TR-82-014

Soft decision decoding based on the combinatorial structures of linear codes —— Generalized minimum distance decoding on majority logic decodable codes*

by

T. Y. Hwang

* This work was sponsored by National Council Grant NSC71-0404-E001-01

September 1982

Abstract

Generalized minimum distance decoding schemes are found for majority logic decodable codes. These decoding schemes are parallel to the classical majority logic decoding schemes and thus can be easily implemented.

I. Introduction

Majority logic decoding [1] - [3] can be very simply implemented; hence, it is attractive from a practical point of view. However, majority logic decoding is basically a hard decision decoding scheme and thus inherits information loss caused by the symbol-by-symbol hard decision quantization. It would be nice to have soft decision decoding schemes for majority logic decodable codes which not only avoid degradation performance but also preserve decoder's simplicity.

Generalized minimum distance(GMD) decoding, on the other hand, is a soft decision decoding scheme which provides asymptotically optimum performance over an additive white Gaussian noise(AWGN) channel [4]. This decoding scheme was not designed for any special class of codes. Therefore it did not try to utilize specific combinatorial structures of block codes to reduce the decoding complexity.

Recently, works have shown that soft decision decoding schemes do exist for majority logic decodable codes [5], [6]. The algebraic analog decoding(AAD) proposed by Rudolph et al [5] adopts a special class of demodulation functions and by which the decoders constructed will have complexities the same as their hard decision counterpart. The performance of AAD, when it does maximum-radius decoding, is conjectured to be equivalent to that of GMD decoding [7]. Yu and Costello [6] showed two decoding algorithms for completely orthogonalizable codes on Qary output channels. Both algorithms achieve GMD decoding and maintain simple implementations.

In this paper, we shall see that the idea of GMD decoding can be easily applied to all majority logic decodable codes, which include 1-step orthogonalizable codes, L-step orthogonalizable codes, and codes using nonorthogonal parity checks. The decoding schemes presented parallel to that of AAD and majority logic decoding, thus have complexities almost the same. By this it again demonstrates that combinatorial structures of block codes can help to reduce decoding complexity, even in soft decision decoding.

II Preliminaries

Consider an (n,k,d) linear binary code C over $\{0,1\}^n$ and let the transmitted version of code word $\underline{c} = (c_1, c_2, \ldots, c_n) \in C$ be $\underline{c}^* = (c_1^*, c_2^*, \ldots, c_n^*)$, where $c_i^* = (-1)^{c_i}$. Thus C* is over $\{+1,-1\}^n$ and the group $\{C, \oplus\}$ is isomorphic to $\{C^*, \times\}$, where $\oplus$ denotes modulo 2 addition and $\times$ denotes component-by-component multiplication.

The received word $\underline{r} = (r_1, r_2, \ldots, r_n)$ is the real sum of $\underline{c}^*$ and an error vector $\underline{e} = (e_1, e_2, \ldots, e_n)$, $e_i \in R$. Assume all the words of C* are equiprobable of being sent and the channel is time-discrete memoryless. Define the bit log likelihood ratio of r_i to be

$$\phi_i = \ell n \left[\frac{P_r(r_i \mid 1)}{P_r(r_i \mid -1)} \right], \quad i = 1,2,\ldots,n,$$

where $P_r(r_i \mid x)$ denotes the probability of r_i given x, x = 1 or -1. Then $\underline{\phi} = (\phi_1, \phi_2, \ldots, \phi_n)$ is the channel measurement information vector of $\underline{r}$. Any decoding method that finds a code word $\underline{c}^*$ which maximizes $\underline{\phi} \cdot \underline{c}^*$ performs maximum likelihood decoding [8].

Let T, a positive number, be some threshold [4] and

$$\alpha_i = \begin{cases} +1, & \text{if } T \le \phi_i \\ \phi_i / T, & \text{if } -T \le \phi_i \le T, \\ -1, & \text{if } \phi_i \le -T, \end{cases} \quad i = 1,2,\ldots,n.$$

Thus, except for the hard-limiting at each end, the bit log likelihood ratios are preserved in $\underline{\alpha}$. Assume α_M is a component in $\underline{\alpha}$ which has the largest absolute value. If $\alpha_M \neq 0$, $\underline{\alpha}$ can be redefined as

$$\underline{\beta} = \underline{\alpha}/|\alpha_M| = (\alpha_1/|\alpha_M|, \alpha_2/|\alpha_M|, \ldots, \alpha_n/|\alpha_M|).$$

Now the ith component of $\underline{\beta}$ satisfies $-1 \leq \beta_i \leq 1$, $1 \leq i \leq n$, and at least one component of $\underline{\beta}$ has its absolute value equal to 1.

Now consider the case where the dual code C' of C has parity checks which satisfy a combinatorial constraint. Suppose there are J parity checks, each checking the first bit position and at most λ of the checks checking any other bit position. Let the J parity checks be

$$\underline{c}'_1 = (c'_{11}, c'_{12}, \ldots, c'_{1n})$$
$$\underline{c}'_2 = (c'_{21}, c'_{22}, \ldots, c'_{2n})$$
$$\vdots$$
$$\underline{c}'_J = (c'_{J1}, c'_{J2}, \ldots, c'_{Jn})$$

where $c'_{j1} = 1$ and $c'_{ji} \in \{0,1\}$ for all $1 \leq j \leq J$ and $1 \leq i \leq n$. Let $\lambda_i = \sum_{j=1}^{n} c'_{ji}$ for $i = 2,3,\ldots,n$. Then $\lambda = \max\{\lambda_2, \lambda_3, \ldots, \lambda_n\}$. Also let $s = \lfloor (J + \lambda)/\lambda \rfloor$, where $\lfloor x \rfloor$ denotes the greatest integer equal to or less than x. Since $d \geq s$ [9], we can prove the following theorem.

Theorem 1. For any received $\underline{\beta}$, there exists at most one code word $\underline{c}^*$ such that

$$\underline{\beta} \cdot \underline{c}^* > n - s . \qquad (1)$$

(Proof) Theorem 1 can be proved by using the same argument given by Forney [4].

Q.E.D.

We note here that when s = d, any decoding method which successfully finds this $\underline{c}^*$(if it exists) is credited with doing GMD decoding.

Suppose there exists a code word which does satisfy(1) and we denote it as $\underline{c}_m^*$. Define $\underline{z} = (z_1, z_2, \ldots, z_n)$ by letting

$$z_i = \begin{cases} +1, & \text{if } \beta_i > 0, \\ -1, & \text{if } \beta_i \leq 0, \end{cases} \qquad i = 1,2,\ldots,n.$$

Then since $|\beta_i| \leq 1$ for all $1 \leq i \leq n$, we have following lemmas.

Lemma 1. $\underline{z} \times \underline{c}_m^*$ have at most s - 1 components which are less than or equal to zero.

Lemma 2. The sum of any s or more components in $\underline{\beta} \times \underline{c}_m^*$ is greater than zero.

The proofs of these lemmas are obvious and are thus omitted.

Let $T = \{i_1, i_2, \ldots, i_t\}$ be a set of t indices such that $\beta_{i_\ell} c^*_{m i_\ell} \leq 0$, $1 \leq \ell \leq t$. Then $0 \leq t \leq s - 1$ by Lemma 1.

Also let $T' = \{j_1, j_2, \ldots, j_{s-t}\}$ be the set of s-t indices such that for a $j_\ell \in T'$, $\beta_{j_\ell} c^*_{mj_\ell}$ is among the s-t smallest components within the n-t positive components of $\underline{\beta} \times \underline{c}^*_m$. Obviously the intersection of T and T' is empty and, by Lemma 2 we have

$$\mathbb{X} \equiv \sum_{j \in T'} \beta_j c^*_{mj} + \sum_{i \in T} \beta_i c^*_{mi} > 0 .$$

It is clear that $\mathbb{X}$ is the smallest value that the sum of any s or more components of $\underline{\beta} \times \underline{c}^*_m$ can have.

Let $\gamma_j = \min_{2 \le i \le n} \left(|\beta_i| c^j_i \right)$ for $j = 1,2,\ldots,J$, with the convention the $a^0 = 1$ for any real a. Now we are able to provide the results in the following.

III. Main Result

Let

$$F_1(\underline{\beta}) = \lambda \beta_1 + \sum_{j=1}^{J} \gamma_j \prod_{i=2}^{n} z_i^{c^j_i} . \qquad (2)$$

It is seen that there are $J + \lambda$ terms in (2) and any z_i as well as β_1 appear less than or equal to λ times in (2). Define

Decision Rule I :

$$\hat{c}^*_1 = \begin{cases} 1 , & \text{if } F_1(\underline{\beta}) > 0 \\ -1 , & \text{otherwise.} \end{cases}$$

$\hat{a}$ denotes an estimate of a. We can now prove the following

Theorem 2. If $\underline{\beta} \cdot \underline{c}^*_m > n - s$, then Decision Rule I gives $\hat{c}^*_1 = c^*_{m1}$.

(Proof) We shall show that $c^*_{m1}F_1(\underline{\beta}) > 0$ whenever (1) is true. From (2) we have

$$c^*_{m1}F_1(\underline{\beta}) = \lambda\beta_1 c^*_{m1} + \sum_{j=1}^{J} \gamma_j c^*_{m1} \prod_{i=2}^{n} z_i^{c'_{ji}} \quad . \qquad (3)$$

Since $\underline{c}' \in C'$, $\underline{c} \cdot \underline{c}' = 0$ (modulo 2),

$$c^*_{m1} = \prod_{i=2}^{n} (c^*_{mi})^{c'_{ji}} \quad , \quad \text{for } j = 1,2,\ldots,J,$$

and we may rewrite (3) as

$$c^*_{m1} F_1(\underline{\beta}) = \sum_{i=1}^{\lambda} |\beta_1| z_1 c^*_{m1} + \sum_{j=1}^{J} \gamma_j \prod_{i=2}^{n} (z_i c^*_{mi})^{c'_{ji}} . \qquad (4)$$

There are $J + \lambda \geq s\lambda$ terms in the right hand side of (4) and by Lemma 1 at most $t\lambda$ terms are less than or equal to zero. Since $t \leq s - 1$, at least λ terms in the right hand side of (4) are greater than zero. Therefore we can arrange (4) to have

$$c^*_{m1}F_1(\underline{\beta}) = \sum_{\ell=1}^{\lambda} \left(|\beta_1| \, z_1 c^*_{m1} + \sum_{j \in L_\ell} \gamma_j \prod_{i=2}^{n} (z_i c^*_{mi})^{c'_{ji}} \right)$$

$$\equiv \sum_{\ell=1}^{\lambda} X_\ell$$

where $L_\ell \subset \{1, 2, \ldots, \lambda\}$, $|L_\ell| \geq s - 1$, $\bigcup_{\ell=1}^{\lambda} L_\ell = \{1, 2, \ldots, \lambda\}$, and $L_i \cap L_j = \phi$ for all $1 \leq i, j \leq \lambda$. A set L_ℓ is chosen such that for all s or more terms summed into X_ℓ, at most $t \leq s - 1$ of them are less than or equal to zero.

According to the definition of γ_j, it is easily seen that X_ℓ is the sum of s or more distinct components in $\underline{\beta} \times \underline{c}^*_m$. So by Lemma 2 we have $X_\ell \geq X > 0$ for all $1 \leq \ell \leq \lambda$ and thereby $c^*_{m1}F_1(\underline{\beta}) > 0$.

Q.E.D.

We illustrate the proof of Theorem 2 by an example.

Example. Consider the (7,4) binary Hamming code. Let

$$\underline{c}'_1 = (1\ 1\ 1\ 0\ 1\ 0\ 0)$$
$$\underline{c}'_2 = (1\ 1\ 0\ 1\ 0\ 0\ 1)$$
$$\underline{c}'_3 = (1\ 0\ 1\ 0\ 0\ 1\ 1)$$
$$\underline{c}'_4 = (1\ 0\ 0\ 1\ 1\ 1\ 0) .$$

In this case J = 4 and $\lambda = 2$. So s = 3 and we have $t \leq 2$. Suppose $\underline{\beta}$ = (0.92,1,0.21,-0.6,-0.98,-0.95,1). Then there

exists a code word $\underline{c}_m^* = (1\ 1\ -1\ 1\ -1\ -1\ 1)$ such that $\underline{\beta} \cdot \underline{c}_m^* > n - s$. By definition, we find that $\gamma_1 = 0.21$, $\gamma_2 = 0.6$, $\gamma_3 = 0.21$, and $\gamma_4 = 0.6$. Inspecting (4) we can group the terms in (4) as following,

$$c_{m1}^* F_1(\underline{\beta}) = \left(|\beta_1| z_1 c_{m1}^* + \gamma_1 \prod_{i=2}^{n} (z_i c_{mi}^*)^{c'_{1i}} + \gamma_2 \prod_{i=2}^{n} (z_i c_{mi}^*)^{c'_{2i}} \right)$$

$$+ \left(|\beta_1| z_1 c_{m1}^* + \gamma_1 \prod_{i=2}^{n} (z_i c_{mi}^*)^{c'_{3i}} + \gamma_2 \prod_{i=2}^{n} (z_i c_{mi}^*)^{c'_{4i}} \right)$$

$$= 2(0.92 - 0.21 - 0.6) > 0 .$$

So $\hat{c}_1^* = 1$ which is a correct estimate.

Corollary 1. A 1-step orthogonalizable code can be GMD decoded.

The proof of Corollary 1 can be shown by noting that it is possible to find $J = d - 1$ parity checks orthogonal on the first bit position and $\lambda = 1$ for other positions. A same result has been found in [6, Theorem 6] from a different approach.

We now extend this result to L-step orthogonalizable codes. Let d be the minimum distance of an L-step orthogna-lizable code and let

$$\underline{c}_1' = (c_{11}', c_{12}', \ldots, c_{1n}')$$
$$\underline{c}_2' = (c_{21}', c_{22}', \ldots, c_{2n}')$$
$$\vdots \qquad\qquad \vdots$$
$$c_{d-1}' = (c_{d-1,1}', c_{d-1,2}', \ldots, c_{d-1,n}')$$

be the set of d - 1 parity checks orthogonal on positions $1, p_1, p_2, \ldots, p_u$. Let $P = \{p_1, p_2, \ldots, p_u\}$,

$$\gamma_{1P} = \min_{i \in P} (|\beta_1|, |\beta_i|),$$

and

$$\gamma_j = \min_{\substack{i \notin P \\ i \neq 1}} (|\beta_i|^{c'_{ji}}), \quad j = 1, 2, \ldots, d-1.$$

Let

$$F_{1P}(\underline{\beta}) = \gamma_{1P} z_1 \prod_{i \in P} z_i + \sum_{j=1}^{d-1} \gamma_j \prod_{\substack{i \notin P \\ i \neq 1}} z_i^{c'_{ji}}.$$

Define

Decision Rule Π :

$$\overset{\frown}{c_1^* \prod_{i \in P} c_i^*} = \begin{cases} 1, & \text{if } F_{1P}(\underline{\beta}) > 0 \\ -1, & \text{otherwise.} \end{cases}$$

Then we have the following corollary.

Corollary 2. If $\underline{\beta} \cdot \underline{c}_m^* > n - d$, then Decision Rule Π gives

$$\overset{\frown}{c_1^* \prod_{i \in P} c_i^*} = c_{m1}^* \prod_{i \in P} c_{mi}^*.$$

The proof of Corollary 2 parallels the proof of Theorem 2 and is thus omitted.

If $\underline{\beta} \cdot \underline{c}_m^* > n - d$, then by Corollary 2

$$F_{1P}(\underline{\beta})c^*_{m1}\prod_{i\in P} c^*_{mi} > 0 . \qquad (5)$$

Now note that

$$F_{1P}(\underline{\beta})\prod_{i\in P} z_i = F_{1P}(\underline{\beta})(c^*_{m1}\prod_{i\in P} c^*_{mi})^2\prod_{i\in P} z_i$$

$$= (F_{1P}(\underline{\beta})c^*_{m1}\prod_{i\in P} c^*_{mi})(c^*_{m1}\prod_{i\in P} c^*_{mi}z_i).$$

By (5), we have that if $\underline{\beta}\cdot\underline{c}^*_m > n-d$, then

$$\text{sign}\left(F_{1P}(\underline{\beta})\prod_{i\in P} z_i\right) = \text{sign}\left(c^*_{m1}\prod_{i\in P} c^*_{mi}\, z_i\right).$$

Since $\underline{\beta}\cdot\underline{c}^*_m > n-d$, we can have at most $d-1$ positions which satisfy $z_i c^*_{mi} \le 0$. Therefore, if we can next find $2d-2$ checks orthogonal on a linear combination of positions $q_1, q_2, \ldots, q_v$, where the set $Q = \{q_1, q_2, \ldots, q_v\} \subset P$, then we can correctly estimate sign $[c^*_{m1}\prod_{i\in Q} c^*_{mi}z_i]$. If it is possible to carry out this procedure for the remaining steps of the decoding procedure —— each time determining at least $2d-2$ orthogonal parity checks —— until a set of parity checks orthogonal on the first position is obtained, then c^*_{m1} will be correctly estimated. We have thus proved the following result.

Corollary 3. An L-step orthogonalizable code can be GMD decoded using the disjoint checks provided that the subcode to be decoded at the second step is $(L-1)$-step orthogonalizable with minimum distance at least $2d-1$.

IV. Conclusion

It has been shown that generalized minimum distance decoding schemes exist for majority logic decodable codes. These decoding schemes utilize the combinatorial structures of majority logic decodable codes and can be very easily implemented. So they are attractive from a practical point of view. Further, it is worth to note that the iterative extension proposed for AAD [5] can also find application here. Though the probability of word error will never be increased by iteration, it is also found that the iterative extension will not always lead to maximum likelihood decoding, even if a sufficient number of iterations were allowed.

The existence of soft decision decoding shemes for majority logic decodable codes, and especially these decoding schemes are parallel to their hard decision counterpart, naturally instigates a question. That is, for all other linear block codes which have simple hard decision decoders, can we construct their parallel soft decision decoders ? There is no answer yet at this moment, we wish more work could appear in the future.

References

1. I. S. Reed, "A class of multiple error-correcting codes and the decoding scheme," IRE Trans. Inform. Theory, vol.IT-4, pp.38-49, Sept. 1954.
2. J. L. Massey, Threshold Decoding, Cambridge, Mass., M.I.T. Press, 1963.
3. L. D. Rudolph, "A class of majority logic decodable codes," IEEE Trans. Inform. Theory, vol.IT-13, pp.305-307, April 1967.
4. G. D. Forney, Jr., "Generalized minimum distance decoding," IEEE Trans. Inform. Theory, vol.IT-12, pp.125-131, April 1966; also Concatenated Codes, Cambridge, Mass., M.I.T. Press, 1966.
5. L. D. Rudolph, C. R. P. Hartmann, T. -Y. Hwang, and N. Q. Duc, "Algebraic analog decoding of linear binary codes," IEEE Trans. Inform. Theory, vol.IT-25, pp.430-440, July 1974.
6. C. C. H. Yu and D. J. Costello, Jr., "Generalized minimum distance decoding algorithms for Qary output channels," IEEE Trans. Inform. Theory, vol.IT-26, pp.238-243, March 1980.
7. T. -Y. Hwang, "On the error-correcting capability of algebraic analog decoding," IEEE Trans. Inform. Theory, vol.IT-26, pp.107-109, Jan. 1980.
8. T. -Y. Hwang, "Decoding linear block codes for minimizing

9. S. W. Ng, "On Rudolph's majority-logic decoding algorithm," IEEE Trans. Inform. Theory, vol.IT-16, pp.651-652, Sept. 1970.