An Upper Bound on the Minimum Distance of Tail-Biting LDPC Convolutional codes

Alexey Frolov

Inst. for Information Transmission Problems
Russian Academy of Sciences
Moscow, Russia
alexey.frolov@iitp.ru

Abstract. The minimum distance of tail-biting low-density parity-check convolutional (TB-LDPCC) codes over $GF(q)$ is investigated. An upper bound on the minimum distance of TB-LDPCC codes is derived. An asymptotic analysis of the new bound is done. It is shown that the bound not only improves all the known upper bounds for linear codes at high rates but at some cases lies under the Gilbert–Varshamov bound.

Keywords: error-correcting coding, LDPC code, convolutional code, minimum distance

1 Introduction

The LDPC convolutional (LDPCC) codes were proposed in [1]. These codes are the convolutional counterparts of LDPC block codes [2, 3]. Note, that a class of LDPCC codes includes spatially-coupled LDPC codes [4, 5]. LDPCC codes have some advantages in comparison to LDPC block codes [6]. An important feature of LDPCC codes is that the same encoder can be used to obtain codes sequences of varying lengths with quite good performance by choosing different termination lengths. However, the introduction of a zero-tail for termination results in the so-called rate loss.

Tail-biting was introduced in [7,8] as a method of terminating a convolutional code without the rate loss caused by standard termination. The resulting tail-biting codes have a dual nature, i.e., they simultaneously have the properties of both block and convolutional codes. TB-LDPCC codes were introduced in [9].

In this paper we investigate the minimum distance of TB-LDPCC codes. Lower bounds on the minimum distance of such codes were given in [10]. Here we derive an upper bound on the minimum distance of TB-LDPCC codes.

Our contribution is as follows. We derive an upper bound on the minimum distance of TB-LDPCC codes. An asymptotic analysis of the new bound is done. It is shown that the bound not only improves all the known bounds for linear codes at high rates but at some cases lies under the Gilbert–Varshamov bound.

2 Preliminaries

Let us construct the parity-check matrix of TB-LDPCC code $\mathcal{C}$. Let us denote the syndrome former memory of mother LDPCC code by m. Let the termination length (in blocks) n be an integer greater or equal to m. Let $\mathbf{H}_i(j)$, $0 \le i \le m$, $0 \le j \le n-1$, be matrices over $\mathbb{F}_q$ of size $(c-b) \times c$. As usual for LDPCC codes we suppose the matrices $\mathbf{H}_0(j)$, $0 \le j \le n-1$, to be of full rank.The parity-check matrix of TB-LDPCC code $\mathcal{C}$ of length $N = nc$ is given by (1).

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_m(0) & \mathbf{H}_{m-1}(0) & \cdots & \mathbf{H}_0(0) & \mathbf{0} & \mathbf{0} & \cdots & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_m(1) & \mathbf{H}_{m-1}(1) & \cdots & \mathbf{H}_0(1) & \mathbf{0} & \cdots & \cdots & \mathbf{0} \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \mathbf{0} & \cdots & \cdots & \mathbf{0} & \mathbf{H}_m(n-m-1) & \mathbf{H}_{m-1}(n-m-1) & \cdots & \cdots & \mathbf{H}_0(n-m-1) \\ \mathbf{H}_0(n-m) & \mathbf{0} & \cdots & \cdots & \mathbf{0} & \mathbf{H}_m(n-m) & \mathbf{H}_{m-1}(n-m) & \cdots & \mathbf{H}_1(n-m) \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \mathbf{H}_{m-1}(n-1) & \cdots & \mathbf{H}_1(n-1) & \mathbf{H}_0(n-1) & \mathbf{0} & \cdots & \cdots & \mathbf{0} & \mathbf{H}_m(n-1) \end{bmatrix} \tag{1}$$

The rate of constructed TB-LDPCC code satisfies the inequality

$$R(\mathcal{C}) \ge \frac{b}{c}. \tag{2}$$

3 Upper bound

To obtain an upper bound we use so-called shortening method [11–13].

Lemma 1. *Let $\mathcal{C}$ be a linear code of length N over $\mathbb{F}_q$. Let the parity-check matrix $\mathbf{H}$ of $\mathcal{C}$ have a special form, shown in Fig.* 1*, then*

$$R(\mathcal{C}) \le R(\mathcal{C}_1)(1-\tau) + R(\mathcal{C}_2)\tau, \tag{3}$$

where the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ correspond to the parity-check matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ accordingly.

Proof. Let $\mathbf{c} \in \mathcal{C}$, then $\mathbf{c}$ can be presented as follows

$$\mathbf{c} = (\mathbf{c}_1 \, \mathbf{c}_2).$$

Note, that $\mathbf{c}_1$ is a codeword of $\mathcal{C}_1$, so there are $|\mathcal{C}_1| = q^{R_1(1-\tau)N}$ different possibilities to choose $\mathbf{c}_1$. To find $\mathbf{c}_2$ given $\mathbf{c}_1$ one need to solve a system of linear equations

$$\mathbf{H}_2 \mathbf{c}_2^T = \mathbf{A} \mathbf{c}_1^T.$$

The system has at most $|\mathcal{C}_2| = q^{R_2 \tau N}$ solutions. Thus,

$$|\mathcal{C}| \le q^{R_1(1-\tau)N + R_2 \tau N}.$$

After taking the logarithm and dividing by N we obtain the needed result.

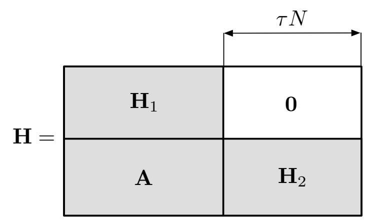

Fig. 1. Special form of $\mathbf{H}$

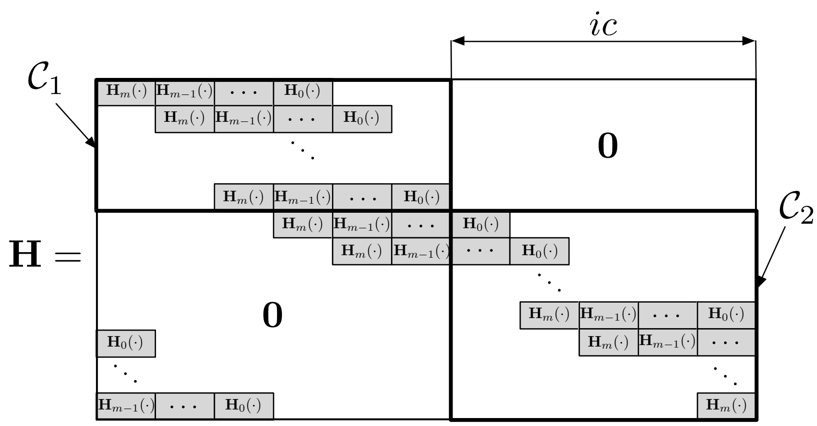

Fig. 2. Parity-check matrix of TB-LDPCC code

Now we are ready to prove a theorem.

Theorem 1. *Let $\mathcal{C}$ be TB-LDPCC code with the length $N = nc$, the syndrome former memory m and the minimum distance d, then*

$$R(\mathcal{C}) \leq \min_{1 \leq i \leq n-m} \left[\frac{m}{m+i} + \frac{i}{m+i} R^* \left(ic, d\right) \right], \tag{4}$$

where $R^*(N, d)$ is any upper bound on the rate of a linear code[1].

Proof. The parity-check matrix of the code $\mathcal{C}$ is shown in Fig. 2. Let us choose $i \in \mathbb{N}$, $1 \leq i \leq n - m$, and apply Lemma 1. We have

$$R(\mathcal{C}) \leq R(\mathcal{C}_1) \left(1 - \frac{i}{n}\right) + R(\mathcal{C}_2) \frac{i}{n}. \tag{5}$$

It is easy to check, that

$$R(\mathcal{C}_1) = 1 - \left(\frac{n-m-i}{n-i}\right) \left(\frac{c-b}{c}\right),$$

[1] we suppose $R^*(N, d)$ to give 0 if the code with parameters N and d does not exist (e.g. $d > N$).

here we used the fact that the matrices $\mathbf{H}_0(j)$, $0 \le j \le n-1$, have full rank (so their rates are equal to b/c).

Note, that in accordance to (2)

$$R(\mathcal{C}) \ge \frac{b}{c},$$

so

$$R(\mathcal{C}_1) \le 1 - \left(\frac{n-m-i}{n-i}\right)(1 - R(\mathcal{C})). \tag{6}$$

The code $\mathcal{C}_2$ corresponds to a subcode $\widetilde{\mathcal{C}}$ of the code $\mathcal{C}$. Indeed, one just need to add a prefix of $(n-i)c$ zeros to the codeword $\mathbf{c}_2$ of $\mathcal{C}_2$ to obtain a codeword $\widetilde{\mathbf{c}}$ of $\widetilde{\mathcal{C}}$, i.e.

$$\widetilde{\mathbf{c}} = (\mathbf{0}\,\mathbf{c_2}).$$

Thus,

$$d(\mathcal{C}_2) = d(\widetilde{\mathcal{C}}) \ge d(\mathcal{C}),$$

hence

$$R(\mathcal{C}_2) \le R^*(ic, d). \tag{7}$$

After substituting of (6) and (7) for (5) we obtain the needed result.

4 Asymptotic analysis

In this section we carry out an asymptotic analysis of the obtained bound. We consider two cases:

- c is fixed, $n \to \infty$, $m = \mu n$;
- n and m are fixed, $c \to \infty$.

4.1 Case 1: c is fixed, $n \to \infty$, $m = \mu n$

Corollary 1. *Let c be fixed. Let $\{\mathcal{C}_n\}_{n=\lceil 1/\mu \rceil}^{\infty}$ be a sequence of TB-LDPCC codes over $\mathbb{F}_q$ with lengths $N(\mathcal{C}_n) = nc$, minimum distances $d(\mathcal{C}_n) = \delta N(\mathcal{C}_n)$ and syndrome former memories $m(\mathcal{C}_n) = \mu n$, then*

$$\begin{aligned} R(\delta, \mu) &= \lim_{n\to\infty} R(\mathcal{C}_n) \\ &\le \min_{\frac{q}{q-1}\delta \le \tau \le 1-\mu} \left[\frac{\mu}{\mu+\tau} + \frac{\tau}{\mu+\tau} R^*\left(\delta/\tau\right)\right], \end{aligned}$$

where $R^*(\delta)$ is any asymptotic upper bound on the rate of a linear code.

Proof. Asymptotic form can be easily derived from (4). For the condition

$$\frac{\delta}{\tau} \le \frac{q-1}{q}$$

to be satisfied we need

$$\tau \ge \frac{q}{q-1}\delta.$$

It is easy to check that minimization domain can be reduced to $\frac{q}{q-1}\delta \le \tau \le 1-\mu$.

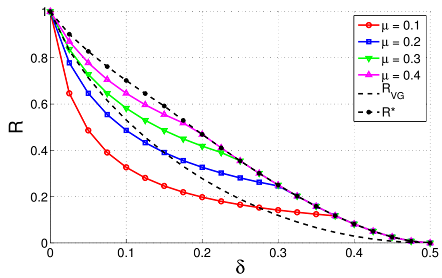

Fig. 3. Case 1: $q = 2$

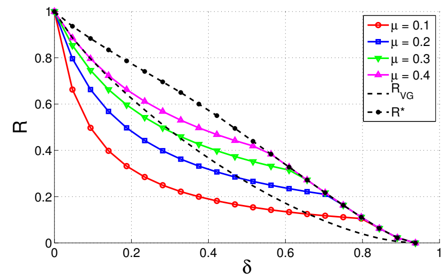

Fig. 4. Case 1: $q = 16$

If we use the Plotkin bound [14] as R^* one can observe that the minimum is reached when $\tau = \frac{q}{q-1}\delta$ and obtain such a bound

$$R(\delta, \mu) \leq 1 - \frac{\frac{q}{q-1}\delta}{\mu + \frac{q}{q-1}\delta}.$$

In what follows we use a minimum of the Elias–Bassalygo bound [15], the McEliece–Rodemich–Rumsey–Welch bound [16] and the Plotkin bound as R^*.

Results obtained for $q = 2$ and $q = 16$ are shown in Figs. 3 and 4, respectively. In each of the figures, six functions are plotted:

– R_{VG}, the Gilbert–Varshamov bound;
– R^*, an upper bound on the rate of linear codes;
– upper bounds for TB-LDPCC codes for $\mu = 0.1$, $\mu = 0.2$, $\mu = 0.3$ and $\mu = 0.4$.

We see that the obtained bound improves R^* at high rates. It should be mentioned that there is an interval of μ such that $R(\delta, \mu)$ lies under the Gilbert-Varshamov bound (at high rates) for any μ in the interval. The interval expands as q grows. This means that TB-LDPCC codes are worse than the best known linear codes at high rates.

4.2 Case 2: n and m are fixed, $c \to \infty$.

Corollary 2. *Let n and m be fixed. Let $\{\mathcal{C}_c\}_{c=1}^{\infty}$ be a sequence of TB-LDPCC codes over $\mathbb{F}_q$ with lengths $N(\mathcal{C}_c) = nc$, minimum distances $d(\mathcal{C}_c) = \delta N(\mathcal{C}_c)$ and syndrome former memories $m(\mathcal{C}_n) = m$, then*

$$\begin{aligned} R(\delta, n, m) &= \lim_{c \to \infty} R(\mathcal{C}_c) \\ &\leq \min_{1 \leq i \leq n-m} \left[\frac{m}{m+i} + \frac{i}{m+i} R^*\left(\delta n / i\right) \right]. \end{aligned}$$

To give an example of the obtained bound we consider a case $m = 1$ and plot the upper bounds for different termination lengths (n). This case corresponds

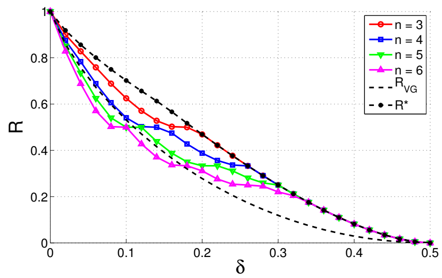

Fig. 5. Case 2: $q = 2$

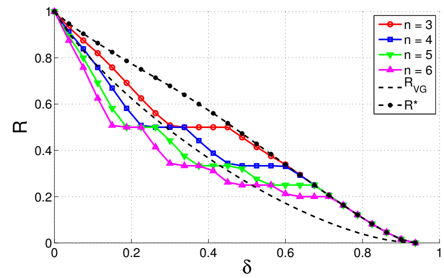

Fig. 6. Case 2: $q = 16$

to a class of tail-biting Unit Memory (TB-UM) codes (see [17–19]), which are a partial case of the codes considered in this paper.

Results obtained for $q = 2$ and $q = 16$ are shown in Figs. 5 and 6, respectively. As in the Case 1 in each of the figures, six functions are plotted:

– R_{VG}, the Gilbert–Varshamov bound;
– R^*, an upper bound on the rate of linear codes;
– upper bounds for TB-UM (TB-LDPCC with $m = 1$) codes for $n = 3$, $n = 4$, $n = 5$ and $n = 6$.

5 Conclusion

We derived an upper bound on the minimum distance of TB-LDPCC codes. An asymptotic analysis of the new bound is done. Two asymptotic cases are considered: c is fixed, $n \to \infty$, $m = \mu n$ and n and m are fixed, $c \to \infty$. It is shown that the bound not only improves all the known bounds for linear codes at high rates but at some cases lies under the Gilbert–Varshamov bound.

Acknowledgment

The reported study was supported by RFBR, research projects no. 13-01-12458, no. 14-07-31197 and no. 14-01-93108.

References

1. A. Jimenez-Feltstrom and K. Sh. Zigangirov. Time-varying periodic convolutional codes with low-density parity-check matrix. *IEEE Trans. Inf. Theory*, vol. 45, pp. 2181–2191, Sep. 1999.
2. R. G. Gallager, *Low-Density Parity-Check Codes.* Cambridge: MIT Press, 1963.
3. R. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

4. S. Kudekar, T. J. Richardson, and R. L. Urbanke. Threshold saturation via spatial coupling: why convolutional LDPC ensembles perform so well over the BEC. *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803–834, Feb. 2011.
5. S. Kudekar, T. J. Richardson, and R. L. Urbanke. Spatially Coupled Ensembles Universally Achieve Capacity Under Belief Propagation. *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7761–7813, Dec. 2013.
6. D. J. Costello, Jr., A. E. Pusane, S. Bates, and K. Sh. Zigangirov. A comparison between LDPC block and convolutional codes. In Proc. *Information Theory and Applications Workshop*, San Diego, USA, 2006.
7. G. Solomon and H. C. A. van Tilborg. A connection between block and convolutional codes. *SIAM J. Appl. Math.*, vol. 37, pp. 358–369, 1979.
8. J. H. Ma and J. K. Wolf. On tail-biting convolutional codes. *IEEE Trans. Commun.*, vol. 34, pp. 104111, 1986.
9. M. B. S. Tavares, K. Sh. Zigangirov, G. P. Fettweis. Tail-Biting LDPC Convolutional Codes. In Proc. *IEEE Int. Symp. Inf. Theory*, pp.2341–2345, 24–29 June 2007
10. D. Truhachev, K. Sh. Zigangirov, and D. J. Costello, Jr. Distance bounds for periodically time-varying and tail-biting LDPC convolutional codes. *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4301–4308, 2010.
11. Y. Ben-Haim and S. Litsyn. Upper bounds on the rate of ldpc codes as a function of minimum distance. *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2092–2100, May 2006.
12. A. Frolov, V. Zyablov. Upper and Lower Bounds on the Minimum Distance of Expander Codes. In Proc. *IEEE Int. Symp. Inf. Theory*, pp. 1302–1306, July 31–August 5, 2011.
13. A. Frolov, V. Zyablov. Bounds on the minimum code distance for nonbinary codes based on bipartite graphs. *Problems Inf. Transm.*, vol. 47, no. 4, pp 327–341, 2011
14. W. W. Peterson and E. J. Weldon, Jr. *Error-Correcting Codes.* Cambridge: MIT Press, 1972.
15. L. A. Bassalygo. New Upper Bounds for Error Correcting Codes. *Problems Inf. Transm.*, vol. 1, no. 4, pp. 32–35, 1965.
16. R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch. New Upper Bounds on the Rate of a Code via the Delsarte–MacWilliams Inequalities. *IEEE Trans. Inf. Theory* vol. 23, no. 2, pp. 157–166, 1977.
17. L. nan Lee. Short unit-memory byte-oriented binary convolutional codes having maximal free distance (corresp.). *IEEE Trans. Inform. Theory*, vol. 22, no. 3, pp. 349–352, May 1976.
18. V. Zyablov and V. Sidorenko. On periodic (partial) unit memory codes with maximum free distance. In *Error Control, Cryptology, and Speech Compression*, ser. Lecture Notes in Computer Science, A. Chmora and S. Wicker, Eds. Springer Berlin Heidelberg, 1994, vol. 829, pp. 74–79.
19. J. Justesen. Bounded distance decoding of unit memory codes. *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1616–1627, Sep. 1993.