Quantum Reed–Solomon Codes

Markus Grassl, Willi Geiselmann, and Thomas Beth
Institut für Algorithmen und Kognitive Systeme
Universität Karlsruhe
76 128 Karlsruhe, Germany
Email: {grassl, geiselma, EISS_Office}@ira.uka.de

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.**

I. 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 [8]) and finding pre–images of an n–ary Boolean function ("searching") in time $O(\sqrt{2^n})$ (see [5]). Quantum computers are not only of theoretical nature—there are several suggestions how to physically realize them (see, e. g., [2, 3]).

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 [6]). Nevertheless, the problem of how to encode and decode quantum error–correcting codes has hardly been addressed, yet.

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 the full paper, together with the quantum implementation of any linear transformation over finite fields. We start with a brief introduction to quantum computation and quantum error–correcting codes, followed by some results about binary codes obtained from codes over extension fields.

II. Qubits and Quantum Registers

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

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

Here $|0\rangle$ and $|1\rangle$ are orthonormal basis states written in Dirac notation. The normalization condition in Eq. (1) 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

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

III. Quantum Error–Correcting Codes

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 π, and their combination. The bit–flip error corresponds to the Pauli matrix σ_x, the phase–flip error to σ_z, and their combination to σ_y. It is sufficient to consider only this discrete set of errors in order to cope with any possible local error (see [6]).

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.

The construction of quantum Reed–Solomon codes is based on the construction of quantum error–correcting codes from weakly self–dual binary codes (see, e. g., [9]). That construction is summarized by the following definition and theorem.

Definition 1 *Let $C = [N, K]$ be a weakly self–dual linear binary code, i. e., $C \le C^\perp$, and 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*

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

Theorem 2 *Let d be the minimum distance of the dual code $C^\perp$ in Definition 1. 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.*

IV. Main Results

The following definition and theorem show how to obtain weakly self–dual binary codes from codes over extension fields.

Definition 3 *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 $C_2 = [kN, kK, d \ge D]$ given by*

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

Theorem 4 *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:*

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

Using these results, we are ready to define quantum Reed–Solomon codes, based on classical weakly self–dual RS codes.

Definition 5 *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 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 1.*

The parameters of the quantum Reed–Solomon code are given by the following theorem.

Theorem 6 *The quantum RS code $\mathcal{C}$ of Definition 5 encodes $k(N-2K)$ qubits using kN qubits. It is able to detect at least up to K errors, i. e., $\mathcal{C} = [[kN, k(N-2K), d \geq K+1]]$.*

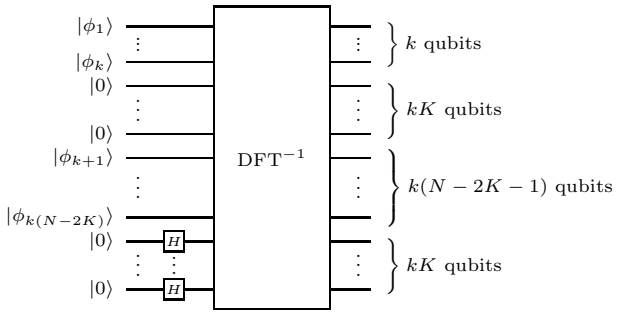

Fig. 1: Encoder for a quantum Reed–Solomon code.

In Figure 1 a quantum circuit for encoding quantum RS codes is presented. The $k(N-2K)$ qubit input state $|\phi\rangle$ is transformed into a superposition of different cosets of the RS code. These cosets are determined in the frequency domain, followed by the quantum version of an inverse Fourier transform DFT^{-1} over $\mathbb{F}_{2^k}$. The DFT is also used for decoding. The syndromes for bit–flip and phase–flip errors are computed in the frequency domain (see Figure 2).

V. 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 [1]). 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 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 $n|2^k - 1$.

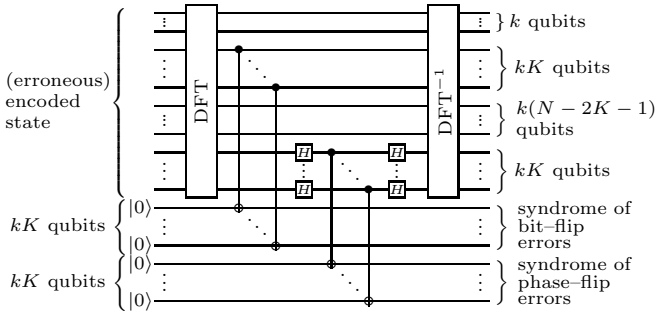

Fig. 2: Quantum circuit for computing the syndrome for a quantum Reed–Solomon code.

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 [4]).

The quantum implementation of linear mappings over finite fields presented in the full paper 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., [7]).

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.

Acknowledgements

The authors would like to thank Martin Rötteler and Rainer Steinwandt for numerous stimulating discussions during the process of writing this paper.

References

[1] 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.

[2] J. I. Cirac and P. Zoller, *Quantum Computation with Cold Trapped Ions*, Physical Review Letters, 74 (1995), pp. 4091–4094.

[3] D. G. Cory, A. F. Fahmy, and T. F. Havel, *Ensemble Quantum Computing by Nuclear Resonance Spectroscopy*, Tech. Rep. TR–10–96, B. C. M. P., Harvard Medical Medical School, Boston, Dec. 1996.

[4] M. Grassl and Th. Beth, *Codierung und Decodierung zyklischer Quantencodes*, in Fachtagung Informations– und Mikrosystemtechnik, B. Michaelis and H. Holub, eds., Magdeburg, 25–27 Mar. 1998.

[5] L. K. Grover, *A fast quantum mechanical algorithm for database search*, in Proc. 28th Annual ACM Symposium on Theory of Computing (STOC), New York, 1996, ACM, pp. 212–219.

[6] E. Knill and R. Laflamme, *Theory of quantum error–correcting codes*, Physical Review A, 55 (1997), pp. 900–911.

[7] M. Püschel, M. Rötteler, and Th. Beth, *Fast Quantum Fourier Transforms for a Class of Non–abelian Groups*, in Proceedings AAECC–13, 1999.

[8] P. W. Shor, *Polynomial–Time Algorithms for Prime Factorization and Discrete Logarithms*, in Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE Computer Society Press, Nov. 1994, pp. 124–134.

[9] A. Steane, *Multiple Particle Interference and Quantum Error Correction*, Proceedings of the Royal Society London Series A, 452 (1996), pp. 2551–2577.