Transactions Letters

Modified Majority Logic Decoding of Cyclic Codes in Hybrid-ARQ Systems

Michael D. Rice and Stephen B. Wicker

Abstract—**Reliability information provided by sets of orthogonal check sums in a majority logic decoder for block codes is used in a type-I hybrid ARQ error control scheme. The reliability information is obtained through a simple modification of the majority logic decoding rule. It is shown that the reliability performance of Reed–Muller and other majority logic decodable codes can be substantially improved at the expense of a very small reduction in throughput. The simplicity of the decoding circuit enables implementation in systems with very high data rates.**

I. Introduction

In traditional automatic-repeat-request (ARQ) schemes, codes are used for error detection in conjunction with a retransmission request protocol [1]. A received word whose syndrome is nonzero generates a request for a retransmission of that word and no attempt at error correction is made. Forward-error-correction (FEC) schemes use the information contained in the syndrome to find the nearest codeword to the received word no matter how many errors may have occurred. In such a complete decoding scheme, retransmission is not an option. In general, a given (n, k) linear block code can detect at least twice as many errors per received word as it can correct using complete decoding. Therefore the probability of a "decoding error" occurring in an FEC protocol is greater than that of an "undetected error" in an ARQ protocol [2]. A given code can thus provide higher reliability in an ARQ scheme than in an FEC scheme. The increased reliability is obtained at the expense of throughput. In FEC schemes the throughput remains constant while in an ARQ scheme it decreases as the channel degrades.

Hybrid-ARQ schemes combine the positive features of both FEC and ARQ schemes, providing high reliability at the expense of a modest reduction in throughput. In a type-I hybrid-ARQ protocol [1], error correction is used to correct only the most common error patterns while those patterns most likely to cause decoder errors generate a retransmission request. Such schemes may be derived from the FEC decoding algorithms through the identification of "reliability information" which is used to determine if the received word can be decoded reliably. These concepts have been applied successfully to the implementation of convolutional codes in type-I hybrid-ARQ systems. Decoding time [3] and metric growth rate [4] have been identified as sources of reliability information in sequential decoders. Similarly, reliability information derived from the metrics used in Viterbi decoders has been developed by Harvey and Wicker [5] and Yamamoto and Itoh [6]. Wicker [7] also used the extent of the majority in a set of orthogonal check sums as the source of reliability information in majority logic decoding of convolutional codes.

In this paper, the use of *block* codes in a type-I hybrid-ARQ system is investigated. In particular, the majority logic decoder is reviewed and modified. The extent of the majority in a set of orthogonal check sums provides the source of reliability information. This reliability information is used to determine when a retransmission request should be issued for the word being decoded. Performance bounds for this system are derived and simulation results are included to test the tightness of the bounds. While the class of codes for which majority logic decoding is optimal is relatively small, majority logic decoders are suitable for implementation at significantly higher data rates than most block decoding algorithms.

II. Modification of the Majority Logic Decoder

Majority logic decoding implements a voting scheme among a set of check sums orthogonal on a bit or subset of error bits. The *majority logic decoding rule* is defined for a set of J check sums orthogonal on error bit e_j as follows [8]:

> Let the estimate $\hat{e}_j$ of error bit e_j be the value assumed by the majority of the J check sums. In the case of a tie, let $\hat{e}_j = 0$.

The majority logic decoding rule guarantees a correct estimate of e_j as long as there are no more than $\lfloor \frac{J}{2} \rfloor$ errors among the error bits being checked. It is clear that for a block code with minimum distance $d_{\min}$, majority logic decoding will be optimal when $J = d_{\min} - 1$. In such a case, the code is said to be *completely orthogonalizable* [8].

The J orthogonal check sums provide reliability information that can be used in a hybrid-ARQ scheme. In general, the greater the number of check sums which agree, the higher the reliability of the estimate. The lack of an extensive majority among the J orthogonal check sums can be used to generate a retransmission request.

Let η be the number of orthogonal check sums which have a value of "1" and let the *retransmission threshold* τ

Paper approved by the Editor for Coding and Applications of the IEEE Communications Society. Manuscript received June 20, 1989; revised December 13, 1990. This paper was presented at the 1990 IEEE International Conference on Communications, Atlanta, GA, April 16–19, 1990.

M. D. Rice is with the Department of Electrical Engineering, Brigham Young University, Provo, UT 84601.

S. B. Wicker is with the School of Electrical Engineering, Georgia Institute of Technology, Atlanta, GA 30332.

IEEE Log Number 9201522.

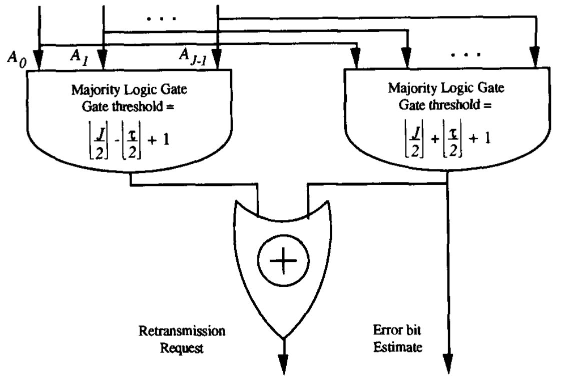
A_0
A_1
A_{J-1}
Majority Logic Gate
Gate threshold =
$\left\lfloor \frac{J}{2} \right\rfloor - \left\lfloor \frac{\tau}{2} \right\rfloor + 1$
Majority Logic Gate
Gate threshold =
$\left\lfloor \frac{J}{2} \right\rfloor + \left\lfloor \frac{\tau}{2} \right\rfloor + 1$
Retransmission Request
Error bit Estimate

Fig. 1. General modification of the estimation circuitry for use of majority logic decoders in hybrid-ARQ systems.

be an integer less than J. A *retransmission region* is defined such that a retransmission is requested by the majority logic decoder whenever the number of ones among the J check sums satisfies

$$\left\lfloor \frac{J}{2} \right\rfloor - \left\lceil \frac{\tau}{2} \right\rceil < \eta < \left\lfloor \frac{J}{2} \right\rfloor + \left\lfloor \frac{\tau}{2} \right\rfloor + 1. \qquad (1)$$

A *modified* majority logic decoding rule can now be defined for a set of J check sums orthogonal on error bit e_j:

Let the error estimate $\hat{e}_j$ of error bit e_j be

$$\begin{cases} 0 & \text{if } \eta \leq \lfloor \frac{J}{2} \rfloor - \lceil \frac{\tau}{2} \rceil \\ 1 & \text{if } \eta \geq \lfloor \frac{J}{2} \rfloor + \lfloor \frac{\tau}{2} \rfloor + 1 \end{cases}$$

otherwise request a retransmission.

By following the modified majority logic decoding rule, a receiver will decode the most frequently occurring error patterns, i.e., those corresponding to a large majority of the orthogonal check sums being in agreement, and generate a retransmission request for the less likely, more difficult patterns. For $\tau \neq 0$, the decoder has been modified to be a $(\lfloor \frac{J}{2} \rfloor - \lceil \frac{\tau}{2} \rceil)$—error correcting $(\lfloor \frac{J}{2} \rfloor + \lceil \frac{\tau}{2} \rceil)$—error detecting decoder. A type-I hybrid ARQ protocol is thus defined [1]. Note that for $\tau = 0$ the modified majority logic rule is equivalent to the FEC majority logic decoding rule.

Fig. 1 illustrates the general modification of the majority logic decoder needed to implement the hybrid-ARQ error control scheme. The modification can be made to the final state (consisting of a single majority logic gate using the J check sums $A_0, A_1, \cdots, A_{J-1}$) in an L-step decoder or to the final majority logic estimation circuit in any of the variations of majority logic decoding [9]. Note that the additional circuitry is not complex and permits the use of a hybrid-ARQ scheme in systems with extremely high data rates.

III. Performance

In a majority logic decoder, each received word is decoded on a bit by bit basis. The reliability information is used to determine when a retransmission of a received word should be requested. When the number of check sums with a value of "1" satisfies (1), a retransmission of the entire word is requested by the decoder. Thus for each received word, three probabilities are used to describe the performance of the decoder [9]:

$P_c =$ the probability that the received word contains a correctable error pattern;

$P_r =$ the probability that the received word contains a detectable (but not correctable) error pattern;

$P_u =$ the probability that the received word contains an undetectable error pattern.

Since a retransmission is requested by the receiver any time a received word contains a detectable but noncorrectable error pattern, P_r represents the probability of retransmission.

The performance of an ARQ scheme is usually measured by two parameters: reliability and throughput [1]. The reliability is defined by the probability of an error event $P(E)$ which occurs when the receiver accepts a word which contains errors. It is given by [9]

$$P(E) = \frac{P_u}{1 - P_r}. \qquad (2)$$

The throughput is defined as the expected value of the number of information bits accepted per transmitted bit. In the case of the FEC scheme, the throughput is just the code rate $\frac{k}{n}$. In a hybrid-ARQ error control scheme, retransmissions cause a reduction in the throughput efficiency which can be represented by the introduction of a multiplicative factor. There are three basic retransmission protocols: stop-and-wait, go-back-N, and selective-repeat [1]. Each of these protocols reduce the throughput to varying degrees by introducing different multiplicative factors. For the selective-repeat protocol, the throughput with probability of retransmission P_r is [1]

$$\begin{aligned} \nu_{\text{SR}} &= \frac{k/n}{[(1 - P_r) + 2P_r(1 - P_r) + 3P_r^2(1 - P_r) + \cdots]} \\ &= \frac{k}{n}(1 - P_r). \end{aligned} \qquad (3)$$

In this section an upper bound for the probability of undetected error P_u for the unmodified decoder is derived. This bound is then altered to yield a similar bound for the modified decoder in a hybrid-ARQ scheme. A tight upper bound for the probability of retransmission is also derived from which a lower bound on the throughput is obtained.

Probability of Undetected Error

Consider an (n, k) cyclic code with J checksums orthogonal on error bit e_{n-1}. (Whether the J check sums are derived directly from the syndrome of the received word or from other sets of check sums orthogonal on subsets of error bits is unimportant here. The performance bounds will be the same.) As long as there are $\lfloor \frac{J}{2} \rfloor$ or fewer errors present in the received word, majority logic decoding will be error-free. There are two possible ways a decoding error can occur.

1) $e_{n-1} = 0$ and $\lfloor \frac{J}{2} \rfloor + 1$ or more of the J checksums are 1. This is caused by $\lfloor \frac{J}{2} \rfloor + 1$ of the other $n - 1$ error bits checked by the check sums being 1.

2) $e_{n-1} = 1$ and $\lfloor \frac{J}{2} \rfloor$ or more of the J checksums are 0 which is caused by $\lceil \frac{J}{2} \rceil$ or more of the other $n - 1$ error bits checked by the check sums being 1.

The above describes an upper bound since it assumes that all of the errors are arranged in the worse possible fashion so as to generate a decoding error. Hence, the probability of decoder error may be bounded above as follows:

$$\begin{aligned} P_u &\leq P\left\{\geq \left\lfloor \frac{J}{2} \right\rfloor + 1 \text{ errors}\right\} P\{e_{n-1} = 0\} \\ &\quad + P\left\{\geq \left\lceil \frac{J}{2} \right\rceil \text{ errors}\right\} P\{e_{n-1} = 1\} \\ &= (1-p) \sum_{l=\lfloor \frac{J}{2} \rfloor + 1}^{n-1} \binom{n-1}{l} p^l (1-p)^{n-l-1} \\ &\quad + p \sum_{l=\lceil \frac{J}{2} \rceil}^{n-1} \binom{n-1}{l} p^l (1-p)^{n-l-1} \qquad (4) \end{aligned}$$

for a binary symmetric channel with transition probability p.

In the hybrid-ARQ modification, the number of errors necessary to cause a decoding error is increased since decoding is only attempted when a large majority of the check sums are in agreement. For the case when e_{n-1} is actually 0, the decoder makes a decoding error when η satisfies

$$\eta \geq \left\lfloor \frac{J}{2} \right\rfloor + \left\lfloor \frac{\tau}{2} \right\rfloor + 1.$$

Such an occurrence is caused by $\lfloor \frac{J}{2} \rfloor + \lfloor \frac{\tau}{2} \rfloor + 1$ or more errors among the other bits. For the case when e_{n-1} is actually 1, a decoding error occurs when η satisfies

$$\eta \leq \left\lfloor \frac{J}{2} \right\rfloor + \left\lceil \frac{\tau}{2} \right\rceil.$$

This requires $J - (\lfloor \frac{J}{2} \rfloor - \lceil \frac{\tau}{2} \rceil) = \lceil \frac{J}{2} \rceil + \lceil \frac{\tau}{2} \rceil$ or more errors. The upper bound (4) is accordingly altered to represent the upper bound for the probability of error for the modified decoder *on a given transmission:*

$$\begin{aligned} P_u &\leq (1-p) \sum_{l=\lfloor \frac{J}{2} \rfloor + \lfloor \frac{\tau}{2} \rfloor + 1}^{n-1} \binom{n-1}{l} p^l (1-p)^{n-l-1} \\ &\quad + p \sum_{l=\lceil \frac{J}{2} \rceil + \lceil \frac{\tau}{2} \rceil}^{n-1} \binom{n-1}{l} p^l (1-p)^{n-l-1}. \qquad (5) \end{aligned}$$

B. Probability of Retransmission

A retransmission is requested by the decoder if at any time during the decoding of a received word the number of orthogonal check sums having a value of "1" satisfies

$$\left\lfloor \frac{J}{2} \right\rfloor - \left\lceil \frac{\tau}{2} \right\rceil < \eta < \left\lfloor \frac{J}{2} \right\rfloor + \left\lfloor \frac{\tau}{2} \right\rfloor + 1.$$

Thus, some patterns of $\lfloor \frac{J}{2} \rfloor - \lceil \frac{\tau}{2} \rceil + 1$ or more errors present in the received word will generate a retransmission request. The probability of retransmission is bounded by

$$P_r \leq \sum_{l=\lfloor \frac{J}{2} \rfloor - \lceil \frac{\tau}{2} \rceil + 1}^{n-1} \binom{n-1}{l} p^l (1-p)^{n-l-1}. \qquad (6)$$

This bound, which assumes a worst case distribution of the errors, is tight for most completely orthogonalizable block codes. During the decoding process, those patterns of $l \geq \lfloor \frac{J}{2} \rfloor - \lceil \frac{\tau}{2} \rceil + 1$ errors which do not cause the generation of a retransmission request are cyclically shifted with the received word in the decoder. Eventually, this error pattern will be shifted into a position which will cause the generation of a retransmission request if fewer than $l - \lfloor \frac{J}{2} \rfloor + \lceil \frac{\tau}{2} \rceil$ of the errors in that pattern have already been corrected. The number of l-error patterns which do not cause the generation of a retransmission request depends on the particular distribution of the checked error bits in the set of check sums being used. However, this number is small compared to the number of patterns which do cause retransmissions. Hence, the bound (6) is a good one. Simulation results supporting this argument are shown in Section V.

Using (5) and (6) in equation (2) creates an upper bound on the probability of decoder error while using (6) in (3) forms a lower bound on the throughput for the selective repeat protocol.

IV. Applicable Codes

There are several small classes of 1-step majority logic decodable binary cyclic codes:

- *Doubly Transitive Invariant (DTI) Codes:* These are comparable to BCH codes in efficiency for short block length [9]. For example, the (63,37) DTI code can correct 4 errors with a single level majority logic circuitry. The corresponding 4-error correcting BCH code of the same length is a (63,39) code, which requires a more complex decoding circuit.
- *Binary Maximal Length Codes [9, 8]:* These are $(2^m - 1, m)$ codes (for $m \geq 3$) with $d_{\min} = 2^{m-1}$.
- *Difference Set Codes:* These are based on the construction of a perfect simple difference set of order p^s where p is a prime number and s is a positive integer [9]. They are $(2^{2s} + 2^s + 1, 2^{2s} + 2^s - 3^s)$ codes with $d_{\min} = 2^s + 2$.
- The (15,7) 2-error correcting BCH code.

Generalization of the majority logic decoding principle to L steps of orthogonalization enlarges the class of binary cyclic codes which can be decoded efficiently. The classes of cyclic codes which are L-step majority logic decodable are

- The following BCH codes, which can be completely orthogonalized in 2 steps [9, 8]:
  1) the 3-error correcting (31,16) code
  2) the 3-error correcting (63,45) code
  3) the 7-error correcting (63,24) code
  4) the $(2^{m-2} - 1)$–error correcting $(2^{m-1} - 1, m+1)$ codes.
- Several large classes of codes based on Euclidean Geometry [9]. For example, rth-order cyclic Reed–Muller Codes, a special case of EG codes, are completely orthogonalizable in $(r+1)$ steps [2]. Many other EG codes are completely orthogonalizable [10].
- Many Projective Geometry Codes (see [9, ch.8] for a

small list). Difference set codes and maximal length codes are special cases of PG codes.

An improvement to the majority logic decoding algorithm which can reduce the number of steps required for complete orthogonalization of EG and PG codes which are completely orthogonalizable is described in [11].

The above list contains only binary codes. Weldon [11] outlines a majority logic decoding scheme for nonbinary codes. The codes for which majority logic decoding would be efficient are difficult to determine. The following theorem gives a necessary condition for L-step decoding of a linear (n, k) block code [11].

Theorem 1: Let d' be the minimum distance of the dual of a linear (n, k) code. The number of errors which can be corrected by L-step majority logic decoding t_L satisfies the bound

$$t_L \le \frac{n - \left\lfloor \frac{d'}{2} \right\rfloor}{2\left\lceil \frac{d'}{2} \right\rceil}. \qquad (7)$$

Proof: Since each null space vector must contain at least d' nonzero digits, each check sum orthogonal on a set of B error digits must contain at least d' error digits. $B \le \frac{d'}{2}$; for if not, the null space vector which is the difference of two of the vectors corresponding to the difference of two of the check sums orthogonal on the set of B error digits would contain fewer than d' nonzero digits.

If J check sums can be formed, then $n - B \ge J(d' - B)$ from which it follows that

$$n - \left\lfloor \frac{d'}{2} \right\rfloor \ge J\left(d' - \left\lfloor \frac{d'}{2} \right\rfloor\right) = J\left\lceil \frac{d'}{2} \right\rceil.$$

Since $t_L = \left\lfloor \frac{J}{2} \right\rfloor$,

$$t_L \le \frac{n - \left\lfloor \frac{d'}{2} \right\rfloor}{2\left\lceil \frac{d'}{2} \right\rceil}.$$

Q.E.D.

Note in the above that for 1-step majority logic decoding, $B = 1$ and

$$t_1 \le \frac{n - 1}{2(d' - 1)}. \qquad (8)$$

The theorem shows, unfortunately, that majority logic decoding is not an efficient way to decode MDS codes and thus precludes the use of majority logic decoding for the more powerful nonbinary codes.

V. Simulation Results

The performance of three codes was simulated in the type-I hybrid-ARQ scheme: the (31, 16) 2nd-order 3-error correcting Reed–Muller code, the (63, 37) 4-error correcting DTI code, and the (73, 45) 4-error correcting difference set code. A binary symmetric channel was simulated with a selective repeat retransmission protocol. Figs. 2–4 illustrate the computed upper bound[1] for the decoder performance of these codes for various values of the threshold τ.

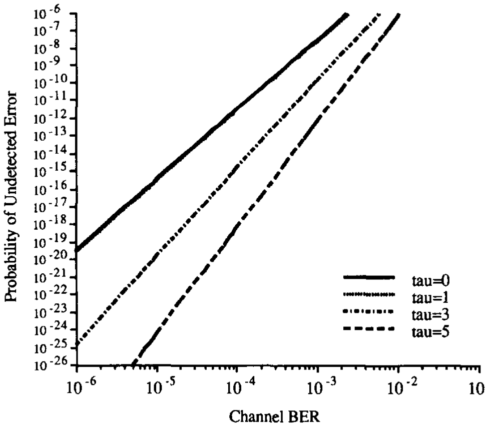

Fig. 2. Computed upper bound on reliability for the (31, 16) Reed–Muller code.

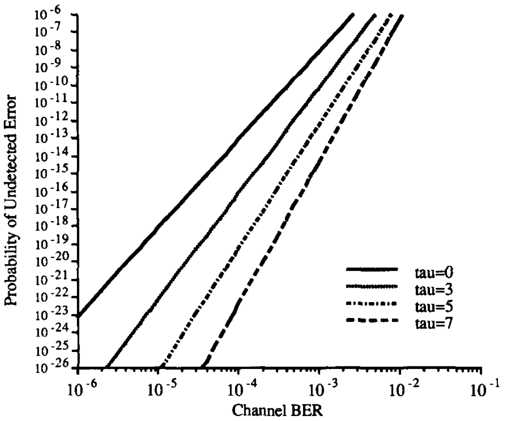

Fig. 3. Computed upper bound on reliability for the (63, 37) DTI code.

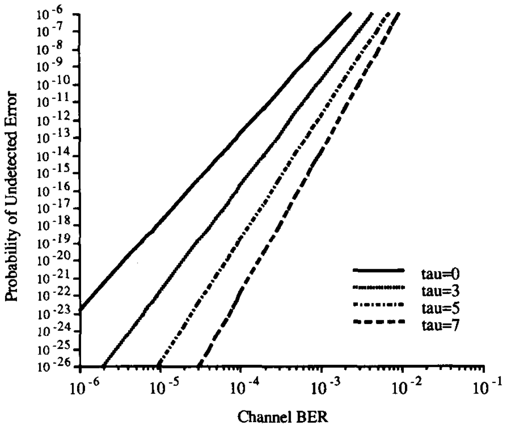

Fig. 4. Computed upper bound on reliability for the (73, 45) difference set code.

[1] Equation (2) using (5) and (6).

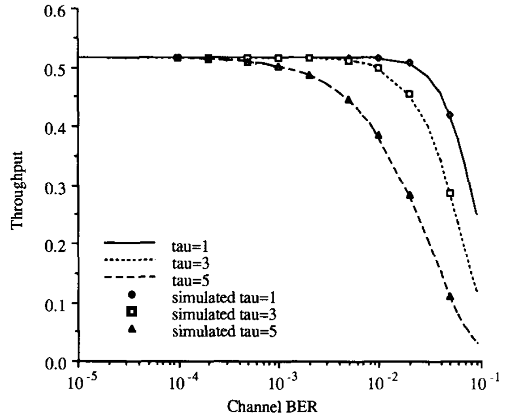

Fig. 5. Throughput performance for the (31, 16) Reed–Muller code.

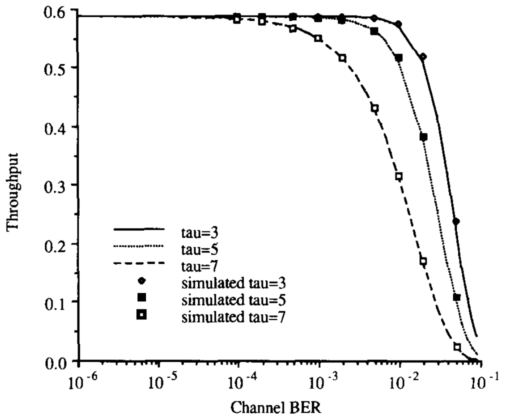

Fig. 6. Throughput performance for the (63, 37) DTI code.

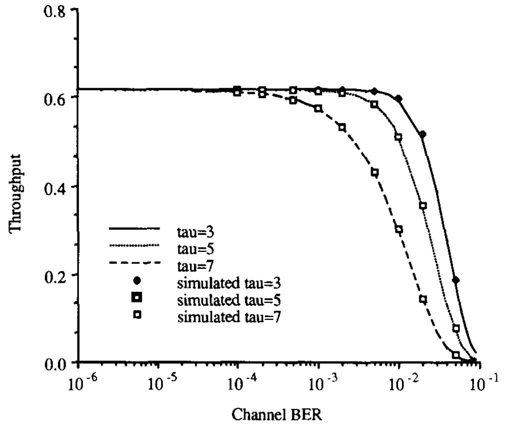

Fig. 7. Throughput performance for the (73, 45) difference set code.

The simulated throughput curves for the three codes are shown in Figs. 5–7. The computed lower bound[2] for the throughput has been included for reference. Note that the lower bound is extremely tight, coinciding closely with the simulation results. Figs. 2–7 illustrate the tradeoff between reliability and throughput. The relationship of this tradeoff to the retransmission threshold can also be seen. For values of τ greater than 1, a substantial improvement in reliability is realized for raw channel bit error rates up to 10^{-2}. Increasing τ, however, sharpens the reduction in throughput for channel bit error rates above 10^{-3}. At channel bit error rates below 10^{-4}, the reduction in throughput is negligible even for large values of the retransmission threshold.

VI. Conclusion

The modification of the FEC block majority logic decoder for use in a type-I hybrid-ARQ system substantially improves the error control performance of the decoder. For raw channel bit error rates up to 10^{-2}, the reliability of the modified decoder is many orders of magnitude greater than that of the unmodified decoder. This improvement is achieved only for values of the retransmission threshold τ greater than 1. Increasing the retransmission threshold improves reliability significantly, but it also causes a sharp reduction in throughput at raw channel bit error rates above 10^{-3}.

Unfortunately, not all cyclic codes are majority logic decodable. However, majority logic decoding can be implemented with simple circuitry which enables the use of this decoding technique at significantly higher data rates than is possible with other decoding techniques. Hence, those codes which are majority logic decodable provide a powerful means of error control for high rate data communication systems.

[2] Equation (3) using (6).

References

[1] S. Lin, D. J. Costello, Jr., and M. J. Miller, "Automatic-repeat-request error control schemes," *IEEE Commun. Mag.*, vol. 22, pp. 5–17, Dec. 1984.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* New York: Elsevier Science, 1977.

[3] R. E. Kahn, S. A. Gronemeyer, J. Burchfiel, and R. E. Kunzelman, "Advances in paclet radio technology," *Proc. IEEE*, vol. 66, pp. 1468–1497, Nov. 1978.

[4] A. Drukarev and D. J. Costello, Jr., "Hybrid ARQ error control using sequential decoding," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 521–535, July 1983.

[5] B. A. Harvey and S. B. Wicker, "Error-trapping Viterbi decoding for type-I hybrid-ARQ protocols," *Canadian J. Elect. Comput. Eng.*, vol. 16, no. 1, pp. 5–12, Jan. 1991.

[6] H. Yamamoto and K. Itoh, "Viterbi decoding algorithm for convolutional codes with repeat request," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 540–547, Sept. 1980.

[7] S. B. Wicker, "Modified majority-logic decoders for use in convolutionally encoded hybrid-ARQ systems," *IEEE Trans. Commun.*, vol. 38, pp. 263–266, Mar. 1990.

[8] J. L. Massey, *Threshold Decoding.* Cambridge, MA: M.I.T. Press, 1963.

[9] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1983.

[10] C. R. P. Hartmann, J. B. Ducey, and L. D. Rudolph, "On the structure of generalized finite geometry codes," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 240–252, Mar. 1974.

[11] E. J. Weldon, Jr., "Some results on majority logic decoding," *Error Correcting Codes*, H. B. Mann. New York: Wiley, 1968.