RZ 3556 (# 99566) 06/28/04
Electrical Engineering 8 pages

Research Report

Minimum Distance of Column-Weight-4 LDPC Codes Derived from Array Codes

Thomas Mittelholzer

IBM Research GmbH
Zurich Research Laboratory
8803 Rüschlikon
Switzerland

tmi@zurich.ibm.com

Minimum Distance of Column-Weight-4 LDPC Codes Derived from Array Codes

Thomas Mittelholzer

IBM Research, Zurich Research Laboratory, 8803 Rüschlikon, Switzerland

Abstract

It has recently been recognized that column-weight-4 array codes give rise to a class of binary high-rate low-density parity-check (LDPC) codes $C(q, j = 4)$ with excellent performance on the AWGN channel. It is shown that the minimum Hamming distance of all these codes $C(q, j = 4)$ of length N=q^2 is 10, provided that q is a prime greater or equal to 11. Furthermore, the corresponding codeword multiplicity is lower bounded by $(q - 1)q^2$.

Index terms: Low-density parity-check (LDPC) codes, iterative decoding, union bound approximation.

1 Introduction

Array-code-based LDPC codes, which where introduced by Fan [1], are attractive mainly for two reasons. First, for moderate code lengths and high rates, array codes perform as well as the best comparable randomly constructed regular LDPC codes given in the on-line repository at the Univerity of Cambrigde [2]. Second, array codes $C(q, j)$ are determined by sparse parity check matrices H, which are characterized by two parameters q and j, where q is an odd prime and j is the column weight of H [1],[3]. This simple deterministic construction of array codes holds the promise that basic code parameters such as minimum distance and codeword multiplicities can be determined. Indeed, for $j = 3$, the minimum distance and the corresponding multiplicity have been determined and for $j = 4, 5, 6$, upper bounds on the minimum distance are known [4]. Furthermore, for the case $j = 4$, it was shown that $d_{\min} \geq 10$ [5]. In this paper, we determine the minimum distance for the class of all $j = 4$ array codes.

2 Array Codes

Let q be an odd prime and let $\zeta = x \bmod (1 - x^q)$ be a generating element of the ring $R = GF(2)[x]/(1 - x^q)$. For any positive integer j, $j \leq q$, the array code $C_R(q, j)$ of length q over R is defined by the following $j \times q$ Reed-Solomon-type parity check matrix over R

$$H_\zeta = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{q-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{2(q-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \zeta^{j-1} & \zeta^{2(j-1)} & \dots & \zeta^{(j-1)(q-1)} \end{bmatrix}. \tag{1}$$

In a similar way as in the field case, it follows that

$$g(z) = (z - 1)(z - \zeta) \dots (z - \zeta^{j-1}) \tag{2}$$

is a codeword (written in polynomial notation) of the cyclic code $C_R(q, j) \subset R[z]/(1 - z^q)$. Despite the fact that R is a ring and not a field, the polynomial $g(z)$ shares most of the properties of a generator polynomial. Any multiple of $g(z)$ is a codeword and the $q - j$ cyclic shifts $g(z), zg(z), \dots, z^{q-j-1}g(z)$ determine a subcode $C_R^{(g)}(q, j)$ of rank $q - j$ over R. In particular, $\dim C_R^{(g)}(q, j) = q(q - j)$ over GF(2).

The remaining codewords, which are not in the subcode $C_R^{(g)}(q, j)$, can be characterized as follows. The ring element $m = 1 + \zeta + \zeta^2 + \ldots + \zeta^{q-1}$ generates the ideal $\{0, m\} \subset R$ and, moreover, it has the property that $r \cdot m = 0$, if in $r = r_0 + r_1\zeta + \ldots + r_{q-1}\zeta^{q-1}$ an even number of the coefficients r_i equal 1, and $r \cdot m = m$, otherwise. Thus, the polynomial

$$p(z) = m \cdot (1 + z) \tag{3}$$

is in the null space of the parity check matrix H_ζ. The R-subcode generated by $p(z)$ and its $q - 2$ cyclic shifts will be denoted $C_R^{(p)}(q, j)$, i.e, $C_R^{(p)}(q, j) = <m \cdot (1 + z)>$ in $R[z]/(1 - z^q)$. One has $\dim C_R^{(p)}(q, j) = q - 1$ over GF(2) and it can be shown that

$$C_R^{(g)}(q, j) \cap C_R^{(p)}(q, j) = <m \cdot g(z)>,$$

which is in accordance with the structure of the generator matrix G in [4]. In particular, $\dim <m \cdot g(z)> = q-j$ over GF(2). Using the fact [4] that $\dim C_R(q,j) = q(q-j)+j-1$ and a dimension argument, one concludes that $C_R^{(g)}(q,j) + C_R^{(p)}(q,j) = C_R(q,j)$, i.e., the cyclic code $C_R(q,j)$ over R is generated by the two generator polynomials $g(z)$ and $p(z)$.
From $C_R(q,j)$, one can derive a binary array code $C(q,j)$ using the regular matrix representation of the ring R (see Chap. 7.3 in [6]), which is determined by the $q \times q$-matrix

$$P = \rho(\zeta) = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}. \tag{4}$$

For instance, for the special case $j=4$, the corresponding binary parity-check matrix for $C(q, j=4)$ is given by the binary $4q \times q^2$ matrix

$$H = \rho(H_\zeta) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & P & P^2 & \dots & P^{q-1} \\ 1 & P^2 & P^4 & \dots & P^{2(q-1)} \\ 1 & P^3 & P^{3\cdot 2} & \dots & P^{3(q-1)} \end{bmatrix}, \tag{5}$$

where by abuse of notation 1 denotes the $q \times q$ identity matrix.
To pass from binary codewords in $C(q,j)$ to corresponding codewords in $C_R(q,j)$ over R, we will use the vector space isomorphism

$$\begin{array}{rccc} \varphi: & \text{GF(2)}^q & \rightarrow & R \\ & [a_0, a_1, \dots, a_{q-1}] & \mapsto & \sum_{\ell=0}^{q-1} a_\ell \zeta^\ell. \end{array} \tag{6}$$

Rewriting the binary vector $\mathbf{x} = [x_0, x_1, \dots, x_{q^2-1}]$ as $\varphi(\mathbf{x}) = [\xi_0, \xi_1, \dots, \xi_{q-1}]$, where $\xi_i = \varphi([x_{i\cdot q}, \dots, x_{(i+1)q-1}])$, one obtains a one-to-one correspondence of binary codewords and codewords over R, namely

$$\mathbf{x}H^T = 0 \Longleftrightarrow \varphi(\mathbf{x})H_\zeta^T = 0. \tag{7}$$

In terms of polynomial representation of codewords, the image of a binary codeword $\mathbf{x} = [x_0, x_1, \dots, x_{q^2-1}]$ under the isomorphism φ is given by $\sum_{i=0}^{q-1} c_i(\zeta) z^i$, where $c_i(\zeta) = x_{i\cdot q} + x_{i\cdot q+1}\zeta + \ldots + x_{(i+1)q-1}\zeta^{q-1}$.

3 Minimum Distance of the Array Codes $C(q, j=4)$

The following proposition summarizes relevant results from [4] and [5].

Proposition 1 *The binary array code $C(q,j)$ has length q^2 and dimension $q^2-j(q-1)-1$ with a minimum distance of $d_{\min}(q,j) \geq j+1$. Furthermore, all $j=3$ array codes have a minimum distance of $d_{\min}(q,3)=6$ and the corresponding multiplicity is $\mu_{\min} = q\begin{pmatrix} q \\ 3 \end{pmatrix}$. For $j=4$ array codes, $d_{\min}(5,4)=8$, $d_{\min}(7,4)=8$ and for $q \geq 11$, the minimum distance is bounded by*

$$10 \leq d_{\min}(q,4) \leq 12.$$

Theorem 1 *For $q \geq 11$, q prime, the binary $j = 4$ array code $C(q, 4)$ has a minimum distance of* 10.

Proof: In view of Prop. 1 it is sufficient to show that there is a codeword of weight 10. Let $g(z)$ be defined by (2) and let

$$\begin{aligned} u(z) &= \zeta^8 + (\zeta^5 + \zeta^7 + \zeta^8)z + (\zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8)z^2 \\ &\quad + (\zeta^3 + \zeta^4 + \zeta^6 + \zeta^7)z^3 + (\zeta^2 + \zeta^3 + \zeta^5)z^4 + (\zeta + \zeta^2 + \zeta^3)z^5 + 1z^6. \end{aligned}$$

By replacing ζ by P in the following codeword of $C_R(q, 4)$, one obtains q binary weight-10 codewords of $C(q, 4)$

$$\begin{aligned} w(z) = u(z)g(z) &= \zeta^{14} + \zeta^{12}z + \zeta^8 z^2 + (\zeta^6 + \zeta^{14})z^3 \\ &\quad + (\zeta^8 + \zeta^{12})z^5 + \zeta^6 z^8 + 1z^9 + 1z^{10}. \end{aligned} \tag{8}$$

To find a lower bound on the multiplicity of weight-10 codewords, we will let a group of weight-preserving automorphisms operate on the codeword given by (8). The group of weight-preserving automorphisms of the binary code $C(q, j)$ will be characterized by R-automorphisms $\theta : C_R(q, j) \to C_R(q, j)$ of the form

$$\theta(\sum_{i=0}^{q-1} c_i(\zeta)z^i) = z^\ell \zeta^m \sum_{i=0}^{q-1} c_i(\zeta^a)z^{a \cdot i}, \tag{9}$$

where $\ell, m \in \{0, 1, \ldots, q-1\}$ and $a \in \{1, \ldots, q-1\}$. To check that the mappings θ leave $C_R(q, j)$ invariant and induce a permutation on the codewords of the binary code $C(q, j)$ (we will call such mappings *binary-weight-preserving*), it is useful to note that each mapping θ is composed of three different types of R-automorphisms of R^q, which are given by

(i) cyclic shifting: $c(z) \mapsto z^\ell c(z)$,

(ii) scaling: $c(z) \mapsto \zeta^m c(z)$,

(iii) applying the power map induced by the two simultaneous maps $z \mapsto z^a$ and $\zeta \mapsto \zeta^a$.

It is clear that these mappings are binary-weight-preserving and, moreover, since $C_R(q, j)$ is cyclic over R, cyclic shifting and scaling are clearly automorphisms. To verify that the power map (iii) is an automorphism it is sufficient to check that the two generator polynomials $g(z)$ and $p(z)$ defined by (2) and (3) are mapped into codewords, i.e., $\theta(g(z)) = (z^a - 1)(z^a - \zeta^a) \ldots (z^a - (\zeta^a)^{j-1})$ is divisible by $g(z)$ and, similarly, $\theta(p(z))$ is divisible by $p(z)$. For $g(z)$, this follows from the fact that in the quotient

$$\frac{\theta(g(z))}{g(z)} = \frac{z^a - 1}{z - 1} \frac{z^a - \zeta^a}{z - \zeta} \cdots \frac{z^a - (\zeta^a)^{j-1}}{z - \zeta^{j-1}}$$

each factor on the right is a polynomial because

$$\frac{z^a - (\zeta^a)^\ell}{z - \zeta^\ell} = z^{a-1} + z^{a-2}\zeta^\ell + z^{a-3}\zeta^{2\ell} + \ldots + \zeta^{(a-1)\ell}.$$

For $p(z)$, the proof is similar.

Let $\mathcal{G}$ denote the group of the $(q-1)q^2$ binary-weight-preserving automorphisms of $C_R(q, j)$ defined by (9). Note that in [5], a different description of these automorphisms is given in terms of "affine" permutations, which act doubly transitive on $C(q, j)$.

Lemma 1 *There is no nontrivial element of the group $\mathcal{G}$ that leaves the weight-10 codeword in (8) fixed.*

Proof: Let $w(z)$ be given by (8) and let $\theta \in \mathcal{G}$. We will show that $\theta(w(z)) = w(z)$ implies $\theta = 1$, i.e., $m = 0 = \ell$ and $a = 1$. There are only six coefficients in $w(z) = \sum w_\ell(\zeta) z^\ell$ that are powers of ζ, viz., $w_0(\zeta) = \zeta^{14}$, $w_1(\zeta) = \zeta^{12}$, $w_2(\zeta) = \zeta^8$, $w_8(\zeta) = \zeta^6$, $w_9(\zeta) = 1$, $w_{10}(\zeta) = 1$. In particular, $w_9(\zeta^a) = 1$ and $w_{10}(\zeta^a) = 1$ and, moreover, $w_9(\zeta)$ and $w_{10}(\zeta)$ are the only two of these coefficients that are equal. Therefore,

$$z^9 + z^{10} = \theta(w_9(\zeta) z^9 + w_{10}(\zeta) z^{10}) = \zeta^m z^{\ell+9a} + \zeta^m z^{\ell+10a},$$

which implies $m = 0$ and either

$$\begin{array}{lll} z^{\ell+9a} = z^9 & \text{and} & z^{\ell+10a} = z^{10} \qquad \text{or} \\ z^{\ell+9a} = z^{10} & \text{and} & z^{\ell+10a} = z^9. \end{array}$$

One can easily show that in both cases, $a = 1$ and $\ell = 0$.

Corollary 1 *The multiplicity of the minimum weight codewords in $C(q, 4)$ is at least $|\mathcal{G}| = (q-1)q^2$.*

4 Union Bound Approximation

It is interesting to compare the performance of the high-rate array-code-based LDPC codes under iterative decoding with the theoretical bounds for maximum likelihood decoding. The bounds are derived from the first term of the weight distribution of the codes. All simulations were carried out for the additive white Gaussian noise (AWGN) channel using the sum-product decoding algorithm with the maximum number of iterations limited to 50.

For $j = 3$, we have considered the code $C(47, 3)$ of length $N = 47^2 = 2209$, dimension $K = 2070$ and $d_{\min}(47, 3) = 6$ (cf. Prop. 1). Figure 1 shows the performance of this code in terms of block and bit error rate. For comparison, capacity bounds (for block and bit error) are shown. The dashed line labelled 'Union bound' is an approximation to the union bound determined by $d_{\min}(47, 3)$ and $\mu_{\min}$. This dominant-term union bound provides a rough approximation to the block error rate performance at high signal-to-noise ratios (SNR). From the shape of the dominant-term union bound, it is apparent that the code does not have a distinct error floor.

For the same codeword length $N = 47^2$, we have considered the $j = 4$ array code $C(47, 4)$ of dimension $K = 2024$ and $d_{\min}(47, 4) = 10$. The performance of this code on the AWGN channel is illustrated in Fig. 2. The dashed line corresponds to a "sub-union-bound", which is determined by the minimum distance and the lower bound $q^2(q-1) = 101614$ on the number of minimum weight codewords. In contrast to the case $j = 3$ (Fig. 1), there is a substantial gap between the block-error rate performance and the sub-union-bound, even at high SNR. One reason for this gap is that the lower bound given in Corollary 1 might not be tight.

5 Conclusions

The minimum distance of the class of column-weight-4 array codes $C(q, 4)$ has been determined. In particular, for $q \geq 11$ a generic minimum-weight codeword was specified. Furthermore, by studying the action of an automorphism group on that codeword, a lower bound on the number of

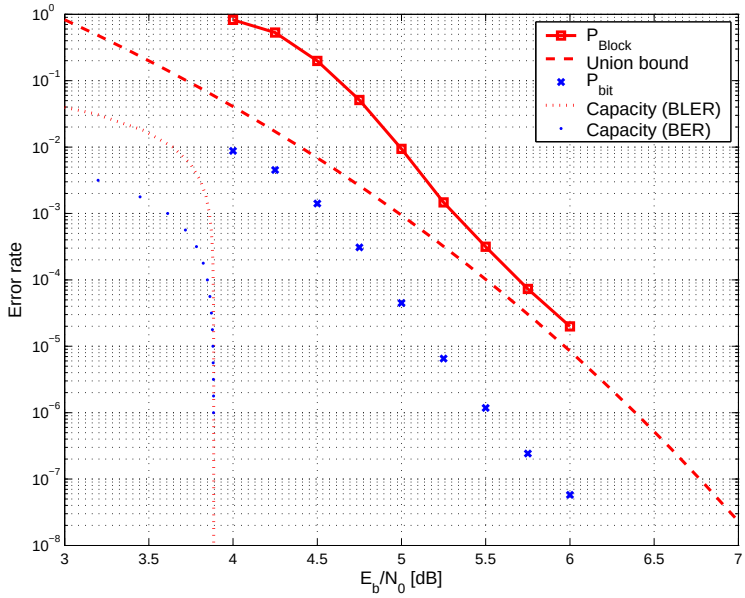

Figure 1: Union bound approximation of the block error rate for the rate-2070/2209 ($j = 3$, $q = 47$) array code.

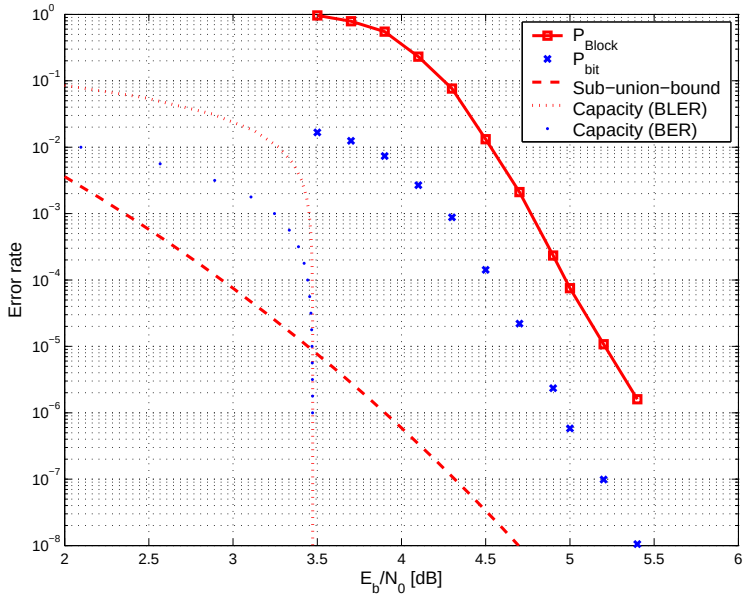

Figure 2: Bit and block error rate performance of the rate-2024/2209 ($j = 4$, $q = 47$) array code and the sub-union-bound.

minimum-weight codewords was obtained. Theorem 1 is also valid for shortened $j = 4$ array codes. Moreover, using a similar proof as for Theorem 1, one concludes that the $j = 4$ modified array codes with simple encoding structure as proposed in [7] have a minimum distance of at most 10.

The sub-union-bound based on the code parameters given in Theorem 1 and Corollary 1 does not provide a good match for the performance of the array code $C(47, 4)$ on the AWGN channel under iterative decoding. A possible explanation for this gap is that the bound in Corollary 1 is not tight and/or iterative decoding does not behave like maximum-likelihood decoding. A better understanding of this gap is a topic of further research.

References

[1] J.L. Fan, "Array codes as low-density parity-check codes," *Proc. 2nd Intl. Symp. on Turbo Codes*, Brest, France, 4-7 Sept. 2000, pp. 543-546.

[2] D.C.J. MacKay, Encyclopedia of sparse graph codes (hypertext archive, 1999). `http://wol.ra.phy.cam.ac.uk/mackay/codes/data.html`.

[3] M. Blaum, R.M. Roth, "New array codes for multiple phased burst correction," *IEEE Trans. Information Th.*, Vol. 39, No. 1, Jan. 1993, pp. 66 – 77.

[4] T. Mittelholzer, "Efficient Encoding and Minimum Distance Bounds of Reed-Solomon-type Array Codes," in *Proc. 2002 IEEE Intl. Symp. Information Th.* (ISIT 2002), Lausanne, Switzerland, June/July 2002, p. 282.

[5] K. Yang, T. Helleseth, "On the Minimum Distance of Array Codes as LDPC Codes," *IEEE Trans. Information Th.*, Vol. 49, No. 12, 2003, pp. 3268 – 3271.

[6] N. Jacobson, *Basic Algebra I*, Freeman, San Francisco, 1980.

[7] E. Eleftheriou and S. Ölçer, "Low-Density Parity-Check Codes for Digital Subscriber Lines," in *Proc. IEEE Intl. Conf. on Communications (ICC 2002)*, Vol. 3, 2002, pp. 1752 – 1757.