Quantum Block and Convolutional Codes from Self-orthogonal Product Codes

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

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

Abstract—We present a construction of self-orthogonal codes using product codes. From the resulting codes, one can construct both block quantum error-correcting codes and quantum convolutional codes. We show that from the examples of convolutional codes found, we can derive ordinary quantum error-correcting codes using tail-biting with parameters [42N, 24N, 3]2. While it is known that the product construction cannot improve the rate in the classical case, we show that this can happen for quantum codes: we show that a code [15, 7, 3]2 is obtained by the product of a code [5, 1, 3]2 with a suitable code.

I. INTRODUCTION
Quantum convolutional codes are motivated by their classical counterparts [3]. As in the classical case the idea is to allow for the protection of arbitrary long streams of information in such a way that as many errors as possible can be corrected. To achieve this the information is “smeared out” to the output stream by adding a certain amount of redundancy, but at the same time meeting the requirement to be local, i.e., encoding/decoding can be done by processes which needs only a constant amount of memory. In [13] the basic theory of quantum convolutional codes has been developed. There it has been shown that, similar to the classical codes, quantum convolutional codes can be decoded by a maximum likelihood error estimation algorithm which has linear complexity. However, the authors only gave an example of one (rate 1/5) quantum convolutional code. This research was motivated by the question to find new examples of quantum convolutional codes. The construction presented in this paper resorts on the idea of product codes. An extra requirement imposed by the applicability to quantum codes is that the dual distance has to be high. The main source of the examples presented at the end of the paper are two-dimensional cyclic codes (sometimes also called “bicyclic codes”). We apply this to the situation where the code is a product code of two Reed-Solomon codes.

II. SELF-ORTHOGONAL PRODUCT CODES
A. Quantum error-correcting codes from classical codes
Most of the constructions for quantum error-correcting codes (QECCs) for a quantum system of dimension q (qudits), where q = p^s is a prime power, are based on classical error-correcting codes over GF(q) or GF(q^2). The so-called CSS codes (see [5, 14]) are based on linear codes C_1 and C_2 over GF(q) with C_2^⊥ ⊆ C_1. Here C_2^⊥ is the dual code of C_2 with respect to the Euclidean inner product. In particular, if C = C_1 = C_2 this implies that C^⊥ is a weakly self-dual code.

Another class of quantum codes can be obtained from codes over GF(q^2) which are self-orthogonal with respect to the Hermitian inner product, denoted by C ⊆ C∗ [11]. Both cases can be generalized to a construction of QECCs based on additive codes over GF(q^2) which are self-orthogonal with respect to the symplectic (trace) inner product, i.e. C ⊆ C∗ [1].

B. Inner products on vector spaces over GF(q) and GF(q^2)
In this paper, we will use three different inner products on vector spaces over GF(q) and GF(q^2) which are defined as follows:

Euclidean:
\[ v \cdot w := \sum_{i=1}^{n} v_i w_i \quad \text{for } v, w \in GF(q)^n \]  \hspace{1cm} (1)

Hermitian:
\[ v \star w := \sum_{i=1}^{n} v_i w_i^q \quad \text{for } v, w \in GF(q^2)^n \]  \hspace{1cm} (2)

Symplectic:
\[ v \star w := \sum_{i=1}^{n} \text{tr}(v_i w_i^q) \quad \text{for } v, w \in GF(q^2)^n, \]  \hspace{1cm} (3)

where \( \text{tr}(x) \) denotes the trace of \( GF(q^2) \) over its prime field \( GF(p) \). Both the Euclidean and the Hermitian inner product are bilinear over \( GF(q) \) respectively \( GF(q^2) \), but the symplectic inner product is only \( GF(p)-\)bilinear because of the trace map. For codes which are linear over \( GF(q) \), linear over \( GF(p^2) \), or additive (i.e. \( GF(p) \)-linear), one can define a dual code with respect to the inner products (1), (2), or (3), respectively. The three cases are summarized in Table I.

Next, we consider inner products on tensor products of vector spaces.
as \(v\) and \(v'\) are vectors over the prime field, the left factor equals their Euclidean inner product \(v \cdot v'\) which takes values in \(GF(p)\) only. Using the \(GF(p)\)-linearity of the trace map, the proof is completed.

### C. Product codes

Next we present the fundamental properties of the product of two codes which combines two codes (see e.g. [2, 11]).

**Lemma 4:** Let \(C_1 = [n_1, k_1, d_1]_q\) and \(C_2 = [n_2, k_2, d_2]_q\) be linear codes over \(GF(q)\) with generator matrices \(G^{(1)}\) and \(G^{(2)}\), respectively. Then the product code \(C_\pi := C_1 \otimes C_2\) is a linear code \(C_\pi := [n_1n_2, k_1k_2, d_1d_2]_q\) generated by the matrix

\[
G := \begin{pmatrix}
  g_{11}^{(1)} G^{(2)} & g_{12}^{(1)} G^{(2)} & \ldots & g_{1n_2}^{(1)} G^{(2)} \\
  g_{21}^{(1)} G^{(2)} & g_{22}^{(1)} G^{(2)} & \ldots & g_{2n_2}^{(1)} G^{(2)} \\
  \vdots & \vdots & \ddots & \vdots \\
  g_{k_1,1}^{(1)} G^{(2)} & g_{k_1,2}^{(1)} G^{(2)} & \ldots & g_{k_1,n_2}^{(1)} G^{(2)}
\end{pmatrix}.
\]

If \(C_1 = [n_1, k_1, d_1]_p\) is a linear code over the prime field \(GF(p)\) and \(C_2 = (n_2, p^{k_2}, d_2)_q\) is an additive code over \(GF(q)\), then \(C_{\pi,p} := C_1 \otimes_p C_2\) is an additive code with parameters \(C_{\pi,p} = (n_1n_2, p^{k_1k_2}, d_1d_2)_q\).

The following theorem is valid for all compatible choices of inner products on the component spaces of a tensor product space and the tensor product space itself.

**Theorem 5:** Let \(C_\pi = C_1 \otimes C_2\) be the product code of the codes \(C_1 = [n_1, k_1, d_1]_q\) and \(C_2 = [n_2, k_2, d_2]_q\). By \(H_1\) and \(H_2\) we denote generator matrices of the corresponding dual codes. Furthermore, let \(A_1\) and \(A_2\) be matrices of size \(k_1 \times n_1\) and \(k_2 \times n_2\), respectively, such that the row span of the matrices \(H_1\) and \(A_1\) is the full vector space and similar for \(H_2\) and \(A_2\).

Then a generator matrix \(H\) of the dual code of \(C_\pi\) is given by

\[
H := \begin{pmatrix}
  H_1 \oplus H_2 \\
  A_1 \oplus H_2 \\
  H_1 \oplus A_2
\end{pmatrix}.
\]

**Proof:** Let \(V_1\) and \(V_2\) be the full vector spaces containing the codes \(C_1\) and \(C_2\). Furthermore, by \(D_1\) and \(D_2\) we denote the dual code of \(C_1\) and \(C_2\) with respect to the inner product on \(V_1\) and \(V_2\), respectively. Using the properties of the inner products on tensor product spaces (see Lemma 2 and Lemma 3), it is obvious that the dual code \(D_\pi\) of \(C_\pi\) contains both \(V_1 \oplus D_2\) and \(D_1 \oplus V_2\). The intersection of these spaces is \(D_0 := D_1 \oplus D_2\), spanned by \(H_1 \oplus H_2\). The complement of \(D_0\) in \(V_1 \oplus D_2\) is spanned by \(A_1 \oplus H_2\), and analogously for the complement of \(D_0\) in \(D_1 \oplus V_2\). Hence \(D_\pi\) can be decomposed as

\[
D_\pi = \left(D_1 \oplus D_2\right) \oplus \left((A_1) \oplus D_2\right) \oplus \left(D_1 \oplus (A_2)\right).
\]

Here \([A]\) denotes the row span of the matrix \(A\). Considering the dimension of the spaces, the result follows.

---

**TABLE I**

Notation used for the three different inner products and the corresponding dual codes.

| Inner Product | Dual Code | Linear Over |
|---------------|-----------|-------------|
| \(v \cdot w\) | \(C\) \(\otimes\) \(\pi\) | \(GF(q)\) |
| \(v \odot w\) | \(C^\ast\) \(\otimes\) \(\pi\) | \(GF(q^2)\) |
| \(v \star w\) | \(C^\ast\) \(\otimes\) \(\pi\) | \(GF(p)\) |
Corollary 6: The minimum distance of the dual of the product code $C_\pi = C_1 \otimes C_2$ cannot exceed the minimum of the dual distance of $C_1$ and the dual distance of $C_2$.

Proof: The dual code $D_\pi$ of $C_\pi$ contains $V_1 \otimes D_2$, i.e., the product of the trivial code $[n_1, n_1, 1]$ and $D_2$. Hence the minimum distance of $D_\pi$ cannot be larger than that of $D_2$. The result follows by interchanging the role of $C_1$ and $C_2$.

Note that despite their poor behavior in terms of minimum distance, the dual of product codes can be used for burst error correction (see [6], [15]). For the construction of QECCs, we will make use of the following property.

Theorem 7: Let $C_E \subseteq C_E^\perp$, $C_H \subseteq C_H^\perp$, and $C_S \subseteq C_S^\perp$ denote codes which are self-orthogonal with respect to the inner products (1), (2), or (3), respectively. Furthermore, let $C$ denote an arbitrary linear code over $GF(q)$, respectively $GF(q^2)$, and let $C_p$ be a linear code over $GF(p)$. Then

(i) $C \otimes C_E$ is Euclidean self-orthogonal.
(ii) $C \otimes C_H$ is Hermitian self-orthogonal.
(iii) $C \otimes C_S$ is symplectic self-orthogonal.

Proof: The result directly follows using Lemma 2 and Theorems 4 and 5

### III. PRODUCT CODES FROM CYCLIC CODES

In this section we investigate the product of two cyclic codes (see [2, Chapter 10.4], [3, Chapter 10.2]).

Let $C_1 = [n_1, k_1]$ and $C_2 = [n_2, k_2]$ be cyclic linear codes with generator polynomials $g_1(X)$ and $g_2(Y)$. Then $C_\pi = C_1 \otimes C_2$ is a bicyclic code generated by $g_1(X)g_2(Y)$. The codewords of $C_\pi$ correspond to all bivariate polynomials $c(X, Y) = i(X, Y)g_1(X)g_2(Y)$ modulo the ideal generated by $X^{n_1} - 1$ and $Y^{n_2} - 1$, where $i(X, Y) \in GF(q)[X, Y]$ is an arbitrary bivariate polynomial. The two-dimensional spectrum of $c(X, Y)$ is the $n_1 \times n_2$ matrix $(\hat{c}_{i,j})$ with entries

$$
\hat{c}_{i,j} := c(\alpha^i, \beta^j),
$$

where $\alpha$ and $\beta$ are primitive roots of unity of order $n_1$ and $n_2$, respectively. The spectrum $\hat{c}$ is zero in all vertical stripes corresponding to the roots $\alpha^i$ of $g_1(X)$ and in all horizontal stripes corresponding to the roots $\beta^j$ of $g_2(X)$ (see Fig. 1a). The generator polynomial $h_1(X)$ of the Euclidean dual $C_1^\perp$ is the reciprocal polynomial of $(X^{n_1} - 1)/g_1(X)$. Hence its one-dimensional spectrum is zero at the negative of those positions where the spectrum of the code $C_1$ takes arbitrary values (cf. Fig. 2). For the generator polynomial $h_2(Y)$ of $C_2^\perp$, the analogous statement is true. Therefore the Euclidean dual code $(C_1 \otimes C_2)^\perp$ of the product code $C_1 \otimes C_2$ consists of all polynomials that are multiples of $h_1(X)$ or $h_2(Y)$. Interchanging the zeros and blanks in the two-dimensional spectrum of the product code and applying the coordinate map (cf. Fig. 2) to both the rows and columns, we obtain the two-dimensional spectrum of the dual code $(C_1 \otimes C_2)^\perp$.

For the Hermitian dual code, we get analogous results. As the Hermitian inner product involves the Frobenius map $x \mapsto x^q$, the transformation on the coordinates now reads $i \mapsto -qi \mod n_1$.
has parameters

\[ K^\perp = q(d_1 + d_2 - 2) - d_1 d_2 + 1 \]
\[ d^\perp = \min(q - \delta_1, q - \delta_2). \]

Moreover, the product code is self-orthogonal if \( C_1 \) or \( C_2 \) is self-orthogonal.

Note that the result is still true when replacing the Reed-Solomon code over \( GF(q) \) of length \((q-1)\) by a cyclic code \( C = [n, k, d]_q \) with generator polynomial \( g(X) = \prod_{i=0}^{d-2}(X - \alpha^i) \) where \( n \) is a divisor of \( q - 1 \) and \( \alpha \) is a primitive \( n \)-th root of unity.

IV. QUANTUM CODES FROM PRODUCT CODES

A. Quantum Block Codes

In the previous section we have seen that the product of a self-orthogonal Reed-Solomon code with an arbitrary Reed-Solomon codes yields a self-orthogonal product code. Using Lemma 1 we can construct quantum error-correcting codes.

**Theorem 9:** Let \( C_1 = [q - 1, \mu_1, q - \mu_1]_q \) and \( C_2 = [q - 1, \mu_2, q - \mu_2]_q \) be Reed-Solomon codes where \( \mu_1 < (q-1)/2 \). Then a quantum error-correcting code

\[ C = [(q-1)^2, (q-1)^2 - 2\mu_1\mu_2, 1 + \min(\mu_1, \mu_2)]_q \]

exists.

**Proof:** For \( \mu_1 < (q-1)/2 \), the code \( C_1 \) is Euclidean self-orthogonal [10]. The dual distance of \( C_1 \) and \( C_2 \) is \( \mu_1 + 1 \) and \( \mu_2 + 1 \), respectively. By Theorem 8 the product code \( C_\pi = C_1 \otimes C_2 = [(q-1)^2, \mu_1\mu_2, (q - \mu_1)(q - \mu_2)]_q \) is self-orthogonal. Its Euclidean dual has parameters \( C_\pi^\perp = [(q-1)^2, (q-1)^2 - \mu_1\mu_2, 1 + \min(\mu_1, \mu_2)]_q \). Hence by Lemma 1 a QECC with the parameters given in eq. (10) exists.

Note that from \( C_1 \) and \( C_2 \) (provided \( \mu_1 < (q-1)/2 \)), one can construct optimal QECCs with parameters \([q - 1, q - 2\mu_1 - 1, \mu_1 + 1]_q \) (see [10]). The product of the rates of these codes is

\[ \left(1 - \frac{2\mu_1}{q-1}\right) \left(1 - \frac{2\mu_2}{q-1}\right) = 1 - \frac{2(\mu_1 + \mu_2)}{q-1} + \frac{4\mu_1\mu_2}{(q-1)^2} \]

The rate of the code of Theorem 9 is

\[ 1 - \frac{2\mu_1\mu_2}{(q-1)^2}. \]

If we choose \( \mu_1 = \mu_2 \), we will obtain a QECC of squared length and the same minimum distance, but higher rate provided \( \mu_1 = \mu_2 < 2(q-1)/3 \).

Note that we can obtain good QECCs by this construction using other codes than Reed-Solomon codes. Let \( C = [5, 2, 4]_4 \) be the Hermitian dual of the quaternary Hamming code. Using \( C \subseteq C^* = [5, 3, 3]_4 \), an optimal QECC \( C = [5, 1, 3]_2 \) can be constructed. The code \( C \) is not a Reed-Solomon code, but its spectrum fulfills the conditions for Theorem 8. Hence the product of \( C \) with itself is a Hermitian self-orthogonal code \( C \otimes C \subseteq \{C \otimes C\}^* = [25, 21, 3]_4 \). This yields a QECC \( C^{(2)} = [25, 17, 3]_2 \), whose rate is more than three times higher than that of \( C \).

The product code of \( C \), considered as additive code, with the binary simplex code \( C_1 = [3, 2, 2]_2 \) is an additive code \( C_2 := C_1 \otimes_p C = (15, 2^8, 8)_2 \) which is contained in its symplectic dual \( C^* = (15, 2^{22}, 3)_2 \). Hence we obtain a QECC \( C_\pi = [15, 7, 3]_2 \).

V. VARIATIONAL CONVOLUTIONAL CODES

Following [13], an \((n, k, m)\) quantum convolutional code can be described in terms of a semi-infinite stabilizer matrix \( S \). The matrix \( S \) has a block band structure where each block \( M \) has size \((n - k) \times (n + m)\). All blocks are equal. In the second block, the matrix \( M \) is shifted by \( n \) columns, hence any two consecutive blocks overlap in \( m \) positions. The general structure of the matrix is as follows:

\[
\begin{pmatrix}
S \\
M \\
M \\
\vdots
\end{pmatrix}
\]

The classical convolutional code generated by \( S \) must be self-orthogonal with respect to some of the inner products of Section 1. The quantum product codes constructed in the previous section naturally lend themselves to convolutional codes because of the following observation. Let \( M = G^{(1)} \otimes G^{(2)} \) be the generator matrix of \( C_1 \otimes C_2 \) as in eq. (6). Assume that \( m = tn_2 \) is a multiple of \( n_2 \), the length of \( C_2 \). Since \( C_2 \) is self-orthogonal, we have that the submatrix of \( M \) which consists of the last \( m \) columns of \( M \) is orthogonal to the submatrix which consists of the first \( m \) columns of \( M \). Hence, we obtain a semi-infinite stabilizer matrix \( S \) by iterative shifting of the block \( M \) by \( n_1n_2 - m = (n_1 - 1)n_2 \) positions.

To give an example, we let \( C = [7, 3, 4]_2 \) be the Euclidean dual of the binary Hamming code. Using \( C \subseteq C^\perp = [7, 4, 3]_2 \), a QECC \( C = [7, 1, 3]_2 \) can be constructed. The product code of \( C \) with itself is a code \( C_\pi = C \otimes C = [49, 9, 16]_2 \) which is contained in its dual \( C_\pi^\perp = [49, 40, 3]_2 \). Hence we obtain a QECC \( C_\pi = [49, 31, 3]_2 \). The possible parameters for quantum convolutional codes obtained from the product code \( C_\pi \) by the CSS construction (i.e., by considering the generator matrix \( C_\pi \otimes GF(4) \)) are \((49 - m, 31, m) \), \( m = 7 \). The free distance of these codes is \( 3 \). Using tail-biting with \( N \geq 2 \) blocks and \( m = 7 \) (see [8]) we obtain QECCs \([42N, 24N, d]_2 \). Using Magma [4] we compute \( d = 3 \).

From the product code \( C_\pi = [15, 7, 3]_2 \) described above we can obtain a quantum convolutional code with parameters \((10, 7, 5)\), i.e., we choose \( m = 5 \).

If the matrix \( M \) defining the semi-infinite band matrix \( S \) is the generator matrix \( G^{(1)} \otimes G^{(2)} \) of a product code, the matrix \( S \) itself can be decomposed as a tensor product \( S = G^{(1)} \otimes G^{(2)} \), provided the overlap \( m \) is a multiple of the length \( n_2 \) of the second code, i.e., \( m = tn_2 \) (see Fig. [3]). The matrix
codes is a challenging task and rises several questions: what compare the performance of such codes? While the first of

\[ \begin{pmatrix} g_{11}(1) G^{(2)} & g_{12}(1) G^{(2)} & \cdots & g_{1,n_1}(1) G^{(2)} \\ g_{21}(1) G^{(2)} & g_{22}(1) G^{(2)} & \cdots & g_{2,n_1}(1) G^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k_1,1}(1) G^{(2)} & g_{k_1,2}(1) G^{(2)} & \cdots & g_{k_1,n_1}(1) G^{(2)} \\ \end{pmatrix} \otimes \mu G^{(2)} \]

is a semi-infinite band matrix with \( M^{(1)} = G^{(1)} \) and overlap \( t \). From Theorem 7 it follows that the product code is self-orthogonal if \( C_2 \) is self-orthogonal. Hence we get the following construction:

**Theorem 10:** Let \( C_1 \) be a classical convolutional code. Furthermore, let \( C_2 \) be a self-orthogonal code. Then the product code \( C_1 \otimes C_2 \) defines a quantum convolutional code, provided at least one of the following holds:

(i) Both \( C_1 \) and \( C_2 \) are linear over \( GF(q) \) and \( C_2 \) is Euclidean self-orthogonal.

(ii) Both \( C_1 \) and \( C_2 \) are linear over \( GF(q^2) \) and \( C_2 \) is Hermitian self-orthogonal.

(iii) \( C_1 \) is linear of \( GF(p) \) and \( C_2 \) is a symplectic self-orthogonal code over \( GF(p^f) \).

**VI. CONCLUSION**

The construction of new examples of quantum convolutional codes is a challenging task and rises several questions: what is a general framework to describe such codes, how can they be constructed, and what are the figures of merit to compare the performance of such codes? While the first of these questions has been answered in a satisfying way at

least for convolutional stabilizer codes in [13], the other two questions are open (but see e.g. [7, 8, 12]). In this paper we have contributed to the second question by establishing a connection between product codes and convolutional codes. We have shown that the dual distance of product codes can be bounded from below which allows to obtain quantum codes for which the minimum distance is at least as large as the smaller of the minimum distances of the factors.

Concerning the third question currently not much is known, e.g., the significance of notions such as free distance which are useful for classical convolutional codes to the quantum case has yet to be investigated.

**ACKNOWLEDGMENT**

This work was carried out while the second author was visiting IAKS. M.R. also acknowledges support by the Institute of Quantum Computing, University of Waterloo. Funding by Deutsche Forschungsgemeinschaft (DFG), Schwerpunktprogramm Quanten-Informationsverarbeitung (SPP 1078), Projekt AQUA (Be 887/13) is acknowledged as well.

**REFERENCES**

[1] A. Ashikhmin and E. Knill, “Nonbinary quantum stabilizer codes,” IEEE Transactions on Information Theory, vol. 47, no. 7, pp. 3065–3072, Nov. 2001, preprint quant-ph/0005008.

[2] R. E. Blahut, Theory and Practice of Error Control Codes. Reading: Addison-Wesley, 1983.

[3] ———, Algebraic Codes for Data Transmission. Cambridge: Cambridge University Press, 2003.

[4] W. Bosma, J. J. Cannon, and C. Playoust, “The Magma Algebra System I: The User Language,” Journal of Symbolic Computation, vol. 24, no. 3–4, pp. 235–266, 1997.

[5] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” Physical Review A, vol. 54, no. 2, pp. 1098–1105, Aug. 1996, preprint quant-ph/9512032.

[6] R. T. Chien and S. W. Ng, “Dual Product Codes for Correction of Multiple Low-Density Burst Errors,” IEEE Transactions on Information Theory, vol. 19, no. 5, pp. 672–677, Sept. 1973.

[7] A. C. de Almeida and R. Palazzo, Jr., “A Concatenated [(1, 1, 3)] Quantum Convolutional Code,” in 2004 IEEE Information Theory Workshop, San Antonio, TX, Oct. 2004.

[8] 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.

[9] M. Grassl and Th. Beth, “Cyclic quantum error-correcting codes and quantum shift registers,” Proceedings of the Royal Society London A, vol. 456, no. 2003, pp. 2689–2706, Nov. 2000, preprint quant-ph/9910061.

[10] M. Grassl, Th. Beth, and M. Rötteler, “On Optimal Quantum Codes,” International Journal of Quantum Information, vol. 2, no. 1, pp. 55–64, 2004, preprint quant-ph/0312164.

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

[12] H. Ollivier and J-P. Tillich, “Description of a quantum convolutional code,” Physical Review Letters, vol. 91, 177902, Oct. 24 2003.

[13] ———, “Quantum convolutional codes: fundamentals,” Nov. 2004, preprint quant-ph/0401134.

[14] A. M. Steane, “Error Correcting Codes in Quantum Theory,” Physical Review Letters, vol. 77, no. 5, pp. 793–797, 29. July 1996.

[15] J. K. Wolf, “On Codes Derivable from the Tensor Product of Check Matrices,” IEEE Transactions on Information Theory, vol. 11, no. 2, pp. 281–284, Apr. 1965.