Performance Bounds for Regular LDPC Codes for Asymmetric Channels

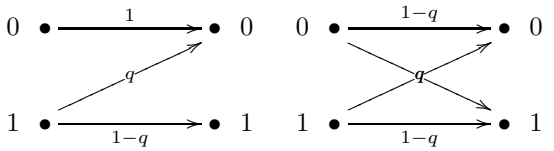
Pål Ellingsen
Department of Computing, Mathematics and Physics
Bergen University College
Bergen, Norway
Email: pal.ellingsen@hib.no

***Abstract*—It is well known that it is not possible to achieve capacity on an asymmetric channel using an even input distribution. In recent literature, complex code constructions has been proposed that gives rise to uneven input distributions to the channel such that capacity in theory can be achieved. However, it is of interest to know how well we can do on these channels with ordinary, linear codes due to the other desirable properties of such codes. In this paper, density evolution for symbol dependent channels is used in combination with a classical theorem by Gallager to bound the performance of regular Low Density Parity Check (LDPC) codes by showing that the check node degree of the graph describing a regular LDPC code, must go to infinity if the code is to achieve capacity on the Z-channel. Based on this, performance bounds for different check node degrees are calculated, and it is also shown that this is only a problem for small error probabilities.**

Keywords–Asymmetric channel; Regular LDPC codes; Gallager's theorem

I. INTRODUCTION

A binary asymmetric channel is a class of channels in which the probability of symbol error depends on the input symbol. In this paper, we will study a particular instance of this class, namely the binary asymmetric channel where the error probabilities of the two input values 0 and 1 are set to 0 and q as shown in Figure 1(a). This channel is also called the the Z-channel.



(a) The Z-channel (b) The binary symmetric channel

Figure 1. Channel models

Since the transition probabilities of the Z-channel are non-equal, the capacity not only depends on the probability of bit errors on the channel, but also on the input bit probability to the channel. Binary asymmetric channels have received considerable attention in classical coding theory, and many important works on this topic were compiled by Kløve in [1]. Since the introduction of iterative decoding, the coding community has succeeded in making codes that approach the Shannon bound on symmetric channels; meanwhile the relative performance of the best known codes for asymmetric channels has fallen behind. The cause for this has probably been the fact that due to their symbol dependent nature, asymmetric channels can not be analyzed using the techniques available for symmetric channels like density evolution in its original form. Further, the optimum input distribution actually depends on the error probability of the channel so it is impossible to achieve capacity on an asymmetric channel using a code with an even input probability. Since all linear codes have an even input distribution to the channel, capacity can not be achieved using a linear code, further complicating the task of approaching capacity on asymmetric channels. In this paper, new performance bounds for such codes are found by using a theorem by Gallager regarding the check node degree distribution of LDPC codes on the binary symmetric channel, and showing a similar result for the Z-channel. A necessary property of regular LDPC codes that are to approach the Shannon bound for all values of the error probability q is also proved.

In the rest of this paper, some background material on LDPC codes is first presented in Section II, then the development of the performance bound is given in Section III. Results are analyzed in Section IV, and finally, conclusions and possible future work are given in Section V and Section VI.

II. BACKGROUND

LDPC codes is a class of codes that uses belief propagation to attain near-capacity decoding. The codes are sparse linear block codes that may be pseudorandom or result of an explicit construction. The code may be represented as a bipartite graph construction called a Tanner graph (see Figure 2) where the parity checks of are represented by $\boxplus$ and the variable nodes are represented by $\bigcirc$. The decoding can be viewed as message passing on the same graph. Initially each variable nodes send messages to its parity check nodes indicating the probability of it being a $+1$ versus a -1. The check nodes returns the probabilities from all its neighbors, except from the node itself. The subsequent iterations proceeds analogously, except for that the information passed form the variable nodes is based on both the channel values and the information received in the previous iteration.

Recently there has been some interest in the use of LDPC codes for asymmetric channels. In [2] the use of LDPC codes on the some types of binary input fading multiple access channels (MAC) without channel state information (CSI) is investigated, while in [3], new code constructions are developed

 ISBN: 978-1-61208-455-8

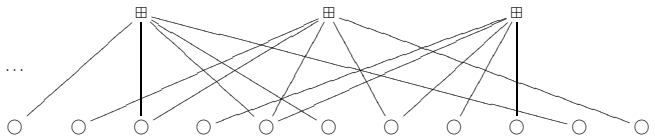


Figure 2. Tanner graph

based on transforming LDPC codes designed for the Binary Symmetric Channel (BSC) to bias the input distribution to the channel. Lately Mondelli, Marco and Urbanke [4] studies three different techniques designing concatenated codes with optimum input distribution for binary asymmetric channels. However, the bounds on performance of ordinary, regular LDPC codes are also of great interest as these codes are well known and widely used.

III. Performance bounds

In his seminal paper "Low-Density Parity-Check Codes", Gallager [5] proved the following theorem which shows that decoding error probability for the binary symmetric channel is bounded away from 0 for all codes of rates above a threshold that depends on the check node degree d of the graph describing the code. We prove that there exists a similar bound for the Z-channel when considering regular, linear codes, and state as a corollary that as a consequence, the check node degree must go to infinity to achieve linear capacity for all values of q.

Theorem 1 (Gallager)**.** Let a regular parity check code of length n and rate r with check node degree d be used on a BSC with crossover probability q and let the codewords be used with equal probability. Let

$$q_d = \frac{1+(1-2q)^d}{2}. \tag{1}$$

Then

$$r > \frac{h(q_d)-h(q)}{h(q_d)}, \tag{2}$$

where $h(\cdot)$ is the binary entropy function, implies that for a fixed d the probability of decoding error is bounded away from 0 by an amount independent of n.

Proof: See [5]. ∎

With certain adaptations, Gallager's theorem is also true for the Z-channel.

Theorem 2. Let a linear, regular LDPC code of rate r and length n with check node degree d be used on a Z-channel with error probability q and assume the codewords are equiprobable. If

$$q_d = \frac{1+(1-2q)^{d/2}}{2} \tag{3}$$

and

$$r > \frac{2h(q_d)-h(q)}{2h(q_d)}, \tag{4}$$

where $h(\cdot)$ is the binary entropy function, then the probability of decoding error is bounded away from 0 by an amount independent of n.

Proof: We will follow Gallager's proof of Theorem 1 closely in the following. Let u be a transmitted codeword, and let v be the received sequence. If we consider u and v as instances of the variables U and V, the mutual information between two variables U and V is given by

$$I(U;V) = h(U) - h(U|V) = \\ -\sum_u p(u)\log(p(u)) + \sum_{u,v} p(u,v)\log(p(u|v)) \tag{5}$$

For simplicity, we will write $\sum_u p(u)\log(p(u)) = \overline{\log(p(u))}$ and $\sum_{u,v} p(u,v)\log(p(u|v)) = \overline{\log(p(u|v))}$. Then, the average mutual information per bit in a codeword can be written

$$\frac{1}{n}I(u,v) = -\frac{1}{n}\overline{\log(p(u))} + \frac{1}{n}\overline{\log(p(u|v))} \tag{6}$$

or, by the symmetry of the mutual information function

$$\frac{1}{n}I(u,v) = -\frac{1}{n}\overline{\log(p(v))} + \frac{1}{n}\overline{\log(p(v|u))} \tag{7}$$

The probability of decoding error is bounded away from 0 if there exists an ϵ independent of n for which the conditional probability $p(u|v)$ satisfies

$$\frac{1}{n}\overline{\log(p(u|v))} \geq \epsilon > 0 \tag{8}$$

We will proceed to prove the existence of such an ϵ by expanding the terms of equation (6).

The code has nr message bits, and thus there are 2^{nr} messages in the code, so assuming the codewords are equiprobable

$$-\frac{1}{n}\overline{\log(p(u))} = -\frac{1}{n}\sum_u p(u)\log(p(u)) \tag{9}$$

$$= -\frac{1}{n}\sum_u 2^{-nr}\log(2^{-nr}) \tag{10}$$

$$= -\frac{1}{n}2^{nr}\cdot 2^{-nr}\cdot(-nr) \tag{11}$$

$$= r$$

For a linear code, the average weight of a codeword is $n/2$, and since each 1-digit in the sequence u has probability q of being different from the corresponding digit in v, the average conditional probability $p(v|u)$ is $q^{qn/2}(1-q)^{(1-q)n/2}$. Then, we can write

$$\frac{1}{n}\overline{\log(p(v|u))} = \frac{1}{n}\log(q^{qn/2}(1-q)^{(1-q)n/2}) \tag{12}$$

$$= \frac{1}{n}\cdot\frac{n}{2}(q\log(q)+(1-q)\log(1-q))$$

$$= -\frac{h(q)}{2} \tag{13}$$

If we average over all parity checks, the weight of the nodes involved in each parity check should be $d/2$. Now, the probability that a parity check is satisfied is the probability that an even number of errors have occurred in the $d/2$ 1-nodes that belongs to the parity check. If we sum over all even-number error events we get the probability q_d that a parity sums to 0.

$$q_d = \sum_{i \text{ even}} \binom{d/2}{i} q^i (1-q)^{d/2-i} \tag{14}$$

$$= \frac{1+(1-2q)^{d/2}}{2} \tag{15}$$

To verify (14), rewrite the right hand side as

$$\frac{(1-q+q)^{d/2}+(1-q-q)^{d/2}}{2} \tag{16}$$

and expand it as a binomial series.

A received word v can be described by the parities of the $n(1-r)$ parity checks together with the received values in some set of nr linearly independent variable nodes. The entropy of a received word is $h(v) = \overline{-\log(p(v))}$ and the entropy of a parity check is $h(q_d)$. Then, since the entropy of a variable node is at most 1 bit and dependencies only can reduce the overall entropy, we have

$$-\frac{1}{n}\overline{\log(p(v))} \leq (1-r)h(q_d) + r \tag{17}$$

If we substitute (9), (12) and (17) into (6) we get

$$\frac{1}{n}\overline{\log(p(u|v))} \geq \frac{h(q)}{2} - (1-r)h(q_d) \tag{18}$$

By hypothesis, there is an $\epsilon > 0$ that satisfies

$$r = \frac{2h(q_d) - h(q) + \epsilon}{2h(q_d)} \tag{19}$$

Substituting for (19) in (18) we get

$$\frac{1}{n}\overline{\log(p(u|v))} \quad \geq \quad \epsilon \tag{20}$$

■

Based on this theorem, we can formulate the following corollary.

Corollary 1. Let $C_{\frac{1}{2}}(q)$ be the maximum achievable rate for error free decoding of a linear code on a Z-channel with error probability q. Given the prerequisites of Theorem 2, a necessary condition for an LDPC code to achieve $C_{\frac{1}{2}}(q)$ for all values of q is that d must go to ∞.

Proof: The capacity of the Z-channel is

$$\max_p(h(p(1-q)) - ph(q)) \tag{21}$$

where p is the input distribution and q is the error probability. Since we restrict ourselves to using linear codes, the highest achievable rate of the channel is

$$C_{\frac{1}{2}}(q) \quad = \quad h(\frac{1}{2}(1-q)) - \frac{1}{2}h(q) \tag{22}$$

$$= \quad 1 - \frac{1}{2}((1+q)\log(1+q) - q\log q) \tag{23}$$

For computational convenience we will use the form

$$1 - \frac{h(q)}{2h(q_d)} \tag{24}$$

instead of the original form of the bound in (4).

Assume d is finite.

Let q^* be the value of q for which

$$C_{\frac{1}{2}}(q) = 1 - \frac{h(q)}{2h(q_d)}. \tag{25}$$

By the monotonicity of the log function there is a unique q^*. When $q = \frac{1}{2}$, $q_d = \frac{1}{2}$ for all values of d so $1 - \frac{h(q)}{2h(q_d)} = \frac{1}{2}$, and also $C_{\frac{1}{2}}(\frac{1}{2}) = h(\frac{1}{4}) - \frac{1}{2}$. Consequently, when $q = \frac{1}{2}$

$$C_{\frac{1}{2}}(q) < 1 - \frac{h(q)}{2h(q_d)} \tag{26}$$

for all values of d.

Further, $h(q_d) = 0$ for $q = 0$ since $q_d(0) = 1$ so $1 - \frac{h(q)}{2h(q_d)}$ is not defined for $q = 0$. We can, however, find an expression for $1 - \frac{h(q)}{2h(q_d)}$ as $q \to 0$ by taking the limit

$$\lim_{q\to 0} 1 - \frac{h(q)}{2h(q_d)}, \tag{27}$$

Initially, we can simplify (27) to

$$\lim_{q\to 0} 1 - \frac{h(q)}{2h(q_d)} \quad = \quad 1 - \frac{1}{2}\lim_{q\to 0}\frac{h(q)}{h(q_d)} \tag{28}$$

Let $d' = \frac{d}{2}$. Then

$$\lim_{q\to 0}\frac{h(q)}{h(q_d)} \qquad = \qquad \lim_{q\to 0}\frac{q\log q}{\frac{1-(1-2q)^{d'}}{2}\log\frac{1-(1-2q)^{d'}}{2}} \tag{29}$$

Since both numerator and denominator in (29) go to 0 when q goes to 0, we can apply L'Hopital's rule so that

$$\lim_{q\to 0}\frac{q\log q}{\frac{1-(1-2q)^{d'}}{2}\log\frac{1-(1-2q)^{d'}}{2}}$$

$$= \lim_{q\to 0}\frac{1+\frac{\log e}{\log q}}{\frac{d'(1-2q)^{d'-1}}{2}\left(2\log\frac{1-(1-2q)^{d'}}{2} + \log e\right)\frac{1}{\log q}} \tag{30}$$

We calculate the limit of the denominator in (30) separately by applying L'Hopital's rule repeatedly:

$$\lim_{q\to 0}\left(2\log\frac{1-(1-2q)^{d'}}{2} + \log e\right)\frac{1}{\log q} \tag{31}$$

$$= \lim_{q\to 0}\frac{2\log\frac{1-(1-2q)^{d'}}{2}}{\log q} + \frac{\log e}{\log q} \tag{32}$$

$$= \lim_{q\to 0}\frac{2\log\frac{1-(1-2q)^{d'}}{2}}{\log q}$$

$$= \lim_{q\to 0}\frac{2\cdot 2d'(1-2q)^{d'}\frac{\log e}{1-(1-2q)^{d'}}}{\frac{\log e}{q}} \tag{33}$$

$$= \lim_{q\to 0}\frac{4qd'(1-2q)^{d'}}{1-(1-2q)^{d'}} \tag{34}$$

Applying L'Hopital's rule to (34) yields

$$\lim_{q\to 0}\frac{4qd'(1-2q)^{d'}}{1-(1-2q)^{d'}} \tag{35}$$

$$= \lim_{q\to 0}\frac{4d'(1-2q)^{d'} - 8q(d'^2-d')(1-2q)^{d'-2}}{2d'(1-2q)^{d'-1}} \tag{36}$$

$$= \lim_{q\to 0}\frac{2d'(1-2q)^{d'}}{d'(1-2q)^{d'-1}} \tag{37}$$

$$= 2 \tag{38}$$

Substituting (38) into (30) gives us

$$\lim_{q\to 0} \frac{1+\frac{\log e}{\log q}}{\frac{d'(1-2q)^{d'-1}}{2}\left(2\log\frac{1-(1-2q)^{d'}}{2}+\log e\right)\frac{1}{\log q}} = \lim_{q\to 0}\frac{1}{d'(1-2q)^{d'-1}} = \frac{1}{d'} \quad (39)$$

Finally, substituting (39) into (28) and setting $d' = \frac{d}{2}$ again we get

$$\lim_{q\to 0} 1-\frac{h(q)}{2h(q_d)} = 1-\frac{1}{d} \quad (40)$$

Now, since we assume d is finite, (26) and (27) imply that $0 < q^* < \frac{1}{2}$ so there exists some interval $\langle 0, q^*\rangle$ for which $1-\frac{h(q)}{2h(q_d)} < C_{\frac{1}{2}}(q)$ making it impossible to achieve $C_{\frac{1}{2}}(q)$ for those values of q.

Assume $d \to \infty$.
Since $(1-2q) \in \langle -1, 1\rangle$ for $q \in \langle 0, 1\rangle$ we see that

$$\lim_{d\to\infty} q_d = \lim_{d\to\infty}\frac{1+(1-2q)^{d/2}}{2} \quad (41)$$

$$= \frac{1}{2} \quad (42)$$

for all $q \in \langle 0, 1\rangle$, and so

$$\forall q \in \langle 0,1\rangle \lim_{d\to\infty} h(q_d) = 1 \quad (43)$$

Thus, under these conditions, the limit of (24) when d goes to infinity becomes

$$\lim_{d\to\infty} 1-\frac{h(q)}{2h(q_d)} = 1-\frac{h(q)}{2} \quad (44)$$

We want to know when

$$C_{\frac{1}{2}}(q) < 1-\frac{h(q)}{2h(q_d)}. \quad (45)$$

Using (21) this expands to

$$h(\frac{1}{2}(1-q)) - \frac{1}{2}h(q) < 1-\frac{h(q)}{2h(q_d)} \quad (46)$$

When $d \to \infty$, we can substitute (44) into (46), and the inequality becomes

$$h(\frac{1}{2}(1-q)) - \frac{h(q)}{2} < 1-\frac{h(q)}{2} \quad (47)$$

This reduces to

$$h(\frac{1}{2}(1-q)) < 1 \quad (48)$$

From the properties of the entropy function of a binary variable we can deduce that this is true for all values of $q \in \langle 0, 1\rangle$. Further, from (40) we get

$$\lim_{d\to\infty}\lim_{q\to 0} 1-\frac{h(q)}{2h(q_d)} = 1 \quad (49)$$

Thus $1-\frac{h(q)}{2h(q_d)}$ goes to 1 when q goes to 0. Further, since the entropy function $h(q)$ is symmetric about the line $q = \frac{1}{2}$, the function $1-\frac{h(q)}{2h(q_d)}$ is also symmetric about $q = \frac{1}{2}$ and therefore $1-\frac{h(q)}{2h(q_d)}$ also goes to 1 when q goes to 1.

We can conclude that $C_{\frac{1}{2}} \leq 1-\frac{h(q)}{2h(q_d)}$ for all $q \in [0,1]$ when $d \to \infty$. Ergo, for a code to achieve capacity for all q, d must go to ∞. ■

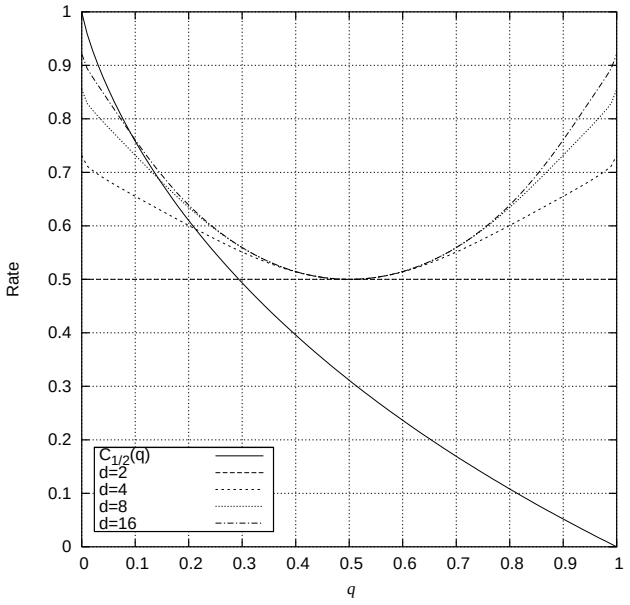


Figure 3. Comparison between $C_{\frac{1}{2}}(q)$ and the upper bound from (4) for different values of d.

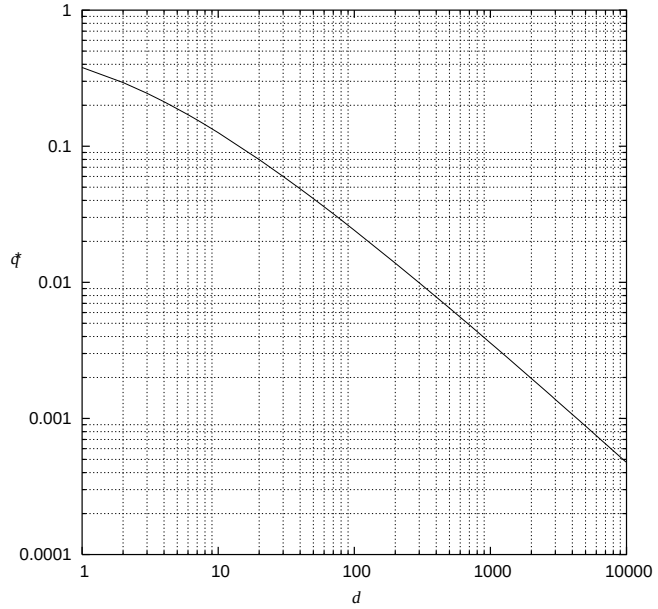


Figure 4. The intersection point q^* as a function of d

IV. Results and Discussion

As stated in Corollary 1: for finite d there will be some values of q for which $1 - h(q)/2h(q_d) > C$ so capacity cannot be achieved for all q. In a practical implementation, d will necessarily have to be finite, so the interesting question is how fast the intersection point q^* between $C_{\frac{1}{2}}(q)$ and $1-h(q)2h(q_d)$, illustrated in Figure 3 for different values of d, approaches 0 as d grows. It appears to be a hard problem to find an exact solution of the equation $C_{\frac{1}{2}}(q) = 1 - h(q)/2h(q_d)$, but numerical evaluation can give an indication of the rate at which q^* approaches 0. Results for d from 1 up to 10000 are given in Figure 4, and it is apparent that q^* decreases relatively slowly with increasing d.

V. Conclusion

Hence, building on Gallager's theorem, we have proved that the check node degree of the Tanner graph of an LDPC code imposes a lower bound on error free decoding also for the Z-channel. We have shown that this implies that capacity can not be achieved for all values of q for finite d, and that as d goes to infinity, the interval of q where error probability is bounded away from zero goes to 0. However, we see that this interval decreases only slowly, so a very high check node degree is a necessary condition to achieve $C_{\frac{1}{2}}$ for small values of q. Thus, these results tell us that the performance of regular LDPC codes on the Z-channel is bounded away from zero for small values of q, and that optimum performance is hard to achieve as q goes to 0. However, the theorem provides a bound on the performance of a regluar LDPC code for a given d.

VI. Future work

The results in this paper have been proved for regular LDPC codes. However, the class of irregular LDPC codes has so far proved to have the best performance, at least for symmetric channels. A natural step would therefore be to extend the above results to irregular codes as well.

References

[1] T. Kløve, Error Correcting Codes for the Asymmetric Channel. HiB, N-5020 Bergen, Norway: Department of Informatics, University of Bergen, 1995.

[2] N. Marina, "Ldpc codes for binary asymmetric channels," in Telecommunications, 2008. ICT 2008. International Conference on. IEEE, 2008, pp. 1–7.

[3] R. Gabrys and L. Dolecek, "Coding for the binary asymmetric channel," in Computing, Networking and Communications (ICNC), 2012 International Conference on. IEEE, 2012, pp. 461–465.

[4] M. Mondelli, R. Urbanke, and S. H. Hassani, "How to achieve the capacity of asymmetric channels," in Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on. IEEE, 2014, pp. 789–796.

[5] R. G. Gallager, "Low density parity check codes," IRE Trans. Information Theory, vol. 8, pp. 21–28, 1962.

[6] P. Ellingsen, "Iterative coding for the asymmetric channel," University of Bergen, Tech. Rep. 295, April 2005.

[7] C.-C. Wang, S. R. Kulkarni, and H. V. Poor, "Density evolution for asymmetric memoryless channels," in Proc. 3rd International Symposium on Turbo Codes, 2003.

 ISBN: 978-1-61208-455-8