Parity Check Codes for Second Order Diversity

Aaqib A. Patel, Member, IEEE, Abdul Mateen Ahmed, Student Member, IEEE, and Mohammed Zafar Ali Khan, Senior Member, IEEE.

Abstract—Block codes are typically not used for fading channels as soft decision decoding is computationally intensive and hard decision decoding results in performance loss. In this paper we propose a diversity preserving hard decision decoding scheme for parity check codes (PCC) over Rayleigh fading channels. The proposed flip decoding scheme has linear complexity in the block length. Theoretical analysis and simulation results verify the correctness of the proposed detection scheme.

Index Terms—Bit error rate, bit-interleaved coded modulation, forward error correction, modulation.

I. INTRODUCTION

Brute-force maximum-likelihood decoding (MLD) of a linear \((n, k)\) block code requires calculation of \(2^k\) metrics. This method becomes too complex to be applied for large \(k\) and so more effective methods are required. As linear block codes have a trellis structure \([1]\), the Viterbi algorithm can be used to reduce the number of computations. Yet, the branch complexity of the states becomes large as \(k\) increases. Block code maximum likelihood decoding has been investigated by many coding theorists; as detailed in \([2]\). Most initial works code maximum likelihood decoding has been investigated by many coding theorists; as detailed in \([2]\). Most initial works

Methods presented in \([7], [8]\) need \(n - k\) to be relatively small. For very high-rate codes, a method to reducing the search space was presented in \([9]\). Other methods take advantage of code structure to reduce the overall complexity of Trellis Decoding \([10] - [13]\). Nevertheless, the trellis complexity still increases exponentially with the code length \([14]\). To maintain complexity, suboptimal multistage decoding on trellis has been proposed \([15], [16]\).

Ordered statistics-based decoding (OSD) is a soft-decision decoder for linear block codes. OSD provides a near maximum-likelihood (ML) performance \([19], [20]\). But suffers from large computational complexity. Algorithms that reduce the complexity of OSD are referred to in the literature \([21] - [23]\).

In this letter we propose a diversity preserving linear complexity hard-decision decoding for parity check codes. The proposed decoding has linear complexity in the block length, \(n\). As PCC have a rate of \(n - 1/n\), this allows use of high rate codes that achieve second order diversity. The contributions of this paper are

- use of parity check codes for error correction over fading channels.
- a diversity preserving hard-decision decoding scheme for parity check codes.
- the proposed flip decoder (FD) has linear complexity.
- theoretical analysis that shows that the proposed decoder achieves second order diversity over Rayleigh fading Channels.
- simulation results that verify the theoretical analysis.

The rest of the paper is organized as follows. Relevant previous work is summarized in Sec. II. The proposed flip decoder is presented Sec. III where the diversity order of the decoder is also derived. Simulation results are presented in Secs. IV and Sec. V concludes the paper.

II. PREVIOUS WORK

A. System Model

Let \(C\) be a \((n, k)\) binary linear code with generator matrix \(G\) and minimum Hamming distance \(d_{\text{min}}\). The code, \(C\), is used for error control over the Rayleigh fading channel. Let \(\bar{c} = (c_1, c_2, \cdots, c_n)\) be a codeword in \(C\). The \(n\) bits of the codeword are sent on a Rayleigh fading channel with ideal interleaving. For BPSK modulation, the codeword \(\bar{c}\) is mapped to a bipolar sequence \(\bar{x} = (x_1, x_2, \cdots, x_n)\) where \(x_i \in \{-1, 1\}, \forall i\). The received signal can be represented as

\[
    r_i = h_i x_i + w_i, 1 \leq i \leq n
\]

where \(w_i\)’s are statistically independent complex Gaussian random variables with zero mean and variance \(N_0\) and \(h_i \in \mathbb{R}\)’s are independent, identically distributed fading coefficients.
B. Decoding and diversity

If a hard-decision decoding is performed, then the probability of error is upper bounded as \(28\)

\[
P(c) \leq \sum_{q=t+1}^{n} \binom{n}{q} \left( \frac{1 - \beta}{2} \right)^{q} \left( \frac{1 + \beta}{2} \right)^{n-q}
\]

where \(\beta = \sqrt{\frac{c_{1}}{2c_{2}}}, t\) is the number of errors that can be corrected by the code, \(\gamma_{c}\) is the average signal to noise ratio (SNR) per code bit and the instantaneous SNR per code bit is given by \(\gamma_{t} = h_{t}^{2} \gamma_{c}\). Note that the average SNR per bit is defined as \(\bar{\gamma}_{b} = \bar{\gamma}_{c}/R\) where \(R\) is the rate of the code. We have

\[\text{Lemma 1: Hard-Decision decoding has a diversity order of } t+1 = \left\lfloor \frac{\log_{2} \left( \frac{1 - \beta}{2} \right)}{\log_{2} \left( \frac{1 + \beta}{2} \right)} \right\rfloor + 1\]

\[\text{Proof: Rearranging } (2),\text{ we have } P(c) \leq \left( \frac{1 - \beta}{2} \right)^{t+1} \sum_{q=0}^{n} \binom{n}{q} \left( \frac{1 - \beta}{2} \right)^{q} \left( \frac{1 + \beta}{2} \right)^{n-q}
\]

As the average SNR tends to a large value, \(\lim_{\gamma_{t} \to \infty} \left( \frac{1 - \beta}{2} \right) = \frac{1}{\gamma_{c}}\) and \(\lim_{\gamma_{t} \to \infty} \left( \frac{1 + \beta}{2} \right)^{q} = 1\). Using the definition of diversity order, \(D\), \(27\) and substituting from above, we have

\[D = \lim_{\gamma_{t} \to \infty} \frac{-\log[P(c)]}{\log[\gamma_{c}]} = \lim_{\gamma_{t} \to \infty} \frac{(t+1) \log[4\gamma_{c}] + \log \left[ 1 + \frac{1}{2\gamma_{c}} + \cdots \right]}{\log[\gamma_{c}]} = t+1.
\]

While hard-decision decoding has lower complexity, it results in a loss of diversity order. This loss of diversity order has a significant impact on performance over fading channels.

Using soft decision decoding, the probability of error is upper bounded as \(28\)

\[P(c) < \left( \frac{4}{2 + \gamma_{c}} \right)^{d_{\min}}\]

We have

\[\text{Lemma 2: Soft-decision decoding has a diversity order of } d_{\min}.
\]

\[\text{Proof: Using the definition of diversity order, } D, \text{ (27) and substituting from (4), we have } D = \lim_{\gamma_{t} \to \infty} \frac{-\log[P(c)]}{\log[\gamma_{c}]} = \lim_{\gamma_{t} \to \infty} \frac{d_{\min} \log[2 + \gamma_{c}] + \log \left[ 1 + \frac{1}{2\gamma_{c}} \right] + \log[4(M-1)]}{\log[\gamma_{c}]} = \frac{d_{\min}}{\gamma_{c}}.
\]

However, soft decision decoding requires comparison of all \(2^{k}\) codewords, which becomes very costly as \(k\) increases.

C. Parity Check Codes

The parity check codes are the most well known error-detecting code. In this linear code, the codeword consists of the \(k\)-bit data word with an extra bit, called the parity bit, to get an \(n = k + 1\)-bit codeword. The parity bit makes the total number of 1s in the code word even or odd. Without loss of generality, in this paper the parity is chosen to be even. The minimum Hamming distance for this code is \(d_{\min} = 2\). This means that the code can detect a single error and it cannot correct any error. The generator matrix and the parity check matrix are given by

\[G = \begin{pmatrix} I_{k} & 1_{k} \end{pmatrix}, H^{T} = \begin{pmatrix} 1_{n} \end{pmatrix}\]

where \(I_{k}\) is an identity matrix of size \(k\) and \(1_{n}\) is a column vector of \(n\)'s. Lemmas \(1\) and \(2\) specialize for this case, so that

\[\text{Corollary 1: The parity check codes have a diversity order of one and two with hard-decision decoding with soft-decision decoding respectively.}
\]

\[\text{Proof: Substituting } d_{\min} = 2 \text{ in Lemmas } 1 \text{ and } 2 \text{ we have the desired result.}
\]

Note that Corollary \(\text{I}\) implies that the diversity order of two can be achieved with PCC with soft decision decoding. However, as the code length increases the decoding complexity increases exponentially. In the next section we propose a hard-decision decoder for PCC that achieves full diversity of \(d_{\min} = 2\).

III. THE PROPOSED HARD-DECISION DECODER FOR PCC

Since the CSI is known at the receiver, if there is a parity mismatch, the most likely bit in error would be the bit with the smallest CSI, \(h\). Based on this intuition we have the proposed decoder in Algorithm \(\text{I}\). Note that Matlab’s notation has been used in Algorithm \(\text{I}\) so that \(\sim\) denotes ‘not equal to’ and \(\sim a\) denotes logical not of bit \(a\).

\[\text{Theorem 1: The proposed hard-decision decoder has a diversity order of } d_{\min} = 2 \text{ for PCC.}
\]

\[\text{Proof: See Appendix A.}
\]

While we have analyzed that the proposed decoder achieves full diversity for PCC by flipping one bit, we would like to explore whether we can flip more than one bit. Clearly, two bits cannot be flipped as that would not change the parity and hence the diversity order would be two or lower.
of one. Further, as diversity and that hard-decision decoding has a diversity order of modulation. Observe that the proposed FD decoder preserves soft-decision decoding. Simulations were also done using 4-
soft-decision decoding but have at-least quadratic complexity due to Gaussian elimination. The proposed hard-decision decoding, proposed Flip Decoding and soft-decision decoding.

IV. SIMULATION RESULTS

Fig. 1 shows the BER vs. SNR per bit, $\gamma_b$, for hard-decision decoding, proposed flip decoding and soft-decision decoding over Rayleigh fading channels. The simulations were performed over code lengths of $n = 2, 4$ and $8$ using BPSK modulation. Observe that the proposed FD decoder preserves diversity and that hard-decision decoding has a diversity order of one. Further, as $n$ increases from 2 to 8, the performance of FD and soft-decision decoding shifts by about 2 dB. Also, note that the performance of the proposed decoder is within 2 dB of soft-decision decoding. Simulations were also done using 4-QAM, 16-QAM and 64-QAM with similar conclusions and so have not been reported. Note that the complexity of brute-force ML soft-decision and hard-decision decoding is exponential in $n-1$. Also for PCC, as $t = \left\lfloor \frac{2n-1}{n} \right\rfloor = 0$, the chase decoder [4] and its variants reduce to hard-decision decoding. OSA and its variants [28] have near-optimal performance and matches soft-decision decoding but have at-least quadratic complexity in $n$ due to Gaussian elimination. The proposed hard-decision decoder’s complexity involves finding the minimum of a vector that is of linear complexity and then flipping the least reliable bit, which is of constant complexity. So the overall complexity of the flip decoder is linear in $n$. Also, note that the PCC rate, $1 - 1/n$, approaches one as $n$ increases. So this scheme is suitable for high data rate communication that requires a diversity order of two.

V. CONCLUSIONS

For the first time, we have proposed a linear complexity hard-decision based decoding scheme that preserves diversity for any error correcting code; the parity check codes. The diversity performance of the decoding scheme was verified by analysis and simulations. Further enhancement of this work for all codes or codes with higher code distance will be an interesting topic of research. Especially in the context of ultra-reliable low latency communications (URLLC) and internet of things (IoT) [26], which require low complexity decoding with high performance gains.

ACKNOWLEDGMENTS

This publication is an outcome of the R&D work under the Visvesvaraya Faculty research fellowship Ph.D. Scheme of Ministry of Electronics & Information Technology, Government of India; implemented by Digital India Corporation.

APPENDIX A

PROOF OF THEOREM 1

For the proposed decoder, an error occurs if there are more than one errors or when there is one error but not in the bit with smallest $\gamma_i$. We denote the probability of one error but not in the bit with smallest $\gamma_i$ as $P_e(\text{error in 1 bit})$ and the probability of more than one errors as $P_e(\text{error in 2 or more bit})$. Accordingly, the probability of error is given by

$$P_e = P_e(\text{error in 1 bit}) + P_e(\text{error in 2 or more bit}) \tag{7}$$

The probability of getting two or more errors, given unordered $\gamma_i$’s is obtained as

$$P_e(\text{error in 2 or more bit}) = \sum_{m=2}^{n} \binom{n}{m} \bar{p}^m (1 - \bar{p})^{n-m} \tag{8}$$

where $\bar{p}$ is the probability of error in a random bit corresponding to unordered $\gamma_i$’s, defined as

$$\bar{p} = E_{\gamma} \left[ \text{Prob} \{ n \geq \gamma \} \right] = E_{\gamma} \left[ Q \left( \sqrt{2\gamma} \right) \right] \leq \frac{1}{1 + \frac{1}{\gamma_c}} \tag{9}$$

where the last inequality is obtained using the Chernoff bound [28] and averaging over the exponential distribution of $\gamma$. Substituting (9) in (8) we obtain

$$P_e(\text{error in 2 or more bit}) = \sum_{m=2}^{n} \binom{n}{m} \left\{ \frac{1}{1 + \bar{\gamma}_c} \right\}^m \left[ \frac{\bar{\gamma}_c}{1 + \bar{\gamma}_c} \right]^{n-m} \tag{10}$$

For finding $P_e(\text{error in 1 bit})$ the $\gamma_i$’s are ordered, so that $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_n$, define

$$p_i = \text{Prob} \{ n_i \geq \gamma_i | \gamma_i \} = Q \left( \sqrt{2\gamma_i} \right) \leq e^{-\gamma_i} \tag{11}$$

where the last inequality is obtained using the Chernoff bound [28]. Let $\bar{p}_i = E_{\gamma_i} \left[ p_i \right]$. This implies $\bar{p}_1 \geq \bar{p}_2 \geq \cdots \geq \bar{p}_n$, and $(1 - \bar{p}_1) \leq (1 - \bar{p}_2) \leq \cdots \leq (1 - \bar{p}_n)$.

Using the last inequality, we have

$$P_e(\text{error in 1 bit}) = \sum_{i=2}^{n} \bar{p}_i \prod_{j=1 \atop j \neq i}^{n} (1 - \bar{p}_j) \leq \sum_{i=2}^{n} \bar{p}_i (1 - \bar{p}_n)^{n-1} \leq (n-1) \bar{p}_2 (1 - \bar{p}_n)^{n-1} \tag{12}$$
\[ p_{FD}(c) \leq \frac{n^2(n-1)^2}{\gamma_c + (n-1)(\gamma_c + n)} \{ \sum_{k=0}^{n-1} \frac{(n-1)^k \gamma_c}{\gamma_c + (k+1)} \} \{ \frac{1}{1 + \gamma_c} \}^n \{ \frac{\gamma_c}{1 + \gamma_c} \}^{n-m} \quad (17) \]

where \( \bar{p}_2 \) and \( \bar{p}_m \) are obtained by averaging over the ordered statistics of \( \gamma_c \). The pdf of the second order and the \( n \)-th order statistic corresponding to \( \gamma_2 \) and \( \gamma_n \) are given by

\[ f_{\gamma_2}(x) = n(n-1)\gamma_c e^{-\frac{x(n-1)}{\gamma_c}} e^{-\frac{1}{\gamma_c} x} \]

\[ f_{\gamma_n}(x) = \frac{1}{\gamma_c} e^{-\frac{x}{\gamma_c}} \left( 1 - e^{-\frac{x}{\gamma_c}} \right)^{(n-1)} \]

\[ \bar{p}_2 = \int_0^\infty n(n-1)\gamma_c e^{-\frac{x(n-1)}{\gamma_c}} e^{-\frac{1}{\gamma_c} x} \, dx \]

\[ = \int_0^\infty n(n-1) \gamma_c e^{-\frac{x(n-1)}{\gamma_c}} e^{-\frac{x}{\gamma_c}} \, dx \]

\[ = n(n-1) \left( \frac{1}{\gamma_c + (n-1)} - \frac{1}{\gamma_c + n} \right) \]

\[ \bar{p}_n = \int_0^\infty \prod_{k=0}^{n-1} \frac{n(n-1)^k \gamma_c}{\gamma_c + (k+1)} e^{-\frac{x}{\gamma_c}} \, dx \]

\[ = \sum_{k=0}^{n-1} \frac{n(n-1)^k \gamma_c}{\gamma_c + (k+1)} \quad (15) \]

Substituting (15) and (14) in (12), we have

\[ P_e(\text{error in 1 bit}) \leq \frac{n^2(n-1)^2}{\gamma_c + (n-1)(\gamma_c + n)} \left( \sum_{k=0}^{n-1} \frac{(n-1)^k}{\gamma_c + (k+1)} \right) \left( \frac{1}{1 + \gamma_c} \right)^n \left( \frac{\gamma_c}{1 + \gamma_c} \right)^{n-m} \quad (16) \]

Substituting from (10), (11) to (7), we have (17). Using the definition of diversity order, \( D \), (27), substituting from (17) and applying the limits we have

\[ D = \lim_{\gamma_c \to \infty} -\log[P_{FD}(c)]/\log(\gamma_c) \]

\[ = \lim_{\gamma_c \to \infty} 2 \log [1 + \gamma_c] + \text{higher order terms} / \log(\gamma_c) \]

\[ = 2 \quad (18) \]

REFERENCES

[1] J. K. Wolf, “Efficient maximum likelihood decoding of linear block codes using a trellis”, IEEE Trans. Inform. Theory, vol. IT-24, pp. 76–80, Jan. 1978.

[2] J. H. Conway and N. J. A. Sloane, “Soft decoding techniques for codes and lattices including the Golay code and the Leech lattice”, IEEE Trans. Inform. Theory, vol. IT-32, pp. 41–50, Jan. 1986.

[3] G. D. Forney, “Generalized minimum distance decoding”, IEEE Trans. Inform. Theory, vol. IT-12, pp. 125-131, Apr. 1966.

[4] D. Chase, “A class of algorithms for decoding block codes with channel measurement information”, IEEE Trans. Inform. Theory, vol. IT-18, pp. 170-182, Jan. 1972.

[5] H. Tanaka and K. Kagiwhara, “Simplified correlation decoding by selecting codewords using erasure information”, IEEE Trans. Inform. Theory, vol. IT-29, pp. 743-748, Sept. 1983.

[6] T. Taneko, T. Nishijima, H. Inagumi and S. Hirasawa, “An efficient maximum likelihood decoding of linear block codes with algebraic decoder”, IEEE Trans. Inform. Theory, vol. 40, pp. 320-327, Mar. 1994.

[7] J. Snyders and Y. Be’ery, “Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes”, IEEE Trans. Inform. Theory, vol. 35, pp. 963-975, Sept. 1989.

[8] N. Lous, P. Bours and H. van Tilborg, “On maximum likelihood soft-decision decoding of binary linear codes”, IEEE Trans. Inform. Theory, vol. 39, pp. 197-203, Jan. 1993.

[9] J. Snyders, “Reduced lists of error patterns for maximum likelihood soft decoding”, IEEE Trans. Inform. Theory, vol. 37, pp. 1194-1200, July 1991.

[10] J. Snyders, “On survivor error patterns for maximum likelihood soft decoding”, Proc. IEEE Int. Symp. on Information Theory, pp. 192-196, June.

[11] G. D. Forney, “Coset codes II: Binary lattices and related codes”, IEEE Trans. on Inform. Theory, vol. 34, pp. 1198-1207, Sept. 1988.

[12] D. Muder, “Minimal trellises for block codes”, IEEE Trans. Inform. Theory, vol. 35, pp. 1039-1053, Sept. 1988.

[13] T. Kasami, T. Takata, T. Fujitaka and S. Lin, “On complexity of trellis structure of linear block codes”, IEEE Trans. Inform. Theory, vol. 39, pp. 1057-1064, May 1993.

[14] A. Lafourcade and A. Vardy, “Asymptotically good codes have infinite trellis complexity”, IEEE Trans. Inform. Theory, vol. 41, pp. 555-559, Mar. 1995.

[15] F. Hemmati, “Closest coset decoding of \(|u|u + u|\) codes”, IEEE J. Selected Areas Commun., vol. 7, pp. 982-988, Aug. 1989.

[16] J. Wu, S. Lin, T. Kasami, T. Takata and T. Fujitaka, “An upper bound on the effective error coefficient of two-stage decoding and good two-level decompositions of some Reed-Muller codes”, IEEE Trans. Commun., vol. 42, pp. 813-818, Feb./Mar./Apr. 1994.

[17] Y. S. Han, C. R. P. Hartmann and C. C. Chen, “Efficient priority-first search maximum-likelihood soft-decision decoding of linear block codes”, IEEE Trans. Inform. Theory, vol. 39, pp. 1514-1523, Sept. 1993.

[18] Y. S. Han, C. R. P. Hartmann and K. G. Mehta, “Further results on decoding linear block codes using a generalized Dijkstra’s algorithm”, Proc. IEEE Int. Symp. on Information Theory, pp. 342, 1994-June.

[19] B. Dorsch, “A decoding algorithm for binary block codes and J-ary output channels,” IEEE Trans. Inf. Theory, vol. IT-20, no. 3, pp. 391–394, May 1974.

[20] M. P. C. Fossorier and S. Lin, “Soft-decision decoding of linear block codes based on ordered statistics,” IEEE Trans. Inf. Theory, vol. 41, no. 5, pp. 1379–1396, Sep. 1995.

[21] Y. Wu and C. N. Hadjicostis, “Soft-decision decoding of linear block codes using preprocessing and diversification,” IEEE Trans. Inf. Theory, vol. 53, no. 1, pp. 378–393, Jan. 2007.

[22] M. Baldi, N. Maturo, E. Paolini, and F. Chiaraluce, “On the use of ordered statistic decoding for low-density parity-check codes in space telecommand links,” EURASIP J. Wireless Commun. Netw., vol. 2016, no. 272, Nov. 2016.

[23] C. Choi and J. Jeong, “Fast and Scalable Soft Decision Decoding of Linear Block Codes,” in IEEE Communications Letters, vol. 23, no. 10, pp. 1753-1756, Oct. 2019.

[24] M. Shirvanimoghaddam et al., “Short block-length codes for ultrareliable low latency communications,” IEEE Commun. Mag., vol. 57, no. 2, pp. 130–137, Feb. 2019.

[25] Lizhong Zheng and D. N. C. Tse, “Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels,” in IEEE Transactions on Information Theory, vol. 49, no. 5, pp. 1073-1096, May 2003.

[26] Proakis, J.G., Digital Communication. McGraw-Hill, 2001.

[27] Rose, C. and Smith, M. D., “Mathematical Statistics with Mathematica”. New York: Springer-Verlag, 2002.