On the Hamming-Like Upper Bound on the Minimum Distance of LDPC Codes

Alexey Frolov

Email: alexey.frolov@iitp.ru

Inst. for Information Transmission Problems
Russian Academy of Sciences

ACCT 2014
September 7–13, 2014
Svetlogorsk, Russia

Outline

1. Task statement
2. Generalized LDPC codes
3. Irregular LDPC codes
4. Numerical results

Task statement

In

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.

a Hamming-like upper bound on the minimum distance of regular binary LDPC codes is given. We extend the bound to the case of irregular and generalized LDPC codes over $\mathbb{F}_q$.

Constituent code

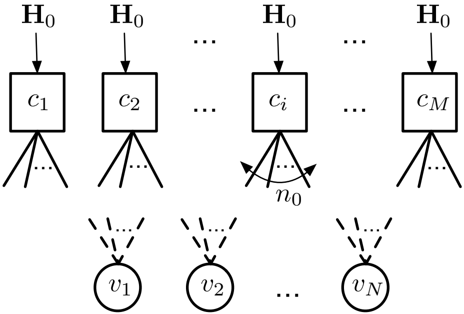
We assume $\mathcal{C}_0$ to be an $[n_0, R_0, d_0]$ code over $\mathbb{F}_q$. Let us denote the parity-check matrix of the *constituent code* by $\mathbf{H}_0$. The matrix has size $m_0 \times n_0$, where $m_0 = (1 - R_0)n_0$.

Let $G(s, n_0, d_0)$ be the *weight enumerator* of the code $\mathcal{C}_0$, i.e.

$$G(s, n_0, d_0) = 1 + \sum_{i=d_0}^{n_0} A(i)s^i,$$

where $A(i)$ is the number of codewords of weight i in a code $\mathcal{C}_0$.

Tanner graph



To check if $\mathbf{v} = (v_1, v_2, \ldots, v_N) \in \mathbb{F}_q^N$ is a codeword of $\mathcal{C}$ we associate the symbols of $\mathbf{v}$ to the variable nodes. The word $\mathbf{v}$ is called a codeword of $\mathcal{C}$ if all the constituent codes are satisfied.

Upper bound for generalized LDPC codes

Theorem

Let $\mathcal{C}$ be a generalized LDPC code of length N, rate R, minimum distance δN, with constituent $[n_0, R_0, d_0]$ code $\mathcal{C}_0$ over $\mathbb{F}_q$. Let $G(s, n_0, d_0)$ be the weight enumerator of $\mathcal{C}_0$. Then for sufficiently large N the following inequality holds

$$R \leq 1 - \frac{h_q(\delta/2)}{h_{q^{m_0}}\left[1 - (1-\delta/2)^{n_0} G\left(\frac{\delta/2}{(1-\delta/2)(q-1)}\right)\right]} + o(1),$$

where

$$h_Q(x) = -x \log_Q x - (1-x)\log_Q(1-x) + x \log_Q(Q-1).$$

is Q-ary entropy function.

Sketch of the proof

Consider all the possible vectors of length N, weight $W = \omega N$ over $\mathbb{F}_q$. We introduce an equiprobable distribution on such vectors. Let us consider the i-th check, by $\mathbf{S} = (\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_M)$ we denote the resulting syndrome of generalized LDPC code.

$$
\begin{aligned}
p_0 &= \Pr(\mathbf{S}_i = \mathbf{0}) \\
&= \frac{1}{\binom{N}{W}(q-1)^W} \left[\sum_{i=0}^{n_0} \left\{ A(i) \binom{N-n_0}{W-i} (q-1)^{W-i} \right\} \right].
\end{aligned}
$$

Sketch of the proof

Consider all the possible vectors of length N, weight $W = \omega N$ over $\mathbb{F}_q$. We introduce an equiprobable distribution on such vectors. Let us consider the i-th check, by $\mathbf{S} = (\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_M)$ we denote the resulting syndrome of generalized LDPC code.

$$
\begin{aligned}
p_0 &= \Pr(\mathbf{S}_i = \mathbf{0}) \\
&= \frac{1}{\binom{N}{W}(q-1)^W} \left[\sum_{i=0}^{n_0} \left\{ A(i) \binom{N-n_0}{W-i} (q-1)^{W-i} \right\} \right].
\end{aligned}
$$

In what follows we are interesting in asymptotic estimate when $N \to \infty$. In this case we have

$$
\begin{aligned}
p_0 &= \left[\sum_{i=0}^{n_0} \left\{ A(i) \omega^i (1-\omega)^{n_0-i} (q-1)^{-i} \right\} \right] + o(1) \\
&= (1-\omega)^{n_0} G\left(\frac{\omega}{(1-\omega)(q-1)}, n_0, d_0 \right) + o(1).
\end{aligned}
$$

Sketch of the proof

Let $H(X)$ be the *binary* entropy of the random variable X,

By the log-sum inequality.

$$\begin{aligned} H(\mathbf{S}_i) &= -\sum_{j=0}^{q^{m_0}-1} \Pr(\mathbf{S}_i = j) \log_2 \Pr(\mathbf{S}_i = j) \\ &\leq -p_0 \log_2 p_0 - (1-p_0) \log_2 \frac{1-p_0}{q^{m_0}-1} \\ &= h_{q^{m_0}}(1-p_0) \log_2 q^{m_0}. \end{aligned}$$

Sketch of the proof

For $\omega < \delta/2$

$$\frac{1}{N} H(\mathbf{S}) = h_q(\omega) \log_2 q + o(1),$$

as all the syndromes corresponding to such vectors are different.

$$H(\mathbf{S}) \leq \sum_{i=1}^{M} H(\mathbf{S}_i) = M h_{q^{m_0}}(1 - p_0) \log_2 q^{m_0}.$$

Notation

The constituent code in this case is a single parity-check (SPC) code over $\mathbb{F}_q$. Thus the enumerator of an SPC code over $\mathbb{F}_q$ is as follows

$$G(s, d_0 = 2, n_0) = \frac{1}{q}(1 + (q-1)s)^{n_0} + \frac{q-1}{q}(1-s)^{n_0}.$$

To formulate a theorem we need a notion of row degree polynomial

$$\rho(x) = \sum_{i=r_{\min}}^{r_{\max}} \rho_i x^i,$$

where ρ_i is a fraction of rows of the parity check matrix of weight i, $r_{\min}$ and $r_{\max}$ are the minimal and maximal row weights accordingly.

Upper bound for irregular LDPC codes

Theorem

Let $\mathcal{C}$ be an LDPC code of length N, rate R, minimum distance δN, with row degree polynomial $\rho(x)$. Then for sufficiently large N the following inequality holds

$$R \leq \overline{R}(q, \rho(x)) = 1 - \frac{h_q(\delta/2)}{h_q\left[\frac{q-1}{q}\left(1 - \rho\left(1 - \frac{q}{q-1}\delta/2\right)\right)\right]} + o(1).$$

Proof

$$
\begin{aligned}
&\frac{1}{\log_2 q}\sum_{i=1}^{M} H(\mathbf{S}_i)\\
&= (1-R)\sum_{i=r_{\min}}^{r_{\max}} \rho_i h_q\left[1-(1-\omega)^{n_0} G\left(\frac{\omega}{(1-\omega)(q-1)}\right)\right]\\
&= (1-R)\sum_{i=r_{\min}}^{r_{\max}} \rho_i h_q\left[\frac{q-1}{q}-\frac{q-1}{q}\left(1-\frac{q}{q-1}\omega\right)^i\right]\\
&\le (1-R)h_q\left[\frac{q-1}{q}-\frac{q-1}{q}\rho\left(1-\frac{q}{q-1}\omega\right)\right].
\end{aligned}
$$

Analysis

Proposition

Let $\ell > 0$ be an integer, let $\rho(x)$ be the row degree distribution of irregular code, such that $\sum_{i=r_{\min}}^{r_{\max}} i\rho_i = \ell$ and let $\rho_{reg} = x^\ell$, then

$$\overline{R}(q, \rho(x)) \leq \overline{R}(q, \rho_{reg}(x)).$$

Numerical results for $q = 8$

As an example we choose regular $(\ell = 3, n_0)$ LDPC codes. We see that at very high rates $(R > 0.994)$ the bound lies below the Varshamov–Gilbert bound. We note that the interval of rates in which we observe this behavior is decreasing when q grows. For $q = 2$ the interval is $R > 0.985$, for $q = 16$ the interval is $R > 0.997$.

(ℓ, n_0); R	(3,10); 0.7	(3,50); 0.94	(3,100); 0.97	(3,200); 0.985	(3,500); 0.994	(3,600); 0.995
VG	0.1260	0.0179	0.0080	0.0036	**0.0013**	**0.0011**
New	0.2282	0.0263	0.0106	0.0043	**0.0013**	**0.0010**
PL	0.2625	0.0525	0.0262	0.0131	0.0052	0.0044
BE	0.2338	0.0355	0.0160	0.0073	0.0026	0.0021
MRRW	0.2494	0.0545	0.0281	0.0144	0.0059	0.0050

Thank you for the attention!