Design of Irregular Graphs for Erasure Decoding*

***Abigail Mitchell*† *and Joachim Rosenthal*‡**

1 Introduction to LDPC Codes

Low-density parity check codes (LDPC codes) were introduced by Gallager [2] and have received intensive study in the last few years, as advances in technology have made their implementation far more practical than when they were originally proposed. Basically, an LDPC code is a binary linear block code defined by a sparse $m \times n$ parity-check matrix H. Equivalently such a code can be thought of as defined by a bipartite graph, called a Tanner graph, whose adjacency matrix is H. In this representation the n left vertices represent columns of H, corresponding to bits in the original message, and the m right vertices represent the rows of H, corresponding to parity check bits; an edge (i, j) exists in the graph whenever the corresponding entry $h_{i,j}$ in H is 1, i.e. whenever the message bit i participates in parity check j. Decoding of LDPC codes is then performed via an iterative algorithm operating on the Tanner graph. See the original paper [11] or the more recent work in [7] for the background on LDPC codes and more general codes on Tanner graphs.

In this paper we will consider a Tanner graph, parity check matrix and the LDPC code they define to be more or less interchangeable (despite the fact that any linear code can in fact have multiple Tanner graph presentations.) In the original work Gallager was working with bipartite graphs which were regular. This means there were positive integers λ, ρ such that every left vertex had degree λ and every right vertex had degree ρ. Such a code is referred to as (λ, ρ)-regular.

*This work was supported in part by a US NSF Graduate Research Fellowship and the Swiss National Science Foundation under Grant no. 113251.

†Institute of Mathematics, University of Zürich, Zürich, Switzerland

‡Institute of Mathematics, University of Zürich, Zürich, Switzerland

Gallager's work already showed that as the block length n increases, the performance of randomly selected (λ, ρ)-regular codes approaches a threshold near the channel capacity but cannot achieve capacity for the channels he was studying. In addition encoding complexity is in general quadratic in n, so approaching the threshold with codes of practical length is rather difficult.

Major progress in achieving capacity using LDPC codes and codes on graphs was made by Luby, Mitzenmacher, Shokrollahi, Spielmann and Stemann [6, 4, 5], who introduced a new class of codes which are encodable as well as decodable in linear time, while performing at rates extremely close to capacity. In their work they showed that for the erasure channel some random irregular graphs with specific degree sequences lead to LDPC codes approaching capacity on the binary erasure channel. Extension of this work can be found in [8, 9].

In this paper we briefly review their results. These papers pose the challenge to come up with explicit constructions of bipartite irregular graphs whose degree sequences match the degree distribution of capacity approaching ensembles. In this paper we explain a new way how to do this in an algebraic way which guarantees that the Tanner graph has no small cycles, something which is desirable if one wants to guarantee that the minimal pseudo-codeword is not too small. See [3, 10] for more details on pseudo-codewords. Related recent work can be found in [1, 12].

2 Irregular Tanner graphs and Capacity Achieving Sequences

Let n be an integer and β be a positive rational number such that βn is an integer as well. For B a bipartite graph with n left vertices and βn right vertices, let $C(B)$ be the code with B as Tanner graph. The n left vertices represent the bits. We can partition the bits into message bits and check bits dependent on the rank of the associated parity check matrix. Encoding is performed simply by setting each check bit to the binary sum of its neighbors, and is thus linear in the number of edges in B.

As a channel we assume the erasure channel. This means with a certain probability p the correct bit is received and with probability $1 - p$ the receiver has no knowledge if the bit was a one or a zero, i.e. an erasure has occurred. Decoding consists of, whenever a check node is identified such that all but one of its participating message bits are known, setting the missing message bit to the binary sum of the check bit and the known message bits. Thus, decoding is also linear in the number of edges.

The innovation of Luby et al. [6, 4, 5] was to cascade a sequence of such codes together: use $C(B_0)$ to produce βn check bits for the original n message bits, then a similar code $C(B_1)$ to produce $\beta^2 n$ check bits for the βn check bits of $C(B_0)$, and so on. Formally, one chooses a sequence of graphs $B_0, B_1, ..., B_m$ such that B_i has $\beta^i n$ left vertices and $\beta^{i+1} n$ right vertices. m is chosen so that $\beta^{m+1} n \approx \sqrt{n}$, the codes $C(B_0), C(B_1), ... C(B_m)$ are cascaded as described above, and the code is

terminated with a small conventional code C of block length $\beta^{m+1}n$ and rate $1-\beta$.

The result is a code $C(B_0, ..., B_m, C)$ with n message bits and $n\beta/(1-\beta)$ check bits, and thus rate $1-\beta$. Assuming the code C can be encoded and decoded in quadratic time, the overall encoding and decoding complexity are linear in n. Additionally, if the graphs B_i are constructed in such a way that each one corrects a $\beta(1-\epsilon)$ fraction of its bits with high probability, the result is a rate $1-\beta$ code which recovers up to a $\beta(1-\epsilon)$ fraction of erasure with high probability.

Such graphs can be obtained by taking random graphs with specific, highly irregular degree distributions. For a bipartite graph, define the *left* (resp. *right*) degree of an edge as the degree of the left (resp. right) node it is incident on. Let λ_i and ρ_i denote the fraction of edges with left (resp. right) degree i, and let $\lambda(x) := \sum_i \lambda_i x^{i-1}$ and $\rho(x) := \sum_i \rho_i x^{i-1}$. We refer to (λ, ρ) as a *degree distribution*.

If a random bipartite graph with degree distribution (λ, ρ) corrects erasures on a randomly located $(1-R)(1-\epsilon)$ fraction of nodes, we say that the degree distribution $\lambda, \rho)$ is *asymptotically optimal* if ϵ/R^{a_r} is bounded by some constant depending on R.

For integer $a \geq 2$ and parameter $\nu \in (0,1)$, let $\alpha := 1/(a-1)$ and $N := \lfloor \nu^{-1/\alpha} \rfloor$. The functions

$$\rho_a(x) := x^{a-1}$$

and

$$\lambda_{\alpha,N}(x) := \alpha \frac{\sum_{k=e}^{N-1} \binom{\alpha}{k} (-1)^{k+1} x^k}{\alpha - N\binom{\alpha}{N}(-1)^{N+1}}$$

form a degree distribution, called a *right-regular* distribution, with right degree a and maximum left degree N. Note that since N depends discretely on ν and a, only a finite number of rates are possible with a given a. However, Shokrollahi showed that appropriate pairs a_n, N can in general be found to approximate a desired rate R.

Theorem 1 (Theorem 3 in [8]) *Right-regular degree distributions are asymptotically optimal.*

3 Construction of Right-Regular Graphs

For a given average right degree a and maximum left degree N (thus rate R), if the desired number of right vertices n is such that $a|\frac{n}{1-R}$, we may construct a right-regular graph of girth at least 6 as follows.

Label the right vertices $1, 2, \ldots, n$, and let the $n/(1-R)$ left vertices be partitioned into a equal sets $V_1, \ldots, V_a$. In each set V_i attach a set of n 'half-edges' with degree distribution according to $\lambda_{\alpha,N}$ (where as above $\alpha = 1/(a-1)$.) Label the half-edges $1, 2, \ldots, n$ and consider the permutation $\pi(x) := c_i x$ for some $c_i \in \mathbb{Z}_n^*$. Let $B(c_1, c_2, \ldots, c_a)$ be the graph with edge set $(x, c_i x) | x \in V_i$.

Clearly any such graph B matches the right-regular degree sequence; it remains to show that the girth can be made at least 6, i.e. that cycles of length four

can be avoided.

Lemma 2 *Let a and N be positive integers and γ an integer with*

$$2aN < \gamma < \frac{n-1}{N-1} - a.$$

Then the equation

$$k_1(\gamma + i) \equiv k_2(\gamma + j) \mod (n-1)$$

has no solutions with $1 \leq i < j \leq a$ and $-N < k_1, k_2 < N$.

Proof. First, note that $k_1(\gamma+i) < n-1$ and $k_2(\gamma+j) < n-1$, so it suffices to show that $k_1(\gamma+i) = k_2(\gamma+j)$ has no integer solutions in the specified range; equivalently, that $\gamma(k_1 - k_2) = k_2 j - k_1 i$ has no solutions. Note that $|\gamma(k_1 - k_2)| \geq |\gamma| > 2aN$, and $|k_2 j - k_1 i| < 2aN$; this completes the proof. □

Theorem 3 *Let a, N, n be as above, with the additional requirement that n is prime. Then for any generator $g \in \mathbb{Z}_n^*$ and any integer γ such that*

$$2aN < \gamma < (n-1)/(N-1) - a,$$

the graph $B(g^{\gamma+1}, g^{\gamma+2}, \ldots, g^{\gamma+a})$ has girth at least 6.

Proof. Consider left vertices $u \in V_i$,$v \in V_j$, both adjacent to a right vertex q. (By construction we exclude the possibility $i = j$.) All other possible edges from u and v are of the form $qg^{(\gamma+i)k_1}$ and $qg^{(\gamma+j)k_2}$ respectively, with $-N < k_1, k_2 < N$; thus the necessary condition for a cycle of length four to exist is that $(\gamma+i)k_1 \equiv (\gamma+j)k_2$ mod $(n-1)$. By the lemma above, no solutions exist; thus, the graph has no 4-cycles and its girth is at least 6. □

Remark 4 If in the cascaded construction n turns out not to be a prime it is possible to take the next larger prime and the extra number of right vertices can then be removed in a final step.

Bibliography

[1] J. Chen, R. M. Tanner, J. Zhang, and M. P. C. Fossorier. Construction of irregular LDPC codes by quasi-cyclic extension. *IEEE Trans. Inform. Theory*, 53(4):1479–1483, 2007.

[2] R.G. Gallager. *Low-Density Parity Check Codes*. M.I.T. Press, Cambridge, MA, 1963. Number 21 in Research monograph series.

[3] C. A. Kelley, D. Sridhara, and J. Rosenthal. Tree-based construction of LDPC codes having good pseudocodeword weights. *IEEE Trans. Inform. Theory*, 53(4):1460–1478, 2007.

[4] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Efficient erasure correcting codes. *IEEE Trans. Inform. Theory*, 47(2):569–584, 2001.

[5] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Improved low-density parity-check codes using irregular graphs. *IEEE Trans. Inform. Theory*, 47(2):585–598, 2001.

[6] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, and V. Stemann. Practical loss-resilient codes. In *Proc. 29th Annu. ACM Symp. Theory of Computing*, pages 150–159, 1997.

[7] B. Marcus and J. Rosenthal, editors. *Codes, Systems and Graphical Models*. IMA Vol. 123. Springer-Verlag, New York, 2001.

[8] P. Oswald and M. A. Shokrollahi. Capacity-achieving sequences for the erasure channel. *IEEE Trans. Inform. Theory*, 48(12):3017–3028, 2002.

[9] M. A. Shokrollahi. New sequences of linear time erasure codes approaching the channel capacity. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 65–76. Springer, Berlin, 1999.

[10] R. Smarandache and P. O. Vontobel. Pseudo-codeword analysis of Tanner graphs from projective and Euclidean planes. *IEEE Trans. Inform. Theory*, 53(7):2376–2393, 2007.

[11] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, 27(5):533–547, 1981.

[12] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar. Construction of regular and irregular LDPC codes: Geometry decomposition and masking. *IEEE Trans. Inform. Theory*, 53(1):121–134, 2007.