SCIENCE CHINA
Information Sciences

• **Supplementary File** •

On the parity-check matrix of a 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*

Appendix A The basic idea of GCCs

A L-level concatenated codes C is formed from L outer codes and a set of L inner codes. We denote each of the L outer codes as A_i with parameters $[N, K_i]_{Q_i}$ where $1 \leqslant i \leqslant L$ and the L inner codes are obtained from a sequence linear codes denoted as B_i with parameters $[n, k_i]_q$ where $0 \leqslant i \leqslant L$. Note, B_i $(1 \leqslant i \leqslant L)$ are just a sequence of linear subcodes of B_0, such that

$$B_0 \supset B_1 \supset B_2 \cdots \supset B_L = \{\boldsymbol{0}\}, \tag{A1}$$

where B_L contains only the all-zero codeword $\boldsymbol{0}$.

It is worth to point out that the codes concatenated with the outer codes are not B_is, but the coset codes yielded from B_is. To see this point clearly, we take $[B_{i-1}/B_i]$ to denote the set of representatives of cosets in the partition B_{i-1}/B_i. $[B_{i-1}/B_i]$ is a linear code with $q^{k_{i-1}-k_i}$ codewords, and hence its dimension is $k_{i-1} - k_i$. This code is so-called a *coset code* [1]. In fact,

$$B_0 = [B_0/B_1] \oplus [B_1/B_2] \oplus \cdots \oplus [B_{L-1}/B_L]. \tag{A2}$$

In this sense, B_0 can be viewed as the *mother code* of inner codes. In the sequel, we call B_0 as mother inner code for short. For multilevel concatenated codes, these L coset codes are used as the inner codes concatenated with the L outer codes A_i, i.e., the ith level concatenated code has A_i as the outer code and $[B_{i-1}/B_i]$ as the corresponding inner code.

During each encoding interval, a message of K_i symbol over $GF(Q_i)$ is encoded with the outer code A_i into a codeword

$$\mathbf{a}^i = (a_0^i, a_1^i, \ldots, a_{N-1}^i). \tag{A3}$$

Then by using the coset code $[B_{i-1}/B_i]$, each symbol a_j^i of $\mathbf{a}^i$ is further encoded into a codeword $f_i(a_j^i)$, where $0 \leqslant j \leqslant N-1$ and $f(\cdot)$ denotes the encoding mapping of $[B_{i-1}/B_i]$. The output turn out to be

$$\mathbf{c}^i = (f_i(a_0^i), f_i(a_1^i), \ldots, f_i(a_{N-1}^i)), \tag{A4}$$

which is a codeword in the ith level concatenated code $A_i \circ [B_{i-1}/B_i]$. The resultant L-level concatenated code C is the direct-sum of L-component concatenated codes (see [1] for detail); i.e.

$$C = A_1 \circ [B_0/B_1] \oplus A_2 \circ [B_1/B_2] \oplus \cdots \oplus A_L \circ [B_{L-1}/B_L]. \tag{A5}$$

Appendix B Examples

To illustrate the matrix representation of elements in Galois field and the parity-check matrix formalism for GCCs, here we give three examples, one for the former and two for the latter. Particulary, to cover all case, in example 2, B_0 is not a trivial code and there are three outer codes all being binary code. In example 3, B_0 is set to be a trivial code and there are two outer codes with one of them is nonbinary.

Example 1: Suppose a Galois Field $GF(4)$ is generated by primitive polynomial $f(x) = 1 + x + x^2$ and α is the primitive root of $f(x)$, then the 4 elements in $GF(4)$ can be represented with its vector form as $\overrightarrow{0}$: (0 0); $\overrightarrow{1}$: (1 0); $\overrightarrow{\alpha}$: (0 1); $\overrightarrow{\alpha^2}$: (1 1). The corresponding matrix representations are as follows.

$$[0] = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, [\alpha^0] = \begin{pmatrix} \overrightarrow{\alpha^0} \\ \overrightarrow{\alpha^1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, [\alpha^1] = \begin{pmatrix} \overrightarrow{\alpha^1} \\ \overrightarrow{\alpha^2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, [\alpha^2] = \begin{pmatrix} \overrightarrow{\alpha^2} \\ \overrightarrow{\alpha^0} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{B1}$$

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

It is clear that both the addition "+" and multiplication "·" on $GF(2^2)$ are reduced to be matrix addition and matrix multiplication on $GF(2)$, respectively. Moreover, one can check that given the multiplier in vector form and the multiplicand in matrix form, the product is just the vector form of the same element that if one realizes the multiplication with both the multiplier and multiplicand in their power form. For example,

$$\overrightarrow{\alpha}\cdot[\alpha^2]=(0\ 1)\cdot\begin{pmatrix}1&1\\1&0\end{pmatrix}=(1\ 0)=\overrightarrow{\alpha^0}=\overrightarrow{\alpha\cdot\alpha^2}. \tag{B2}$$

Example 2: For the outer codes, let A_1 and A_2 are same both with parameters $[3,2]_2$ and with generator matrix $G(A_1)$ $(G(A_2))$ and parity-check matrix $H(A_1)$ $(H(A_2))$ as shown in Eq. (B3). Take $A_3=[3,1]_2$ being a repetition code with generator matrix $G(A_3)$ and parity-check matrix $H(A_3)$. Consider $B_0=[4,3]_2$, $B_1=[4,2]_2$, $B_2=[4,1]_2$ and $B_3=[4,0]_2=\{\boldsymbol{0}\}$ as usual. The corresponding generator matrices and parity-check matrices are as follows.

$$G(A_1)=G(A_2)=\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix},G(A_3)=\begin{pmatrix}1&1&1\end{pmatrix},H(A_1)=H(A_2)=\begin{pmatrix}1&1&1\end{pmatrix},H(A_3)=\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix}, \tag{B3}$$

$$G(B_0)=\begin{pmatrix}1&1&0&1\\1&0&1&0\\1&1&1&1\end{pmatrix},H(B_0)=\begin{pmatrix}0&1&0&1\end{pmatrix},G(B_1)=\begin{pmatrix}1&0&1&0\\1&1&1&1\end{pmatrix},G(B_2)=\begin{pmatrix}1&1&1&1\end{pmatrix}. \tag{B4}$$

As $\mathcal{B}_1=[B_0/B_1]$, $\mathcal{B}_2=[B_1/B_2]$ and $\mathcal{B}_3=[B_2/B_3]$, we have

$$G(\mathcal{B}_1)=\begin{pmatrix}1&1&0&1\end{pmatrix},G(\mathcal{B}_2)=\begin{pmatrix}1&0&1&0\end{pmatrix},G(\mathcal{B}_3)=\begin{pmatrix}1&1&1&1\end{pmatrix}. \tag{B5}$$

Consequently,

$$G([B_0/\mathcal{B}_1])=\begin{pmatrix}1&0&1&0\\1&1&1&1\end{pmatrix},G([B_0/\mathcal{B}_2])=\begin{pmatrix}1&1&0&1\\1&1&1&1\end{pmatrix},G([B_0/\mathcal{B}_3])=\begin{pmatrix}1&1&0&1\\1&0&1&0\end{pmatrix}. \tag{B6}$$

Thus,

$$G(\widetilde{[B_0/\mathcal{B}_1]})=\begin{pmatrix}0&1&0&1\\1&0&1&0\end{pmatrix},G(\widetilde{[B_0/\mathcal{B}_2]})=\begin{pmatrix}0&1&0&1\\1&1&0&0\end{pmatrix},G(\widetilde{[B_0/\mathcal{B}_3]})=\begin{pmatrix}0&1&0&1\\1&1&1&0\end{pmatrix}. \tag{B7}$$

As $G(\widetilde{B_0})=H(B_0)=\{0\ 1\ 0\ 1\}$, and $\mathbb{B}_i=[\widetilde{[B_0/\mathcal{B}_i]}/\widetilde{B_0}]$, we have

$$G(\mathbb{B}_1)=\begin{pmatrix}1&0&1&0\end{pmatrix},G(\mathbb{B}_2)=\begin{pmatrix}1&1&0&0\end{pmatrix},G(\mathbb{B}_3)=\begin{pmatrix}1&1&1&0\end{pmatrix}. \tag{B8}$$

Therefore, according to Eq. (5) in the main body, the parity-check matrix of the resultant GCC is as follows,

$$\begin{aligned}H(C)&=\overline{C}_I\cup\bigcup_{i=1}^{3}\overline{C}_{A_i}\\&=I\otimes H(B_0)\cup[H(A_1)]\otimes G(\mathbb{B}_1)\cup[H(A_2)]\otimes G(\mathbb{B}_2)\cup[H(A_3)]\otimes G(\mathbb{B}_3)\\&=\begin{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}&\otimes\ (0\ 1\ 0\ 1)\\(1\ 1\ 1)&\otimes\ (1\ 0\ 1\ 0)\\(1\ 1\ 1)&\otimes\ (1\ 1\ 0\ 0)\\\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix}&\otimes\ (1\ 1\ 1\ 0)\end{pmatrix}=\begin{pmatrix}0&1&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&1&0&0&0&0\\0&0&0&0&0&0&0&0&0&1&0&1\\1&0&1&0&1&0&1&0&1&0&1&0\\1&1&0&0&1&1&0&0&1&1&0&0\\1&1&1&0&1&1&1&0&0&0&0&0\\1&1&1&0&0&0&0&0&1&1&1&0\end{pmatrix}\end{aligned} \tag{B9}$$

The generator matrix of the resultant GCC is

$$\begin{aligned}G(C)&=\bigcup_{i=1}^{3}[G(A_i)]\otimes G(\mathcal{B}_i)\\&=\begin{pmatrix}\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix}&\otimes\ (1\ 1\ 0\ 1)\\\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix}&\otimes\ (1\ 0\ 1\ 0)\\(1\ 1\ 1)&\otimes\ (1\ 1\ 1\ 1)\end{pmatrix}=\begin{pmatrix}1&1&0&1&1&1&0&1&0&0&0&0\\1&1&0&1&0&0&0&0&1&1&0&1\\1&0&1&0&1&0&1&0&0&0&0&0\\1&0&1&0&0&0&0&0&1&0&1&0\\1&1&1&1&1&1&1&1&1&1&1&1\end{pmatrix}\end{aligned} \tag{B10}$$

It is clear that $G(C)\cdot(H(C))^T=0$ and $R_{G(C)}+R_{H(C)}=7+5=3\times4=12$. Thus $H(C)$ in Eq. (B9) is exactly the parity-check matrix of the resultant generalized concatenated code. We want to point out that, as the outer codes are binary, the matrix form of each entry in $G(A_i)$ or $H(A_i)$ is just its original form, i.e. $0\rightarrow(0)$ and $1\rightarrow(1)$. Therefore, in the last step of Eq. (B10) and Eq. (B9), we give $[H(A_i)]$ and $[G(A_i)]$ directly. In the following example, we show the case that the outer codes being nonbinary, where the quick way to obtain $[H(A_i)]$ and $[G(A_i)]$ by using our concise matrix representation of Galois Field in (see Eq. (1) and Eq. (2) in the letter).

Example 3: Take $A_1 = [3, 2]_4$ with generator matrix $G(A_1)$ and parity-check matrix $H(A_1)$, $A_2 = [3, 3]_2$ is a trivial code. Consider $B_0 = [3, 3]_2$, $B_1 = [3, 1]_2$ with generator matrix $G(B_1)$ and parity-check matrix $H(B_1)$, $B_2 = \{\boldsymbol{0}\}$ as usual. Here,

$$G(A_1) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{pmatrix}, H(A_1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, G(B_1) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, H(B_1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \tag{B11}$$

and α is just the primitive root of the primitive polynomial in *Example 1*. Given B_0 and A_2 being two trivial codes, we can give their generator matrices as follows,

$$G(A_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, G(B_0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}. \tag{B12}$$

Because $\mathcal{B}_1 = [B_0/B_1]$ and $\mathcal{B}_2 = [B_1/B_2]$, we have

$$G(\mathcal{B}_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, G(\mathcal{B}_2) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \tag{B13}$$

It is evident, $G(\widetilde{B_0}) = H(B_0) = \{\boldsymbol{0}\}$ given B_0 being trivial, thus $\mathbb{B}_1 = [\widetilde{B_0/\mathcal{B}_1}]$ and $\mathbb{B}_2 = [\widetilde{B_0/\mathcal{B}_2}]$, so

$$G(\mathbb{B}_1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, G(\mathbb{B}_2) = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}. \tag{B14}$$

Thus,

$$\begin{aligned} H_C &= \overline{C}_I \cup \overline{C}_{A_1} \cup \overline{C}_{A_2} \\ &= I \otimes H(B_0) \cup [H(A_1)] \otimes G(\mathbb{B}_1) \cup [H(A_2)] \otimes G(\mathbb{B}_2) \\ &= I \otimes \boldsymbol{0} \cup [H(A_1)] \otimes G(\mathbb{B}_1) \cup \boldsymbol{0} \otimes G(\mathbb{B}_2) \\ &= [H(A_1)] \otimes G(\mathbb{B}_1) \\ &= \left(\begin{array}{cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right) \otimes \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} && \text{(B15)} \\ &= \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix} && \text{(B16)} \end{aligned}$$

The generator matrix of the resultant concatenated code C can be given as follows,

$$\begin{aligned} G(C) &= [G(A_1)] \otimes G(\mathcal{B}_1) \cup [G(A_2)] \otimes G(\mathcal{B}_2) \\ &= \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cup \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\ &= \left(\begin{array}{cc|cc|cc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right) \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cup \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} && \text{(B17)} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}. && \text{(B18)} \end{aligned}$$

It is evident to check that $G(C) \cdot (H(C))^T = 0$ and $R_{G(C)} + R_{H(C)} = 7 + 2 = 3 \times 3 = 9$. So we conclude that $H(C)$ in Eq. (B16) is exactly the parity-check matrix of the resultant generalized concatenated code. Please note in Eq. (B15) and Eq. (B17), the matrix representation of elements in GF(4) is used as shown in Eq. (B1).

References

1 Lin S, Costello D J, Jr. Error control coding 2nd ed. Pearson Education Inc., 2004, 739