# Constructions of Quantum Convolutional Codes

Markus Grassl
Institut für Algorithmen und Kognitive Systeme
Fakultät für Informatik, Universität Karlsruhe (TH)
Am Fasanengarten 5, 76 128 Karlsruhe, Germany
Email: grassl@ira.uka.de

Martin Rötteler
NEC Laboratories America, Inc.
4 Independence Way, Suite 200
Princeton, NJ 08540, USA
Email: mroetteler@nec-labs.com



***Abstract*— We address the problems of constructing quantum convolutional codes (QCCs) and of encoding them. The first construction is a CSS-type construction which allows us to find QCCs of rate 2/4. The second construction yields a quantum convolutional code by applying a product code construction to an arbitrary classical convolutional code and an arbitrary quantum block code. We show that the resulting codes have highly structured and efficient encoders. Furthermore, we show that the resulting quantum circuits have finite depth, independent of the lengths of the input stream, and show that this depth is polynomial in the degree and frame size of the code.**

## I. Introduction

Similar to the classical case a quantum convolutional code (QCC) encodes an incoming stream of quantum information into an outgoing stream. A basic theory of quantum convolutional codes obtained from infinite stabilizer matrices has been developed recently, see [13].

Only few constructions of quantum convolutional codes are known, see [2], [3], [4], [5], [6], [8], [13]. In this paper, we construct some new quantum convolutional codes using a CSS-type construction which uses the same principle as the CSS construction for block codes [12]. Furthermore, we revisit the product code construction introduced in [8] and show that for these codes the algorithm presented in [9] for computing a non-catastrophic encoder takes a particularly simple form. This allows us to show that the depth of the encoding circuit is polynomial in the frame size and the constraint length of the code.

## II. Quantum convolutional codes

### A. Basic definitions

QCCs are defined as infinite versions of quantum stabilizer codes. The appropriate generalization of stabilizer block codes to QCCs is provided by the polynomial formalism introduced in [13]. We briefly sketch this approach.[1]

The code is specified by its stabilizer which is a subgroup of the infinite version $\mathcal{G}_\infty$ of the Pauli group, which consists of tensor products of generalized Pauli matrices acting on an semi-infinite stream of qudits. The stabilizer can be described by a matrix with polynomial entries

$$S(D) = (X(D)|Z(D)) \in \mathbb{F}_q[D]^{(n-k)\times 2n}. \qquad (1)$$

[1]We describe the approach for $q$ dimensional subsystems (qudits) which is a straightforward generalization of the binary case.

*Definition 1:* Let $\mathcal{C}$ be a QCC defined by a full-rank stabilizer matrix as in eq. (1). Then $n$ is called the frame size, $k$ the number of logical qudits per frame, and $k/n$ the rate of the QCC. The constraint lengths are defined as $\nu_i = \max_{1\le j\le n}(\max(\deg X_{ij}(D), \deg Z_{ij}(D)))$, the overall constraint length is the defined as the sum $\nu = \sum_{i=1}^{n-k}\nu_i$, and the memory $m$ is given by $m = \max_{1\le i\le n-k}\nu_i$.

Like in the classical case, a QCC can also be described in terms of a semi-infinite stabilizer matrix $S$ which has entries in $\mathbb{F}_q\times\mathbb{F}_q$. First, we write $S(D) = \sum_{i=0}^m G_i D^i$ using $m+1$ matrices $G_0, G_1, \ldots, G_m$ which are of size $(n-k)\times n$ each. Then we define the semi-infinite matrix

$$S := \begin{pmatrix} G_0 & G_1 & \ldots & G_m & 0 & \ldots & \\ 0 & G_0 & G_1 & \ldots & G_m & 0 & \ldots \\ \vdots & & \ddots & \ddots & & \ddots & \ddots \end{pmatrix}. \qquad (2)$$

Note that $S$ has a block band structure where each block is of size $(n-k)\times(m+1)n$. A useful property of $S$ is that every qudit in the semi-infinite stream of qudits is acted upon non-trivially by only a finite number of generators. Moreover, those generators have bounded support. Hence their eigenvalues can be measured as soon as the corresponding qudits have been received. Therefore, it is possible to compute the error syndrome for the quantum convolutional code online.

There is a condition to check whether $S$ is well-defined, *i.e.*, if it defines a commutative subgroup of $\mathcal{G}_\infty$ [13]. If $S(D) = (X(D)|Z(D))$ as in eq. (1), then the condition of symplectic orthogonality of $S$ translates to

$$X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0. \qquad (3)$$

*Example 2:* As an example we consider the QCC defined by the stabilizer matrix (see [5])

$$S(D) = \left(\begin{array}{ccc|ccc} 1+D & 1 & 1+D & 0 & D & D \\ 0 & D & D & 1+D & 1+D & 1 \end{array}\right).$$

This code is derived from the classical $\mathbb{F}_4$-linear code generated by $(1+D, 1+\omega D, 1+\omega^2 D)$. We can easily check self-orthogonality by computing $X(D)Z(1/D)^t - Z(D)X(1/D)^t$ which turns out to be the $2\times 2$ all zero matrix. Hence the code indeed is self-orthogonal to all shifted versions of itself, *i.e.*, it defines a QCC where $n = 3$, $k = 1$, and $m = 1$. To illustrate the structure in terms of Pauli matrices

TABLE I

ACTION OF VARIOUS GENERALIZED CLIFFORD OPERATIONS. CONJUGATION BY THE UNITARY $U$ CORRESPONDS TO THE ACTION OF $\overline{U}$ ON THE COLUMNS OF $S(D) = (X(D)|Z(D))$.

| unitary gate $U$ | matrix $\overline{U}$ |
|---|---|
| Fourier transform DFT | $\overline{\mathrm{DFT}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathbb{F}_q^{2\times 2}$ |
| multiplication gate $M_\gamma$ | $\overline{M_\gamma} = \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix} \in \mathbb{F}_q^{2\times 2}$ |
| diagonal gate $P_\gamma$ | $\overline{P_\gamma} = \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2}$ |
| $\mathrm{ADD}^{(i,j+\ell n)}, i \not\equiv j \pmod n$ | $\overline{\mathrm{ADD}} = \left(\begin{array}{cc\|cc} 1 & D^\ell & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & -D^{-\ell} & 1 \end{array}\right)$ |
| $P_\ell := \mathrm{CPHASE}^{(i,i+\ell n)}, \ell \neq 0$ | $\overline{P_\ell} = \begin{pmatrix} 1 & D^\ell - D^{-\ell} \\ 0 & 1 \end{pmatrix}$ |

we consider the corresponding semi-infinite stabilizer matrix, which is given (in Pauli form) as follows:

$$S = \begin{pmatrix} X & X & X & X & Z & Y & & & & & & & & \\ Z & Z & Z & Z & Y & X & & & & & & & & \\ & & & X & X & X & X & Z & Y & & & & & \\ & & & Z & Z & Z & Z & Y & X & & & & & \\ & & & & & & X & X & X & X & Z & Y & & \\ & & & & & & Z & Z & Z & Z & Y & X & & \\ & & & & & & & & & & & & \ddots \end{pmatrix}$$

It is easy to see that the QCC corresponding to $S$ can correct an arbitrary number of errors, as long as they do not occur in *bursts*, meaning in this example that at least six unaffected qubits are between two erroneous ones.

### B. Encoding circuits

In [7] it has been shown that for any block quantum error-correcting code $\mathcal{C} = [\![n, k, d]\!]_q$ there is quantum circuit of polynomial size for encoding. In order to encode $k$ qudits into $n$ qudits, the circuit acts on the $k$ input qudits and $n-k$ ancillae which are initialized in the state $|0\rangle$. The input state can be described by a $Z$-only stabilizer matrix $S_0 = (X|Z) = (0|I0)$, where $I$ is an $(n-k)\times(n-k)$ identity matrix. The operation of the encoding circuit corresponds to a transformation changing $S_0$ into the stabilizer $S$ of the quantum code. This idea can be adapted to quantum convolutional codes (see [9] for qubit codes). The encoding circuit can be realized by generalized Clifford gates whose action is summarized in Table I, for the gates and the corresponding actions, see [7, Theorem 2].

## III. EFFICIENT ENCODERS FOR CSS TYPE QCCS

The CSS-like construction of QCCs uses two classical convolutional codes $C_1 = (n, k_1)$ and $C_2 = (n, n - k_2)$ with equal frame length $n$ and $C_2^\perp \subseteq C_1$. The stabilizer matrix $(X(D)|Z(D))$ is of block diagonal form, given by

$$\left(\begin{array}{c|c} H_2(D) & 0 \\ 0 & H_1(D) \end{array}\right) \in \mathbb{F}_q[D]^{(n-k_1+k_2)\times 2n}, \qquad (4)$$

where $H_1(D), H_2(D)$ denote parity check matrices of $C_1$ and $C_2$, respectively. We assume that both $H_1(D)$ and $H_2(D)$ correspond to non-catastrophic, delay-free encoders and have full ranks $n - k_1$ and $k_2$, respectively. This implies that their Smith normal form is $(I\ 0)$ with a suitable unit matrix $I$ (see [10, Chapter 2]). In particular there are unimodular matrices $A_1(D) \in \mathbb{F}_q[D]^{k_2\times k_2}$ and $B_1(D) \in \mathbb{F}_q^{n\times n}$ such that

$$A_1(D)H_2(D)B_1(D) = (I\ 0). \qquad (5)$$

There is an algorithm for computing the Smith normal form and the transformation matrices $A_1(D)$ and $B_1(D)$ whose bit-complexity is polynomial in the size and degree of the matrix $H_2(D)$ [11]. This implies that the corresponding quantum circuit implementing the matrix $B_1(D)$ can be realized using polynomially many generalized Clifford gates. The transformed stabilizer matrix is given by

$$(X'(D)|Z'(D)) = \left(\begin{array}{cc|c} I & 0 & 0 \\ 0 & 0 & Z_2(D) \end{array}\right). \qquad (6)$$

The action of the gates results in a modified $Z$-part as well. From condition (3) it follows that $Z_2(D)$ is of the form $Z_2(D) = (0\ Z_2'(D))$ with $Z_2'(D) \in \mathbb{F}_q[D]^{(n-k_1)\times(n-k_2)}$. Using Fourier transformation (DFT) gates on the last $n - k_2$ qudits, the stabilizer matrix reads

$$(X'(D)|Z'(D)) = \left(\begin{array}{cc|c} I & 0 & 0 \\ 0 & Z_2'(D) & 0 \end{array}\right). \qquad (7)$$

Computing the Smith form of $Z_2'(D)$ yields matrices $A_2(D)$ and $B_2(D)$ with $A_2(D)Z_2'(D)B_2(D) = (I\ 0)$. Another Fourier transform on the first $n - k_1 + k_2$ qudits yields an $Z$-only stabilizer matrix of the form $(0|I0)$. The resulting quantum code encodes $k_1 - k_2$ qudits per frame of size $n$. Overall, we obtain the following result.

*Theorem 3:* Let $\mathcal{C}$ be a quantum convolutional code constructed using the CSS-like construction from two classical convolutional codes $C_1$ and $C_2$ with stabilizer matrix as in eq. (4). Denote the frame size with $n$ and the constraint length with $\nu$. Then $\mathcal{C}$ has an encoding circuit whose depth is finite, *i. e.*, does not depend on the length of the input stream. Furthermore, the depth of this circuit is upper bounded by $poly(n, \nu)$.

## IV. CSS-TYPE QCCS OF RATE 2/4

In [6], optimal quantum convolutional codes of rate $1/3$ are listed which are based on self-orthogonal binary convolutional codes of rate $1/3$. In order to construct quantum convolutional codes of rate $2/4$, we search for self-orthogonal binary convolutional codes $C$ of rate $1/4$ which have a dual code $C^\perp$ with

| $\nu$ | $g_1(D)$ | $g_2(D)$ | $g_3(D)$ | $g_4(D)$ | $d^\perp$ | $N_{d^\perp}$ |
|---|---|---|---|---|---|---|
| 3 | 1100 | 1110 | 1001 | 1101 | 3 | 2 |
| 4 | 11001 | 11101 | 10011 | 10111 | 4 | 1 |
| 4 | 10001 | 10101 | 11011 | 11111 | 4 | 1 |
| 5 | 110010 | 111010 | 100001 | 110111 | 5 | 14 |
| 6 | 1010010 | 1111010 | 1000101 | 1100111 | 6 | 63 |
| 7 | 10101001 | 11111001 | 10000011 | 11000111 | 6 | 8 |
| 8 | 101100001 | 100100101 | 111110011 | 111011011 | 6 | 2 |
| 9 | 1001001001 | 1100111101 | 1110110111 | 1010101111 | 7 | 10 |
| 10 | 11011011001 | 10100001101 | 10011000011 | 11001001111 | 8 | 67 |
| 11 | 101101100011 | 101010110011 | 111101001011 | 110001101111 | 8 | 25 |

Fig. 1. Generators for self-orthogonal binary convolutional codes of rate $1/4$ yielding quantum convolutional codes of rate $2/4$ found by random search.

high minimum distance $d^\perp$. Applying the CSS construction with $C_1 = C_2 = C^\perp$, we then obtain a quantum convolutional code of rate $2/4$ and minimum distance $d^\perp$.

The results of a randomized search for such codes is presented in Table 1. The entries of the generator matrix $g(D) = (g_1(D), g_2(D), g_3(D), g_4(D))$ of the code $C$ are given in abbreviated form, listing the coefficients in increasing order. For example, the generator matrix of the first code with constraint length $\nu = 3$ is $g(D) = (1 + D, 1 + D + D^2, 1 + D^3, 1 + D + D^3)$. The last column lists the number $N_{d^\perp}$ of sequences of minimum weight. Note that it is desirable to have as few sequences of minimum weight as possible. The size of the search space grows with $O(2^{4\nu})$, so we have only performed an exhaustive search up to constraint length $\nu = 6$, and a randomized search for larger values of $\nu$.

## V. Efficient encoders for product codes

### A. Product code construction

The following theorem, taken from [8], allows to construct a quantum convolutional code using a classical convolutional code and a quantum code.

*Theorem 4:* Let $C_1 = (n_1, k_1)_p$ be a classical convolutional code over $\mathbb{F}_p$ with dual distance $d_1^\perp$ and let $G_1(D)$ be a generator matrix of $C_1$ corresponding to a non-catastrophic, delay-free encoder. Furthermore, let $\mathcal{C}$ be a quantum error-correcting code for $q$-dimensional quantum systems ($q = p^\ell$) with minimum distance $d_2$ and stabilizer matrix $S_2 = (X|Z)$ if $\mathcal{C}$ is a block code or $S_2 = (X(D)|Z(D))$ if $\mathcal{C}$ is a convolutional code. Then the stabilizer matrix

$$G(D) = G_1(D) \otimes_p S_2 \tag{8}$$

defines a quantum convolutional code with minimum distance $d \le \min(d_1^\perp, d_2)$.

The tensor product $\otimes_p$ corresponds to the Kronecker product of the stabilizer matrices. We use the index $p$ to stress that the coefficients of the polynomials in the matrix $G_1(D)$ are in the prime field $\mathbb{F}_p$ while the stabilizer matrix $S_2$ might be defined over an extension field $\mathbb{F}_q = \mathbb{F}_{p^\ell}$.

### B. Encoding product codes

Instead of applying the general algorithm of [9] to the matrix $G(D)$ in order to compute an encoding circuit for the product code, we will exploit the additional structure of the stabilizer matrix. The first step is to compute an inverse encoding circuit for the quantum code $\mathcal{C}$ with stabilizer $S_2$. The quantum circuit corresponds to a symplectic transformation yielding the trivial $Z$-only stabilizer $S_0 = (0|I\ 0)$. Note that the trivial stabilizer is of this form, regardless whether the code $\mathcal{C}$ is a block or a convolutional quantum code. Omitting the final Fourier transformation gates in the quantum circuit, we obtain an $X$-only stabilizer $S_0' = (I\ 0|0)$.

Expanding the matrix $G_1(D)$ as semi-infinite matrix, we get the following semi-infinite version of the stabilizer matrix $G(D)$ of eq. (8):

$$\begin{pmatrix}
g_{11}S_2 & g_{12}S_2 & \dots & g_{1,n_1}S_2 & & & & & \\
g_{21}S_2 & g_{22}S_2 & \dots & g_{2,n_1}S_2 & & & & & \\
\vdots & \vdots & \ddots & \vdots & & & & & \\
g_{k_1,1}S_2 & g_{k_1,2}S_2 & \dots & g_{k_1,n_1}S_2 & & & & & \\
& & & g_{11}S_2 & g_{12}S_2 & \dots & g_{1,n_1}S_2 & & \\
& & & g_{21}S_2 & g_{22}S_2 & \dots & g_{2,n_1}S_2 & & \\
& & & \vdots & \vdots & \ddots & \vdots & & \\
& & & g_{k_1,1}S_2 & g_{k_1,2}S_2 & \dots & g_{k_1,n_1}S_2 & & \\
& & & & & & \vdots & \ddots &
\end{pmatrix}$$

This matrix indicates that we have to apply the inverse encoding circuit of the code $\mathcal{C}$ to every block of qudits corresponding to the submatrices $g_{ij}S_2$. This first step corresponds to the leftmost boxes marked BC in the example of Fig. 4. The stabilizer matrix is now of the form

$$G'(D) = G_1(D) \otimes_p (I\ 0|0) = (G_1(D) \otimes I|0). \tag{9}$$

This $X$-only generator matrix corresponds to a CSS code (see eq. (4)) where

$$H_2(D) = \begin{pmatrix} G_1(D) & & \\ & \ddots & \\ & & G_1(D) \end{pmatrix}.$$

Using the algorithm of Sect. III, we obtain an inverse encoding circuit for the convolutional CSS code corresponding to

$G_1(D)$. This circuit has to be repeated $r$ times if the identity matrix in eq. (9) has rank $r$. The $j$-th copy of this quantum circuits acts on qudits $j, j+r, j+2r, \ldots$ (see the blocks marked $\mathrm{CC}_j$ in the example of Fig. 4). Overall, we obtain the following result.

*Theorem 5:* Let $\mathcal{C}$ be a quantum convolutional code which has been constructed using the product code construction described in Theorem 4. Denote the frame size with $n$ and the constraint length with $\nu$. Then $\mathcal{C}$ has an encoding circuit whose depth is finite, *i. e.*, does not depend on the length of the input stream. Furthermore, the depth of this circuit is upper bounded by $poly(n, \nu)$.

### C. QCCs from products of cyclic codes

In [8, Theorem 8], we have shown that product codes based on Reed-Solomon codes achieve the upper bound on the minimum distance of the resulting quantum code. Here we consider the following variant:

*Theorem 6:* Let $C$ be a cyclic code over $\mathbb{F}_q$ of composite length $n = n_1 n_2$ with $n_2 | (q-1)$. Furthermore, we assume that $C$ can be decomposed as $C = C_1 \otimes C_2$ where $C_2$ has generator polynomial $g_2(X) = \prod_{i=1}^{d-1}(X - \alpha^i)$ where $d - 1 \leq n_2/2$ and $\alpha$ is an $n_2$-th root of unity in $\mathbb{F}_q$. Then the code $C$ is self-orthogonal and has dual distance $d^\perp \geq \min(\delta_1, d)$ where $\delta_1$ is the BCH bound of $C_1^\perp$.

*Proof:* The code $C_2$ is generated by

$$G_2 = \begin{pmatrix} \alpha^0 & \alpha & \alpha^2 & \ldots & \alpha^{n_2-1} \\ \alpha^0 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n_2-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & \alpha^{d-1} & \alpha^{2(d-1)} & \ldots & \alpha^{(d-1)(n_2-1)} \end{pmatrix}.$$

The inner product of row $i$ and row $j$ of $G_2$ is

$$\sum_{\ell=0}^{n_2-1} \alpha^{(i+j)\ell} = 0$$

as $i + j \not\equiv 0 \bmod n_2$. Hence $C_2$ is self-orthogonal and so is $C$. The bound on the minimum distance follows from the two-dimensional BCH bound [1, p. 320]. ∎

Starting with a generator matrix $G = G_1 \otimes G_2$ of a (permuted) cyclic code as in Theorem 6, we can construct convolutional quantum codes of CSS type. The semi-infinite generator matrix of the corresponding self-orthogonal convolutional code is formed by the copies of the generator matrix $G$ which overlap in $\mu n_2$ positions. For $\mu = 2$ we get

$$\begin{pmatrix} g_{11}G_2 & g_{12}G_2 & \ldots & g_{1,n_1}G_2 & & & \\ g_{21}G_2 & g_{22}G_2 & \ldots & g_{2,n_1}G_2 & & & \\ \vdots & \vdots & \ddots & \vdots & & & \\ g_{k_1,1}G_2 & g_{k_1,2}G_2 & \ldots & g_{k_1,n_1}G_2 & & & \\ & & g_{11}G_2 & g_{12}G_2 & \ldots\, g_{1,n_1}G_2 & & \\ & & g_{21}G_2 & g_{22}G_2 & \ldots\, g_{2,n_1}G_2 & & \\ & & \vdots & \vdots & \ddots \quad \vdots & & \\ & & g_{k_1,1}G_2 & g_{k_1,2}G_2 & \ldots\, g_{k_1,n_1}G_2 & & \\ & & & & \vdots & \ddots & \end{pmatrix}. \quad (10)$$

The inner product of any two rows of this matrix is zero, as already $G_2 \cdot G_2^t = 0$. The dual distance of the dual of the convolution code defined by eq. (10) is lower bounded by the dual distance of $C$, as any sequence in the dual of the convolutional code fulfills the parity checks given by the matrix $G$. Note that the encoder corresponding to the matrix (10) might be catastrophic. Then, in some cases, the minimal non-catastrophic encoder can have constraint length zero, *i. e.*, corresponds to a block code.

## VI. Example

We illustrate the product construction and the corresponding encoding circuit using the five qubit code $[\![5,1,3]\!]_2$ and a classical convolutional code of rate $R = 2/3$.

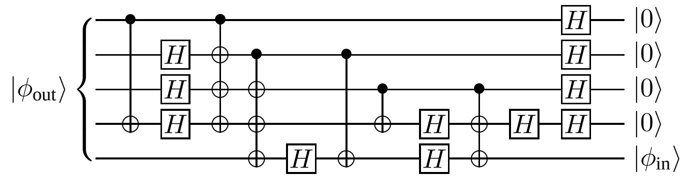


Fig. 2. Inverse Encoding Circuit for the five qubit code.

Using the inverse encoding circuit shown in Fig. 2, the stabilizer

$$S = \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right) \quad (11)$$

of the five qubit code is transformed into

$$S' = \left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right).$$

Note that the two Hadamard transforms on the fourth qubit cancel, but when omitting the final four Hadamard transformations, we obtain an $X$-only stabilizer.

In [10, Table 8.14] we find a nonsystematic rate $R = 2/3$ convolutional code with memory $\nu = 2$ and free distance $d_{\text{free}} = 3$. An encoding matrix for that code is

$$G(D) = \begin{pmatrix} D + D^2 & 1 & 1 + D^2 \\ 1 & D + D^2 & 1 + D + D^2 \end{pmatrix}.$$

A minimal polynomial generator matrix for the dual code is given by

$$H(D) = \begin{pmatrix} 1 + D + D^4 \\ 1 + D^2 + D^3 + D^4 \\ 1 + D^2 + D^4 \end{pmatrix}^t. \quad (12)$$

If we apply our algorithm to the stabilizer code with $X$-only stabilizer matrix $(X(D)|Z(D)) := (H(D)|0)$ we obtain the circuit shown in Fig. 3. The resulting transformed stabilizer is of the simple form $(XII)$

Using the product construction, we take the tensor product of the stabilizer matrix $S$ in eq. (11) and the generator matrix

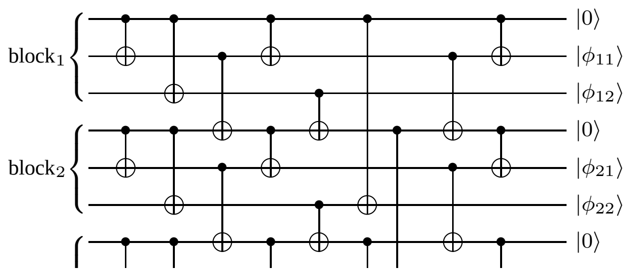


Fig. 3. Quantum circuit transforming the stabilizer $(X(D)|Z(D)) := (H(D)|0)$ into the simple form $(XII)$.

$H(D)$ of the binary convolutional code in eq. (12). The stabilizer matrix has the form

$$S_{\text{product}} = \big(H(D) \otimes S_X \bigm| H(D) \otimes S_Z\big), \tag{13}$$

where $S_X$ and $S_Z$ denote the corresponding parts of $S$.

Note that the circuit shown in Fig. 2 corresponds to a binary symplectic matrix $T = T_1T_2$, i.e., $ST = S'$, where $T_2$ corresponds to the last four Hadamard gates. Replicating the circuit without these Hadamard gates three times as indicated in Fig. 4, we get the matrix $I_3 \otimes T_1$, where $I_3$ denotes a $3 \times 3$ identity matrix. Now the $Z$-part of the stabilizer is zero, and the $X$-part has the form

$$\begin{pmatrix} 1+D+D^4 \\ 1+D^2+D^3+D^4 \\ 1+D^2+D^4 \end{pmatrix}^t \otimes \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

So replicating the circuit of Fig. 3 four times (but spread out to any every fifth qubit), we get an $X$-only stabilizer. The final four Hadamard gates in Fig. 4 transform it into a $Z$-only stabilizer.

The structure of the whole encoding circuit is illustrated in Fig. 4. Only the first block is shown, but every quantum gate in the circuit has to be applied repeatedly, shifted by the corresponding number of qubits. Each block encodes 11 qubits into 15. The inputs marked with $bc^{(i)}$ correspond to the input of the $i$-th copy of the block code $[\![5,1,3]\!]$, the inputs of the four copies of the convolutional code are marked with $cc^{(j)}$. The boxes marked with $\mathrm{BC}$ correspond to the encoder for the block code in Fig. 2, the blocks $\mathrm{CC}_j$ correspond to the encoding circuit for the convolutional code in Fig. 3.

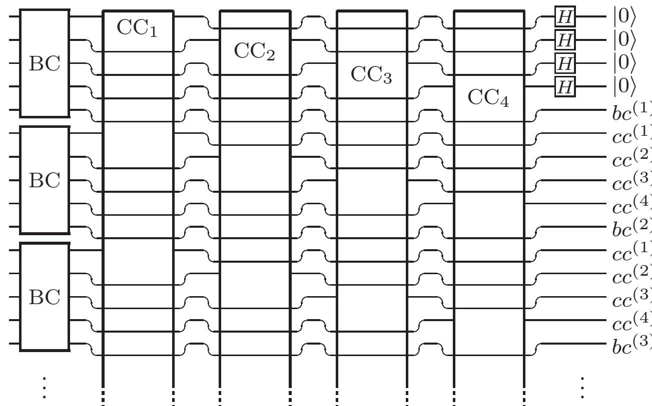


Fig. 4. Schematic inverse encoding circuit for the quantum convolutional code of rate $R = 11/15$ obtained by the product code from the quantum block code $[\![5,1,3]\!]_2$ and a classical convolutional code with rate $R = 2/3$.

## VII. Conclusions

The problem of constructing quantum convolutional codes and their encoders was addressed. Using a CSS-type construction, we derived new examples of QCCs of rate $2/4$. For constraint lengths up to $\nu = 6$ we performed an exhaustive search of the search space, and for constraint lengths up to 11 we employed a randomized search which found several good codes. Using a product code construction which takes as inputs a classical convolutional code on the one hand and a quantum block code on the other, it is possible to derive many examples of QCCs. We show that these codes all have the property that their encoder is of polynomial depth. We conjecture that any stabilizer QCC has a polynomial depth encoder. It seems that a more detailed study of the algorithm given in [9], which is based on iterative Smith normal form computation on the stabilizer matrix, would be required to resolve this question.

## References

[1] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge: Cambridge University Press, 2003.

[2] H. F. Chau, "Quantum convolutional error-correcting codes," *Phys. Rev. A*, vol. 58, no. 2, pp. 905–909, 1998.

[3] ——, "Good quantum-convolutional error-correction codes and their decoding algorithm exist," *Phys. Rev. A*, vol. 60, no. 3, pp. 1966–1974, 1999.

[4] A. C. A. de Almeida and R. Palazzo, Jr., "A concatenated $[(4,1,3)]$ quantum convolutional code," in *Proc. ITW'04, San Antonio, USA*, 2004, pp. 28–33.

[5] G. D. Forney, Jr. and S. Guha, "Simple rate-$1/3$ convolutional and tail-biting quantum error-correcting codes," in *Proc. ISIT'05, Adelaide, Australia*, 2005, pp. 1028–1032.

[6] G. D. Forney Jr., M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 865–880, 2007.

[7] M. Grassl, Th. Beth, and M. Rötteler, "Efficient quantum circuits for non-qubit quantum error-correcting codes," *International Journal of Foundations of Computer Science*, vol. 14, no. 5, pp. 757–775, 2003.

[8] M. Grassl and M. Rötteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *Proc. ISIT'05, Adelaide, Australia*, 2005, pp. 1018–1022.

[9] ——, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proc. ISIT'06, Seattle, USA*, 2006, pp. 1109–1113.

[10] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*, New York: IEEE Press, 1999.

[11] R. Kannan, "Solving systems of linear equations over polynomials," *Theoretical Computer Science*, vol. 39, pp. 69–88, 1985.

[12] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000.

[13] H. Ollivier and J.-P. Tillich, "Quantum convolutional codes: fundamentals," 2004, preprint quant-ph/0401134.