QUANTUM BCH CODES

Markus Grassl and Thomas Beth
Institut für Algorithmen und Kognitive Systeme (IAKS)
Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany
Email: grassl@ira.uka.de, EISS_Office@ira.uka.de

Abstract

After a brief introduction to both quantum computation and quantum error correction, we show how to construct quantum error-correcting codes based on classical BCH codes. With these codes, decoding can exploit additional information about the position of errors. This error model—the quantum erasure channel—is discussed. Finally, parameters of quantum BCH codes are provided.

1 Introduction

Motivated by the statement

"*BCH codes are among the best (classical) codes we know*"

(cited from Ch. 9, §1, p. 258 of [14]), we present the translation of classical Bose-Chaudhuri-Hocquenghem (BCH) codes into quantum quantum error-correcting codes. Without error correction, the promising new field of quantum computing (see, e. g., [16, 13]) would be mainly of theoretical nature. A main ingredient of quantum computation is constructive and destructive interference of different computation paths which is only possible when using quantum states. But on the other hand, any possible computing device exploiting quantum mechanics has to cope with uncontrollable interactions with the environment, e. g., single photons. Quantum error-correcting codes help to actively reduce the decoherence due to coupling to the environment.

2 Background

2.1 Quantum Registers

Classically, information is often represented by bits. A single bit takes either the value 0 or 1. In physical systems, 0 and 1 are represented by two different states of the system. These could be two different voltages, signals with two different frequencies, but also states on the quantum mechanical level, e. g., ground state and excited state of an electron of an atom or ion, the spin of a nucleus, or the polarization of photons. In Dirac notation [7], the two states are written as

$$\text{“0”} \mathrel{\hat{=}} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathrm{C}^2$$

and

$$\text{“1”} \mathrel{\hat{=}} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathrm{C}^2.$$

In quantum mechanics, the principle of superposition allows a system to be simultaneously in different states. Mathematically, the state of the basic unit of quantum information, a *quantum bit* (or short *qubit*), is represented by the normalized linear combination

$$|q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \text{where } \alpha, \beta \in \mathrm{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

The normalization condition stems from the fact that when extracting classical information from the quantum system by a measurement, the values 0 and 1 occur with probability $|\alpha|^2$ and $|\beta|^2$, resp.

Similar to classical registers, a quantum register is built by combining several qubits. Mathematically, this corresponds to the tensor product of two-dimensional vector spaces[1]. Hence the state of a quantum register of length n can be any normalized complex linear combination of the 2^n mutually orthogonal basis states

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

2.2 Quantum Gates

The laws of quantum mechanics say that any transformation on quantum systems is linear. Furthermore, in order to preserve the normalization any operation has to be unitary. Let us first consider operations involving only one qubit, i. e., one subsystem. Similar to the classical NOT gate, there is a quantum operation exchanging the states $|0\rangle$ and $|1\rangle$ given by the matrix

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

But on a single qubit, there is not only this “classical” operation. Examples for non-classical operations on single qubits are given by

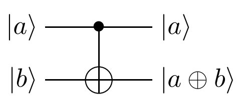
$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1}$$

Besides single qubit operations, the so-called controlled NOT gate ($CNOT$) plays an important rôle since any unitary operation on a 2^n-dimensional space can be implemented using only single qubit operations and $CNOT$ gates (see [1]). As a classical gate, the $CNOT$ gate corresponds to a gate with two inputs and two outputs. One of the inputs is copied to the first output, the second output is the XOR of the inputs. The transformation matrix of the

[1] In quantum mechanics, the underlying structures are *Hilbert spaces*. We do not stress this fact since here all vector spaces are finite dimensional and thus complete w. r. t. the standard Hermitian inner product.

$CNOT$ gate is given by:

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



On the right hand side, the notation for the $CNOT$ gate as a quantum circuit is given. Each of the horizontal lines (*wires*) corresponds to a qubit of the whole quantum register. The dot on the upper wire indicates that the transformation on the lower qubit (the target)—a NOT gate—is only applied when the state of the upper qubit (the control) is $|1\rangle$. More examples for quantum circuits can be found in [15].

3 Quantum Error Correction

Classically, a major technique for protecting information against channel errors is to add redundant information. The simplest example is a repetition code where information is replicated by the sender. At the receiver's end of the channel, the most likely information is chosen based on comparing all received messages and taking a majority vote.

This technique cannot be translated directly to quantum systems since it is not possible to copy unknown quantum information (*no-cloning theorem* [19]), and comparison of quantum states is only possible statistically. Nevertheless, quantum states can be protected against errors. The main idea is to embed quantum information represented by k qubits into a larger Hilbert space of n qubits where $n > k$.

For the construction of quantum error-correcting codes, we have to model which types of errors occur during the transmission over a quantum channel. This topic will be addressed next.

3.1 Error Models

3.1.1 Open Quantum Systems

We assume that our quantum system interacts with an environment which is not or only partially accessible. Nevertheless, we can *model* the interaction by a unitary transformation $U_{\text{interaction}} = U_{\text{int}}$ on the Hilbert space formed by the system and its environment. Assuming that there is no prior entanglement of the system with the environment, the interaction operator reads as

$$|\psi\rangle_{\text{sys}} \otimes |\Psi\rangle_{\text{env}} \longmapsto U_{\text{interaction}} \left(|\psi\rangle_{\text{sys}} \otimes |\Psi\rangle_{\text{env}} \right).$$

After this interaction, the state need no longer be a tensor product. Since we cannot control the environment, we have to discard any information about the environment. This is mathematically reflected by *tracing out the environment*:

$$\begin{aligned} \rho_{\text{sys}} &= \text{Tr}_{\text{env}} \left(U_{\text{int}} \left(|\psi\rangle \langle\psi|_{\text{sys}} \otimes |\Psi\rangle \langle\Psi|_{\text{env}} \right) U_{\text{int}}^{\dagger} \right) \\ &= \sum_j A_j \left(|\psi\rangle \langle\psi|_{\text{sys}} \right) A_j^{\dagger}. \end{aligned} \quad (2)$$

The state of our quantum system is now, in general, a mixed state given by the density operator ρ_{sys}. One interpretation of a mixed quantum state is that we have an ensemble of pure quantum states chosen according to a probability distribution. In our case, one can think of a measurement performed on the environment. Due to entanglement with the system, this may lead to different states of the system depending on the measurement outcome—but we do not know which one since the result of the measurement is discarded.

In order to model a quantum channel, we make use of equation (2). The disturbed quantum state ρ_{sys} can be expressed only in terms of the initial state $|\psi\rangle \langle\psi|_{\text{sys}}$ of the system and some interaction operators A_j which completely specify the channel.

For a single qubit, i. e., a two-dimensional quantum system, the operators A_j can be chosen to be proportional to the identity operator and the Pauli matrices

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

where ($i^2 = -1$). Surprisingly, in order to correct an arbitrary error it is sufficient to be able to correct any of these four errors.

For more than one qubit, an *error basis* can be formed by tensor products of the one qubit interaction operators. A common assumption is that the errors act independently on each qubit. Furthermore, errors are assumed to be small, i. e., *near* identity (with respect to a suitable operator norm). Then errors with a small number of tensor factors different from identity are *more likely* than those errors with a large number of tensor factors different from identity.

3.1.2 Depolarizing and Erasure Channel

To illustrate the preceding, we consider two important quantum channels. Over a depolarizing channel [2], quantum information is transmitted undisturbed with probability $1 - \varepsilon$, and it is replaced by a completely randomized quantum state with probability ε. In this case, equation (2) reads

$$\begin{aligned} \rho_{\text{sys}} &= (1-\varepsilon) \cdot |\psi\rangle \langle\psi|_{\text{sys}} + \epsilon \cdot 1 \\ &= (1 - 3/4 \cdot \varepsilon)\, id \left(|\psi\rangle \langle\psi|_{\text{sys}} \right) id \\ &\quad + \varepsilon/4 \sum_{j=x,y,z} \sigma_j \left(|\psi\rangle \langle\psi|_{\text{sys}} \right) \sigma_j. \end{aligned}$$

A related quantum channel is the quantum erasure channel [11]. Again, the quantum state is transmitted undisturbed with probability $1 - \varepsilon$. In case of an error, the quantum state is replaced by a quantum state $|e\rangle$ that is orthogonal to all other quantum states. Equation (2) now reads

$$\rho_{\text{sys}} = (1-\varepsilon) \cdot |\psi\rangle \langle\psi|_{\text{sys}} + \epsilon \cdot |e\rangle \langle e|.$$

Similar to classical erasures, the state $|e\rangle$ indicates that an error occurred, i. e., side-information about positions of errors is available for the decoding process. Note that we have increased the dimension of the Hilbert space of the

system by one adding the state $|e\rangle$. Alternatively, we may use any state of the original space instead of $|e\rangle$ and describe the positions of errors by other means.

3.2 Code Constructions

In this section, we will briefly describe several constructions of quantum error-correcting codes based on classical linear error-correcting codes. As discussed above, for qubit systems it is sufficient to be able to correct any error that is a tensor product of identity and Pauli matrices. The *weight* of such an error (or the *number of errors*) is defined as the number of tensor factors different from identity. Moreover, as $\sigma_y = i\sigma_x\sigma_z$ we can restrict ourselves to no-error, σ_x-errors, σ_z-errors, and combinations of them. The operator σ_x interchanges the states $|0\rangle$ and $|1\rangle$. Hence, it corresponds to a classical bit-flip error. The operator σ_z changes the relative phase of $|0\rangle$ and $|1\rangle$ and has no classical counterpart. But the operator σ_z interchanges the orthogonal states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$, i. e., it acts as a bit-flip with respect to this basis. Hence, the corresponding change of basis—the Hadamard transform H (see equation (1))—interchanges bit-flip and phase-flip errors:

$$H\sigma_x H = \sigma_z \quad \text{and} \quad H\sigma_z H = \sigma_x.$$

In summary, this enables us to use certain classical linear binary codes for the construction of quantum codes.

The following construction is due to [17, 18] and [6]. More details (and proofs) can also be found in [3, 10].

Construction 3.1 (Binary Codes)
Let $C = [n, k, d]$ be a weakly self-dual linear binary code, i. e., C is contained in its dual $C^\perp = [n, n-k, d^\perp]$. Furthermore, let $\{\boldsymbol{w}_j : 0 \le j \le 2^{n-2k}\}$ be a system of coset representatives of $C^\perp/C$.

Then the 2^{n-2k} mutually orthogonal states

$$|\psi_j\rangle = \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c}\in C} |\boldsymbol{c} + \boldsymbol{w}_j\rangle \tag{3}$$

span a quantum error-correcting code $\mathcal{C} = [[n, n-2k]]$ of length n and dimension 2^{n-2k} (The notation is similar to that for classical linear block codes.) Based on classical decoding algorithms for the code $C^\perp$, up to $(d^\perp - 1)/2$ errors can be corrected. Moreover, the code can correct errors up to weight $(d' - 1)/2$ where

$$d' = \min\{\operatorname{wgt} \boldsymbol{c} : \boldsymbol{c} \in C^\perp \setminus C\} \ge d^\perp. \tag{4}$$

The outline of the decoding process is as follows: Any superposition of code states $|\psi_j\rangle$ is a superposition of quantum states corresponding to codewords of the dual code $C^\perp$. A (correctable) bit-flip error takes the superposition of codewords into a superposition of the corresponding coset. Similar to classical decoding algorithms, this coset can be identified by computing an error syndrome using auxiliary qubits. Measuring this syndrome reveals information about the error, but not about the original superposition. After correction of the bit-flip errors, a Hadamard transform turns the remaining phase-flip errors into sign-flip errors. The Hadamard transform changes the code state (3) into

$$H^{\otimes n} |\psi_j\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{\boldsymbol{c}\in C^\perp} (-1)^{\boldsymbol{c}\cdot\boldsymbol{w}_j} |\boldsymbol{c}\rangle . \tag{5}$$

Here $\boldsymbol{c} \cdot \boldsymbol{w}_j$ is the standard inner product $\boldsymbol{x} \cdot \boldsymbol{y} = \sum_i x_i y_i$. Again, any superposition of states (5) is a superposition of quantum states corresponding to codewords of the dual code $C^\perp$. Hence the errors can be corrected in the same manner. The last step is another Hadamard transform returning to the original basis.

A generalization of this construction was given in [8] and [5]. It is based on the algebraic properties of the group generated by tensor products of Pauli matrices (see also [3]). Here we will only present the prerequisites and the parameters of the resulting quantum codes. Furthermore, we restrict ourselves to linear codes (in contrast to *additive* codes).

Construction 3.2 (Quaternary Codes)
By $\overline{x}$ we denote the conjugation $x \mapsto x^2 =: \overline{x}$ in the field $\mathrm{F}_4 = GF(4) = \{0, 1, \omega, \overline{\omega} = \omega^2 = \omega + 1\}$. Furthermore, for a linear space $C \le \mathrm{F}_4^n$, by C^* we denote the linear space that is orthogonal with respect to the inner product $\boldsymbol{x} \cdot \boldsymbol{y} := \sum_j \overline{x_j} y_j$.

Let $C = [n, k, d]$ be a self-orthogonal linear quaternary code, i. e., C is contained in $C^* = [n, n-k, d^*]$.

Then a quantum error-correcting code $\mathcal{C} = [[n, n-2k]]$ of length n and dimension 2^{n-2k} exists. Based on classical decoding algorithms for the code C^*, up to $(d^* - 1)/2$ errors can be corrected. Moreover, the code can correct errors up to weight $(d' - 1)/2$ where

$$d' = \min\{\operatorname{wgt} \boldsymbol{c} : \boldsymbol{c} \in C^* \setminus C\} \ge d^*. \tag{6}$$

Note that $C^\perp$ and C^* are related by conjugation and thus $d^* = d^\perp$.

Recently, it has been shown how to use linear codes over any finite field of characteristic two, i. e., fields F_{2^ℓ} with 2^ℓ elements for the construction of quantum error-correcting codes [12]. Again, we only present the main parameters of the construction.

Construction 3.3 (Codes from Extension Fields)
Let $C = [n, k, d]$ be a weakly self-dual code over F_{2^ℓ}, i. e., C is contained in its dual $C^\perp = [n, n-k, d^\perp]$ (with respect to the standard inner product). Furthermore, let B be a self-dual basis of F_{2^ℓ} over F_2.

Expanding each element of F_{2^ℓ} with respect to the basis B yields a weakly self-dual linear binary code $C_2 = [\ell n, \ell k, d_2 \ge d]$. Its dual $C_2^\perp = [\ell n, \ell(n-k), d_2^\perp \ge d^\perp]$ is obtained in the same manner.

Based on the classical codes C_2 and $C_2^\perp$, a quantum error-correcting code can be obtained using Construction 3.1. The resulting quantum code can be decoded as a binary code or as a code over the field F_{2^ℓ}. In the latter case, ℓ qubits are grouped into one block, and errors can be corrected if they are restricted to up to $(d^\perp - 1)/2$ blocks.

4 Quantum BCH Codes

The quantum version of binary BCH codes was introduced in [11]. In [5], the term quantum BCH code was used for quaternary quantum BCH codes (see Construction 3.2). In the context of [11], for the quantum erasure channel, it is important to use codes that allow the use of the side-information on the positions of the errors provided by the channel. For BCH codes, a variety of such decoding algorithms exists. Being cyclic codes, BCH codes allow also decoding based on spectral techniques. This is in particular true for Reed-Solomon (RS) codes where no field extension is needed to implement the Fourier transform. The quantum version of RS codes and their spectral decoding is discussed in [12]. Another technique for encoding and decoding cyclic codes is based on linear shift registers (see [9]).

In the sequel, we focus on the definition and the computation of the parameters of quantum BCH codes, supplemented by examples in Section 5. A good reference for the theory of classical error-correcting codes is [14]. All theorems below can be found in a similar version in [11] and [5], we will omit the proofs.

Definition 4.1 ($\mathcal{Q}$BCH Codes)
A quantum BCH code ($\mathcal{Q}$BCH code) is a quantum error-correcting code that is derived from a classical, weakly self-dual (respectively self-orthogonal) BCH code using Construction 3.1, 3.2, or 3.3.

Usually, BCH codes are specified by the *zero sets*, i. e., the exponents of the roots α^z of their generator polynomial $g(X)|X^n-1$ where α is a primitive n-th root of unity. For a BCH code over the field F_q, the zero set is a union of cyclotomic cosets modulo n closed under multiplication by q, i. e.,

$$\mathcal{Z}_C = \bigcup_z C_z \quad \text{where } C_z = \{q^i z \bmod n : i \geq 0\}.$$

The zero sets of a code and its dual are related as follows.

Theorem 4.2 *Let $\mathcal{Z}_C$ denote the zero set of a BCH code C over the field F_q, i. e., the generator polynomial of C is given by*

$$g(X) = \prod_{z \in \mathcal{Z}_C} (X - \alpha^z).$$

Then the generator polynomial of the dual code $C^\perp$ is given by

$$h(X) = \prod_{z \in \{0,\ldots,n-1\} \setminus \mathcal{Z}_C} (X - \alpha^{-z}),$$

i. e., the zero set of the dual code is given by

$$\mathcal{Z}_{C^\perp} = \{-z \bmod n : z \in \{0,\ldots,n-1\} \setminus \mathcal{Z}_C\}.$$

For codes over F_4, the generator polynomial of the orthogonal code C^* is given by

$$h(X) = \prod_{z \in \{0,\ldots,n-1\} \setminus \mathcal{Z}_C} (X - \alpha^{-2z}),$$

i. e., the zero set of the orthogonal code is given by

$$\mathcal{Z}_{C^*} = \{-2z \bmod n : z \in \{0,\ldots,n-1\} \setminus \mathcal{Z}_C\}.$$

Corollary 4.3 *A BCH code is weakly self-dual if and only if $\mathcal{Z}_{C^\perp} \subseteq \mathcal{Z}_C$ or, equivalently,*

$$\forall z : (z \in \mathcal{Z}_{C^\perp} \Rightarrow (-z \bmod n) \notin \mathcal{Z}_C).$$

A BCH code over F_4 is self-orthogonal if and only if $\mathcal{Z}_{C^*} \subseteq \mathcal{Z}_C$ or, equivalently,

$$\forall z : \left(z \in \mathcal{Z}_{C^*} \Rightarrow (-2^{-1} z \bmod n) \notin \mathcal{Z}_C\right).$$

A lower bound for the minimum distance of a BCH code—and in turn for the corresponding $\mathcal{Q}BCH$ code—can be derived from its zero set.

Theorem 4.4 (BCH bound) *If the zero set $\mathcal{Z}_{C^\perp}$ of the dual of a weakly self-dual BCH code C contains $d_{BCH}-1$ consecutive numbers, i. e.,*

$$\bigcup_{z=z_0}^{z_0+d_{BCH}-2} C_z \subseteq \mathcal{Z}_{C^\perp}, \tag{7}$$

then the minimum distance $d^\perp$ of $C^\perp$ is at least d_{BCH}.

On the other hand, if a BCH code is specified by the left hand side of equation (7), d_{BCH} is called the *designed distance*.

The actual minimum distance of a BCH code may be larger than d_{BCH}. This yields another lower bound for the error correcting capability of the $\mathcal{Q}BCH$ code.

Theorem 4.5 (Code bound) *The minimum distance of a $\mathcal{Q}BCH$ code is at least the minimum distance $d^\perp$ of the dual $C^\perp = [n, n-k, d^\perp]$ of the underlying BCH code.*

According to equations (4) and (6), the true minimum distance of a $\mathcal{Q}BCH$ code may be even larger, see the examples in the next section.

5 Examples

Finally, we present the main results of this paper. Using the computer algebra system MAGMA [4], we have computed the parameters for $\mathcal{Q}$BCH codes derived from classical BCH codes over various fields (see Tables 1–6).

In Table 1 parameters of binary $\mathcal{Q}$BCH codes are given. A noteable code is the one with parameters $\mathcal{C} = [[49, 1, 9]]$. The corresponding BCH code is $C^\perp = [49, 25, 4]$ and $C = [49, 24, 4]$ is the even weight subcode of $C^\perp$. Therefore, $d' = \min\{\mathrm{wgt}\, \boldsymbol{c} : \boldsymbol{c} \in C^\perp \setminus C\}$ must be odd. Computing the weight distribution of $C^\perp$, we obtain $d' = 9$.

Similarly, for the code $\mathcal{C} = [[89, 1, 17]]$ the BCH bound yields $d' \geq 7$, whereas the actual minimum distance of the BCH code $C^\perp$ is $d^\perp = 12$. Again, $C = [89, 44, 12]$ is the even weight subcode of $C^\perp$, hence $d' \geq 13$ and d' is odd. Sampling codewords at random, we find $d' \leq 17$. Moreover, using MAGMA we were able to show that indeed $d' = 17$.

Quaternary $\mathcal{Q}$BCH codes are listed in Table 2. Here are the codes $\mathcal{C} = [[25, 1, 9]]$ and $\mathcal{C} = [[35, 1, 9]]$ of special interest. For the first code, the BCH bound yields $d' \geq 4$, the minimum distance of both C and C^* is $d = 8$, but the minimum distance of the quantum code is $d' = 9$. For $\mathcal{C} = [[35, 1, 9]]$, we obtain $d_{\text{BCH}} = 5$, $d = 8$, and $d' = 9$.

Finally, in Tables 3–6 we present $\mathcal{Q}$BCH codes constructed from BCH codes over fields of size 8, 16, 32, and 64. The corresponding binary codes are obtained by expanding each element of the extension field with respect to a fixed self-dual basis. For these codes, we have listed both the minimum distance d_2 as binary code and the minimum distance d_q as code over the field F_q which is relevant for blockwise decoding.

$[[7, 1, 3]]$	$[[69, 3, 11]]$	$[[95, 23, 5]]$
$[[15, 7, 3]]$	$[[69, 25, 3]]$	$[[103, 1, 19]]$
	$[[69, 47, 2]]$	
$[[21, 3, 5]]$	$[[71, 1, 11]]$	$[[105, 37, 9]]$
$[[21, 9, 3]]$		$[[105, 45, 7]]$
$[[21, 15, 2]]$	$[[73, 19, 9]]$	$[[105, 61, 5]]$
	$[[73, 37, 6]]$	$[[105, 75, 4]]$
$[[23, 1, 7]]$	$[[73, 55, 3]]$	$[[105, 91, 3]]$
$[[31, 1, 7]]$	$[[75, 35, 3]]$	$[[105, 99, 2]]$
$[[31, 11, 5]]$	$[[75, 67, 2]]$	
$[[31, 21, 3]]$		$[[111, 39, 3]]$
	$[[77, 11, 6]]$	
$[[35, 5, 6]]$	$[[77, 17, 3]]$	$[[115, 5, 14]]$
$[[35, 11, 3]]$	$[[77, 71, 2]]$	$[[115, 27, 5]]$
$[[35, 29, 2]]$		$[[115, 93, 2]]$
	$[[79, 1, 15]]$	
$[[39, 15, 3]]$	$[[85, 53, 5]]$	$[[117, 45, 9]]$
	$[[85, 69, 3]]$	$[[117, 69, 7]]$
$[[45, 13, 5]]$		$[[117, 93, 3]]$
$[[45, 21, 3]]$	$[[87, 31, 3]]$	
$[[45, 37, 2]]$		$[[119, 23, 7]]$
	$[[89, 1, 17]]^b$	$[[119, 65, 6]]$
$[[47, 1, 11]]$	$[[89, 23, 11]]$	$[[119, 71, 3]]$
	$[[89, 45, 7]]$	$[[119, 113, 2]]$
$[[49, 1, 9]]^a$	$[[89, 67, 4]]$	
$[[49, 7, 3]]$		$[[123, 83, 3]]$
$[[49, 43, 2]]$	$[[91, 43, 7]]$	
	$[[91, 67, 3]]$	$[[127, 1, 19]]$
$[[51, 35, 3]]$	$[[91, 85, 2]]$	$[[127, 15, 16]]$
		$[[127, 29, 15]]$
$[[55, 15, 5]]$	$[[93, 13, 12]]$	$[[127, 43, 13]]$
	$[[93, 23, 9]]$	$[[127, 57, 11]]$
$[[63, 27, 7]]$	$[[93, 33, 8]]$	$[[127, 71, 9]]$
$[[63, 39, 5]]$	$[[93, 43, 7]]$	$[[127, 85, 7]]$
$[[63, 45, 4]]$	$[[93, 63, 5]]$	$[[127, 99, 5]]$
$[[63, 51, 3]]$	$[[93, 73, 3]]$	$[[127, 113, 3]]$
$[[63, 57, 2]]$	$[[93, 83, 2]]$	

[a] The code bound yields only $d \geq 4$.
[b] The code bound yields only $d \geq 12$.

Table 1: Parameters of some binary $\mathcal{Q}$BCH codes given in the form $[[n, k, d]]$.

6 Acknowledgments

The authors would like to thank Rainer Steinwandt for his comments. This work was supported by *Deutsche Forschungsgemeinschaft (DFG), Schwerpunktprogramm Quanten-Informationsverarbeitung (SPP 1078), Projekt AQUA (Be 887/13-1)*.

$[[5, 1, 3]]$	$[[29, 1, 11]]$	$[[45, 41, 2]]$
$[[7, 1, 3]]$	$[[31, 1, 7]]$	$[[47, 1, 11]]$
$[[13, 1, 5]]$	$[[31, 11, 5]]$	$[[49, 1, 9]]^c$
	$[[31, 21, 3]]$	$[[49, 7, 3]]$
$[[15, 3, 5]]$	$[[35, 1, 9]]^b$	$[[49, 43, 2]]$
$[[15, 7, 3]]$	$[[35, 13, 7]]$	
$[[15, 11, 2]]$	$[[35, 25, 4]]$	$[[51, 3, 11]]$
	$[[35, 31, 2]]$	$[[51, 19, 9]]$
$[[17, 1, 7]]$		$[[51, 27, 6]]$
$[[17, 9, 4]]$	$[[37, 1, 11]]$	$[[51, 35, 3]]$
$[[21, 3, 5]]$	$[[39, 3, 9]]$	$[[51, 43, 2]]$
$[[21, 9, 3]]$	$[[39, 15, 3]]$	
$[[21, 15, 2]]$	$[[39, 27, 2]]$	$[[53, 1, 15]]$
$[[23, 1, 7]]$	$[[41, 1, 11]]$	$[[55, 31, 5]]$
	$[[41, 21, 6]]$	$[[55, 35, 3]]$
$[[25, 1, 9]]^a$		$[[55, 51, 2]]$
$[[25, 5, 3]]$	$[[45, 17, 5]]$	
$[[25, 21, 2]]$	$[[45, 29, 3]]$	$[[61, 1, 17]]$

[a] The code bound yields only $d \geq 4$.
[b] The code bound yields only $d \geq 8$.
[c] The code bound yields only $d \geq 4$.

Table 2: Parameters of some quaternary $\mathcal{Q}$BCH codes given in the form $[[n, k, d]]$.

$[[21, 15, 2\|2]]$	$[[69, 3, 7\|7]]$	$[[117, 93, 3\|3]]$
$[[21, 9, 3\|3]]$	$[[93, 3, 7\|7]]$	$[[117, 69, 3\|3]]$
$[[45, 21, 3\|3]]$	$[[93, 33, 5\|5]]$	
$[[63, 27, 6\|5]]$	$[[93, 63, 3\|3]]$	
$[[63, 21, 5\|5]]$	$[[105, 27, 6\|5]]$	
$[[63, 33, 4\|4]]$	$[[105, 51, 5\|4]]$	
$[[63, 45, 3\|3]]$	$[[105, 75, 3\|3]]$	$[[135, 87, 5\|5]]$
$[[63, 57, 2\|2]]$	$[[105, 99, 2\|2]]$	$[[135, 111, 3\|3]]$

Table 3: Parameters of some binary quantum codes derived from BCH codes over F_8 given in the form $[[n, k, d_2|d_8]]$. Binary expansion with respect to the self-dual basis $B_8 = (u^3, u^6, u^5)$ where $u^3 = u + 1$.

$[[20, 12, 2\|2]]$	$[[60, 28, 6\|5]]$	$[[84, 76, 2\|2]]$
$[[28, 4, 3\|3]]$	$[[60, 36, 4\|4]]$	$[[92, 4, 7\|7]]$
	$[[60, 44, 3\|3]]$	
$[[36, 4, 4\|3]]$	$[[60, 52, 2\|2]]$	$[[100, 12, 9\|6]]^a$
$[[36, 28, 2\|2]]$		$[[100, 52, 4\|3]]$
	$[[76, 4, 7\|7]]$	$[[100, 92, 2\|2]]$
$[[44, 4, 6\|5]]$		
	$[[84, 4, 6\|6]]$	$[[108, 28, 4\|4]]^b$
$[[52, 4, 7\|6]]$	$[[84, 28, 5\|5]]$	$[[108, 100, 2\|2]]$
$[[52, 28, 4\|4]]$	$[[84, 36, 4\|3]]$	$[[116, 4, 15\|11]]^c$
$[[60, 12, 8\|7]]$	$[[84, 52, 3\|3]]$	$[[116, 60, 7\|6]]$

[a] The code bound yields only $d_2 \geq 8$ and $d_{16} \geq 4$.
[b] The code bound yields $d_2 \geq 4$ and $d_{16} \geq 3$. In contrast to similar cases, $C_2^{\perp} \setminus C_2$ contains words of minimum weight, hence $d_2 = 4$.
[c] The set $C^{\perp} \setminus C$ contains words of minimum weight, hence the true minimum distance meets the code bound.

Table 4: Parameters of some binary quantum codes derived from BCH codes over F_{16} given in the form $[[n, k, d_2|d_{16}]]$. Binary expansion with respect to the self-dual basis $B_{16} = (v^3, v^7, v^{13}, v^{12})$ where $v^4 = v + 1$.

$[[35, 5, 3\|3]]$	$[[105, 45, 3\|3]]$	$[[175, 25, 6\|6]]$
$[[75, 35, 3\|3]]$	$[[105, 75, 2\|2]]$	$[[175, 55, 3\|3]]$
$[[105, 15, 5\|5]]$	$[[115, 5, 7\|7]]$	$[[175, 145, 2\|2]]$

Table 5: Parameters of some binary quantum codes derived from BCH codes over F_{32} given in the form $[[n, k, d_2|d_{32}]]$. Binary expansion with respect to the self-dual basis $B_{32} = (w^9, w^{18}, w^5, w^{10}, w^{20})$ where $w^5 = w^2 + 1$.

$[[42, 18, 3\|3]]$	$[[66, 6, 6\|5]]$	$[[126, 54, 8\|7]]$
$[[42, 30, 2\|2]]$	$[[90, 54, 3\|3]]$	$[[126, 78, 6\|5]]$
$[[54, 18, 6\|4]]$	$[[90, 78, 2\|2]]$	$[[126, 90, 4\|4]]$
$[[54, 30, 4\|3]]$	$[[114, 42, 8\|6]]$	$[[126, 102, 3\|3]]$
$[[54, 42, 2\|2]]$	$[[114, 78, 6\|4]]$	$[[126, 114, 2\|2]]$

Table 6: Parameters of some binary quantum codes derived from BCH codes over F_{64} given in the form $[[n, k, d_2|d_{64}]]$. Binary expansion with respect to the self-dual basis $B_{64} = (z^{12}, z^{24}, z^{48}, z^{33}, z^3, z^6)$ where $z^6 = z^4 + z^3 + z + 1$.

7 References

[1] Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A., and Weinfurter, H. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, Nov. 1995. See also LANL preprint quant-ph/9503016.

[2] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wootters, W. K. Mixed State Entanglement and Quantum Error Correction. *Physical Review A*, 54(5):3824–3851, Nov. 1996.

[3] Beth, T. and Grassl, M. The Quantum Hamming and Hexacodes. *Fortschritte der Physik*, 46(4–5):459–491, 1998.

[4] Bosma, W., Cannon, J., and Playoust, C. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3–4):235–266, 1997.

[5] Calderbank, A. R., Rains, E. M., Shor, P. W., and Sloane, N. J. A. Quantum Error Correction Via Codes over GF(4). *IEEE Transactions on Information Theory*, IT–44(4):1369–1387, July 1998. See also LANL preprint quant-ph/9608006.

[6] Calderbank, A. R. and Shor, P. W. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, Aug. 1996. See also LANL preprint quant-ph/9512032.

[7] Dirac, P. M. A. *The Principles of Quantum Mechanics*. Clarendon Press, Oxford, 4th edition, 1958.

[8] Gottesman, D. A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound. *Physical Review A*, 54(3):1862–1868, Sept. 1996. See also LANL preprint quant-ph/9604038.

[9] Grassl, M. and Beth, T. Codierung und Decodierung zyklischer Quantencodes. In Michaelis, B. and Holub, H., editors, *Fachtagung Informations- und Mikrosystemtechnik*, pp. 137–144, Magdeburg, Mar. 1998.

[10] Grassl, M. and Beth, T. Relations between Classical and Quantum Error-Correcting Codes. In Kluge, W., editor, *Workshop "Physik und Informatik"*, pp. 45–58, DPG-Frühjahrstagung, Heidelberg, 1999.

[11] Grassl, M., Beth, T., and Pellizzari, T. Codes for the Quantum Erasure Channel. *Physical Review A*, 56(1):33–38, July 1997. See also LANL preprint quant-ph/9610042.

[12] Grassl, M., Geiselmann, W., and Beth, T. Quantum Reed-Solomon Codes. In *Proceedings AAECC-13*, 1999. To appear.

[13] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 212–219, New York, 1996. ACM. See also LANL preprint quant-ph/9605043.

[14] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[15] Rötteler, M. and Beth, T. Efficient Realisation of Discrete Cosine Transforms on a Quantum Computer. In *Proceedings ISTET 99*, Magdeburg, 1999.

[16] Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[17] Steane, A. Error Correcting Codes in Quantum Theory. *Physical Review Letters*, 77(5):793–797, July 1996.

[18] Steane, A. Multiple Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society London Series A*, 452:2551–2577, 1996. See also LANL preprint quant-ph/9601029.

[19] Wootters, W. K. and Zurek, W. H. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct. 1982.