubit:

1. *A scalable physical system with well characterized qubits.* Trapped ions are well characterized qubits since they are physically separate and thus can be independently addressed for manipulation and detection. Scalability means being able to increase the system size to an arbitrary number of qubits while still being able to apply a universal set of quantum operations on the whole system. This can be done using surface trap architectures and shuttling techniques [25], or separate traps and photonic interfaces [26]. The control resources needed, such as lasers or radio-frequency (RF) electronics, scale linearly with the number of qubits.
2. *The ability to initialize the state of the qubits to a simple fiducial state.* Standard techniques such as optical pumping and laser cooling allow one to bring the electronic and motional state of the ions to a well-defined ground state [5].

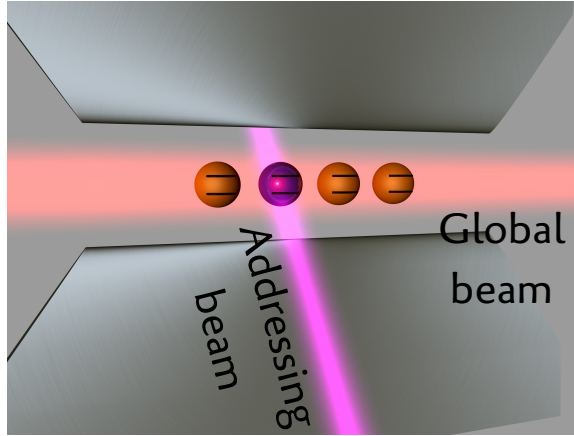


Figure 7: Beam configuration in our experimental setup.

3. *Long relevant decoherence times, much longer than the gate operation time.* Typical decoherence times of optical qubits are on the order of tens or hundreds of ms¹ and typical gate operations are performed on μ s timescales [18].
4. *A “universal” set of gates.* An arbitrary quantum operation can be implemented using single-qubit operations together with entangling gates such as the MS gate [30], which are available in trapped ion experiments (see Section 2.4).
5. *A qubit-specific measurement capability.* The electron shelving technique [31] allows one to detect the electronic state of an ion, providing a state-dependent fluorescence measurement.
6. *The ability to interconvert stationary and flying qubits and*
7. *The ability faithfully to transmit flying qubits between specified locations.* The electronic state of trapped ions can be mapped onto photons by means of optical cavities [32]. The photons can be transmitted over long distances through optical fibers. Alternatively, ions themselves can be turned into flying qubits by means of shuttling techniques [25], or can be interconnected with wires [33].

EXPERIMENTAL TOOLBOX

In this section, the set of quantum operations available in the experimental setup considered in this thesis is introduced:

- Collective single-qubit rotations applied to the whole qubit register are implemented by means of laser pulses resonant with

¹ Coherence times of over tens of seconds have been shown on magnetic field-insensitive transitions [27–29].

the qubit transition, coupled to the entire ion string. Such rotations can be made about any axis on the equator of the Bloch sphere, depending on the optical phase ϕ of the laser pulses. We denote these rotations $C(\theta, \phi)$, where θ is the rotation angle and ϕ is the phase, so that:

$$C(\theta, \phi) = e^{-i\theta(S_x \cos \phi + S_y \sin \phi)/2}, \quad (17)$$

where $S_{x,y} = \sigma_1^{x,y} + \dots + \sigma_N^{x,y}$ are the global spin projections on the x or y axes, and $\sigma_j^{x,y,z}$ are the respective Pauli operators corresponding to qubit j . For the sake of brevity we also define rotations around the X and Y axes as:

$$X(\theta) = C(\theta, 0), \quad (18)$$

$$Y(\theta) = C(\theta, \pi/2). \quad (19)$$

- Single qubit rotations around the Z axis can be implemented by means of tightly-focused off-resonant laser pulses addressed on individual qubits. This induces an AC-Stark shift, which detunes the qubit and thus induces a phase that is proportional to the pulse duration. These are denoted by $Z_n(\theta)$, where θ is the rotation angle, and n is the qubit index:

$$Z_n(\theta) = e^{-i\theta\sigma_n^z/2}, \quad (20)$$

with σ_n^z being the Pauli Z operator applied to the n -th ion.

- Entangling Mølmer-Sørensen (MS) gates [30] are carried out by means of bichromatic laser pulses coupled to the entire ion string, detuned with respect to the red and blue motional sidebands. These gates are denoted by $MS_\phi(\theta)$, where θ is the rotation angle and ϕ is the phase of the gate, resulting in:

$$MS_\phi(\theta) = e^{-i\theta(S_x \cos \phi + S_y \sin \phi)^2/4}, \quad (21)$$

where $S_{x,y} = \sigma_1^{x,y} + \dots + \sigma_N^{x,y}$ are the total spin projections on the x or y axes, as before. For $\phi = 0$ or $\phi = \pi/2$ we obtain gates that act around the X or Y axes respectively, which we will denote:

$$MS_{x,y}(\theta) = e^{-i\theta S_{x,y}^2/4}. \quad (22)$$

The addressed Z rotations, together with the collective rotations, allow us to implement arbitrary local unitaries, as is shown in Section 5.1. These operations, together with a suitable entangling gate like the MS gate, form a universal set of gates [34]. A similar toolbox of operations is available for other atomic, molecular and opti-

cal physics (AMO) architectures, like trapped-ion hyperfine qubits or neutral Rydberg atoms [35–38].

Let us note that our MS gates couple to the entire qubit register. This can be an advantage, as they allow one to implement non-local interactions directly, but can also be a drawback if some of the qubits have to be left unaffected by the interaction. One way to achieve this is by spectroscopically decoupling certain qubits from the interaction, as illustrated in Figure 8. Our usual qubit is encoded in the states $S_{1/2}(m = -1/2)$ and $D_{5/2}(m = -1/2)$. To decouple it, the population in the $S_{1/2}(m = -1/2)$ state is transferred to the $D_{5/2}(m = -5/2)$ state, and the population in the $D_{5/2}(m = -1/2)$ state is first transferred to $S_{1/2}(m = +1/2)$ and then to $D_{5/2}(m = -3/2)$, by means of laser pulses resonant with the respective transitions. This technique is used in the experiments described in Chapters 8 and 9.

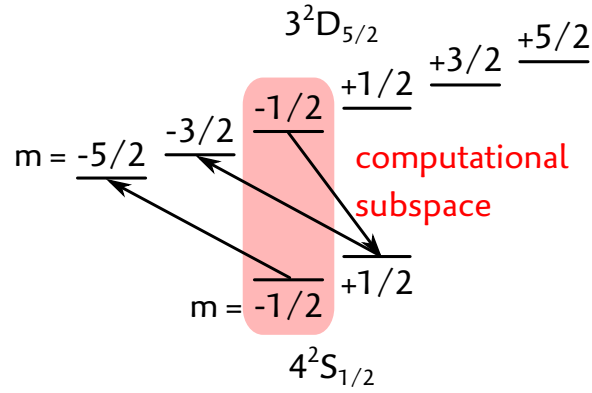


Figure 8: Electronic level manifold of $^{40}\text{Ca}^+$ with Zeeman splitting. The qubit is encoded in the $m = -1/2$ to $m = -1/2$ transition, and MS interactions are resonant with this transition. To decouple the qubit from the interactions, its population is coherently transferred to the $m = -5/2$ and $m = -3/2$ levels of the $3^2D_{5/2}$ manifold.

DIGITAL QUANTUM SIMULATION

In the previous section we described an implementation of a universal quantum computer. Richard Feynman posed the question in 1982: “Can physics be simulated with a universal computer?” [10]. The answer is negative if we restrict ourselves to classical computers, since the memory required merely to store a quantum state grows exponentially with the size of the system. Moreover, directly reproducing the measured probabilities of a quantum-mechanical system on a local classical device is impossible (the *hidden-variable problem*) [10]. However, a universal *quantum* computer can indeed be used to simulate any local quantum system, as Seth Lloyd answered affirmatively in Ref. [12]. This possibility is appealing, since a quantum simulator with tens of qubits and hundreds of operations, which seems feasible in the near future, could outperform any classical computer [12].

The problem of quantum simulation is, given a physical system of interest with local interactions, to map it to another physical system that we can control and measure: a *quantum simulator*. The dynamics of the simulator must approximate the time evolution of the system of interest with arbitrarily small error. Suppose the system of interest evolves during a time t under a Hamiltonian

$$H = \sum_{i=1}^l H_i. \quad (23)$$

Since the interactions are local, each of the terms H_i acts on a Hilbert space of dimension d at most, where d is independent of the size of the system. In general, the H_i do not commute with each other, and cannot be implemented simultaneously in the laboratory. To solve this issue, we slice the evolution into n time windows $\Delta t = t/n$, and in each time window we evolve the simulator under each H_i successively, as depicted in Figure 9. This technique is known as the Trotter-Suzuki decomposition [39, 40], and is based on the fact that:

$$e^{i(H_1 + \dots + H_l)t} \approx (e^{iH_1\Delta t} \dots e^{iH_l\Delta t})^n. \quad (24)$$

More exactly, the error terms are given by:

$$e^{iHt} = (e^{iH_1\Delta t} \dots e^{iH_l\Delta t})^n + \sum_{i>j} [H_i, H_j] \frac{t^2}{2n} + \sum_{k=3}^{\infty} E(k), \quad (25)$$

where the higher order error terms $E(k)$ are bounded by:

$$\|E(k)\|_{\text{sup}} \leq n \frac{\|H\Delta t\|_{\text{sup}}^k}{k!}, \quad (26)$$

where $\|A\|_{\text{sup}}$ is the maximum expectation value (*supremum*) of the operator A over the states of interest. The total error in this approximation is less than $\|n(e^{iHt/n} - 1 - iHt/n)\|_{\text{sup}}$, and can be made arbitrarily small by making n large enough.

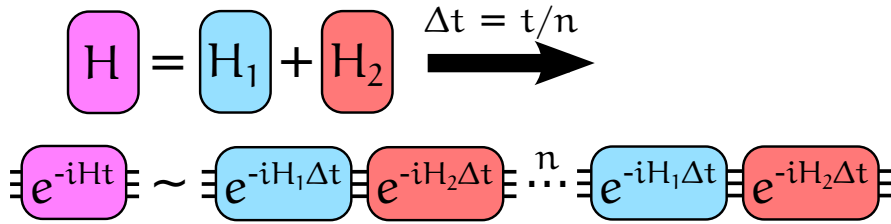


Figure 9: Stroboscopic implementation of a time evolution.

It remains to implement each of the local Hamiltonians H_i on our simulator, which in general requires less than d^2 operations [12]. Each local operator is implemented n times, so the total number of operations required is less than nld^2 . The number of local components l

“By going forward and backing up a sufficiently small distance a large enough number of times, it is possible to parallel park in a space only ϵ longer than the length of the car.” Seth Lloyd, [12].

depends on the physical system to be simulated, but for typical local interactions (e.g. nearest or next-nearest neighbor) it is proportional to the system size. In such cases, the number of operations required scales linearly with the system size, so this scheme provides a feasible way of simulating the system dynamics. The scheme described here is the basis of the experiments described in Chapters 8 and 9.

SHOR'S ALGORITHM

Dass das Problem, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen zu den wichtigsten und nützlichsten der ganzen Arithmetik gehört und den Fleiss und die Weisheit der Geometer der Antike und der Neuzeit beschäftigt hat, ist so bekannt, dass es überflüssig ist, viel darüber zu sagen.

—C. F. Gauss, *Disquisitiones Arithmeticae* [41]

Shor's algorithm, formulated in 1994 by Peter Shor [7, 42], is a quantum algorithm to solve the *integer factorization problem*: given an integer N , what are its prime factors? It is a paradigmatic example of the power of quantum computing because it solves a problem with practical applications and yet outperforms every known classical algorithm. Beyond the pure mathematical interest in factoring large numbers, this problem is relevant since the security of widely used cryptographic schemes such as the Rivest-Shamir-Adleman (RSA) scheme [43] relies on the assumption that it is exponentially difficult to factor big numbers. Shor's algorithm runs in polynomial time in the size of the input, so a large-scale implementation would render such cryptographic schemes insecure.

At the heart of this algorithm lies the capability of quantum computers to evaluate a function on all possible inputs at the same time. However, much of the difficulty in designing quantum algorithms lies in retrieving useful results from the vast space of quantum states that are populated. In this chapter the quantum algorithms that constitute the building blocks of Shor's algorithm are explored. In Section 3.1 a basic quantum algorithm is described, the quantum Fourier transform (QFT), that allows to find periodicities in data encoded in a quantum state. The QFT is a building block for the quantum order-finding algorithm, which is introduced in Section 3.2. Finally, in Section 3.3 it is shown how the integer factorization problem can be reduced to the order-finding problem, applied to the concrete example of factoring the number $N = 15$ and outlining the implementation shown in Chapter 7.

THE QUANTUM FOURIER TRANSFORM

In classical computing, the discrete Fourier transform (DFT) is an algorithm useful for finding periodicities in discrete data. Given a

vector of complex numbers $\{x_0, x_1, \dots, x_{N-1}\}$, their DFT is another vector of complex numbers $\{y_0, y_1, \dots, y_{N-1}\}$ given by:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j. \quad (27)$$

Let us now consider a system of N qubits, which we will call a *register*. Any integer $0 \leq j \leq 2^N - 1$ can be encoded as a quantum state of this system if we write j as a binary string:

$$j = b_{N-1} \dots b_0, \quad (b_j = \{0, 1\}), \quad (28)$$

since then we can associate j with the quantum state:

$$|j\rangle = |b_{N-1} \dots b_0\rangle, \quad (29)$$

where $|b_i\rangle = \{|0\rangle, |1\rangle\}$ is the state of the i -th qubit.

We can likewise encode a vector of complex numbers $\{x_j\}$, normalized such that $\sum_j |x_j|^2 = 1$, in the quantum state $\sum_{j=0}^{2^N-1} x_j |j\rangle$. The quantum Fourier transform (QFT) of such a state is defined as [6]:

$$\text{QFT} \left(\sum_{j=0}^{2^N-1} x_j |j\rangle \right) = \sum_{k=0}^{2^N-1} y_k |k\rangle, \quad (30)$$

where the vector $\{y_j\}$ is the DFT of the vector $\{x_j\}$. Equivalently, the action of the QFT on the basis states $|j\rangle$ is:

$$\text{QFT} |j\rangle = \frac{1}{\sqrt{2^N}} \sum_{k=0}^{2^N-1} e^{2\pi i j k / 2^N} |k\rangle. \quad (31)$$

The QFT is a unitary operation, and thus can be implemented on a quantum computer, as well as its inverse operation:

$$\text{QFT}^\dagger |j\rangle = \frac{1}{\sqrt{2^N}} \sum_{k=0}^{2^N-1} e^{-2\pi i j k / 2^N} |k\rangle. \quad (32)$$

As in the classical case, the QFT is useful for finding periodicities of an input. Suppose we consider an input state:

$$|\psi\rangle = \frac{1}{\sqrt{m}} (|j_0\rangle + |j_0 + r\rangle + |j_0 + 2r\rangle + \dots), \quad (33)$$

where m is a normalization factor. The state $|\psi\rangle$ has a periodicity of r , or frequency of N/r . The output state $\text{QFT} |\psi\rangle$ is a linear combination of the basis states $|k\rangle$, where the $|k\rangle$ with the greatest weight are those such that k is close to a multiple of N/r . Therefore, to find r we can measure $\text{QFT} |\psi\rangle$, and we will obtain with high probability

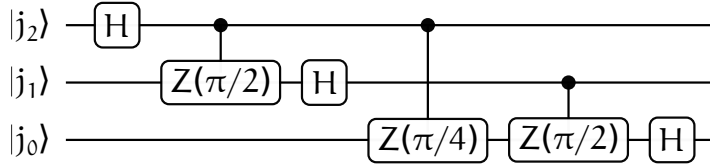


Figure 10: Implementation of the inverse quantum Fourier transform ($\text{QFT}^\dagger$) on 3 qubits.

the outcome corresponding to state $|k\rangle$, corresponding to the fraction mN/r . From this fraction we can estimate the period r of the input. The precise procedure for finding the denominator r of this fraction makes use of the *continued fraction algorithm*, see [6, Theorem 5.1].

An quantum algorithm for the inverse QFT on 3 qubits is shown in Figure 10. Such a quantum circuit for implementing the QFT (or the inverse QFT) in the general n -qubit case requires $\sim n^2$ gates [6]. Hence, it offers an exponential speedup over the best classical algorithms, which require $\sim n2^n$ gates. However, the output values of the quantum version cannot be directly accessed.

Quantum hardware is scarce, so available qubits ought to be used as efficiently as possible. A. Kitaev has proposed [44] a variation of the QFT that manages to reduce the size of the register to a single qubit if only the classical information in the output is required. Suppose we perform a QFT and measure the outcome immediately afterwards (Figure 11a). In this case, the measurements can actually be performed before the conditional operations (Figure 11b), and these can be replaced by classical feed-forward (Figure 11c).

ORDER-FINDING

Let us begin by recalling the definition of the *modulo* operation. This is written as $a \bmod N$, and is the remainder of dividing a by N . The *order-finding* problem is the following: given integers a and N , what is the least integer $r > 0$ such that $a^r \bmod N = 1$? The integer r is called the *order* of $a \bmod N$. The order-finding problem can also be expressed as finding the periodicity of the function $f(s) = a^s \bmod N$. For instance, if we take $N = 15$ and $a = 7$ then:

$$\begin{aligned}
 a^0 \bmod N &= 1, \\
 a^1 \bmod N &= 7, \\
 a^2 \bmod N &= 4, \\
 a^3 \bmod N &= 13, \\
 a^4 \bmod N &= 1, \dots
 \end{aligned} \tag{34}$$

so the order of $7 \bmod 15$ is 4.

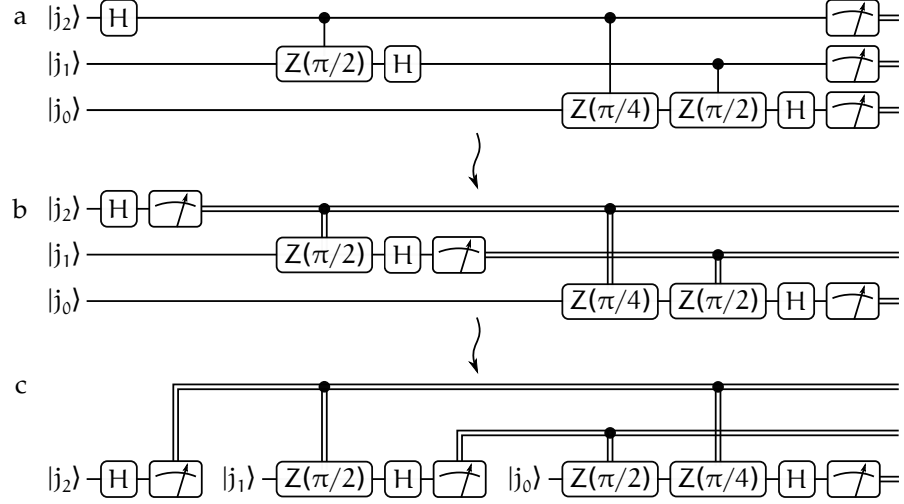


Figure 11: Successive optimizations of the QFT [44]. a) Full inverse QFT followed by a measurement. b) Since only the classical information is preserved, the measurements can be made before the controlled operations and these can be replaced by classical feed-forward. c) The outcome of each measurement is stored classically, so the same qubit can be reused by resetting it after each measurement and preparing it in the correct input state.

There is no known classical algorithm that solves the order-finding problem in polynomial time. However, since it involves finding the periodicity of a function, it seems plausible that the QFT may be of help. If we consider the unitary

$$U|y\rangle = \begin{cases} |ay \bmod N\rangle & \text{if } y < N \\ |y\rangle & \text{if } y \geq N, \end{cases} \quad (35)$$

and we apply it repeatedly to the state $|1\rangle$, we obtain:

$$U^j|1\rangle = |a^j \bmod N\rangle, \quad (36)$$

which is the desired function. Therefore, the problem can also be expressed as finding the least integer r such that $U^r = 1$; it has been shown that it can be solved using the QFT [6]. The outcome r is known as the *order* or *period* of the unitary U [6].

In order to find the order of U we use two registers, each containing multiple qubits, as illustrated in Figure 12. The first register is initialized to the state $|0\rangle = |00\dots 0\rangle$, and its size t determines the success probability of the algorithm, as we shall see. The second register is initialized to the state $|1\rangle = |00\dots 01\rangle$, and it must be big enough to hold the number N , so it must consist of at least $L \geq \log_2 N$ qubits. Applying Hadamard gates on every qubit in the first register creates a superposition of all possible input states $|j\rangle$. We then apply the unitary U on the second register j times, conditionally on the state $|j\rangle$ of

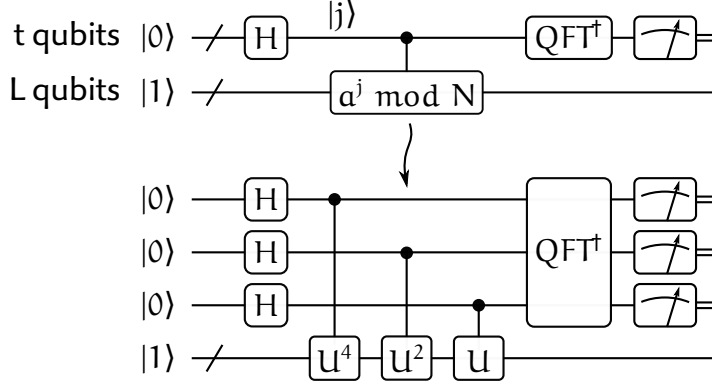


Figure 12: The order-finding algorithm, exemplified for a QFT qubit register of size $t = 3$. U is the modular multiplication unitary defined in Eq. (35).

the first register. The result is a superposition of every possible value of $|a^j \bmod N\rangle$ on the second register, which is at this point entangled with the first register. This means that, for any particular value of the second register, the state of the first register is a superposition of basis states $|j\rangle$ spaced with periodicity r . Therefore, as we have already seen in Section 3.1, by applying the inverse QFT on the first register we can find the value of r .¹ This procedure is summarized in Algorithm 1.

Algorithm 1 Quantum order-finding [6]

Input: an eigenstate $|u\rangle$ of U with eigenvalue $e^{2\pi i \phi_u}$.

Output: an n -bit approximation $\tilde{\phi}_u$ to ϕ_u .

- 1: Prepare the initial state $|0\rangle|1\rangle$.
 - 2: Create the superposition $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ on the first register.
 - 3: Apply U to the computation register to obtain the state $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|a^j \bmod N\rangle$.
 - 4: Apply the inverse QFT to the first register to obtain $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{s}/r\rangle|u_s\rangle$, where $\tilde{s}/r$ is an approximation to s/r .
 - 5: Measure the first register to obtain $\tilde{s}/r$.
 - 6: Apply the continued fractions algorithm to obtain the order r .
-

As a concrete example of the order-finding algorithm, let us calculate the order of $a = 7 \bmod 15$, using a first register with $t = 3$ qubits. After preparing the initial state $|\psi_1\rangle = |0\rangle|1\rangle$ and applying Hadamard gates on the first register, the state is the following:

$$|\psi_2\rangle = \frac{1}{\sqrt{8}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)|1\rangle, \quad (37)$$

¹ If $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$, the result of the QFT will be accurate to $2L + 1$ bits with probability at least $(1 - \epsilon)/r$. [6]

that is, we have a superposition of every possible input state on the first register. Next, we apply the unitary U^j to the second register, conditioned on the state $|j\rangle$ of the first register, and obtain:

$$|\psi_3\rangle = \frac{1}{\sqrt{8}}(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + |7\rangle|13\rangle), \quad (38)$$

which contains every possible result of the modular multiplication. If we measured the second register, we would project the first register to a superposition of states with a periodicity of r , independently of the outcome of the second register. Suppose this outcome was $|7\rangle$, then the first register would be projected to $\frac{1}{\sqrt{2}}(|1\rangle + |5\rangle)$. To find the periodicity in the state after measurement, we apply the inverse QFT on the first register and get the state:

$$|\psi_4\rangle = (|0\rangle - i|2\rangle - |4\rangle + i|6\rangle). \quad (39)$$

Finally, we perform a measurement on the first register. We can obtain as a result either 0, 2, 4 or 6, with probability $1/4$ each, and all of these are multiples of $2^t/r = 8/r = 2$. If we measure 2 or 6 we can calculate the right period $r = 4$ immediately. Otherwise, we can repeat the algorithm to obtain the correct order, since we can check efficiently whether the obtained value of r is indeed the order of $a \bmod N$ or not.

Note that the order-finding algorithm as we have presented it can be optimized with respect to the register size. Since the QFT at the end is followed by a measurement, its fully coherent version is not necessary and can be replaced by Kitaev's QFT, as shown in Figure 13. Using this approach, we can reduce the size of the first register to a single qubit.

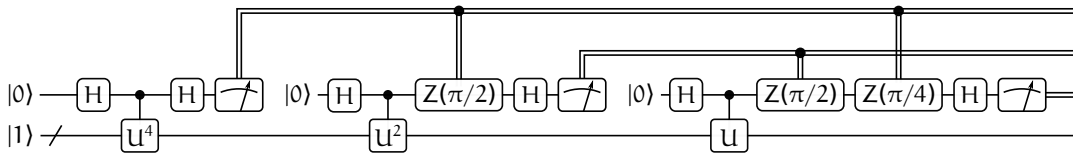


Figure 13: The optimized order-finding algorithm integrated with Kitaev's QFT. U is the modular multiplication unitary defined in Eq. (35).

SHOR'S ALGORITHM

We reduce now the integer factorization problem to the order-finding problem. The starting point of this reduction is the following observation: if x is a solution of

$$x^2 \bmod N = 1, \quad (40)$$

where $x \bmod N \neq \pm 1$, then we have that

$$x^2 - 1 \bmod N = (y + 1)(y - 1) \bmod N = 0. \quad (41)$$

Therefore N divides $(x + 1)(x - 1)$, so the prime factors of N must be contained among the prime factors of $x + 1$ and $x - 1$. In other words, N must have at least a common prime factor with one of these numbers. We can find these common factors by calculating $\gcd(N, x + 1)$ and $\gcd(N, x - 1)$ using Euclid's algorithm.

The rest of the problem is finding such an integer x . Let us choose a random integer $a < N$ *coprime* with N , that is, without any common prime factors with N . Then, let us find the order r of $a \bmod N$, which we can do using the quantum order-finding algorithm. As shown in [6, Theorem A4.13], if N has m distinct prime factors, with probability $p > 1 - 2^{-m}$ it is the case that r is even and:

$$a^{r/2} \bmod N \neq N - 1. \quad (42)$$

If this happens, then $x = a^{r/2}$ is an integer that satisfies Eq. (40) and we can find a prime factor of N . If our choice of a does not succeed, then we choose another a randomly and continue until we obtain a prime factor. This algorithm is summarized in Algorithm 2.

Algorithm 2 Shor's algorithm [6]

Input: an integer N

Output: a prime factor of N

```

1: if  $N$  is even then return 2
2: if  $N = b^c$  for integers  $b \geq 1$  and  $c \geq 2$  then return  $b$ 
3: loop
4:    $a \leftarrow$  random integer in the range from 1 to  $N - 1$ 
5:   if  $\gcd(a, N) > 1$  then return  $\gcd(a, N)$ 
6:    $r \leftarrow$  order of  $a \bmod N$  ▷ the quantum step!
7:   if  $r$  is even and  $a^{r/2} \bmod N \neq N - 1$  then
8:     if  $\gcd(a^{r/2} - 1, N) \neq -1$  then return  $\gcd(a^{r/2} - 1, N)$ 
9:     else if  $\gcd(a^{r/2} + 1, N) \neq -1$  then return  $\gcd(a^{r/2} + 1, N)$ 

```

The time required by Shor's algorithm to factor an n -bit number scales as [45]:

$$O(n^2 \log n \log \log n), \quad (43)$$

whereas the fastest classical algorithm published to date, the *general number field sieve*, has a complexity of [46]:

$$O\left(\exp\left((64/9)^{1/3} n^{1/3} (\log n)^{2/3}\right)\right). \quad (44)$$

Therefore, Shor's algorithm offers an exponential improvement over the best classical algorithm known. Where does this speedup come

from? Shor's algorithm would also have exponential complexity if carried out on a classical computer, since there is no known efficient classical algorithm for the order-finding step. However, we have already seen in Section 3.2 that this problem can be solved efficiently on a quantum computer. The rest of the algorithm consists of pre- and post-processing computation steps that can be carried out classically in an efficient way.

As an example of Shor's algorithm, let us see how to factor $N = 15$. Steps 1 and 2 check that $N = 15$ is neither an even number nor a power of a prime number. For step 4, let us "randomly" choose $a = 7$. In step 5 we calculate $\gcd(7, 15) = 1$, which is *not* a non-trivial factor of 15. Therefore, the algorithm proceeds to the quantum order-finding step, which we have already shown in Section 3.2 and yields the value $r = 4$. This number is even, and $a^{r/2} \bmod N = 4 \neq 1$, so we know that the algorithm will succeed. We compute $\gcd(a^{r/2} + 1, N) = 5$ and $\gcd(a^{r/2} - 1, N) = 3$, so the algorithm succeeds. If the algorithm had failed, we would have had to go back to line 4 and try again with a different a .

You boil it in sawdust: you salt it in glue:
 You condense it with locusts and tape:
 Still keeping one principal object in view –
 To preserve its symmetrical shape.

—Lewis Carroll, *The Hunting of the Snark* [47]

Our most fundamental and complete understanding of nature, gravity aside, is given by the *Standard Model* of particle physics [48]. This framework classifies all the subatomic particles known, and describes their interactions via *gauge theories*, thus called because they obey certain physical symmetries (*gauge symmetries*). Some examples of these gauge theories are the electroweak theory, which combines electromagnetism and the weak interaction, and quantum chromodynamics (QCD), which describes quarks, the fundamental constituents of hadrons, and their interactions via the strong force.

The Standard Model has had tremendous success in explaining experimental observations in high-energy physics and predicting the existence of new particles like the W and Z bosons and the charm, bottom and top quarks. However, there are still phenomena – particularly in quantum chromodynamics (QCD) – that are not well understood due to the inability to solve the equations of motion, either analytically or numerically. Since the coupling of quarks to the strong interaction is – not surprisingly – strong, the perturbative approaches that are so successful in the case of quantum electrodynamics cannot be applied. This has led to the development of non-perturbative approaches, for example *lattice gauge theories* (LGTs), where space-time is discretized to a lattice. This approach is more amenable to numerical calculations and has proven useful to determine hadron masses [49] and properties of quark-gluon plasmas [50]. However, it is still extremely computationally expensive because of exponentially growing memory requirements, which make simulating the real-time dynamics of QCD systems unfeasible.

For this reason, quantum simulation is a promising approach for studying LGTs. For this, these theories can be reduced to spin models, which in turn can be efficiently simulated on a quantum computer [12]. State-of-the-art quantum computers do not yet allow us to carry out full-fledged calculations of QCD. However, theories such as quantum electrodynamics (QED) in $1 + 1$ dimensions (one spatial dimension plus time) are simpler to study and also feature some phenomena characteristic of QCD. Therefore, we perform a quantum simulation of this theory as a testbed for tackling more challenging ones.

In Section 4.1 QED in $1 + 1$ dimensions is introduced, also known as the *Schwinger model* [13]. Then, in Section 4.2 we see how this model can be reduced to a discrete spatial lattice. Finally, in Section 4.3 we encode the fermionic and gauge fields as spins, thus showing that the Schwinger model is analogous to a spin model, which can be efficiently simulated on a quantum computer.

THE SCHWINGER MODEL

In this section we study QED in one spatial dimension, known as the *Schwinger model* [13], and explain some important phenomena that arise in this theory. Throughout this chapter we adopt natural units where $\hbar = c = 1$, as is usual in the literature.

The dynamics of spin-1/2 (fermionic) particles with mass m , e.g. electrons and positrons, are described by a relativistic generalization of the Schrödinger equation, the *Dirac equation* [51]. The Dirac equation is usually formulated in three spatial dimensions ($3 + 1$ dimensions), for evident reasons. Here we restrict our study to one spatial dimension, a theory studied by J. Schwinger in Ref. [13] in the massless case, and described by him as “physical, if unworldly”. Because of its conceptual simplicity, this theory is an ideal testbed for more complicated gauge theories. The Dirac equation for the wavefunction ψ of fermions in $1 + 1$ dimensions is:

$$(i\gamma^\mu \partial_\mu - m)\psi = 0. \quad (45)$$

The derivatives ∂_μ ($\mu = 0, 1$) are $(\partial/\partial t, -\partial/\partial x)$, and the γ^μ are 2×2 matrices that satisfy the following anticommutation relations:

$$\{\gamma^\mu, \gamma^\nu\} = 2g^{\mu\nu} \mathbb{1}_{2 \times 2}, \quad (46)$$

where $g^{\mu\nu}$ is the Minkowski metric in $1 + 1$ dimensions:

$$g^{\mu\nu} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (47)$$

A pair of suitable γ^μ matrices is:

$$\gamma^0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (48)$$

$$\gamma^1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (49)$$

“Doubtless we cannot see that other higher Spaceland now, because we have no eye in our stomachs.” – Edwin A. Abbott, *Flatland: A Romance of Many Dimensions* [52]

The solutions of this equation are two-component fields ψ :

$$\psi = \begin{pmatrix} \psi_- \\ \psi_+ \end{pmatrix}. \quad (50)$$

As in the $3 + 1$ -dimensional case, there exist positive and negative energy solutions, which represent particles and antiparticles, respectively. Solutions of the form $\psi = (\psi_- \ 0)$ have positive energy, whereas solutions of the form $\psi = (0 \ \psi_+)$ have negative energy. We shall occasionally call the particles “electrons” and the antiparticles “positrons”, by analogy to standard QED.

The $1 + 1$ version of QED displays some particular phenomena different from $3 + 1$ QED. As shown in Figure 14a, the electric field lines in three spatial dimensions diverge. Their density, which corresponds to the electric field strength, decays with the inverse square of the distance. Therefore, the electric potential, which is the integral of the field strength, decays linearly with the distance. On the other hand, in one spatial dimension the electric field lines do not diverge (Figure 14b), so the electric field strength does not decay with distance. Thus, the electric potential grows linearly with distance.

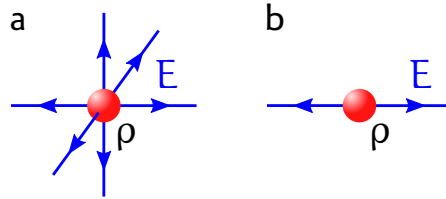


Figure 14: a) The electric field lines in three spatial dimensions diverge and their density, which corresponds to the electric field strength, decays as the inverse square of the distance. Therefore, the electric potential decays linearly with distance. b) In one spatial dimension, the electric field lines do not diverge and their density (the electric field strength) remains constant. Thus, the electric potential grows linearly with distance.

This particular distance dependence of the potential has important consequences for QED. Suppose that an electron-positron ($e^- e^+$) pair is created and gets separated, as depicted in Figure 15a-b. As the distance between the particles increases, the potential energy of the system grows. At some point it becomes energetically favorable for a new $e^- e^+$ pair to be created spontaneously from the vacuum (Figure 15c). Now there are two $e^- e^+$ pairs linked by electric flux strings, and no field in between. This mechanism is known as *string breaking*, since the flux string breaks and leads to the creation of new particle-antiparticle pairs. This leads to *confinement* of the individual particles, since they cannot be isolated. This phenomenon is also observed in QCD, since the strong force is asymptotically constant for large distances [53], thus confining quarks inside hadrons. For this reason, the

Schwinger model provides some insight into the dynamics of confinement in QCD, which cannot be studied analytically.

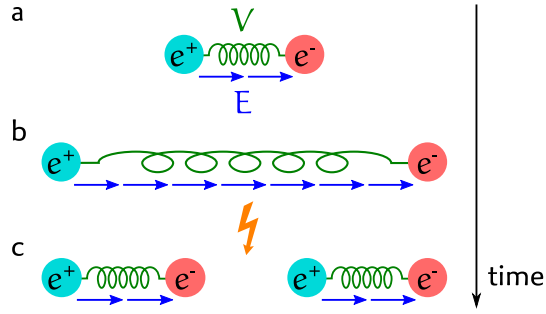


Figure 15: The *string breaking* (or *hadronization*) mechanism. a) An electron-positron pair are linked by an electric field flux string. b) If the particles get separated, the potential energy of the system increases. c) At some point it becomes energetically favorable for a new particle-antiparticle pair to be spontaneously created from the vacuum. Now there are two pairs linked by electric flux strings, and no field in between. In this way the flux string breaks and new “hadrons” (particle-antiparticle pairs) are created.

A related phenomenon predicted by QED is the spontaneous creation of particle-antiparticle pairs in the presence of a strong background electric field, known as the *Schwinger mechanism* [54]. This mechanism has been used as a model of string breaking in QCD [55, 56] and black hole physics [57]. The Schwinger mechanism has, up to now, never been tested experimentally. Its observation is currently pursued at high intensity laser facilities Extreme Light Infrastructure (ELI) and Exawatt Center for Extreme Light Studies (XCELS) [58]. There exist also numerous theoretical proposals [59–62] to study it in AMO systems. An implementation of the Schwinger mechanism in our trapped-ion setup is reported in Chapter 8.

The Schwinger model with massless fermions has been solved exactly by J. Schwinger in Ref. [13]. However, the massive Schwinger model, where fermions have a mass $m \neq 0$, has not been solved analytically. The dynamics of the system can be investigated numerically after discretizing the theory and restricting the dimension of its Hilbert space to finite dimension. These steps are the focus of the following sections.

LATTICE GAUGE THEORIES

In this section we show how to discretize the continuous Schwinger model to a lattice in space. The discussion here mainly follows Ref. [63]. We will only consider the Schwinger model, but this construction can be generalized to more spatial dimensions or non-Abelian gauge theories [14].

Dirac fermions on a lattice

We first formulate the Dirac equation on a spatial one-dimensional lattice, as illustrated in Figure 16. The intersite spacing will be denoted by a . A point in the lattice is denoted by an integer index n . The spaces between neighboring lattice points are known as *links*, and are indicated by a pair $(n, n + 1)$. A lattice site can be *even* or *odd* depending on its position n .

To encode the two-component fermion fields ψ on the lattice, we will encode their upper (particle) components ψ_- on the even sites, and their lower (antiparticle) components ψ_+ on the odd sites. As we will see, this allows us to retrieve the Dirac equation in the continuum limit of small lattice spacing a . Thus, on each lattice site we define a *one*-component fermion field $\phi(n)$, which satisfies the fermionic anticommutation relations:

$$\{\phi^\dagger(j), \phi(k)\} = \delta_{jk}, \quad (51)$$

$$\{\phi(j), \phi(k)\} = 0. \quad (52)$$

The two-component field ψ is built from the one-component fields ϕ as follows:

$$\psi(n) = \begin{cases} \begin{pmatrix} \phi(n) \\ \phi(n+1) \end{pmatrix} & \text{for even } n, \\ \begin{pmatrix} \phi(n+1) \\ \phi(n) \end{pmatrix} & \text{for odd } n. \end{cases} \quad (53)$$

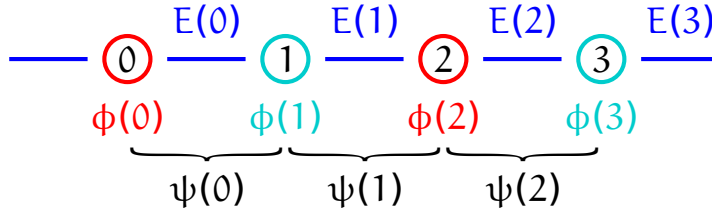


Figure 16: Definition of the lattice. A one-component fermion field $\phi(n)$ is placed on each lattice site. The fields $\phi(n)$ on even and odd sites correspond to particles and antiparticles, respectively. The two-component fermions $\psi(n)$ are built from two adjacent sites. The gauge fields $E(n)$ are placed in the links in between lattice sites.

We propose now a Hamiltonian that generates the Dirac equation (45) in the continuum limit, where the lattice spacing a goes to zero:

$$H = \frac{i}{2a} \sum_n \left[\phi^\dagger(n) \phi(n+1) - \phi^\dagger(n+1) \phi(n) \right] + m \sum_n (-1)^n \phi^\dagger(n) \phi(n). \quad (54)$$

The equation of motion for the one-component fields ϕ is therefore:

$$\dot{\phi}(n) = i[H, \phi(n)] = \frac{1}{2a} [\phi(n+1) - \phi(n-1)] - im(-1)^n \phi(n). \quad (55)$$

To obtain the equation of motion for the two-component fields ψ we join Eq. (55) for two neighboring even and odd sites:

$$\dot{\psi}(n) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} [\psi(n+1) - \psi(n-1)] - im \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \psi(n). \quad (56)$$

Multiplying Eq. (56) on the left by $i\gamma^0$ we obtain:

$$i\gamma^0 \dot{\psi}(n) - i\gamma^1 \frac{\psi(n+1) - \psi(n-1)}{2a} - m\psi(n) = 0, \quad (57)$$

which yields the Dirac equation (45) as $a \rightarrow 0$, where the finite difference $[\psi(n+1) - \psi(n-1)]/(2a)$ becomes the spatial derivative.

Coupling to gauge fields

We will now describe how fermions in $1+1$ dimensions couple to the electric field and interact through it, that is, QED in $1+1$ dimensions. In modern particle physics, interactions are described by means of *gauge theories*, which are theories that are invariant (symmetric) when certain transformations (*gauge transformations*) are applied to the fields. The gauge symmetry group of QED is $U(1)$, which means that the theory must be invariant if the fermion fields $\phi(n)$ are multiplied by arbitrary local phases $\alpha(n)$ [51], since these phases are not observable. Here we consider only the time-independent case, so the most general transformation on the fermion fields is:

$$\phi(n) \rightarrow e^{i\alpha(n)} \phi(n). \quad (58)$$

The kinetic energy terms $\phi^\dagger(n)\phi(n+1) - \phi^\dagger(n+1)\phi(n)$ in the Hamiltonian (54) are not invariant under such transformations, since the phases $\alpha(n)$ depend on n . We can achieve gauge invariance by coupling the fermion fields to additional fields, following Ref. [63]. Let us introduce on each link, between the sites n and $n+1$, a di-

dimensionless field operator $\theta(n)$, which is proportional to the spatial component of the electric vector potential A_μ :

$$\theta(n) = agA_1(n), \quad (59)$$

where a is the lattice spacing and g the strength of the coupling of the fermions to the electric field. We now replace the kinetic energy term in (54) by one that couples the fermions ϕ to the fields θ :

$$\begin{aligned} H_f = & \frac{i}{2a} \sum_n [\phi^\dagger(n) e^{i\theta(n)} \phi(n+1) - \text{H.c.}] + \\ & + m \sum_n (-1)^n \phi^\dagger(n) \phi(n). \end{aligned} \quad (60)$$

This Hamiltonian is invariant under gauge transformations of the form (58) if the link operators $\theta(n)$ transform as:

$$\theta(n) \rightarrow \theta(n) - [\alpha(n+1) - \alpha(n)] \quad (61)$$

In this way, the transformation law for the link operators absorbs the phases from the fermion fields.

On each link we will also define the electric field operators $E(n)$, that are canonically conjugate to the vector potential $A(n)$:

$$[A(j), E(k)] = \frac{i}{a} \delta_{jk}. \quad (62)$$

It will be more convenient to work with the fields $L(n)$, which are proportional to the electric field and dimensionless:

$$L(n) = \frac{1}{g} E(n), \quad (63)$$

The fields $L(n)$ are canonically conjugate to the $\theta(n)$:

$$[\theta(j), L(k)] = i\delta_{jk}. \quad (64)$$

Applying (64) it can be shown [63] that the Hilbert space of the gauge fields $L(n)$ is spanned by their discrete eigenstates $|l\rangle$:

$$L(n) |l\rangle = l |l\rangle \quad (l = 0, \pm 1, \pm 2, \dots), \quad (65)$$

and each of these corresponds to an electric field strength gl . The operators $e^{\pm i\theta(n)}$ act as raising/lowering operators for the electric field:

$$e^{\pm i\theta(n)} |l\rangle = |l \pm 1\rangle. \quad (66)$$

The energy of the gauge fields is the quantized version of the classical electric field energy:

$$H_g = \frac{a}{2} \sum_n E^2(n) \quad (67)$$

$$= \frac{ag^2}{2} \sum_n L^2(n). \quad (68)$$

Therefore, the full Hamiltonian for this lattice gauge theory, the *Kogut-Susskind Hamiltonian*, is the sum of H_f in Eq. (60) and H_g in Eq. (68):

$$\begin{aligned} H = & \frac{i}{2a} \sum_n [\phi^\dagger(n) e^{i\theta(n)} \phi(n+1) - \text{H.c.}] + \\ & + m \sum_n (-1)^n \phi^\dagger(n) \phi(n) + \frac{ag^2}{2} \sum_n L^2(n). \end{aligned} \quad (69)$$

SPIN MODELS

In the previous section we have seen how to encode QED in $1+1$ dimensions on a one-dimensional spatial lattice, and the Hamiltonian that generates the dynamics of this discrete version of the system. However, it is still not clear how to reduce this model to an experimental implementation. We show first how to map the lattice of fermionic fields to a chain of spins (Section 4.3.1). Then, we show two alternative ways to deal with the infinite-dimensional Hilbert space of the gauge fields: either realizing them as spin systems (Section 4.3.2), or encoding these into long-range interactions (Section 4.3.3).

Mapping fermions to spins

Fermionic systems can be mapped onto spin systems using the so-called *Jordan-Wigner transformation* [64], which preserves the fermionic anticommutation relations (51). Following Ref. [63], let us encode a spin $1/2$ on each lattice site, whose possible states are $|\uparrow\rangle$ and $|\downarrow\rangle$. Let $\sigma^i(n)$ ($i = x, y, z$) be the Pauli matrices at each site, and $\sigma^\pm(n) = [\sigma^x(n) \pm i\sigma^y(n)]/2$ the usual raising and lowering operators. Then one can represent the fermionic field operators as:

$$\phi(n) = \left(\prod_{l < n} i\sigma^z(l) \right) \sigma^-(n), \quad (70)$$

$$\phi^\dagger(n) = \left(\prod_{l < n} -i\sigma^z(l) \right) \sigma^+(n). \quad (71)$$

It can be verified that these operators satisfy the fermionic anticommutation relations (51). Here we adopt the convention that $\phi(n)$ cre-

ates a particle at site n if n is odd, or destroys an antiparticle at site n if n is even. Therefore, the spin states $|\uparrow\rangle$ and $|\downarrow\rangle$ represent particles $|e^-\rangle$, antiparticles $|e^+\rangle$ or the vacuum state $|0\rangle$ in the following way:

$$|\uparrow\rangle = \begin{cases} |0\rangle & n \text{ odd,} \\ |e^+\rangle & n \text{ even,} \end{cases} \quad (72)$$

$$|\downarrow\rangle = \begin{cases} |e^-\rangle & n \text{ odd,} \\ |0\rangle & n \text{ even.} \end{cases} \quad (73)$$

Rewriting the Kogut-Susskind Hamiltonian (69) in terms of the spin operators we obtain:

$$\begin{aligned} H = & \frac{1}{2a} \sum_n [\sigma^+(n) e^{i\theta(n)} \sigma^-(n+1) + \text{H.c.}] + \\ & + m \sum_n (-1)^n \left(\frac{1 + \sigma^z(n)}{2} \right) + \frac{g^2 a}{2} \sum_n L^2(n). \end{aligned} \quad (74)$$

In this way, the Schwinger model on a lattice is equivalent to a spin chain coupled to the gauge fields. Next, we need to consider how to encode the gauge fields.

Mapping gauge fields to spins

One way of tracking the evolution of the gauge fields is to encode them as spins, and to consider them together with the fermion fields. It can be seen from Eqs. (65) and (66) that the field operators $L(n)$ behave analogously to the z -component S^z of an angular momentum operator, and the operators $e^{\pm i\theta(n)}$ are analogous to the raising/lowering operators $S^\pm$ for angular momentum. Therefore, each field operator can be encoded as a spin system of arbitrary dimension. This is known as a *quantum link model* (QLM) [65]. The dimension of the spins chosen for the encoding restricts the maximum values of the electric field, and as it goes to infinity we recover the continuum limit. An experimental implementation of a quantum link model where the gauge fields are encoded in spin-1/2 systems is shown in Chapter 9.

Encoding gauge fields into long-range interactions

In the previous section we showed that the gauge fields can be mapped to spin systems. This approach requires additional quantum resources to encode the dynamics of the gauge fields. Moreover, we only recover the exact dynamics in the limit of infinite spin dimension, since otherwise the possible values of the electric field are restricted. For these reasons, it is desirable to look for a scheme where only the dynam-

ics of the fermion fields appear explicitly. This is possible because the gauge fields are completely determined by their boundary conditions (the background field) and the distribution of the fermions, that is, the charge distribution.

In one spatial dimension, the continuum version of Gauss' law is:

$$\frac{\partial E}{\partial x} = \rho(x), \quad (75)$$

where ρ is the charge density. Gauss' law is enough to determine the fields at every point if $\rho(x)$ and the boundary conditions for the field E are known. On the lattice, the spatial derivative must be transformed into a discrete difference of the link operators L_n :

$$\frac{\partial E}{\partial x} \rightarrow L_n - L_{n-1}. \quad (76)$$

The particle number on each site is $\phi_n^\dagger \phi_n$, and the charge of the particles has a staggered sign depending on whether the site is odd or even. Thus, the charge density on each site of the lattice is:

$$\rho(n) = \phi_n^\dagger \phi_n - \frac{1}{2} [1 - (-1)^n]. \quad (77)$$

Therefore, the discrete version of Gauss' law on the lattice is:

$$L_n - L_{n-1} = \phi_n^\dagger \phi_n - \frac{1}{2} [1 - (-1)^n], \quad (78)$$

This equation can be understood by considering a fixed field operator L_n and an adjacent spin ϕ_n to its right. Spins in state $|\uparrow\rangle$ ($|\downarrow\rangle$) on an odd (even) lattice site indicate that this lattice site is in the vacuum state, i.e. not occupied by a particle or antiparticle. Accordingly, $L_n = L_{n-1}$. Spins in the state $|\uparrow\rangle$ on even lattice sites (corresponding to positrons) generate (+1) unit of electric flux to the right, so $L_n = L_{n-1} + 1$. Similarly, spins in the state $|\downarrow\rangle$ on odd lattice sites (corresponding to electrons) lead to a decrease of one unit, and thus $L_n = L_{n-1} - 1$.

Following Ref. [66], we use this constraint to eliminate the operators L_n from the dynamics in a two-step procedure. First, the operators θ_n are eliminated by a gauge transformation,

$$\sigma_n^- \rightarrow \prod_{l < n} [e^{-i\theta_l}] \sigma_n^-. \quad (79)$$

In a second step, the electric field operators L_n are eliminated using the spin version of Gauss' law, which can be obtained by applying a Jordan-Wigner transformation (70,71) to Eq. (78):

$$L_n - L_{n-1} = \frac{1}{2} [\sigma_n^z + (-1)^n]. \quad (80)$$

The field operators L_n can be eliminated iteratively from left to right as depicted in Figure 17.

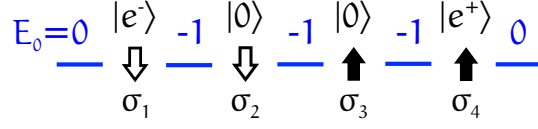


Figure 17: The electric field operators L_n are eliminated iteratively, using the spin version of Gauss' law given in Eq. (78). The elimination starts from the far left, where the value of the field is 0 in this case, and proceeds towards the right. Whenever an e^- is met, the field value decreases by one unit, and whenever a e^+ is met, the field value increases by one unit.

This procedure yields an effective spin Hamiltonian which involves only the fermionic degrees of freedom and a free parameter E_0 that corresponds to the boundary electric field on the link to the left of the first lattice site:

$$\begin{aligned} \hat{H}_S = & \frac{m}{2} \sum_{n=1}^N (-1)^n \sigma_n^z + w \sum_{n=1}^{N-1} [\sigma_n^+ \sigma_{n+1}^- + \text{H.c.}] \\ & + J \sum_{n=1}^{N-1} \left[E_0 + \frac{1}{2} \sum_{m=1}^n [\sigma_m^z + (-1)^m] \right]^2. \end{aligned} \quad (81)$$

The effect of the gauge fields transforms into a long-range $\sigma^z \sigma^z$ interaction that corresponds to the Coulomb interaction between the simulated charged particles. In this thesis only consider the case of zero background field is considered, where $E_0 = 0$. So far, this encoding approach has only been employed as a tool for analytical or numerical calculations [66–68]. In contrast, in Chapter 8 we investigate the use of this idea for a quantum simulation scheme, i.e. the realization of the Schwinger model in its encoded form in an actual physical system.

I had a running compiler and nobody would touch it... they carefully told me, computers could only do arithmetic; they could not do programs.

—Grace Hopper [69]

The contents of this chapter are extracted from Ref. [70].

As we have seen in the previous chapters, quantum technologies open new possibilities that are inaccessible with classical devices. To utilize the full computational power of quantum systems, one needs a *universal quantum computer*: a device able to implement arbitrary unitary operations, or at least to approximate them to arbitrary accuracy. However, in any specific physical system, only a certain set of operations is readily available. Therefore, it is necessary to decompose the desired unitary operation as a sequence of these experimentally available gates. An available set of gates is known as *universal* if it is possible to find such a decomposition for an arbitrary unitary quantum operation acting on the qubit register.

A canonical universal set of gates consists of two-qubit CNOT gates and arbitrary single qubit rotations. There exist deterministic algorithms that can provide near-optimal decompositions of unitaries in terms of these gates [6]. However, the set of gates that yields the highest fidelities depends on the particular experimental implementation. In particular, two-qubit CNOT gates may not be the most efficient to implement. Architectures like trapped ions [18, 36] or atom lattices [37] include in their toolboxes high-fidelity N-qubit gates that act on the entire qubit register (see Section 2.4). Implementing two-qubit gates in terms of these requires refocusing [71] or decoupling [18] techniques, and thus increases the overhead. Therefore it is desirable to find a direct decomposition of the target unitary into the available operations. In general, entangling operations are more prone to errors than single-qubit operations, so the number of entangling operations needs to be minimized.

Compiling unitaries using multi-qubit gates that act on the whole qubit register is more challenging than using two-qubit gates. Even if a sequence implements correctly a unitary for N qubits, it might not work for N + 1 qubits, since additional “spectator” qubits will also be affected by the sequence instead of being left unchanged [34]. Therefore, one has to define a qubit register of interest where the unitary will be compiled, and the experimental implementation of the resulting sequence has to be limited to this subregister, as explained

in Section 2.4. Moreover, the existing analytical methods for finding decompositions of unitaries in terms of two-qubit gates (see for instance Ref. [72]) do not seem to apply to multi-qubit gates. Therefore, an approach based on numerical optimization is used here.

A similar algorithm for finding multi-qubit gate decompositions has been studied in Ref. [34], where optimal control techniques are used to find a pulse sequence for a given target unitary operation. The procedure described there starts with long sequences and then removes pulses, if possible. This often results in sequences with more entangling operations than actually required. In this chapter an algorithm designed to produce decompositions with a minimal number of entangling gates is presented. In addition, a deterministic algorithm for finding decompositions of local unitaries is introduced. The algorithm is extended to operations required for state preparation or measurement, which are particular cases of more general operations known as *isometries* [73, 74].

This chapter is organized as follows: in Section 5.1 an analytic algorithm to compile local unitaries is shown, which can be used to find efficient implementations of state and process tomographies. Then, in Section 5.2 an algorithm to compile fully general unitaries which relies on numerical optimization is described and analyzed.

COMPILATION OF LOCAL UNITARIES

Local quantum unitaries are those that can be written as a product of single-qubit unitaries. In this section a fully deterministic algorithm is shown that produces decompositions of any local unitary as a sequence of collective equatorial rotations and addressed Z rotations, as described in Section 2.4. The decompositions presented here are optimal in the number of pulses. These techniques are particularly useful for the implementation of state and process tomographies, as exemplified in Figure 18, since both require only local operations at the beginning and end of the algorithm.

Let us consider a register of N qubits, and a local unitary $U = U_1 \otimes U_2 \otimes \cdots \otimes U_N$ to be applied to them, where U_i is the action of the unitary on the i -th qubit. If the same operation has to be applied to more than one qubit ($U_i = U_j$), we can replace both with a single instance of the operation, and then apply the same addressed rotations on all qubits subject to the same operation U_i . Therefore, we only have to consider the case where every U_i is unique.

In order to apply a general local unitary to each qubit we need to have at least three degrees of freedom per qubit [6], so the decomposition must have at least $3N$ free parameters. During the sequence at least $N - 1$ of the qubits must eventually be addressed, since a different unitary has to be applied to each qubit. Therefore, addressed operations of the form $Z_1(\theta_1), Z_2(\theta_2), \dots, Z_{N-1}(\theta_{N-1})$ must be included

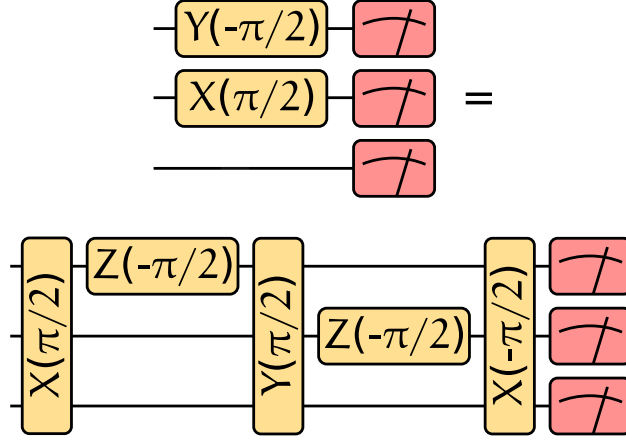


Figure 18: Pulse sequence to perform a projective measurement on the $\{X, Y, Z\}$ bases for qubits $\{1, 2, 3\}$, respectively.

in the decomposition. These provide $N - 1$ parameters, so $2N + 1$ more degrees of freedom are required. The most economic way to provide these is by means of collective gates $C(\theta_i, \phi_i)$, which have two degrees of freedom each, so the shortest sequence possible must add at least N global operations to the addressed gates, for a total of $3N - 1$ free parameters. One additional degree of freedom remains, so we must add a last gate. This can be either an addressed operation on qubit N or a collective gate. If we add an addressed gate Z_N , we obtain a sequence of the form:

$$U = Z_N C_N Z_{N-1} C_{N-1} \cdots Z_2 C_2 Z_1 C_1, \quad (82)$$

where $C_i = C(\theta_i, \phi_i)$ and $Z_i = Z_i(\theta_i)$ are collective and single-qubit rotations respectively, as explained in Section 2.4. Such a sequence is useful for compiling local unitaries up to arbitrary phases, as explained in Appendices A.1.3 and A.1.4. The second alternative is to add a collective rotation C'_N :

$$U = C'_N C_N Z_{N-1} C_{N-1} \cdots Z_2 C_2 Z_1 C_1, \quad (83)$$

which is the type of sequence we consider in this section.

For particular unitaries, some of the C_i and Z_i in Eq. (83) may actually be the identity, in which case the sequence is simpler. Since the decomposition depends on the ordering of the qubits, by reordering them a simpler sequence might be obtained. For small numbers of qubits, one can compile the unitary for every possible permutation, although this becomes inefficient for large numbers of qubits. However, let us remember that, for the purposes of the compilation, the qubits are grouped together according to which of them experience the same single-qubit unitary U_i . For an application such as state tomography, there are only three possible unitaries to be applied to each qubit in the register (shown in Figure 18), since one only wants

to perform a measurement in one of three different bases. Therefore, effectively we only need to consider three qubits, in which case trying out all the permutations is perfectly feasible.

We shall now see how to compile a generic local unitary $U = U_1 \otimes U_2 \otimes \cdots \otimes U_N$ exactly, using a decomposition of the form (83). Let us first note that the unitaries in Eq. (83) act on the N -qubit Hilbert space, which is the tensor product of the single-qubit Hilbert spaces. For the sake of simplifying the notation, we will now refer to these unitaries as $\tilde{C}_i$, $\tilde{Z}_i$, and will reuse the notations C_i and Z_i for their action on the single qubits, so that:

$$\begin{aligned}\tilde{C}_i &= C_i \otimes C_i \otimes \cdots \otimes C_i, \\ \tilde{Z}_i &= \mathbb{1} \otimes \mathbb{1} \otimes \cdots \otimes Z_i \otimes \cdots \otimes \mathbb{1},\end{aligned}\tag{84}$$

where $\mathbb{1}$ is the 2×2 identity matrix, and Z_i appears at the i -th place (since it only addresses the i -th qubit).

In terms of these single-qubit unitaries, factoring Eq. (83) for each qubit we obtain N equations:

$$\begin{aligned}U_1 &= C'_N C_N \cdots C_2 Z_1 C_1, \\ U_2 &= C'_N C_N \cdots Z_2 C_2 C_1, \\ &\vdots \\ U_N &= C'_N C_N \cdots C_2 C_1.\end{aligned}\tag{85}$$

From the last equation we can determine $C'_N C_N$:

$$C'_N C_N = U_N C_1^{-1} C_2^{-1} \cdots C_{N-1}^{-1},\tag{86}$$

and eliminating this factor from the remaining equations we obtain:

$$\begin{aligned}U_N^{-1} U_1 &= C_1^{-1} Z_1 C_1, \\ U_N^{-1} U_2 &= C_1^{-1} C_2^{-1} Z_2 C_2 C_1, \\ &\vdots \\ U_N^{-1} U_{N-1} &= C_1^{-1} C_2^{-1} \cdots C_{N-1}^{-1} Z_{N-1} C_{N-1} \cdots C_2 C_1.\end{aligned}\tag{87}$$

We solve each equation in (87) consecutively. To solve the first equation, let us notice that its left-hand side is a unitary operation that can be directly calculated from the target operation. This unitary, as any single-qubit unitary, can be written as:

$$U_N^{-1} U_1 = e^{-i\alpha_1 u_1/2},\tag{88}$$

where α_1 is the angle of the rotation and u_1 its generator. The right-hand side is simply a rotation around Z and a change of basis. There-

fore, the rotation angle of Z_1 must be equal to α_1 , and the change of basis must be such that:

$$u_1 = C_1^{-1} \sigma_z C_1. \quad (89)$$

It is shown in Appendix A.1.1 how to find the generator and angle of the collective rotation C_1 .

Having determined C_1 , we can write the second equation in (87) as:

$$C_1 U_N^{-1} U_2 C_1^{-1} = C_2^{-1} Z_2 C_2. \quad (90)$$

As before, the left-hand side of this equation is a known unitary, and the right-hand side consists of a rotation around Z and a change of basis, so the rotation angle θ_2 and generator of the change of basis C_2 can be found as for the previous equation. This procedure can be repeated until all of the C_k and Z_k with $k \leq N - 1$ are determined. The last collective operations C_N and C'_N can be determined from Equation (86). For this we need to decompose an arbitrary unitary into a product of two equatorial rotations; this can be done as explained in Appendix A.1.2.

We have seen so far how to compile a local unitary exactly. However, in certain cases the constraints on the target unitary are weaker, so that it can be implemented with a simpler sequence. For instance, a unitary that is followed by global gates whose phase can be freely adjusted must only be specified up to a collective Z rotation afterwards, since this rotation can be absorbed into the phase. This removes one free parameter from the sequence, thus simplifying its implementation. The mathematical details of this procedure are presented in Appendix A (Section A.1.3). Another case of interest is when the target unitary is specified up to arbitrary independent Z rotations afterwards, for instance when the unitary is followed by a projective measurement on the Z basis. This is particularly useful for tomographic measurements, since at the end only populations are measured, and the state is determined up to arbitrary local Z rotations. The procedure for finding these rotations is explained in Appendix A (Section A.1.4).

COMPILATION OF GENERAL UNITARIES

In Section 5.1 we studied how to compile local unitaries in terms of collective and addressed rotations. However, a universal quantum computer also requires entangling unitaries, which must be compiled into the experimentally available local and entangling gates. For example, in Figure 19 a decomposition of a Toffoli gate into a sequence of local and entangling gates applied consecutively is shown. In this

section, an algorithm is presented to find such decompositions for arbitrary unitaries.

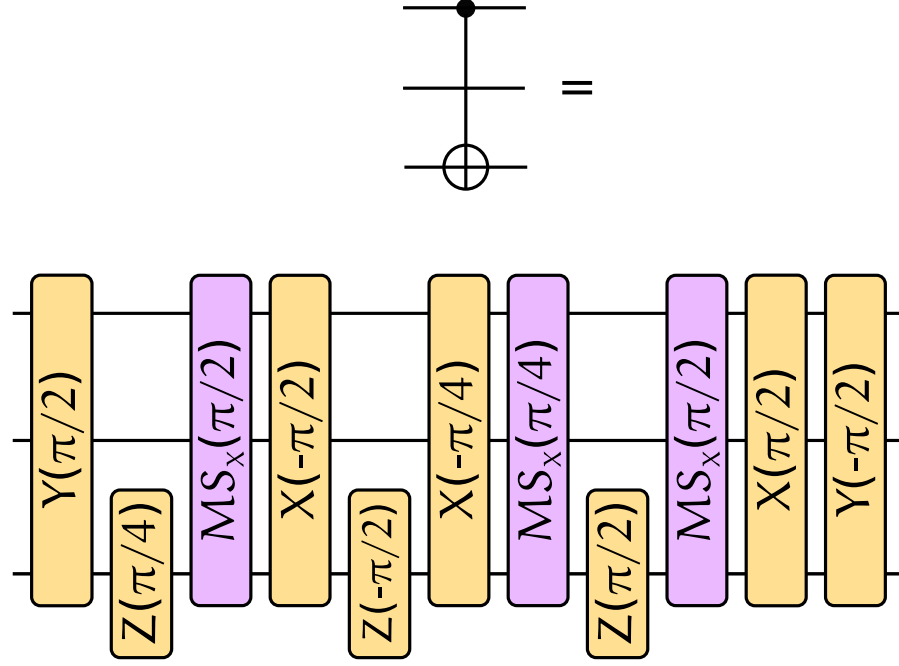


Figure 19: Decomposition of a Toffoli gate into a pulse sequence of collective equatorial rotations, addressed Z rotations and entangling Mølmer-Sørensen (MS) gates.

We seek decompositions directly in terms of multi-qubit entangling gates, since these are often more efficient than decompositions in terms of two-qubit gates. For example, a Toffoli gate can be implemented using only 3 Mølmer-Sørensen (MS) gates [34], while 6 CNOT gates are needed to implement it [75], and a Fredkin gate can be implemented using 4 MS gates [76], while the least number of two-qubit gates required is 5 [77]. As described in section 2.4, many equivalent types of entangling gates are experimentally available. We will consider MS gates, but the methods shown here are applicable to any entangling gate that forms a universal set together with local operations.

Compilation in layers

In many quantum information processing experiments the most costly operations in terms of fidelity are entangling gates. Therefore, when trying to compile a unitary we seek to minimize the number of those. A straightforward way to do this is to use pulse sequences where layers of local unitaries and entangling gates are applied consecutively, as shown in Figure 20.

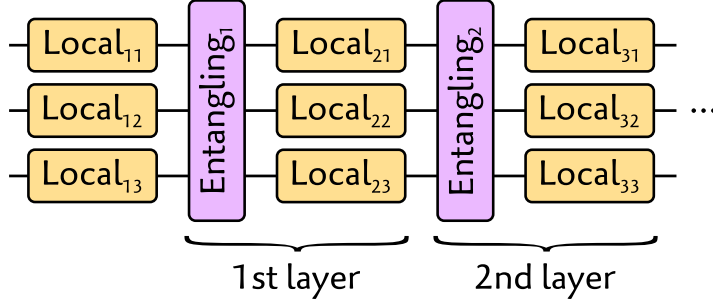


Figure 20: Sequence with layers of local and entangling gates applied consecutively.

Any unitary can be decomposed in terms of single-qubit gates and two-qubit CNOT gates [78]:

$$U = L_M \text{CNOT}_M L_{M-1} \cdots \text{CNOT}_1 L_0, \quad (91)$$

where L_i denotes an arbitrary local unitary on the whole qubit register and CNOT_i denotes a gate between some two qubits. A two-qubit CNOT gate can be implemented in an arbitrary N -qubit register as a sequence of local unitaries and $\text{MS}_x(\pi/8)$ gates [34]. Therefore, the following decomposition is always possible:

$$U = L_M \text{MS}_x(\pi/8) L_{M-1} \text{MS}_x(\pi/8) \cdots \text{MS}_x(\pi/8) L_0. \quad (92)$$

However, some of the local unitaries L_i in a decomposition of the form (92) may actually be identity, so after removing them the resulting sequence has the following structure:

$$U = L_M \text{MS}_x(\alpha_M) L_{M-1} \cdots \text{MS}_x(\alpha_1) L_0. \quad (93)$$

The decomposition consists of M entangling gates, and the MS rotation angles α_i are multiples of $\pi/8$. It is not necessary to consider angles $\alpha_i \geq \pi$ since $\text{MS}_x(\pi)$ is either the identity for an odd number of qubits, or a π rotation around X for an even number of qubits, which can be absorbed into a local operation.

We now seek to further simplify sequence (93). Every single-qubit unitary U_i on qubit i can be written as a composition of rotations around two different fixed axes [6], which means that we can always choose α_{i1} , α_{i2} and α_{i3} such that:

$$U_i = X_i(\alpha_{i3}) Z_i(\alpha_{i2}) X_i(\alpha_{i1}). \quad (94)$$

Any local unitary $L = \prod_{i=1}^N U_i$ can therefore be written as:

$$L = \prod_{i=1}^N X_i(\alpha_{i3}) Z_i(\alpha_{i2}) X_i(\alpha_{i1}), \quad (95)$$

where the product goes over the N qubits in the register. Since unitaries acting on different qubits commute, we can write this as:

$$L = \prod_{i=1}^N X_i(\alpha_{i3}) \prod_{i=1}^N Z_i(\alpha_{i2}) \prod_{i=1}^N X_i(\alpha_{i1}) \quad (96)$$

$$= \tilde{X}' \tilde{Z} \tilde{X}, \quad (97)$$

where $\tilde{X}$ and $\tilde{Z}$ denote arbitrary products of rotations around the X or Z axes for all qubits. Therefore, the sequence in (93) can be written as:

$$U = \tilde{X}'_M \tilde{Z}_M \tilde{X}_M \text{MS}_x(\alpha_M) \cdots \tilde{X}'_1 \tilde{Z}_1 \tilde{X}_1 \text{MS}_x(\alpha_1) \tilde{X}'_0 \tilde{Z}_0 \tilde{X}_0. \quad (98)$$

Commuting the X rotations with the MS gates we obtain a sequence of the form:

$$U = \tilde{X}'_M \tilde{Z}_M \tilde{X}_M \text{MS}_x(\alpha_M) \cdots \times \\ \times \tilde{X}'_2 \tilde{Z}_2 \tilde{X}_2 \text{MS}_x(\alpha_2) \tilde{Z}_1 \text{MS}_x(\alpha_1) \tilde{X}'_0 \tilde{Z}_0 \tilde{X}_0. \quad (99)$$

Every odd local unitary (except for the last one) is a product of Z rotations on all qubits, and the even local unitaries can be grouped as $L_i = \tilde{X}'_i \tilde{Z}_i \tilde{X}_i$. Moreover, a collective Z rotation can be extracted from each even local unitary L_i and absorbed into the phase of the subsequent MS gates and collective operations to simplify the implementation of L_i . Therefore the sequence can be written as:

$$U = L_M \text{MS}_{\phi_M}(\alpha_M) \cdots L_2 \text{MS}_{\phi_2}(\alpha_2) \tilde{Z}_1 \text{MS}_{\phi_1}(\alpha_1) L_0. \quad (100)$$

We have thus shown that any N -qubit unitary U can be decomposed into a sequence of the form shown in (100). These sequences always have the same structure, which makes it easier to identify patterns if one wants to compile families of unitaries, i.e. unitaries that depend on some tunable parameter.

Numerical optimization

We have seen a general form of a sequence of local operations and global entangling gates that implements any desired target unitary. It remains to find the actual sequence parameters, that is, the rotation angles and phases of the gates. However, it is not known, a priori, how many entangling gates will be needed for a given unitary. Therefore, the following algorithm can be applied:

1. Propose a sequence with $M = 0$ entangling gates.
2. Search numerically for the sequence parameters that maximize the fidelity with the target unitary.

3. If the sequence has converged to the desired unitary (i.e. the fidelity equals 1), stop. Otherwise increase M by 1 and go back to step 2.

When performing the numerical optimization in step 2, there might be a number of local optima in addition to the true global optimum, making fully deterministic optimization methods difficult to apply. Therefore a *repeated local search* can be applied, where an efficient deterministic optimization method is iterated, each time using randomly determined initial conditions. The initial conditions are chosen randomly for every optimization run, as experience has shown us that starting close to previously found local minima does not offer any improvement. The search is finalized whenever the fidelity with the target unitary is above some predefined threshold, or when a maximum number of tries is exceeded. An advantage of this method is that, since each optimization run starts from random initial conditions, these are easy to perform in parallel.

The algorithm chosen for each numerical optimization is the quasi-Newton method of Broyden, Fletcher, Goldfarb, and Shanno (BFGS) [79]. The function to be maximized is the fidelity of the unitary resulting from the pulse sequence with the target unitary. The gradient of the fidelity can be calculated analytically as a function of the sequence parameters, which speeds up the computation as compared to using several evaluations of the fidelity function.

A previously used approach to this optimization problem was a combination of local gradient descent and simulated annealing (SA) [34], which also helps to avoid local maxima. However, this method did not make use of the analytic expression for the fidelity gradient, which speeds up the search. Moreover, its performance depends on the “topography” of the optimization space and requires manual tuning of the search parameters to achieve optimal results. The BFGS and simulated annealing approaches were compared by compiling 100 unitaries randomly distributed in the Haar measure as explained in [80] for different numbers of qubits. Repeated application of the BFGS method seems to scale better with the number of qubits than simulated annealing (see Figure 21). The median number of search repetitions needed to find the global optimum was 1 in all the cases.

The minimum number of entangling gates required to compile a given unitary is an intrinsic property of the unitary and does not depend on the search algorithm. It is known that the number of gates required to implement an arbitrary N -qubit unitary in terms of two-qubit gates grows exponentially with the number of qubits N [6]. Our numerical results suggest a similar result for N -qubit gates. In the two-qubit case the compilation always succeeded with 3 entangling gates, and not less (using 200 search repetitions with random initial conditions). This was to be expected, since for two qubits an MS gate is equivalent to a CNOT gate, and it is known that 3 CNOT gates

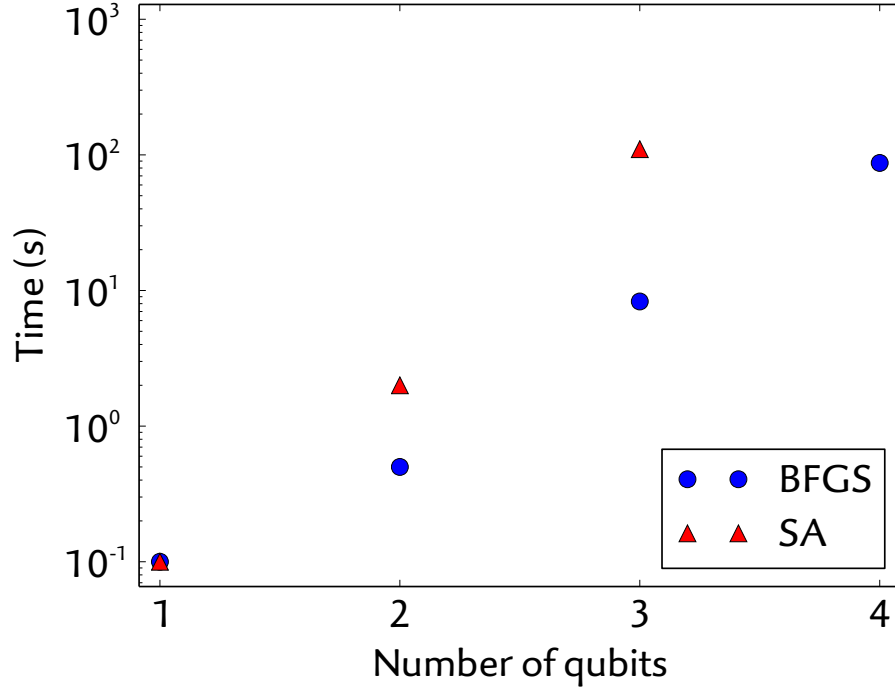


Figure 21: Average time required to find the global optimum for 100 unitaries randomly distributed in the Haar measure with the BFGS and simulated annealing methods, using an Intel®Core i5-4670s CPU 550 @ 3.10 GHz x 4 (one processing thread per optimization run). No data was obtained for the simulated annealing approach for 4 qubits owing to the excessive time required.

are enough (and in general necessary) to implement an arbitrary two-qubit unitary [81, 82]. In the three-qubit case, the optimization always succeeded with 8 entangling gates, and never with fewer (also using 200 repetitions). For 4 qubits, the optimization always succeeded for 25 entangling gates, and succeeded only 4% of the time with 24 entangling gates. However, only 4 optimization repeats were carried out in the four-qubit case, owing to the increased time it takes for these to converge. Therefore, it might be the case that given enough optimization runs, more unitaries would have been compiled with only 24 gates. I am not aware of any result in the literature concerning the number of N -qubit global entangling gates required for implementing a general N -qubit unitary for more than $N = 2$ qubits. From the numerical results, it can be conjectured that any three-qubit unitary can be implemented using at most 8 MS gates, and any four-qubit unitary using at most 24 or 25 MS gates.

A particularly interesting group of unitaries are Clifford gates, which map Pauli operators to Pauli operators. Clifford gates find applications in quantum error correction [83], randomized benchmarking [84], and state distillation protocols [6]. To explore the difficulty of compiling such gates, the algorithm was tested with randomly generated Clifford gates, as explained in Ref. [85]. In Figure 22 the

distribution of the optimal number of entangling gates required for compiling two-, three- and four-qubit unitaries is shown. The results agree with the literature [86] for the two-qubit case, since MS gates are then equivalent to controlled-Z (or CNOT) gates. For larger numbers of qubits, the performance of our algorithm in terms of number of multi-qubit gates required is also similar to that of algorithms based on two-qubit gates [86].

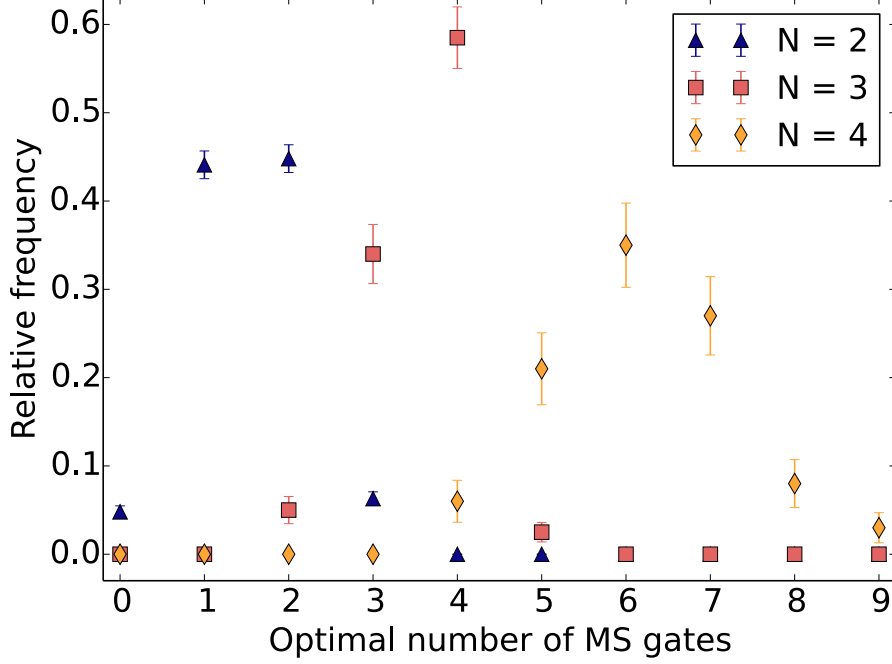


Figure 22: Optimal number of entangling gates needed to compile random Clifford operations, for sample sizes $\{1000, 200, 100\}$ for $N = \{2, 3, 4\}$ qubits. Each Clifford gate was generated using $10N^8$ steps of the random walk described in Ref. [85]. Error bars correspond to one standard deviation.

Compilation of isometries

A particular case of interest is the compilation of a unitary whose action is only specified on certain input states. This is helpful, for instance, for state preparation starting from some fixed input state. Such operations belong to the more general class of operations known as *isometries*: operations that preserve the overlap between states, but in general map two Hilbert spaces with different dimensions [74, 84]. In this case, the problem to be solved has less constraints than specifying a full target unitary, so a simpler sequence may exist. In this

section we focus on compiling a unitary that is only specified in a particular subspace of the input states, for example:

$$U_{\text{target}} = \begin{pmatrix} u_{11} & u_{12} & \vdots & \vdots \\ u_{21} & u_{22} & \text{free} & \text{free} \\ u_{31} & u_{32} & \vdots & \vdots \\ u_{41} & u_{42} & \vdots & \vdots \end{pmatrix}, \quad (101)$$

where the columns marked as ‘free’ are left unspecified. In this case, a suitable fidelity function for the numerical optimization is:

$$f(U) = \left| \text{tr} \left(U|_S U_{\text{target}}^\dagger|_S \right) \right|^2, \quad (102)$$

where $U|_S$ is a rectangular matrix with the components of the desired unitary in the restricted subspace.

A more general case is where some of the relative phases of the projections of the unitary acting on different subspaces of the whole Hilbert space are irrelevant. For example, suppose that one wants to apply a unitary to map some observable onto an ancilla qubit and then measure the ancilla, as shown in Figure 23. Since the input state of qubit 3 is known to be $|0\rangle$, only the subspace of input states spanned by $\{|000\rangle, |010\rangle, |100\rangle, |110\rangle\}$ is relevant. Moreover, the measurement will project the state of the system onto either the subspace spanned by $\{|000\rangle, |010\rangle, |100\rangle\}$, or that spanned by $\{|111\rangle\}$, and all phase coherence between these alternatives will be lost. Therefore, the compiled sequence can be sought such that it matches the desired unitary in each of the subspaces but allowing an arbitrary phase ϕ between them:

$$U_{\text{target}} = \begin{pmatrix} 1 & \vdots & 0 & \vdots & 0 & \vdots & 0 & \vdots \\ 0 & \vdots & 0 & \vdots & 0 & \vdots & 0 & \vdots \\ 0 & \vdots & 1 & \vdots & 0 & \vdots & 0 & \vdots \\ 0 & \text{free} & 0 & \text{free} & 0 & \text{free} & 0 & \text{free} \\ 0 & \vdots & 0 & \vdots & 1 & \vdots & 0 & \vdots \\ 0 & \vdots & 0 & \vdots & 0 & \vdots & 0 & \vdots \\ 0 & \vdots & 0 & \vdots & 0 & \vdots & 0 & \vdots \\ 0 & \vdots & 0 & \vdots & 0 & \vdots & e^{i\phi} & \vdots \end{pmatrix} \quad (103)$$

In this case (Figure 23) it is possible to find a simpler implementation than in the fully constrained case (Figure 19), owing to the additional degrees of freedom available, namely arbitrary outputs for the $|\psi_3\rangle = |1\rangle$ input states and an arbitrary relative phase between the two possible measurement outcomes.

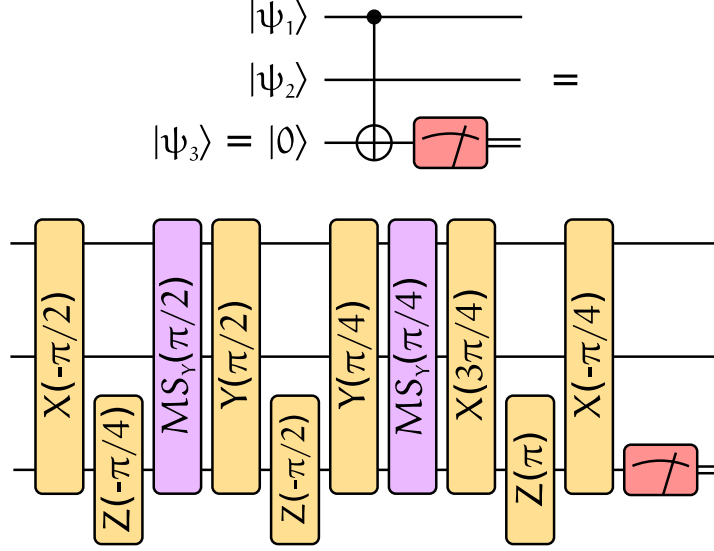


Figure 23: Top: a unitary mapping (Toffoli gate) is applied, after which qubit 3 is measured. Bottom: a pulse sequence for implementing the circuit on the left. This implementation is simpler than in the fully constrained case (Figure 19) because of the additional degrees of freedom when compiling.

In the case considered here we want to maximize the fidelity in each subspace, without regard to the relative phases between these. Therefore we can seek to maximize the function f consisting of the sum of the fidelity functions (102) corresponding to each subspace:

$$f(U) = \sum_j \left| \text{tr} \left(U|_{S_j} U_{\text{target}}^\dagger|_{S_j} \right) \right|^2, \quad (104)$$

where the sum goes over all the subspaces with different relative phases, and $U|_{S_j}$ is a rectangular matrix with the components of the desired unitary in the j -th subspace.

Compensation of systematic errors

Another strength of the compilation procedure is that it is able to compensate for systematic errors. Owing to these, the operations experimentally applied may still be unitary but deviate from the intended ones. An example of this is addressing crosstalk due to the finite waist of the addressing beam, since qubits neighboring the target qubit might also be rotated. If it is possible to characterize the actual experimental operations being applied, then they can be taken into account for the compilation by adapting our optimization procedure:

1. Compile the target unitary in terms of the ideal gates.

2. Replace the ideal gates by the experimentally characterized operations.
3. Add operations to obtain a higher fidelity with the ideal target unitary.

As an example, it is shown that excessive crosstalk can be corrected in an implementation of a Toffoli gate. Figure 24 depicts experimental data corresponding to the action of the Toffoli gate on the 8 input basis states. It can be seen that, by adding just two pulses, the output fidelity for each input state increased in some cases by up to 20%. The sequence with 11 pulses is actually only an approximate correction to the uncorrected case. The exact correction requires 14 pulses, and actually yields a lower fidelity than the approximate one, since it requires more pulses and each of these has a non-zero error probability.

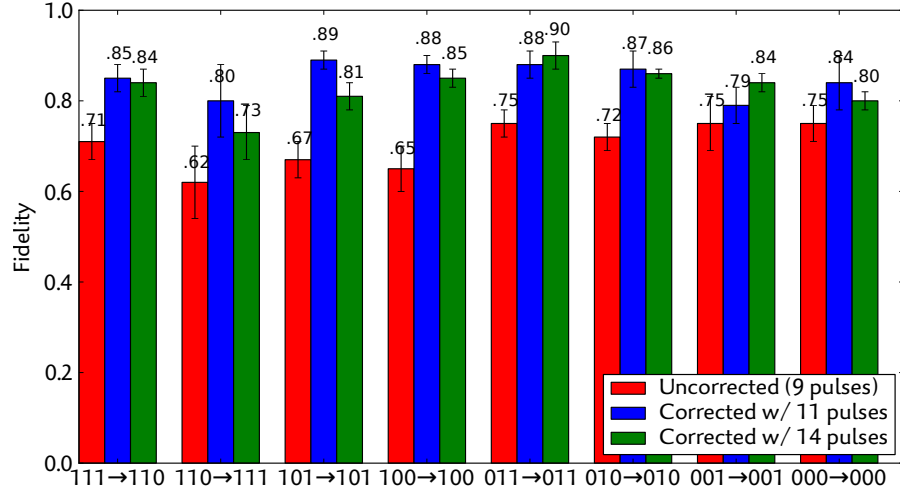


Figure 24: State fidelity for a Toffoli gate applied on the 8 canonical input states.

A LASER SETUP FOR RAMAN COOLING

For most quantum information applications, it is desired that trapped ions have the least possible motional temperature. Various methods exist to cool down ions using lasers; for example, Doppler cooling and sideband cooling on the qubit transition are routinely employed in our laboratory [18]. Doppler cooling is faster, while sideband cooling achieves lower phonon numbers. However, neither of these techniques are suitable if one wishes to recool the ion string during the execution of an algorithm. Doppler cooling does not achieve ground-state cooling, and sideband cooling on the qubit transition destroys the quantum information. *Raman sideband cooling* [87, 88] is advantageous for this application, since it allows one to achieve lower temperatures than Doppler cooling and can be implemented on a different transition than the qubit transition, so as to preserve the quantum information.

The fundamentals of Raman cooling are explained in Section 6.1. Then, in Section 6.2 a new laser setup is described, designed for implementing this cooling method in quantum information processing experiments, such as the one described in Chapter 7. Finally, in Section 6.3 the basic experimental steps to implement and calibrate the cooling scheme are outlined.

RAMAN COOLING

Raman cooling is a particular case of sideband cooling where a two-photon transition is used, as we will now discuss. Resolved sideband cooling (SBC) [17, 89] is widely used for cooling down trapped ions to the ground state of the confining potential. The basic SBC scheme is illustrated in Figure 25: starting from the electronic ground state, the red motional sideband of some electronic transition is addressed, thus exciting the electronic state of the ions and removing one excitation (phonon) from the motional degree of freedom. The ions then decay again to the ground electronic state, without changing their motional state with high probability.

The cooling rate R_n for SBC for a state with a phonon number n is given by [4]:

$$R_n = \Gamma \frac{(\eta\sqrt{n}\Omega)^2}{2(\eta\sqrt{n}\Omega)^2 + \Gamma^2}, \quad (105)$$

where Ω is the Rabi frequency of the transition, η its Lamb-Dicke parameter, and Γ its effective decay rate. This cooling rate is balanced

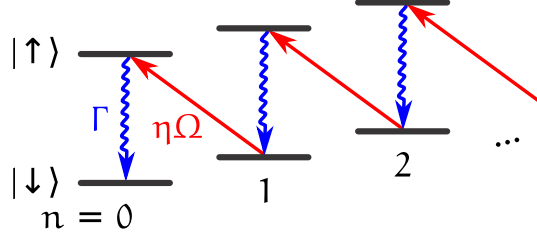


Figure 25: Level scheme for sideband cooling.

by off-resonant excitation of the carrier and the first blue sideband, reaching a steady state mean phonon number [4]:

$$\langle n \rangle = \left(\frac{\Gamma}{2\nu} \right)^2 \left[\left(\frac{\tilde{\eta}}{\eta} \right)^2 + \frac{1}{4} \right], \quad (106)$$

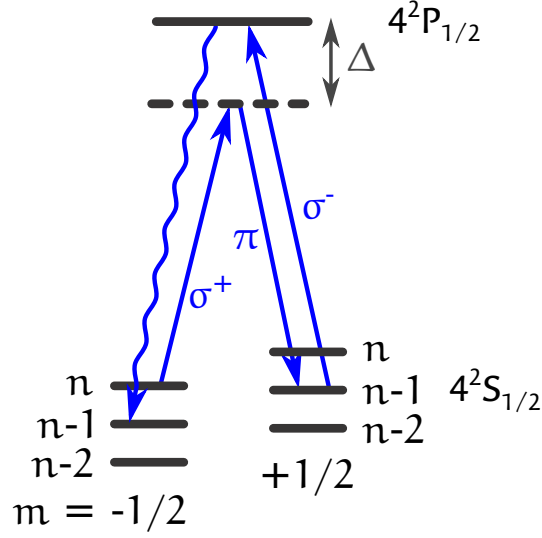
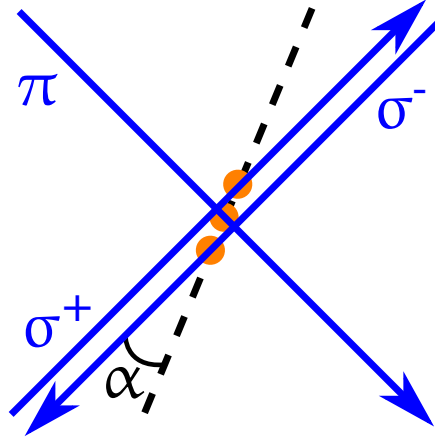
where ν is the trap frequency, and $\tilde{\eta}$ is the Lamb-Dicke parameter corresponding to the decay process.

Suppose now that we want to implement SBC on a dipole transition, such as $4^2S_{1/2}$ to $4^2P_{1/2}$ for $^{40}\text{Ca}^+$ ions. This avoids the need to scatter photons from the qubit transition $4^2S_{1/2}$ to $3^2D_{5/2}$, thus preserving quantum information stored there. Moreover, the coupling strength and Lamb-Dicke factors are bigger on the dipole transition, so faster cooling rates can be achieved. However, typical trap frequencies ν are on the order of a few MHz, while the spontaneous width Γ of dipole allowed transitions is typically on the order of tens or hundreds of MHz, so the motional sidebands cannot be resolved. This issue can be circumvented, so as to reach the resolved sideband regime, by reducing the effective spontaneous decay rate of the transition. One way to achieve this is to couple two atomic ground states with a Raman transition far detuned from a fast decaying excited state [90].

Let us consider a three-level Λ system, as depicted in Figure 26 for $^{40}\text{Ca}^+$. The two-photon Raman coupling is formally equivalent to a single-photon transition if one considers the frequency difference of the applied light fields $\Delta\omega$ as the transition frequency, and the wave vector difference $\Delta\vec{k}$ as the wave vector of the driving field. In this way, the same sideband cooling scheme already described can be applied: the red sideband $n \rightarrow n-1$ of the transition is excited using σ^+ - and π -polarized beams. The spontaneous decay is realized by optically pumping the ion back to the ground state with a σ^- -polarized beam close to resonance.

The Lamb-Dicke parameter η for the interaction with the effective two-level transition is given by:

$$\eta = |\Delta\vec{k} \cdot \vec{x}_0|, \quad (107)$$

Figure 26: Three-level Λ system.Figure 27: Spatial arrangement of the three Raman cooling beams. The π beam is perpendicular to the σ beams, and $\alpha = 22.5^\circ$.

where $\Delta\vec{k}$ is the difference between the wave vectors of the σ^+ and π beams, and $\vec{x}_0$ is a vector along the trap axis with magnitude corresponding to the extension of the ground-state wavefunction:

$$x_0 = \sqrt{\frac{\hbar}{2m\omega_{\text{trap}}}}, \quad (108)$$

which yields $x_0 \approx 11$ nm for our experimental parameters. Considering our beam geometry, as shown in Figure 27, we obtain $\eta \approx 22.7\%$, compared to $\eta \approx 8.8\%$ for the 729 nm qubit transition. Because of this bigger Lamb-Dicke parameter, we can achieve faster cooling using the Raman transition.

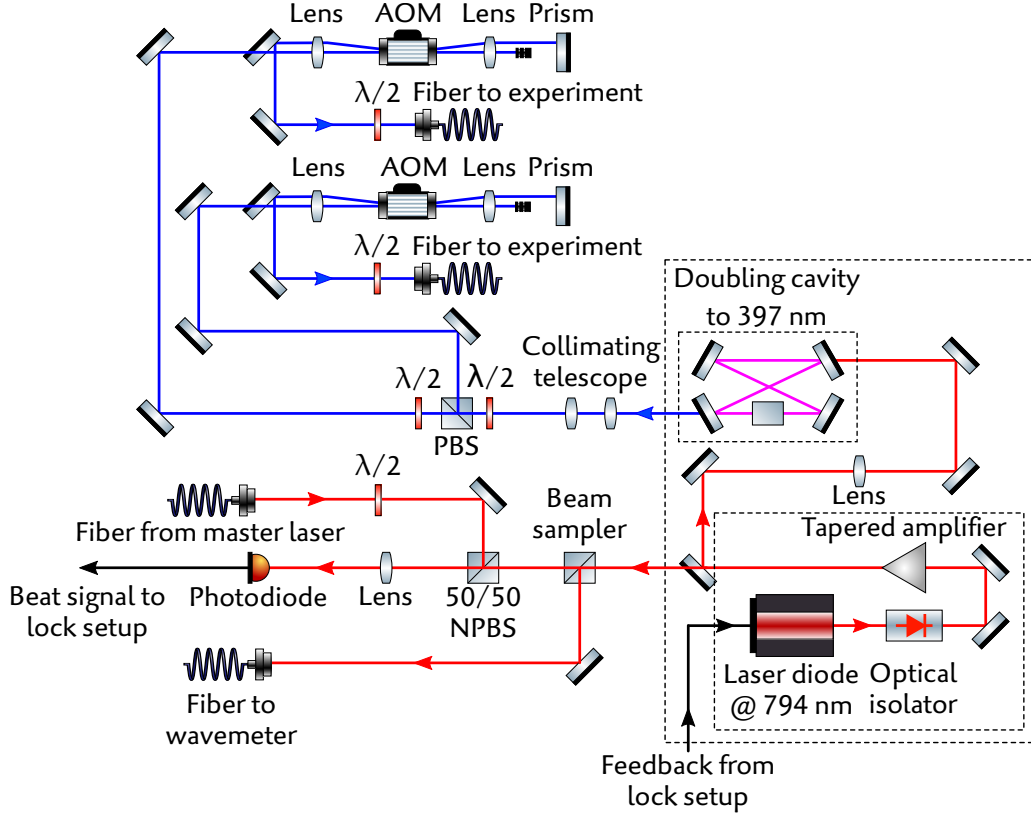


Figure 28: Optical setup for producing and tuning the Raman cooling light.

OPTICAL SETUP

The stimulated Raman process requires σ^+ - and π -polarized beams whose frequency has to be tunable to be resonant with the Raman transition. For generating and tuning this light the setup shown in Figure 28 was assembled. The laser source is a laser diode (Toptica TA-SHG 110) with a wavelength of 793.699 nm, frequency doubled with a non-linear crystal in a bow-tie cavity to produce about 100 mW of light with a wavelength of 396.8495 nm, resonant with the $4^2S_{1/2}$ to $4^2P_{1/2}$ transition of $^{40}\text{Ca}^+$. The beam is split into two independent paths, each of which passes an acousto-optic modulator (AOM) in double-pass configuration to tune the light frequency. Both paths are then coupled into optical fibers to deliver the light to the ion string. The beam geometry is shown in Figure 27. Right before the trap, the intensity of the σ^+ beam is stabilized with a sample and hold (S/H) circuit, described in detail in Ref. [92].

The Raman cooling light must also be stabilized against frequency drifts. Most of the lasers in our laboratory are frequency-locked by means of the Pound-Drever-Hall (PDH) technique [93] to stabilization cavities. An alternative to this is to use a *frequency-offset stabilization* (or *offset lock*) method, where the frequency difference of two lasers is stabilized. In this way, a laser (*slave*) can be locked to another one (*mas-*

*Never fire a laser at
a mirror. —Larry
Niven [91]*

ter) that is already stabilized. In this case, the master laser is the laser used for state detection, that is close to resonance with the dipole transition. This technique avoids the experimental overhead of stabilizing the laser to an additional optical cavity. A thorough overview of methods for offset locking can be found in Ref. [94].

To stabilize the Raman laser described here, we use the offset lock method presented in Ref. [95]. This technique consists in measuring the beat signal of both lasers with a photodiode and then transforming the frequency of this signal into an electric error signal. The scheme to do this is shown in Figure 29. The beat signal, of frequency ω_Δ , is first mixed down with a local oscillator of frequency ω_{lo} to the intermediate frequency $\omega = \omega_\Delta - \omega_{lo}$. Then, this signal is split in two paths with a length difference ΔL , where it acquires a phase difference $\Delta\phi = \omega\Delta L$, proportional to the frequency ω . This phase difference is converted with a phase detector (or mixer) to a voltage that can be used as an error signal. A sketch of the resulting error signal is shown in Figure 30.

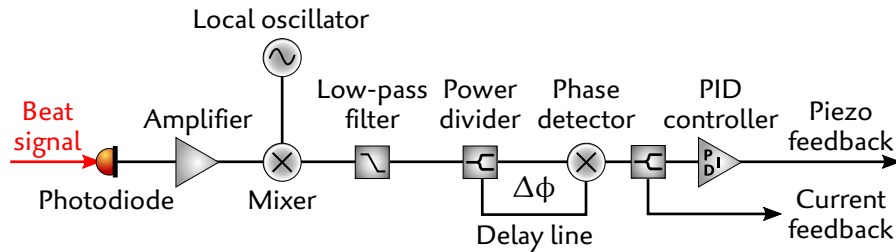


Figure 29: Offset lock scheme for stabilizing the Raman cooling laser to an already locked laser.

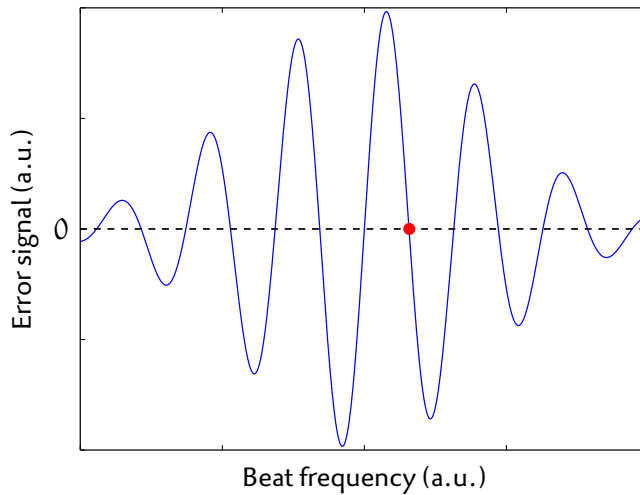


Figure 30: A sketch of the error signal after conversion of the beat frequency to voltage. The dot indicates one of the lock points (crossings of the error signal with 0). Locking to the center crossing is inadvisable since it corresponds to a zero-frequency signal.

The error signal is split in two parts, for slow and fast feedback respectively. The first part is used as the input of a Proportional-Integral-Differential (PID) controller, whose output is fed back to a piezo actuator that controls the laser diode grating. This provides a slow feedback loop with a bandwidth of a few kHz, which corrects for slow thermal and acoustic drifts. The second part of the error signal is fed directly into a field-effect transistor (FET) current control that modulates the DC current of the laser diode. This provides a proportional controller with a bandwidth of 5 MHz, and provides fast feedback to narrow the linewidth of the laser. The achieved linewidth of the beat between the slave and master lasers is on the order of 200 kHz.

This locking method is simple and inexpensive to implement, since everything can be achieved with commercial off-the-shelf electronic components. Moreover, the capture range and slope of the error signal can be tuned by simply changing the length of the cable. However, this also means that the slope and the capture range cannot be tuned independently.

EXPERIMENTAL IMPLEMENTATION OF RAMAN COOLING

The first step is to focus and align the cooling beams on the ions. For this purpose, we set the frequency of each beam several MHz red-detuned from the dipole transition and maximized the fluorescence counts from the ions. Next, the polarization of the beams was adjusted. The polarization of the π beam is adjusted by maximizing the fluorescence counts. Next, the σ^- beam can be adjusted by turning only this one on, and adjusting the polarization to minimize the fluorescence counts, since this pumps the population out from the $4^2S_{1/2}$ ($m = +1/2$) state. Finally, the σ^+ is turned on together with the σ^- beam and its polarization is adjusted to maximize the fluorescence counts.

Next, we detuned both lasers $\Delta = 2.84$ GHz to the red from the dipole transition. The frequencies of the σ^+ and π beams must be fine-tuned so that their frequency difference is resonant with the $4^2S_{1/2}$ ($m = -1/2$) to $4^2S_{1/2}$ ($m = +1/2$) transition. For this purpose, the qubit is initialized in the $4^2S_{1/2}$ ($m = -1/2$) state and then the σ^+ and π beams are turned on to excite the Raman transition to $4^2S_{1/2}$ ($m = +1/2$). To measure the excitation of the $4^2S_{1/2}$ ($m = +1/2$) state, we apply a π pulse on the $4^2S_{1/2}$ ($m = -1/2$) to $3^2D_{5/2}$ ($m = -1/2$) transition, and then perform a fluorescence measurement. Figure 31 shows an excitation spectrum measured in this way, which shows the carrier transition ($\Delta n = 0$), as well as the red ($\Delta n = -1$) and blue ($\Delta n = +1$) motional sidebands.

Since we have a single light source for both σ^+ and π beams, the optical power must be distributed between them to optimize the

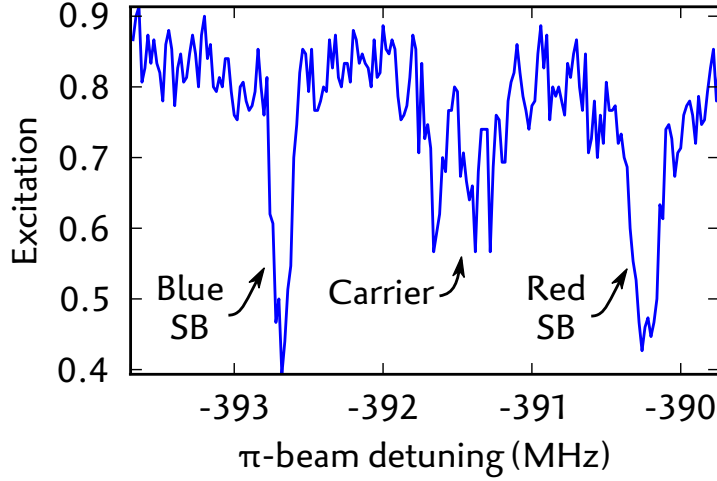


Figure 31: Excitation spectrum of the Raman transition $4^2S_{1/2}(m = -1/2)$ to $4^2S_{1/2}(m = +1/2)$ (without sideband cooling). Dataset from 2013-11-08, qc1106.

cooling efficiency. The effective Rabi frequency Ω of the Raman process is proportional to the product of the Rabi frequencies of both beams, so it is maximized whenever $\Omega_{\sigma^+} = \Omega_{\pi}$. These Rabi frequencies can be measured by optically pumping population from the $4^2S_{1/2}(m = -1/2)$ level by an excitation of the $4^2P_{1/2}$ levels and spontaneous decay. The σ^+ beam completely pumps away the population from the $4^2S_{1/2}(m = -1/2)$ state, while the π beam pumps only half of the population. The effective decay rates of the population in the $4^2S_{1/2}(m = -1/2)$ level are given by the product of the excitation rates and the decay rates to the $4^2S_{1/2}(m = +1/2)$ level:

$$\Gamma_{\sigma^+} = \frac{1}{3}\Gamma_{P \rightarrow S} \left(\frac{\Omega_{\sigma^+}}{2\Delta} \right)^2, \quad (109)$$

$$\Gamma_{\pi} = \frac{2}{3}\Gamma_{P \rightarrow S} \left(\frac{\Omega_{\pi}}{2\Delta} \right)^2. \quad (110)$$

The Rabi frequencies of the beams can therefore be extracted from a measurement of this decay time, as shown in Figure 32. In this case we have: $\Omega_{\sigma^+} = (58.2 \pm 0.7)$ MHz, $\Omega_{\pi} = (50.5 \pm 1.6)$ MHz. The effective Rabi frequency of the two-photon process is then:

$$\Omega = \frac{\Omega_{\sigma^+}\Omega_{\pi}}{2\Delta} \approx (517 \pm 23) \text{ kHz}. \quad (111)$$

The optimal frequency difference for the Raman cooling lasers can be found by minimizing the excitation probability of the red motional sideband after cooling. This excitation is shown in Figure 33 as a function of the detuning of the π -polarized beam.

To estimate the performance of the Raman cooling scheme more precisely, we studied Rabi oscillations on the blue sideband on the

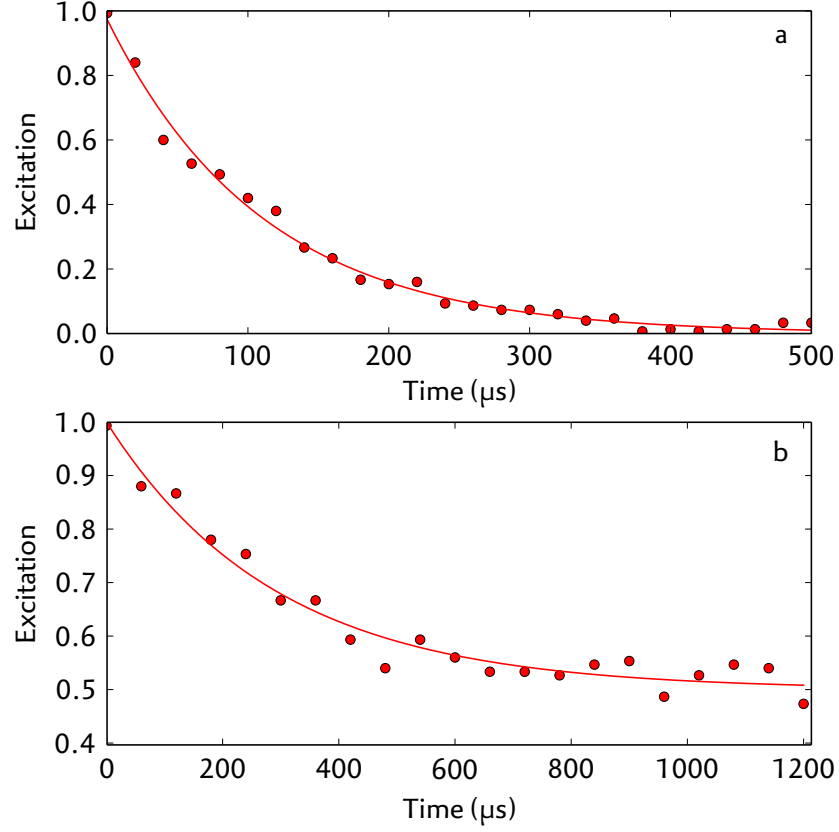


Figure 32: Exponential decays of the $4^2S_{1/2}(m = -1/2)$ population for: a) σ^+ beam, decay time $\tau = (110 \pm 3) \mu\text{s}$ (dataset from 2013-11-08, qc1421). b) π beam, decay time of $\tau = (292 \pm 19) \mu\text{s}$ (dataset from 2013-11-08, qc1423).

qubit transition $4^2S_{1/2}$ to $3^2D_{5/2}$, as shown in Figure 34. For a phonon distribution with populations c_n , these oscillations are described by [18]:

$$p_1 = \sum_n c_n \sin^2 \left(\frac{\eta \Omega_0}{2\sqrt{n+1}} t \right), \quad (112)$$

where η is the Lamb-Dicke parameter and Ω_0 is the Rabi frequency on the carrier transition. If we assume a thermal distribution, the populations are given by:

$$c_n = \frac{\langle n \rangle^n}{(\langle n \rangle + 1)^{n+1}}. \quad (113)$$

From a fit with this distribution we measured a mean phonon number $\langle n \rangle = 0.17 \pm 0.02$.

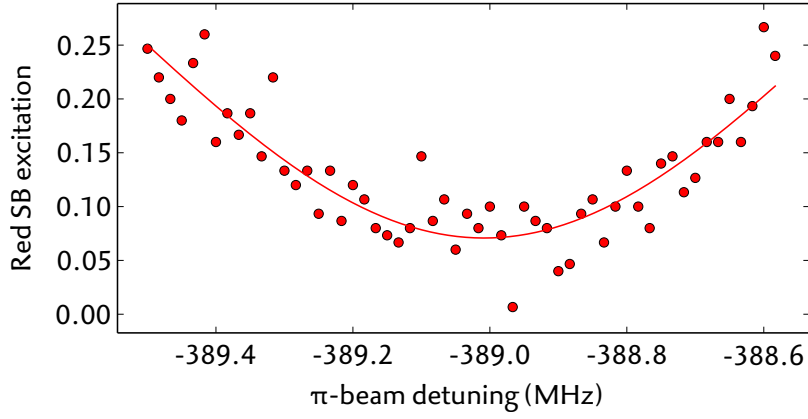


Figure 33: Frequency scan around the Raman cooling transition. This data was taken for a different σ^+ power as Fig. 31, so the optimal cooling frequency differs from the red sideband frequency. Dataset from 2013-11-08, qc1146.

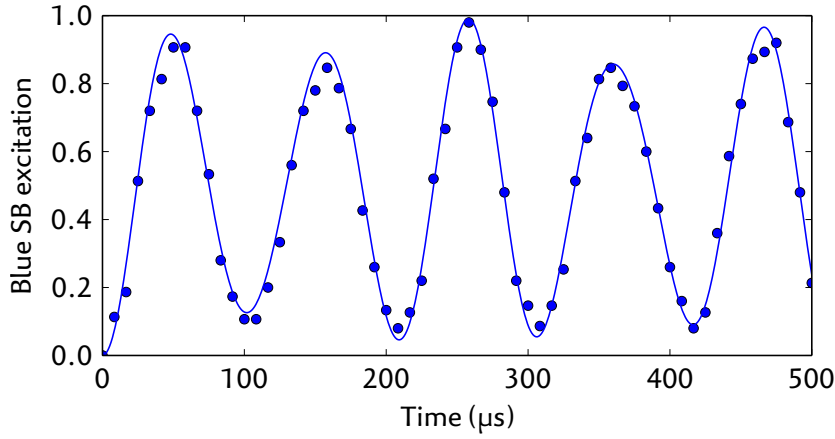


Figure 34: Rabi flops on the blue sideband of the qubit transition (dataset from 2013-11-08, qc1150). The fit indicates a mean phonon number of $\langle n \rangle = 0.17 \pm 0.02$.

REALIZATION OF A SCALABLE SHOR ALGORITHM

The contents of this chapter are extracted from Ref. [76].

As we have seen in Chapter 3, Shor’s algorithm for factoring integers [7] is one example in which a quantum computer (QC) outperforms the most efficient known classical algorithms. Experimentally, its implementation is highly demanding [96–101] as it requires both a sufficiently large quantum register and high-fidelity control. Such challenging requirements raise the question whether optimizations and experimental shortcuts are possible. Optimizations, especially system-specific or architectural, are certainly possible. However, for a demonstration of Shor’s algorithm in a scalable manner, special care has to be taken not to oversimplify the implementation – for instance by employing knowledge about the solution prior to the actual experimental implementation – as pointed out in Ref. [102].

Let us remember the basic scheme presented in Chapter 3. First, we consider a classical factoring recipe, assuming as an example that the number we want to factor is $N = 15$. We pick a random number $a \in [2, N - 1]$ (the base), say, $a = 7$. We check if the greatest common divisor $\gcd(a, N) = 1$; if not, a factor is already determined. This is the case for $a = \{3, 5, 6, 9, 10, 12\}$, and thus we can stop here. For all other values of a , we calculate the modular exponentiation $a^x \bmod N$ for $x = 0, 1, 2, \dots$ and find its period r : the first $x > 0$ such that $a^x \bmod N = 1$. Given r , finding the factors of N requires calculating the greatest common divisors of $a^{r/2} \pm 1$ and N , which is efficiently possible classically – for instance, using Euclid’s algorithm. For our example ($N = 15, a = 7$) the modular exponentiation yields $1, 7, 4, 13, 1, \dots$, which has period 4. The greatest common divisors of $a^{r/2} \pm 1 = 7^{4/2} \pm 1 = \{48, 50\}$ and $N = 15$ are $\{3, 5\}$, the non-trivial factors of N . In this example, the cases $a = \{4, 11, 14\}$ have periodicity $r = 2$ and require a single multiplication step ($a^2 \bmod N = 1$), which is considered an “easy” case [102].

How can this recipe be implemented in a QC? A QC has to calculate $a^x \bmod N$ in a computational register for $x = 0, 1, 2, \dots$ and then extract r . Using the quantum Fourier transform (QFT), applied to the period register, the period of $a^x \bmod N$ can be extracted from $\mathcal{O}(1)$ measurements.

REQUIREMENTS FOR A SCALABLE IMPLEMENTATION

What are the requirements and challenges to implement Shor’s algorithm? We first focus on the period register and will subsequently

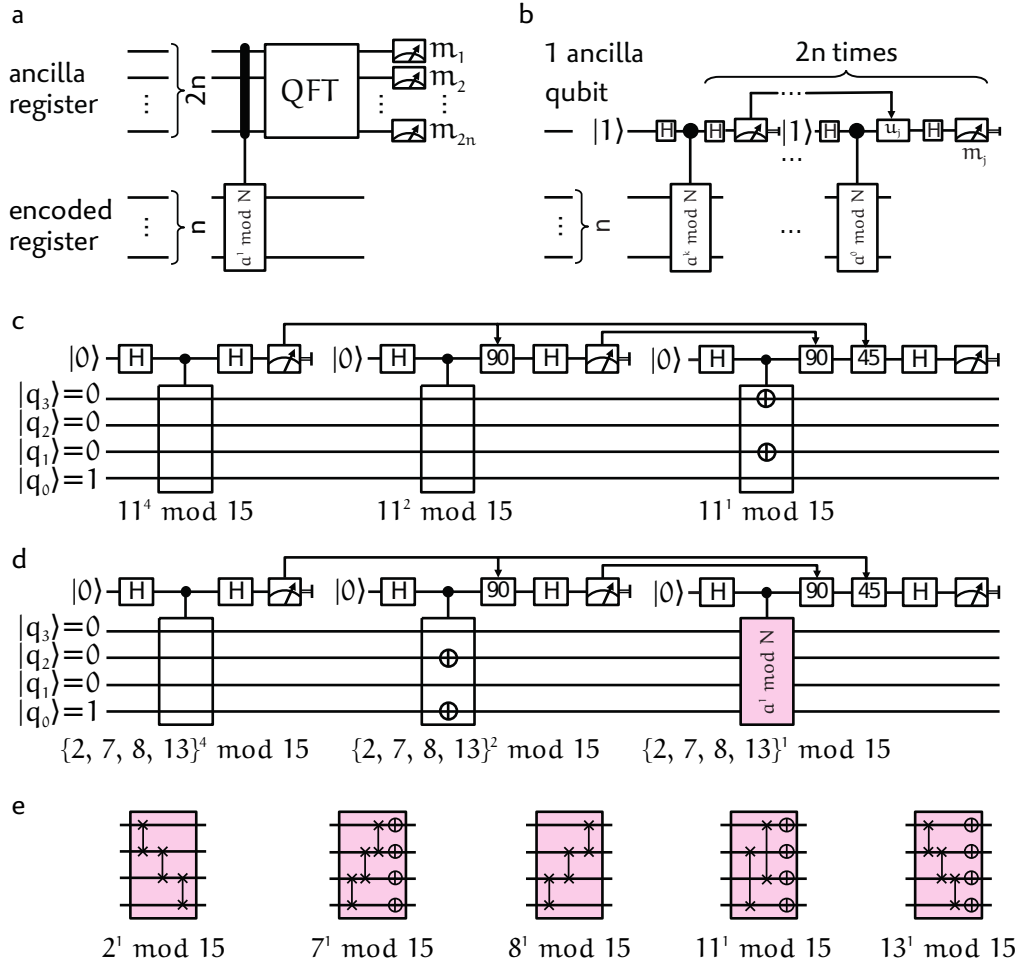


Figure 35: Quantum circuits of Shor's algorithm for factoring 15: a) generic text-book approach; b) Kitaev's approach for a generic base a ; c) the actual implementation for factoring 15 to base 11, optimized for the single input state it is subject to; d) Kitaev's approach to Shor's algorithm for the bases $\{2, 7, 8, 13\}$. Here, the optimized map of the first multiplier is identical in all 4 cases, and the last multiplier is implemented with full modular multipliers as depicted in e). In all cases, the single QFT qubit is used three times, which, together with four qubits in the computation register, adds up to seven effective qubits. e) Circuit diagrams of the modular multipliers of the form $a \bmod N$ for bases $a = \{2, 7, 8, 11, 13\}$.

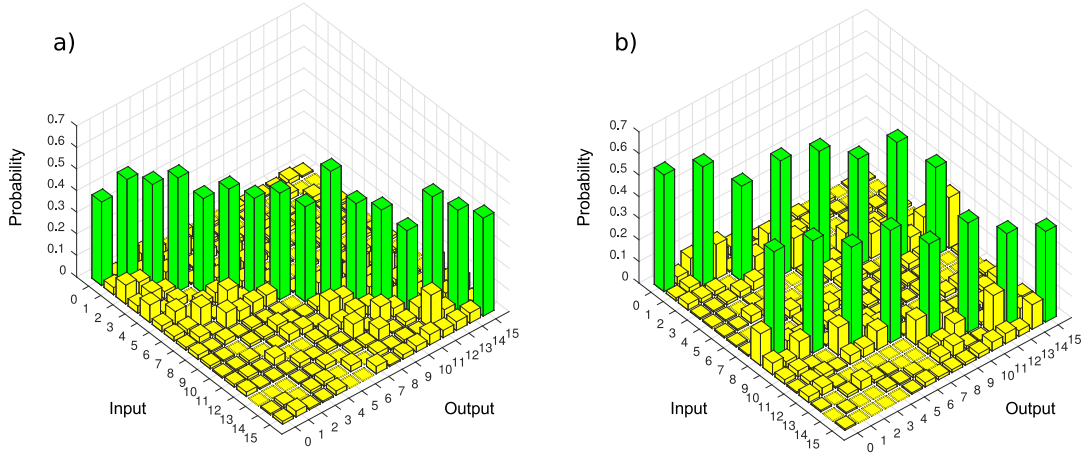


Figure 36: Experimentally obtained truth table of the controlled 2 mod 15 multiplier: a) with the control-qubit being in state 0, the truth table corresponds to the identity operation; b) when the control qubit triggers the multiplication, the truth table illustrates the multiplication of the input state with 2 mod 15. The mean fidelity with respect to the expected output state is 48(5)%.

address modular exponentiation in the computational register. Factoring N , which can be described by $n = \lceil \log_2(N) \rceil$ classical bits (with $\lceil \cdot \rceil$ rounding up to next integer number), requires a minimum of n qubits in the computational register (to store the results of $a^x \bmod N$) and generally about $2n$ qubits in the period register [6, 19]. Thus, even a seemingly simple example such as factoring 15 (an $n = 4$ -bit number), requires $3n = 12$ qubits. These qubits then have to be manipulated with high fidelity gate operations. Given the current state-of-the-art control over quantum systems [23], such an approach would likely yield an unsatisfactory performance. However, a full quantum implementation of the order finding part of the algorithm is not necessary. In Ref. [44], Kitaev notes that, if only the classical information of the QFT (such as the period r) is of interest, $2n$ qubits subject to a QFT can be replaced by a single qubit, as already explained in Chapter 3. This approach, however, requires qubit recycling (specifically: in-sequence single-qubit readout and reinitialization) paired with feed-forward.

In the following, Kitaev's QFT will be referred to as $\text{KQFT}^{(M)}$; it replaces a QFT acting on M qubits with a semiclassical QFT acting repeatedly on a single qubit. Similar applications of Kitaev's approach to a semiclassical QFT in quantum algorithms have been investigated in Refs. [103–105]. For the implementation of Shor's algorithm, Kitaev's approach provides a reduction from the previous n computational qubits and $2n$ QFT qubits (in total, $3n$ qubits) to only n computational qubits and 1 $\text{KQFT}^{(2^n)}$ qubit (in total, $n + 1$ qubits).

A notably more challenging aspect than the QFT, and the second key ingredient of Shor's algorithm, is modular exponentiation, which admits the following general simplifications:

1. Considering Kitaev's approach (see Fig. 35), the input state $|1\rangle$ (in decimal representation) is subject to a conditional multiplication based on the most significant bit k of the period register. At most, there will be two results after this first step. It follows that, for the very first step, it is sufficient to implement an optimized operation that conditionally maps $|1\rangle \rightarrow |a^{2^k} \bmod N\rangle$.
2. Subsequent multipliers could, in principle, also be replaced with maps by considering only possible outputs of the previous multiplications. However, using such maps will become intractable, as the number of input and output states to be considered grows exponentially with the number of steps: after n steps, $2^n > N$ possible outcomes need to be considered, a numerical task as challenging as factoring N by classical means. Thus, to ensure scalability, full controlled modular multipliers need to be implemented. Fig. 36 shows the experimentally obtained truth table for the modular multiplier $(2 \bmod 15)$ (see also Appendix B for modular multipliers with bases $\{7, 8, 11, 13\}$). These quantum circuits can be efficiently derived from classical procedures using a variety of standard techniques for reversible quantum arithmetic and local logic optimization [106, 107].
3. The very last multiplier allows one more simplification: Considering that the results of the modular exponentiation are not required for Shor's algorithm (as only the period encoded in the period register is of interest), the last multiplier only has to create the correct correlations between the period register and the computation register. Local operations after the conditional (entangling) operations may be discarded to facilitate the final multiplication without affecting the results of the implementation.
4. In rare cases, certain qubits are not subject to operations in the computation. Thus, these qubits can be removed from the algorithm entirely.

For large-scale quantum computation, optimization steps 1, 3 and 4 will only marginally affect the performance of the implementation. They represent only a small subset of the entire computation which mainly consists of the full modular multipliers. Thus, the realization of these modular multipliers is a core requirement for the implementation of a scalable Shor algorithm. Furthermore, Kitaev's approach requires in-sequence measurements, qubit recycling to reset the measured qubit, feed-forward of gate settings based on previous measurement results, as well as controlled quantum operations – tasks that have not been realized in a combined experiment so far.

EXPERIMENTAL IMPLEMENTATION

These techniques are demonstrated in a realization of Shor's algorithm in an ion-trap quantum computer, with five $^{40}\text{Ca}^+$ ions in a linear Paul trap, as introduced in Chapter 2. The qubit is encoded in the ground state $4^2S_{1/2}$ and the metastable state $3^2D_{5/2}$ (for more details see Appendix B and Ref. [23]). Unitary operations, illustrated in Fig. 35, are decomposed into a sequence of experimentally available gates described in Section 2.4, using the techniques described in Chapter 5 or in Ref. [34].

To complete the toolbox necessary for Kitaev's approach to Shor's algorithm, we also implement: single-qubit readout, by transferring all other qubits to the $\{|D\rangle, |D'\rangle\}$ subspace and subsequent electron shelving [31] on the $S_{1/2} \leftrightarrow P_{1/2}$ transition. Classical feed-forward can be realized by storing counts detected during the single-qubit readout [108] in a classical register and applying subsequent conditional laser pulses. The measured qubit is reinitialized using optical pumping for the electronic state, and Raman cooling (see Chapter 6 and Refs. [17, 90]) for the motional state of the ions. The pulse sequences and additional information on the implementation of the modular multipliers are available in Appendix B.

Electron-shelving [31] on the $S_{1/2} \leftrightarrow P_{1/2}$ transition addresses, and thus projects, all qubits of the quantum register. For Kitaev's implementation, however, only one qubit needs to be measured. With collective illumination, this can be achieved by transferring quantum information encoded in qubits that should not be measured into the D-state manifold. Here, the quantum information is protected against shelving light on the $S_{1/2} \leftrightarrow P_{1/2}$ transition – the ion will not scatter any photons. Using light resonant with the $S_{1/2}(m = -1/2) \leftrightarrow D_{5/2}(m = -5/2)$ transition (denoted by $R_2(\theta, \phi)$), a refocusing sequence of the form $R_2(0.5, 0) \cdot S_z(1, j) \cdot R_2(0.5, 0)$ efficiently encodes all but qubit j in $D_{5/2}(m = -1/2)$ and $D_{5/2}(m = -5/2)$. Subsequently, the entire quantum register may be subject to shelving light, yet only qubit i will be projected.

When all qubits that need to be protected against projection have been encoded in the $\{D_{5/2}(m = -1/2), D_{5/2}(m = -5/2)\}$ manifold, light at 397 nm resonant with the $S_{1/2} \leftrightarrow P_{1/2}$ transition scatters photons on the remaining ion-qubits depending on the electronic state. The illumination time is set to 300 μs . A histogram of the photon counts detected at the photomultiplier tube is shown in Figure 38. Using counter electronics with discriminator set at 4 counts within the detection window, the states in the $D_{5/2}$ manifold with a mean count rate of 0.24 counts/ms (or 0.07 counts within the detection window) and states in the $S_{1/2}$ manifold with a mean count rate of 48 counts/ms (or 14.4 counts in the detection window) which leads to a detection fidelity better than 99.8%. The Boolean output of the dis-

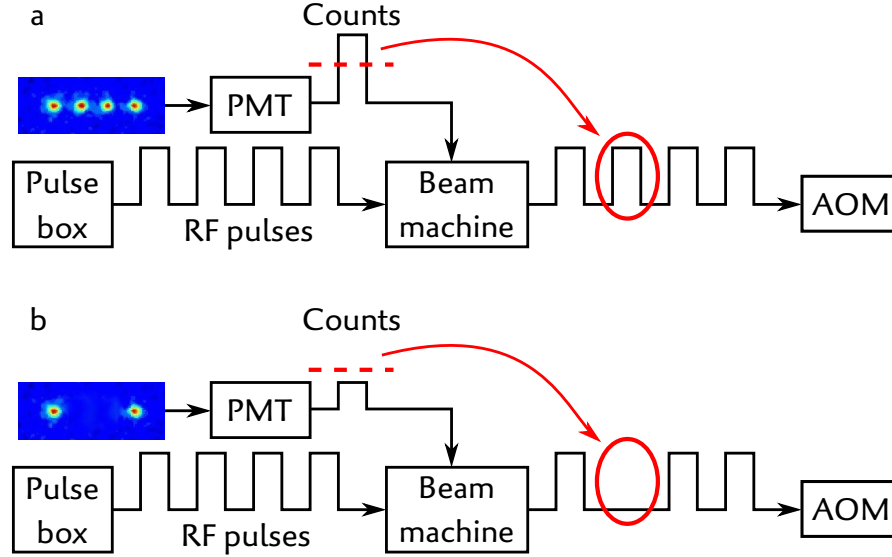


Figure 37: Setup for performing conditional operations depending on the state of the ions. The so-called “beam machine” is an device that counts pulses coming from the PMT. If these are above a predefined threshold, the device allows RF pulses to go through. For technical details, see Ref. [109, p. 127].

criminator is subsequently used in the electronics for state-dependent pulses and thus state-dependent operations, as illustrated in Figure 37.

Scattering photons during the detection window heats up the ion string and reduces the quality of subsequent quantum operations applied to the register. Therefore recoiling of the ion-string after the illumination with electron-shelving light is necessary. However, this recoiling must not destroy any quantum information stored in the other qubits. Considering that, after the measurement, the remaining quantum information is stored in the $D_{5/2}$ manifold, we can employ three-beam Raman cooling (see Chapter 6) in the $S_{1/2} \leftrightarrow P_{1/2}$ manifold without affecting the information. The Raman light field, consisting of σ^+ and π light with respect to the quantization axis, is detuned by 1.5 GHz from the resonant $S_{1/2} \leftrightarrow P_{1/2}$ transition. The relative detuning between σ^+ and π is chosen such that it creates resonant coupling between $S_{1/2}(m = -1/2) \otimes |n\rangle \leftrightarrow S_{1/2}(m = 1/2) \otimes |n-1\rangle$, with $|n\rangle$ representing the quantized axial state of motion of the ion. The transfer is reset by resonant σ^- light. Raman cooling is employed for 500 μ s. The qubit is reinitialized to the $S_{1/2}(m = -1/2)$ after cooling by an additional 50 μ s of resonant σ^- light. However, if the measured qubit was found to be in the $D_{5/2}$ manifold, neither does the measurement heat the ion string nor does the Raman cooling affect the register. To reinitialize the measured qubit, it is transferred from $D_{5/2}(m = -1/2)$ to $S_{1/2}(m = 1/2)$ (which was depleted by the previous 50 μ s of σ^-). An additional pulse of σ^- light for 50 μ s finally initializes the qubit, regardless whether it was projected onto the S

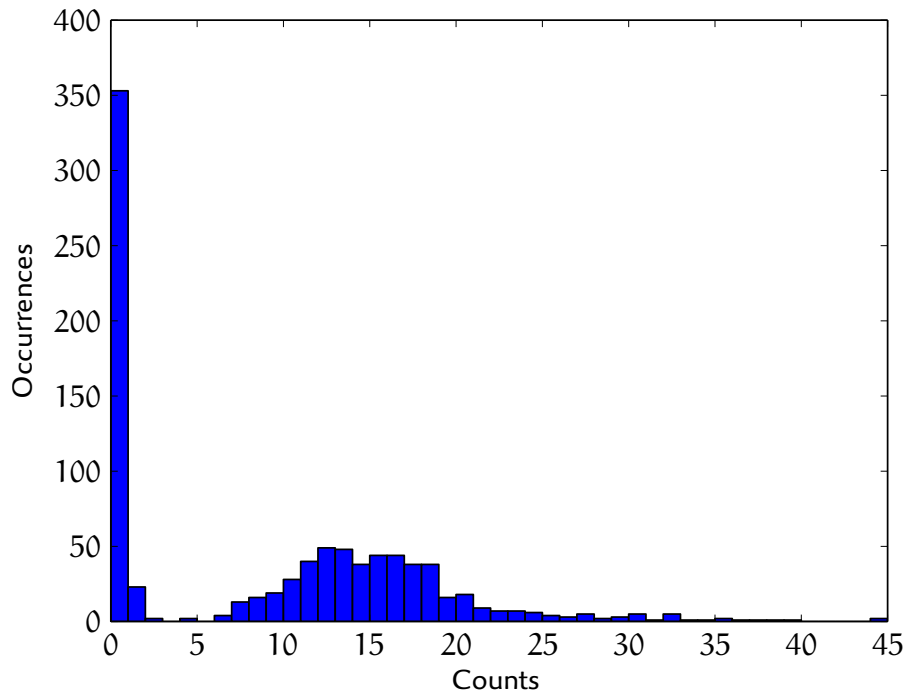


Figure 38: In-sequence photon-count histogram. Using a detection window of $300\ \mu\text{s}$, the photomultiplier tube collects on average 0.07 counts when the qubit is in state D and 14.4 counts when it is in state S. As can be seen in the figure, these two Poisson distributions are well distinguishable.

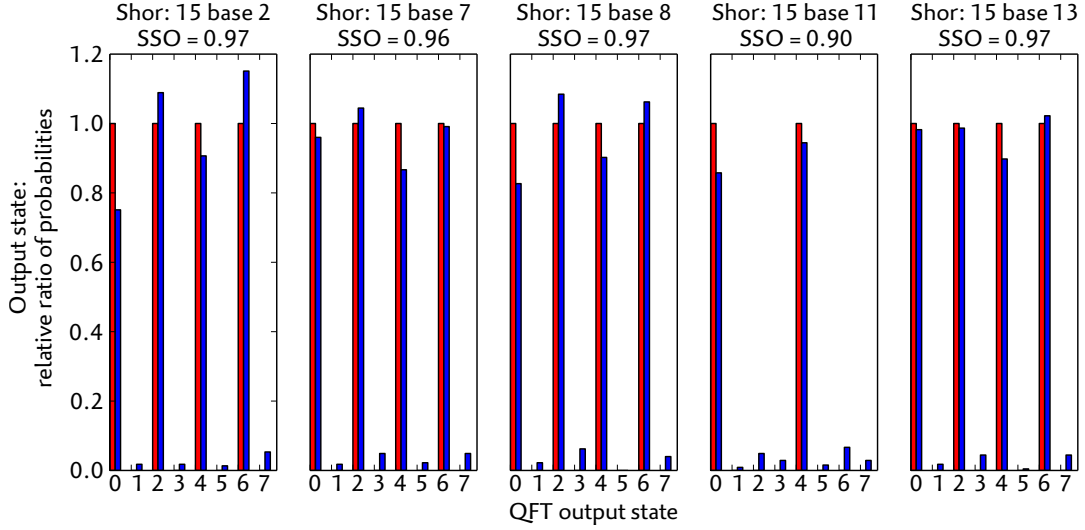


Figure 39: Results and correct order-assign probability for the different implementations to factor 15: a) Three-digit results (in decimal representation) of Shor’s algorithm for the different bases. The ideal data (red) for period $\{2, 4\}$ is superimposed on the raw data (blue). The squared statistical overlap is larger than 90% for all cases.

or D manifolds. During the entire time when the qubit is subject to Raman cooling or initializing σ^- light, a repump laser at 866 nm is applied to prevent population trapping in the $D_{3/2}$ manifold due to spontaneous decay from the $P_{1/2}$ state to $D_{3/2}$.

RESULTS

The measurement results for the output of the QFT for bases $\alpha = \{2, 7, 8, 11, 13\}$ with periods $r = \{4, 4, 4, 2, 4\}$ are shown in Fig. 39. In order to quantify the performance of the implementation, previous realizations mainly focused on the squared statistical overlap (SSO) [110], the classical equivalent to the Uhlmann fidelity [6]. While an SSO of $\{0.968(1), 0.964(1), 0.966(1), 0.901(1), 0.972(1)\}$ was achieved for the cases $\alpha = \{2, 7, 8, 11, 13\}$, this does not answer the question of a user in front of the quantum computer: “What is the period?” Shor’s algorithm allows one to deduce the period with high probability from a single-shot measurement, since the output of the QFT, x , is, in the exact case, a ratio of integers, where the denominator gives the desired period. This period is extracted using a continued fraction expansion applied to $x/2^k$, a good approximation of the ideal case when k , the number of qubits, is sufficiently large. In our realizations with bases $\alpha = \{2, 7, 8, 11, 13\}$, the probabilities (and their error estimates in parenthesis) to obtain output states that allow the derivation of the correct period are $\{56(2), 51(2), 54(2), 47(2), 50(2)\}\%$. Thus, a confidence at a level of more than 99% that the correct periodicity is obtained requires the experiment to run about eight times.

To sum up, a realization of Kitaev's vision of Shor's algorithm was presented here, based on scalable building blocks with three-digit resolution to factor 15 using bases $\{2, 7, 8, 11, 13\}$. Here, a semiclassical QFT combined with single-qubit readout, feed-forward and qubit recycling was successfully employed. Compared to the traditional approach, this algorithm reduces the required number of qubits by almost a factor of three. Furthermore, the entire quantum register has been subject to the computation without requiring previous knowledge of the result. Employing the equivalent of a quantum cache by spectroscopic decoupling significantly facilitated the derivation of the necessary pulse sequences to achieve high-fidelity results. This scalable algorithm implementation, combined with a scalable trap architecture [25] and quantum error correction, has the potential to enable factoring of large integers that are not feasible on classical computers.

SIMULATION OF A WILSON MODEL

The contents of this chapter are extracted from Ref. [111].

INTRODUCTION

As discussed in Chapter 4, gauge theories are fundamental to our understanding of interactions between the elementary constituents of matter as mediated by gauge bosons [8, 9]. However, computing the real-time dynamics in gauge theories is a notorious challenge for classical computational methods. In the spirit of Feynman’s vision of a quantum simulator [10, 11], this has recently stimulated theoretical effort to devise schemes for simulating such theories on engineered quantum devices, with the difficulty that gauge invariance and the associated local conservation laws (Gauss laws) need to be implemented [60, 62, 112].

In this chapter, the first experimental demonstration of a digital quantum simulation of a lattice gauge theory is reported. The theory we consider is quantum electrodynamics (QED) in $1 + 1$ dimensions (one spatial dimension plus time), known as the *Schwinger model* [13, 14], which we already studied in Chapter 4. We are interested in the real-time evolution of the Schwinger mechanism [113, 114], describing the instability of the bare vacuum due to quantum fluctuations, which manifests itself in the creation of electron-positron pairs. To make efficient use of the quantum resources available, the original problem is mapped to a spin model by eliminating the gauge fields [66] in favor of exotic long-range interactions, which have a direct and efficient implementation on an ion trap architecture [115]. The Schwinger mechanism of particle-antiparticle generation is explored by monitoring the mass production and the vacuum persistence amplitude. Moreover, the real-time evolution of entanglement in the system is tracked, which illustrates how particle creation and entanglement generation are directly related. This work represents a first step towards quantum simulating high-energy theories with atomic physics experiments, the long-term vision being the extension to real-time quantum simulations of non-Abelian lattice gauge theories.

This few-qubit demonstration is a first step towards simulating real time dynamics in gauge theories, which is fundamental for the understanding of many physical phenomena including the thermalization after heavy-ion collisions and pair creation studied at high-intensity laser facilities such as the ELI and the XCELS [58, 60]. While exist-

ing classical numerical methods such as Quantum Monte Carlo techniques have been remarkably successful for describing equilibrium phenomena, no systematic techniques exist to study the dynamical long-time behavior of all but very small systems. Quantum simulations aim at the long-term goal of solving the specific yet fundamental class of problems that currently cannot be tackled by these classical techniques. The digital approach employed here is based on the Hamiltonian formulation of gauge theories [14], and enables direct access to the system wavefunction. As I show below, this allows one to investigate quantities that are not accessible in high-energy experiments, such as entanglement generation during particle-antiparticle production. This emphasizes a novel perspective on the dynamics of the Schwinger mechanism [9].

Digital quantum simulations described here are conceptually different from, and fundamentally more challenging than, previously reported condensed matter-motivated simulations of spin and Hubbard-type models [11, 116, 117]. In gauge theories, local symmetries lead to the introduction of dynamical gauge fields obeying a Gauss law [60]. Formally, this crucial feature is described by local symmetry generators $\{\hat{G}_i\}$ that commute with the Hamiltonian of the system and restrict the dynamics to a subspace of physical states which satisfy:

$$\hat{G}_i |\Psi_{\text{physical}}\rangle = q_i |\Psi_{\text{physical}}\rangle, \quad (114)$$

where q_i are background (static) charges. We will be interested in the case $q_i = 0$ for all i (zero background charges).

Realizing such constrained dynamics on a quantum simulator is demanding and has been the focus of theoretical research [60, 62, 114, 118–121]. To optimally use the finite resources represented by a few qubits of existing quantum hardware, we encode the gauge degrees of freedom in a long-range interaction between the fermions, which can be implemented efficiently on our experimental platform. This allows us to explore quantum simulation of coherent real-time dynamics with four qubits, exemplified here by the creation of electron-positron pairs.

ENCODING OF THE SCHWINGER MODEL

We have studied in Chapter 4 the Kogut-Susskind formulation of the Schwinger model [13, 14], where it is discretized to a one-dimensional spatial lattice. As explained there, for realizing this model we map the fermions (particles and antiparticles) and gauge fields to a spin model. The particles and antiparticles are mapped to spin 1/2 particles on the sites of a one-dimensional lattice, whose states (up or down) represent the presence or absence of fermions, following the encoding depicted in Figure 40. The gauge fields, which are encoded in the links between the sites, are eliminated by a gauge transforma-

tion, as explained in Chapter 4. This procedure results in an effective long-range interaction that reflects the Coulomb interactions between the simulated particles. In this way we obtain, as in Eq. (81), a pure spin Hamiltonian involving only the fermionic degrees of freedom:

$$\begin{aligned} \hat{H}_S = & \frac{m}{2} \sum_{n=1}^N (-1)^n \hat{\sigma}_n^z + w \sum_{n=1}^{N-1} [\hat{\sigma}_n^+ \hat{\sigma}_{n+1}^- + \text{H.c.}] \\ & + J \sum_{n=1}^{N-1} \left[E_0 + \frac{1}{2} \sum_{m=1}^n [\hat{\sigma}_m^z + (-1)^m] \right]^2. \end{aligned} \quad (115)$$

The first term corresponds to the rest mass m of the fermions, and obtains a staggered sign because of the alternating placement of particles and antiparticles on the lattice. The second term corresponds to the creation and annihilation of particle-antiparticle pairs, and the third term reflects the energy stored in the electric field. Their energy scales $w = 1/(2a)$ and $J = g^2 a/2$ depend on the lattice spacing a and the fermion-light coupling constant g . We use natural units $\hbar = c = 1$; therefore, a and t have the dimension of length, while w , J , m and g have the dimension of inverse length.

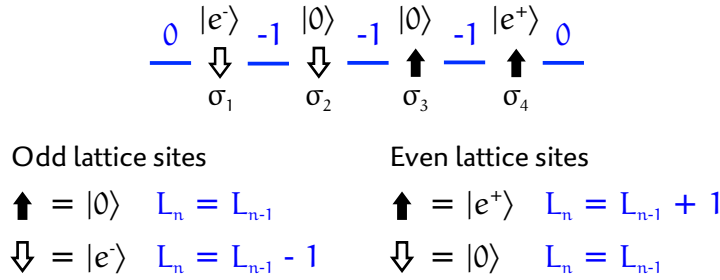


Figure 40: Encoding fermions in Wilson's lattice gauge theories into spins.

This encoding allows an efficient use of resources, since N spins can be used to simulate N particles and their accompanying $N - 1$ gauge fields. However, as shown in Figure 41, the required couplings and local terms have a very unusual distance and position dependence. The challenge has thus been moved from engineering a constrained dynamics of $2N - 1$ quantum systems on a gauge-invariant Hilbert space to the realization of an exotic and asymmetric interaction of N spins.

Our platform is ideally suited for this task, since long-range interactions and precise single qubit operations are available in trapped-ion systems. These capabilities allow us to realize the required interactions by means of a digital quantum simulation scheme, known as the Trotter scheme [12]. To this end, the desired Hamiltonian is split into parts that can be directly implemented and are applied separately in subsequent time windows, as explained in Section 2.5. By repeating the sequence multiple times, the resulting time evolution of the sys-

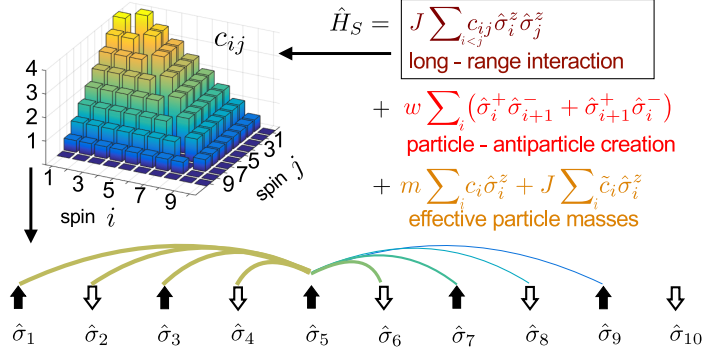


Figure 41: Effective long-range interactions emerging from the elimination of the gauge fields.

tem $U(t)$ closely resembles an evolution where the individual parts of the Hamiltonian act simultaneously.

The scheme is depicted in Figures 42 and 43. It allows for an efficient realization of the required dynamics and implements the coupling matrix of the long-range interactions (shown in Figure 41) with a minimal number of time steps, scaling only linearly in the number of sites N . The scheme is therefore scalable to larger systems. A discussion of finite size effects can be found in Section 8.7.

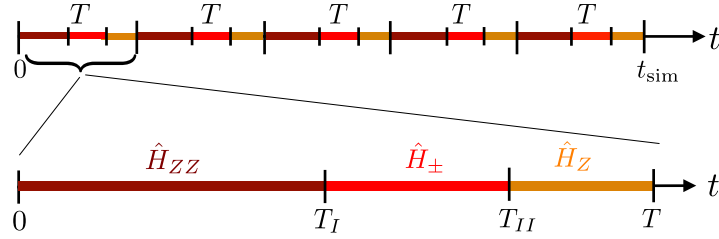


Figure 42: Time-discretization scheme for the digital quantum simulation of our model.

IMPLEMENTATION OF THE ENCODED SCHWINGER MODEL

The experimental platform for realizing the simulation is the trapped $^{40}\text{Ca}^+$ quantum information processor described in Chapter 2. There, each qubit is encoded in the electronic states $|\downarrow\rangle = 4^2S_{1/2}$ (with magnetic quantum number $m = -1/2$), $|\uparrow\rangle = 3^2D_{5/2}(m = -1/2)$ of a single ion. As explained in Section 2.4, a universal set of high-fidelity quantum operations is available, consisting of collective rotations around the equator of the Bloch sphere, addressed rotations around the Z axis and entangling MS gates [30]. With a sequence of these gates, arbitrary unitary operations can be implemented [18]. Thus, we are able to simulate the required interactions by means of digital quantum simulation techniques, as shown in Figure 42. Each of the implemented time evolutions consists of a sequence of over

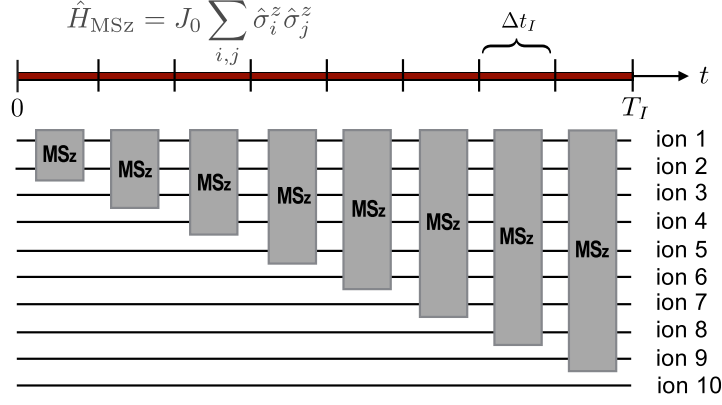


Figure 43: Implementation of the long-range interactions by means of MS gates.

200 quantum gates (see Figure 44). In order to realize the non-local interactions H_{ZZ} and $H_{\pm}$ with their specific long-range interactions, we use global MS entangling gates together with a spectroscopic decoupling method to tailor the range of the interaction. There, the population of the ions that are not involved in the specific operations are shelved into additional electronic states that are not affected by the light for the entangling operations (see Section 2.4). The local terms in H_z correspond to Z rotations that are directly available in our set of operations. The strength of all terms can be tuned by changing the duration of the laser pulses corresponding to the physical operations.

We implement the Hamiltonian $\hat{H}_S$ given in Eq. (115) by means of a digital quantum simulation scheme, as explained in Section 2.5. For convenience, we express the simulated Hamiltonian in the form

$$\hat{H}_S = \hat{H}_{ZZ} + \hat{H}_{\pm} + \hat{H}_Z, \quad (116)$$

where the three parts of the Hamiltonian correspond to the two different types of two-body couplings $\hat{H}_{ZZ}$ and $\hat{H}_{\pm}$, as well as local terms $\hat{H}_Z$,

$$\begin{aligned} \hat{H}_{ZZ} &= J \sum_{n < m} c_{nm} \hat{\sigma}_n^z \hat{\sigma}_m^z, \\ \hat{H}_{\pm} &= w \sum_n (\hat{\sigma}_n^+ \hat{\sigma}_{n+1}^- + \hat{\sigma}_{n+1}^+ \hat{\sigma}_n^-), \\ \hat{H}_Z &= m \sum_n c_n \hat{\sigma}_n^z + J \sum_n \tilde{c}_n \hat{\sigma}_n^z. \end{aligned}$$

The simulation protocol is based on time coarse-graining, where the desired dynamics of the Hamiltonian given by Eq. (115) is obtained within a time-averaged description. As illustrated in Figure 42, the total simulation time t_{sim} is divided into individual time windows of duration T . During each of these time windows, a full cycle of the protocol that is described below is performed. This cycle is repeated

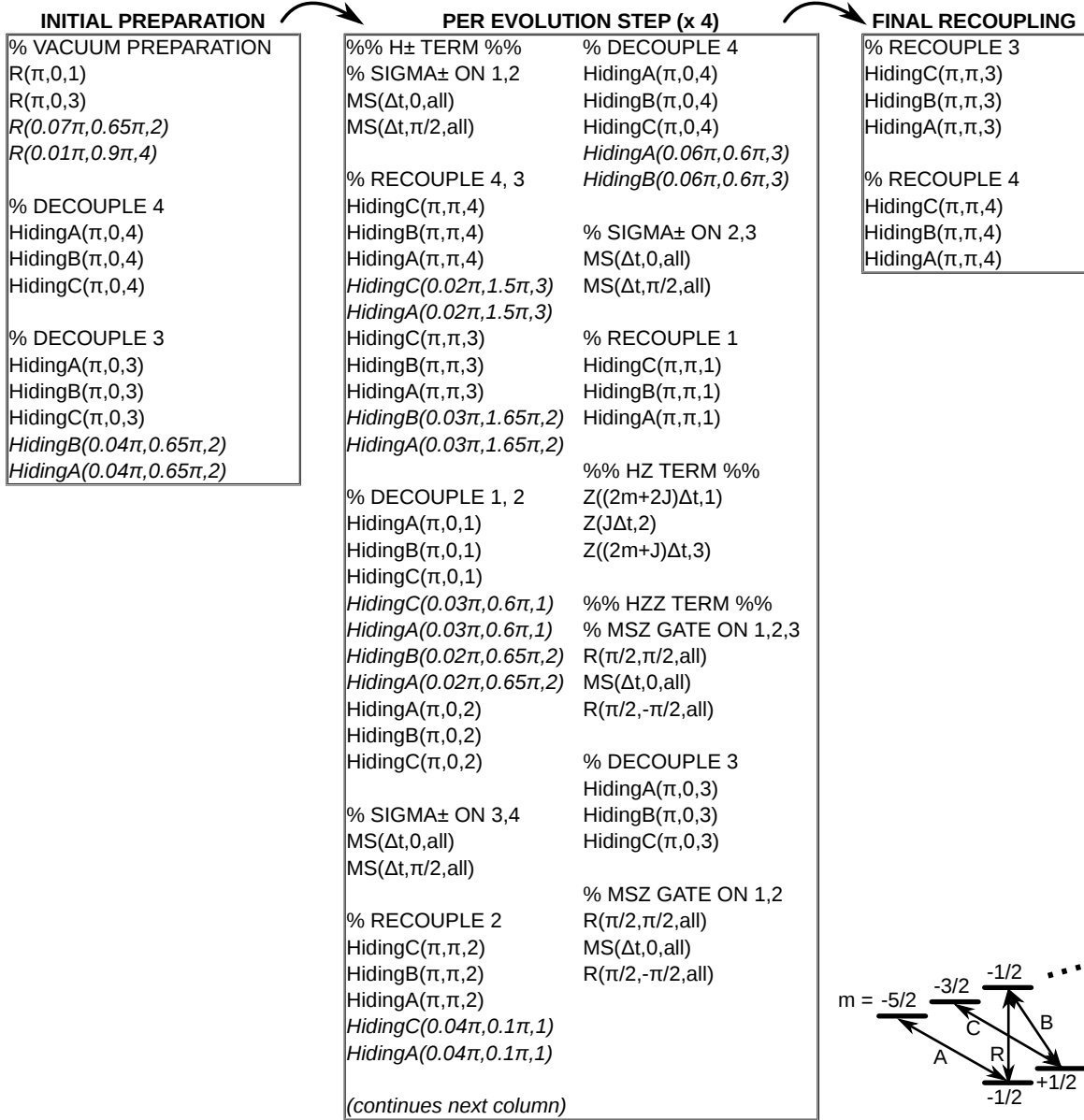


Figure 44: Experimental pulse sequence. The pulses are listed in the order in which they are applied. The operations shown in the middle box are repeated once per evolution step, resulting in a total number of $12 + 51 \times 4 + 6 = 222$ pulses for 4 evolution steps. The pulses are labeled in the form Pulse($\theta, \phi, \text{target qubit}$), where θ is the rotation angle (length) of the pulse, ϕ its phase, and the target qubit is an integer from 1 to 4 for addressed operations or “all” for global operations. “R” denotes a pulse on the qubit transition $4S_{1/2}(m = -1/2)$ to $3D_{5/2}(m = -1/2)$. “MS” corresponds to a Mølmer-Sørensen gate on the same transition. The hiding pulses “HidingA,B,C” are applied on the transitions: A) $4S_{1/2}(m = -1/2)$ to $3D_{5/2}(m = -5/2)$, B) $4S_{1/2}(m = +1/2)$ to $3D_{5/2}(m = -1/2)$, C) $4S_{1/2}(m = +1/2)$ to $3D_{5/2}(m = -3/2)$. The pulses shown in italics serve the purpose of correcting addressing crosstalk.

multiple times from $t = 0$ to $t = t_{\text{sim}}$ and consists of three sections. Each of these sections corresponds to one of the three parts of the desired Hamiltonian given by Eq. (116). In the first section, $\hat{H}_{ZZ}$ is simulated, in the second, the nearest neighbor terms $\hat{H}_{\pm}$ are realized and in the third, the single particle rotations $\hat{H}_Z$ are performed. In this way, the simulation scheme uses only two types of interactions, local rotations and an infinite-range entangling operation

$$\hat{H}_{\text{MSX}} = J_0 \sum_{n,m} \hat{\sigma}_n^x \hat{\sigma}_m^x, \quad (117)$$

which is routinely implemented in trapped ions by means of MS gates [30]. Below, we explain how the individual parts of the encoded Kogut-Susskind Hamiltonian (115) are realized.

Long-range interactions $\hat{H}_{ZZ}$

The first part of Eq. (116) originates from the third term in Eq. (115) representing the electric-field energy. It takes the form

$$\hat{H}_{ZZ} = \frac{J}{2} \sum_{m=1}^{N-2} \sum_{n=m+1}^{N-1} (N-n) \hat{\sigma}_m^z \hat{\sigma}_n^z, \quad (118)$$

and describes two-body interactions with an asymmetric distance dependence, where each spin interacts with constant strength with all spins to its left, while the coupling to the spins on its right decreases linearly with distance (see Figure 41). As the number of elements in the spin coupling matrix is proportional to N^2 , a brute force digital simulation approach to this problem would require N^2 time steps. Using our protocol, which is inspired by techniques put forward in [122], the required resources scale only linearly in N . This is accomplished using the scheme illustrated in Figure 42. We introduce $N-2$ time windows, which can be shown to be the minimal number of time steps required to simulate the Hamiltonian in Eq. (118). Each elementary time window has length Δt_I . In the n -th time window, the Hamiltonian

$$\hat{H}_{\text{MSZ}}^{(n)} = J_0 \sum_{i,j}^{n+1} \hat{\sigma}_i^z \hat{\sigma}_j^z \quad (119)$$

is applied. $\hat{H}_{\text{MSZ}}^{(n)}$ is realized by applying the Hamiltonian given in Eq. (117) in combination with local rotations, $R(y) \hat{H}_{\text{MSX}} R^\dagger(y) = \hat{H}_{\text{MSZ}}$, where $R(y) = \exp(i\frac{\pi}{4} \sum_{i=1}^N \hat{\sigma}_i^y)$. The resulting time-averaged Hamiltonian for the first section of the time interval T ,

$$\bar{H}_I = \frac{1}{N-2} \sum_{n=1}^{N-2} \hat{H}_{\text{MSZ}}^{(n)} \quad (120)$$

is proportional to the desired Hamiltonian in Eq. (118),

$$\bar{H}_I = \frac{2}{N-2} \frac{J_0}{J} H_{ZZ}. \quad (121)$$

As shown in Figure 43, only ions 1 to $n+1$ participate in the entangling interaction in time step n . Since the interaction is implemented via a global beam that couples to the entire ion string, ions $n+2$ to N are decoupled by applying hiding pulses, as explained in Section 2.4. The population in the qubit states of these ions is transferred to electronic levels that are not affected by the interaction using suitable laser pulses. The population in the state $|\downarrow\rangle = 4S_{1/2}$ (magnetic number $m = -1/2$) is transferred to the state $3D_{5/2}$ ($m = -5/2$), and the population in $|\uparrow\rangle = 3D_{5/2}$ ($m = -1/2$) is transferred to the state $3D_{5/2}$ ($m = -3/2$) via $4S_{1/2}$ ($m = +1/2$).

Nearest neighbor terms $\hat{H}_\pm$

The second part of Eq. (116),

$$\hat{H}_\pm = w \sum_{n=1}^{N-1} (\hat{\sigma}_n^+ \hat{\sigma}_{n+1}^- + \text{H.c.}) \quad (122)$$

corresponds to the creation and annihilation of particle-antiparticle pairs. For realizing this Hamiltonian, the interaction given in Eq. (117) needs to be modified not only in range, but also regarding the type of coupling. This is accomplished by dividing the time window dedicated to realizing $\hat{H}_\pm$ into $N-1$ elementary time slots of length Δt_{II} . Each of these is used for inducing the required type of interaction between a specific pair of neighboring ions. For example, the first elementary time slot of length Δt_{II} is used to engineer an interaction of the type $\hat{H}_{ij} \propto \hat{\sigma}_i^+ \sigma_j^- + \text{H.c.}$ between the first and the second spin, the second time slot is used to do the same for the second and the third spin, and so on. This can be done by applying suitable hiding pulses, to all spins except for a selected pair of ions i and j . The selected pair undergoes a sequence of gates, which transforms the $\hat{\sigma}_i^x \hat{\sigma}_j^x$ -type coupling in Eq. (117) into an interaction of the required form and consists of four steps:

1. a single qubit operation on the two selected spins i and j ,

$$U = e^{i\frac{\pi}{4}(\hat{\sigma}_i^z + \hat{\sigma}_j^z)}$$
2. an evolution under the Hamiltonian given in Eq. (117) for the selected pair of spins, $\hat{H}_{MSX}^{(ij)}$ during a time $\Delta t_{II}/2$, $e^{-i\hat{H}_{MSX}^{(ij)}\Delta t_{II}/2}$
3. another single qubit operation $U^\dagger = e^{-i\frac{\pi}{4}(\hat{\sigma}_i^z + \hat{\sigma}_j^z)}$ and finally
4. another two-qubit gate $e^{i\hat{H}_{MSX}^{(ij)}\Delta t_{II}/2}$.

The time evolution operator associated with the described sequence of gates is given by $e^{iH_{II}^{(ij)}\Delta t_{II}}$ with

$$\hat{H}_{II}^{(ij)} = \frac{1}{2} \left(\hat{H}_{MSx}^{(ij)} + U^\dagger \hat{H}_{MSx}^{(ij)} U \right) \quad (123)$$

$$= J_0 \left(\hat{\sigma}_i^+ \hat{\sigma}_j^- + \text{H.c.} \right), \quad (124)$$

as desired. The relative strength of the nearest neighbor terms $\hat{H}_\pm$ and the long-range couplings $\hat{H}_{ZZ}$, w/J can be adjusted by tuning the ratio of the lengths of the elementary time windows Δ_{II}/Δ_I .

Single particle terms $\hat{H}_Z$

The last contribution to the Hamiltonian in Eq. (116) consists of two terms $\hat{H}_Z = m \sum_n c_n \hat{\sigma}_n^z + J \sum_n \tilde{c}_n \hat{\sigma}_n^z$. The first term in this expression reflects the rest masses of the fermions. The second term is an effective single-particle contribution originating from the third part of Eq. (115) and corresponds to a change in the effective fermion masses due to the elimination of the electric fields. The local terms of the simulated Hamiltonian are given by

$$\hat{H}_Z = \frac{m}{2} \sum_{n=1}^N (-1)^n \hat{\sigma}_n^z - \frac{J}{2} \sum_{n=1}^{N-1} (n \bmod 2) \sum_{l=1}^n \hat{\sigma}_l^z.$$

These are implemented by means of AC-Stark shifts, induced by laser pulses that are about 20 MHz red-detuned from the qubit transition [18, 115].

MEASUREMENT AND POSTSELECTION

For each set of system parameters and number of simulation time steps, we perform a full state tomography to determine the density matrix that corresponds to the quantum state of the system. The electronic state of the ions is detected via a fluorescence measurement using the electron shelving technique [18]. The entire string is imaged by a charge coupled device (CCD) camera, performing a full projective measurement in the Z basis. This procedure is repeated 100 times to gather sufficient statistics.

As a consequence of charge conservation, an equal number of particles and antiparticles is created during the ideal dynamics of the

system. Since our evolution starts with the vacuum state, the physical Hilbert space of the simulation is spanned by the six states:

$$|\uparrow\downarrow\uparrow\downarrow\rangle = |0000\rangle \quad (125)$$

$$|\downarrow\uparrow\uparrow\downarrow\rangle = |e^-e^+00\rangle \quad (126)$$

$$|\uparrow\uparrow\downarrow\downarrow\rangle = |0e^+e^-0\rangle \quad (127)$$

$$|\uparrow\downarrow\downarrow\uparrow\rangle = |00e^-e^+\rangle \quad (128)$$

$$|\downarrow\downarrow\uparrow\uparrow\rangle = |e^-00e^+\rangle \quad (129)$$

$$|\downarrow\uparrow\downarrow\uparrow\rangle = |e^-e^+e^-e^+\rangle, \quad (130)$$

where $|0\rangle$ denotes the vacuum, $|e^- \rangle$ a particle and $|e^+ \rangle$ an antiparticle. However, experimental errors during the simulation produce leakage from this subspace, such that nonphysical states like $|e^-000\rangle = |\downarrow\downarrow\uparrow\downarrow\rangle$ get populated. Therefore, the raw measured density matrices ρ_{raw} are projected onto the Hilbert space spanned by the physical states and normalized,

$$\rho_{\text{phys}} = \frac{P\rho_{\text{raw}}P}{\text{tr}(P\rho_{\text{raw}}P)},$$

where P is the projector onto the physical subspace. All experimental data presented in this work correspond to physical density matrices ρ_{phys} postselected in this way.

EXPERIMENTAL RESULTS

To simulate the dynamics of pair creation we consider, as is usual [9, 113], the *bare vacuum* as initial state, where matter is completely absent, $|\text{vacuum}\rangle = |0000\rangle$. In the spin representation this state is given by $|\uparrow\downarrow\uparrow\downarrow\rangle$ accordingly. Note that the bare vacuum is different from the *dressed vacuum state*, which is the ground state of the full Hamiltonian.

After initializing the system in this state, which corresponds to the ground state for $m \rightarrow \infty$ (see Fig. 45(a)), we apply the Hamiltonian $\hat{H}_S$ for different masses and coupling strengths. As a first step, we measure the particle number density

$$\nu(t) = \frac{1}{2N} \sum_{l=1}^N (-1)^l \langle \hat{\sigma}_l^z(t) \rangle + 1 \quad (131)$$

generated after a simulated time evolution of duration t . The value $\nu = 1/2$ corresponds to a state containing on average one pair (see Figure 40). As Fig. 45c shows, an initial phase of rapid pair creation is followed by a reduction of $\nu(t)$ due to recombination effects. The measured evolution shows excellent agreement with theoretical predictions, assuming uncorrelated dephasing with an error probability $p = 0.038$ per qubit and per step, as explained in Section 8.6.

In Fig. 45b, we probe the particle-antiparticle generation for a broad range of masses m . Larger values of m increase the energy cost of pair production and thus lead to faster oscillations with a suppressed magnitude.

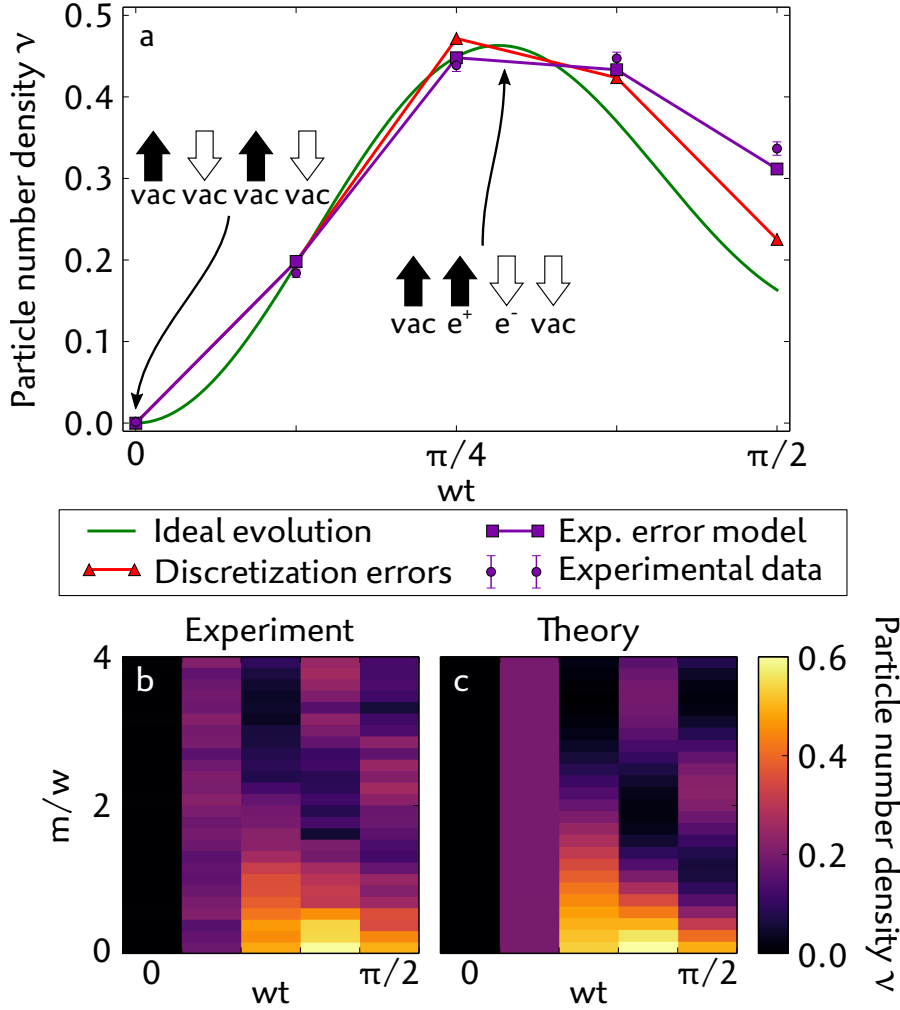


Figure 45: Time evolution of the particle number density ν . (a) We show the ideal evolution under the Schwinger Hamiltonian $\hat{H}_S$, the ideal evolution using discrete time steps, the expected evolution including an experimental error model (see Section 8.6) and the experimental data for electric field energy $J = w$ and particle mass $m = 0.5w$. After postselection of the experimental data, the remaining populations are $\{86 \pm 2, 79 \pm 1, 73 \pm 1, 69 \pm 1\}\%$ after $\{1, 2, 3, 4\}$ time steps (averaged over all datasets). Error bars correspond to standard deviations estimated from a Monte Carlo bootstrapping procedure. The insets show the initial state of the simulation, corresponding to the bare vacuum with particle number density $\nu = 0$, as well as one example of a state containing one pair, i.e. a state with $\nu = 0.5$. (b) Experimental data and (c) theoretical prediction for the evolution of the particle number density ν as a function of the dimensionless time wt and the dimensionless particle mass m/w , with $J = w$.

Our platform allows direct measurements of the vacuum persistence amplitude and of the generated entanglement. The natural quantity characterizing the decay of the unstable vacuum is the vacuum persistence amplitude, introduced by J. Schwinger [54], which is defined as the overlap of the initial state $|\Psi(0)\rangle = |\text{vacuum}\rangle$ with the time-evolved state:

$$G(t) = \langle \text{vacuum} | e^{-i\hat{H}_S t} | \text{vacuum} \rangle. \quad (132)$$

The associated probability $|G(t)|^2$ shown in Fig. 46a,c, also known as the Loschmidt echo, is important in contexts such as quantum chaos [123] and dynamical critical phenomena far from equilibrium [124].

In its original formulation, the Schwinger mechanism was considered for the continuum system and a classical electric field of strength E [54]. There, it has been shown that the particle number density $\nu(t)$ is directly related to the rate function $\lambda(t)$, that characterizes the decay of the vacuum persistence probability $|G(t)|^2$,

$$\lambda(t) = - \lim_{N \rightarrow \infty} \frac{1}{N} \log \left[|G(t)|^2 \right]. \quad (133)$$

Specifically, in the limit of large fermion masses $m \gg \sqrt{qE}$ with q the electric charge, as relevant in the high-energy context, $\lambda(t) = \nu(t)$ for thermodynamically large systems in the continuum.

Since vacuum persistence amplitudes have so far not been measured, this connection between $\lambda(t)$ and $\nu(t)$ has not yet been tested experimentally. In Figure 47, we show the measured rate function $\lambda(t)$ and find good qualitative agreement with $\nu(t)$, even for the few qubits in our digital quantum simulation.

The vacuum decay continuously produces entanglement, as particles and antiparticles are constantly generated and propagate away from each other, thus correlating distant parts of the system. Entanglement plays a crucial role in the characterization of dynamical processes in quantum many-body systems, and its analysis permits us to quantify the quantum character of the generated correlations. To this end, we reconstruct the density matrix after each time step by full state tomography, and evaluate the entanglement of one half of the system with the other by calculating the logarithmic negativity. This quantity is an entanglement measure for mixed states [125], which is defined as the sum of the negative eigenvalues of the partially transposed density matrix. The entanglement between two contiguous blocks of our spin system is equivalent to the entanglement in the simulated fermionic system described by Eq. (115), i.e. including the gauge fields [126].

In Fig. 46b,d, we show the real-time dynamics of the logarithmic negativity for different parameter regimes. Entanglement between the

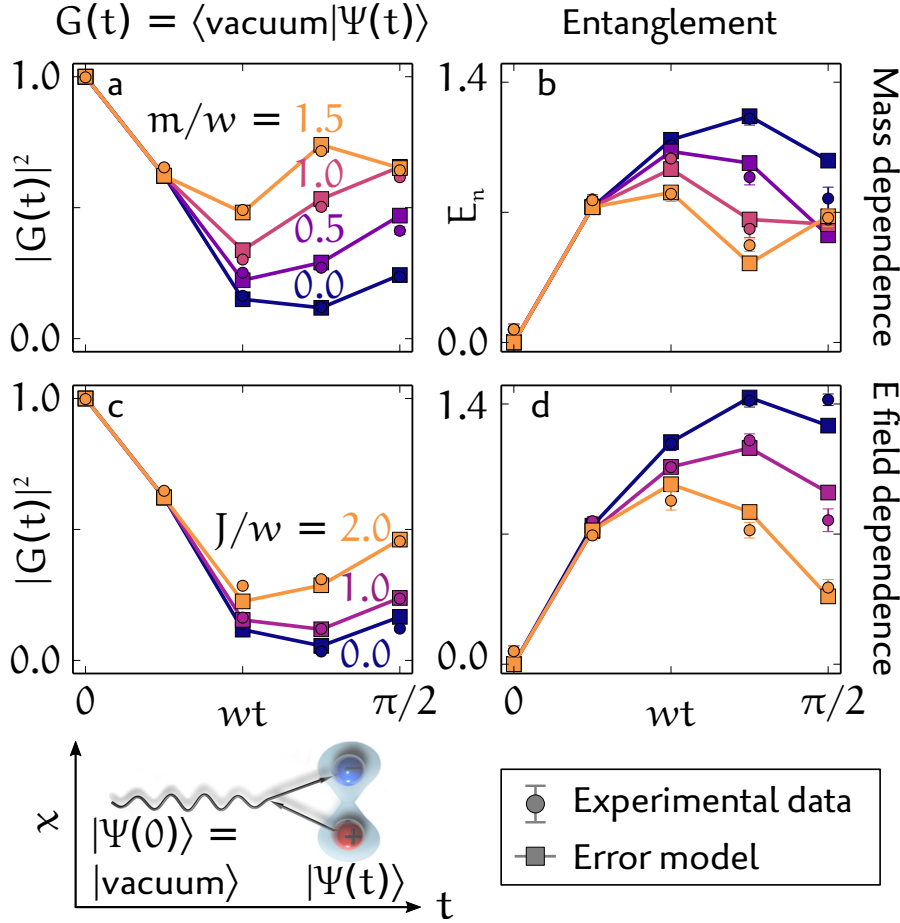


Figure 46: Time evolution of the vacuum persistence amplitude and entanglement. We show the square of the vacuum persistence amplitude $|G(t)|^2$ (the Loschmidt echo), which quantifies the decay of the unstable vacuum, and the logarithmic negativity E_n , a measure of the entanglement between the left and right half of the system. Panels (a) and (b) show the time evolution of these quantities for different values of the particle mass m and fixed electric field energy $J = w$, where w is the rate of particle-antiparticle creation and annihilation. Panels (c) and (d) show how the time evolution of $|G(t)|^2$ and E_n changes for different values of J and fixed particle mass $m = 0$. Circles correspond to the experimental data and squares connected by solid lines to the expected evolution assuming an experimental error model explained in Section 8.6. Error bars correspond to standard deviations estimated from a Monte Carlo bootstrapping procedure.

two halves of the system is due to the presence of a pair distributed across them. Accordingly, less entanglement is produced for increasing particle masses m and field energies J . The latter has a stronger influence, as it not only raises the energy cost for the creation of a pair, but also for increasing the distance between particle and antiparticle.

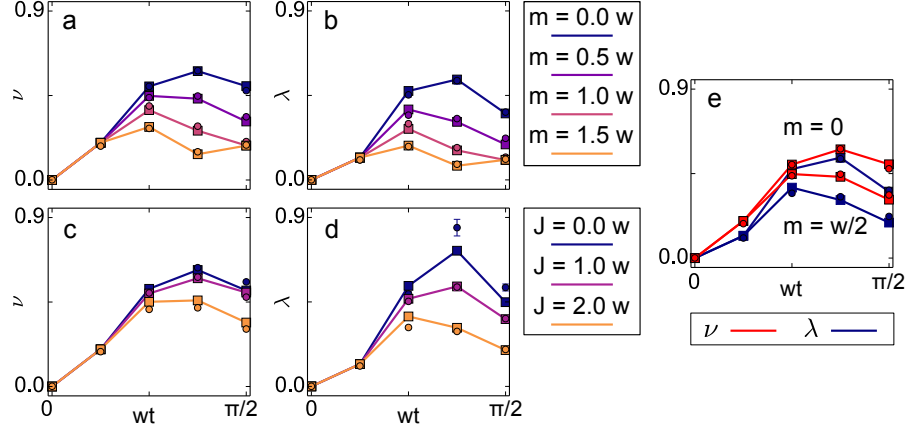


Figure 47: Comparison of the evolutions of the particle number density $\nu(t)$ and the rate function $\lambda(t)$. The decay of the vacuum persistence probability is characterized by the rate function $\lambda(t)$, defined by $|G(t)|^2 = e^{-N\lambda(t)}$. Panels (a) and (b) show the time evolution of these quantities for different values of the particle mass m and fixed electric field energy $J = w$, where w is the rate of particle-antiparticle creation and annihilation. Panels (c) and (d) show the evolution of $\nu(t)$ and $\lambda(t)$ for different values of J and fixed particle mass $m = 0$ as a function of the dimensionless time wt . Panel (e) compares the evolutions of $\nu(t)$ and $\lambda(t)$ for $J = w$ and masses $m = 0$ (upper two curves) and $m = w/2$ (lower two curves). Error bars correspond to standard deviations estimated from a Monte Carlo bootstrapping procedure.

EXPERIMENTAL ERRORS

The bulk of the quantum gates in the simulation consists of hiding/unhiding pulses and MS gates (see Figure 44). Each π pulse on a hiding transition has a fidelity of around 99.5%, and there are 30 such pulses per step, yielding a lower bound on the fidelity per step of $(0.995)^{30} = 0.86$. The fidelity of a fully-entangling ($\pi/2$) MS gate on 4 ions is around 97.5%, and one simulation step has 8 quarter-entangling ($\pi/8$) gates, yielding a lower bound of $(0.975)^{8/4} = 0.95$. The total lower bound for the fidelity per step is $\mathcal{F} = (0.995)^{30} \cdot (0.975)^{8/4} = 76\%$; it is indeed lower than the average fidelity of the raw (not postselected) state after the first step, which is 89%. The sequence performs better than might be expected from the raw fidelities; this is probably owing to the fact that the ideal evolution stays at all times in a decoherence-free subspace.

A useful measure of the performance of the evolution is the population leakage from the physical subspace. After $\{1, 2, 3, 4\}$ evolution time steps, the measured populations remaining in the physical subspace were on average $\{86 \pm 2, 79 \pm 1, 73 \pm 1, 69 \pm 1\}\%$ of the populations before postselection (the average is taken over the 7 simulation runs shown in the paper). Comparing the performance of the first simulation step with the total infidelity of the hiding/unhiding oper-

ations, the population loss per simulation step seems consistent with it.

The remaining errors can be quantified by the average fidelity of the postselected state with the ideal state. After the first evolution step this is 96%, which is consistent with the total fidelity of the MS gates. To quantify the performance of the simulation along the whole evolution, we compare the experimental data to a simple phenomenological error model. Since the postselection already partially corrects for population errors, an error model that consists of uncorrelated dephasing was considered, parameterized with an phase flip error probability p per qubit and per evolution time step. The density matrix ρ is then, at each evolution step, subject to the composition of the error channels $\mathcal{E}_i$ for each qubit,

$$\rho \rightarrow \mathcal{E}_4 \circ \mathcal{E}_3 \circ \mathcal{E}_2 \circ \mathcal{E}_1(\rho), \text{ where:} \\ \mathcal{E}_i(\rho) = (1 - p)\rho + p\sigma_i^z \rho \sigma_i^z.$$

The value for the error probability p was extracted from a fit to all of the experimental data collected. For all the data taken with nonzero J a value of $p = 0.038$ is found. Whenever $J = 0$, the simulation does not require any ZZ interactions. Thus, several entangling gates are omitted from the sequence and consequently higher fidelities are expected. Indeed, for this case the error probability per time step was found to be $p = 0.031$.

FINITE SIZE EFFECTS

In the following, the dependence of the results on the number of lattice sites N is discussed. Figure 48 shows the time evolution of the particle number density and the entanglement for different system sizes N .

Already for our experimental system with $N = 4$, there is qualitative agreement with respect to the results expected for larger N . By scaling up the system, the dynamics quickly converges for the considered parameters. The continuum limit $a \rightarrow 0$, $N \rightarrow \infty$ for fixed values of the coupling g and the mass m is addressed in a manuscript in preparation [126].

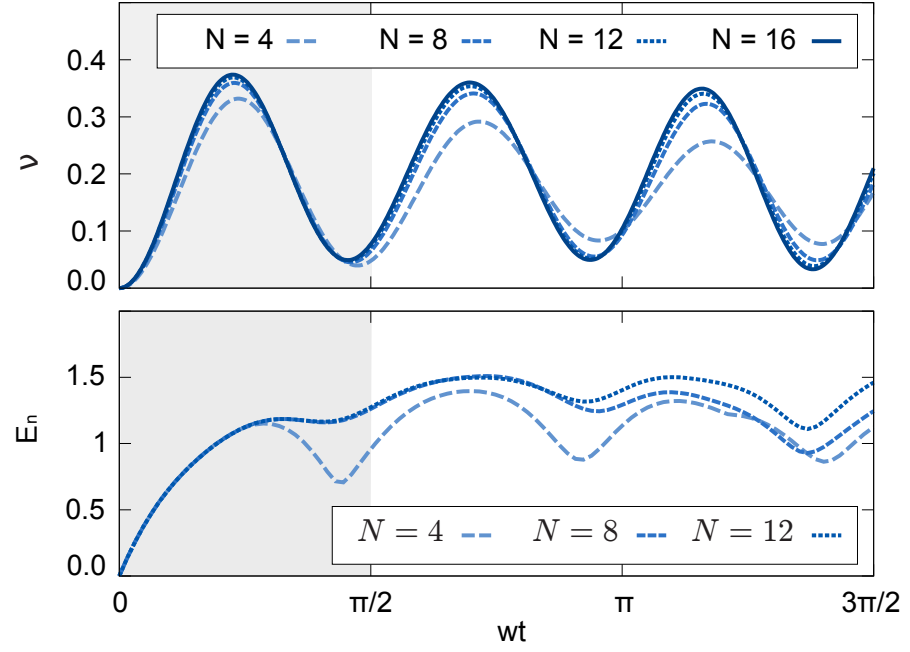


Figure 48: Evolution of the particle number density ν and the logarithmic negativity E_n for different system sizes N . The logarithmic negativity is evaluated with respect to a cut in the middle of the considered spin chain and quantifies the entanglement between the two halves of the system. Both quantities are shown as a function of the dimensionless time wt for $J = m = w$. The shaded area corresponds to the time interval explored in the experiment.

SIMULATION OF A QUANTUM LINK MODEL

Quantum link models (QLMs), as already introduced in Chapter 4, are lattice gauge theories (LGTs) where the degrees of freedom of both the fermions and the gauge fields are encoded as spins [65, 127, 128]. QLMs provide a non-perturbative formulation of dynamical gauge field theories in particle physics [65, 129, 130]. Moreover, they are also relevant for the study of condensed matter systems that cannot be treated by perturbative methods, such as spin liquids and frustrated systems [131–133]. In this chapter, the experimental simulation of a QLM is reported, following the proposal in Ref. [120] and adapting it to an ion trap quantum information processor. In Section 9.1, the model to simulate is described: QED in one spatial dimension. Then, in Section 9.2 the experimental implementation of the simulation and its results are shown.

THE SCHWINGER MODEL

The concrete QLM we consider describes QED in $1 + 1$ dimensions (the *Schwinger model*): a single species of fermions in a one-dimensional lattice coupled to the electric field, as depicted in Figure 49. We have also studied this model in Chapter 8, encoding the gauge fields as long-range interactions. Here, instead, we encode the gauge fields as spins on a lattice, and will also track them dynamically. This approach is more flexible than the encoding used in Chapter 8, and can be applied to any lattice gauge theory. However, it has the disadvantage that additional qubits are required to simulate the same number of fermionic lattice sites; owing to the additional ones that are required for the gauge fields.

The spins that encode the fermions occupy every second site in the lattice, and the spins corresponding to the gauge fields are located between the fermions. The odd fermionic sites correspond to particles and the even sites to antiparticles. The fermions we will consider have only one degree of freedom per lattice site and will be represented by a single spin $1/2$ particle ψ , whose two states represent the presence or absence of a particle. In our particular implementation, the gauge fields will be represented by particles U of spin $1/2$, whose state represents the value of the field. For simulating a more realistic field, one would need to use spin- J particles for the gauge fields, and in the limit $J \rightarrow \infty$ one would recover a continuously-valued field. A lattice with L sites can be represented with $2L + 1$ particles of the appropriate spins: L spin $1/2$ particles for the sites plus $L - 1$ spin J

particles for the links. Each spin- J particle can also be represented as a system of $2J$ qubits.

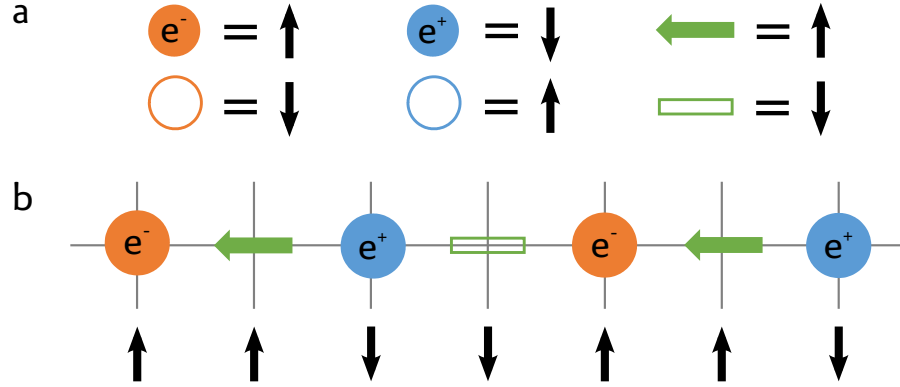


Figure 49: a) Encoding of the fermions and gauge fields into spins $1/2$ ($|\uparrow\rangle$ and $|\downarrow\rangle$). b) An example of a 1D lattice for a minimal QLM.

Our model is described by the Hamiltonian (74) derived in Chapter 4:

$$H = \frac{1}{2a} \sum_n [\sigma^+(n) e^{i\theta(n)} \sigma^-(n+1) + \text{H.c.}] + \\ + m \sum_n (-1)^n \left(\frac{1 + \sigma^z(n)}{2} \right) + \frac{g^2 a}{2} \sum_n L^2(n), \quad (134)$$

where the sums are taken over the fermionic lattice sites n , and a is the lattice spacing. The first term consists of three-body interactions with coupling

$$k = \frac{1}{2a} \quad (135)$$

that induce tunneling of fermions from one site to the next, increasing or reducing the value of the field L between these sites by one unit. The second is a mass term, where m is the fermion mass, which has opposite signs for odd and even fermionic sites, corresponding to particles and antiparticles. The last term is the self-energy of the fields, where g is the gauge coupling.

The minimal instance of this model requires three spins- $1/2$ for simulation: a particle at lattice site 1, an antiparticle at lattice site 3 and a gauge field in between, at lattice site 2. The only physical states allowed by Gauss' law in this minimal system are either a particle-antiparticle pair with a gauge field in the middle, or the *vacuum*, without any particles nor field. The encoding of these states are depicted in Figure 50. The interaction induces tunneling between these two states with strength k , and the states have a relative energy difference given by the mass m of the particles. In this model the field energy would effectively only add to this detuning, and can be absorbed by a redefinition of the mass. Therefore, in what follows we set $g = 0$.

The dynamics of the system in terms of the spins are then given by the Hamiltonian:

$$H = k\sigma_1^+\sigma_2^+\sigma_3^- + \text{H.c.} - \frac{m}{2}(\sigma_1^z - \sigma_3^z). \quad (136)$$

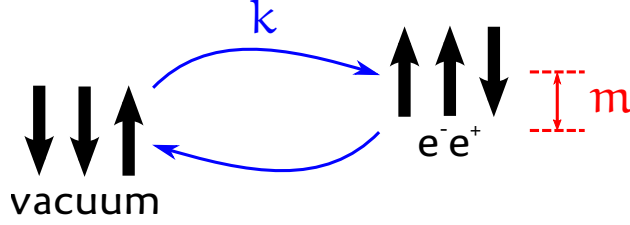


Figure 50: The two physical states of our minimal QLM.

This model is effectively a two-level system spanned by the states $|\downarrow\downarrow\uparrow\rangle$ (vacuum) and $|\uparrow\uparrow\downarrow\rangle$ (e^-e^+ pair). Figure 51 shows the expected dynamics of the system. If the interaction is turned on, one should observe oscillations between the vacuum state and the e^-e^+ state, equivalent to detuned Rabi oscillations. These dynamics simulate the creation of particle-antiparticle pairs from vacuum fluctuations [134]. For $m = 0$ the excitation of the e^-e^+ state should reach 1, whereas for $m > 0$ there is an energy cost to create massive particles, and thus the maximum population of the excited state decreases. The added energy detuning also increases the frequency of the oscillations. Explicitly, the frequency of the oscillations is given by:

$$\Omega = \sqrt{k^2 + m^2}, \quad (137)$$

and their amplitude (the maximum e^-e^+ state population) by:

$$A = \frac{k^2}{\Omega^2}. \quad (138)$$

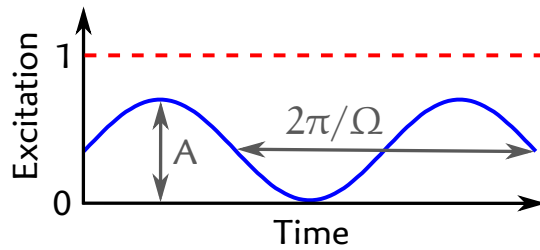


Figure 51: Excitation of the e^-e^+ state as a function of time.

EXPERIMENTAL IMPLEMENTATION AND RESULTS

The experiment carried out is a simulation of the three-ion model explained in Section 9.1. Each time step of the interaction was implemented using the sequence of laser pulses shown in Figure 52. The mass term corresponds to a rotation around the Z axis and was implemented with an addressed off-resonant pulse, as explained in Section 2.4, where the value of the mass corresponds to the length of the pulse. For 7 different values of the mass m in the range from 0 to $1.5k$ an increasing number of evolution steps of fixed length was applied and the populations of the vacuum state and the e^+e^- state were measured. These two states are the only valid states allowed by Gauss' law, so we can postselect results that belong to the Hilbert space spanned by these. After 6 steps, consisting of 24 entangling gates, the population of the valid subspace was over 60%. The evolution of the populations is shown in Figure 53 for different values of the mass. As can be seen, the amplitude of the oscillations decreases and their frequency increases for increasing mass, in agreement with the theory predictions (compare with Figure 51).

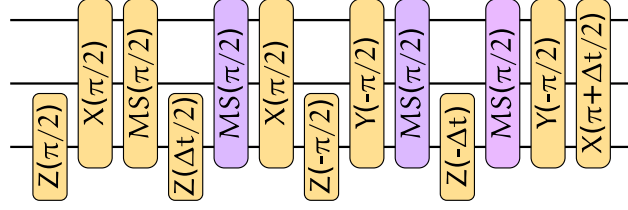


Figure 52: Pulse sequence for the experimental implementation of the QLM simulation.

In order to quantify the dynamics of the system for different masses, a theoretical model was fitted to the measured data consisting of damped oscillations with steady state value 0.5. This model describes an effective depolarizing noise in our system. The parameters extracted from such fits are plotted as a function of the mass in Figure 54. The qualitative dependence of the fitted parameters on the mass predicted by the theory can be clearly observed. However, there seems to be a systematic shift in the observed parameters, with frequencies appearing to be lower and amplitudes bigger than expected. The reason for this is not yet fully clear. At the time of the experiment, a systematic frequency shift on the order of 100 Hz was found between the middle ion and the outer ions, which originates from the quadrupole shift of the $D_{5/2}(m = -1/2)$ state. This shift could be a source of systematic errors.

In the next months, further experiments on QLMs are planned with four ions. The model to be simulated consists of a fermion-antifermion pair and two gauge fields with periodic boundary conditions, as depicted in Figure 55. This model has a richer Hilbert

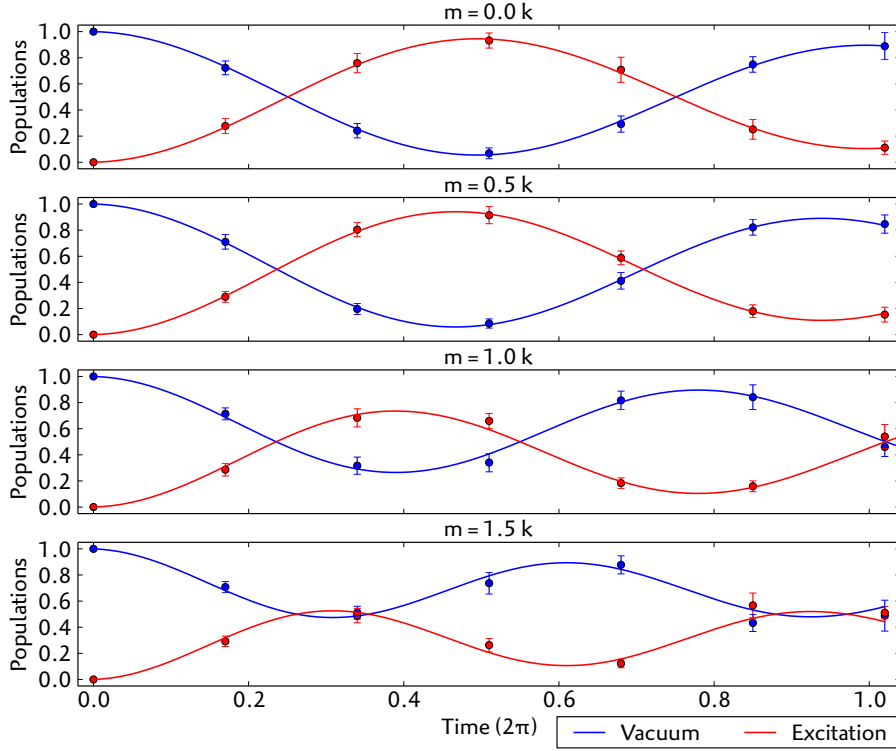


Figure 53: Discretized time evolutions for masses = $\{0, 0.5, 1, 1.5\}$. Dots: experimental data, solid lines: fit from theoretical model.

space than the already simulated one, since it has three physically allowable states: the vacuum, and a particle-antiparticle pair with either gauge field excited. Moreover, periodic boundary conditions are convenient from a theoretical point of view to avoid boundary effects in the simulation.

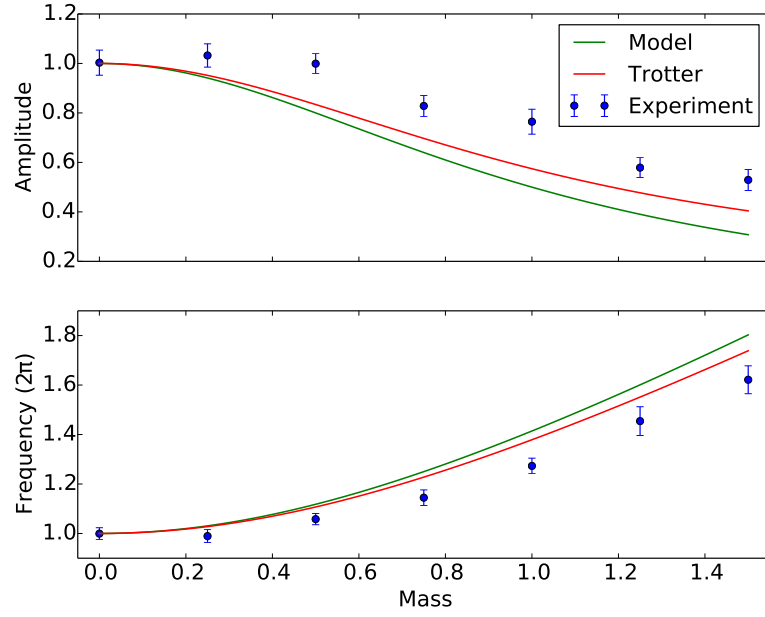


Figure 54: Observed evolution parameters as a function of the mass. Green: exact theoretical model, red: theoretical model including errors coming from time discretization, blue: experimental data from fit parameters.

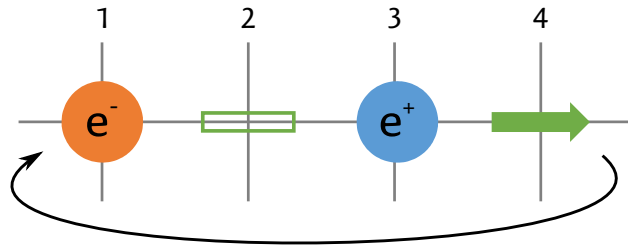


Figure 55: Quantum link model with periodic boundary conditions, consisting of a fermion-antifermion pair and two gauge fields. The periodic boundary conditions are implemented by carrying out interaction steps between sites $\{1, 2, 3\}$ and $\{3, 4, 1\}$.

SUMMARY AND OUTLOOK

So long, and thanks.

—Douglas Adams, *So Long, and Thanks for All the Fish* [135]

In this thesis, recent contributions to experimental quantum information processing with trapped ions have been presented, consisting of both technical developments and experiments. The experiments shown in this thesis explore the applications of quantum technologies in two directions: computation (Shor’s algorithm, Chapter 7 and simulation (lattice gauge theories, Chapters 8 and 9).

The quantum compiler explained in Chapter 5 has proven to be a useful tool in several recent experiments, for instance those reported in Refs. [18, 92, 136]. This compiler is particularly suitable for optimizing sequences for error correction experiments and state and process tomographies. Further improvements to the compiler are desirable: the capability to consider spectroscopic decoupling of qubits, and the optimization of sequences with respect to experimental noise sources. For instance, the compilation process could attempt to maximize the time spent in decoherence-free subspaces during a sequence, or otherwise favor spin-echo-like sequences to improve coherence. Such features would greatly improve the usefulness of this tool. Moreover, some fundamental questions remain open: Is there an analytical procedure to compile general quantum unitaries in terms of multi-qubit gates, as there is for two-qubit gates? Which unitaries are “easy” and which are “hard” to implement using such gates? Answers to this questions would be, not only of fundamental interest for quantum information theory, but also of great practical importance for finding efficient implementations of quantum operations.

The scalable implementation of Shor’s algorithm, explained in Chapter 7, is the first demonstration of the algorithm without requiring previous knowledge of the answer. Namely, all meaningful combinations of the gates required to implement Shor’s algorithm were tested without any unfair optimization.

The experiments described in Chapters 8 and 9 are the first quantum simulation of a lattice gauge theory. Such theories are fundamental to understanding interactions between elementary particles, but studying their real-time dynamics for large system sizes is not feasible on classical computers. These experiments show that quantum simulation of these theories can be performed on a quantum computer, and open up a promising line of research. As we scale our system up, we will be able to tackle problems that are still insoluble

with classical computers. The long-term goal is to solve problems like hadronization and confinement in quantum chromodynamics, which are of fundamental interest for understanding the basic constituents of nature, but difficult to study using current approaches.

The technical advances and experiments shown in this thesis are stepping stones in the quest for a useful quantum computer. Many challenges lie ahead, and technological improvements to the experimental setup, as well as architectural changes, are required to realize the goal of outperforming classical computers with a quantum device. Current efforts by our team to improve the fidelity of our quantum gates show promising results. A new laser setup installed recently offers coherence times on the order of 200 ms, almost twice as long as during the experiments shown in this thesis. We have also found and reduced sources of laser intensity fluctuations. Moreover, we plan to install permanent magnets to achieve more stable magnetic fields, and to actively stabilize the radial trapping frequency. We expect that these improvements will allow us to perform even more complex experiments in the near future, like extensions of the quantum link model experiments mentioned in Chapter 9.

APPENDIX TO THE QUANTUM COMPILER

The contents of this appendix are extracted from Ref. [70].

COMPILING LOCAL UNITARIES

Finding basis changes

In this appendix we will show how to satisfy equation (89). We need to find a rotation C around the equator of the Bloch sphere such that:

$$u = C^{-1} \sigma_z C, \quad (139)$$

where u is the generator of a given known unitary U , and it can always be written as:

$$u = \sin \theta \cos \phi \sigma_x + \sin \theta \sin \phi \sigma_y + \cos \theta \sigma_z, \quad (140)$$

for some angles θ, ϕ .

In general C is of the form:

$$C = e^{-i\gamma c/2}, \quad (141)$$

where γ is its rotation angle and c its generator, which must lie on the equator and thus be a linear combination of σ_x and σ_y . If we propose:

$$c = \sin \phi \sigma_x - \cos \phi \sigma_y, \quad (142)$$

and replace in equation (139), we find that the angle of rotation must be:

$$\gamma = \theta. \quad (143)$$

Writing a unitary as a product of two equatorial rotations

We will show here how to decompose an arbitrary unitary as a product of two rotations around the equator of the Bloch sphere, namely:

$$U = C_2 C_1. \quad (144)$$

The target unitary can be written as:

$$\begin{aligned} U &= \cos\left(\frac{\beta}{2}\right) \mathbb{1} - i \sin\left(\frac{\beta}{2}\right) \times \\ &\quad \times (\sin\theta \cos\phi \sigma_x + \sin\theta \sin\phi \sigma_y + \cos\theta \sigma_z), \end{aligned} \quad (145)$$

where β is its rotation angle, and θ, ϕ determine its rotation axis. Similarly, the equatorial rotations can be written as:

$$C_i = \cos\left(\frac{\alpha_i}{2}\right) \mathbb{1} - i \sin\left(\frac{\alpha_i}{2}\right) (\cos\phi'_i \sigma_x + \sin\phi'_i \sigma_y), \quad (146)$$

for some rotation angles α_i and phases ϕ'_i .

We shall assume that:

$$\alpha_1 = \alpha_2 = \alpha, \quad (147)$$

$$\phi'_1 = \phi + \Delta/2, \quad (148)$$

$$\phi'_2 = \phi - \Delta/2. \quad (149)$$

Replacing these into (144) and solving for α and Δ we obtain:

$$\cos^2\left(\frac{\alpha}{2}\right) = \frac{1}{2} \left(\cos\left(\frac{\beta}{2}\right) + 1 \right) \sin^2\theta, \quad (150)$$

$$\cos\Delta = \frac{\cos^2\left(\frac{\alpha}{2}\right) - \cos\left(\frac{\beta}{2}\right)}{1 - \cos^2\left(\frac{\alpha}{2}\right)}. \quad (151)$$

Unitaries up to a collective Z rotation

Suppose that the unitary U we want to implement is followed by gates whose phase can be freely chosen. Then it must only be specified up to an arbitrary collective rotation Z' , since this phase can be absorbed in the following gates. To compile U , we shall consider a decomposition of the form (82):

$$U = Z' C_N Z_{N-1} C_{N-1} \cdots Z_2 C_2 Z_1 C_1. \quad (152)$$

Such a decomposition is more convenient in this case because the last addressed pulse Z_N has been eliminated by taking advantage of the additional degree of freedom provided by Z' . We can now follow the same steps as in section 5.1. The unitary C_N is given by:

$$C_N = Z'^{-1} U_N C_1^{-1} C_2^{-1} \cdots C_{N-1}^{-1}, \quad (153)$$

and eliminating this factor from the rest of the equations we obtain:

$$\begin{aligned} U_N^{-1} U_1 &= C_1^{-1} Z_1 C_1, \\ U_N^{-1} U_2 &= C_1^{-1} C_2^{-1} Z_2 C_2 C_1, \\ &\vdots \\ U_N^{-1} U_{N-1} &= C_1^{-1} C_2^{-1} \cdots C_{N-1}^{-1} Z_{N-1} C_{N-1} \cdots C_2 C_1. \end{aligned} \quad (154)$$

Equations (154) can be satisfied in exactly the same way as explained in section 5.1. In order to satisfy equation (153) we need to find a rotation Z' such that the generator of C_N lies on the equator. This can be done as follows.

We wish to find how to satisfy equation (153). For this we need to find a rotation Z around the Z axis and a rotation C around an axis on the equator of the Bloch sphere such that, for a given unitary U , the following equation holds:

$$C = ZU. \quad (155)$$

U is in general of the form:

$$U = e^{-i\alpha u/2}, \quad (156)$$

and Z is of the form:

$$Z = e^{-i\beta \sigma_z/2}. \quad (157)$$

We will first find the angle of rotation β . If we write out (155) in terms of the generators of U and Z we have:

$$\begin{aligned} C &= \left(\cos\left(\frac{\beta}{2}\right) \mathbb{1} - i \sin\left(\frac{\beta}{2}\right) \sigma_z \right) \times \\ &\quad \times \left(\cos\left(\frac{\alpha}{2}\right) \mathbb{1} - i \sin\left(\frac{\alpha}{2}\right) u \right). \end{aligned} \quad (158)$$

Since the axis of rotation of C lies on the equator, its generator must not have any Z component, and thus:

$$0 = \sin\left(\frac{\beta}{2}\right) \cos\left(\frac{\alpha}{2}\right) + \cos\left(\frac{\beta}{2}\right) \sin\left(\frac{\alpha}{2}\right) u_z, \quad (159)$$

that is:

$$\beta = -2 \arctan\left(\tan\left(\frac{\alpha}{2}\right) u_z\right). \quad (160)$$

Once β is known, the unitary on the right-hand side of (155) is fully determined, and thus C as well.

Unitaries up to independent Z rotations

Finally, suppose that the unitary we want to implement is defined up to arbitrary independent rotations for each qubit around the Z axis. This is useful if the unitary is followed by a projective measurement, since any final rotation around the measurement axis for any qubit simply adds a phase and will not change the measured probabilities.

Let us again consider a sequence of the form (82). The decomposition must now satisfy, for each qubit:

$$\begin{aligned} Z'_1 U_1 &= C_N \cdots C_2 Z_1 C_1, \\ Z'_2 U_2 &= C_N \cdots Z_2 C_2 C_1, \\ &\vdots \\ Z'_N U_N &= Z_N C_N \cdots C_2 C_1, \end{aligned} \tag{161}$$

where the Z'_i are arbitrary rotations around the Z axis. As before, we can set $Z_N = \mathbb{1}$ and find C_N :

$$C_N = Z'_N U_N C_1^{-1} C_2^{-1} \cdots C_{N-1}^{-1}. \tag{162}$$

Eliminating C_N from the remaining equations we obtain:

$$\begin{aligned} U_N^{-1} Z_N'^{-1} Z'_1 U_1 &= C_1^{-1} Z_1 C_1, \\ U_N^{-1} Z_N'^{-1} Z'_2 U_2 &= C_1^{-1} C_2^{-1} Z_2 C_2 C_1, \\ &\vdots \\ U_N^{-1} Z_N'^{-1} Z'_{N-1} U_{N-1} &= C_1^{-1} \cdots C_{N-1}^{-1} Z_{N-1} C_{N-1} \cdots C_1. \end{aligned} \tag{163}$$

Each equation has now an extra degree of freedom coming from the angle of the Z'_k rotation. Let us for simplicity consider the case where the number of qubits N is odd. If we group equations (163) in pairs we get two degrees of freedom per pair, which can be used to remove one of the global operations. Therefore we will discard every even-numbered global operation C_{2k} from our decomposition and look for the solution of the following system of equations:

$$\begin{aligned} U_N^{-1} Z_1'' U_1 &= C_1^{-1} Z_1 C_1, \\ U_N^{-1} Z_2'' U_2 &= C_1^{-1} Z_2 C_1, \\ U_N^{-1} Z_3'' U_3 &= C_1^{-1} C_3^{-1} Z_3 C_3 C_1, \\ U_N^{-1} Z_4'' U_4 &= C_1^{-1} C_3^{-1} Z_4 C_3 C_1, \\ &\vdots \\ U_N^{-1} Z_{N-2}'' U_{N-2} &= C_1^{-1} \cdots C_{N-2}^{-1} Z_{N-2} C_{N-2} \cdots C_1, \\ U_N^{-1} Z_{N-1}'' U_{N-1} &= C_1^{-1} \cdots C_{N-2}^{-1} Z_{N-1} C_{N-2} \cdots C_1, \end{aligned} \tag{164}$$

where $Z_k'' = Z_N'^{-1} Z_k'$. If the number of qubits N is even, then the last equation is simply left unpaired. It is easy to verify that for each pair of equations the right-hand sides commute, and therefore we must have:

$$[U_N^{-1} Z_{2k-1}'' U_{2k-1}, U_N^{-1} Z_{2k}'' U_{2k}] = 0, \quad (165)$$

or equivalently:

$$[Z_{2k-1}'' U_{2k-1} U_N^{-1}, Z_{2k}'' U_{2k} U_N^{-1}] = 0. \quad (166)$$

In order to solve equation (166) we need to find rotations $Z_1 = Z(\beta_1)$, $Z_2 = Z(\beta_2)$ that satisfy a general equation of the form:

$$[Z_1 U_1, Z_2 U_2] = 0, \quad (167)$$

for given arbitrary U_1, U_2 , whose generators are u_1 and u_2 respectively.

Let us define:

$$V_i = Z_i U_i, \quad (168)$$

and let v_i be the generators of the V_i . In order to satisfy (167), the v_i must satisfy:

$$v_1 = v_2 = v, \quad (169)$$

since if two unitaries commute their generators must be the same. Our first goal is to determine the generator v . Let us consider the unitary:

$$W_i = Z_i^{1/2} U_i Z_i^{1/2}. \quad (170)$$

By writing down W_i explicitly in terms of the generators of each factor, it can be seen that its generator w_i satisfies:

$$\{w_i, [\sigma_z, u_i]\} = 0. \quad (171)$$

Since we have:

$$V_i = Z_i^{1/2} W_i Z_i^{-1/2}, \quad (172)$$

from equation (171) we see that:

$$\left\{ v, Z_i^{1/2} [\sigma_z, u_i] Z_i^{-1/2} \right\} = 0. \quad (173)$$

The geometrical meaning of this equation is that the vector defined by v on the Bloch sphere is perpendicular to that defined by $Z_i^{1/2} [\sigma_z, u_i] Z_i^{-1/2}$.

Since (173) must hold for $i = 1, 2$, v must correspond to the cross product of these vectors:

$$v = \mathcal{N} \left[Z_1^{1/2} [z, u_1] Z_1^{-1/2}, Z_2^{1/2} [\sigma_z, u_2] Z_2^{-1/2} \right], \quad (174)$$

where $\mathcal{N}$ is chosen such that:

$$\frac{1}{2} \text{tr}(v^2) = 1. \quad (175)$$

Having found v , it remains to find the rotation angles β_i . Now, v must satisfy $[Z_i U_i, v] = 0$, and therefore:

$$U_i v U_i^{-1} = Z(\beta_i)^{-1} v Z(\beta_i). \quad (176)$$

Both v and U_i are known, so v and $U_i v U_i^{-1}$ can be written down explicitly as:

$$v = \sin \theta \cos \phi \sigma_x + \sin \theta \sin \phi \sigma_y + \cos \theta \sigma_z, \quad (177)$$

$$U_i v U_i^{-1} = \sin \theta \cos \phi'_i \sigma_x + \sin \theta \sin \phi'_i \sigma_y + \cos \theta \sigma_z, \quad (178)$$

and therefore:

$$\beta_i = \phi - \phi'_i. \quad (179)$$

We have shown how to find suitable rotations Z'' that fulfill condition (166). Once these are found, all the left-hand sides of (164) are known unitaries and the system can be solved as before. The last collective rotation C_N can be determined from (162) as shown in appendix A.1.3. We have thus shown how to compile the sought unitary U into a sequence of the form:

$$U = \begin{cases} C_N Z_{N-1} Z_{N-2} C_{N-2} \cdots C_3 Z_2 Z_1 C_1 & \text{for odd } N, \\ C_N Z_{N-1} C_{N-1} \cdots C_3 Z_2 Z_1 C_1 & \text{for even } N. \end{cases} \quad (180)$$

APPENDIX TO SHOR'S ALGORITHM

The contents of this appendix are extracted from Ref. [76].

PULSE SEQUENCE OPTIMISATION

For a sufficiently large Hilbert-space it will no longer be possible to directly optimize unitary operations acting on the entire register, as the quantum state of the register will not fit into memory. Decomposing the necessary unitary operations into building blocks acting on smaller register sizes will allow one the use of optimized pulse sequences for large-scale quantum computation. From a methodological point of view it may be preferred to physically decouple the qubits from any interactions (for instance by splitting and moving part of ion-qubit quantum register out of an interaction region, such as proposed in Ref. [25]). However, given the technical requirements and challenges for splitting and moving ion-strings, we focus on spectroscopically decoupling certain ion-qubits from the interaction. In particular, we spectroscopically decouple an ion from subsequent interactions by transferring any quantum information from the $\{S_{1/2}(m = -1/2), D_{5/2}(m = -1/2)\}$ manifold to the $\{S_{1/2}(m = 1/2), D_{5/2}(m = -5/2)\}$ manifold using refocusing techniques on the $D_{5/2}(m = -1/2)$ to $S_{1/2}(m = 1/2)$ and $S_{1/2}(m = -1/2)$ to $D_{5/2}(m = -5/2)$ transitions. Using this approach, we optimise the controlled SWAP operation in a three-qubit Hilbert space rather than a five-qubit Hilbert space.

CONTROLLED-SWAP

The controlled-SWAP operation, also known as Fredkin operation, plays a crucial role in the modular multiplication. For its implementation, however, we could not derive a pulse sequence that can incorporate an arbitrary number of spectator qubits – qubits, that should be subject to the identity operation – in the presented case, i.e. two spectator qubits in the computational register. However, using decoupling of spectator qubits, this additional requirement on the implementation is not necessary. Using pulse sequence optimization [34], we obtained a sequence for the exact three-qubit case as shown in Table 1. In total the sequence consists of 18 pulses, including four MS interactions.

Pulse Nr.	Pulse	Pulse Nr.	Pulse
1	$R(1/2, 1/2)$	10	$R(1/2, 1)$
2	$S_z(3/2, 3)$	11	$S_z(1/4, 2)$
3	$MS(4/8)$	12	$S_z(3/2, 3)$
4	$S_z(3/2, 2)$	13	$MS(4/8)$
5	$S_z(1/2, 3)$	14	$S_z(3/2, 2)$
6	$R(3/4, 0)$	15	$S_z(3/2, 1)$
7	$MS(6/8)$	16	$R(1/2, 1)$
8	$S_z(3/2, 2)$	17	$S_z(3/2, 1)$
9	$MS(4/8)$	18	$S_z(3/2, 2)$

Table 1: Controlled SWAP operation: In a system of three ion-qubits, qubit 1 represents the control qubit and qubits $\{2, 3\}$ are to be swapped depending on the state of the first qubit. Note that this sequence only works for three-qubit systems. Spectator qubits would not experience the identity operation.

Pulse Nr.	Pulse	Pulse Nr.	Pulse
1	$R(1/2, 1)$	6	$MS(1/4)$
2	$S_z(3/2, 1)$	7	$R(3/4, 0)$
3	$MS(3/4)$	8	$S_z(3/2, 1)$
4	$R(5/4, 1)$	9	$R(1/2, 0)$
5	$S_z(1, 1)$		

Table 2: Four-target controlled NOT: Depending on the state of qubit one, the remaining four qubits $\{2-5\}$ are subject to a conditional NOT operation.

FOUR-TARGET CONTROLLED-NOT

The modular multipliers $(7 \bmod 15)$ and $(13 \bmod 15)$ require, besides Fredkin operations, CNOT operations which act on one qubit as the control and on the rest of qubits in the computational register as targets. Such an operation can be implemented (see Ref. [34], p.90, eq. 5.21) with two MS operations plus local operations only, regardless of the size of the computational register. The respective sequence is shown in Tab. 2.

TWO-TARGET CONTROLLED-NOT

There exists an analytic solution to realize multi-target controlled-NOT operations in the presence of spectator qubits with the presented set of gates [34], as required for the $\{2, 7, 8, 13\}^2 \bmod 15$ mul-

tiplier. However, we find that performing decoupling of subsets of qubits of the quantum register prior to the application of the multi-target controlled-NOT operation presented above both facilitates the optimisation, and improves the performance of the realisation of a two-target controlled-NOT operation. Thus, the required two-target controlled-NOT operation is implemented via (i) decoupling qubits 2 and 4, (ii) performing a multi-target controlled-not on all qubits with the first qubit acting as control, and (iii) recoupling of qubits 2 and 4. Here, again, decoupling scales linearly with the system size.

Note that all presented building blocks (Controlled-SWAP, Four-Target Controlled-NOT, Two-Target Controlled-NOT) have been realized in a scalable way, applicable on arbitrarily large ion-strings.

CONTROLLED QUANTUM MODULAR MULTIPLIERS

Based on the decomposition shown in Fig. 35d and the respective pulse sequences outlined in the previous section, we investigate the performance of the building blocks as well as the respective conditional multipliers. In the following, the fidelities are defined as mean probabilities and standard deviations to observe the correct output state. The elements in the respective truth tables have been obtained as average over 200 repetitions.

- The Fredkin operation, controlled by qubit 1 and acting on qubits $ij \in \{35, 23, 34, 45\}$, yields fidelities of $\{76(4), 73(6), 72(4), 68(7)\}\%$. These numbers are consistent with MS gate interactions at a fidelity of about 95% acting on three ions (in the presence of two decoupled ions) and local operations at a fidelity of 99.3%.
- The 4-target CNOT gate operates at a fidelity of 86(3)%.
- Considering the quality for modular multipliers of $\{2, 7, 8, 11, 13\} \bmod 15$, we find fidelities of $\{48(5), 40(5), 50(6), 46(5), 38(5)\}\%$. This performance is consistent with the multiplication of the performance of the individual building blocks: $\{37(6), 36(5), 37(6), 48(5), 36(5)\}\%$.

The experimentally obtained truth tables of the five modular multipliers are presented in Fig. 56.

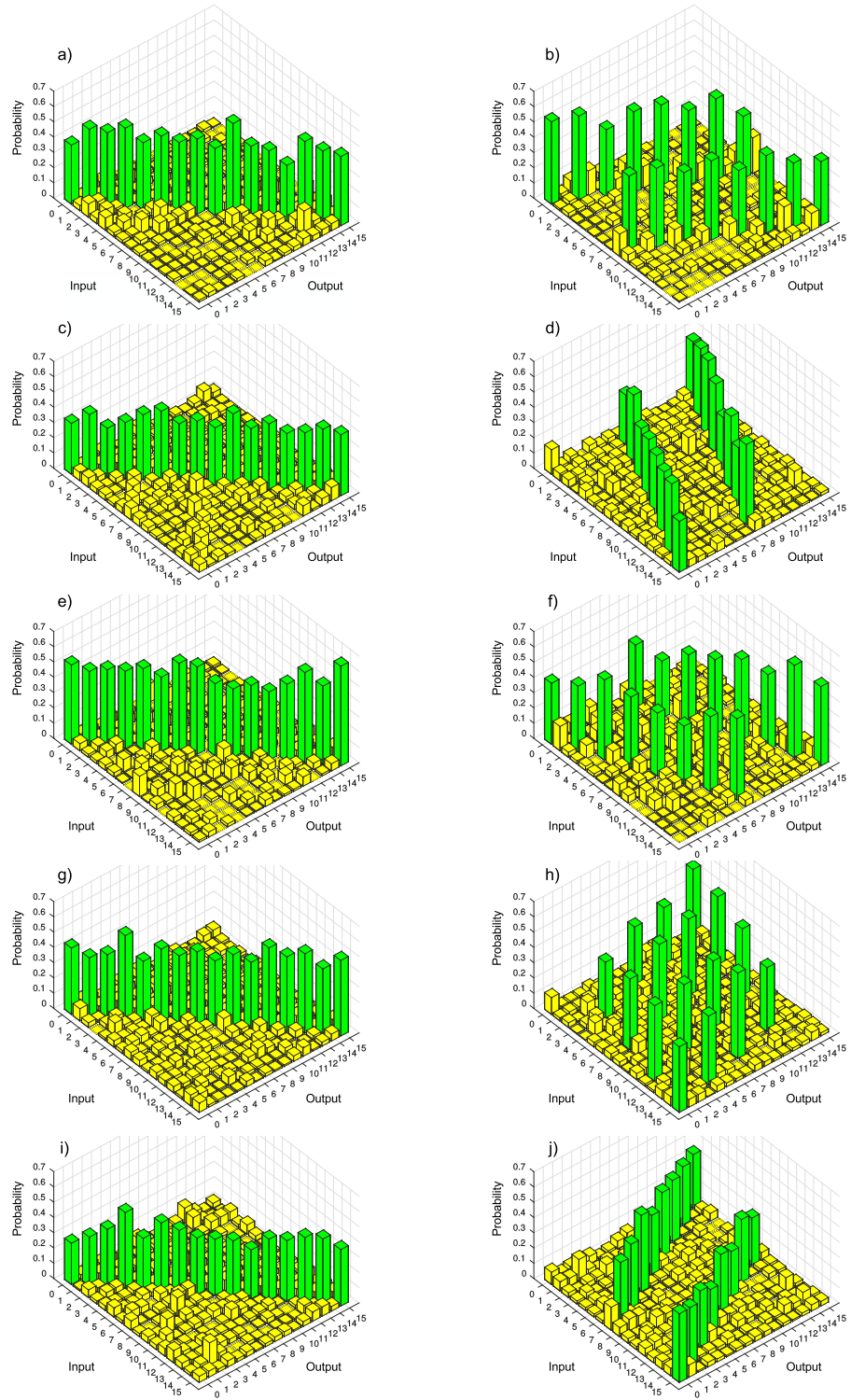


Figure 56: Controlled modular multipliers: While the full truth tables have been obtained, for improved visibility only the subset of data for the computational register (in decimal basis) is presented for modular multipliers ($\{2, 7, 8, 11, 13\} \bmod 15$) where the control bit maps from $|0\rangle$ to $|0\rangle$ (a,c,e,g,i) as well as when $|1\rangle$ maps onto $|1\rangle$ (b,d,f,h,j). When the control qubit is in state $|0\rangle$, one expects to find the identity operation implemented, as shown in (a,c,e,g,i). If the control qubit is in state $|1\rangle$, the input state gets multiplied by ($\{2, 7, 8, 11, 13\} \bmod 15$). This behaviour is visually demonstrated as the output state increases in steps of $\{2, 7, 8, 11, 13\}$ until it reaches 15, where the output is then returned to its value modulo 15.

PUBLICATIONS

The experiments presented in this thesis resulted in the following journal publications:

1. Martinez, E. A. *et al.* Real-time dynamics of lattice gauge theories with a few-qubit quantum computer. *Nature* **534**, 516–519 (June 2016).
2. Martinez, E. A., Monz, T., Nigg, D., Schindler, P. & Blatt, R. Compiling quantum algorithms for architectures with multi-qubit gates. *New J. Phys.* **18**, 063029 (June 2016).
3. Monz, T. *et al.* Realization of a scalable Shor algorithm. *Science* **351**, 1068–1070 (Mar. 2016).

In a more general context, during my PhD I contributed to research work that led to the following publications:

4. Müller, M. *et al.* Iterative Phase Optimization of Elementary Quantum Error Correcting Codes. *Phys. Rev. X* **6**, 031030 (Aug. 2016).
5. Nigg, D. *et al.* Can different quantum state vectors correspond to the same physical state? An experimental test. *New J. Phys.* **18**, 13007 (Jan. 2016).
6. Freitas, N., Martinez, E. A. & Paz, J. P. Heat transport through ion crystals. *Phys. Scr.* **91**, 13007 (Jan. 2016).
7. Nigg, D. *et al.* Quantum computations on a topologically encoded qubit. *Science* **345**, 302–305 (July 2014).
8. Schindler, P. *et al.* A quantum information processor with trapped ions. *New J. Phys.* **15**, 123012 (Dec. 2013).
9. Lanyon, B. P. *et al.* Measurement-based quantum computation with trapped ions. *Phys. Rev. Lett.* **111**, 210501 (Nov. 2013).
10. Schindler, P. *et al.* Quantum simulation of dynamical maps with trapped ions. *Nat. Phys.* **9**, 361–367 (May 2013).

BIBLIOGRAPHY

1. Carroll, L. *Alice's Adventures in Wonderland* (Macmillan, London, 1865).
2. Schrödinger, E. Are there quantum jumps? *Brit. J. Phil. Sci.* **3**, 233–242 (1952).
3. Feynman, R. *There's Plenty of Room at the Bottom* Pasadena, 1959.
4. Leibfried, D., Blatt, R., Monroe, C. & Wineland, D. Quantum dynamics of single trapped ions. *Rev. Mod. Phys.* **75**, 281–324 (Mar. 2003).
5. Häffner, H., Roos, C. F. & Blatt, R. Quantum computing with trapped ions. *Phys. Rep.* **469**, 155–203 (2008).
6. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* 1st, 191–193 (Cambridge University Press, 2004).
7. Shor, P. *Algorithms for quantum computation: discrete logarithms and factoring* in *Proc. 35th Annu. Symp. Found. Comput. Sci.* (IEEE Comput. Soc. Press, 1994), 124–134.
8. Gatttringer, C. & Lang, C. B. *Quantum chromodynamics on the lattice* 1–211 (Springer-Verlag, 2010).
9. Calzetta, E. A. & Hu, B. L. *Nonequilibrium Quantum Field Theory* (Cambridge Univ. Press, Cambridge, 2008).
10. Feynman, R. P. Simulating physics with computers. *Int. J. Theor. Phys.* **21**, 467–488 (June 1982).
11. Georgescu, I. M., Ashhab, S. & Nori, F. Quantum simulation. *Rev. Mod. Phys.* **86**, 153–185 (Mar. 2014).
12. Lloyd, S. Universal Quantum Simulators. *Science* **273**, 1073–1078 (1996).
13. Schwinger, J. Gauge invariance and mass. II. *Phys. Rev.* **128**, 2425–2429 (Dec. 1962).
14. Kogut, J. & Susskind, L. Hamiltonian formulation of Wilson's lattice gauge theories. *Phys. Rev. D* **11**, 395–408 (Jan. 1975).
15. Aaronson, S. *Quantum Computing since Democritus* 1st ed. (Cambridge University Press, 2013).
16. Cirac, J. I. & Zoller, P. Quantum Computations with Cold Trapped Ions. *Phys. Rev. Lett.* **74**, 4091–4094 (May 1995).
17. Wineland, D. *et al.* Experimental Issues in Coherent Quantum-State Manipulation of Trapped Atomic Ions. *J. Res. Natl. Inst. Stand. Tech.* 259 (1998).

18. Schindler, P. *et al.* A quantum information processor with trapped ions. *New J. Phys.* **15**, 123012 (Dec. 2013).
19. Rieffel, E. G. & Polak, W. H. *Quantum Computing: A Gentle Introduction* (2011).
20. Życzkowski, K., Horodecki, P., Sanpera, A. & Lewenstein, M. Volume of the set of separable states. *Phys. Rev. A* **58**, 883–892 (Aug. 1998).
21. Barenco, A. *et al.* Elementary gates for quantum computation. *Phys. Rev. A* **52**, 3457–3467 (Nov. 1995).
22. DiVincenzo, D. P. The Physical Implementation of Quantum Computation. *Fortschritte der Phys.* **48**, 771–783 (Sept. 2000).
23. Schindler, P. *et al.* Quantum simulation of dynamical maps with trapped ions. *Nat. Phys.* **9**, 361–367 (May 2013).
24. James, D. F. V. Quantum dynamics of cold trapped ions with application to quantum computation. *Appl. Phys. B-Lasers Opt.* **66**, 181–190 (Feb. 1998).
25. Kielpinski, D., Monroe, C. & Wineland, D. J. Architecture for a large-scale ion-trap quantum computer. *Nature* **417**, 709–711 (June 2002).
26. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (June 2008).
27. Langer, C. *et al.* Long-Lived Qubit Memory Using Atomic Ions. *Phys. Rev. Lett.* **95**, 060502 (Aug. 2005).
28. Lucas, D. M. *et al.* A long-lived memory qubit on a low-decoherence quantum bus. arXiv: **0710.4421** (Oct. 2007).
29. Benhelm, J., Kirchmair, G., Roos, C. F. & Blatt, R. Experimental quantum-information processing with $^{43}\text{Ca}^+$ ions. *Phys. Rev. A* **77**, 062306 (June 2008).
30. Sørensen, A. & Mølmer, K. Entanglement and quantum computation with ions in thermal motion. *Phys. Rev. A* **62**, 22311 (July 2000).
31. Dehmelt, H. Proposed $10^{14} \Delta\nu/\nu$ laser fluorescence spectroscopy on Ti^+ mono-ion oscillator II (spontaneous quantum jumps). *Bull. Am. Phys. Soc.* **20**, 60 (1975).
32. Cirac, J. I., Zoller, P., Kimble, H. J. & Mabuchi, H. Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network. *Phys. Rev. Lett.* **78**, 3221–3224 (Apr. 1997).
33. Daniilidis, N., Lee, T., Clark, R., Narayanan, S. & Häffner, H. Wiring up trapped ions to study aspects of quantum information. *J. Phys. B At. Mol. Opt. Phys.* **42**, 154012 (2009).

34. Nebendahl, V., Häffner, H. & Roos, C. F. Optimal control of entangling operations for trapped-ion quantum computing. *Phys. Rev. A* **79**, 012312 (2009).
35. Isenhower, L., Saffman, M. & Molmer, K. Multibit CNOT quantum gates via Rydberg blockade. *Quantum Inf. Process.* **10**, 755 (Apr. 2011).
36. Harty, T. P. *et al.* High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit. *Phys. Rev. Lett.* **113**, 220501 (Nov. 2014).
37. Xia, T. *et al.* Randomized benchmarking of single qubit gates in a 2D array of neutral atom qubits. *Phys. Rev. Lett.* **114**, 100503 (Jan. 2015).
38. Ballance, C. J., Harty, T. P., Linke, N. M., Sepiol, M. a. & Lucas, D. M. Laser-driven quantum logic gates with precision beyond the fault-tolerant threshold, 1–12 (Dec. 2015).
39. Trotter, H. F. On the product of semi-groups of operators. *Proc. Am. Math. Soc.* **10**, 545–551 (1959).
40. Suzuki, M. Relationship between d-Dimensional Quantal Spin Systems and (d+1)-Dimensional Ising Systems. *Prog. Theor. Phys.* **56**, 1454–1469 (1976).
41. Gauss, C. F. *Disquisitiones Arithmeticae* (1801).
42. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **41**, 303–332 (Jan. 1999).
43. Menezes, A. *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)* 1st, 780 (CRC Press, 1996).
44. Kitaev, A. Y. Quantum measurements and the Abelian stabilizer problem. *arXiv Prepr. quant-ph/9511026*, 1–22 (Nov. 1995).
45. Beckman, D., Chari, A. N., Devabhaktuni, S. & Preskill, J. Efficient Networks for Quantum Factoring. *Phys. Rev. A* **54**, 1034–1063 (Aug. 1996).
46. Pomerance, C. A Tale of Two Sieves. *Science* **43**, 1473–1485 (1996).
47. Carroll, L. *The Hunting of the Snark* (Macmillan Publishers, 1876).
48. Oerter, R. *The Theory of Almost Everything* (Plume, 2006).
49. Dürr, S. *et al.* Ab initio determination of light hadron masses. *Science* **322**, 1224–1227 (Nov. 2008).
50. Satz, H. The Quark-Gluon Plasma - A Short Introduction. *Nucl. Phys. A* **862-863**, 4–12 (July 2011).
51. Halzen, F. & Martin, A. D. *Quarks and leptons: an introductory course in modern particle physics* (Wiley, 1984).
52. Abbott, E. A. *Flatland: A Romance of Many Dimensions* (Seely & Co., London, 1884).

53. Fritzsch, H. *Quarks: The Stuff of Matter* (Basic Books, 1983).
54. Schwinger, J. On Gauge Invariance and Vacuum Polarization. *Phys. Rev.* **82**, 664–679 (1951).
55. Casher, A., Neuberger, H. & Nussinov, S. Chromoelectric-flux-tube model of particle production. *Phys. Rev. D* **20**, 179–188 (July 1979).
56. Neuberger, H. Finite-time corrections to the chromoelectric-flux-tube model. *Phys. Rev. D* **20**, 2936–2946 (Dec. 1979).
57. Brout, R., Massar, S., Parentani, R., Popescu, S. & Spindel, P. Quantum source of the back reaction on a classical field. *Phys. Rev. D* **52**, 1119–1133 (July 1995).
58. Narozhny, N. B. & Fedotov, A. M. Creation of electron-positron plasma with superstrong laser field. *Eur. Phys. J. Spec. Top.* **223**, 1083–1092 (June 2014).
59. Casanova, J. *et al.* Quantum simulation of quantum field theories in trapped ions. *Phys. Rev. Lett.* **107**, 260501 (Dec. 2011).
60. Wiese, U. J. Ultracold quantum gases and lattice systems: quantum simulation of lattice gauge theories. *Ann. Phys.* **525**, 777–796 (2013).
61. García-Álvarez, L. *et al.* Fermion-Fermion Scattering in Quantum Field Theory with Superconducting Circuits. *Phys. Rev. Lett.* **114**, 70502 (Feb. 2015).
62. Zohar, E., Cirac, I. I., Reznik, B. & Erez Zohar J. Ignacio Cirac, B. R. Quantum Simulations of Lattice Gauge Theories using Ultracold Atoms in Optical Lattices. *Rep. Prog. Phys.* **79**, 14401 (2015).
63. Banks, T., Susskind, L. & Kogut, J. Strong-coupling calculations of lattice gauge theories: $(1 + 1)$ -dimensional exercises. *Phys. Rev. D* **13**, 1043–1053 (Feb. 1976).
64. Jordan, P. & Wigner, E. Über das Paulische Äquivalenzverbot. *Zeitschrift für Phys.* **47**, 631–651 (1928).
65. Chandrasekharan, S. & Wiese, U.-J. Quantum link models : A discrete approach to gauge theories. *Nucl. Phys. B* **492**, 455–471 (1997).
66. Hamer, C. J., Weihong, Z. & Oitmaa, J. Series expansions for the massive Schwinger model in Hamiltonian lattice theory. *Phys. Rev. D* **56**, 55–67 (July 1997).
67. Bañuls, M. C., Cichy, K., Cirac, J. I., Jansen, K. & Saito, H. *Matrix Product States for Lattice Field Theories* in (), 332.
68. Bañuls, M., Cichy, K., Cirac, J. & Jansen, K. The mass spectrum of the Schwinger model with matrix product states. *J. High Energy Phys.* **2013**, 158 (Nov. 2013).

69. Billings, C. W. *Grace Hopper: Navy Admiral and Computer Pioneer* (Enslow Pub, 1989).
70. Martinez, E. A., Monz, T., Nigg, D., Schindler, P. & Blatt, R. Compiling quantum algorithms for architectures with multi-qubit gates. *New J. Phys.* **18**, 063029 (June 2016).
71. Vandersypen, L. M. K. & Chuang, I. L. NMR techniques for quantum control and computation. *Rev. Mod. Phys.* **76**, 1037–1069 (Jan. 2005).
72. Khaneja, N. & Glaser, S. J. Cartan decomposition of $SU(2n)$ and control of spin systems. *Chem. Phys.* **267**, 11–23 (June 2001).
73. Knill, E. *Approximation by Quantum Circuits* tech. rep. (1995).
74. Iten, R., Colbeck, R., Kukuljan, I., Home, J. & Christandl, M. Quantum Circuits for Isometries. *Phys. Rev. A* **93**, 032318 (2016).
75. Shende, V. V. & Markov, I. L. On the CNOT-cost of TOFFOLI gates. *Quant. Inf. Comp.* **9**, 461–486 (Mar. 2009).
76. Monz, T. *et al.* Realization of a scalable Shor algorithm. *Science* **351**, 1068–1070 (Mar. 2016).
77. Yu, N. & Ying, M. Optimal simulation of three-qubit gates. arXiv: [1301.3727](#) (Jan. 2013).
78. DiVincenzo, D. P. Two-bit gates are universal for quantum computation. *Phys. Rev. A* **51**, 1015–1022 (Feb. 1995).
79. Nocedal, J. & Wright, S. J. *Numerical Optimization* (Springer, 1999).
80. Mezzadri, F. How to generate random matrices from the classical compact groups. *Not. Am. Math. Soc.* **54**, 592–604 (2007).
81. Vatan, F. & Williams, C. Optimal quantum circuits for general two-qubit gates. *Phys. Rev. A* **69**, 032315 (Mar. 2004).
82. Hanneke, D. *et al.* Realization of a programmable two-qubit quantum processor. *Nat. Phys.* **6**, 13–16 (Nov. 2009).
83. Gottesman, D. *The Heisenberg Representation of Quantum Computers* in *Proc. XXII Int. Colloq. Gr. Theor. Methods Phys.* (eds Corney, S. P., Delbourgo, R. & Jarvis, P. D.) (International Press, Cambridge, MA, July 1999), 32–43. arXiv: [9807006](#) [quant-ph].
84. Knill, E. *et al.* Randomized benchmarking of quantum gates. *Phys. Rev. A* **77**, 012307 (Jan. 2008).
85. DiVincenzo, D. P., Leung, D. W. & Terhal, B. M. Quantum Data Hiding. *IEEE Trans. Inf. Theory* **48**, 580–599 (Mar. 2002).
86. Kliuchnikov, V. & Maslov, D. Optimization of Clifford circuits. *Phys. Rev. A* **88**, 052307 (Nov. 2013).
87. Lindberg, M. & Javanainen, J. Temperature of a laser-cooled trapped three-level ion. *J. Opt. Soc. Am. B* **3**, 1008 (July 1986).

88. Monroe, C. *et al.* Resolved-sideband Raman cooling of a bound atom to the 3D zero-point energy. *Phys. Rev. Lett.* **75**, 4011–4014 (Nov. 1995).
89. Eschner, J., Morigi, G., Schmidt-Kaler, F. & Blatt, R. Laser cooling of trapped ions. *J. Opt. Soc. Am. B* **20**, 1003 (May 2003).
90. Marzoli, I., Cirac, J. I., Blatt, R. & Zoller, P. Laser cooling of trapped three-level ions: Designing two-level systems for sideband cooling. *Phys. Rev. A* **49**, 2771–2779 (Apr. 1994).
91. Niven, L. Niven's laws. *Analog Magazine* (Nov. 2002).
92. Nigg, D. *et al.* Can different quantum state vectors correspond to the same physical state? An experimental test. *New J. Phys.* **18**, 13007 (Jan. 2016).
93. Drever, R. W. P. *et al.* Laser phase and frequency stabilization using an optical resonator. *Appl. Phys. B Photophysics Laser Chem.* **31**, 97–105 (June 1983).
94. Monz, T. *A frequency offset lock for cavity-driven Raman transitions* PhD thesis (University of Innsbruck, 2005).
95. Schünemann, U., Engler, H., Grimm, R., Weidemüller, M. & Zielonkowski, M. Simple scheme for tunable frequency offset locking of two lasers. *Rev. Sci. Instrum.* **70**, 242 (Jan. 1999).
96. Politi, A., Matthews, J. C. F. & O'Brien, J. L. Shor's quantum factoring algorithm on a photonic chip. *Science* **325**, 1221 (Sept. 2009).
97. Martín-López, E. *et al.* Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics* **6**, 773–776 (Oct. 2012).
98. Lucero, E. *et al.* Computing prime factors with a Josephson phase qubit quantum processor. *Nat. Phys.* **8**, 719–723 (Aug. 2012).
99. Lu, C. Y., Browne, D. E., Yang, T. & Pan, J. W. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.* **99**, 250504 (Dec. 2007).
100. Lanyon, B. P. *et al.* Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement. *Phys. Rev. Lett.* **99**, 250505 (Dec. 2007).
101. Vandersypen, L. M. *et al.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883–7 (Jan. 2001).
102. Smolin, J. A., Smith, G. & Vargo, A. Oversimplifying quantum factoring. *Nature* **499**, 163–5 (July 2013).
103. Griffiths, R. B. & Niu, C.-S. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.* **76**, 3228–3231 (Apr. 1996).

104. Parker, S. & Plenio, M. B. Efficient factorization with a single pure qubit and log N mixed qubits. *Phys. Rev. Lett.* **85**, 3049–3052 (Oct. 2000).
105. Mosca, M. & Ekert, A. *The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer* (ed Williams, C. P.) 174–188 (Springer Berlin Heidelberg, Berlin, Heidelberg, May 1999).
106. Vedral, V., Barenco, A. & Ekert, A. Quantum networks for elementary arithmetic operations. *Phys. Rev. A* **54**, 147–153 (July 1996).
107. Van Meter, R. & Itoh, K. M. Fast quantum modular exponentiation. *Phys. Rev. A* **71**, 052320 (May 2005).
108. Riebe, M. *et al.* Deterministic quantum teleportation with atoms. *Nature* **429**, 734–737 (June 2004).
109. Riebe, M. *Preparation of entangled states and quantum teleportation with atomic qubits* PhD thesis (2005).
110. Chiaverini, J. *et al.* Implementation of the Semiclassical Quantum Fourier Transform in a Scalable System. *Science* **308**, 997–1000 (May 2005).
111. Martinez, E. A. *et al.* Real-time dynamics of lattice gauge theories with a few-qubit quantum computer. *Nature* **534**, 516–519 (June 2016).
112. Jordan, S. P., Lee, K. S. M. & Preskill, J. Quantum Algorithms for Quantum Field Theories. *Science* **336**, 1130–1133 (2012).
113. Hebenstreit, F., Berges, J. & Gelfand, D. Real-time dynamics of string breaking. *Phys. Rev. Lett.* **111**, 201601 (2013).
114. Kasper, V., Hebenstreit, F., Oberthaler, M. & Berges, J. Schwinger pair production with ultracold atoms. *arXiv*, 1506.012238 (2015).
115. Blatt, R. & Roos, C. F. Quantum simulations with trapped ions. *Nat. Phys.* **8**, 277–284 (Apr. 2012).
116. Barends, R. *et al.* Digital quantum simulation of fermionic models with a superconducting circuit. *Nat. Commun.* **6**, 7654 (2015).
117. Salathé, Y. *et al.* Digital quantum simulation of spin models with circuit quantum electrodynamics. *Phys. Rev. X* **5**, 21027 (June 2015).
118. Zohar, E., Cirac, J. I. & Reznik, B. Simulating Compact Quantum Electrodynamics with Ultracold Atoms: Probing Confinement and Nonperturbative Effects. *Phys. Rev. Lett.* **109**, 125302 (Sept. 2012).
119. Tagliacozzo, L., Celi, A., Zamora, A. & Lewenstein, M. Optical Abelian Lattice Gauge Theories. *Ann. Phys. (N. Y.)* **330**, 160–191 (2013).

120. Banerjee, D. *et al.* Atomic quantum simulation of dynamical gauge fields coupled to fermionic matter: From string breaking to evolution after a quench. *Phys. Rev. Lett.* **109**, 175302 (Oct. 2012).
121. Hauke, P., Marcos, D., Dalmonte, M. & Zoller, P. Quantum simulation of a lattice Schwinger model in a chain of trapped ions. *Phys. Rev. X* **3**, 41018 (2013).
122. Graß, T., Muschik, C., Celi, A., Chhajlany, R. W. & Lewenstein, M. Synthetic magnetic fluxes and topological order in one-dimensional spin systems. *Phys. Rev. A* **91**, 63612 (June 2015).
123. Gorin, T., Prosen, T., Seligman, T. H. & Žnidarič, M. Dynamics of Loschmidt echoes and fidelity decay. *Phys. Rep.* **435**, 33–156 (2006).
124. Heyl, M., Polkovnikov, A. & Kehrein, S. Dynamical Quantum Phase Transitions in the Transverse Field Ising Model. *Phys. Rev. Lett.* **110**, 135704 (2013).
125. Plenio, M. B. & Virmani, S. An Introduction to Entanglement Measures. *Quantum Info. Comput.* **7**, 1–51 (Jan. 2007).
126. Muschik, C. *et al.* Encoding Wilson’s lattice gauge theories in digital quantum simulators (in preparation).
127. Horn, D. Finite matrix models with continuous local gauge invariance. *Phys. Lett. B* **100**, 149 (1981).
128. Orland, P. & Rohrlich, D. Lattice gauge magnets: Local isospin from spin. *Nucl. Phys. B* **338**, 647–672 (1990).
129. Brower, R., Chandrasekharan, S. & Wiese, U.-J. QCD as a quantum link model. *Phys. Rev. D* **60**, 27 (Sept. 1999).
130. Brower, R., Chandrasekharan, S., Riederer, S. & Wiese, U.-J. D-theory: field quantization by dimensional reduction of discrete variables. *Nucl. Phys. B* **693**, 149–175 (Aug. 2004).
131. Duan, L.-M., Demler, E. & Lukin, M. D. Controlling Spin Exchange Interactions of Ultracold Atoms in Optical Lattices. *Phys. Rev. Lett.* **91**, 90402 (Aug. 2003).
132. Hermele, M., Fisher, M. P. A. & Balents, L. Pyrochlore photons: The $U(1)$ spin liquid in a $S=1/2$ three-dimensional frustrated magnet. *Phys. Rev. B* **69**, 64404 (Feb. 2004).
133. Levin, M. & Wen, X. G. Colloquium: Photons and electrons as emergent phenomena. *Rev. Mod. Phys.* **77**, 871–879 (Sept. 2005).
134. Popov, V. On Schwinger mechanism of e^+e^- pair production from vacuum by the field of optical and X-ray lasers. *Phys. Lett. A* **298**, 83–90 (June 2002).
135. Adams, D. *So Long, and Thanks for All the Fish* (Harmony Books, New York, 1984).

136. Lanyon, B. P. *et al.* Measurement-based quantum computation with trapped ions. *Phys. Rev. Lett.* **111**, 210501 (Nov. 2013).

INDEX

antiparticles, 27
Bloch sphere, 7
Clifford gates, 46
confinement, 27
control qubit, 9
coprime, 23
density matrix, 6
Dirac equation, 26
discrete Fourier transform, 17
DiVincenzo criteria, 9
electrons, 27
entanglement, 8
gamma matrices, 26
gauge theories, 30
Gauss' law, 34
Hadamard gate, 9
hidden-variable problem, 14
Hilbert space, 6
Kitaev's QFT, 19
Kogut-Susskind Hamiltonian, 32
lattice gauge theories, 25
logarithmic negativity, 8
mixed state, 6
modulo operation (mod), 19
negativity, 8
number field sieve, 23
observable, 6
particles, 27
Pauli matrices, 7
phonon, 10
positrons, 27
pure state, 6
quantum algorithms, 9
quantum circuits, 9
quantum computer, 8
quantum Fourier transform, 18
quantum link model, 33
qubit, 6
register, 18
repeated local search, 45
Schwinger mechanism, 28
secular potential, 10
Shor's algorithm, 17, 23
string breaking, 27
target qubit, 9
Trotter procedure, 74
Trotter-Suzuki decomposition, 15
unitary operator, 8
universal quantum computer, 8
universal set of gates, 9

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst’s seminal book on typography “*The Elements of Typographic Style*”. `classicthesis` is available for both $\text{\LaTeX}$ and $\text{\LyX}$:

<https://bitbucket.org/amiede/classicthesis/>

Hermann Zapf’s *Palatino* and *Euler* type faces (Type 1 PostScript fonts *URW Palladio L* and *FPL*) are used for the body text, and *Palatino Sans* is used for figures. The “typewriter” text is typeset in *Bera Mono*, originally developed by Bitstream, Inc. as “Bitstream Vera”. (Type 1 PostScript fonts were made available by Malte Rosenau and Ulrich Dirr.)