# Quantum Reed–Solomon Codes

Markus Grassl, Willi Geiselmann, and Thomas Beth

Institut für Algorithmen und Kognitive Systeme
Arbeitsgruppe Quantum Computing
Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany.

**Abstract.** We introduce a new class of quantum error–correcting codes derived from (classical) Reed–Solomon codes over finite fields of characteristic two. Quantum circuits for encoding and decoding based on the discrete cyclic Fourier transform over finite fields are presented.

## 1 Introduction

During the last years it has been shown that computers taking advantage of quantum mechanical phenomena outperform currently used computers. The striking examples are integer factoring in polynomial time (see [18]) and finding pre–images of an $n$–ary Boolean function ("searching") in time $O(\sqrt{2^n})$ (see [12]). Quantum computers are not only of theoretical nature—there are several suggestions how to physically realize them (see, e. g., [6, 7]).

On the way towards building a quantum computer, one very important problem is to stabilize quantum mechanical systems since they are very vulnerable. A theory of quantum error–correcting codes has already been established (see [15]). Nevertheless, the problem of how to encode and decode quantum error–correcting codes has hardly been addressed, yet.

In this paper, we present the construction of quantum error–correcting codes based on classical Reed–Solomon (RS) codes. For RS codes, many classical decoding techniques exist. RS codes can also be used in the context of erasures and for concatenated codes. Encoding and decoding of quantum RS codes is based on quantum circuits for the cyclic discrete Fourier transform over finite fields which are presented in Section 4, together with the quantum implementation of any linear transformation over finite fields. We start with some results about binary codes obtained from codes over extension fields, followed by a brief introduction to quantum computation and quantum error–correcting codes.

## 2 Binary Codes from Codes over $\mathbb{F}_{2^k}$

### 2.1 Bases of Finite Fields

First, we recall some facts about finite fields (see, e. g., [13]).

Any finite field of characteristic $p$, i. e., a finite field $\mathbb{F}_q$ where $q = p^k$, is a vector space of dimension $k$ over $\mathbb{F}_p$. For a fixed basis $\mathcal{B}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, any

M. Fossorier, H. Imai, S. Lin, and A. Poli (Ed.): AAECC-13, LNCS 1709, pp. 231–244, 1999.

element of $\mathbb{F}_q$ can thus be represented by a row vector of length $k$ over $\mathbb{F}_p$. To stress the dependence on the choice of the basis $\mathcal{B}$, we will denote this $\mathbb{F}_p$ vector space homomorphism by

$$\mathcal{B}\colon\ \mathbb{F}_q = \mathbb{F}_{p^k} \to \mathbb{F}_p^k, \quad a \mapsto \mathcal{B}(a). \tag{1}$$

The multiplication with a fixed element $a \in \mathbb{F}_q$ defines an $\mathbb{F}_p$–linear mapping. Thus it can be written as a $k \times k$ matrix $M_{\mathcal{B}}(a)$ over $\mathbb{F}_p$ where $\mathcal{B}(a' \cdot a) = \mathcal{B}(a') \cdot M_{\mathcal{B}}(a)$. The trace of $M_{\mathcal{B}}(a)$ is independent of the choice of the basis and defines an $\mathbb{F}_p$–linear mapping

$$\mathrm{tr}\colon\ \mathbb{F}_q \to \mathbb{F}_p, \quad a \mapsto \mathrm{tr}(a) := \sum_{i=0}^{k-1} a^{p^i} = \mathrm{tr}(M_{\mathcal{B}}(a))$$

(for the last equality see, e. g., [9, Satz 1.24]).

To be able to proceed further, we recall the definition of the dual basis. Given a basis $\mathcal{B} = (b_1, \ldots, b_k)$ of a finite field $\mathbb{F}_q$ over $\mathbb{F}_p$, the *dual basis* of $\mathcal{B}$ is a basis $\mathcal{B}^\perp = (b'_1, \ldots, b'_k)$ with

$$\forall i,j\colon\ \mathrm{tr}(b_i b'_j) = \delta_{ij}. \tag{2}$$

For any basis there exists a unique dual basis (see [13, Theorem 4.1.1]). Furthermore, for any finite field of characteristic two there exists a self–dual basis, i. e., a basis $\mathcal{B}$ with $\mathcal{B}^\perp = \mathcal{B}$ (see [13, Theorem 4.3.5]). For a self–dual basis $\mathcal{B}$, the matrix $M_{\mathcal{B}}(a)$ is symmetric. This follows from [9, Satz 1.22], where

$$M_{\mathcal{B}^\perp}(a) = M_{\mathcal{B}}(a)^{\mathsf{t}} \tag{3}$$

is shown.

Finally, any linear transformation $A \in GL(n, \mathbb{F}_{p^k})$ can be written as a linear transformation $\mathcal{B}(A) \in GL(nk, \mathbb{F}_p)$ by replacing each entry $a_{ij}$ of $A$ by $M_{\mathcal{B}}(a_{ij})$. Moreover, the diagram (4) is commutative, i. e., the change to the ground field can be done after or before the linear transformation—a fact that will be essential later.

$$\begin{array}{ccc} \mathbb{F}_{p^k}^n & \xrightarrow{A} & \mathbb{F}_{p^k}^n \\ \mathcal{B}\ \big\downarrow & & \big\downarrow\ \mathcal{B} \\ \mathbb{F}_p^{kn} & \xrightarrow{\mathcal{B}(A)} & \mathbb{F}_p^{kn} \end{array} \tag{4}$$

### 2.2 Subfield Expansion of Linear Codes

In the following, we restrict ourselves to the case $p = 2$, but the results are valid for any characteristic $p > 0$.

**Definition 1.** *Let $C = [N, K, D]$ denote a linear code of length $N$, dimension $K$, and minimum distance $D$ over the field $\mathbb{F}_{2^k}$, and let $\mathcal{B} = (b_1, \ldots, b_k)$ be a basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. Then the* binary expansion *of $C$ with respect to the basis $\mathcal{B}$, denoted by $\mathcal{B}(C)$, is the linear binary code $C_2 = [kN, kK, d \geq D]$ given by*

$$C_2 = \mathcal{B}(C) := \left\{ (c_{ij})_{i,j} \in \mathbb{F}_2^{kN} \;\middle|\; \boldsymbol{c} = \left(\sum_j c_{ij} b_j\right)_i \in C \right\}.$$

The following theorem relates the dual codes of a code and its binary expansion.

**Theorem 1.** *Let $C = [N, K]$ be a linear code over the field $\mathbb{F}_{2^k}$ and let $C^\perp$ be its dual. Then the dual code of the binary expansion $\mathcal{B}(C)$ of $C$ with respect to the basis $\mathcal{B}$ is the binary expansion $\mathcal{B}^\perp(C^\perp)$ of the dual code $C^\perp$ with respect to the dual basis $\mathcal{B}^\perp$, i. e., the following diagram is commutative:*

$$\begin{array}{ccc} C & \longrightarrow & C^\perp \\ \text{basis } \mathcal{B} \Big\downarrow & & \Big\downarrow \text{ dual basis } \mathcal{B}^\perp \\ \mathcal{B}(C) & \longrightarrow & \mathcal{B}^\perp(C^\perp) = \mathcal{B}(C)^\perp \end{array}$$

*Proof.* Let $\boldsymbol{c} \in C$ and $\boldsymbol{d} \in C^\perp$ be arbitrary elements of the code and its dual, resp. Then

$$0 = \sum_{i=1}^{N} c_i d_i = \sum_{i=1}^{N} \left( \sum_{j=1}^{k} c_{ij} b_j \right) \left( \sum_{l=1}^{k} d_{il} b'_l \right), \tag{5}$$

where $\mathcal{B} = (b_1, \ldots, b_k)$ is a basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$ and $\mathcal{B}^\perp = (b'_1, \ldots, b'_k)$ is the corresponding dual basis. Taking the trace in (5) and rewriting the summation yields

$$0 = \sum_{i=1}^{N} \sum_{j=1}^{k} \sum_{l=1}^{k} c_{ij} d_{il} \operatorname{tr}(b_j b'_l) = \sum_{i=1}^{N} \sum_{j=1}^{k} c_{ij} d_{ij}$$

(the last equality follows from Eq. (2)). Hence the binary expansions of the codewords $\boldsymbol{c}$ and $\boldsymbol{d}$ are orthogonal which proves that the binary expansion of $C^\perp$ is contained in $\mathcal{B}(C)^\perp$. The theorem follows from the observation that both sets have $2^{k(N-K)}$ elements. □

**Corollary 1.** *Let $C = [N, K]$ be a weakly self–dual linear code over the field $\mathbb{F}_{2^k}$. Then the binary expansion $\mathcal{B}(C)$ of $C$ with respect to a self–dual basis $\mathcal{B}$ is weakly self–dual, too.*

## 3 Quantum Error–Correcting Codes

### 3.1 Qubits and Quantum Circuits

In this section, we give a brief introduction to quantum computation (for a more comprehensive introduction see, e. g., [2, 21]).

The basic unit of quantum information, a *quantum bit* (or short *qubit*), is represented by the normalized linear combination

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \text{where } \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1. \tag{6}$$

Here $|0\rangle$ and $|1\rangle$ are orthonormal basis states written in Dirac notation (see [8]). The normalization condition in Eq. (6) stems from the fact that when extracting classical information from the quantum system by a measurement, the results "0" and "1" occur with probability $|\alpha|^2$ and $|\beta|^2$, resp.

A *quantum register* of length $n$ is obtained by combining $n$ qubits modelled by the $n$–fold tensor product $(\mathbb{C}^2)^{\otimes n}$. The canonical orthonormal basis of $(\mathbb{C}^2)^{\otimes n}$ is

$$B := \big\{ |b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \;\big|\; b_i \in \{0,1\} \big\}.$$

Hence the state of an $n$ qubit register is given by

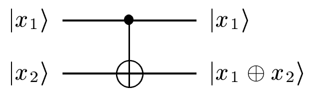
$$|\psi\rangle = \sum_{\boldsymbol{b} \in \{0,1\}^n} c_{\boldsymbol{b}} |\boldsymbol{b}\rangle, \qquad \text{where } c_{\boldsymbol{b}} \in \mathbb{C} \text{ and } \sum_{\boldsymbol{b} \in \{0,1\}^n} |c_{\boldsymbol{b}}|^2 = 1. \tag{7}$$

All operations of a quantum computer are linear. Furthermore, in order to preserve the normalization condition in Eq. (7), the operations have to be unitary. Basic operations are single qubit operations and two qubit operations. A single qubit operation on the $j$th qubit is given by $U = I_{2^{j-1}} \otimes U_2 \otimes I_{2^{n-j}}$, where $U_2 \in \mathcal{U}(2)$ is a $2 \times 2$ unitary matrix. Important examples for single qubit operations are the Hadamard transform $H$ and the Pauli matrices $\sigma_x$, $\sigma_y$, $\sigma_z$

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; \sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{8}$$

where $i^2 = -1$. The most important example for a two qubit gate is the so–called controlled $NOT$ gate ($CNOT$) since any unitary operation on a $2^n$–dimensional space can be implemented using only single qubit operations and $CNOT$ gates (see [1]). The transformation matrix of the $CNOT$ gate is given by:

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{array} \tag{9}$$




The $CNOT$ gate corresponds to the classical $XOR$ gate since $CNOT|x_1\rangle|x_2\rangle = |x_1\rangle|x_1 \oplus x_2\rangle$. (For the graphical notation on the right hand side see, e. g., [1].)

### 3.2 Error Model

In the following, we briefly summarize some results about quantum error–correcting codes. For a more comprehensive treatment, we refer to, e. g., [3, 15].

One common assumption in the theory of quantum error–correcting codes is that errors are local, i. e., only a small number of qubits are disturbed when transmitting or storing the state of an $n$ qubit register. The basic types of errors are bit–flip errors exchanging the states $|0\rangle$ and $|1\rangle$, phase–flip errors changing the relative phase of $|0\rangle$ and $|1\rangle$ by $\pi$, and their combination. The bit–flip error corresponds to the Pauli matrix $\sigma_x$, the phase–flip error to $\sigma_z$, and their combination to $\sigma_y$. It is sufficient to consider only this discrete set of errors in order to cope with any possible local error (see [15]). The important duality of bit–flip errors and phase–flip errors is shown by the following lemma.

**Lemma 1.** *Bit–flip and phase–flip errors are conjugated to each other by the Hadamard transform, i. e.,* $H\sigma_x H^{-1} = \sigma_z$ *and* $H\sigma_z H^{-1} = \sigma_x$.

Errors operating on an $n$ qubit system are represented by tensor products of Pauli matrices and identity. The *weight* of an error $\boldsymbol{e} = e_1 \otimes \ldots \otimes e_n$, where $e_i \in \{id, \sigma_x, \sigma_y, \sigma_z\}$ is the number of local errors $e_i$ that differ from identity.

### 3.3 Quantum Codes

Analogously to the notation $C = [N, K, d]$ for a classical error–correcting code encoding $K$ information symbols using $N$ code symbols and being capable of detecting up to $d-1$ errors, a *quantum error–correcting code* encoding $K$ qubits using $N$ qubits is denoted by $\mathcal{C} = [[N, K, d]]$. The code $\mathcal{C}$ is a $2^K$–dimensional subspace of the $2^N$–dimensional complex vector space $(\mathbb{C}^2)^{\otimes N}$ such that any error of weight less than $d$ can be detected or, equivalently, any error of weight less than $d/2$ can be corrected.

The construction of quantum Reed–Solomon codes is based on the construction of quantum error–correcting codes from weakly self–dual binary codes presented in [5] and [19, 20] as summarized by the following definition and theorem.

**Definition 2.** *Let* $C = [N, K]$ *be a weakly self–dual linear binary code, i. e.,* $C \leq C^\perp$. *Furthermore, let* $\{\boldsymbol{w}_j \mid j = 1, \ldots, 2^{N-2K}\}$ *be a system of representatives of the cosets* $C^\perp/C$. *Then the basis states of a quantum code* $\mathcal{C} = [[N, N-2K]]$ *are given by*

$$|\psi_j\rangle = \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\boldsymbol{c} + \boldsymbol{w}_j\rangle. \tag{10}$$

**Theorem 2.** *Let $d$ be the minimum distance of the dual code $C^\perp$ in Definition 2. Then the corresponding quantum code is capable of detecting up to $d-1$ errors or, equivalently, is capable of correcting up to $(d-1)/2$ errors.*

*Proof. (Sketch)* A general state of the quantum code is a linear combination of the states in Eq. (10), i. e.,

$$|\psi\rangle = \sum_j \alpha_j |\psi_j\rangle = \sum_j \alpha_j \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\boldsymbol{c} + \boldsymbol{w}_j\rangle = \sum_{\boldsymbol{c} \in C^\perp} \beta_{\boldsymbol{c}} |\boldsymbol{c}\rangle. \tag{11}$$

A combination of bit–flip and phase–flip errors can be written as

$$\boldsymbol{e} = (\sigma_x^{e_{b,1}} \sigma_z^{e_{p,1}}) \otimes \ldots \otimes (\sigma_x^{e_{b,n}} \sigma_z^{e_{p,n}}), \tag{12}$$

where $\boldsymbol{e}_b$ and $\boldsymbol{e}_p$ are binary vectors. The effect of this error on the state (11) is

$$\boldsymbol{e}|\psi\rangle = \sum_{\boldsymbol{c} \in C^\perp} \beta_{\boldsymbol{c}} (-1)^{\boldsymbol{c} \cdot \boldsymbol{e}_p} |\boldsymbol{c} + \boldsymbol{e}_b\rangle. \tag{13}$$

Computing the syndrome with respect to the binary code $C^\perp$ using auxiliary qubits, we obtain the state

$$\sum_{\boldsymbol{c} \in C^\perp} \beta_{\boldsymbol{c}} (-1)^{\boldsymbol{c} \cdot \boldsymbol{e}_p} |\boldsymbol{c} + \boldsymbol{e}_b\rangle |\boldsymbol{s}(\boldsymbol{c} + \boldsymbol{e}_b)\rangle. \tag{14}$$

As the syndrome $\boldsymbol{s}(\boldsymbol{c}+\boldsymbol{e}_b)$ depends only on the error $\boldsymbol{e}_b$, the state (14) is a tensor product and we can measure the syndrome without disturbing the first part of the quantum register. Using a classical decoding algorithm for the code $C^\perp$, the error vector $\boldsymbol{e}_b$ is computed from the measured syndrome $\boldsymbol{s}(\boldsymbol{e}_b)$. For each non–zero position of $\boldsymbol{e}_b$, a $\sigma_x$ gate is applied to correct the error.

From Lemma 1 follows that the Hadamard transform exchanges the rôle of $\boldsymbol{e}_b$ and $\boldsymbol{e}_p$ in Eq. (12). Furthermore, computing the Hadamard transform of the states in (10) yields

$$H^{\otimes N}|\psi_j\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{\boldsymbol{c}\in C^\perp} (-1)^{\boldsymbol{c}\cdot\boldsymbol{w}_j}|\boldsymbol{c}\rangle. \tag{15}$$

Hence, the Hadamard transform changes the state (13) into

$$H^{\otimes N}\boldsymbol{e}|\psi\rangle = \sum_{\boldsymbol{c}\in C^\perp} \gamma_{\boldsymbol{c}}(-1)^{\boldsymbol{c}\cdot\boldsymbol{e}_b}|\boldsymbol{c}+\boldsymbol{e}_p\rangle.$$

The error vector $\boldsymbol{e}_p$ can be determined as before. □

The general outline of decoding is shown in Fig. 1.

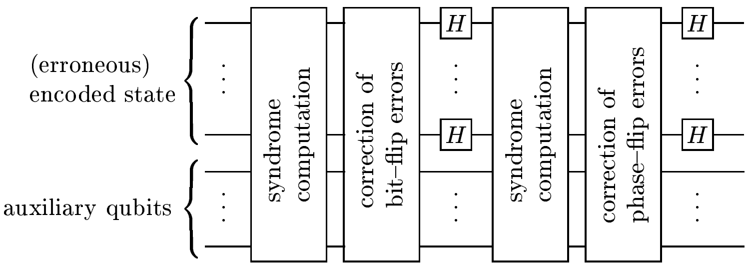



**Fig. 1.** General decoding scheme for a quantum error–correcting code constructed from a weakly self–dual binary code

Before we will be ready to present quantum Reed–Solomon codes, we need to show how to implement a discrete Fourier transform over a finite field on a quantum computer.

## 4 Quantum Implementation of the Cyclic DFT over $\mathbb{F}_{2^k}$

Recall from Section 3.1 that the state of an $n$ qubit system can be written as

$$|\psi\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_2^n} c_{\boldsymbol{x}}|\boldsymbol{x}\rangle, \qquad \text{where } c_{\boldsymbol{x}} \in \mathbb{C} \text{ and } \sum_{\boldsymbol{x}\in\mathbb{F}_2^n} |c_{\boldsymbol{x}}|^2 = 1. \tag{16}$$

Hence any invertible linear transformation $A \in GL(n, \mathbb{F}_2)$ on the binary vector space $\mathbb{F}_2^n$ induces a linear transformation $\mathcal{Q}(A) \in GL(2^n, \mathbb{C})$ on the complex vector space $\mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$. The transformation $\mathcal{Q}(A)$ permutes the basis states $|\boldsymbol{x}\rangle$ according to $\mathcal{Q}(A) : |\boldsymbol{x}\rangle \mapsto |\boldsymbol{x}A\rangle$. In the following we will show how this transformation can be implemented efficiently using only $CNOT$ gates.

**Theorem 3.** *Let $\pi \in S_n$ be a permutation and let $P \in GL(n, \mathbb{F}_2)$ be the corresponding permutation matrix acting on the binary vector space $\mathbb{F}_2^n$. Then the quantum transformation $\mathcal{Q}(P) \in GL(2^n, \mathbb{C})$ defined by $\mathcal{Q}(P) : |\boldsymbol{x}\rangle \mapsto |\boldsymbol{x}P\rangle$ is a permutation matrix permuting the $n$ tensor factors $\mathbb{C}^2$ of the complex vector space $\mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$. It can be implemented using at most $3(n-1)$ $CNOT$ gates.*

*Proof.* Any permutation $\pi \in S_n$ on $n$ letters can be written as product of at most $n-1$ transpositions. Each transposition $(i,j)$ can be implemented by a quantum circuit with three $CNOT$ gates, see Fig. 2. □

$(i,j) \;\widehat{=}$

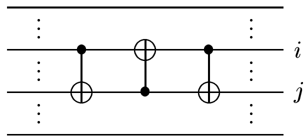



**Fig. 2.** Implementing a transposition of two qubits using three $CNOT$ gates

**Theorem 4.** *Let $A \in GL(n, \mathbb{F}_2)$ be an invertible linear mapping on the binary vector space $\mathbb{F}_2^n$. Then the quantum transformation $\mathcal{Q}(A) \in GL(2^n, \mathbb{C})$ defined by $\mathcal{Q}(A) : |\boldsymbol{x}\rangle \mapsto |\boldsymbol{x}A\rangle$ is a permutation matrix acting on the complex vector space $\mathbb{C}^{2^n}$. It can be implemented using at most $n(n-1) + 3(n-1)$ $CNOT$ gates.*

*Proof.* Any matrix $A \in GL(n, \mathbb{F}_2)$ can be decomposed as $A = P \cdot L \cdot U$, where $P$ is a permutation matrix and $L$ (resp. $U$) is a lower (upper) triangular matrix. By Theorem 3 we need at most $3(n-1)$ $CNOT$ gates for the implementation of $\mathcal{Q}(P)$.

For the implementation of the lower diagonal matrix $L$, we use the factorization $L = L_1 \cdot \ldots \cdot L_n$, where $L_i$ is almost an identity matrix, but the $i$th row equals the $i$th row of $L$. Hence multiplication of a binary vector $\boldsymbol{x}$ with $L_i$ is given by

$$\boldsymbol{x}L_i = (x_1 + x_i L_{i1}, \ldots, x_{i-1} + x_i L_{i,i-1}, x_i, x_{i+1}, \ldots, x_n),$$

i. e., the $j$th position of $\boldsymbol{x}$ is inverted iff both $x_i$ and $L_{ij}$ are equal to one. This translates into a sequence of at most $i-1$ $CNOT$ gates with control qubit $i$ and target qubit $j$ whenever $L_{ij}$ equals one. In total, the implementation of $\mathcal{Q}(L)$ needs at most $n(n-1)/2$ $CNOT$ gates. The quantum transformation $\mathcal{Q}(U)$ can be implemented similarly. □

The quantum implementation of linear mappings over an extension field $\mathbb{F}_{2^k}$ can be reduced to implementing linear mappings over $\mathbb{F}_2$. First, we fix a basis $\mathcal{B}$ of $\mathbb{F}_{2^k}$. By extending the homomorphism $\mathcal{B}$ given in Eq. (1) we obtain a homomorphism $\mathbb{F}_{2^k}^n \to \mathbb{F}_2^{kn}$. Vectors $\boldsymbol{v} \in \mathbb{F}_{2^k}^n$ are mapped to binary vectors of length $kn$ represented by $kn$ qubits. Similarly to Eq. (16), we get

$$|\psi\rangle = \sum_{\boldsymbol{v} \in \mathbb{F}_{2^k}^n} c_{\boldsymbol{v}} |\boldsymbol{v}\rangle = \sum_{\boldsymbol{v} \in \mathbb{F}_{2^k}^n} c_{\boldsymbol{v}} |\mathcal{B}(v_1)\rangle \otimes \ldots \otimes |\mathcal{B}(v_n)\rangle. \tag{17}$$

In this representation, a linear mapping $A \in GL(n, \mathbb{F}_{2^k})$ corresponds to a linear mapping $\mathcal{B}(A) \in GL(nk, \mathbb{F}_2)$ (see Eq. (4)).

In the context of quantum Reed–Solomon codes, we will use the cyclic discrete Fourier transform over $\mathbb{F}_{2^k}$ which can be implemented efficiently as a quantum circuit.

**Theorem 5.** *Let $n$ be a divisor of $2^k - 1$ and let $\alpha \in \mathbb{F}_{2^k}$ be an element of order $n$. Then the cyclic* DFT *of length $n$ over the field $\mathbb{F}_{2^k}$, given by the matrix*

$$\mathrm{DFT} = \left(\alpha^{ij}\right)_{i,j=0,\ldots,n-1} \tag{18}$$

*can be implemented on a quantum computer using $O(k^2 n^2)$ $CNOT$ gates.*

*Proof.* The condition $n|(2^k - 1)$ ensures that the field $\mathbb{F}_{2^k}$ contains a primitive $n$th root of unity $\alpha$. Thus, we have $\mathrm{DFT} \in GL(n, \mathbb{F}_{2^k})$. Fixing a basis $\mathcal{B}$ of $\mathbb{F}_{2^k}$, we obtain a linear transformation $\mathcal{B}(\mathrm{DFT}) \in GL(nk, \mathbb{F}_2)$ which can be implemented using $O(k^2 n^2)$ $CNOT$ gates using Theorem 4. □

# 5 Quantum Reed–Solomon Codes

## 5.1 Definition of Quantum Reed–Solomon Codes

First, we recall the definition of Reed–Solomon codes (see [16, Fig. 10.6]).

**Definition 3.** *A (classical) Reed–Solomon (RS) code of length $N = 2^k - 1$ over the field $\mathbb{F}_{2^k}$ is a cyclic code with generator polynomial*

$$\boldsymbol{g}(X) = (X - \alpha^b)(X - \alpha^{b+1}) \ldots (X - \alpha^{b+\delta-2}),$$

*where $\alpha$ is a primitive element of $\mathbb{F}_{2^k}$, i. e., an element of order $2^k - 1 = N$. The dimension of the code is $K = N - \delta + 1$ and the minimum distance is $\delta$.*

Alternatively, an RS code can be described by the *spectrum* with respect to the cyclic discrete Fourier transform of length $N$ over $\mathbb{F}_{2^k}$, see Eq. (18). For any vector $\boldsymbol{v} \in \mathbb{F}_{2^k}^N$, the spectrum is defined by

$$\widehat{\boldsymbol{v}} := \boldsymbol{v} \cdot \mathrm{DFT} = \left(\boldsymbol{v}(\alpha^i)\right)_{i=0,\ldots,N-1},$$

where $\boldsymbol{v}(X) = \sum_{j=0}^{N-1} v_j X^j$. Then for any codeword $\boldsymbol{c}$ of an RS code, $\widehat{\boldsymbol{c}}$ has $\delta - 1$ consecutive (possibly cyclically wrapped around) zeros starting at position $b$. Fixing the zeros in the spectrum, all codewords can be obtained by the inverse Fourier transform, i. e., the set of codewords is given by

$$C = \left\{\widehat{\boldsymbol{v}} \cdot \mathrm{DFT}^{-1} \mid \widehat{\boldsymbol{v}} \in \mathbb{F}_{2^k}^N,\ \widehat{v}_b = \widehat{v}_{b+1} = \ldots = \widehat{v}_{b+\delta-1} = 0\right\}, \tag{19}$$

where the indices are computed modulo $N$.

**Lemma 2.** *For $b = 0$ and $\delta > N/2 + 1$, RS codes are weakly self–dual.*

*Proof.* The generator polynomial of $C$ is $\boldsymbol{g}(X) = (X-1)(X-\alpha)\ldots(X-\alpha^{\delta-2})$. The generator polynomial of the dual code $C^\perp$ is the reciprocal polynomial of $(X^N-1)/\boldsymbol{g}(X)$, i. e.,

$$\begin{aligned} \boldsymbol{g}^\perp(X) &= (X-\alpha^{-(\delta-1)})(X-\alpha^{-\delta})\ldots(X-\alpha^{-(N-1)}) \\ &= (X-\alpha^1)(X-\alpha^2)\ldots(X-\alpha^{N-\delta+1}). \end{aligned}$$

For $\delta > N/2+1$, $N-\delta+1 \le \delta-2$. Thus $\boldsymbol{g}(X)^\perp$ is a divisor of $\boldsymbol{g}(X)$ which proves $C \le C^\perp$. □

The relation between the spectra of an RS code $C$ and its dual is illustrated in Fig. 3. The spectrum of any codeword $\boldsymbol{c} \in C$ is zero at the first $\delta-1$ positions,

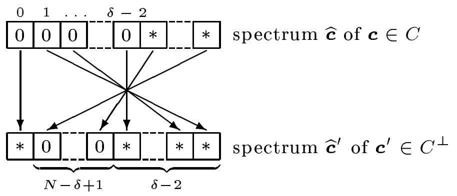



**Fig. 3.** Relation between the spectra of a Reed–Solomon code $C$ and its dual. Positions taking arbitrary values (marked with $*$) and positions being zero are interchanged

whereas the spectrum of any codeword $\boldsymbol{c}' \in C^\perp$ may take any value at the corresponding positions, the first one and the last $\delta-2$ positions. In contrast, the last $N-\delta+1$ positions of the spectrum of $\boldsymbol{c} \in C$ are arbitrary, and positions 1 to $N-\delta+1$ in the spectrum of $\boldsymbol{c}' \in C^\perp$ are zero.

Combining Lemma 2 and Corollary 1, we are ready to define quantum Reed–Solomon codes.

**Definition 4.** *Let $C = [N, K, \delta]$ where $N = 2^k-1$, $K = N-\delta+1$, and $\delta > N/2+1$ be a Reed–Solomon code over $\mathbb{F}_{2^k}$ (with $b = 0$). Furthermore, let $\mathcal{B}$ be a self–dual basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. Then the* quantum Reed–Solomon ($\mathcal{QRS}$) code *is the quantum error–correcting code $\mathcal{C}$ of length $kN$ derived from the weakly self–dual binary code $\mathcal{B}(C)$ according to Definition 2.*

The parameters of the $\mathcal{QRS}$ code are given by the following theorem.

**Theorem 6.** *The $\mathcal{QRS}$ code $\mathcal{C}$ of Definition 4 encodes $k(N-2K)$ qubits using $kN$ qubits. It is able to detect at least up to $K$ errors, i. e., the parameters are $\mathcal{C} = [[kN, k(N-2K), d \ge K+1]]$.*

*Proof.* The weakly self–dual binary code $\mathcal{B}(C)$ has length $kN$ and dimension $kK$. Hence, by Definition 2 the corresponding quantum code encodes $kN - 2kK = k(N-2K)$ qubits. The dual code $\mathcal{B}(C^\perp)$ has dimension $k(\delta-1)$ and minimum distance $d \ge K+1$. From Theorem 2 follows that the $\mathcal{QRS}$ code can detect up to $d-1 \ge K$ errors. □

### 5.2 Encoding Quantum Reed–Solomon Codes

Encoding of $\mathcal{QRS}$ codes is based on the quantum version of the cyclic discrete Fourier transform over $\mathbb{F}_{2^k}$ presented in Section 4. In the sequel, let $C$ be an RS code over $\mathbb{F}_{2^k}$ and let $\mathcal{B}$ be a self–dual basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. Furthermore, we fix a primitive element $\alpha \in \mathbb{F}_{2^k}$.

**Theorem 7.** *Let $\mathcal{C} = [[kN, k(N-2K), d > K]]$ where $N = 2^k - 1$, $K = N - \delta + 1$, and $\delta > N/2 + 1$ be a quantum Reed–Solomon code constructed from the Reed–Solomon code $C = [N, K, \delta]$ over $\mathbb{F}_{2^k}$. The transformation*

$$E = \mathcal{Q}(\mathcal{B}(\mathrm{DFT}^{-1})) \cdot \left(I_2^{\otimes k(\delta-1)} \otimes H^{\otimes kK}\right)$$

*operating on states of the form*

$$\underbrace{|\phi_1\rangle \otimes \ldots \otimes |\phi_k\rangle}_{k} \otimes \underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{kK} \otimes \underbrace{|\phi_{k+1}\rangle \otimes \ldots \otimes |\phi_{k(N-2K)}\rangle}_{k(N-2K-1)} \otimes \underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{kK}$$

*is an encoder for the $\mathcal{QRS}$ code. The corresponding quantum circuit is shown in Fig. 4.*

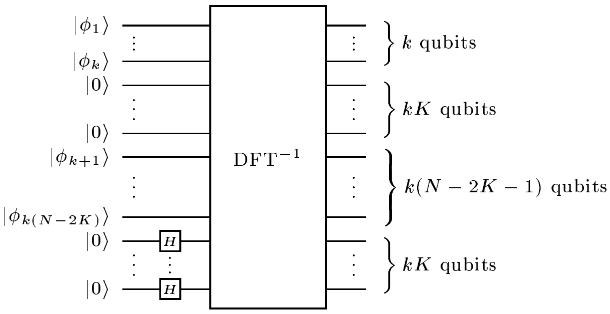



**Fig. 4.** Encoder for a quantum Reed–Solomon code

*Proof.* Similarly to Eq. (10), any basis state of the $\mathcal{QRS}$ code can be written as

$$|\psi_j\rangle = \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\mathcal{B}(\boldsymbol{c} + \boldsymbol{w}_j)\rangle, \tag{20}$$

where the coset representatives $\boldsymbol{w}_j \in C^\perp$ will be specified later. The first $\delta - 1$ positions of the spectrum of $\boldsymbol{c}$ are zero. From Eq. (19), the other positions may take any value. Thus computing the Fourier transform of the state (20) yields

$$\mathcal{Q}(\mathcal{B}(\mathrm{DFT}))|\psi_j\rangle = \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{i} \in \mathbb{F}_{2^k}^K} |\mathcal{B}(\underbrace{0, \ldots, 0}_{\delta-1}, i_1, \ldots, i_K) + \mathcal{B}(\widehat{\boldsymbol{w}_j})\rangle.$$

Without loss of generality, the last $K$ positions of $\widehat{\boldsymbol{w}_j}$ can be chosen to be zero. Hence applying the Hadamard transform to the last $kK$ qubits yields

$$\left(I_2^{\otimes k(\delta-1)} \otimes H^{\otimes kK}\right) \cdot \mathcal{Q}(\mathcal{B}(\mathrm{DFT}))|\psi_j\rangle = E^{-1}|\psi_j\rangle = |\mathcal{B}(\widehat{\boldsymbol{w}_j})\rangle.$$

Furthermore, positions $i = 1, \ldots, K$ of $\widehat{\boldsymbol{w}_j}$ are zero, too, since $\boldsymbol{w}_j \in C^\perp$ (see Fig. 3). For any set of values for the remaining positions, we get a different coset of $C$ in $C^\perp$. □

### 5.3 Decoding Quantum Reed–Solomon Codes

Decoding procedures for quantum Reed–Solomon codes follow the scheme of Fig. 1. The syndrome of a vector $\boldsymbol{v} \in \mathbb{F}_{2^k}^N$ are positions $i = 1, \ldots, K$ of the spectrum $\widehat{\boldsymbol{v}}$ of $\boldsymbol{v}$ which is obtained by computing the DFT of $\boldsymbol{v}$. This syndrome, indicating bit–flip–errors, is "copied" to $kK$ auxiliary qubits using $CNOT$ gates. Computing the inverse Fourier transform $\mathrm{DFT}^{-1}$ returns to the original basis. After a Hadamard transform, the same circuit is used to compute the syndrome of the phase–flip errors. The whole quantum circuit is shown in Fig. 5. Both the

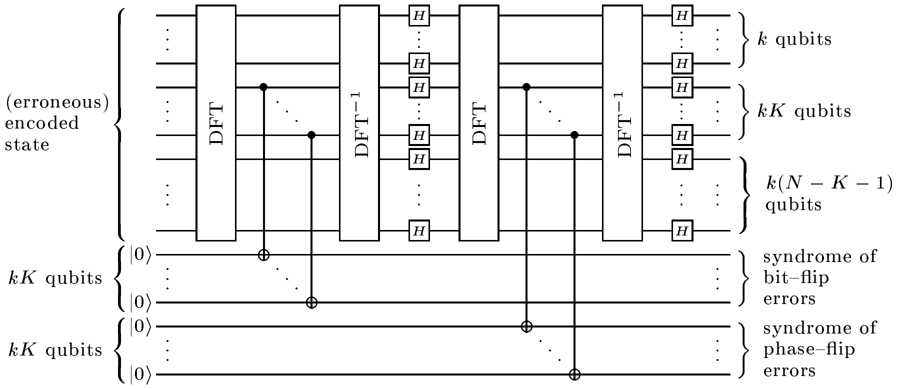



**Fig. 5.** Computation of the syndrome for a quantum Reed–Solomon code

syndrome of bit–flip errors and the syndrome of phase–flip errors are measured yielding *classical* syndrome vectors. Then the most likely positions of errors are computed using a classical algorithm, e. g., the Berlekamp–Massey algorithm or the Euclidean algorithm (see [16]).

The quantum circuit in Fig. 5 can be simplified using the following theorem.

**Theorem 8.** *Let* DFT *denote the cyclic discrete Fourier transform of length $n$ over the field $\mathbb{F}_{2^k}$ and be $\mathcal{B}$ a self–dual basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. Then the following identities hold:*

$$\begin{aligned}\mathcal{Q}(\mathcal{B}(\mathrm{DFT}^{-1})) \cdot H^{\otimes kn} \cdot \mathcal{Q}(\mathcal{B}(\mathrm{DFT})) &= H^{\otimes kn} \cdot \mathcal{Q}(\mathcal{B}(\pi)) \\ &= \mathcal{Q}(\mathcal{B}(\pi)) \cdot H^{\otimes kn},\end{aligned} \tag{21}$$

*where $\pi$ is the permutation $x \mapsto -x \bmod n$. Using the factorization on the right hand side of Eq. (21) instead of the factorization on the left hand side for the implementation as a quantum circuit reduces the complexity from $O(k^2n^2)$ to $O(kn)$.*

*Proof.* Let $D := \mathcal{B}(\mathrm{DFT})$ denote the binary matrix obtained by replacing each entry $\alpha^{ij}$ of DFT by $M_{\mathcal{B}}(\alpha^{ij})$. For a self–dual basis, $M_{\mathcal{B}}(\alpha^{ij})$ is symmetric (see Eq. (3)), and the Fourier matrix is symmetric, too. Hence the matrix $D$ is also symmetric. Using Dirac notation, the matrices read

$$\mathcal{Q}(D) = \sum_{\boldsymbol{x}\in\mathbb{F}_2^{kn}} |\boldsymbol{x}D\rangle\langle\boldsymbol{x}| = \sum_{\boldsymbol{x}\in\mathbb{F}_2^{kn}} |\boldsymbol{x}\rangle\langle\boldsymbol{x}D^{-1}| \quad \text{and} \quad H^{\otimes kn} = \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{x}\rangle\langle\boldsymbol{y}|.$$

Multiplying the matrices results in

$$\begin{aligned}
&\mathcal{Q}(D^{-1})H^{\otimes kn}\mathcal{Q}(D)\\
&\quad= \sum_{\boldsymbol{u}\in\mathbb{F}_2^{kn}}\ \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}}\ \sum_{\boldsymbol{v}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{u}D^{-1}\rangle \underbrace{\langle\boldsymbol{u}|\boldsymbol{x}\rangle}_{=\delta_{\boldsymbol{u}\boldsymbol{x}}} \underbrace{\langle\boldsymbol{y}|\boldsymbol{v}\rangle}_{=\delta_{\boldsymbol{y}\boldsymbol{v}}} \langle\boldsymbol{v}D^{-1}|\\
&\quad= \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{x}D^{-1}\rangle\langle\boldsymbol{y}D^{-1}| = \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}D\cdot\boldsymbol{y}D}|\boldsymbol{x}\rangle\langle\boldsymbol{y}|.
\end{aligned}$$

The inner product of $\boldsymbol{x}D$ and $\boldsymbol{y}D$ is the same as the inner product of $\boldsymbol{x}DD^{\mathsf{t}}$ and $\boldsymbol{y}$. Since $D$ is symmetric, $DD^{\mathsf{t}} = D^2 = \mathcal{B}(\mathrm{DFT}^2) = \mathcal{B}(\pi)$. Finally, we obtain

$$\begin{aligned}
&\mathcal{Q}(D^{-1})H^{\otimes kn}\mathcal{Q}(D)\\
&\quad= \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{x}\rangle\langle\boldsymbol{y}\mathcal{B}(\pi)| = \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{x}\rangle\langle\boldsymbol{y}| \sum_{\boldsymbol{v}\in\mathbb{F}_2^{kn}} |\boldsymbol{v}\rangle\langle\boldsymbol{v}\mathcal{B}(\pi)|\\
&\quad= \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{x}\mathcal{B}(\pi)\rangle\langle\boldsymbol{y}| = \sum_{\boldsymbol{v}\in\mathbb{F}_2^{kn}} |\boldsymbol{v}\mathcal{B}(\pi)\rangle\langle\boldsymbol{v}| \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^{kn}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{x}\rangle\langle\boldsymbol{y}|.
\end{aligned}$$

□

From Eq. (21) in the preceding theorem it follows that

$$\mathcal{Q}(\mathcal{B}(\mathrm{DFT}^{-1}))\cdot H^{\otimes kn} = \mathcal{Q}(\mathcal{B}(\pi))\cdot H^{\otimes kn}\mathcal{Q}(\mathcal{B}(\mathrm{DFT}^{-1})). \tag{22}$$

Using the identities (21) and (22), and conjugating the $CNOT$ gates by the permutation of qubits $\mathcal{Q}(\mathcal{B}(\pi))$, we obtain the simplified quantum circuit shown in Fig. 6.

## 6 Example

We construct a quantum Reed–Solomon code from an RS code over the field $\mathbb{F}_8$. We choose $\delta = 5$ and obtain an RS code $C = [7, 3, 5]$ with generator polynomial

$$\boldsymbol{g}(X) = (X - \alpha^0)(X - \alpha^1)(X - \alpha^2)(X - \alpha^3),$$

where $\alpha$ is a primitive element of $\mathbb{F}_8$ fulfilling $\alpha^3 + \alpha + 1 = 0$. The dual code $C^\perp = [7, 4, 4]$ is generated by

$$\boldsymbol{g}^\perp(X) = (X - \alpha^{-4})(X - \alpha^{-5})(X - \alpha^{-6}) = (X - \alpha^3)(X - \alpha^2)(X - \alpha^1).$$

From Theorem 6, the resulting $\mathcal{QRS}$ code has parameters $\mathcal{C} = [[21, 3, d \geq 4]]$.

As self–dual basis of $\mathbb{F}_8$ we choose $\mathcal{B} = (\alpha^3, \alpha^6, \alpha^5)$. The binary expansions of $C$ and $C^\perp$ yield binary codes $C_2 = \mathcal{B}(C) = [21, 9, 8]$ and $C_2^\perp = \mathcal{B}(C^\perp) = [21, 12, 5]$. Thus the $\mathcal{QRS}$ code has parameters $\mathcal{C} = [[21, 3, 5]]$.

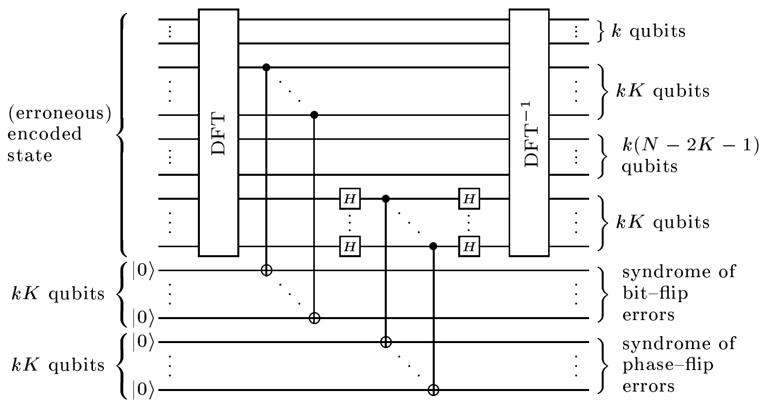



**Fig. 6.** Simplified quantum circuit for computing the syndrome for a $\mathcal{QRS}$ code

## 7 Conclusion

Most quantum error–correcting codes known so far are based on classical binary codes or codes over $GF(4) = \mathbb{F}_{2^2}$ (see [4]). In this paper, we have demonstrated how codes over extension fields of higher degree can be used. They might prove useful, e. g., for concatenated coding.

The spectral techniques for encoding and decoding presented in this paper do not only apply to Reed–Solomon codes, but in general to all cyclic codes. The main advantage of Reed–Solomon codes is that no field extension is necessary. The same is true for all BCH codes of length $n$ over the field $\mathbb{F}_{2^k}$ where $n|2^k - 1$. In addition to the spectral techniques, cyclic codes provide a great variety of encoding/decoding principles, e. g., based on linear shift registers that can be translated into quantum algorithms (see [10]).

The quantum implementation of linear mappings over finite fields presented in Section 4 enlarges the set of efficient quantum subroutines. In contrast, the transforms used in most quantum algorithms—such as cyclic and generalized Fourier transforms—are defined over the complex field (see, e. g., [17]).

It has to be investigated how efficient fully quantum algorithms for error–correction can be obtained, e. g., using quantum versions of the Berlekamp–Massey algorithm or of the Euclidean algorithm.

## Acknowledgments

The authors would like to thank Martin Rötteler and Rainer Steinwandt for numerous stimulating discussions during the process of writing this paper. Part of this work was supported by *Deutsche Forschungsgemeinschaft, Schwerpunkt-programm QIV (SPP 1078), Projekt AQUA (Be 887/13-1).*

## References


1. A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Physical Review A, 52 (1995), pp. 3457–3467.
2. A. Berthiaume, *Quantum Computation*, in Complexity Theory Retrospective II, L. A. Hemaspaandra and A. L. Selman, eds., Springer, New York, 1997, pp. 23–51.
3. T. Beth and M. Grassl, *The Quantum Hamming and Hexacodes*, Fortschritte der Physik, 46 (1998), pp. 459–491.
4. A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum Error Correction Via Codes over GF(4)*, IEEE Transactions on Information Theory, IT–44 (1998), pp. 1369–1387.
5. A. R. Calderbank and P. W. Shor, *Good quantum error–correcting codes exist.*, Physical Review A, 54 (1996), pp. 1098–1105.
6. J. I. Cirac and P. Zoller, *Quantum Computation with Cold Trapped Ions*, Physical Review Letters, 74 (1995), pp. 4091–4094.
7. D. G. Cory, A. F. Fahmy, and T. F. Havel, *Ensemble Quantum Computing by Nuclear Resonance Spectroscopy*, Technical Report TR–10–96, B. C. M. P., Harvard Medical Medical School, Boston, Dec. 1996.
8. P. M. A. Dirac, *The Principles of Quantum Mechanics*, Clarendon Press, Oxford, 4th ed., 1958.
9. W. Geiselmann, *Algebraische Algorithmenentwicklung am Beispiel der Arithmetik in endlichen Körpern*, Shaker, Aachen, 1994. Zugleich Dissertation, Universität Karlsruhe, 1993.
10. M. Grassl and T. Beth, *Codierung und Decodierung zyklischer Quantencodes*, in Fachtagung Informations– und Mikrosystemtechnik, B. Michaelis and H. Holub, eds., Magdeburg, 25–27 Mar. 1998.
11. M. Grassl, T. Beth, and T. Pellizzari, *Codes for the Quantum Erasure Channel*, Physical Review A, 56 (1997), pp. 33–38.
12. L. K. Grover, *A fast quantum mechanical algorithm for database search*, in Proceedings 28th Annual ACM Symposium on Theory of Computing (STOC), New York, 1996, ACM, pp. 212–219.
13. D. Jungnickel, *Finite Fields*, BI–Wissenschaftsverlag, Mannheim, 1993.
14. E. Knill and R. Laflamme, *Concatenated Quantum Codes.* LANL preprint quant–ph/9608012, 1996.
15. ———, *Theory of quantum error–correcting codes*, Physical Review A, 55 (1997), pp. 900–911.
16. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, North–Holland, Amsterdam, 1977.
17. M. Püschel, M. Rötteler, and T. Beth, *Fast Quantum Fourier Transforms for a Class of Non–abelian Groups*, in Proceedings AAECC–13, 1999.
18. P. W. Shor, *Polynomial–Time Algorithms for Prime Factorization and Discrete Logarithms*, in Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE Computer Society Press, Nov. 1994, pp. 124–134.
19. A. Steane, *Error Correcting Codes in Quantum Theory*, Physical Review Letters, 77 (1996), pp. 793–797.
20. ———, *Multiple Particle Interference and Quantum Error Correction*, Proceedings of the Royal Society London Series A, 452 (1996), pp. 2551–2577.
21. ———, *Quantum computing*, Reports on Progress in Physics, 61 (1998), pp. 117–173.