Proof of Theorem 1

Theorem 1: Assume a Raptor-Like base matrix $\mathbf{B}$ is defined as follows, with the first $V > 1$ column punctured. If $\mathbf{B}$ has a non-zero minimum distance upper bound $d_{\min,\text{upp}} > 0$ which can be computed as in [1], $\mathbf{B}$ has no parallel edges and all the punctured columns have not smaller than V non-zero elements in $\mathbf{B}_H$, then $d_{\min,\text{upp}}$ could be achieved in some $M \times (M+1)$ sub-matrix of $\mathbf{B}$, such that all the last $(M-G)$ parity-check columns of $\mathbf{B}$ are in that sub-matrix.

$$\mathbf{B} = \begin{bmatrix} (\mathbf{B}_H)_{G\times(K+G)} & \mathbf{0}_{G\times(M-G)} \\ (\mathbf{B}_U)_{(M-G)\times(K+G)} & \mathbf{I}_{(M-G)\times(M-G)} \end{bmatrix}.$$

Appendix A
Proof of Theorem 1

Suppose $\mathcal{S}$ denotes a set of $(M+1)$ columns in the total $N = M + K$ columns of $\mathbf{B}$, and all the possible $\binom{N}{M+1}$ sets $\mathcal{S}$ forms a set Λ. $\mathcal{P}$ is the set of V punctured columns. It is further assumed that all the columns are indexed as 1 to N in order, and the punctured columns are the leftmost V columns indexed 1 to V, i.e., $\mathcal{P} = \{1, 2, \cdots, V\}$. From [1], we have

$$d_{\min,\text{upp}} = \min_{\mathcal{S}\in\Lambda}{}^{*} \sum_{i\in\mathcal{S}\backslash\mathcal{P}} \text{Perm}\left(\mathbf{B}_{\mathcal{S}\backslash i}\right) > 0, \tag{1}$$

where $\min^*$ means the minimum of all the non-zero elements, Perm means the permanent of a $M \times M$ square matrix. $\mathbf{B}_{\mathcal{S}\backslash i}$ means the $M \times M$ sub-matrix composed of the M columns in $\mathcal{S}\backslash i$ in order. Then we only need to show that $\exists \mathcal{S} \in \Lambda, \{N - M + G + 1, \cdots, N\} \subseteq \mathcal{S}, \text{s.t.}$

$$d_{\min,\text{upp}} = \sum_{i\in\mathcal{S}\backslash\mathcal{P}} \text{Perm}\left(\mathbf{B}_{\mathcal{S}\backslash i}\right). \tag{2}$$

For convenience, we denote $\mathcal{T} = \{N - M + G + 1, \cdots, N\}$ as set of the last $M - G$ columns in $\mathbf{B}$. Then we firstly prove the following lemma.

Lemma 1: If $\exists \mathcal{S} \in \Lambda, |\mathcal{S} \cap \mathcal{T}| = t < M - G, \text{s.t.}$

$$d = \sum_{i\in\mathcal{S}\backslash\mathcal{P}} \text{Perm}\left(\mathbf{B}_{\mathcal{S}\backslash i}\right) > 0, \tag{3}$$

then $\exists \mathcal{S}^* \in \Lambda, |\mathcal{S}^* \cap \mathcal{T}| = t + 1, \text{s.t.}$

$$d \geq d^* = \sum_{i\in\mathcal{S}^*\backslash\mathcal{P}} \text{Perm}\left(\mathbf{B}_{\mathcal{S}^*\backslash i}\right) > 0. \tag{4}$$

Proof: According to equation (3), There exists an bijection $\sigma : \mathcal{S} \to \{0, 1, 2, \cdots M\}, \text{s.t.}$

$$\forall j \in \mathcal{S}\backslash\sigma^{-1}(0), \mathbf{B}(\sigma(j), j) = 1.$$

Case 1: $\exists j_1 \in \mathcal{S}\backslash(\mathcal{P} \cup \mathcal{T} \cup \{\sigma^{-1}(0)\}), \sigma(j_1) > G$. Suppose that $\sigma(j_1) + K \neq \sigma^{-1}(0)$, otherwise there exists only one j_1 such that $\sigma(j_1) + K = \sigma^{-1}(0)$, and then we could change the bijection σ to σ^* such that $\sigma^*(j_1) = 0, \sigma^*(\sigma^{-1}(0)) = j_1$ and for other $j \in \mathcal{S}$, $\sigma(j) = \sigma^*(j)$. Then it can be convert to Case 2. Now that $\sigma(j_1) + K \neq \sigma^{-1}(0)$, and we can directly change the column j_1 in $\mathcal{S}$ to the column $\sigma(j_1) + K \in \mathcal{T}$, to form a new set $\mathcal{S}^* = (\mathcal{S}\backslash j_1) \cup \{\sigma(j_1) + K\}$. Since the set of non-zero entry positions in the column $\sigma(j_1) + K$ are included in the set of non-zero entry positions in the column j_1, we have

$$d \geq d^* = \sum_{i\in\mathcal{S}^*\backslash\mathcal{P}} \text{Perm}\left(\mathbf{B}_{\mathcal{S}^*\backslash i}\right).$$

Note that we also have

$$d^* \geq \text{Perm}(\mathbf{B}_{\mathcal{S}^*\backslash\sigma^{-1}(0)}),$$

and since $\mathbf{B}(j_1, \sigma(j_1)) = \mathbf{B}(\sigma(j_1) + K, \sigma(j_1)) = 1$, then

$$\text{Perm}(\mathbf{B}_{\mathcal{S}^*\backslash\sigma^{-1}(0)}) \geq \prod_{j'\in\mathcal{S}\backslash\sigma^{-1}(0)} \mathbf{B}(j', \sigma(j')) > 0.$$

We also have $|\mathcal{S}^* \cap \mathcal{T}| = t + 1$, then Lemma 1 is valid.

Case 2: $\forall j \in \mathcal{S}\backslash(\mathcal{P} \cup \mathcal{T} \cup \{\sigma^{-1}(0)\}), \sigma(j) \leq G$. Then since $|\mathcal{S} \cap \mathcal{T}| = t < M - G$, $\exists j_1 \in \mathcal{P}$, s.t. $\sigma(j_1) > G$, otherwise all the columns $\sigma(j) > G$ are in $\mathcal{T}$ and thus $|\mathcal{S} \cap \mathcal{T}| = M - G$, which contradicts. Now we could change the column j_1 in $\mathcal{S}$ to the column $\sigma(j_1) + K \in \mathcal{T}$, to form a new set of columns $\mathcal{S}^* = (\mathcal{S}\backslash j_1) \cup \{\sigma(j_1) + K\}$. Then the set of punctured columns in $\mathcal{S}^*$ is changed to $\mathcal{P}^* = \mathcal{P}\backslash j_1$. Similar to Case 1, we have

$$d^* = \sum_{i\in\mathcal{S}\backslash\mathcal{P}^*} \text{Perm}(\mathbf{B}_{\mathcal{S}^*\backslash i}) > 0.$$

Now we only need to prove $d - d^* \geq 0$, and since $|\mathcal{S}^* \cap \mathcal{T}| = t + 1$, then Lemma 1 is valid. For simplicity, suppose $\mathcal{W}$ is a set of M columns in $\mathbf{B}$, and $\omega_{\mathcal{W}} : \mathcal{W} \to \{1, 2, \cdots, M\}$ is a bijection. We define

$$p(\omega_{\mathcal{W}}, \mathcal{W}) = \prod_{j\in\mathcal{W}} \mathbf{B}(j, \omega_{\mathcal{W}}(j)) > 0.$$

Then we have

$$d - d^* = \sum_{i\in\mathcal{S}\backslash\mathcal{P}} \sum_{\omega\in\chi_1(\mathcal{S}\backslash i)} p(\omega, \mathcal{S}\backslash i) - \sum_{w\in\chi(\mathcal{S}\backslash j_1)} p(\omega, \mathcal{S}\backslash j_1),$$

where $\chi_1(S\backslash i)$ is the set of all the valid bijections $\omega : \mathcal{S}\backslash i \to \{1, 2, \cdots, M\}$ such that $\omega(j_1) \neq \sigma(j_1)$ and $\mathbf{B}(j, \omega(j)) = 1$ for any $j \in \mathcal{S}\backslash i$, $\chi(S\backslash j_1)$ is the set of all the valid bijections $\omega : \mathcal{S}\backslash j_1 \to \{1, 2, \cdots, M\}$ such that $\mathbf{B}(j, \omega(j)) = 1, \forall j \in \mathcal{S}\backslash j_1$. Then we would show that there exists an injection $q : \chi(\mathcal{S}\backslash j_1) \to \{(i, \chi_1(\mathcal{S}\backslash i)) | i \in \mathcal{S}\backslash\mathcal{P}\}$ such that if $(i, \omega^*) = q(\omega)$, then $p(\omega^*, \mathcal{S}\backslash i) = p(\omega, \mathcal{S}\backslash j_1)$. Thus $d - d^* \geq 0$.

Note that according to the assumptions in Theorem 1, for any $\omega \in \mathcal{S}\backslash j_1$, $\exists t \leq G, \text{s.t. } \mathbf{B}(t, j_1) = 1$ and $\omega^{-1}(t) \notin \mathcal{T} \cup \mathcal{P}$. That is because at most $V - 1$ punctured columns are in $\mathcal{S}\backslash j_1$, and each punctured column has at least V non-zero elements in $\mathbf{B}_H$. Then we can construct $\omega^* : \mathcal{S}\backslash\omega^{-1}(t) \to \{1, 2, \cdots M\}$ such that $\omega^*(j_1) = t$ and $\omega^*(j) = \omega(j), \forall j \in \mathcal{S}\backslash\{\omega^{-1}(t), j_1\}$. Obviously $p(\omega^*, \mathcal{S}\backslash\omega^{-1}(t)) = p(\omega, \mathcal{S}\backslash j_1) = 1$, and we define $(\omega^{-1}(t), \omega^*) = q(\omega)$. Now we show that q is an injection. For any $\omega_1, \omega_2 \in \mathcal{S}\backslash j_1$, if $q(\omega_1) = q(\omega_2)$, we denote the t chosen for ω_1, ω_2 as t_1, t_2, respectively. Then because $\mathcal{S}\backslash\omega_1^{-1}(t_1) = \mathcal{S}\backslash\omega_2^{-1}(t_2)$, we have $\omega_1^{-1}(t_1) = \omega_2^{-1}(t_2)$. Then $\omega_1(j) = \omega_2(j)$

for all $j \in \mathcal{S}\backslash\omega_1^{-1}(t_1)$, according to the definition of ω^*. Since ω_1, ω_2 are both bijections, we have $t_1 = t_2$ and then $\omega_1 = \omega_2$. That completes the proof of Lemma 1. ■

According to Lemma 1 and mathematic induction, suppose that $\exists\mathcal{S} \in \Lambda, d_{\min,\text{upp}} = \sum_{i\in\mathcal{S}\backslash\mathcal{P}}(\mathbf{B}_{\mathcal{S}\backslash i})$, we have that $\exists\mathcal{S}^* \in \Lambda, |\mathcal{S}^* \cap \mathcal{T}| = M - G, d = \sum_{i\in\mathcal{S}^*\backslash\mathcal{P}}(\mathbf{B}_{\mathcal{S}^*\backslash i}), \text{s.t.}$

$$d_{\min,\text{upp}} \geq d \geq d_{\min,\text{upp}} \Rightarrow d = d_{\min,\text{upp}}.$$

That completes the proof of Theorem 1.

References

[1] B. K. Butler and P. H. Siegel, “Bounds on the Minimum Distance of Punctured Quasi-Cyclic LDPC Codes,” *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4584–4597, 2013.