Parameter Independent Performance Analysis of Cyclic Codes

Andreas Rieke
University of Hagen
Feithstr. 142, 58084 Hagen, Germany
andreas.rieke@fernuni-hagen.de

Abstract

This paper deals with two different methods of performance analysis of channel coding systems which are both based on exhaustive search. Using cyclic codes with the binary symmetric channel (BSC) and the Gilbert Channel (GC) as examples, the first method, the parameter independent performance analysis, supplies fast and comparable results which are not only valid in certain cases, because the validity area in which the channel parameters may be varied is analytically derived. The second method, the approximately exact analysis, is applicable for concrete problems and leads to lower and upper bounds for well known performance characteristics.

1 Introduction

In case of communication over unreliable channels, coding of information is used in order to achieve better quality. For that reason, performance analysis of channel coding systems is of particular interest. The main purpose of this paper is to provide a performance analysis with the prove that achieved results are valid not only in certain cases, but within a large area in which the channel parameters may be varied.

For example, the Gilbert Channel (GC, [Gil60]) has three parameters that describe the channel. In many other papers, certain values are selected in order to be able to analyze the performance of a system. Often, a single or even two parameters are varied to make the results more general. Unfortunately, often only some parameters are varied and there is usually no statement which parameters may be varied in which intervals without changing the main result of an analysis. In this paper, a new method of analysis, the parameter independent performance analysis which is based on exhaustive search, is introduced and enables a comparative analysis including the determination of the parameter variation area. Additionally, a second method, the approximately exact analysis, is presented. This method is able to specify lower and upper bounds for the probability of undetected errors in case of concrete parameters.

The rest of this paper is structured as follows: In section 2, the channel coding system is described, whereas section 3 describes the channel models. The performance characteristics which are used in this paper are given in section 4, before section 5 deals with the parameter independent performance analysis. The approximately exact analysis is given in section 6. Section 7 shows some numerical results, before section 8 summarizes the paper.

2 Encoder and Decoder

In this paper, cyclic codes are used as an example because both methods of performance analysis are in principle independent of the coding system. Cyclic codes in this paper include not only those codes who have the property to be cyclic, but also shortened cyclic codes.

A cyclic $(n,\ k)$ code with generator polynomial $g(x)$ which is able to correct either t independent errors or a single burst error with maximum length u is considered. The code is able to simultaneously correct and detect errors.

3 Channel Models

In this paper, the well-known binary symmetric channel (BSC) and the generic GC (Gilbert Channel) are used as channel models. An additive error process is assumed.

The GC consists of two states, the so-called good state (G) and the bad state (B). The state transitions are specified by $p = P(B/G)$ and $q = P(G/B)$, respectively. In the good state, no bit errors occur ($r_G = 0$), whereas, in the bad state, errors occur with probability r_B. It is sufficient to consider $0 \leq r_B \leq 0.5$ in this paper. It is further assumed that $0 < p < q \leq 1$, that means the probability of being in the good state is higher than its opposite.

4 Performance Characteristics

Besides well known basic performance characteristics, such as

P_c: Probability of correct decoding,

P_d: Probability of detected error(s) without correction, and

P_u: Probability of undetected error(s),

conditional probabilities are introduced: $P_{c,bit}(g(x), k, t, u/a)$ is the probability that a independent bit errors in a block of length n with a code of k information bits with generator polynomial $g(x)$ which can correct t independent bit errors and a burst of maximum length u are corrected without error. The probabilities $P_{d,bit}$ and $P_{u,bit}$ are derived in the same way, and the sum of the three probabilities is 1.

$P_{c,burst}$=$P_{c,burst}(g(x), k, t, u, r_B/b)$, $P_{d,burst}$ and $P_{u,burst}$ give the conditional probability of correct decoding, detected error(s) and undetected error(s), respectively, in case of a burst of length b, where a burst is defined to consist of bits which are wrong with probability r_B.

5 Parameter Independent Performance Analysis

The parameter independent performance analysis is based on the exhaustive search method which was introduced in [RZ97]. It is of particular interest if the block sizes k and n are given and a generator polynomial $g(x)$ of degree $m = n - k$ which performs well under the actual requirements is searched. In this paper, the parameter independent performance analysis is applied for bit and burst errors.

In case of bit errors, the parameter $a_{u,min}$ denotes the minimum number of independent bit errors that lead to undetected errors after decoding. All combinations of $a_{u,min}$ independent bit errors in the zero codeword are generated; in each case, the decoder decides whether to accept the received word or whether to detect errors. If the received word is accepted with or without correction, the decoder decision is correct if $a \leq t$, but for $a > t$, statements are only possible if $a > u$ since in this case the decoder decision is certainly incorrect. All decoder decisions are counted in the variables $N_{c,bit}$, $N_{d,bit}$ and $N_{u,bit}$ in order to calculate the corresponding probabilities $P_{c,bit}$, $P_{d,bit}$ and $P_{u,bit}$.

A comparison of different codes with the BSC is useful if the probability of more than $a_{u,min}$ errors is negligible. Using $P_{BSC}(n, r, a)$ as the probability of a bit errors in the block of length n, this is fulfilled if $P_{BSC}(n, r, a) \ll P_{BSC}(n, r, a_{u,min})$ for $a_{u,min} < a \leq n$. It can be shown [Rie98] that this is true if

$$r \ll \frac{a_{u,min} + 1}{n + 1}. \tag{1}$$

In case of burst errors, $b_{u,min}$ is the minimum length of burst errors which lead to undetected errors. All possibilities of inserting bursts of length $b_{u,min}$ into the zero codeword are analyzed; depending on the decoder decision, one of the counters $N_{c,burst}$, $N_{d,burst}$ and $N_{u,burst}$ is increased by the weighting which depends on the bit error probability r_B in the burst. Depending on the number of correct decodings, detected errors and undetected errors, the corresponding probabilities $P_{c,burst}$, $P_{d,burst}$ and $P_{u,burst}$ are determined. Fig. 1 shows the algorithm to calculate the conditional probabilities.

1. Set the counters $N_{c,burst}$, $N_{d,burst}$ and $N_{u,burst}$ to zero.
2. Process the syndrome table.
3. Generate all possible bursts of length $b_{u,min}$:
    4. Determine the weighting ${r_B}^w\,(1-r_B)^{b_{u,min}-w}$.
    5. Place the burst at all possible positions in the block of length n:
        6. Calculate the syndrome.
        7. Select the case from the decoder decision.
        8. Increase the corresponding counter by the weighting.
9. Determine the probabilities $P_{c,burst}$, $P_{d,burst}$ and $P_{u,burst}$ from the counters.

Figure 1: Calculation of the probabilities $P_{c,burst}$, $P_{d,burst}$ and $P_{u,burst}$

With $b_{u,min}$ as the minimum length of a burst error which causes undetected errors, the probability $P_{u,burst}(b_{u,min})$ is of particular interest especially if the probability of bursts of length b with $b_{u,min} < b \leq n$ may be neglected. In case of a GC, the probability of a single burst of length b within a block of length n is given for small p [Rie98] by

$$P_{GC}(n,p,q,b) = \begin{cases} \frac{q}{p+q}(1-p)^{n-1} & \text{if } b=0 \\ \frac{pq}{p+q}(1-q)^{b-1}(1-p)^{n-b-2}\left[q(n-b-1)+2(1-p)\right] & \text{if } 1 \leq b \leq n-2 \\ 2\frac{pq}{p+q}(1-q)^{n-2} & \text{if } 1 \leq b = n-1 \\ \frac{p}{p+q}(1-q)^{n-1} & \text{if } 1 \leq b = n \end{cases} \tag{2}$$

If $P_{GC}(n,p,q,b_{u,min}) \gg P_{GC}(n,p,q,b)$ for all $1 \leq b_{u,min} < b \leq n$, $P_{u,burst}(b_{u,min})$ is a parameter independent performance measure. An evaluation of this condition leads to

$$p \ll \frac{nq^2 - b_{u,min}q^2 - 2q^2 + 3q}{nq - b_{u,min}q + q + 2}, \tag{3}$$

$$p \leq \frac{q^2+3q}{4q+2}, \text{ and} \tag{4}$$

$$q \geq \frac{1}{3}. \tag{5}$$

For large n, the equations may be simplified with the result $p \ll q \geq 1/3$.

Up to this point, single criteria a good code has to meet are analyzed. Unfortunately, there are several criteria that are important in practice, for example the code has to correct errors from different channels and in different modes of operation. The following definition allows the identification of good codes when several criteria are given:

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

6 Approximately Exact Analysis

In contrast to the parameter independent performance analysis, the main objective in this section is to determine the performance in terms of limits for the basic probabilities P_c, P_d, and P_u in case of given parameters. If x denotes one of the three possible decoder decisions of correct decoding (c), detection of errors (d) and undetected errors (u), that means, $x \in \{c, d, u\}$, the approximately exact analysis provides a lower (L_x) and an upper (U_x) bound for the probability P_x.

In case of a BSC, all relevant possibilities of a bit errors in a block of length n are considered to calculate the limits $L_{x,BSC}$ and $U_{x,BSC}$. As a compromise between expenditure and accuracy, a maximum number of bit errors a_{max} is introduced so that only the area $0 \leq a \leq a_{max}$ is analyzed. For each a, the product of the probability of a errors multiplied with the conditional probability of $P_{x,bit}(g(x), k, t, u/a)$ is added to the lower limit since the channel behavior is independent of the decoder behavior. The upper limit is computed from the complementary probabilities.

$$L_{x,BSC} = \sum_{a=0}^{a_{max}} P_{BSC}(n, r, a) P_{x,bit}(g(x), k, t, u/a) \tag{6}$$

$$U_{x,BSC} = 1 - \sum_{a=0}^{a_{max}} P_{BSC}(n, r, a)\left(1 - P_{x,bit}(g(x), k, t, u/a)\right) \tag{7}$$

This approach introduces an error as long as $a_{max} < n$ since all cases of $a > a_{max}$ errors are not considered. The probability of this error is

$$P_{BSC,rest}(n, r, a_{max}) = 1 - \sum_{a=0}^{a_{max}} P_{BSC}(n, r, a). \tag{8}$$

Applying the GC as channel model, the products of the probabilities of a burst of length b with $P_{x,burst}$ in the same cases, summed up for $0 \leq b \leq b_{max} \leq n$, is connected with P_x. Using $L_{x,GC}$ as the lower bound and $U_{x,GC}$ as the upper bound for P_x, the following holds with $x \in \{c, d, u\}$:

$$L_{x,GC} = \sum_{b=0}^{b_{max}} P_{GC}(n, p, q, b) P_{x,burst}(g(x), k, t, u, r_B/b) \tag{9}$$

$$U_{x,GC} = 1 - \sum_{b=0}^{b_{max}} P_{GC}(n, p, q, b)\left(1 - P_{x,burst}(g(x), k, t, u, r_B/b)\right) \tag{10}$$

The rest error in this approach is

$$P_{GC,rest}(n, p, q, b_{max}) = 1 - \sum_{b=0}^{b_{max}} P_{GC}(n, p, q, b) \tag{11}$$

and consists of two parts:

1. $P_{GC,rest}(n, p, q, n)$ is the error which is introduced by multiple bursts in a block. It can be shown [Rie98] that
$$P_{GC,rest}(n, p, q, n) \approx \left(\frac{1}{2}n^2 - \frac{3}{2}n + 1\right) p^2. \tag{12}$$

2. $P_{GC,rest}(n, p, q, b_{max}) - P_{GC,rest}(n, p, q, n)$ is the error which is – like in case of the BSC – caused by $b_{max} < n$.

7 Numerical Results

In the following, the parameter independent performance analysis is applied to find a good generator polynomial for a cyclic $(40, 32)$ block code. The code shall perform well in case of bit- and burst errors in detection $(t = 0, u = 0)$ and correction $(t = 1, u = 1)$ mode.

Table 1 shows the results of the parameter independent performance analysis. All relevant polynomials of degree $m = 8$ have been analyzed, and the performance is assessed in the undetected error probability. In the columns a, b, e, and f, bit errors are examined. In each mode, the minimum number of bit errors which cause undetected errors $(a_{u,min})$ is given in the columns a and e, respectively. In both modes, the corresponding probabilities of undetected errors $P_{u,bit}(a = a_{u,min})$ are shown in the columns b and f, respectively.

Table 1: Good polynomials obtained by the parameter independent performance analysis in case of a $(40, 32)$ code (probabilities in %)
a, e: $a_{u,min}$; b, f: $P_{u,bit}(a = a_{u,min})$; c, g: $b_{u,min}$; d, h: $P_{u,burst}(b = b_{u,min})$

octal	polynomial	detection mode				correction mode			
		bit errors		burst errors		bit errors		burst errors	
		a	b	c	d	e	f	g	h
445	$x^8+x^5+x^2+1$	4	0.7517	9	0.1953	3	27.8138	3	4.9342
511	$x^8+x^6+x^3+1$	4	0.7517	9	0.1953	3	27.8138	3	4.9342
633	$x^8+x^7+x^4+x^3+x+1$	4	0.7605	9	0.1953	3	28.1377	3	4.6053
663	$x^8+x^7+x^5+x^4+x+1$	4	0.7605	9	0.1953	3	28.1377	3	4.6053
533	$x^8+x^6+x^4+x^3+x+1$	4	0.7725	9	0.1953	3	28.5830	3	4.2763
665	$x^8+x^7+x^5+x^4+x^2+1$	4	0.7725	9	0.1953	3	28.5830	3	4.2763
431	$x^8+x^4+x^3+1$	4	0.7736	9	0.1953	3	28.6235	3	2.3026
461	$x^8+x^5+x^4+1$	4	0.7736	9	0.1953	3	28.6235	3	2.3026
677	$x^8+x^7+x^5+x^4+x^3+x^2+x+1$	4	0.7747	9	0.1953	3	28.6640	3	1.6447
773	$x^8+x^7+x^6+x^5+x^4+x^3+x+1$	4	0.7747	9	0.1953	3	28.6640	3	1.6447
517	$x^8+x^6+x^3+x^2+x+1$	4	0.7791	9	0.1953	3	28.8259	3	0.3290
745	$x^8+x^7+x^6+x^5+x^2+1$	4	0.7791	9	0.1953	3	28.8259	3	0.3290
467	$x^8+x^5+x^4+x^2+x+1$	4	0.7802	9	0.1953	3	28.8664	4	7.0946
731	$x^8+x^7+x^6+x^4+x^3+1$	4	0.7802	9	0.1953	3	28.8664	4	7.0946
503	x^8+x^6+x+1	4	0.7824	9	0.1953	3	28.9474	4	1.5203
605	$x^8+x^7+x^2+1$	4	0.7824	9	0.1953	3	28.9474	4	1.5203
437	$x^8+x^4+x^3+x^2+x+1$	4	0.8119	9	0.1953	3	30.0405	4	1.0135
761	$x^8+x^7+x^6+x^5+x^4+1$	4	0.8119	9	0.1953	3	30.0405	4	1.0135
473	$x^8+x^5+x^4+x^3+x+1$	4	0.8798	9	0.1953	3	32.5506	5	2.9514
671	$x^8+x^7+x^5+x^4+x^3+1$	4	0.8798	9	0.1953	3	32.5506	5	2.9514

Concerning burst errors, the results are given in the columns c, d, g, and h. In this case, the minimum burst length which leads to undetected errors $b_{u,min}$ is given in the columns c and g, and the corresponding probability of undetected errors $P_{u,burst}(b = b_{u,min})$ is shown in the columns d and h. Finally, the good polynomials according to the definition are listed in the table. Since a polynomial has the same performance characteristics as its reciprocal polynomial, the table provides pairs of polynomials with the same data.

In case of burst errors in detection mode, all polynomials show the same performance characteristics. Since an error occurs in only one of $2^9 = 512$ possibilities, the undetected error probability is computed by 2^{-9} independent of the generator polynomial. In case of bit errors, all polynomials provide a distance of 4 and show only minor performance differences. For burst errors in correction mode, significant differences in performance are visible: The last two polynomials in the table are able to reliably detect bursts of length 4 while correcting single bit errors, while other good polynomials cause undetected errors in this case. For that reason, either the polynomial 473 $(x^8 + x^5 + x^4 + x^3 + x + 1)$ or the polynomial 671 $(x^8 + x^7 + x^5 + x^4 + x^3 + 1)$ should be used.

The results of this analysis are valid for the BSC and the GC as long as (1) and (3) – (5) are true. In the example, this leads to

$$r \ll \frac{4}{41} \tag{13}$$

and

$$p \ll q \geq \frac{1}{3}. \tag{14}$$

The results of the approximately exact analysis are given using the generator polynomial $g(x) = x^8 + x^2 + x + 1$ as an example. Figure 2 shows both limits in case of a BSC with $r = 0.001$ using correction and detection mode. The probability of correct decoding is near to 1 in both modes. Detection of errors occurs with a probability of 0.0392 in detection mode, and for $a_{max} > 0$, both limits lead to this value. If $a_{max} = 0$, there are no errors and thus detection of errors takes place with probability 0. Since 0 corresponds to $-\infty$ in logarithmic representation, the lower limit is the vertical line at $a_{max} = 1$. In correction mode, a single error is corrected and detected errors occur if $a_{max} \geq 2$. Thus, the lower limit comes from $-\infty$ at $a_{max} = 2$ and leads to a probability of 0.000758. Undetected errors occur at $a_{max} = 3$ in correction mode and at $a_{max} = 4$ in detection mode.

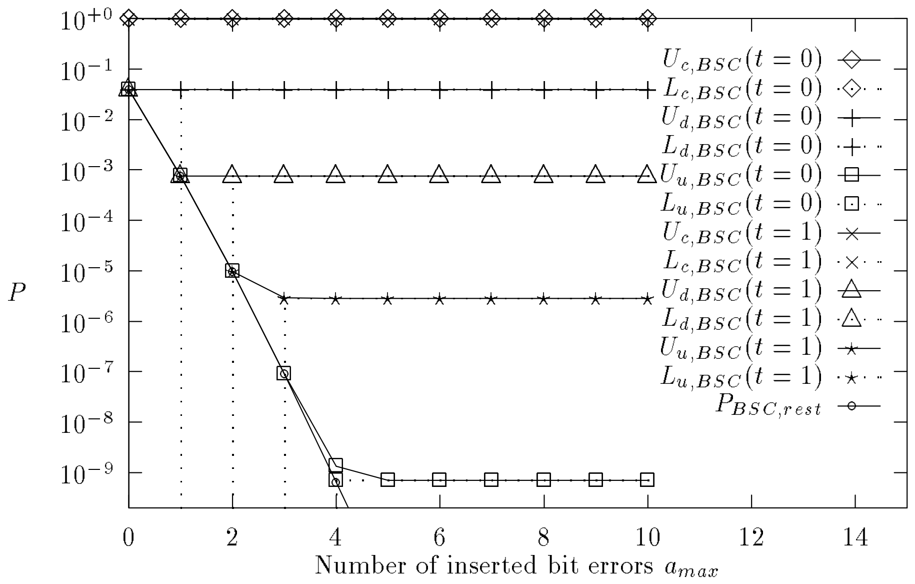

Figure 2: Performance of a $(40, 32)$ code over a BSC with variation of a_{max}
Parameters: $g(x) = x^8 + x^2 + x + 1$, $k = 32$, $r = 0.001$

It is obvious that the consideration of a few bit errors is sufficient to get good results using the approximately exact performance analysis. Using the GC as channel model, figure 3 shows the result of the analysis with $p = 0.001002$, $q = 0.5$[1], $r_G = 0$ and $r_B = 0.5$. The probability of correct decoding is again near to 1. For detection of errors, there are slight differences between the two borders even for large b_{max}. In case of undetected errors, especially in detection mode, the exact determination of the undetected error probability is not possible since there is much space between the two limits. This is due to the fact that multiple bursts in a block are possible, the probability for this is given in $P_{GC,rest}(n)$. This probability does not depend on b_{max}, thus increasing b_{max} does not lead to any improvements.

Figure 4 shows the behavior of the system with a BSC in case of $a_{max} = 10$ under variation of the bit error probability r. It is obvious that useful results are possible only for $r < 0.1$ since otherwise the difference between the limits is so high that exact statements are impossible. The rest error probability $P_{BSC,rest}$ is a good measure of the exactness of the analysis.

[1] In this case, the average bit error probability is the same in comparison to figure 2.

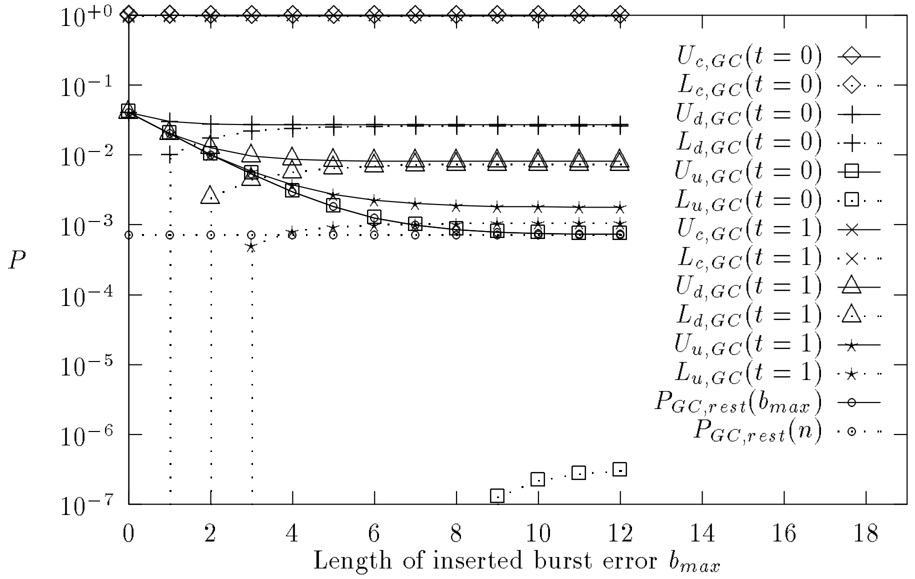

Figure 3: Performance of a $(40, 32)$ code over a GC with variation of b_{max}
Parameters: $g(x) = x^8 + x^2 + x + 1$, $k = 32$, $p = 0.001002$, $q = 0.5$, $r = 0.001$, $r_G = 0$, $r_B = 0.5$

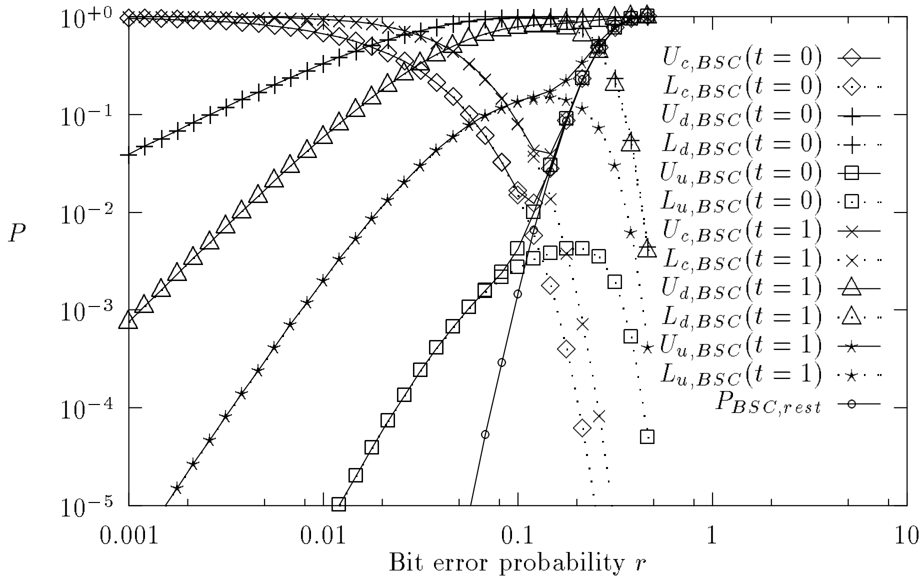

Figure 4: Performance of a $(40, 32)$ code over a BSC with variation of the bit error probability r
Parameters: $g(x) = x^8 + x^2 + x + 1$, $k = 32$, $a_{max} = 10$

In case of the Gilbert Channel, figure 5 shows the results of the approximately exact analysis under variation of the average bit error probability. For large r, the error which is introduced due to multiple bursts in a block outweighs those which arises because of $b_{max} < n$, whereas for small r, the error caused by $b_{max} < n$ becomes worse. Due to these errors, the undetected error probability in detection mode can not exactly be determined.

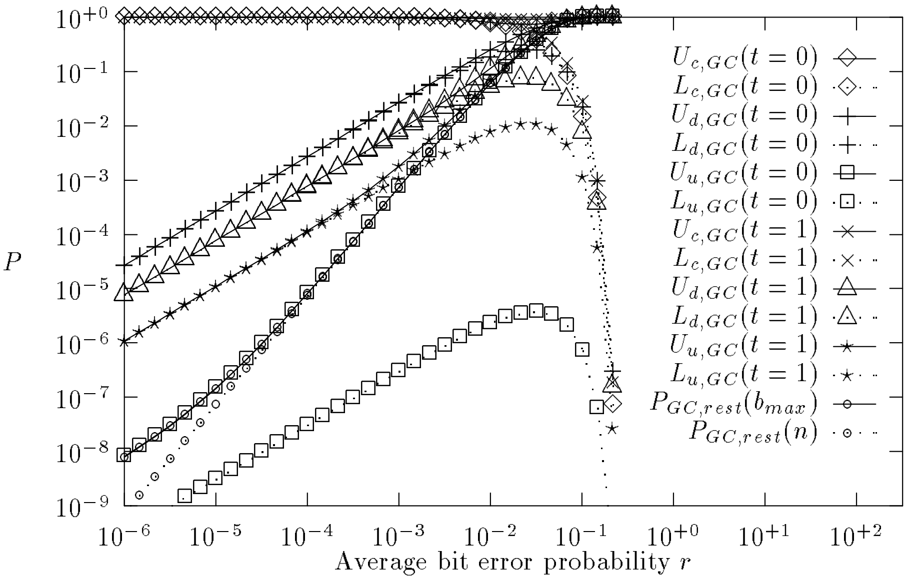

Figure 5: Performance of a $(40, 32)$ code over a GC with variation of the average bit error probability r Parameters: $g(x) = x^8 + x^2 + x + 1$, $k = 32$, $q = 0.5$, $r_G = 0$, $r_B = 0.5$, $b_{max} = 10$

8 Summary

Stimulated by a question on cryptology [Rie97], this paper presents a general performance analysis of forward error control. Besides an approximately exact analysis in case of given parameters, a new form of performance analysis is developed. Its main objective is to achieve a parameter independent analysis and to give areas in which the parameters may be varied.

This work was carried out at the Institute of Communication Systems, University of Hagen, Germany under the supervision of Prof. Kaderali. I would like to thank Prof. Kaderali, Dr. Zepernick and my colleagues for interesting discussions.

References

[Gil60] E. N. Gilbert. Capacity of a burst-noise channel. *Bell System Technical Journal*, 39:1253–1265, September 1960.

[Rie97] Andreas Rieke. Link encryption in ATM systems. In Sokratis Katsikas, editor, *Communications and Multimedia Security*, volume 3, pages 143–154. Chapman & Hall, London, 1997.

[Rie98] Andreas Rieke. *Die Anwendung von Verschlüsselungsverfahren in ATM-Systemen*. Dissertation, University of Hagen, Hagen, Germany, 1998. To appear.

[RZ97] Andreas Rieke and Hans-Jürgen Zepernick. On header forward error control in ATM systems. In Tadeusz Wysocki, Hashem Razavi, and Bahram Honary, editors, *Digital Signal Processing for Communication Systems*, pages 45–54. Kluwer Academic Publishers, Boston, 1997.