SCIENCE CHINA
Information Sciences

• LETTER •

April 2020, Vol. 63 149301:1–149301:3
https://doi.org/10.1007/s11432-019-9871-y

On the parity-check matrix of generalized concatenated code

Sha SHI[1†], Yang LIU[2†*], Junzhi YAN[3], Jingliang GAO[4] & Yunjiang WANG[4*]

[1]*Engineering Research Center of Molecular and Neuro Imaging Ministry of Education, School of Life Science and Technology, Xidian University, Xi'an* 710071*, China;*
[2]*National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing* 100029*, China;*
[3]*China Mobile Research Institute, Beijing* 100053*, China;*
[4]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China*

Received 21 February 2019/Revised 10 April 2019/Accepted 18 April 2019/Published online 12 September 2019

Citation Shi S, Liu Y, Yan J Z, et al. On the parity-check matrix of generalized concatenated code. Sci China Inf Sci, 2020, 63(4): 149301, https://doi.org/10.1007/s11432-019-9871-y

Dear editor,

Single-level concatenation using a nonbinary code as outer code and a binary code as inner code is widely used in communication and digital data storage systems to achieve high reliability with reduced decoding complexity [1]. Moreover, concatenation can be multilevel, where multiple outer codes are concatenated with multiple inner codes; it is referred as generalized concatenated codes (GCCs). Compared with the single-level concatenated codes, GCCs offer more flexibility for constructing good codes and designing error-control systems with different code rates for various communication environments [2].

For a linear code, generator and parity-check matrices are important to understand the structures and properties of the code, and both play key roles in the corresponding encoding and decoding procedures [3, 4]. The generator matrix of a GCC has been well studied [5]. In contrast, the parity-check matrix of a GCC has not been investigated to date. Fortunately, the space generated by the parity-check matrix of a GCC can be considered as the zero space or solution space of the generator matrix [1].

Unfortunately, it is difficult to obtain a parity-check matrix directly when the dimensionality of the generator matrix is huge. Although the parity-check matrix can be obtained by computing linear equations yielded from the generator matrix, the structure of the parity-check matrix of a GCC remains unknown.

We introduce a parity-check matrix formalism for a GCC using a matrix representation of elements in the Galois field (GF). As the main result, we provide the general structure of the parity-check matrix for a GCC, which applies to traditional concatenated codes as well. This formalism completes the matrix formalism of a GCC and provides a new perspective that enables effective design and analysis of GCCs.

Matrix representation of elements in Galois field. Given a Galois field e.g., $\mathrm{GF}(q^m)$ with its vector representation, we can define a nonzero element in $\mathrm{GF}(q^m)$, e.g., α^i, as follows:

$$[\alpha^i] = \begin{pmatrix} \alpha^i_{\mathrm{vec}} \\ \alpha^{i+1}_{\mathrm{vec}} \\ \vdots \\ \alpha^{i+m-1}_{\mathrm{vec}} \end{pmatrix}, \quad (1)$$

where $0 \leqslant i \leqslant q^{m-2}$, α is a primitive element of $\mathrm{GF}(q^m)$, α^i_{vec} represents the vector form of α^i, and the addition of the powers of α is a mod-q^{m-1} addition. Each entry in the brackets of (1) can be represented as an m-tuple vector; thus, the matrix

* Corresponding author (email: liuyang18@iie.ac.cn, yunjiangw@xidian.edu.cn)
† Shi S and Liu Y have the same contribution to this work.

representation of α^i is the following square matrix:

$$[\alpha^i] = \begin{pmatrix} \alpha_{i,1} & \alpha_{i,2} & \cdots & \alpha_{i,m} \\ \alpha_{i+1,1} & \alpha_{i+1,2} & \cdots & \alpha_{i+1,m} \\ \vdots & \vdots & & \vdots \\ \alpha_{i+m-1,1} & \alpha_{i+m-1,2} & \cdots & \alpha_{i+m-1,m} \end{pmatrix}, \quad (2)$$

where $\alpha^i_{\text{vec}} = (\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,m})$. The 0 element in $\text{GF}(q^m)$ is represented by the zero matrix; thus, each of the q^m elements in $\text{GF}(q^m)$ is represented by one and only one of these matrices, and each of these matrices represents one and only one element in $\text{GF}(q^m)$. It is easy to determine that the matrix representation of α^i in (2) is equivalent to the typical one obtained in [6]; however, Eq. (1) is obviously much more concise than (2).

Parity-check matrix formalism of GCC. Herein, we discuss the parity-check matrix formalism for a GCC with a mother inner code B_0 and its m-level partitions, each with parameters $[n, k_i]_q$, $i = 1, 2, \ldots, m$, such that $B_0 \supset B_1 \supset B_2 \cdots \supset B_L = \{\mathbf{0}\}$. The generator matrix of B_i is denoted as $G(B_i)$, and the parity-check matrix is denoted as $H(B_i)$.

We also have m outer codes A_i each with parameters $[N, K_i]_{Q_i}$, where $Q_i = q^{k_{i-1}-k_i}$. The parity-check matrix of A_i is denoted as $H(A_i)$, where

$$H(A_i) = \begin{pmatrix} \alpha^{(i)}_{1,1} & \alpha^{(i)}_{1,2} & \cdots & \alpha^{(i)}_{1,N} \\ \alpha^{(i)}_{2,1} & \alpha^{(i)}_{2,2} & \cdots & \alpha^{(i)}_{2,N} \\ \vdots & \vdots & & \vdots \\ \alpha^{(i)}_{N-K_i,1} & \alpha^{(i)}_{N-K_i,2} & \cdots & \alpha^{(i)}_{N-K_i,N} \end{pmatrix}. \quad (3)$$

Certainly, the resultant GCC C has parameters $[N \times n, K_1 \times K_2 \cdots \times K_i]_q$, and each sub-block of length n is derived from the so-called mother code B_0. Thus, this set is expressed as $\bar{C}_I$, where

$$\bar{C}_I = \begin{pmatrix} H_{B_0} & \mathbf{0}_{k\times n} & \cdots & \mathbf{0}_{k\times n} \\ \mathbf{0}_{k\times n} & H_{B_0} & \cdots & \mathbf{0}_{k\times n} \\ \vdots & \vdots & & \vdots \\ \mathbf{0}_{k\times n} & \mathbf{0}_{k\times n} & \cdots & H_{B_0} \end{pmatrix}. \quad (4)$$

The details of the structure of a GCC is shown in Appendix A. Here we give the parity-check matrix formalism in the following.

Proposition 1 (Parity-check matrix formalism for GCC)**.** The parity-check matrix of a GCC of order L comprises $L+1$ submatrices, where the 0th submatrix is the Kronecker product of the identity matrix and parity-check matrix of the mother inner code B_0, the i-th $(1 \leqslant i \leqslant L)$ submatrix is the Kronecker product of the parity-check matrix of the i-th outer code with each entry in its matrix form and the generator matrix of the i-th coset code $\mathbb{B}_i$ relative to B_0. If $H(C)$ is taken as the parity-check matrix of the resultant concatenated code C, then

$$H(C) = \bar{C}_I \cup \bigcup_{i=1}^{L} \bar{C}_{A_i}, \quad (5)$$

where

$$\bar{C}_{A_i} = [H(A_i)] \otimes G(\mathbb{B}_i) = \begin{pmatrix} \bar{C}^{(1,1)}_{A_i} & \bar{C}^{(1,2)}_{A_i} & \cdots & \bar{C}^{(1,N)}_{A_i} \\ \vdots & \vdots & & \vdots \\ \bar{C}^{(N-K_i,1)}_{A_i} & \bar{C}^{(N-K_i,2)}_{A_i} & \cdots & \bar{C}^{(N-K_i,N)}_{A_i} \end{pmatrix},$$

$$\bar{C}^{(h,k)}_{A_i} = \big[\alpha^{(i)}_{h,k}\big] \cdot G(\mathbb{B}_i), \quad \mathbb{B}_i = \big[\widetilde{[B_0/\mathcal{B}_i]}/\widetilde{B_0}\big],$$

and $\mathcal{B}_i = [B_{i-1}/B_i]$ is simply the i-th inner code concatenated with the outer code A_i in the i-th level concatenation. Herein, we use $\widetilde{X}$ to denote the dual code of X.

Given that B_0 is a trivial code with the entire space of size q^n being its codeword space, we obtain: $\mathbb{B}_i = \widetilde{[B_0/\mathcal{B}_i]}$. Therefore, $G(\mathbb{B}_i) = G(\widetilde{[B_0/\mathcal{B}_i]}) = H([B_0/\mathcal{B}_i]) = H([B_0/[B_{i-1}/B_i]])$. Furthermore, $[B_0/[B_{i-1}/B_i]]$ can be considered as the coset code of inner code $[B_{i-1}/B_i]$ relative to B_0. Considering $H(B_0) = (\mathbf{0})$, we obtain

$$H(C) = \bigcup_{i=1}^{L} \bar{C}_{A_i}, \quad (6)$$

where

$$\bar{C}_{A_i} = [H(A_i)] \otimes H([B_0/\mathcal{B}_i]) = \begin{pmatrix} \bar{C}^{(1,1)}_{A_i} & \bar{C}^{(1,2)}_{A_i} & \cdots & \bar{C}^{(1,N)}_{A_i} \\ \vdots & \vdots & & \vdots \\ \bar{C}^{(N-K_i,1)}_{A_i} & \bar{C}^{(N-K_i,2)}_{A_i} & \cdots & \bar{C}^{(N-K_i,N)}_{A_i} \end{pmatrix}.$$

Herein, $\bar{C}^{(h,k)}_{A_i} = [\alpha^{(i)}_{h,k}] \cdot H([B_0/\mathcal{B}_i])$.

Proof. To demonstrate that $H(C)$ in (5) is the parity-check matrix of the resultant GCC, we must verify whether the following two conditions are satisfied.

(1) $G(C) \cdot (H(C))^{\mathrm{T}} = \mathbf{0}$;

(2) $R_{G(C)} + R_{H(C)} = N \times n$,

where $R_{G(C)}$ and $R_{H(C)}$ are the rank of $G(C)$ and $H(C)$, respectively.

Before proving anything, we must demonstrate that the Kronecker products in (5) and (6) make sense. As $\mathcal{B}_i = [B_{i-1}/B_i]$, the size of $\mathcal{B}_i$ is $q^{(k_{i-1}-k_i)}$ and that of $[B_0/\mathcal{B}_i]$ is $q^{(k_0-(k_{i-1}-k_i))}$. Certainly, $[B_0/\mathcal{B}_i] \subset B_0$; thus, $\widetilde{B_0} \subset \widetilde{[B_0/\mathcal{B}_i]}$. Therefore, $\mathbb{B}_i = [\widetilde{[B_0/\mathcal{B}_i]}/\widetilde{B_0}]$ is a coset code of size

$q^{(k_{i-1}-k_i)}$ relative to B_0. The i-th outer code A_i is based on Q_i and $Q_i = q^{(k_{i-1}-k_i)}$; thus, each entry in $[H(A_i)]$ is a matrix of $\mathrm{GF}(q)^{(k_{i-1}-k_i)\times(k_{i-1}-k_i)}$. Because $G(\mathbb{B}_i)$ is a matrix of $\mathrm{GF}(q)^{(k_{i-1}-k_i)\times n}$, the Kronecker products in (6) and (7) seem sensible.

Herein, we demonstrate that the first condition holds. The generator matrix of a GCC with level L is given as follows:

$$G(C) = \bigcup_{i=1}^{L} [G(A_i)] \otimes G(\mathcal{B}_i). \tag{7}$$

Here, $[G(A_i)]$ again implies that each entry in $G(A_i)$ is in its matrix form. In particular, we obtain the following:

$$G(C) = \begin{pmatrix} [G(A_1)] & \otimes & G([B_0/B_1]) \\ [G(A_2)] & \otimes & G([B_1/B_2]) \\ \vdots & \vdots & \vdots \\ [G(A_L)] & \otimes & G([B_{L-1}/B_L]) \end{pmatrix}. \tag{8}$$

First, it is easy to observe that any row of $\bar{C}_I$ is orthogonal to all rows in $G(C)$ because each sub-block of the rows of the former comes from the rows of the parity-check matrix of B_0, and each sub-block of the rows of the latter comes from the sub-codes of B_0.

As shown in (6), each sub-block b_i of b is from $\mathbb{B}_i$. Here, $\mathbb{B}_i = [[\widetilde{B_0/\mathcal{B}_i}]/\widetilde{B_0}]$; thus, it is easy to confirm that b_i is orthogonal to any sub-block of rows yielded by $[G(A_j)] \otimes G([B_{j-1}/B_j])$ in (8) given $i \neq j$. Consequently, b is orthogonal to any rows from $[G(A_j)] \otimes G([B_{j-1}/B_j])$ for $j \neq i$. Notably, $G(A_i) \cdot (H(A_i))^{\mathrm{T}} = 0$; thus, it is easy to know that b is orthogonal to any row from $[G(A_i)] \otimes G([B_{i-1}/B_i])$. We can deliberately say that any row in $H(C)$ is orthogonal to all rows of $G(C)$, i.e., $G(C) \cdot (H(C))^{\mathrm{T}} = 0$; thus, the first condition is satisfied.

Finally, we demonstrate that the second condition holds. According to (8), $G(C)$ is based on $\mathrm{GF}(q)$ and its rank is given as follows:

$$R_{G(C)} = K_1 \times (k_0 - k_1) + \cdots + K_L \times (k_{L-1} - k_L).$$

According to (5), the rank of $H(C)$ is as follows:

$$R_{H(C)} = (n - K_0) \times N + \cdots + (N - K_L) \times (k_{L-1} - k_L).$$

Thus it is easy to see that

$$R_{G(C)} + R_{H(C)} = N \times n.$$

Examples for the parity-check formalism of a GCC are given in Appendix B.

Conclusion. For both theoretical and potentially practical reasons, we have introduced a parity-check matrix formalism for a GCC that is achieved by revisiting the matrix representation of the elements in a Galois Field in a concise manner. We have demonstrated that the parity-check matrix $(H(C))$ of a GCC of order L comprises L submatrices given that the mother inner code of a GCC is trivial; otherwise, it comprises $L+1$ submatrices when the mother inner code is nontrivial. The extra submatrix comes from the Kronecker product of the identity matrix and the parity-check matrix of the mother inner code. Recently, a belief propagation algorithm (BPA) was introduced to decode concatenated quantum codes [7, 8], which also demonstrates promising potential for decoding GCCs. As the parity-check matrix of a code is important for the BPA, we plan to explore decoding GCCs using the BPA in future.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61771377, 61502376, 61703175), Projects of International Cooperation and Exchanges of Shannxi Province (Grant Nos. 2017KW-003, 2016KW-037), and Fundamental Research Funds for the Central Universities.

Supporting information Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Lin S, Costello D J. Error Control Coding. 2nd ed. Upper Saddle River: Prentice-Hall, 2004
2 Dumer I. Concatenated codes and their multilevel generatlizations. In: Handbook of Coding Theory. Amsterdam: Elsevier, 1998. 1911–1988
3 Lin S J, Al-Naffouri T Y, Han Y S. FFT algorithm for binary extension finite fields and its application to reed-solomon codes. IEEE Trans Inform Theory, 2016, 62: 5343–5358
4 Gao J, Wang X F, Shi M J, et al. Gray maps on linear codes over $\mathbb{F}_p[v]/(v^m - v)$ and their applications. Sci Sin Math, 2016, 46: 1329–1336
5 Maucher J, Zyablov V V, Bossert M. On the equivalence of generalized concatenated codes and generalized error location codes. IEEE Trans Inform Theory, 2000, 46: 642–649
6 Wardlaw W P. Matrix representation of finite fields. Math Mag, 1994, 67: 289–293
7 Poulin D. Optimal and efficient decoding of concatenated quantum block codes. Phys Rev A, 2006, 74: 052333
8 Wang Y J, Zeng B, Grassl M, et al. Stabilzier formalism for generalized concatenated quantum codes. In: Proceedings of IEEE International Symposium on Information Theory, Istanbul, 2013. 529–533