1 Algorithms for Quantum Systems — Quantum Algorithms

Th. Beth, M. Grassl, D. Janzing, M. Rötteler, P. Wocjan, and R. Zeier

Institut für Algorithmen und Kognitive Systeme
Universität Karlsruhe
Germany

1.1 Introduction

Since the presentation of polynomial time quantum algorithms for discrete log and factoring [Sho94] it is generally accepted that quantum computers may—at least for some problems—outperform classical ones. But the field of quantum information processing does not only have implications for computational problems. Using quantum mechanical systems for information processing naturally leads to the problem of finding efficient ways to control quantum mechanical systems.

Here we address several algorithmic aspects of quantum information processing in different areas. First, the state of the art of quantum signal transforms which are at the core of a huge class of quantum algorithms, namely hidden subgroup problems, is presented. Second, we discuss aspects of quantum error-correcting codes, in particular an interesting view on stabilizer codes which relates them to simple interaction Hamiltonians. The efficient implementation of unitary operations by given Hamiltonians is investigated next. Finally, results on the simulation of one quantum mechanical system by another are discussed.

1.2 Fast Quantum Signal Transforms

A basic task in classical signal processing is to find fast algorithms which compute the matrix-vector-product of a given transformation with an arbitrary input vector. Suppose that the input is a vector of length N with complex entries. A transformation is said to have a *fast* algorithm if the number of arithmetic operations needed to compute the matrix vector product—i. e., the number of additions and multiplications—is bounded by $O(N \log^c N)$, for some constant c. Amongst the most useful algorithms in computer science, physics, and engineering is the discrete Fourier transform DFT_N which is given by the unitary matrix

$$F_N := \frac{1}{\sqrt{N}} \cdot \left[\omega^{i \cdot j}\right]_{i,j=0,\ldots,N-1},$$

where $\omega = e^{2\pi i/N}$ denotes a primitive N-th root of unity. The computational complexity of computing the product $F_N \cdot x$ for an input vector $x \in \mathbb{C}^N$ is $O(N \log N)$.

In quantum computing the unitary transformation F_N is used in the following way. Suppose that a system consisting of n qubits holds a normalized state vector $|\psi\rangle = \sum_{i=1}^{N} x_i |i\rangle \in$

Quantum Information Processing, 2nd Edition. Edited by Thomas Beth and Gerd Leuchs

ISBN: 3-527-40541-0

$\mathbb{C}^N$, where $N := 2^n$. Note that here the information is encoded into the amplitudes of the basis states. To this state the unitary transformation F_N can be applied resulting in a state $F_N|\psi\rangle$. Unlike the situation in classical signal processing the components of $|\psi\rangle$ and $F_N|\psi\rangle$ are not directly accessible; they merely can be extracted by (POVM) measurements. However, for feature detecting purposes like the location of spectral peaks this approach is well-suited.

A quantum Fourier transform can be computed using $O(\log^2 N)$ elementary operations. This exponential speed-up compared to the classical complexity of the DFT, which surprisingly enough is obtained by a direct adaptation of the classic Cooley-Tukey algorithm to the quantum circuit model, is an essential indication for the power of quantum computing. This becomes manifest in the fact that the ability to compute a DFT in polylogarithmic time is the backbone of Shor's algorithms for factoring and computing the discrete logarithm [Sho94].

A natural question is whether other signal transforms which have desirable feature extraction properties in classical signal processing can be used for quantum algorithms. In a series of works [PRB99, RPB99, KR00, ABH+01, KR01, Röt02] it has been shown that many well-known signal transforms allow highly efficient realizations on a quantum computer. In particular the following classes of unitary transformations have been shown to be efficiently implementable on a quantum computer:

- Discrete Fourier transforms for finite abelian groups [ABH+01, Röt02].
- Generalized Fourier transforms for
  - 2-groups with maximal cyclic normal subgroup [PRB99, Röt02].
  - wreath products of the form $G = A \wr Z_2$, where A is abelian [RB98, Röt02].
  - Heisenberg groups over the finite fields $\mathbb{F}_{2^n}$ [Röt02].
- Discrete cosine and sine transforms of types I, II, III, and IV [RB99, KR01, Röt02].
- Discrete Hartley transforms [KR00, Röt02].

More precisely, we have shown that for discrete cosine transforms, discrete sine transforms, and discrete Hartley transforms $O(\log^2 N)$ elementary quantum gates are sufficient to implement any of those transforms for input sequences of length N. The Fourier transforms for finite groups which have been mentioned above have the same computational complexity, except for the Heisenberg group where an implementation using $O(\log^3 N)$ gates has been found.

The underlying theory which allows to find efficient factorizations in the above mentioned cases relies on two techniques which have been developed at the Institut für Algorithmen und Kognitive Systeme. The first technique is the so-called method of symmetry-based matrix factorizations. Here a matrix $M \in \mathbb{C}^{n\times n}$ is said to have symmetry (G, ϕ, ψ) if ϕ and ψ are representations of a finite group G and furthermore

$$\phi(g) \cdot M = M \cdot \psi(g), \quad \text{for all } g \in G.$$

The importance of symmetry in connection with generalized Fourier transforms was first recognized in the work of Th. Beth [Bet84]. An important feature of this approach is that classical fast algorithms can be explained—and automatically derived—in terms of symmetry of matrices [Min93, Egn97, Püs98].

In the thesis of M. Rötteler [Röt02] symmetry-based matrix factorizations have been taken as a starting point for further optimizations. This has led to efficient implementations of several generalized Fourier transforms, trigonometric transforms, and the Hartley transform.

A second technique has been developed by A. Klappenecker and M. Rötteler and is described in [Röt02]and [KR03]. The basic idea is to reuse previously found factorizations for the construction of higher level operations. A prime example is given by the problem of implementing functions of unitary transformations, i. e., operations of the form $f(U)$, where U is a unitary transformation of finite order and $f(U)$ is also unitary.

1.3 Quantum Error-correcting Codes

Owing to the high sensitivity of quantum mechanical systems to even small perturbations, means of error protection are essential for any computation or communication process based on quantum mechanics. A general theory of quantum error-correcting codes (QECC) has been developed (see, e. g., [KL97]), but many algorithmic aspects are still open. The main tasks are to find methods for constructing good QECC and efficient algorithms for encoding and decoding, including the correction of the errors.

A large family of QECC can be derived from cyclic codes (see [GB99, GGB99, GB00]). Those QECC admit various techniques for encoding and decoding, e. g., based on Fourier transformations over finite fields and quantum shift registers [BG00]. An interesting new class of QECC has been developed in cooperation with the group of G. Alber [ABC$^+$01, AMD03]. Those so-called jump codes exploit side-information about the errors due to the emission of quanta (quantum jumps). The side-information is obtained by continuously monitoring the quantum system and recording which subsystem emitted, e. g., a photon. An interesting connection to design theory leads to various constructions of jump codes [BCG$^+$03].

Another new concept of QECC linking various groups in the *Schwerpunktprogramm QIV* are so-called graph codes which have been introduced by D. Schlingemann and R. F. Werner [SW02]. Similar to the cluster states used in the one-way quantum computer of R. Raussendorf and H. J. Briegel [RB01], the basis states of a graph code are defined via an interaction graph corresponding to the spin–spin coupling Hamiltonian which can be used for encoding. Compared to the standard gate model of quantum computation, such a coupling Hamiltonian yields a very efficient—intrinsically parallel—algorithm.

We have shown that the concepts of graph codes and that of so-called stabilizer codes are equivalent, i. e., any graph code is a stabilizer code and vice versa [GKR02, Sch02, WSR$^+$02]. In the following, we will present the main ideas used in the proof.

Starting from an α-dimensional Hilbert space $\mathcal{H}$, a graph code is an α^k-dimensional subspace Q of $\mathcal{H}^{\otimes n}$ which is spanned by the vectors

$$|\underline{x}\rangle = \frac{1}{\sqrt{\alpha^n}} \sum_{y \in \mathbb{F}_{p^m}^n} \Big(\prod_{j=1}^{k+n} \prod_{i=1}^{j-1} \chi(z_i, z_j)^{\Gamma_{ij}} \Big) |y\rangle. \tag{1.1}$$

Here the dimension α is a prime power, i. e., $\alpha = p^m$ for some prime number p. The basis states $|y\rangle$ of $\mathcal{H}^{\otimes n}$ are labeled by vectors $y \in \mathbb{F}_{p^m}^n$ over the finite field $\mathbb{F}_{p^m}$, and the encoded states $|\underline{x}\rangle$ are labeled by vectors $x \in \mathbb{F}_{p^m}^k$. The coefficients on the right hand side are given by the values of a non-degenerate symmetric bicharacter χ on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, where $z = (x, y)$. Finally, the exponents Γ_{ij} are given by the adjacency matrix Γ of a weighted undirected graph with integral weights (corresponding to the coupling strength between the subsystems i and j). Equivalently, the states (1.1) of the graph code Q can be expressed in the form

$$|\underline{x}\rangle = \frac{1}{\sqrt{\alpha^n}} \sum_{y \in \mathbb{F}_{p^m}^n} \zeta(q(x+y))|y\rangle, \tag{1.2}$$

where ζ is a non-trivial additive character of $\mathbb{F}_p$ and q is a quadratic form on $\mathbb{F}_{p^m}^{k+n} \cong \mathbb{F}_p^{m(k+n)}$. This isomorphism shows that it is sufficient to consider graphical quantum codes which are defined over prime fields.

First we show that a graph code defined over the finite field $\mathbb{F}_p$ is a stabilizer code, i. e., a joint eigenspace of an abelian subgroup of the error group G generated by

$$X^a := \sum_{y \in \mathbb{F}_p^n} |y + a\rangle\langle y|, \quad \text{and } Z^d := \sum_{y \in \mathbb{F}_p^n} \exp(2\pi i/p)^{d^t y} |y\rangle\langle y|,$$

for $a, d \in \mathbb{F}_p^n$ (cf. [KR02a, KR02b]). Starting from (1.2) one can show that the stabilizer of Q is given by

$$S_Q = \{\exp(2\pi i/p)^{q(a)} X^a Z^{aM_y} \mid a \in \mathbb{F}_p^n \text{ such that } Ba = 0\}.$$

The matrices $M_y \in \mathbb{F}_p^{n\times n}$ and $B \in \mathbb{F}_p^{k\times n}$ are submatrices of the adjacency matrix Γ defining the quadratic form q which can be written as

$$\Gamma = \left(\begin{array}{c|c} M_x & B \\ \hline B^t & M_y \end{array}\right).$$

Additionally, the orthogonal projection onto the joint eigenspace for the eigenvalue 1 of the operators in S_Q coincides with Q, showing that Q indeed is a stabilizer code.

In order to show that any stabilizer code defined over the finite field $\mathbb{F}_{p^m}$ can be realized as a graph code, we first note that those stabilizer codes can equivalently be considered as stabilizer codes over $\mathbb{F}_p$ (see [AK01]). To any stabilizer code corresponds a (classical) symplectic code $\mathcal{C}$ over $\mathbb{F}_{p^2}$. The generator matrix of $\mathcal{C}$ can be written as $(X|Z)$ where $X, Z \in \mathbb{F}_p^{(n-k)\times n}$ and $XZ^t - ZX^t = 0$. As the code $\mathcal{C}$ is self-orthogonal, i. e., contained in the orthogonal code $\mathcal{C}^\perp$ with respect to the symplectic inner product on $\mathbb{F}_{p^2}^n$, there exists a self-dual code $\mathcal{D}$ with $\mathcal{C} \subseteq \mathcal{D} = \mathcal{D}^\perp \subseteq \mathcal{C}^\perp$. We can choose a generator matrix for $\mathcal{D}$ of the form

$$G' := (X'|Z') = \left(\begin{array}{c|c} X & Z \\ \hline \widetilde{X} & \widetilde{Z} \end{array}\right).$$

Similar to Gauß' algorithm, the matrix G' can be transformed into standard form $(\, I \mid C\,)$ where C is symmetric [Gra02a, Gra02b]. Quantum mechanically, the transformations correspond to local unitary operations which do not change the error-correcting properties of the QECC. Applying the same transformations to the subcode $\mathcal{C}$ of $\mathcal{D}$, we obtain an equivalent code whose generator matrix can be written as $(D|DC)$ where $D \in \mathbb{F}^{(n-k)\times n}$. Finally, we obtain the symmetric matrix

$$\Gamma := \left(\begin{array}{c|c} 0 & B \\ \hline B^t & C \end{array}\right),$$

where $DB^t = 0$. Using this matrix Γ as adjacency matrix in (1.1), we obtain a graph code which is equivalent to the stabilizer code corresponding to $\mathcal{C}$. Hence, for any stabilizer code over $\mathbb{F}_{p^m}$ there exists an equivalent graph code.

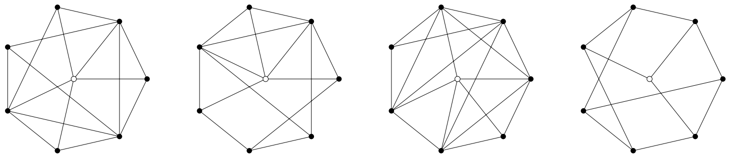

Figure 1.1: Non-isomorphic graphs which all yield graphical quantum codes that are equivalent to the CSS code $[\![7, 1, 3]\!]$.

In general, the corresponding graph is not uniquely determined, as illustrated in Fig. 1.1. All four graphs yield equivalent QECC, but the graphs are non-isomorphic. Therefore it is not straightforward to relate basic properties of the graph and the error-correcting properties of the resulting graph code. But the possibility to choose among different graphs results in different interaction Hamiltonians which may yield more efficient algorithms for encoding (cf. Section 1.5).

1.4 Efficient Decomposition of Quantum Operations into Given One-parameter Groups

The time evolution of all quantum mechanical systems is governed by the Schrödinger equation. To control the time evolution of a concrete physical implementation, we apply different Hamilton operators which are supposed to be time independent. This gives us the ability to implement computational operators on the state space. Equipped with m one-parameter groups

$$\{t \mapsto \exp(-i\mathrm{H}_1 t), t \mapsto \exp(-i\mathrm{H}_2 t), \ldots, t \mapsto \exp(-i\mathrm{H}_m t)\}$$

generated by the different Hamilton operators H_j, the goal is to build up each unitary U as a product of elements of the given one-parameter groups:

$$\mathrm{U} = \prod_{j=1}^{l} \exp(-i\mathrm{H}_{p_j} t_{p_j}), \quad \text{where } \mathrm{H}_{p_j} \in \{\mathrm{H}_1, \mathrm{H}_2, \ldots, \mathrm{H}_m\} \text{ and } t_{p_j} \in \mathbb{R}, t_{p_j} > 0.$$

As an efficiency measure we consider the minimal number of terms needed to express each unitary as a product of the given one-parameter groups. This efficiency measure is called the order of generation [Low71]. In a physical implementation of the given unitary operator this corresponds to the number of switches between different Hamilton operators.

As a first step we derive conditions on the set of Hamilton operators to be universal, i.e., to be able to generate each unitary. From the work of Chow [Cho39] follows the Lie algebra rank condition which states that each unitary can be implemented if the rank of the subalgebra generated by the given Hamilton operators equals the dimension of the Lie algebra belonging to the considered unitary operators. The work of Jurdjevic and Sussmann [JS72] states in addition that the order of generation is finite if the Lie algebra rank condition is fulfilled. To exclude—in the case of compact and connected Lie groups—the possibility of an infinite order of generation in the closure the work in [D'A02] can be used.

We emphasize that the order of generation depends heavily on the given one-parameter groups. The problem of determining bounds on the order of generation in the case of up to three Hamilton operators from the $\mathrm{su}(2)$ was considered in [ZB02]. Describing Hamilton operators as infinitesimal rotations of the Bloch sphere we can depict the application of an Hamilton operator in the complex plane after a stereographic projection from the Bloch sphere to the one-point compactification of the complex numbers. It is known [Gau19] that under stereographic projection the rotations of the sphere correspond to rotational Möbius transformations:

$$z \mapsto \frac{az - \bar{c}}{cz - \bar{a}}, \quad \text{where } a\bar{a} + c\bar{c} = 1.$$

The orbit of a rotational Möbius transformation is an Apollonian circle in the complex plane.

Beginning with the case of two Hamilton operators—we suppose that the Lie algebra rank condition is fulfilled—we follow [Low71] in order to derive bounds on the order of generation. Since Hamilton operators are identified with infinitesimal rotations of the Bloch sphere, we assume without loss of generality that one rotation axis is normalized to the z-axis and the other rotation axis lies in the x-z-plane. The orbits of an Hamilton operator correspond to a system of Apollonian circles in the complex plane. We track the alternating application of the two Hamilton operators on the state space starting from zero in the complex plane, which corresponds to the south pole of the Bloch sphere. Going from one circle to a tangent one we use a greedy-type algorithm to cover all of the complex plane. Figure 1.2 shows tangent circles corresponding to the alternating application of Hamilton operators to the state space visualized in the complex plane. One further step in the alternating application of Hamilton operators is necessary and sufficient to cover all of the complex plane in Figure 1.2.

By an analysis of figures similar to Figure 1.2 it is possible to get the minimal number of terms in a product of two one-parameter groups needed to transform each point on the Bloch sphere to the south pole, which corresponds in the complex plane to a transformation of each complex number into zero. We obtain a bound on the order of generation adding one to this minimal number. The reason for this is that each point of the Bloch sphere (and each point in the complex plane) can be identified pointwise with right cosets of rotations of the Bloch sphere representing all unitary operations. To distinguish the rotations in one coset in general this additional step is necessary.

In [Low71], figures similar to Figure 1.2 are analyzed. The analysis implies:

Theorem 1.1 *Let α denote the angle between two Hamilton operators in the Bloch vector representation and ξ the order of generation.*

1. $\alpha = \pi/2 \implies \xi = 3$ *(Euler decomposition),*
2. $\forall\ k \geq 2: \quad \pi/(k+1) \leq \alpha < \pi/k \implies \xi \leq k+2.$

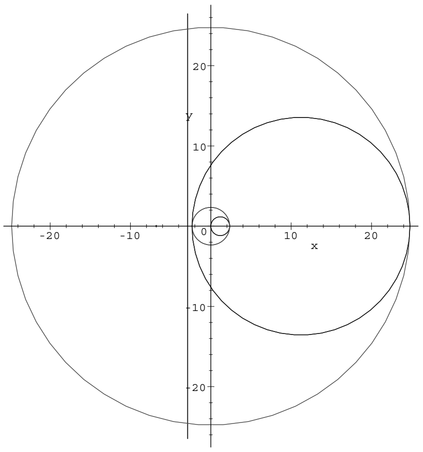

Figure 1.2: As described in the text, the figure shows tangent circles corresponding to the alternating application of two Hamilton operators to the state space visualized through stereographic projection to the complex plane. One further step in the alternating application of Hamilton operators is necessary and sufficient to cover all of the complex plane. Notice that for better orientation one Apollonian circle with infinite radius is pictured by a vertical line. The angle between the rotation axes in the Bloch sphere representation belonging to this figure is $(2 \cdot \pi/4 + \pi/5)/3$. In this case we get an order of generation less than or equal to 6.

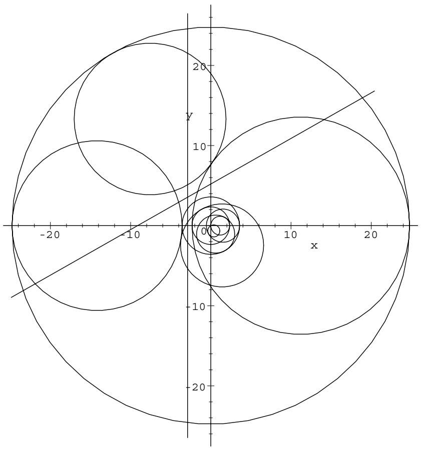

Figure 1.3: As in Figure 1.2 tangent circles corresponding to the application of three Hamilton operators to the stereographically projected state space are shown in the complex plane. To cover all of the complex plane no further step in the alternating application of Hamilton operators is needed. Notice that for better orientation two Apollonian circles with infinite radius are shown by two lines. In this example the angles between the rotation axes are $(2 \cdot \pi/4 + \pi/5)/3$, $\pi/5$, and $\pi/6$. Though all angles are less than or equal to the angle in example of Figure 1.2 we get a smaller upper bound of 5 steps.

The next step is to generalize the analysis from two to three Hamilton operators. Since we have a third Hamilton operator we have to consider a third axis of rotation in the representation of Hamilton operators as infinitesimal rotations of the Bloch sphere leading to a third system of Apollonian circles. The three axes of rotation can be characterized by specifying the three angles α_1, α_2, and α_3 between them. We get a valid triple of angles if

$$\alpha_3 \in [\min\{\pi - (\alpha_1 + \alpha_2), |\alpha_1 - \alpha_2|\}, \pi/2]\,.$$

As in the case of two Hamilton operators it is important to determine the minimal number of terms in a product of one-parameter groups necessary to transform each point in the complex plane to zero. In Figure 1.3, the tangent circles describing the application of the different Hamilton operators can be received from a similar greedy-type algorithm. As remarked in Figure 1.3 we can get with this type of analysis better bounds on the order of generation when using three Hamilton operators even though no greater angles between two rotation axes are present. Summarizing, this is a first step towards a systematic and efficient implementation of unitary operators.

1.5 Simulation of Hamiltonians

Historically, the first motivation for constructing a quantum computer was the efficient simulation of quantum dynamics. Feynman observed a profound difference in the nature of physical evolution governed by the laws of quantum physics as compared to the evolution under the laws of classical physics. It appears that the simulation of general quantum dynamics by any classical computers involves an unavoidable exponential slowdown in running time. Therefore it would be an interesting application of quantum computers to simulate Hamiltonian dynamics of many-particle systems. In our approach to this problem, we do not construct sequences of quantum gates to simulate the Hamiltonian evolution of a quantum system. The computational resource in our setting is the interaction of the qubits or qudits in the quantum register. The natural time evolution according to this interaction is interspersed with external control operations in such a way that the resulting dynamics is the evolution according to the simulated Hamiltonian evolution. We have restricted ourselves to the mutual simulation of Hamiltonians that are given by pair-interactions among n qudits.

The theoretical framework is as follows. The underlying Hilbert space of each subsystem is d-dimensional and the joint space of n qudits is $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$. The (d^2-1)-dimensional Lie algebra of traceless Hermitian matrices of size d is denoted by $su(d)$. We set in the following $m := d^2 - 1$. Let $B = \{\sigma_\alpha \mid \alpha := 1, \ldots, m\}$ be an orthogonal basis of $su(d)$ with respect to the trace inner product $\langle A|B\rangle := \mathrm{tr}(A^\dagger B)/d$. We denote by $\sigma_\alpha^{(k)}$ the operator that acts as σ_α on the kth qudit and as identity on the other qudits. We represent the interaction (which is assumed to contain only two-body terms) by a so-called coupling matrix $J = (J_{kl;\alpha\beta})$ of size $nm \times nm$ such that

$$H = \sum_{k<l} \sum_{\alpha\beta} J_{kl;\alpha\beta} \sigma_\alpha^{(k)} \sigma_\beta^{(l)}\,.$$

We chose the coupling matrix to be symmetric and set $J_{kk;\alpha\beta} = 0$ for all k. Now we use the so-called fast control limit and assume that all operations in $K = U(d) \otimes U(d) \otimes \cdots \otimes U(d)$ can be performed arbitrarily fast, where $U(d)$ denotes the group of unitary operations on a qudit. This assumption is a good approximation if the external control operations act on a considerably smaller time scale than the natural evolution of the considered Hamiltonians. For instance, this is the case for NMR-experiments.

A starting point for simulating an infinitesimal time evolution is that if a Hamiltonian $\tilde{H}$ can be written as the sum $\tilde{H} = \sum_{j=1}^{N} H_j$, then the concatenation of time evolutions according to each H_j for a small time approximates the evolution according to $\tilde{H}$ by the Trotter formula. This "average Hamiltonian approach" leads to the following definition [WJB02, WRJB02a, JWB03].

Definition 1.2 *Let $\tilde{H}$ be an arbitrary Hamiltonian. We say $\tilde{H}$ can be simulated by H with time overhead τ, written $\tilde{H} \le \tau H$, and N time steps if there are N positive real numbers τ_j summing to τ and N control operations $U_j \in K$ such that*

$$\tilde{H} = \sum_{j=1}^{N} \tau_j U_j^\dagger H U_j \,, \tag{1.3}$$

The time overhead gives the slowdown of the simulated interaction with respect to the system Hamiltonian. Time optimal simulation leads therefore to a convex optimization problem.

To derive lower bounds on the time overhead and the number of time steps it is possible to work with the coupling matrices instead of the Hamiltonians themselves. This is because the condition in Eq. (1.3) translates into

$$\tilde{J} = \sum_{j=1}^{N} \tau_j O_j J O_j^T \,, \tag{1.4}$$

where O_j are orthogonal transformations corresponding to the local operations U_j for $j = 1, \ldots, N$ [WRJB02a]. The advantage is that the size of the coupling matrices grows only linearly with n, whereas the size of the Hamiltonians grows exponentially.

Let H and $\tilde{H}$ be arbitrary Hamiltonians with coupling matrices J and $\tilde{J}$, respectively. A necessary condition that H can simulate $\tilde{H}$ with time overhead τ follows from Eq. (1.4) and Uhlmann's theorem [WJB02, WRJB02a]: If $\tilde{H} \le \tau H$ then we necessarily have

$$\sum_{i=1}^{k} \lambda_i(\tilde{J}) \le \tau \sum_{i=1}^{k} \lambda_i(J) \,,$$

for $k = 1, \ldots, nm$, where $\lambda_1(\tilde{J}) \ge \lambda_2(\tilde{J}) \ge \cdots \ge \lambda_{nm}(\tilde{J})$ and $\lambda_1(J) \ge \lambda_2(J) \ge \cdots \ge \lambda_{nm}(J)$ denote the eigenvalues of $\tilde{J}$ and J, respectively. This so-called *spectral majorization criterion* has still to be satisfied after rescaling the strengths $J_{kl;\alpha\beta}$ and $\tilde{J}_{kl;\alpha\beta}$ of corresponding interactions in H and $\tilde{H}$ by the same real factor $s_{kl} \in \mathbb{R}$. The reason is that the same sequence of local operations may be used for the rescaled problem.

One of the nicest applications of spectral majorization theory is to derive lower bounds on time-reversal schemes [JWB02], i. e., to simulate $-H$ when H is the quantum computer's Hamiltonian. This is the usual problem of efficient refocusing techniques in NMR. For the case of coupled qubits, i. e., $d = 2$, we consider the Hamiltonian $H = \sum_{k<l} w_{kl} \sigma_z^{(k)} \sigma_z^{(l)}$ such

that all w_{kl} are non-zero. We denote by K the matrix whose all diagonal entries are 0 and whose all off-diagonal entries are 1. Then after rescaling the coupling between the qubits k and l by $-w_{kl}$ we have $J' := -K \otimes \mathrm{diag}(0,0,1)$ and $\tilde{J}' := K \otimes \mathrm{diag}(0,0,1)$. By considering the largest eigenvalues of J' and $\tilde{J}'$ we obtain $n-1$ as a lower bound on the time overhead for time-reversal. A related problem is to switch off some interactions if there is an interaction between all qudits, i. e., to reduce the interaction graph. Then the lower bounds on the time overhead depend on the spectrum of the adjacency matrices corresponding to the graphs that indicate the remaining interactions. The intuitive meaning of the time overhead is the factor by which the remaining interactions are weakened.

The time overhead is not the only complexity measure for simulation schemes. The number N of time steps is also of importance. We have presented a general method to obtain lower bounds on the number of time steps by comparing the rank of coupling matrices [JWB03]. Consider the problem to switch off an interaction with coupling matrix J, i. e., $\sum_j \tau_j O_j J O_j^T = 0$. By adding τA with an arbitrary matrix A to the equation we have

$$\tau A = \sum_{j=1}^{N} \tau_j O_j (J + O_j^T A O_j) O_j^T \,.$$

By suitably choosing the matrix A it is possible to give an upper bound on the rank of each term $J + O_j^T A O_j$. In this way we obtain lower bounds on N. Especially, the method yields a classification of spin–spin interactions with respect to the complexity of the required schemes for decoupling and time reversal [JWB02].

Upper bounds on the time overhead and the number of time steps for mutual simulation of Hamiltonians have been constructed using selective decoupling techniques based on the concepts of orthogonal arrays from combinatorics and nice error bases from quantum coding theory [WRJB02a, JWB03]. The assumption that all local operations are allowed can be weakened. Finite groups of control operations to enable universal simulation of Hamiltonians are characterized in [WRJB02b].

References

[ABC$^+$01] G. Alber, Th. Beth, Ch. Charnes, A. Delgado, M. Grassl, and M. Mussinger. Stabilizing Distinguishable Qubits against Spontaneous Decay by Detected-Jump Correcting Quantum Codes. *Phys. Rev. Lett.*, 86(19):4402–4405, May 2001. See also LANL preprint quant-ph/0103042.

[ABH$^+$01] G. Alber, Th. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger. *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*, *Springer Texts in Modern Physics*, vol. 173. Springer, 2001.

[AK01] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inf. Theory*, 47(7):3065–3072, November 2001.

[AMD03] G. Alber, M. Mussinger, and A. Delgado. Quantum information processing and error correction with jump codes. In Th. Beth and G. Leuchs, eds., *Quantum Information Processing*. Wiley VCH, 2002, pp. 14-27.

[BCG$^+$03] Th. Beth, Ch. Charnes, M. Grassl, G. Alber, A. Delgado, and M. Mussinger. A New Class of Designs which Protect against Quantum Jumps. *Designs, Codes and Cryptography*, 29(1-3):51-70, 2003.

[Bet84] Th. Beth. *Verfahren der Schnellen Fouriertransformation*. Teubner, 1984.

[BG00] Th. Beth and M. Grassl. Algorithmen zur spektralen Codierung und Decodierung von zyklischen Quantencodes. Vortrag beim DFG-Kolloquium in Bad Honnef, 10.–12. January 2000.

[Cho39] W.-L. Chow. Über Systeme von linearen partiellen Differentialgleichungen erster Ordnung. *Math. Ann.*, 117:98–105, 1939.

[D'A02] D. D'Alessandro. Uniform Finite Generation of Compact Lie Groups. *Systems & Control Lettes*, September 2002. See also LANL preprint quant-ph/0111133.

[Egn97] S. Egner. Zur Algorithmischen Zerlegungstheorie Linearer Transformationen mit Symmetrie. Dissertation, Universität Karlsruhe, Informatik, 1997.

[Gau19] C. F. Gauss. Die Kugel. *Werke*, 8:351–356, c. 1819.

[GB99] M. Grassl and Th. Beth. Quantum BCH Codes. In W. Mathis and T. Schindler, eds., *Proceedings X. International Symposium on Theoretical Electrical Engineering*, pp. 207–212, Magdeburg, September 1999. Universität Magdeburg.

[GB00] M. Grassl and Th. Beth. Cyclic quantum error-correcting codes and quantum shift registers. *Proceedings of the Royal Society London A*, 456(2003):2689–2706, November 2000. See also LANL preprint quant-ph/9910061.

[GGB99] M. Grassl, W. Geiselmann, and Th. Beth. Quantum Reed-Solomon Codes. In M. Fossorier, H. Imai, S. Lin, and A. Poli, eds., *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13)*, *Lecture Notes in Computer Science*, vol. 1719, pp. 231–244, Honolulu, Hawaii, November 1999. Springer. See also LANL preprint quant-ph/9910059.

[GKR02] M. Grassl, A. Klappenecker, and M. Rötteler. Graphs, Quadratic Forms, and Quantum Codes. In *Proceedings 2002 IEEE International Symposium on Information Theory*, Lausanne, 2002, p. 45.

[Gra02a] M. Grassl. *Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen*. Shaker, Aachen, 2002. Zugl.: Universität Karlsruhe, Dissertation, 2001.

[Gra02b] M. Grassl. Algorithmic aspects of quantum error-correcting codes. In R. K. Brylinski and G. Chen, eds., *Mathematics of Quantum Computation*, pp. 223–252. CRC-Press, 2002.

[JS72] V. Jurdjevic and H. J. Sussmann. Control systems on Lie groups. *J. Differ. Equations*, 12:313–329, 1972.

[JWB02] D. Janzing, P. Wocjan, and Th. Beth. Complexity of decoupling and time-reversal for n spins with pair-interactions: Arrow of time in quantum control. *Phys. Rev. A*, 66:042311, 2002. See also LANL-preprint quant-ph/0106085v2.

[JWB03] D. Janzing, P. Wocjan, and Th. Beth. On the Computational Power of Physical Interactions: Bounds on the Number of Time Steps for Simulating Arbitrary Interaction Graphs. *International Journal of Foundations of Computer Science*, 14(5):889-903, 2003. See also LANL-preprint quant-ph/0203061.

[KL97] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, February 1997. See also LANL preprint quant-ph/9604034.

[KR00] A. Klappenecker and M. Rötteler. On the irresistible efficiency of signal processing methods in quantum computing. In R. Creutzburg and K. Egiazarian, eds., *Spectral Techniques and Logic Design for Future Digital Systems: Proceedings of the First International Workshop on Spectral Techniques and Logic Design for Future Digital Systems, Tampere, Finland, June 2–3*, 2000.

[KR01] A. Klappenecker and M. Rötteler. Discrete Cosine Transforms on Quantum Computers. In S. Loncaric and H. Babic, eds., *Proceedings of the 2nd International Symposium on Image and Signal Processing and Analysis (ISPA01)*, pp. 464–468, Pula, Croatia, 2001.

[KR02a] A. Klappenecker and M. Rötteler. Beyond Stabilizer Codes I: Nice Error Bases. *IEEE Trans. Inf. Theory*, 48(8):2392–2395, August 2002. See also LANL preprint quant-ph/0010082.

[KR02b] A. Klappenecker and M. Rötteler. Beyond Stabilizer Codes II: Clifford Codes. *IEEE Trans. Inf. Theory*, 48(8):2396–2399, August 2002. See also LANL preprint quant-ph/0010076.

[KR03] A. Klappenecker and M. Rötteler. Engineering Functional Quantum Algorithms. *Phys. Rev. A*, 67:010302(R), 2003. See also LANL preprint quant-ph/0109088.

[Low71] F. Lowenthal. Uniform finite generation of the rotation group. *Rocky Mountain J. Math.*, 1:575–586, 1971.

[Min93] T. Minkwitz. Algorithmensynthese für lineare Systeme mit Symmetrie. Dissertation, Universität Karlsruhe, Informatik, 1993.

[PRB99] M. Püschel, M. Rötteler, and Th. Beth. Fast Quantum Fourier Transforms for a Class of non-abelian Groups. In M. Fossorier, H. Imai, S. Lin, and A. Poli, eds., *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13)*, *Lecture Notes in Computer Science*, vol. 1719, pp. 148–159, Honolulu, Hawaii, November 1999. Springer. See also LANL preprint quant-ph/9910059.

[Püs98] M. Püschel. Konstruktive Darstellungstheorie und Algorithmengenerierung. Dissertation, Universität Karlsruhe, Informatik, 1998.

[RB98] M. Rötteler and Th. Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. LANL preprint quant-ph/9812070, 1998.

[RB99] M. Rötteler and Th. Beth. Efficient Realisation of Discrete Cosine Transforms on a Quantum Computer. *Proceedings X. International Symposium on Theoretical Electrical Engineering*, pp. 85–89, Magdeburg, September 1999. Universität Magdeburg.

[RB01] R. Raussendorf and H. J. Briegel. A One-Way Quantum Computer. *Phys. Rev. Lett.*, 86(22):5188–5191, May 2001. See also LANL preprint quant-ph/0010033.

[Röt02] M. Rötteler. *Schnelle Signaltransformationen für Quantenrechner*. Shaker, Aachen, 2002. Zugl.: Universität Karlsruhe, Dissertation, 2001.

[RPB99] M. Rötteler, M. Püschel, and Th. Beth. Fast Signal Transforms for Quantum Computers. In W. Kluge, ed., *Proceedings of the Workshop on Physics and Computer Science, Heidelberg*, DPG–Frühjahrstagung, Heidelberg, 1999.

[Sch02] D. Schlingemann. Stabilizer codes can be realized as graph codes. *Quant. Inf. Comp.*, 2(4):307-323, 2002. See also LANL preprint quant-ph/0111080, 2001.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithm and factoring. In *Proc. FOCS 94*, pp. 124–134. IEEE Computer Society Press, 1994.

[SW02] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65(1):012308, 2002. See also LANL preprint quant-ph/0012111.

[WJB02] P. Wocjan, D. Janzing, and Th. Beth. Simulating arbitrary pair-interactions by a given Hamiltonian: Graph-theoretical bounds on the time complexity. *Quant. Inform. & Comp.*, 2(2):117–132, 2002. See also LANL-preprint quant-ph/0106077.

[WRJB02a] P. Wocjan, M. Rötteler, D. Janzing, and Th. Beth. Simulating Hamiltonians in quantum Networks: Efficient schemes and complexity bounds. *Phys. Rev. A*, 65(4):042309, April 2002. See also LANL preprint quant-ph/0109088.

[WRJB02b] P. Wocjan, M. Rötteler, D. Janzing, and Th. Beth. Universal Simulation of Hamiltonians using a finite set of control operations. *Quant. Inform. & Comp.*, 2(2):133–150, 2002. See also LANL-preprint quant-ph/0109063.

[WSR$^+$02] R. F. Werner, D. Schlingemann, M. Reimpell, Th. Beth, M. Grassl, A. Klappenecker, and M. Rötteler. Quantum error correction: Graph codes and stabilizer codes. Poster at the DFG-Colloquium in Bad Honnef, 28.–30. January 2002.

[ZB02] R. Zeier and Th. Beth. Efficient decomposition of quantum operations into given one-parameter groups. Poster at the DFG-Colloquium in Bad Honnef, 28.–30. January 2002.