On Regular Quasi-Cyclic LDPC Codes from Binomials

Roxana Smarandache
Dept. of Mathematics and Statistics
San Diego State University
e-mail: rsmarand@math.sdsu.edu

Pascal O. Vontobel[1]
Coordinated Science Laboratory
University of Illinois at U-C
email: vontobel@ifp.uiuc.edu

Abstract — **In the past, several authors have considered quasi-cyclic LDPC codes whose circulant matrices in the parity-check matrix are cyclically shifted identity matrices. By composing a parity-check matrix not only with such matrices but also with sums of two cyclically shifted identity matrices and with zero matrices, one can increase the minimum distance while keeping the same regularity. Specifically, whereas for $(3,4)$-regular codes in the first class the best minimum distance is 24, the best minimum distance in the second class is 32. We give examples of codes that achieve these bounds.**

Any quasi-cyclic (QC) linear code C of length $n \triangleq r \cdot P$ and period P is equivalent to a code whose parity-check matrix $\mathbf{H}$ consists of circulant matrices of size $r \times r$. By the well-known isomorphism between the ring of circulant matrices of size $r \times r$ and the ring of polynomials of degree less than r, $\mathbb{F}_2[X]/\langle X^r - 1\rangle$, we can associate a polynomial parity-check matrix matrix $\mathbf{H}(X) \in \big(\mathbb{F}_2[X]/\langle X^r - 1\rangle\big)^{(m/n)P \times P}$ to such an $\mathbf{H}$-matrix. In the following we will use polynomial parity-check matrices to describe the codes.

Definition 1. *We say that a QC code is of type I if it is given by a matrix $\mathbf{H}(X)$ with all entries either monomials or zero and we say that a QC code is of type II if it is given by a matrix $\mathbf{H}(X)$ with all entries either binomials, monomials, or zero.*

Subsequently, we will mainly focus on type-I and type-II QC LDPC given by parity-check matrices $\mathbf{H}(X)$ of size $J \times L$ that are also (J,L)-regular, $J < L$. For a polynomial parity-check matrix $\mathbf{H}(X)$ we let $\mathbf{A}_{\mathrm{wt}} \triangleq \mathbf{A}_{\mathrm{wt}}(\mathbf{H}(X)) \triangleq [a_{ij}]_{ij} \triangleq \big[\mathrm{wt}\,(h_{ij}(X))\big]_{ij}$ be the matrix of the Hamming weights of the $\mathbf{H}(X)$ matrix. We have the following extension of an upper bound by MacKay and Davey [1] on the minimum distance.

Theorem 2. *Let C be a QC code with a $J \times L$ polynomial parity-check matrix $\mathbf{H}(X)$ with weight matrix $\mathbf{A}_{\mathrm{wt}} \triangleq [a_{ij}]_{ij}$.*

$$d_{\min} \leqslant \min_{\substack{\mathcal{S} \subseteq \{1,\ldots,L\} \\ |\mathcal{S}| = J+1}} \sum_{\substack{\mathcal{S}' \subset \mathcal{S} \\ \mathcal{S}' = \{i_1,\ldots,i_J\}}} \sum_{\sigma \in \mathcal{P}} a_{\sigma(1),i_1} \cdots a_{\sigma(J),i_J},$$

where $\mathcal{P}$ is the set of all permutations of $\{1,\ldots,J\}$.

Corollary 3. *A $(3,4)$-regular QC LDPC code C with a 3×4 polynomial parity-check matrix $\mathbf{H}(X)$ has $d_{\min} \leqslant 24$ if the code is of type I, and $d_{\min} \leqslant 32$ if the code is of type II.*

Example 4. Let $r \triangleq 31$. The $(3,4)$-regular QC LDPC code given by the polynomial parity-check matrix

$$\mathbf{H}(X) = \begin{bmatrix} X & X^2 & X^4 & X^8 \\ X^5 & X^{10} & X^{20} & X^9 \\ X^{25} & X^{19} & X^7 & X^{14} \end{bmatrix}$$

has parameters $[124, 33, 24]$, so the upper bound of 24 in Th. 2 can indeed be achieved. This code was inspired by a code presented in [2].

Using type-II codes we can go beyond the upper bound $d_{\min} \leqslant 24$ for type-I codes as shown in the following example.

Example 5. Let $r \triangleq 46$. The $(3,4)$-regular QC LDPC code given by the polynomial parity-check matrix

$$\mathbf{H}(X) = \begin{bmatrix} X + X^2 & 0 & X^4 & X^8 \\ X^5 & X^9 & X^{10} + X^{20} & 0 \\ 0 & X^{25} + X^{19} & 0 & X^7 + X^{14} \end{bmatrix}$$

has parameters $[184, 47, 32]$ and was obtained from Ex. 4 by pairing together some monomials, careful to keep the $(3,4)$-regularity unchanged. The Tanner graph of the code has girth 8 and diameter 8, the same values as the Tanner graph of the $[124, 33, 24]$ code in Ex. 4 had.

Using the $[184, 47, 32]$ code for transmission over a binary-input AWGNC and decoding using the standard sum-product algorithm, we observed no error floor down to a word-error rate (WER) of $3 \cdot 10^{-7}$ and an improvement of ca. 0.3 dB (at WER 10^{-6}) compared to a randomly generated $(3,4)$-regular $[184, 46]$-code. Looking at the minimum AWGNC pseudo-weight of these codes, we got upper bounds of 27.6 and 21.0 for the QC LDPC code and the randomly generated code, respectively.

It is possible to establish the following connections (which can be seen as extensions of observations made e.g. in [3]) between the existence of cycles in the Tanner graph and minors of the polynomial parity-check matrix of a type-I QC LDPC code. (Similar statements can also be made about type-II QC LDPC codes.)

Theorem 6. *Let $\mathbf{H}(X)$ be the polynomial parity-check matrix of a QC LDPC code C of type I. The code C is four-cycle free if and only if all 2×2 minors of $\mathbf{H}(X)$ have no weight loss (no cancellation of the monomials in the determinant sum). (Note that the worthwhile conditions are the ones imposed on the 2×2 submatrices with all entries non-zero.) The code C is four- and six-cycle free if and only if the all 3×3 minors of $\mathbf{H}(X)$ have no weight loss. Moreover, if the girth of a code C is larger than $2J$ then all full-size minors have no weight loss. (The converse of this last statement is not necessarily true.)*

[1] Supported by NSF Grants CCR 99-84515 and CCR 01-05719.

References

[1] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999)* (B. Marcus and J. Rosenthal, eds.), pp. 113–130, Springer Verlag, New York, Inc., 2001.

[2] R. M. Tanner, D. Sridhara, and T. Fuja, "A class of group-structured LDPC codes," in *Proc. of ICSTA 2001*, (Ambleside, England), 2001.

[3] M. Fossorier, "Quasi-cyclic low density parity check codes from circulant permutation matrices," *submitted to IEEE Trans. Inform. Theory*, 2003.