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

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 $C_0$ 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 $H_0$. 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 $C_0$, 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 $C_0$. 
To check if $\mathbf{v} = (v_1, v_2, \ldots, v_N) \in \mathbb{F}_q^N$ is a codeword of $C$ we associate the symbols of $\mathbf{v}$ to the variable nodes. The word $\mathbf{v}$ is called a codeword of $C$ if all the constituent codes are satisfied.
Upper bound for generalized LDPC codes

Theorem

Let $C$ be a generalized LDPC code of length $N$, rate $R$, minimum distance $\delta N$, with constituent $[n_0, R_0, d_0]$ code $C_0$ over $\mathbb{F}_q$. Let $G(s, n_0, d_0)$ be the weight enumerator of $C_0$. 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 $\mathbf{S} = (S_1, S_2, \ldots, S_M)$ we denote the resulting syndrome of generalized LDPC code.

$$p_0 = \Pr(S_i = 0) = \frac{1}{\binom{N}{W}(q-1)^W} \left[ \sum_{i=0}^{n_0} \left\{ A(i) \binom{N-n_0}{W-i} (q-1)^{W-i} \right\} \right].$$
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 $S = (S_1, S_2, \ldots, S_M)$ we denote the resulting syndrome of generalized LDPC code.

$$p_0 = \Pr(S_i = 0) = \frac{1}{\binom{N}{W}(q-1)^W} \left[ \sum_{i=0}^{n_0} \left\{ A(i) \left( \frac{N-n_0}{W-i} \right)(q-1)^{W-i} \right\} \right].$$

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

$$p_0 = \left[ \sum_{i=0}^{n_0} \left\{ A(i)\omega^i(1-\omega)^{n_0-i}(q-1)^{-i} \right\} \right] + o(1)$$

$$= (1-\omega)^{n_0} G \left( \frac{\omega}{(1-\omega)(q-1)}, n_0, d_0 \right) + o(1).$$
Let $H(X)$ be the \textit{binary} entropy of the random variable $X$,

By the log-sum inequality.

$$H(S_i) = - \sum_{j=0}^{q^{m_0}-1} \Pr(S_i = j) \log_2 \Pr(S_i = j)$$

$$\leq -p_0 \log_2 p_0 - (1 - p_0) \log_2 \frac{1 - p_0}{q^{m_0} - 1}$$

$$= h_{q^{m_0}} (1 - p_0) \log_2 q^{m_0}.$$
Sketch of the proof

For $\omega < \delta/2$

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

as all the syndromes corresponding to such vectors are different.

$$H(S) \leq \sum_{i=1}^{M} H(S_i) = M h_{q^m_0} (1 - p_0) \log_2 q^{m_0}.$$
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 $\rho_i$ 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 $\delta N$, 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

\[ \frac{1}{\log_2 q} \sum_{i=1}^{M} H(S_i) \]

\[ = (1 - R) \sum_{i=r_{\min}}^{r_{\max}} \rho_i h_q \left[ 1 - (1 - \omega)^{n_0} G \left( \frac{\omega}{(1 - \omega)(q - 1)} \right) \right] \]

\[ = (1 - R) \sum_{i=r_{\min}}^{r_{\max}} \rho_i h_q \left[ \frac{q - 1}{q} - \frac{q - 1}{q} \left( 1 - \frac{q}{q - 1} \omega \right)^i \right] \]

\[ \leq (1 - R) h_q \left[ \frac{q - 1}{q} - \frac{q - 1}{q} \rho \left( 1 - \frac{q}{q - 1} \omega \right) \right]. \]
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 \( \rho_{\text{reg}} = x^\ell \), then

\[
\overline{R}(q, \rho(x)) \leq \overline{R}(q, \rho_{\text{reg}}(x)).
\]
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 \(R > 0.997\).

<table>
<thead>
<tr>
<th>((\ell, n_0); R)</th>
<th>(3,10); 0.7</th>
<th>(3,50); 0.94</th>
<th>(3,100); 0.97</th>
<th>(3,200); 0.985</th>
<th>(3,500); 0.994</th>
<th>(3,600); 0.995</th>
</tr>
</thead>
<tbody>
<tr>
<td>VG</td>
<td>0.1260</td>
<td>0.0179</td>
<td>0.0080</td>
<td>0.0036</td>
<td><strong>0.0013</strong></td>
<td><strong>0.0011</strong></td>
</tr>
<tr>
<td>New</td>
<td>0.2282</td>
<td>0.0263</td>
<td>0.0106</td>
<td>0.0043</td>
<td><strong>0.0013</strong></td>
<td><strong>0.0010</strong></td>
</tr>
<tr>
<td>PL</td>
<td>0.2625</td>
<td>0.0525</td>
<td>0.0262</td>
<td>0.0131</td>
<td>0.0052</td>
<td>0.0044</td>
</tr>
<tr>
<td>BE</td>
<td>0.2338</td>
<td>0.0355</td>
<td>0.0160</td>
<td>0.0073</td>
<td>0.0026</td>
<td>0.0021</td>
</tr>
<tr>
<td>MRRW</td>
<td>0.2494</td>
<td>0.0545</td>
<td>0.0281</td>
<td>0.0144</td>
<td>0.0059</td>
<td>0.0050</td>
</tr>
</tbody>
</table>
Thank you for the attention!