Chase Decoding of Linear $\mathbb{Z}_4$ Codes at Low to Moderate Rates

Marc A. Armand, *Senior Member, IEEE*, A. Halim, and A. Nallanathan, *Senior Member, IEEE*

***Abstract*— A free $\mathbb{Z}_4$ code $\mathcal{C}$ may be decoded by decoding its canonical image $\overline{\mathcal{C}}$ over $\mathbb{Z}_2$ twice in succession. Hence, a Chase decoder for $\mathcal{C}$ could employ as its hard-decision (HD) decoder, a two-stage decoder which performs HD decoding on $\overline{\mathcal{C}}$ in each stage. Alternatively, one could have a two-stage soft-decision decoder by employing a Chase decoder for $\overline{\mathcal{C}}$ in each stage. We demonstrate that the latter approach can offer a significant reduction in complexity over the other, with little or no price to pay in terms of word error rate performance, particularly at low to moderate code rates.**

***Index Terms*— BCH codes, Chase decoding, $\mathbb{Z}_4$ codes.**

I. Introduction

CHASE decoding [2] is a suboptimal decoding technique which can provide substantial coding gains over conventional hard-decision (HD) decoding with significant reduction in decoding complexity compared to maximum-likelihood decoding. Of particular interest to coding theorists are techniques enabling a Chase decoder to employ fewer test patterns with little sacrifice in performance – see e.g. [1], [3]. In [4], the word error rate (WER) performance of Chase decoding when applied to a t-error correcting, free[1] (n, k) $\mathbb{Z}_4$ code $\mathcal{C}$ of design distance $2t+1$ on an AWGN channel with QPSK modulation, was investigated. The HD decoder considered there was a two-stage decoder based on the algorithm in [6, Section III] where each stage was a conventional (errors-only) HD decoder acting on the canonical image $\overline{\mathcal{C}}$ of $\mathcal{C}$ over $\mathbb{Z}_2$, as depicted in Fig. 1(a). It was shown that with such a HD decoder, a Chase decoder utilizing about 2^{t-1} test patterns can yield a better WER over one that uses a conventional HD decoder and 2^t test patterns.

An alternative, and obvious, way of realizing Chase-like decoding of the code $\mathcal{C}$ is to employ in each stage of the algorithm in [6, Section III], a Chase decoder for $\overline{\mathcal{C}}$, as depicted in Fig. 1(b), with each Chase decoder employing a conventional HD decoder. It is however *not* obvious whether this alternative approach offers any advantage over the Chase decoder advocated in [4]. Indeed, no insight is offered there in this regard. The purpose of this letter is therefore to fill that void. Specifically, we demonstrate that the latter approach can offer a significant reduction in complexity over the other, with little or no price to pay in terms of WER performance, particularly at low to moderate code rates.

Manuscript received May 21, 2007. The associate editor coordinating the review of this letter and approving it for publication was Prof. Marc Fossorier.

The authors are with the Communications & Information Engineering Group, Department of Electrical & Computer Engineering, National University of Singapore (email: eleama@nus.edu.sg).

Digital Object Identifier 10.1109/LCOMM.2007.070821.

[1]From [5, Corollary 4.7(i)], if there is a linear $\mathbb{Z}_4$ code which is not free, there exists a free $\mathbb{Z}_4$ code of the same length and minimum Hamming distance but of higher rate. For this reason, it suffices to limit our study to free codes.

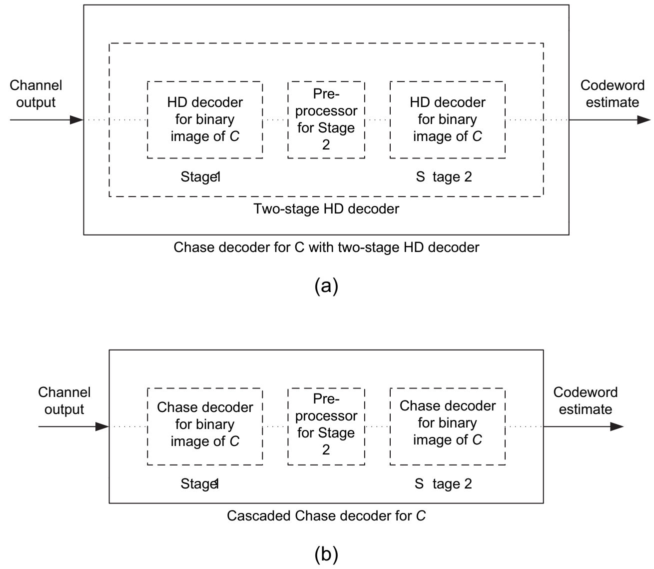

Fig. 1. (a) The Chase decoder with two-stage HD decoder; (b) the cascaded Chase decoder.

Henceforth, we refer to the decoders depicted in Fig. 1(a) and 1(b) as the non-cascaded Chase decoder (NCD) and cascaded Chase decoder (CCD), respectively. We proceed with a more detailed description of the CCD.

II. The CCD

A. Decoder Description

Consider encoding the message block $\mathbf{m}$ as the codeword $\mathbf{v} := \mathbf{mG}$ of $\mathcal{C}$ where $\mathbf{G}$ is a generator matrix for the code. Writing the 2-adic expansions of $\mathbf{m}$, $\mathbf{v}$ and $\mathbf{G}$ as $2\mathbf{m}_1 + \mathbf{m}_0$, $2\mathbf{v}_1 + \mathbf{v}_0$ and $2\mathbf{G}_1 + \mathbf{G}_0$, respectively, one readily sees that $\mathbf{v}_0 = \mathbf{m}_0 \odot \mathbf{G}_0 \in \overline{\mathcal{C}}$ while $\mathbf{v}_1 = \mathbf{m}_0 \odot \mathbf{G}_1 \oplus \mathbf{m}_1 \odot \mathbf{G}_0 \in \mathbb{Z}_2^n$ where $\odot$ and $\oplus$ denote the respective operations over $\mathbb{Z}_2$.

Suppose $\mathbf{v}$ is QPSK modulated such that each pair $(v_{j,1}, v_{j,0})$ is mapped to the signal point given by $(2v_{j,1} - 1, 2v_{j,0} - 1)$ and then transmitted, where $\mathbf{v}_0 := (v_{1,0}, \ldots, v_{n,0})$ and $\mathbf{v}_1 := (v_{1,1}, \ldots, v_{n,1})$. Evaluating the sign of the corresponding $2n$ unquantized detector outputs $(r_{1,1}, r_{1,0}, r_{2,1}, r_{2,0}, \ldots, r_{n,1}, r_{n,0})$ yields the HD received word $\mathbf{h} := (h_{1,1}, h_{1,0}, h_{2,1}, h_{2,0}, \ldots, h_{n,1}, h_{n,0}) \in \mathbb{Z}_2^{2n}$. It is convenient to define $\mathbf{r}_0 := (r_{1,0}, \ldots, r_{n,0})$, $\mathbf{r}_1 := (r_{1,1}, \ldots, r_{n,1})$, $\mathbf{h}_0 := (h_{1,0}, \ldots, h_{n,0})$ and $\widetilde{\mathbf{h}} := (\widetilde{h}_1, \ldots, \widetilde{h}_n) \in \mathbb{Z}_4^n$ such that the 2-adic expansion of $\widetilde{h}_j$ is $2h_{j,1} + h_{j,0}$.

Now, let $\{\mathbf{e}_{1,j}, \ldots, \mathbf{e}_{2^{s_j},j}\}$ be a set of 2^{s_j} binary test patterns of length n and Hamming weight at most s_j where the ones are restricted to the s_j least reliable positions in $\mathbf{r}_j$. For each i, $1 \le i \le 2^{s_0}$, the first Chase decoder of the

CCD computes $\mathbf{h}_0 \oplus \mathbf{e}_{i,0}$ and feeds it to a (conventional) HD decoder[2] which outputs an estimate $\hat{\mathbf{v}}_0 := (\hat{v}_{1,0}, \ldots, \hat{v}_{n,0})$ of $\mathbf{v}_0$. The output $\hat{\mathbf{v}}_0^*$ of the first Chase decoder is the estimate $\hat{\mathbf{v}}_0$ of $\mathbf{v}_0$ that maximizes the correlation $-\sum_{j=1}^{n}(-1)^{\hat{v}_{j,0}} r_{j,0}$ between $\mathbf{r}_0$ and the modulated version of $\hat{\mathbf{v}}_0$. This completes the description of the first decoding stage of the CCD.

Next, denote by $\hat{\mathbf{m}}_0^*$, the message corresponding to $\hat{\mathbf{v}}_0^*$. The task of the pre-processor for the second decoding stage indicated in Fig. 1(b) is to compute $\mathbf{h}_1 := (\widetilde{\mathbf{h}} - \hat{\mathbf{m}}_0^* \mathbf{G} - (\mathbf{h}_0 \oplus \hat{\mathbf{v}}_0^*))/2 \in \mathbb{Z}_2^n$ where $-$ here denotes subtraction over $\mathbb{Z}_4$. Following [6, Step i in Section III], $\mathbf{h}_1$ is the hard-decision "received word" to be fed to the HD decoder in the second Chase decoder after modification by the $\mathbf{e}_{i,1}$'s. That is, for each i, $1 \le i \le 2^{s_1}$, the second Chase decoder computes $\mathbf{h}_1 \oplus \mathbf{e}_{i,1}$ and feeds it to a HD decoder which outputs an estimate $\hat{\mathbf{m}}_1 \odot \mathbf{G}_0$ of $\mathbf{m}_1 \odot \mathbf{G}_0 \in \overline{\mathcal{C}}$. The output $\hat{\mathbf{m}}_1^* \odot \mathbf{G}_0$ of the second Chase decoder is the estimate $\hat{\mathbf{m}}_1 \odot \mathbf{G}_0$ that maximizes $-\sum_{j=1}^{n}(-1)^{\hat{v}_{j,1}} r_{j,1}$ where $(\hat{v}_{1,1}, \ldots, \hat{v}_{n,1}) := \hat{\mathbf{m}}_0^* \odot \mathbf{G}_1 \oplus \hat{\mathbf{m}}_1 \odot \mathbf{G}_0$. The estimate of $\mathbf{m}$ computed by the CCD is therefore given by $2\hat{\mathbf{m}}_1^* + \hat{\mathbf{m}}_0^*$.

Hereafter, take CCD(s_0, s_1) to mean the CCD employing 2^{s_0} and 2^{s_1} test patterns in the first and second stage, respectively. The complexity of CCD(s_0, s_1) will be measured in terms of the *total* number of test patterns used, or equivalently, the total number of calls made to the HD decoder for $\overline{\mathcal{C}}$.

B. Choice of s_0 and s_1

Turning our attention now to choosing s_0 and s_1, observe that errors of values 1 and 3 are "visible" to the first decoding stage of the CCD while errors of values 2 and 3 are "visible" to the second. Thus, a reasonable choice of value for s_0/s_1 is the ratio of the average number of errors of values 1 and 3, to the average number of errors of values 2 and 3, in $\widetilde{\mathbf{h}}$. Assuming transmission on an AWGN channel with QPSK modulation and all codewords are equally likely, we therefore have from [4],

$$\frac{s_0}{s_1} \approx \frac{n}{n + 2^{-k} B'(1)}$$

where $B'(x)$ is the first-order derivative of the weight enumerator of $\overline{\mathcal{C}}$ with respect to x.

Now, it is well-known that among the three versions of the Chase decoder in [2], the second one, i.e., [2, Algorithm 2], has the best performance/complexity trade-off and utilizes 2^t test patterns. For this reason, we fix

$$s_1 = t \tag{1}$$

and in turn,

$$s_0 = \left[\frac{nt}{n + 2^{-k} B'(1)}\right] \tag{2}$$

where $[\cdot]$ denotes rounding-off to the nearest integer.

It is interesting to note that codes whose canonical images over $\mathbb{Z}_2$ satisfy $B'(1) = 2^{k-1} n$ do exist. Indeed, the codes used in our computer simulations all have this property. In this case, with s_0 and s_1 as specified by (1) and (2), the complexity of CCD(s_0, s_1) is therefore about $2^{2t/3} + 2^t$. On the other hand, the NCD(t), i.e., the NCD employing 2^t test patterns, incurs 2^{t+1} calls[3] to its HD decoder for $\overline{\mathcal{C}}$. Thus, for sufficiently large t, e.g. $t > 9$, the complexity of CCD(s_0, s_1) is close to half of that of NCD(t).

We next present our simulation results which focus on this special case.

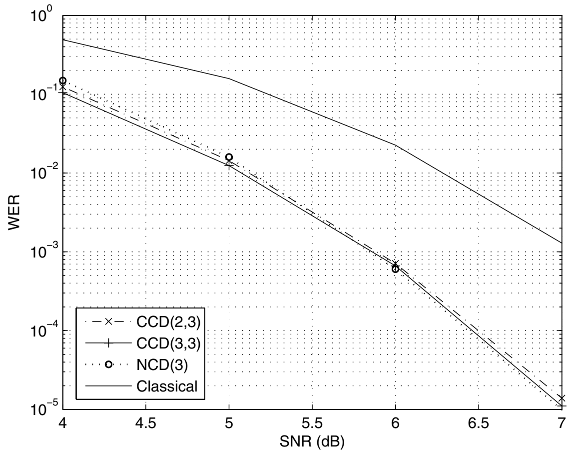

Fig. 2. WER's of CCD$(s_0, 3)$ and NCD(3) when applied to $(63, 45)$ BCH code for $s_0 = 2, 3$.

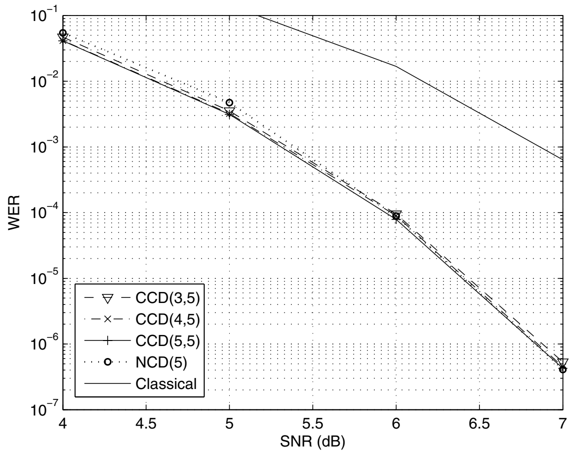

Fig. 3. WER's of CCD$(s_0, 5)$ and NCD(5) when applied to $(63, 36)$ BCH code for $s_0 = 3, 4, 5$.

III. Simulation Results

We begin by comparing the WER performance of CCD$([2t/3], t)$ and NCD(t) on an AWGN channel with QPSK modulation. Three codes whose canonical images over $\mathbb{Z}_2$ satisfy $B'(1) = 2^{k-1} n$ are considered, namely, a $(63, 45)$, $(63, 36)$ and $(63, 24)$ BCH code, for which t is $3, 5$ and 7, respectively.

From Figs. 2 and 3, we see that for the high and moderate rate codes, NCD(t) performs better than CCD$([2t/3], t)$ in the

[2]Since $\mathcal{C}$ is free, $\overline{\mathcal{C}}$ is consequently a linear code over $\mathbb{Z}_2$. Hence, decoding $\overline{\mathcal{C}}$ need not be a hard task as compared to the problem of decoding a nonlinear binary code.

[3]Note that for the NCD, each test pattern leads to two calls to the HD decoder for $\overline{\mathcal{C}}$. Therefore, for a fair comparison to be made between the complexity of CCD and that of NCD, we measure the complexity of NCD in terms of the number of calls made to the HD for $\overline{\mathcal{C}}$, rather than the number of test patterns used.

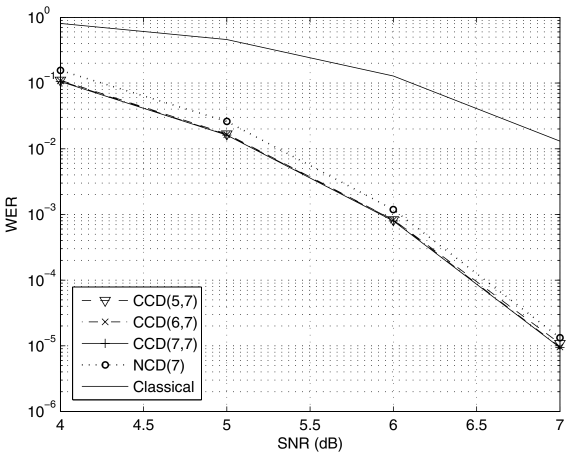

Fig. 4. WER's of CCD$(s_0, 7)$ and NCD(7) when applied to $(63, 24)$ BCH code for $s_0 = 5, 6, 7$.

WER region of practical interest although only marginally, particularly for the latter code. From Fig. 4 however, we see that for the low rate code, CCD$([2t/3], t)$ performs better than NCD(t) over the entire SNR range considered. On the other hand, the complexity of CCD$([2t/3], t)$ is only 75% (respectively, 62.5%) that of NCD(t) for the high rate code (respectively, moderate and low rate codes).

The WER performance of CCD(s_0, t) for $[2t/3] < s_0 \leq t$ is also given so that additional comparisons can be made between the two decoders. Observe that CCD(t, t) and NCD(t) have the same complexity. Thus as s_0 increases, the reduction in complexity that CCD(s_0, t) offers over NCD(t) diminishes.

Not surprisingly, as Figs. 2 to 4 show, the performance of CCD(s_0, t) improves as s_0 increases. In particular, Fig. 3 shows that for the moderate rate code, CCD$(t-1, t)$ and NCD(t) essentially have identical performance in the WER region of practical interest. The complexity of the former decoder however is only 75% that of the other.

IV. Concluding Remarks

Through our computer simulations, we have demonstrated that for codes whose canonical images over $\mathbb{Z}_2$ satisfy $B'(1) = 2^{k-1}n$, CCD(s_0, t) can offer a significant reduction in complexity over NCD(t) for $[2t/3] \leq s_0 < t$, with little or no price to pay in terms of WER performance (within the WER region of practical interest at least), particularly at low to moderate rates. It would be interesting to see if CCD(s_0, t) will continue to offer similar performance/complexity tradeoffs in cases where $B'(1) \neq 2^{k-1}n$.

Finally, we note that there are obviously several ways to further improve the performance of CCD(s_0, s_1). One way is for the first decoding stage to pass a list of two or more codeword estimates to the second stage, instead of just one. However, we have found that the performance improvements this approach brings is too small to warrant the corresponding large increase in complexity.

Acknowledgement

The authors gratefully acknowledge financial support from the Singapore's Ministry of Education's AcRF Tier 1 grant number R-263-000-361-112. The authors would also like to thank the anonymous referees for their useful comments which helped improve the quality of this Letter.

References

[1] G. Arico and J. H. Weber, "Limited-trial Chase decoding," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2972–2975, Nov. 2003.

[2] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 170–182, Jan. 1972.

[3] J. H. Weber and M. P. C. Fossorier, "Limited-trial Chase-like algorithms achieving bounded-distance decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3318-3323, Dec. 2004.

[4] M. A. Armand, "Chase decoding of linear $\mathbb{Z}_4$ codes," *Electronics Lett.*, vol. 42, no. 18, pp. 1049–1051, Aug. 2006.

[5] G. H. Norton and A. Sălăgean, "On the Hamming distance of linear codes over a finite chain ring," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 1060–1067, May 2000.

[6] M. Greferath and U. Velbinger,"Efficient decoding of $\mathbb{Z}_{p^k}$-linear codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1288–1291, May 1998.