Lecture 12

Lecture date: Oct 10 | *Scribe: Elchanan Mossel*

In the previous lecture we saw how to express the function $\varphi(\rho)$ which is the normalized log of the expected number of code words with relative weight ρ. This was given by the formula:

$$\varphi(\rho) = \sup_{\xi \in \{0,1\}} \inf_{\substack{x \geq 0 \\ y \geq 0 \\ z \geq 0}} \left\{ -\Lambda'(1) H(\xi) - \rho \log x - \Lambda'(1) \xi \log(yz) + \sum_{l=2}^{l_{\max}} \Lambda_l \log(1 + xy^l) + \frac{\Lambda'(1)}{P'(1)} \sum_{k=2}^{k_{\max}} P_k \log q_k(z) \right\}$$

$$= -\rho \log x - \Lambda'(1) \log(1 + yz) + \sum_{l=1}^{l_{\max}} \Lambda_l (1 + xy^l) + \frac{\Lambda'(1)}{P'(1)} \sum_{k=2}^{k_{\max}} P_k \log q_k(z),$$

where

$$\rho = \sum_{l=1}^{l_{\max}} \Lambda_l \frac{xy^l}{1 + xy^l} \qquad y = \frac{\sum_{k=2}^{k_{\max}} \rho_k P_k^-(z)}{\sum_{k=2}^{k_{\max}} \rho_k P_k^+(z)}$$

$$z = \frac{\sum_{l=1}^{l_{\max}} \lambda_l x y^{l-1}/(1 + xy^l)}{\sum_{l=1}^{l_{\max}} \lambda_l/(1 + xy^l)} \qquad P_k^{\pm}(z) = \frac{(1+z)^{k-1} \pm (1-z)^{k-1}}{(1+z)^k + (1-z)^k}.$$

In this lecture we will use the formula above to obtain short-distance properties of LDPC codes. If there are no code words of weight greater than δn then for each pattern of up to $\delta n/2$ errors we can recover the transmitted codeword correctly. This also implies that if errors are introduced independently on each coordinate with probability $\delta' < \delta/2$ then w.h.p. the correct transmitted word can be recovered.

In order to derive short distance properties we will apply the formula above when

$$\rho \to 0,$$

Looking at the equation for ρ we see that $\rho \to 0$ implies that either $x \to 0$ or $y \to 0$. From the equation for y we see that $y \to 0$ implies $z \to 0$. On the other hand $x \to 0$ implies that $z \to 0$ by the equation for z and $z \to 0$ implies $y \to 0$ by the equation for y. We thus conclude:

Corollary 1 *When $\rho \to 0$ we have $y \to 0$ and $z \to 0$ and therefore*

$$y \sim \frac{\sum_{k=2}^{k(\max)} \rho_k (k-1) z}{\sum_{k=2}^{k(\max)} \rho_k} = \rho'(1) z.$$

$$z \sim \frac{\lambda_{\ell(\min)} x y^{\ell(\min)-1}}{\sum \lambda_\ell} = \lambda_{\ell(\min)} x y^{\ell(\min)-1},$$

and

$$\rho \sim \Lambda_{\ell(\min)} x y^{\ell(\min)-1}.$$

From the corollary, it is clear that the short distance properties depend very strongly on the minimal possible variable degree. We will discuss the three cases: $\ell(\min) = 1, \ell(\min) = 2$ and $\ell(\min) \geq 3$.

$\ell(\min) = 1$. In this case we obtain:

$$y \sim \rho'(z), \quad z \sim \lambda_1 x, \quad \rho \sim \Lambda_1 xy$$

and therefore

Corollary 2

$$\varphi(\rho) = -\frac{1}{2}\rho \log \rho + O(\rho)$$

and therefore for each ρ the expected number of code words of weight ρ is exponential in n.

In fact one can obtain the fact that in the case $\ell(\min) = 1$ there are many codewords of small weight also with high-probability observing that

Claim 3 *If $\ell(\min) = 1$ then w.h.p. every codeword has $\Omega(N)$ code-words at distance 2 from it.*

The proof of the claim follows by observing that w.h.p there is a linear fraction of factor nodes connected to variable nodes of degree 1 only.

$\ell(\min) = 2$

Claim 4 *If $\ell(\min) = 2$ then $\varphi(\rho) \sim A\rho$ where*

$$A = \log \frac{P''(1) 2\Lambda_2}{P'(1)\Lambda'(1)}$$

The proof of this claim is left as an exercise (1 point)

$\ell(\min) = 3$

Claim 5 *If $\ell(\min) = 3$ then*

$$\varphi(\rho) \sim \frac{\ell(\min) - 2}{2} \rho \log(\rho/\Lambda_{\ell(\min)}).$$

The proof of this claim is left as an exercise (1 point).

Small linear distances and sub-linear distances Using the previous two claims and a first moment argument we obtain:

Corollary 6 *Consider LDPC with $\ell(\min) \geq 3$ or $\ell(\min) = 2$ and $A < 0$. Let ρ^* be the first non-trivial zero of φ. Then for any open interval $(\rho_1, \rho_2) \subset [0, \rho^*]$ it holds that w.h.p there are no code words with weight in the interval $N(\rho_1, \rho_2)$.*

Remark 7 *Note that the claim above does not exclude the case of codewords of sub-linear weight. In fact,*

- *When $\ell(\min) = 2$ a small (but positive) number of code-words of sub-linear weight exists with high probability.*
- *When $\ell(\min) \geq 3$ w.h.p. there are no code-words of sub-linear weight. The proof of this fact is similar to expansion proofs we will see later.*

0.1 Rate of LDPC codes

Recall that the *rate* of a linear code $C \subset F_2^n$ is given by $\log ||C|/\log n$. We have seen that for any code with degree distribution Λ', P' it holds that the rate R of the code satisfies:

$$R \geq 1 - \frac{\Lambda'(1)}{P'(1)}.$$

We will now see that generally for LDPC codes, it holds that the rate is indeed given w.h.p by

$$R = 1 - \frac{\Lambda'(1)}{P'(1)}.$$

One way to find an upper bound on the rate is to upper bound the maximum value of $\varphi(\rho)$. It is natural to expect that the maximum is obtained at $\rho = 1/2$.

Exercise 8 *Find conditions on the degree distributions implying that the maximum of φ is obtained at $\rho = 1/2$.*

Claim 9 *Suppose that the maximum of φ is obtained at $\rho = 1/2$ and that $\delta > 0$ the w.h.p. it holds that*

$$\mathbb{R} \leq 1 - \frac{\Lambda'(1)}{P'(1)} + \delta.$$

Proof: Using a first moment argument it suffices to show that

$$\varphi(1/2) \leq \log(2)\left(1 - \frac{\Lambda'(1)}{P'(1)}\right).$$

Next one verifies that $\rho = 1/2$ correspond to $x = y = z = 1$ in the formula for φ. Plugging this into the formula then gives:

$$\varphi(1/2) = \log(2)\left(1 - \frac{\Lambda'(1)}{P'(1)}\right).$$

$\square$