6

ON HEADER FORWARD ERROR CONTROL IN ATM SYSTEMS

Andreas Rieke[1] and Hans-Jürgen Zepernick[2]

[1] *Forschungsinstitut für Telekommunikation*
Martin-Schmeißer-Weg 4, 44227 Dortmund, Germany
[2] *Cooperative Research Centre for*
Broadband Telecommunications and Networking
GPO Box U1987, Perth, WA 6001, Australia

1. INTRODUCTION

In modern telecommunication systems and computer network applications the Asynchronous Transfer Mode (ATM) promises to achieve service independence, flexibility in adaptation of future services and efficient use of resources [1].

Because of channel noise and other impairments, error control techniques are commonly used to achieve communication services of satisfactory quality. Concerning the ATM physical layer functions, shortened cyclic codes are defined for error detection and correction [2]. Especially, an 8-bit shortened cyclic code is used for protecting the ATM header.

Stimulated by a particular formulation of a question on cryptology and an autonomous investigation on error control in ATM based mobile radio, this paper presents a general performance analysis of header forward error control in ATM systems by shortened cyclic codes. We compare the error control performance of the standardized header code with various shortened cyclic codes as well as performance achievable on different classes of transmission channels. The performance is assessed in terms of random-error-control capability, burst-error-control capability and undetected error probability. The results show options for an efficient utilization of redundancy in ATM systems.

The outline of the paper is as follows. In Section 2, a review of cyclic codes and the standardized ATM header is given along with the channel models and performance characteristics employed. The exhaustive search method and the automata approach used for performance analysis are contained in Section 3. Numerical results comparing the performance of several shortened cyclic codes are presented in Section 4. Finally, Section 5 summarizes the paper.

2. SYSTEM DESCRIPTION AND PROBLEM FORMULATION

2.1 Cyclic Codes

Cyclic codes are often used for error control purposes in digital communication systems and can be easily implemented by shift register circuits. A cyclic code is a linear block code possessing the property that every cyclic shift of a codeword is also a codeword. For an (n, k) cyclic code V_0, k information bits are encoded into an n bit codeword. The number of parity check bits introduced is $m = n - k$. Usually, a binary cyclic code is defined by a generator polynomial

$$g(x) = g_m \cdot x^m + \cdots + g_1 \cdot x^1 + g_0; \qquad g_\mu \in GF(2). \tag{1}$$

To avoid trivial cases, we suppose that the coefficients g_m and g_0 are nonzero.

Using polynomial representations, encoding of a cyclic code in so-called systematic form can be written as

$$u(x) \quad = \quad x^m \cdot i(x) + R_{g(x)}[x^m \cdot i(x)], \tag{2}$$

where $i(x) = \sum_{\kappa=0}^{k-1} i_\kappa x^\kappa$; $i_\kappa \in GF(2)$ and $u(x) = \sum_{\nu=0}^{n-1} u_\nu x^\nu$; $u_\nu \in GF(2)$ represent the information and codeword, respectively, and $R_{g(x)}[\cdot]$ denotes the remainder of $[\cdot]$ upon division by $g(x)$.

A codeword $u(x)$ transmitted through the channel may be corrupted by an error word $e(x)$ and transformed into a received word $v(x)$. We assume an additive error process, i.e. $v(x) = u(x) + e(x)$. At the receiving end a decoder tests whether $v(x)$ is a codeword by computing the syndrome $s(x) = R_{g(x)}[v(x)]$. If the all-zero syndrome is obtained, the received word is assumed to be the transmitted codeword. Otherwise, an error word is detected and an error-correcting algorithm may be applied.

The natural code length n of a cyclic code often exceeds the given block format of a particular application. An adaptation on such a constraint can be achieved by shortening the given cyclic code, where a finite number of higher significant information bits are defined to be zero.

2.2 Standardized ATM Header Error Control and Alternatives

In ATM systems a data packet is denoted as cell. An ATM cell consists of a 5-octet header and 48-octet payload. The header is divided into several fields, each field having a separate control function. The 5^{th} byte in the header is designated the Header Error Control (HEC) field. The polynomial taken to compute the HEC is standardized by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to be

$$g_{ITU}(x) = (x+1)(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) = x^8 + x^2 + x + 1. \quad (3)$$

In the ATM physical layer functions there are two modes of error control established. These are the detection mode and the correction mode. In the detection mode the code is used for error detection only whereas in the correction mode a single bit error will be corrected.

Although the HEC is defined by (3) other choices are practicable. Concerning the capability to detect or correct a number t of random errors or detect a burst error of given length b, a set of generator polynomials of same degree can solve the task. If the stochastic properties of a channel are taken into consideration, the performance of competitive shortened cyclic codes are not solely determined by their fundamental parameters but also by the actual structure of codewords and can differ significantly. Therefore, it seems to be promising to undertake a thorough and comparative performance assessment of the complete set of binary cyclic codes shortened to ATM header length and based on generator polynomials of the form

$$g(x) = \sum_{\mu=0}^{8} g_\mu \cdot x^\mu, \qquad g_\mu \in GF(2). \quad (4)$$

2.3 Channel Models

We distinguish between bit errors and burst errors. Corresponding to bit errors, we are simply interested in particular error patterns. This is in contrast to our burst error model, which inherently allows for a rough channel model. The two error types are defined as follows:

Bit error:	A bit error affects a single bit in a block of length n. Bit errors are statistically independent.
Burst error:	Errors occur only within a span of length b (Figure 1). Errors within that span occur randomly with a bit error probability of 50%. End-around burst errors are not considered.

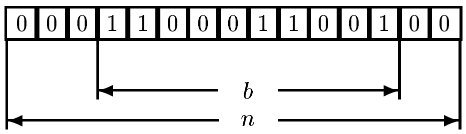

Figure 1 Burst error structure (b: length of a burst; n: block length)

In order to compute the exact performance of a cyclic coded system under less restrictive conditions compared to the error types defined above, we employ generative stochastic channel models. These mathematical models are able not only to characterize the error patterns caused by a realistic channel but also to generate typical error sequences. Here, we focus on the Gilbert-Elliott channel (GEC). The GEC is modeled by a two-state Markov model. It consists of a good state G and a bad state B. State transitions between the states G and B are specified by the transition probabilities $P = Prob(B|G)$ and $Q = Prob(G|B)$, respectively. In state G bit errors occur with a low bit error probability p_G while the bit error probability p_B assigned to state B is relatively high. The average bit error rate is given by $\overline{p}_b = Q/(P+Q) \cdot p_G + P/(P+Q) \cdot p_B$.

2.4 Performance Characteristics

We consider an (n, k) cyclic code V_0 over $GF(2)$ defined by a generator polynomial $g(x)$ of degree m. Let d_{min} be the minimum distance of V_0. Then, a fundamental characterization of code performance is given by its error-control capability. The error-detecting and error-correcting capability of a linear block code are defined as the maximum number e_{max} and t_{max} of guaranteed detectable/correctable errors per word, respectively, and are given by [3]

$$e_{max} = d_{min} - 1 \quad \text{and} \quad t_{max} = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor, \tag{5}$$

where $\lfloor x \rfloor$ represents the largest integer not to exceed x. The relationship between the numbers e and t for simultaneous error detection and correction per codeword can be expressed as [3]

$$e = d_{min} - t - 1, \quad \text{where} \quad t \leq t_{max}. \tag{6}$$

In addition, assuming $t = 0$ and a nontrivial generator polynomial $g(x)$ of degree m, such a cyclic code is capable to detect all single bursts of length [3]

$$b \quad \leq \quad b_{max} = m. \tag{7}$$

Based on the fundamental parameters e, b, and t, we aim to further assess the error-control capability in terms of the following probabilities:

$P_{bit}(e+\epsilon,t)$: Probability of simultaneous detection of $e+\epsilon$ and correction of t errors per word,

$P_{burst}(b+\beta,t)$: Probability of simultaneous detection of bursts of length $b+\beta$ and correction of t errors per word.

Finally, performance of an error control code can be characterized by rating decoding events, which are correct decoding, erroneous decoding, and error detection. Taking a discrete channel into account, the performance corresponding to these events can be specified by

P_c: Probability of correct decoding,

P_u: Probability of undetected error (undetected error probability),

P_d: Probability of error detection without correction.

2.5 Characterization of Good Polynomials

To identify a subset of good generator polynomials out of a given set of polynomials, we suggest the following four criteria

C1:	$e_{max}+1$	and	$P_{bit}(e_{max}+1,t=0)$,
C2:	$e+1$	and	$P_{bit}(e+1,t=1)$,
C3:	$b_{max}+1$	and	$P_{burst}(b_{max}+1,t=0)$,
C4:	$b+1$	and	$P_{burst}(b+1,t=1)$.

Each criterion classifies the error-control capability provided when the parameters e_{max}, e, b_{max}, or b exceed the guaranteed value by one. Besides these parameters, the probabilities $P_{bit,burst}(\cdot,\cdot)$ or their complements $\overline{P}_{bit,burst}(\cdot,\cdot)$ are taken to quantify the performance under such error conditions.

If only a single criterion has been chosen, a ranking of polynomials can be easily established. Because a polynomial may perform good in respect to a first criterion but bad in a second, it is more difficult to identify a good polynomial when all four criteria are considered. Therefore, we define a good polynomial by its opposite:

> A polynomial is classified as "bad", if there exists a polynomial of the same degree which is better in at least one criterion and not worse in the remaining criteria. A polynomial which is not "bad" is classified as a "good" polynomial.

A set of good polynomials obtained in such a way is going to be verified by computing the related undetected error probability P_u. This allows the inclusion of a more realistic channel model.

3. METHODS USED FOR PERFORMANCE ANALYSIS

3.1 Exhaustive Search

We examine the class of binary cyclic codes generated by a finite set of nontrivial polynomials $g(x)$ of a given degree m. The block length of the codes considered may be shortened to a suitable n. To assess the error-control capability of each code in the set, we employ an exhaustive search method. For both, bit errors and burst errors, a specific subset of the n-dimensional vector space of binary error words is chosen and processed by the decoder.

First, let us consider bit errors. For each code, we generate all N_{bit} possible error words of weight $e+1 = d_{min}-t$ out of n. These patterns are subsequently processed by a decoder. Counting decoder outcomes results in the number N_u of undetected errors. Hence, we are able to approach the desired criteria by

$$P_{bit}(e+1,t) = (N_{bit} - N_u)/N_{bit} \quad , \quad \overline{P}_{bit}(e+1,t) = N_u/N_{bit}. \tag{8}$$

Next, we examine performance in burst errors. Similarly, all N_{burst} bursts of a proper length b are generated and processed by a decoder. Again, by counting events, we obtain the number N_u of undetected bursts. We have

$$P_{burst}(b+1,t) = (N_{burst} - N_u)/N_{burst} \quad , \quad \overline{P}_{burst}(b+1,t) = N_u/N_{burst}. \tag{9}$$

3.2 Modal Analysis of Discrete Systems

The method of modal analysis is based on an automata approach for discrete system modeling. It enables an exact computation of the probabilities rating decoding events, e.g. in terms of the undetected error probability. Because a detailed description of the modal analysis is presented in [4],[5] we restrict ourselves on briefly reviewing relevant aspects used for HEC analysis.

To compute the performance of a block coded system, the cascade of a channel followed by a syndrome decoder are modeled as a compound automaton. A channel is modeled as stochastic automaton and a decoder as deterministic automaton. The compound automaton of the channel-decoder-cascade is considered to be a description in an original domain. It enables on principle the exact calculation of fundamental performance characteristics and is taken as a mathematical system setting. To reduce the computational complexity and storage requirements, which are usually related to the original domain, the analysis task can be transformed into a spectral domain of easier structure. This can be achieved by an examination of the response of the compound automaton on its eigenvectors, which are considered as the modes of the discrete system. Thus, we obtain spectral coefficients which are related to the fundamental performance of the original domain by a Walsh-Hadamard transform.

4. NUMERICAL RESULTS

We present the obtained good polynomials and their performance. Because the header is standardized, we examine shortened $(40, 40-m)$ cyclic codes. Polynomials $g(x)$ of degree $m = 6$,7, and 8 are investigated. Polynomials of degree 6 achieve a minimum distance d_{min} of three, 16 polynomials of degree 7 and 50 polynomials of degree 8 obtain $d_{min} = 4$. These polynomials possess maximum d_{min} for the given length and number of parity bits but are only in part good. First, we use the definition suggested in Section 2.5 to select good polynomials by exhaustive search. Table 1 shows the good polynomials determined.

Table 1 Good polynomials obtained by search compared to ITU-polynomial

polynomial	oct	detection mode				correction mode			
		bit		burst		bit		burst	
		a	b	c	d	e	f	g	h
$x^6+x^4+x^3+x+1$	133	3	1.609	7	0.781	2	61.15	2	20.51
$x^6+x^5+x^3+x^2+1$	155	3	1.609	7	0.781	2	61.15	2	20.51
$x^6+x^5+x^2+x+1$	147	3	1.660	7	0.781	2	63.08	2	10.26
$x^6+x^5+x^4+x+1$	163	3	1.660	7	0.781	2	63.08	2	10.26
$x^7+x^3+x^2+1$	215	4	1.630	8	0.391	3	60.32	3	9.54
$x^7+x^5+x^4+1$	261	4	1.630	8	0.391	3	60.32	3	9.54
$x^7+x^4+x^2+1$	225	4	1.631	8	0.391	3	60.36	3	4.93
$x^7+x^5+x^3+1$	251	4	1.631	8	0.391	3	60.36	3	4.93
$x^7+x^5+x^3+x^2+x+1$	257	4	1.686	8	0.391	3	62.39	4	5.91
$x^7+x^6+x^5+x^4+x^2+1$	365	4	1.686	8	0.391	3	62.39	4	5.91
$x^8+x^5+x^2+1$	445	4	0.752	9	0.195	3	27.81	3	4.93
$x^8+x^6+x^3+1$	511	4	0.752	9	0.195	3	27.81	3	4.93
$x^8+x^7+x^4+x^3+x+1$	633	4	0.760	9	0.195	3	28.14	3	4.61
$x^8+x^7+x^5+x^4+x+1$	663	4	0.760	9	0.195	3	28.14	3	4.61
$x^8+x^6+x^4+x^3+x+1$	533	4	0.773	9	0.195	3	28.58	3	4.28
$x^8+x^7+x^5+x^4+x^2+1$	665	4	0.773	9	0.195	3	28.58	3	4.28
$x^8+x^4+x^3+1$	431	4	0.774	9	0.195	3	28.62	3	2.30
$x^8+x^5+x^4+1$	461	4	0.774	9	0.195	3	28.62	3	2.30
$x^8+x^7+x^5+x^4+x^3+x^2+x+1$	677	4	0.775	9	0.195	3	28.66	3	1.64
$x^8+x^7+x^6+x^5+x^4+x^3+x+1$	773	4	0.775	9	0.195	3	28.66	3	1.64
$x^8+x^6+x^3+x^2+x+1$	517	4	0.779	9	0.195	3	28.83	3	0.33
$x^8+x^7+x^6+x^5+x^2+1$	745	4	0.779	9	0.195	3	28.83	3	0.33
$x^8+x^5+x^4+x^2+x+1$	467	4	0.780	9	0.195	3	28.87	4	7.09
$x^8+x^7+x^6+x^4+x^3+1$	731	4	0.780	9	0.195	3	28.87	4	7.09
x^8+x^6+x+1	503	4	0.782	9	0.195	3	28.95	4	1.52
$x^8+x^7+x^2+1$	605	4	0.782	9	0.195	3	28.95	4	1.52
$x^8+x^4+x^3+x^2+x+1$	437	4	0.812	9	0.195	3	30.04	4	1.01
$x^8+x^7+x^6+x^5+x^4+1$	761	4	0.812	9	0.195	3	30.04	4	1.01
$x^8+x^5+x^4+x^3+x+1$	473	4	0.880	9	0.195	3	32.55	5	2.95
$x^8+x^7+x^5+x^4+x^3+1$	671	4	0.880	9	0.195	3	32.55	5	2.95
$g_{ITU}(x) = x^8+x^2+x+1$	407	4	0.795	9	0.195	3	29.43	3	10.53

a, b, c, d: $e_{max}+1$, $\overline{P}_{bit}(e_{max}+1, t=0)$ in %, $b_{max}+1$, $\overline{P}_{burst}(b_{max}+1, t=0)$ in %,
e, f, g, h: $e+1$, $\overline{P}_{bit}(e+1, t=1)$ in %, $b+1$, $\overline{P}_{burst}(b+1, t=1)$ in %

We obtain a number of 4, 6, and 20 good polynomials of degree $m = 6$, 7, and 8, respectively. The standardized polynomial $g_{ITU}(x)$ does not satisfy the criteria of a good polynomial but is listed to make a comparison. We see that in detection mode all good polynomials provide almost the same random-error-control capability and even equal burst-error-control capability. In correction mode, good polynomials still show similar random-error-control capability but differ significantly in the capability to control bursts. Obviously, $g_{ITU}(x)$ is not the best choice in case of burst errors. Note that always two polynomials, i.e. those which are reciprocal to each other, provide the same performance.

The good polynomials obtained are further assessed by using the method of modal analysis. Since the most spectacular results are expected in burst errors, we focus on that case and employ a GEC to model a bursty channel. The GEC parameters are chosen as follows. The bit error probabilities are $p_G = 10^{-8}$ in state G and $p_B = 0.5$ in state B. The transition probability between B and G is chosen as $Q = 0.5$. The average bit error rate $\overline{p}_b = f(P)$ is taken as variable and controlled by P. By ignoring the mutual dependence of errors and taking the average bit error rate of a GEC to specify an effective binary symmetric channel (BSC), we are able to illustrate the performance of good polynomials in random errors. In Figure 2 and Figure 3, we use octal numbers to represent generator polynomials.

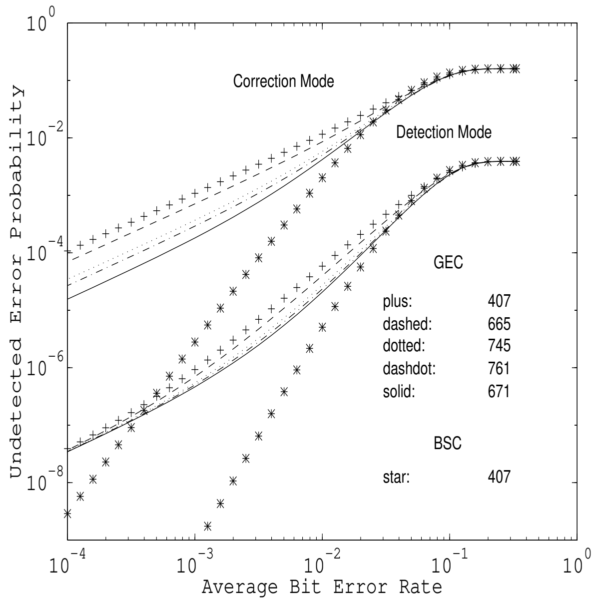

Figure 2 P_u of shortened $(40, 32)$ cyclic codes on GEC and effective BSC

Figure 2 shows the undetected error probability P_u for selected good shortened $(40, 32)$ cyclic codes. The polynomials of degree 8 chosen reflect the ranking of burst-error-control capability in correction mode as indicated in Table 1. For the GEC, we notice a difference in performance not only in the correction mode but also in the detection mode. This is because in nonindependent channel errors the structure of codewords effect the performance, which obviously differs for different generator polynomials. In nice keeping with Table 1, we obtain the same code ranking concerning the capability to combat burst errors. For average bit error rates less than 10^{-3}, the performance of a good polynomial in correction mode outperforms the standardized code up to nearly a factor of ten. In accordance with the results obtained by exhaustive search, there are only minor differences in statistically independent errors as modeled by an effective BSC. Hence, the results for the generator polynomial $g_{ITU}(x)$ are representative. Note that the undetected error probability on the effective BSC is more and more underestimated the lower the average bit error rate.

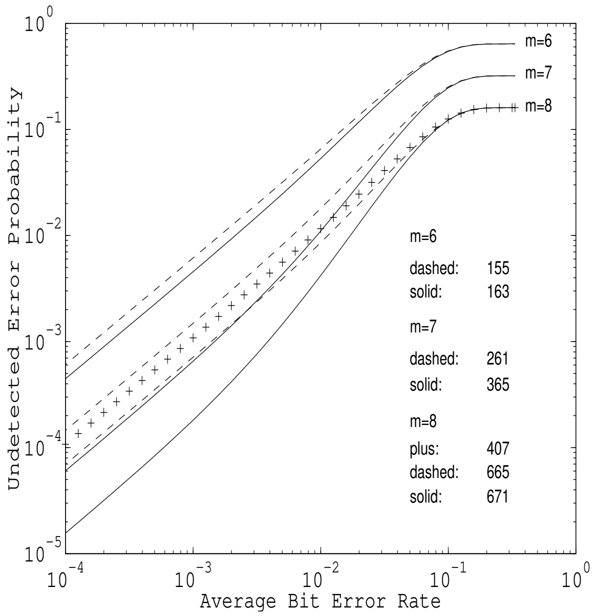

Figure 3 P_u of shortened $(40, 40-m)$ cyclic codes in correction mode on GEC

Figure 3 shows the undetected error probability P_u of shortened $(40, 40-m)$ cyclic codes for degree 6, 7, and 8 in correction mode used on the GEC as specified above. Because of the fixed block length $n = 40$, a generator polynomial of a degree $m < 8$ provides less redundancy to protect a longer information sequence and gives on principle worse performance. Although, for $m = 7$ and

$m = 8$ an interval of overlapping exists in which a polynomial of degree 7 may outperform a polynomial of degree 8. Obviously, the standardized polynomial $g_{ITU}(x)$ could be replaced by a more efficient polynomial of degree 7.

5. SUMMARY

In this paper, we present a performance analysis of header forward error control in ATM systems. We compute the random-error-control and burst-error-control capability of various shortened cyclic codes by means of an exhaustive search strategy. Furthermore, shortened cyclic codes used on discrete channels are examined on the basis of an automata approach and assessed by the undetected error probability. The obtained classification of shortened cyclic codes shows options for an efficient usage of redundancy in ATM system design.

ACKNOWLEDGMENTS

The authors wish to thank Prof. F. Kaderali and their colleagues for helpful discussions. H.-J. Zepernick also wishes to thank Prof. L. Kittel, who introduced him to the modal analysis of discrete systems.

REFERENCES

[1] M. de Prycker; *Asynchronous Transfer Mode - Solution for Broadband ISDN*, Ellis Horwood, New York, 1993, 2nd ed.

[2] ITU-T; *B-ISDN User-Network Interface – Physical Layer Specification. Recommendation I.432*, 1993.

[3] S. Lin and D.J. Costello; *Error Control Coding - Fundamentals and Applications*, Prentice Hall, Englewood Cliffs, 1983.

[4] L. Kittel; *Modal Analysis of Block Coded Transmission Systems with Application to Error Control Performance Evaluation.* ITG-Fachbericht 107, VDE-Verlag GmbH, Berlin 1989, pp. 281-288.

[5] H.-J. Zepernick; *Modal Analysis of Coding Schemes Used on Channels Without and With Memory* (in German), Ph.D. dissertation, University of Hagen, 1994.