Bounds on the Error Probability of ML Decoding for Block and Turbo-Block Codes

Igal Sason and Shlomo Shamai (Shitz)
Department of Electrical Engineering
Technion—Israel Institute of Technology
Haifa 32000, Israel

March 1999

Abstract

The performance of either structured or random turbo-block codes and binary, systematic block codes operating over the additive white Gaussian noise (AWGN) channel, is assessed by upper bounds on the error probabilities of maximum likelihood (ML) decoding. These bounds on the block and bit error probability which depend respectively on the distance spectrum and the input-output weight enumeration function (IOWEF) of these codes, are compared, for a variety of cases, to simulated performance of iterative decoding and also to some reported simulated lower bounds on the performance of ML decoders. The comparisons facilitate to assess the efficiency of iterative decoding (as compared to the optimal ML decoding rule) on one hand and the tightness of the examined upper bounds on the other.

We focus here on uniformly interleaved and parallel concatenated turbo-Hamming codes, and to that end the IOWEFs of Hamming and turbo-Hamming codes are calculated by an efficient algorithm. The usefulness of the bounds is demonstrated for uniformly interleaved turbo-Hamming codes at rates exceeding the cutoff rate, where the results are compared to the simulated performance of iteratively decoded turbo-Hamming codes with structured and statistical interleavers. We consider also the ensemble performance of 'repeat and accumulate' (RA) codes, a family of serially concatenated turbo-block codes, introduced by Divsalar, Jin and McEliece. Although, the outer and inner codes possess a very simple structure: a repetitive and a differential encoder respectively, our upper bounds indicate impressive performance at rates considerably beyond the cutoff rate. This is also evidenced in literature by computer simulations of the performance of iteratively decoded RA codes with a particular structured interleaver.

1. Introduction

Turbo codes, one of the most recent and dramatic discoveries in coding theory, have demonstrated near Shannon limit performance on a Gaussian channel with relatively simple convolutional or block component codes and large interleavers. For applications that require error correcting codes to operate with much shorter delays, Berrou, Evano and Battail [8] have advocated block component codes, maintaining turbo coding/ decoding principle. These codes, called turbo-block codes, exhibit a coding gain that is considerably larger than that of the stand alone component block codes. Moreover, the decoding complexity for these turbo-block codes is quite reasonable, as long as the decoding complexity of the component block codes is so.

Simulation results demonstrated the importance and efficiency of turbo-block codes: Nickl, Hagenauer and Burkert [24] presented a possibility to approach Shannon's capacity limit by 0.27 dB using turbo-Hamming codes operating at a high coding rate of 0.981 bits/symbol. Huber, Schetelig and Wachsmann [16] have simulated some turbo-Hamming codes for different types of interleavers, providing some insight on the influence of the interleaver's structure on the performance of these codes. Pyndiah and his collaborators ([1],[2],[3],[13],[27],[28],[29],[30],[31]) have suggested an alternative suboptimal iterative decoding algorithm for these turbo-block codes, discussed the complexity of the decoding process, implemented these ideas on hardware (especially for turbo-Hamming codes) and examined the performance of these turbo-block codes for a binary-input AWGN and Rayleigh fading channels. These turbo-Hamming codes were demonstrated to have a good performance with the suboptimal iterative decoding algorithm for both channels. Hence, as evidenced by most of the references here, a turbo-block code is one of the worthiest coding options in terms of performance and decoding complexity for high code rate applications.

In addition to simulation results, theoretical upper bounds on the error probability of ML decoding for block and turbo-block codes operating over the binary-input AWGN channel are reported. Mostly, these bounds are based on the union bounding technique ([6],[7],[10],[36],[38]), and therefore they apparently render useless results at rates exceeding the cutoff rate (R_0), a region where efficient complex codes demonstrate satisfactory performance.

Since explicit results for a particular chosen structure of an interleaver appears yet intractable, the bounds are developed as averages over certain ensembles, featuring random coding properties. Comparisons between bounds for ML decoding and simulation results of the iterative decoding algorithm for some block and turbo-block codes, facilitate the theoretical assessment of the potential good performance of these codes (referring to soft decision ML decoding), as well as the examination of the efficiency of suboptimal and practical iterative decoding algorithms (as compared to the optimal prohibitively complex ML decoding.

The focus of this paper is directed towards the application of efficient bounding techniques on ML decoding performance, which are not subjected to the deficiencies of the union bounds and therefore provide useful results at rates reasonably higher than the cut-off rate, where union bounds are usually useless. In particular, we apply some versions of the tangential sphere bounds [26],[32], as well as original versions of Gallager's 1963 bounds [33].

The paper is structured as follows: In section 2, we state our underlying assumptions and introduce notations and relevant relations. In section 3, bounds on the decoding error probability of ML decoding and iterative decoding simulation results are compared for binary, systematic block codes (the simulation results are taken from the contribution of Lucas, Bossert and Breitbach[20],[21]). Based on these comparisons and results presented by Soljanin and Urbanke [35], we discuss the performance of the iterative decoding algorithm for the considered block codes (as compared to soft decision ML decoding). In section 4, we apply our bounds on ML decoding for an ensemble of random serially concatenated turbo-block codes, called 'Repeat and Accumulate' (RA) codes, that were introduced by Divsalar, Jin and McEliece [11]. Finally section 5 focuses on turbo-Hamming codes, where the upper bounds on the error probability of their soft decision ML decoding are compared to iterative decoding simulation results (as presented by Huber, Schetelig and Wachsmann [16]) with respect to certain types of interleavers. Since in general our upper bounds for turbo-block codes are based on the input-output weight enumeration function (IOWEF) of their component codes, we derive analytically the IOWEF of Hamming codes in the appendix. This derivation facilitates the determination of the IOWEF of the considered turbo-Hamming codes and the application of our bounds for soft decision ML decoding. Finally, our conclusions are discussed and summarized in Section 6.

2. Preliminaries

In this section, we state the underlying assumptions for our bounding technique, introduce notations and relations from [6],[7],[11],[12],[16],[21],[26],[32],[33], which apply to the discussion here on block and turbo-block codes. We state further relations and comments useful to our analysis and conclusions.

A. Assumptions

We assume throughout a binary-input additive white Gaussian noise (AWGN) channel having a double-sided noise spectral density $\frac{N_0}{2}$. The modulation of the transmitted signals is antipodal, which is coherently detected and ML decoded (with soft decision).

B. Notations and relations

B.1 Tangential sphere bound

The tangential sphere bound is an upper bound on the block error probability of ML decoding, derived in [26]. Suppose that equi-energy signals are transmitted through a binary-input AWGN channel corresponding to each one of the codewords of a linear and binary block code C. The energy of each signal is $E = nE_s$, when n designates the block length and E_s is the energy transmitted per symbol.

It can be shown that the tangential sphere bound is always tighter than the tangential bound and the union bound at low and moderate values of $\frac{E_b}{N_0}$ [26]. The properties of the tangential sphere bound follow by the central inequality which governs this and other bounds ([12],[26] and references therein)

$$\text{Prob}\,(A) \leq \text{Prob}\,(\underline{z} \in B, A) + \text{Prob}\,(\underline{z} \notin B)\,. \tag{1}$$

In the case of the tangential sphere bound, A is an event that represents a block ML decoding error, B is an n-dimensional cone with a half angle θ and radius r, and $\underline{z}$ is the Gaussian noise vector added to the transmitted signal by the channel. Since an optimization is carried over r (r and θ are related) for deriving the tightest upper bound on the block error probability, within this family, it follows that this upper bound does not exceed 1 in contrast to the union bound, especially for moderate and low values of $\frac{E_b}{N_0}$. The tangential sphere bound on the block error probability P_e is based only on the distance spectrum $\{S_k\}_{k=1}^{n}$ of the linear block code C and it reads:

$$\begin{aligned} P_e \;\leq\; & \int_{-\infty}^{+\infty} \frac{dz_1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_1^2}{2\sigma^2}} \left\{ \begin{array}{l} 1 - \overline{\gamma}\left(\dfrac{n-1}{2}\,,\, \dfrac{r_{z_1}^2}{2\sigma^2}\right) \\ + \displaystyle\sum_{k:\,\frac{\delta_k}{2}<\alpha_k} S_k \left[Q\left(\frac{\beta_k(z_1)}{\sigma}\right) - Q\left(\frac{r_{z_1}}{\sigma}\right)\right] \overline{\gamma}\left(\frac{n-2}{2}\,,\, \frac{r_{z_1}^2 - \beta_k^2(z_1)}{2\sigma^2}\right) \end{array} \right\} \\ & + \; Q\left(\sqrt{\frac{2nRE_b}{N_0}}\right)\,, \end{aligned} \tag{2}$$

where the following notations are used in (2):

$$\left\{ \begin{array}{lcl} \sigma^2 & = & \dfrac{N_0}{2}\,, \\ r_{z_1} & = & \left(1 - \dfrac{z_1}{\sqrt{nE_s}}\right) r\,, \\ \beta_k(z_1) & = & \dfrac{r_{z_1}}{\sqrt{1 - \dfrac{\delta_k^2}{4nE_s}}}\, \dfrac{\delta_k}{2r} \\ \alpha_k & = & r\sqrt{1 - \dfrac{\delta_k^2}{4nE_s}}\,. \end{array} \right. \tag{3}$$

δ_k denotes the Euclidean distance between two signals that their corresponding codewords differ in k symbols ($k \leq n$). Thus, for the case of antipodal signals, $\delta_k = 2\sqrt{kE_s}$. Also,

$$\overline{\gamma}(a,x) = \frac{1}{\Gamma(a)} \int_0^x t^{a-1}\, e^{-t}\, dt\ , \quad a, x > 0 \tag{4}$$

denotes the normalized incomplete gamma function.

In the upper bound (2), the optimal radius r (in the sense of achieving the tightest upper bound, within this family of bounds) is determined by nulling the derivate of the bound (2) with respect to the free parameter r, which yields the following optimization equation ([26]):

$$\begin{cases} \displaystyle\sum_{k:\, \frac{\delta_k}{2} < \alpha_k} S_k \int_0^{\theta_k} \sin^{n-3}\, \phi\, d\phi = \frac{\sqrt{\pi}\, \Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} \\ \theta_k = \cos^{-1}\left(\dfrac{\delta_k}{2r}\, \dfrac{1}{\sqrt{1 - \dfrac{\delta_k^2}{4nE_s}}}\right) \end{cases} . \tag{5}$$

In [32], we derive an upper bound on the bit error probability of linear block codes, based on the concept of the derivation of the tangential sphere bound in [26]. This upper bound is based on the IOWEF of the linear binary block code C (rather than its distance spectrum).

Let $B_{w,\ell}$ be the number of codewords encoded by information bits of Hamming weight w having also an overall Hamming weight of ℓ (if the code C is systematic, then for $\ell < w$, $B_{w,\ell} = 0$). Define:

$$S'_\ell = \sum_{w=1}^{nR} \left(\frac{w}{nR}\right) B_{w,\ell} \quad \ell = 0, 1, \ldots, n\ , \tag{6}$$

where $R\left[\frac{\text{bits}}{\text{symbol}}\right]$ is the rate of the code C. The derived upper bound on the bit error probability in [32] is similar to the upper bound on the block error probability (Eqs. (2)-(5)), with $\{S'_\ell\}_{\ell=0}^n$ replacing the distance spectrum $\{S_\ell\}_{\ell=0}^n$ of the code C. The validity of the upper bounds on the block and bit error probabilities is addressed in [32], where the existence and uniqueness of a solution r to the optimization equation (5) (or the modified optimization equation that refers to the upper bound on the bit error probability) is also proved. Efficient algorithms for solving the optimization equations of the tangential sphere upper bounds on the block and bit error probabilities are suggested in [32].

B.2 Gallager's 1963 bound for structured and random binary block codes

Gallager derived in [12] a general upper bound on the decoding error probability of ML decoded binary block codes transmitted through a binary-input symmetric-output memoryless channel. New observations on Gallager's 1963 bound are presented in [33], and the upper bounds derived there are applicable for upper bounding the ML decoding error probability of block and turbo-block codes. The efficiency of the upper bounds was demonstrated for certain high rate turbo codes with random binary, linear and systematic block component codes incorporated with a sufficiently large interleaver. In these cases, a particular version of Gallager's 1963 bound outperforms the tangential sphere bound, as is demonstrated in [33], and therefore we apply here this advantageous upper bound. The upper bound on the block error probability reads as follows:

$$P_e \leq c(\rho) \quad \cdot \quad 2^{n\rho R} \left\{ \int_{-\infty}^{+\infty} \Big[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \Big]^{1+\rho} dy \right\}^n$$

$$\cdot \quad \left[\sum_{\ell=0}^{n} r_{\ell,n} \left(\begin{array}{c} n \\ \ell \end{array} \right) \lambda(\rho)^{\ell} \Big(1 - \lambda(\rho) \Big)^{n-\ell} \right]^{\rho} \qquad 0 \leq \rho \leq 1 \,, \tag{7}$$

where n is the block length of the code, R is its rate and ρ is an optimized parameter in the interval $[0, 1]$ (for minimizing the upper bound on P_e). The conditional probability density functions of the channel are denoted by p_0 and p_1, corresponding to the transmitted '0' or '1' respectively. Since the considered channel is a binary-input symmetric-output memoryless channel, then $p_0(y) = p_1(-y)$ for $-\infty < y < +\infty$. Moreover, based on the analysis in [33]:

$$\lambda(\rho) = \frac{1}{2}\, \frac{\displaystyle\int_{-\infty}^{+\infty} \Big[p_0(y)\, p_1(y) \Big]^{\frac{1}{1+\rho}} \Big[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \Big]^{\rho-1} dy}{\displaystyle\int_{-\infty}^{+\infty} \Big[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \Big]^{1+\rho} dy} \,, \tag{8}$$

which yields $0 \leq \lambda(\rho) \leq \dfrac{1}{2}$ for $0 \leq \rho \leq 1$. In (7), $\{r_{\ell,n}\}_{\ell=0}^{n}$ is defined as follows:

$$r_{\ell,n} = \frac{S_\ell}{2^{-n(1-R)} \left(\begin{array}{c} n \\ \ell \end{array} \right)} \,, \quad \ell = 0, 1, 2, \ldots, n \tag{9}$$

which is the ratio of the number of codewords in the code C with Hamming weight ℓ and the corresponding average number of codewords in a fully random block code having the same block length n and rate R. Finally, $c(\rho)$ in (7) is:

$$c(\rho) = \left\{ \begin{array}{ccc} \rho^{-1} \Big(\rho^{-1} - 1 \Big)^{\rho-1} & , & 0 < \rho < 1 \\ 1 & , & \rho = 0, 1 \end{array} \right. \tag{10}$$

noticing that $1 \leq c(\rho) \leq 2$ for $0 \leq \rho \leq 1$ [33].

The upper bound on the bit error probability takes on the same form as the upper bound on the block error probability, as defined in Eq. (6) replacing though $\{S_\ell\}_{\ell=0}^n$ (the distance spectrum of the code C) with $\{S'_\ell\}_{\ell=0}^n$, Therefore, we define for the upper bound on the bit error probability:

$$r'_{\ell,n} = \frac{S'_\ell}{2^{-n(1-R)} \left(\begin{array}{c} n \\ \ell \end{array} \right)} \ , \quad \ell = 0, 1, 2, \ldots, n \tag{11}$$

and then the upper bound on the bit error probability is the same expression as that for the upper bound on the block error probability (7), but for $\{r'_{\ell,n}\}_{\ell=0}^n$ replacing the sequence $\{r_{\ell,n}\}_{\ell=0}^n$. The upper bound on the bit error probability derived in [33], reads then:

$$P_b \leq c(\rho) \quad \cdot \quad 2^{n\rho R} \left\{ \int_{-\infty}^{+\infty} \left[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \right]^{1+\rho} dy \right\}^n$$

$$\cdot \quad \left[\sum_{\ell=0}^{n} r'_{\ell,n} \left(\begin{array}{c} n \\ \ell \end{array} \right) \lambda(\rho)^\ell \Big(1 - \lambda(\rho)\Big)^{n-\ell} \right]^\rho \ , \quad 0 \leq \rho \leq 1 \ . \tag{12}$$

The ensemble performance of random, binary and *systematic* (n, k) block codes is investigated in [33], and based on (12) the following upper bound on the average bit error probability for ML decoding is derived,

$$P_b \leq c(\rho) \cdot 2^{n\rho R} \cdot \lambda(\rho)^\rho \left\{ \int_{-\infty}^{+\infty} \left[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \right]^{1+\rho} dy \right\}^n \ , \quad 0 \leq \rho \leq 1 \ . \tag{13}$$

Moreover, for the extended ensemble of random binary (n, k) block codes (which are not necessarily systematic), the following upper bound on the average bit error probability for ML decoding is derived in [33]:

$$P_b \leq c(\rho) \cdot 2^{n\rho R} \cdot \left(\frac{1}{2}\right)^\rho \left\{ \int_{-\infty}^{+\infty} \left[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \right]^{1+\rho} dy \right\}^n \ , \quad 0 \leq \rho \leq 1 \ .$$

Since for $0 \leq \rho \leq 1$, we get $0 \leq \lambda(\rho) \leq \dfrac{1}{2}$, the upper bound on the *bit* error probability for the ensemble of random, binary and *systematic* (n, k) block codes is tighter than the corresponding upper bound for the ensemble of random, binary (n, k) block codes. The average upper bound on the *block* error probability is the same though for the two ensembles above (i.e., for systematic and non-systematic codes) due to their spectral distance equivalence and reads:

$$P_e \leq c(\rho) \cdot 2^{n\rho R} \left\{ \int_{-\infty}^{+\infty} \left[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}} \right]^{1+\rho} dy \right\}^n \ , \quad 0 \leq \rho \leq 1 \ . \tag{14}$$

It is noted that the upper bound on the block error probability (14) is the same as the known random coding bound of Gallager (from 1965), except for the factor $c(\rho)$ that does not exceed 2 as $0 \leq \rho \leq 1$, as is pointed out also in [12].

For the particular case of a binary-input AWGN channel, we get from Eq. (8) (based on the analysis in [33]):

$$\lambda(\rho) = \frac{1}{2} \frac{\int_{-\infty}^{+\infty} \exp(-x^2) \left[\cosh\left(2\sqrt{\frac{RE_b}{N_0}} \frac{x}{1+\rho}\right)\right]^{\rho-1} dx}{\int_{-\infty}^{+\infty} \exp(-x^2) \left[\cosh\left(2\sqrt{\frac{RE_b}{N_0}} \frac{x}{1+\rho}\right)\right]^{\rho+1} dx} \tag{15}$$

and also,

$$\int_{-\infty}^{+\infty} \left[\frac{1}{2}\, p_0(y)^{\frac{1}{1+\rho}} + \frac{1}{2}\, p_1(y)^{\frac{1}{1+\rho}}\right]^{1+\rho} dy$$

$$= \frac{1}{\sqrt{\pi}} \exp\left(-\frac{RE_b}{N_0}\right) \int_{-\infty}^{+\infty} \exp(-x^2) \cdot \left[\cosh\left(2\sqrt{\frac{RE_b}{N_0}} \frac{x}{1+\rho}\right)\right]^{1+\rho} dx\,. \tag{16}$$

For the numerical evaluation of the integrals (15),(16), the Gauss-Hermite integration technique was performed.

B.3 Types of interleavers

B.3.1 Uniform interleaver A uniform interleaver of length N is a statistical interleaver which maps a given input word of weight ℓ into all its $\binom{N}{\ell}$ distinct permutations, equally weighted. Note that the identity permutation (that doesn't permute the bits of the word) is also considered as a possible "interleaving". This type of statistical interleaving was introduced in [6], permitting an easy derivation of the distance spectrum (and the IOWEF) of parallel and serial concatenated turbo codes, relying on the IOWEFs of its components.

B.3.2 Block interleaver A block interleaver is a structured interleaver in which $N = n_1 n_2$ bits are arranged in a matrix of n_1 rows and n_2 columns. After the permutation of the bits, we get simply the transpose of the matrix (i.e., the bits are arranged in the matrix row by row and transmitted column by column).

B.3.3 Diagonal interleaver A diagonal interleaver is a structured interleaver in which the input bits are arranged in the rows of a matrix, and the permutation of the bits is performed in such a

way, that the data is transmitted in cyclic diagonals, in a reverse direction. This type of interleaving is introduced in [16] where its efficiency for turbo-Hamming codes is demonstrated.

B.4 Some notations for the IOWEF

In general, for a binary, systematic linear (n, k) block code C, let $A_{w,j}$ be the number of codewords having an information weight w and parity weight j. Moreover, for a binary block code (not necessarily systematic), let $B_{w,\ell}$ be the number of codewords encoded by information bits of weight w having also an overall Hamming weight of ℓ. Therefore, if the code C is systematic, we get the relation: $A_{w,j} = B_{w,w+j}$ for $0 \leq w \leq k$ and $0 \leq j \leq n-k$. The notion of $A_{w,j}$ is more convenient for analyzing the performance of *parallel* concatenated turbo codes with a uniform interleaving (as for example the turbo-Hamming codes, discussed in section 5), while on the other hand the notation of $B_{w,\ell}$ is preferred for analyzing the performance of *serially* concatenated turbo codes with a uniform interleaving (as for example the RA codes, discussed in section 4).

B.5 Repeat and accumulate (RA) codes

In [11], Divsalar et al. introduce an ensemble of turbo-like codes, called there RA codes. The general idea in these codes is that an information block of length N is repeated q times, scrambled by a uniform interleaver of length qN, and then encoded by a differential encoder. Although the differential encoder can be viewed as a rate–1 recursive convolutional encoder, it can also be treated as a binary block code of rate 1 with the following generator matrix G:

$$G = \begin{bmatrix} 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 1 & & & 0 & & & \\ & & & & 1 & & & & & \\ & & & & & 1 & & & & \\ & & & & & & 1 & & & \\ & & & 1 & & & & 1 & & \\ & & & & & & & & 1 & \\ & & & & & & & & & 1 \end{bmatrix}, \tag{17}$$

of dimensions $(qN) \times (qN)$, playing the role of an accumulator. Moreover, the repetitive outer code is also a simple (structured) binary and systematic (qN, N) block code, of rate $R = \frac{1}{q}$. Therefore, RA codes can be viewed as an ensemble of serially concatenated turbo-block codes. It is also noted in [11] that $B_{w,\ell}^{(N)}$ the average number of codewords in the ensemble of uniformly interleaved (qN, N)

RA codes having an information weight w and an overall Hamming weight ℓ is

$$B_{w,\ell}^{(N)} = \frac{\left(\begin{array}{c} N \\ w \end{array} \right) \left(\begin{array}{c} qN-\ell \\ \lfloor qw/2 \rfloor \end{array} \right) \left(\begin{array}{c} \ell-1 \\ \lceil qw/2 \rceil - 1 \end{array} \right)}{\left(\begin{array}{c} qN \\ qw \end{array} \right)} \, , \tag{18}$$

where $0 \leq w \leq N$ and $0 \leq \ell \leq qN$, and where $\lfloor x \rfloor$, $\lceil x \rceil$ denote respectively the maximal and minimal integers that satisfy the inequality $\lfloor x \rfloor \leq x \leq \lceil x \rceil$.

B.6 A simulated lower bound for soft decision ML decoding

The simulated lower bound on the block error probability of a binary block code C with soft decision ML decoding is introduced in [21]. The bound is based on examining the performance of a hypothetical decoder which has access also to the true sequence (Genie aided): the all-zero codeword is transmitted as an all 1–sequence ('0' and '1' are mapped to '+1' or '-1' respectively). Suppose the decoder receives the vector $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ and define $\mathbf{r}^H = (x_1, x_2, \ldots, x_n)$, such that $x_i = 0$ or 1 if r_i is positive or negative respectively (a hard decision). If $\mathbf{r}^H \in C$, then the Euclidean distance between the vector $\mathbf{r}$ and each one of the two vectors $\mathbf{r}^H$ and the all 1–sequence are measured. The decision on which signal was transmitted is based on the minimal Euclidean distance between the two measured distances. If $\mathbf{r}^H \notin C$, then this hypothetical decoder decided correctly that the all-zero codeword was transmitted. Clearly, computer simulations of the performance of that decision rule, as in [21], yields a lower bound on the block error probability for soft decision ML decoding.

3. The Performance of the Iterative Decoding Algorithm for Binary, Systematic and Linear Block Codes

In this section, we discuss the degradation in performance of the suboptimal and practical iterative decoding algorithm derived in [21], as compared to bounds on the performance of soft decision ML decoding. The latter is known to be an optimal decoding rule, in the sense of minimizing the block error probability, but is prohibitively complex to implement for most of the block codes. The exact evaluation of performance, though possible for very selected classes of block codes, is commonly intractable and therefore we resort to bounds (as is also performed in [21]). However, one of the aspects in the discussion here is that we narrow the gap between the simulated lower bound for soft decision ML decoding in [21] and the ubiquitous union bound, by applying improved upper bounds (that are considerably more efficient than the union bound especially at rates exceeding the cutoff rate of the channel). Some versions of the tangential sphere bound [26], [32] (see also

2.B.1) and also some original version of Gallager's 1963 bound [33] (see also 2.B.2) are applied. These upper and lower bounds for the soft-decision ML decoding on one hand and the iterative decoding simulation results on the other, facilitate to assess the loss in performance due to the iterative decoding algorithm in [21], for a variety of binary and systematic block codes.

The improved upper bounds introduced here are based on the distance spectrum or the IOWEF of the considered block code, to get respectively upper bounds on the block and bit error probabilities of soft decision ML decoding. Therefore, for some of the structured block codes examined here, where the computation of their distance spectrum or their IOWEF are not available, we compare the simulation results of the iterative decoding rule from [21], with some upper bounds on the bit/block error probability of soft-decision ML decoding for an ensemble of random, binary and systematic (n, k) block codes with the same parameters of n, k as of the structured block codes under examination (2.B.2). In these cases, the comparison with the random ensemble of binary and systematic block codes, seems to be more appropriate than comparing the performance of such a binary and systematic (n, k) block code with a non-systematic convolutional code of the same code rate R, as is reported in [21].

In Figs. 1–5, comparisons between the performance of the iterative decoding algorithm [21] and bounds on the block error probability of soft decision ML decoding are presented for some structured block codes of moderate length. These block codes, were already investigated in [21], however the tangential sphere bounds were added here and their advantage over the union bound in Q-form is demonstrated. It is interesting to note, that the iterative decoding results in [21] for the (42, 21) double circulant (DC) code and (64, 42) Reed-Muller (RM) code fall very close to the corresponding tangential sphere upper bounds of these codes (see Figs. 1 and 5). Moreover, for the block codes examined in Figs. 1–5, the tangential sphere bound is a rather efficient upper bound on the block error probability for soft decision ML decoding, as evidenced by the simulated lower bound. The suboptimality of the iterative decoding algorithm [21] is also indicated, as compared to the optimal ML decoding rule. This observation is consistent with results in [32], considering turbo codes with convolutional component codes, where it was demonstrated there that in certain cases, the upper bounds on the block and bit error probabilities of ML decoding fall below simulated performance of iterative decoding, pointing on the mild suboptimality of the iterative decoding for moderate and low values of $\frac{E_b}{N_0}$.

The degradiation in performance of the iterative decoding algorithm as compared to ML decoding for certain structured binary block codes of moderate length, is summarized in Table 1 (based on Figs. 1–5).

It is noted that the range of values of the energy per bit to noise spectral density $\left(\frac{E_b}{N_0}\right)$ required

for soft-decision ML decoding is determined for each considered block code by the tangential sphere bound on the block error probability and also by the simulated lower bound in [21] (see also 2.B.6).

In Figs. 6 and 7, the performance of the iterative decoding algorithm in [21] is examined for two structured long block codes. The examined block codes in Figs. 6,7 are respectively the (1023, 781) EG (Euclidean Geometry) code and also a product (3969, 1369) code, constructed by a direct product of two (63, 37) EG codes. As is demonstrated by examples in [37], the *full* distance spectrum of a product code is not completely determined by the distance spectrum of its component codes, but only for relatively *low* Hamming weights of the product code. In particular, the computation of the distance spectrum of the considered product code, cannot be fully evaluated from the distance spectrum of the (63, 37) EG code. On the other hand, the direct calculation of the distance spectrum of the considered product code based on its generator matrix is impractical, due to the enormous number of codewords. Moreover, as for the considered structured block code in Fig. 7, calculating its IOWEF seems to be problematic (bounds on the distance spectrum of arbitrary EG codes are derived in [17], but the derivation of the corresponding IOWEF seems not to appear in the literature). Therefore, the performance of the iterative decoding algorithm [21] for structured, binary and systematic long block codes is compared in Table 2 to upper bounds for ML decoding on the bit error probability for the ensemble of random, binary and *systematic* block codes having the same length and rate.

Based on the results presented in Tables 1 and 2, we conclude that for relatively simple structured block codes, the degradation in performance due to the suboptimality of the iterative decoding algorithm is reasonable, as compared to soft decision ML decoding. On the other hand, the loss in performance is increased with the complication of the code's structure and the increased number of the codewords, as is indicated by comparing the estimated loss in the suboptimality of the iterative decoding algorithm (compared to ML decoding) in Tables 1 and 2.

These conclusions are consistent also with those in [32], considering turbo codes with recursive systematic convolutional codes as components. It is demonstrated there that the degradation in the performance of the iterative decoding, as compared to soft-decision ML decoding, increases with the increased number of the component codes and the interleaver length.

4. The Ensemble Performance of RA Codes

The ensemble performance of uniformly interleaved RA codes is considered by Divsalar, Jin and McEliece [11]. The structure of these codes and the expressions for the IOWEF of this ensemble of codes are introduced in 2.B.5 (based on the analysis in [11]).

Based on the IOWEF of these RA codes (Eq. (18)), the distance spectrum of some ensembles of (qN, N) RA codes, are illustrated in Fig. 8, versus the normalized Hamming weight of the codewords (the normalization relates to block length qN), where $N = 1024$ and $q = 2, 3, 4$. It is observed there that for a fixed value of N, the number of codewords with relatively low Hamming weights is decreased by increasing the value of q (although the overall number of codewords (2^N) remains constant). Therefore, it is indicated in Fig. 8 that the ensemble performance of the uniformly interleaved and serially concatenated RA codes is improved by increasing the value of q, as expected (since the number of repetitions of the outer encoder is increased and the interleaver length qN is also increased).

Upper bounds on the block and bit error probabilities of soft decision ML decoding for uniformly interleaved RA codes, are illustrated in Fig. 9. The usefulness of the tangential sphere bounds [26],[32] is demonstrated at rates considerably exceeding the cutoff rate of the channel: for $q = 3, 4$ (the code rate of the RA code is $\frac{1}{3}$ or $\frac{1}{4}$ respectively), the cutoff rate of the binary-input AWGN channel corresponds to $\frac{E_b}{N_0} = 2.03$ and 1.85 dB respectively. From Fig. 9, it is indicated that for $q = 3$, the tangential sphere upper bound on the bit error probability [32], yields 10^{-5} at $\frac{E_b}{N_0} = 1.58$ dB (i.e, 0.45 dB below the value of $\frac{E_b}{N_0}$ that corresponds to the cutoff rate). Moreover, for $q = 4$, this improved upper bound equals 10^{-5} at $\frac{E_b}{N_0} = 0.79$ dB (that is 1.06 dB below the value of $\frac{E_b}{N_0}$ that corresponds to the cutoff rate, but 1.59 dB above the value of $\frac{E_b}{N_0}$ that corresponds to the capacity of the binary-input AWGN channel). On the other hand, it is indicated in Fig. 9, that the union bounds in Q-form are useless at rates beyond the cutoff rate of the channel, as expected for long enough block codes (the interleaver length for these RA codes is 3072 or 4096 for $q = 3, 4$ respectively).

Based on the analysis in [11] for uniformly interleaved RA codes of sufficiently large block lengths: for values of $\frac{E_b}{N_0}$ above a certain value γ (which depends on the parameter q), the upper bound on block error probability of the ensemble of these (qN, N) RA codes, behaves asymptotically (for large values of N) like N^β, where $\beta = -\left\lceil \frac{q-2}{2} \right\rceil$. Therefore, for $q = 3, 4$, the upper bound on the block error probability behaves asymptotically like $\frac{1}{N}$, for $\frac{E_b}{N_0} > \gamma$. Based on the analysis in [11], $\gamma = 1.11$ or 0.31 dB for $q = 3, 4$ respectively, considering the asymptotic case where $N \to \infty$. It is demonstrated in Fig. 9 that the upper bounds on the block error probability of these ensembles of (qN, N) RA codes do not differ too much for moderate and high values of $\frac{E_b}{N_0}$, where $N = 1024$ and $q = 3, 4$. That verifies the same basic trend of the block error probability for these values of q.

The tangential sphere upper bound [26] and the union bound in Q-form (referring to soft-decision ML decoding and examined for a uniform interleaver), are compared with some simulation

results in [11], for the iterative decoding algorithm for a *specific* structured interleaver, where $N = 1024$ and $q = 3, 4$ (see Figs. 10,11). It is indicated (especially in Fig. 10), that the error floor of these RA codes is improved by this specific choice of interleaver (in comparison to the error floor that corresponds to the analysis referring to uniform interleaving). On the other hand, the tightness of the tangential sphere bound for moderate and low values of $\frac{E_b}{N_0}$ is demonstrated by Figs. 10,11, based on a comparison of this upper bound of ML decoding with the iterative decoding simulation results from [11] (although the structured interleaver simulated in [11], is advantageous over the statistical uniform interleaver).

5. Turbo-Hamming Codes

In this section, we discuss (parallel concatenated) turbo-Hamming codes of the following structure: the component codes are two identical $(2^m - 1,\, 2^m - m - 1)$ Hamming codes and the interleaver operates on the bits of $2^m - m - 1$ *different* Hamming codewords, having thus an interleaver length N of $(2^m - m - 1)^2$ bits. As in general the interleaver length N of turbo-Hamming codes is *not uniquely* determined by its Hamming component codes (in general, N should be an integer multiple of $2^m - m - 1$), it therefore provides a flexibility in the design of the turbo-Hamming codes in contrast to product codes which are constructed from the same component codes.

In subsection 5.A, we describe the algorithm derived in the appendix, for the calculation of the IOWEF of $(2^m - 1,\, 2^m - m - 1)$ Hamming codes (when $m \geq 3$). In subsection 5.B, we derive the IOWEF for the ensemble of these turbo-Hamming codes, when the statistical expectation is performed over the uniform interleaver of length N. Finally, in subsection 5.C, we discuss the ensemble performance of these turbo-Hamming codes, as reflected by the tangential sphere upper bounds on the bit error probability of soft decision ML decoding and by a comparison of these bounds for ML decoding with simulation results for iteratively decoded turbo-Hamming codes with structured and statistical interleavers [16].

A. A summary of the algorithm used for calculating the IOWEF of the $(2^m - 1, 2^m - m - 1)$ Hamming codes

The IOWEF of the (7, 4) Hamming code is straightforwardly derived in [6] based on its 16 codewords. However, since the number of codewords of a general $(2^m - 1,\, 2^m - m - 1)$ Hamming code increases considerably with the increased value m, it is obvious that the approach in [6], used for the derivation of the IOWEF of this particular Hamming code, is impractical for $m \geq 5$ (already for $m = 5$, there are more than $67 \cdot 10^6$ Hamming codewords, and therefore checking

the Hamming weights of each one of the individual codewords becomes rather tedious). In the appendix, we present an efficient analytical algorithm for the derivation of IOWEF for a general $(2^m-1,\, 2^m-m-1)$ Hamming code. The steps of the algorithm are summarized here adhering to the notations in section 2.B.4.

Step 0: Determine: $A_{0,0}=1$ and $A_{0,j}=0$ for $1\le j\le m$.

Step 1: Calculate the coefficients $A_{1,j}$ and $A_{2,j}$, $(0\le j\le m)$, based on equations (A.1) and (A.6) respectively.

Step 2: Calculate the coefficients $A_{i,j}\left(3\le i\le \lfloor\frac{2^m-m-1}{2}\rfloor,\ 0\le j\le m\right)$ based on the recursive equation (A.9) and the initial values of $A_{i,j}$ calculated in step 1.

Step 3: Calculate all the rest of the coefficients $A_{i,j}\,(\lfloor\frac{2^m-m-1}{2}\rfloor+1\le i\le 2^m-m-1\,,\ 0\le j\le m)$ based on equation (A.10) and the coefficients determined in steps 0–2.

The IOWEF of two Hamming codes are presented in Figs. 12,13: $\log_{10}(A_{i,j})$ is plotted as a function of the information weight i and the parity weight j of the Hamming codewords (where $0\le i\le 2^m-m-1$ and $0\le j\le m$).

B. Derivation of the IOWEF for the ensemble of turbo-Hamming codes with uniform interleaving

The IOWEF of the ensemble of (parallel concatenated) turbo-Hamming codes (C_p), with two identical $(2^m-1,\, 2^m-m-1)$ Hamming codes (C) as components and a uniform interleaver of length N, has the following form:

$$A^{C_p}(W,Z)=\sum_{i=0}^{N}\sum_{j=0}^{J}A_{i,j}^{C_p}\,W^i\,Z^j\ , \tag{19}$$

where $N=(2^m-m-1)^2$ and $J=2m(2^m-m-1)$ are the number of information bits and parity bits of the turbo-Hamming code. Equations (8),(16)-(18) in [6] facilitate to find the IOWEF of the considered ensemble of turbo-Hamming codes C_p, based on the IOWEFs of its component codes. However, to circumvent the need to calculate polynomials (including calculations of partial derivatives of high orders, as results from Eq. (17) in [6]), the complexity of the following algorithm is reduced by operating on matrices instead of polynomials.

For the generality of the proposed method here, we consider the general case where the component codes of a (parallel concatenated) turbo-block code are $(n_1,\, k_1)$ and (n_2, k_2) binary systematic block codes, denoted here as C_1 and C_2, respectively. The *uniform* interleaver in the general case

is of length $N = sk_1 = \ell k_2$, where ℓ, s are integers, operating on N *bits*. Therefore, s codewords are encoded by the block code C_1, ℓ codewords are encoded by the block code C_2, and the rate of the overall parallel concatenated code is:

$$R = \frac{1}{\frac{n_1}{k_1} + \frac{n_2}{k_2} - 1} \ \frac{\text{bits}}{\text{symbol}} \ . \tag{20}$$

The IOWEFs of its component codes are represented by the following matrices: $P_1 = [A_{i,j}^{C_1}]$ $(0 \le i \le k_1, \, 0 \le j \le n_1 - k_1)$ is a matrix of dimension $(k_1 + 1) \times (n_1 - k_1 + 1)$ for the block code C_1, and similarly $P_2 = [A_{i,j}^{C_2}]$ is a matrix of dimension $(k_2 + 1) \times (n_2 - k_2 + 1)$ for the block code C_2.

The IOWEF constructed of s codewords of block code C_1 can be represented by matrix Q_1 of dimensions $(sk_1 + 1) \times \Big(s(n_1 - k_1) + 1\Big)$, resulting in $s - 1$ consecutive two-dimensional convolutions of matrix P_1. This matrix represents the IOWEF of the (sn_1, N) block code. Similarly, the IOWEF constructed by ℓ codewords of block code C_2 can be represented by a matrix of dimensions $(\ell k_2 + 1) \times \Big(\ell(n_2 - k_2) + 1\Big)$ resulting in $\ell - 1$ consecutive two-dimensional convolutions of matrix P_2. Matrix Q_2 represents the IOWEF of the $(\ell n_2, N)$ block code. These operations, performed on matrices, are equivalent to equation (16) in [6], referring to polynomials. It is noted that the $(i+1)$th row of such a matrix refers to the coefficients of the *conditional* IOWEF of the corresponding code, if the information weight of the binary systematic code is i. Therefore, the calculation of a partial derivative order i, used for calculating the conditional IOWEF from the IOWEF code (equation (17) in [6]) is *avoided* here.

Finally, the matrix $S = [A_{i,j}^{C_p}]$ representing the IOWEF turbo-block code C_p is determined by calculating each one of the $N + 1$ rows separately: the $(i + 1)$th row of matrix $S \, (0 \le i \le N)$ is $\begin{pmatrix} N \\ i \end{pmatrix}^{-1}$ times the one-dimensional convolution between the two vectors in the $(i + 1)$th row of matrices Q_1 and Q_2 (both matrices have the same number of rows, as the equality: $sk_1 = \ell k_2$ holds). This operation on vectors is analogous to equation (18) in [6], that refers to polynomials.

The algorithm suggested here is very efficient, as it operates only on matrices and vectors. Moreover, one and two dimensional convolutions are built-in functions in some general computer facilities, and therefore this algorithm is easily implemented . For the particular case where C_1 and C_2 are similar binary systematic block codes and also $s = l$ (as in our case here), the complexity of the algorithm is further reduced due to the equalities: $P_1 = P_2$ and $Q_1 = Q_2$.

The IOWEF of two turbo-Hamming codes are presented in Figs. 14,16: $\log_{10}(A_{i,j})$ is plotted, as a function of the information weight i and the parity weight j of the codewords (where $0 \le i \le N$ and $0 \le j \le J$).

C. Upper Bounds on the bit error probability of soft decision ML decoding for turbo-Hamming codes

In this section we apply some upper bounds on the bit error probability of soft decision ML decoding for turbo-Hamming codes, and compare these bounds with simulation results of the iterative decoding algorithm [16], where different types structured and statistical of interleavers of length N are considered.

The ensemble performance of turbo-Hamming codes with (7, 4) Hamming component codes and a uniform interleaver of length $N = 16$, is analyzed in [6], relying on the union bounding technique (in its looser exponential form). In general, for large enough values of N, the usefulness of the union bounding technique (even in its Q-form), is limited to rates below the cutoff rate of the channel. Therefore, we apply here in addition to the union bound (in its Q-form), an improved upper bound that is a version of the tangential sphere bound, derived in [32].

The usefulness of the later bound is demonstrated for these ensembled codes, at rates exceeding the cutoff rate of the binary-input AWGN channel, where the performance of the iterative decoding is satisfactory, but the union bounds become useless (see Figs. 15,17). For example, in Fig. 17, the rate $R = 0.722$ bits/symbol turbo-Hamming code is constructed by the two identical (31, 26) Hamming codes and a uniform interleaver of length $N = 676$. The value of $\frac{E_b}{N_0}$ that corresponds to the cutoff rate of the binary-input AWGN channel is 3.32 dB. By the union bounding technique (Q-from), the upper bound on the bit error probability yields 10^{-3} at $\frac{E_b}{N_0} = 3.38$ dB, while with the version of the tangential sphere bound from [32], the same upper bound on the bit error probability (10^{-3}) is achieved at $\frac{E_b}{N_0} = 3.02$ dB (an improvement of 0.36 dB).

Moreover, it is reflected in Figs. 15 and 17 that the upper bounds on the bit error probability of soft decision ML decoding are sufficiently close to the iterative decoding simulation results [16], at rates below the cutoff rate of the channel.

Finally, based on the insight provided in [16] for the influence of the interleaver structure on the ensemble performance of turbo-Hamming codes and the advantage of the diagonal interleaver over the block and uniform interleavers (as is indicated also in Figs. 15,17), we get some results substantiating the advantage of this diagonal interleaver for a general value of $m \geq 3$ (and not only for $m = 3$, as explained in [16]). This is concluded straightforwardly, based on the interpretation in [16], and are therefore summarized here briefly. For a block interleaver, the quantity of the different numbers of check equations per data symbol increases linearly with m (equals $2m - 3$, for $m \geq 3$). On the other hand, for a diagonal interleaver, the quantity of the different numbers of check equations per data symbol is constant for $m \geq 4$, and equals 3. Therefore, the quantity

of the different numbers of check equations per data symbol is smaller for a diagonal interleaver than for a block interleaver. As expected the *average* number of check equations per data symbol is independent on the type of the interleaver. On the other hand, the standard deviation of the quantity of the different number of check equations per data symbol is an increasing function of m for a block interleaver, in contrast to the case for a diagonal interleaver, where it is approximately constant and gets its maximal value for $m = 5$. The results above are summarized in Table 3.

Based on the insight provided in [16], that the interleaving scheme is improved by choosing a permutation, such that the standard deviation of the number of check equations per symbol is reduced, it follows that for a turbo-Hamming code the diagonal interleaver provides better performance than block interleaving. Finally, the turbo-Hamming codes considered here, can be viewed as a direct product code of two identical Hamming codes, excluding the m^2 parity bits encoded by the parity bits of its components. Therefore, the code rates of these turbo-Hamming codes are slightly above the corresponding rates of the product codes having the same component codes. There is however a slight associated degradation in their performance, in comparison to product codes, as is evidenced by simulation results in [16].

6. Summary and Conclusions

The performance of structured binary, systematic block codes operating over the Gaussian channel is assessed by bounds on the error probability of soft decision ML decoding and is compared to reported results of the suboptimal iterative decoding algorithm [21]. It is observed that for such block codes of short length, the degradation in the performance of the iterative decoding algorithm is moderate (as compared to ML decoding). On the other hand, for long block codes that possess also a large number of codewords, the degradation in performance of the suboptimal algorithm is considerably increased. These conclusions based on comparisons between the two decoding rules for a variety of block codes, are consistent also with previous results reported for turbo codes with recursive systematic convolutional codes. It is demonstrated here that the degradation in the performance of the iterative decoding algorithm as compared to optimal ML decoding, increases considerably for complex and long enough structured block codes (see Tables 1,2).

Our bounding techniques are based on the tangential sphere bounds [26],[32] and some versions of the Gallager's 1963 bound [12],[33]. There is a slight improvement in the upper bound on the bit error probability (derived from Gallager's 1963 bound) [33] where the ensemble of random, binary and *systematic* (n, k) block codes is considered, instead of the whole ensemble of random, binary block codes (including also the non-systematic block codes), as is indeed demonstrated here. The error exponents of the upper bounds for these two ensembles of codes are evidently the same

(asymptotically if $n \to \infty$) as are also the upper bounds on the *block* error probability for these two ensembles of codes.

Although, the outer and the inner code components of *uniformly* interleaved and serially concatenated RA codes possess a very simple structure: a repetition and a differential encoder respectively, the tangential sphere bounds on their block and bit error probabilities indicate impressive performance at rates exceeding the cutoff rate. This is also evidenced by simulations of the iterative decoding algorithm (reported by Divsalar, Jin and McEliece) for a *specific* structured interleaver (evidently better than the statistical uniform interleaver, as is demonstrated in [11]).

We focus here on parallel concatenated turbo-Hamming codes, and as the upper bounds on the block and bit error probabilities rely on the distance spectrum and IOWEF codes respectively, efficient algorithms are derived for their calculation. The tangential sphere upper bounds applied to ML-decoded uniformly interleaved turbo-Hamming codes are compared with simulation results for iterative decoding (with some types of interleavers) reported by Huber, Schetelig and Wachsmann [16]. Finally, based on the insight provided in [16] for the advantage of the diagonal interleaver over the block and uniform interleavers for these turbo-Hamming codes, we present some further analytical results related to the comparison between diagonal and block interleavers for these codes (see Table 3).

Appendix: Derivation of IOWEF for $(2^m - 1,\, 2^m - m - 1)$ Hamming Codes

The IOWEF of a binary, linear and systematic (n, k) block code is of the form:

$W(x, y) = \sum_{i=0}^{k} \sum_{j=0}^{n-k} A_{i,j}\, x^i y^j$, where $A_{i,j}$ denotes the number of codewords with information weight i and parity weight j $(0 \le i \le k\,,\ 0 \le j \le n-k)$.

The derivation of IOWEF for $(2^m - 1, 2^m - m - 1)$ Hamming codes is based on its particular algebraic structure: In systematic form, the vectors of the parity-bits in the generator matrix G are all the binary vectors of length m, with a Hamming weight of at least 2. These vectors of length m bits are the parity bits of all the $2^m - m - 1$ Hamming codewords, encoded by $2^m - m - 1$ information bits of weight $i = 1$. As Hamming codes are linear, we get $A_{0,0} = 1$ (that corresponds to the all-zero codeword), and $A_{0,j} = 0$ for $1 \le j \le m$. Moreover, based on this particular property of Hamming codes:

$$A_{1,0} = A_{1,1} = 0 \quad \text{and also} \quad A_{1,j} = \begin{pmatrix} m \\ j \end{pmatrix} \quad \text{for} \quad 2 \le j \le m\,. \tag{A.1}$$

For calculating the coefficient $A_{2,1}$, we address the following two cases:

1. For any codeword c having an information weight $i = 1$ and parity weight $j = 2$, there are $m - 2$ codewords having an information weight $i = 1$ and parity weight $j = 3$, such that their sum $c + c'$ is a codeword with an information weight $i = 2$ and parity weight $j = 1$. The reason is that for Hamming codes, the binary vectors of the parity bits are all the vectors of length m with Hamming weights of at least 2, and therefore, for every chosen parity vector of weight $j = 2$, there are $m - 2$ other parity vectors of weight $j = 3$, that each one of them differs from the first vector in a single place (the two parity vectors with a unique '1' that also differ from the first vector in a single place are not accepted, since the parity bits of codewords with information weight $i = 1$ have weights $j \ge 2$).

2. For any codeword c having an information weight $i = 1$ and parity weight $j \ge 3$, there are m codewords c' with an information weight $i = 1$ and a parity weight $j \ge 2$, such that their sum $c + c'$ is a codeword with information weight $i = 2$ and a parity weight $j = 1$. The argument is based again on the particular vectors of parity bits of the Hamming codewords.

Therefore, we find:

$$\begin{aligned} A_{2,1} &= \frac{1}{2}\left\{\sum_{j=3}^{m}\Big[m\binom{m}{j}\Big]+(m-2)\binom{m}{2}\right\} \\ &= \frac{1}{2}\left[m\sum_{j=3}^{m}\binom{m}{j}+\frac{m(m-1)(m-2)}{2}\right] \\ &= \frac{1}{2}\left[m\Big(2^m-1-m-\frac{m(m-1)}{2}\Big)+\frac{m(m-1)(m-2)}{2}\right] \\ &= m\Big(2^{m-1}-m\Big)\,. \end{aligned} \tag{A.2}$$

Similarly, based on the same property of Hamming codes, we also calculate the coefficient $A_{2,2}$: if the binary vector of parity bits in one of the 2^m-m-1 codewords in the matrix G has weight $j\geq 4$, then every vector of length m that differs from it in two places has a weight of at least two, $j\geq 2$, and each one of these parity vectors corresponds to a Hamming codeword in the matrix G in its systematic form (that each one of its codewords has an information weight $i=1$). Alternatively, if for such a Hamming codeword, the parity weight is $j=3$, there are three vectors of parity bits having weight $j=1$, that each one of them differs from the parity bits above in two places. These three vectors of length m, cannot be Hamming codewords with information weight $i=1$ (i.e, these parity bits cannot correspond to one of the 2^m-m-1 codewords in the generator matrix G, expressed in its systematic form). Moreover, for a Hamming codeword with an information weight $i=1$ and a parity weight $j=2$, all the codewords that their parity vectors differ in two places from the parity vector of the considered codeword, except the all-zero codeword, are Hamming codewords having an information weight $i=1$ (as, except for the all-zero codeword, the parity weight of these codewords is at least 2. So relying the property of Hamming codes, such a codeword is one of the Hamming codewords in the matrix G).

These considerations yield the following expression for the coefficient $A_{2,2}$ of the IOWEF:

$$\begin{aligned} A_{2,2} &= \frac{1}{2}\left\{\sum_{j=4}^{m}\binom{m}{j}\binom{m}{2}+\binom{m}{3}\Big[\binom{m}{2}-3\Big]+\binom{m}{2}\Big[\binom{m}{2}-1\Big]\right\} \\ &= \frac{1}{2}\left[\binom{m}{2}\sum_{j=2}^{m}\binom{m}{j}-3\binom{m}{3}-\binom{m}{2}\right] \\ &= \frac{1}{2}\left[\binom{m}{2}\Big(2^m-m-1\Big)-\frac{m(m-1)(m-2)}{2}-\frac{m(m-1)}{2}\right] \\ &= \frac{1}{2}\left[\binom{m}{2}\Big(2^m-m-1\Big)-(m-1)\binom{m}{2}\right] \\ &= \binom{m}{2}\Big(2^{m-1}-m\Big)\,. \end{aligned} \tag{A.3}$$

Similar considerations for an integer p such that $3 \leq p \leq m$, give rise to the following expression for the coefficient $A_{2,p}$ of IOWEF of the $(2^m - 1,\, 2^m - m - 1)$ Hamming code:

$$\begin{aligned} A_{2,p} \;=\; & \frac{1}{2}\left\{ \sum_{k=p+2}^{m} \binom{m}{k} \cdot \binom{m}{p} + \binom{m}{p+1} \left[\binom{m}{p} - (p+1) \right] \right. \\ & + \binom{m}{p} \left[\binom{m}{p} - 1 \right] + \left[\binom{m}{p-1} \left[\binom{m}{p} - (m-p+1) \right] \right. \\ & \left. \left. + \sum_{k=2}^{p-2} \binom{m}{k} \cdot \binom{m}{p} \right\} \right. . \end{aligned} \tag{A.4}$$

If $p = 3$, the last term in (A.4) is zero and if $p > m-2$, the first term in (A.4) is zero. However, for any integer p, such that $3 \leq p \leq m$, the expression above can be further simplified to the following form:

$$\begin{aligned} A_{2,p} \;&=\; \frac{1}{2}\left[\binom{m}{p} \sum_{k=2}^{m} \binom{m}{k} - (p+1)\binom{m}{p+1} - \binom{m}{p} - (m-p+1)\binom{m}{p-1} \right] \\ &=\; \left[\binom{m}{p} \left(2^m - m - 1\right) - \frac{(p+1)\,m!}{(p+1)!\,(m-p-1)!} - \binom{m}{p} - \frac{(m-p+1)\,m!}{(p-1)!\,(m-p+1)!} \right] \\ &=\; \frac{1}{2}\left[\binom{m}{p} \left(2^m - m - 2\right) - \frac{(m-p)\,m!}{p!\,(m-p)!} - \frac{p \cdot m!}{p!\,(m-p)!} \right] \\ &=\; \frac{1}{2}\left[\binom{m}{p} \left(2^m - m - 2\right) - m\binom{m}{p} \right] \\ &=\; \binom{m}{p} \left(2^{m-1} - m - 1\right), \quad 3 \leq p \leq m \,. \end{aligned} \tag{A.5}$$

To conclude, by (A.2),(A.3) and (A.5), we find that:

$$A_{2,j} = \begin{cases} 0 & \text{if } j = 0 \\ \binom{m}{j} \left(2^{m-1} - m\right) & \text{if } j = 1, 2 \\ \binom{m}{j} \left(2^{m-1} - m - 1\right) & \text{if } 3 \leq j \leq m \,. \end{cases} \tag{A.6}$$

For calculating the coefficients $A_{i,j}$ of the IOWEF in case that $2 < i \leq 2^m - m - 1$ and $1 \leq j \leq m$, we derive here a recursive equation, based again on the particular property of Hamming codes:

Suppose that we have a Hamming codeword c with an information weight of $i-1$ and a parity weight of k. If $k \geq j+2$, then any vector of parity bits (of length m) that differs from the vector of the parity bits of the considered codeword c in j places, has a parity weight of at least $k - j \geq 2$. Therefore, the information weight of such a codeword c', is therefore 1 (as this is one of

the codewords in the $2^m - m - 1$ rows of the generator matrix G of the Hamming code, when it is expressed in a systematic form). The codeword $c + c'$ is a Hamming codeword with information weight that may only be $i - 2$ or i. If, however, $k = j + 1$, then all the vectors of length m that differ from the vector of parity bits of c in j places, all of them (except $j + 1$ vectors of length m that are of weight 1), have at least a weight of 2. Therefore, all the codewords c' (except for $j + 1$ codewords with the corresponding $j + 1$ vectors of parity bits), are Hamming codewords with an information weight 1. As before, the codeword $c + c'$ is a codeword with an information weight i or $i - 2$. The same considerations are performed when $k \leq j$ (we divide it to the three sub-cases $k = j$, $k = j - 1$ and finally $k \leq j - 2$).

Moreover, if the Hamming codeword $c + c'$ has an information weight i and a parity weight j, as the addition (modulo 2) is commutative and associative, then by covering all the possibilities of codewords c with an information weight $i - 1$ and codewords c' from the $2^m - m - 1$ rows of the generator matrix G (in its systematic form) that differ from c in j parity bits (and have also an information weight of 1), we get that the number of possibilities of $c + c'$ is i times the number of codewords with an information weight i and a parity weight j (i.e, $iA_{i,j}$). The reason is by this procedure we get i times each codeword of information weight i and parity weight j. If, however, the Hamming codeword $c + c'$ has an information weight $i - 2$ and a parity weight j, then by covering all the possibilities of the codewords c with an information weight $i - 1$ and codewords c' from the rows of the generator matrix G of the Hamming code, that their parity bits differ from those of the codewords c in j places (and as before each of the codewords c' has an information weight of 1), this procedure yields $2^m - m - 1 - (i - 2)$ times the number of the codewords with an information weight $i - 2$ and a parity weight j (i.e, $(2^m - m - i + 1)A_{i-2,j}$).

Based on the arguments above, we find the following recursive equation for calculating the coefficients $A_{i,j}$ (when $2 < i \leq 2^m - m - 1$ and $1 \leq j \leq m$) for IOWEF of Hamming codes:

$$\begin{aligned} & iA_{i,j} + \left[2^m - m - 1 - (i-2)\right] A_{i-2,j} \\ = & \sum_{k=j+2}^{m} A_{i-1,k} \cdot \left(\begin{array}{c} m \\ j \end{array} \right) + A_{i-1,j+1} \cdot \left[\left(\begin{array}{c} m \\ j \end{array} \right) - (j+1) \right] \\ + & A_{i-1,j} \cdot \left[\left(\begin{array}{c} m \\ j \end{array} \right) - 1 \right] + A_{i-1,j-1} \cdot \left[\left(\begin{array}{c} m \\ j \end{array} \right) - (m-j+1) \right] \\ + & \sum_{k=0}^{j-2} A_{i-1,k} \cdot \left(\begin{array}{c} m \\ j \end{array} \right) . \end{aligned} \tag{A.7}$$

A simplication of the right hand side of (A.7), results in the following:

$$\begin{aligned}
& \sum_{k=j+2}^{m} A_{i-1,k} \cdot \left(\begin{array}{c} m \\ j \end{array} \right) + A_{i-1,j+1} \cdot \left[\left(\begin{array}{c} m \\ j \end{array} \right) - (j+1) \right] \\
+ \quad & A_{i-1,j} \cdot \left[\left(\begin{array}{c} m \\ j \end{array} \right) - 1 \right] + A_{i-1,j-1} \cdot \left[\left(\begin{array}{c} m \\ j \end{array} \right) - (m-j+1) \right] \\
+ \quad & \sum_{k=0}^{j-2} A_{i-1,k} \cdot \left(\begin{array}{c} m \\ j \end{array} \right) \\
= \quad & \sum_{k=0}^{m} A_{i-1,k} \cdot \left(\begin{array}{c} m \\ j \end{array} \right) - (j+1) A_{i-1,j+1} - A_{i-1,j} - (m-j+1) A_{i-1,j-1} \\
= \quad & \left(\begin{array}{c} 2^m - m - 1 \\ i-1 \end{array} \right) \left(\begin{array}{c} m \\ j \end{array} \right) - (j+1) A_{i-1,j+1} - A_{i-1,j} - (m-j+1) A_{i-1,j-1} \, .
\end{aligned} \tag{A.8}$$

Hence, we get the recursive equation:

$$\begin{aligned}
& i A_{i,j} + (2^m - m - i + 1) A_{i-2,j} \\
= \quad & \left(\begin{array}{c} 2^m - m - 1 \\ i-1 \end{array} \right) \left(\begin{array}{c} m \\ j \end{array} \right) - (j+1) A_{i-1,j+1} - A_{i-1,j} - (m-j+1) A_{i-1,j-1} \, . \\
\Rightarrow \quad & A_{i,j} = \frac{1}{i} \left[\left(\begin{array}{c} 2^m - m - 1 \\ i-1 \end{array} \right) \left(\begin{array}{c} m \\ j \end{array} \right) - (j+1) A_{i-1,j+1} - A_{i-1,j} \right. \\
& \left. -(m-j+1) A_{i-1,j-1} - \left(2^m - m - i + 1 \right) A_{i-2,j} \right] \, .
\end{aligned} \tag{A.9}$$

where $1 \leq i \leq 2^m - m - 1$, $1 \leq j \leq m$ (if $j = m$, then $A_{i-1,j+1} \equiv 0$).

Since the $\left(2^m - 1, \, 2^m - m - 1 \right)$ Hamming code is linear, we find also that:

$$\begin{aligned}
& A_{i,j} = A_{2^m - m - 1 - i, m - j} \quad (m \text{ parity bits and } 2^m - m - 1 \text{ information bits}) \quad \text{for} \\
& i = 0, 1, 2 \ldots \left\lfloor \frac{2^m - m - 1}{2} \right\rfloor \, , \; j = 0, 1, 2 \ldots m \, .
\end{aligned} \tag{A.10}$$

It seems that the number of Hamming codewords having an information weight i and a parity weight j is approximately:

$$A_{i,j} \approx 2^{-m} \left(\begin{array}{c} 2^m - m - 1 \\ i \end{array} \right) \left(\begin{array}{c} m \\ j \end{array} \right) \, , \tag{A.11}$$

where $0 \leq i \leq 2^m - m - 1$ and $0 \leq j \leq m$. Surprisingly, the approximated expression (A.11) is also a *particular* solution of the recursive equation (A.9). Moreover, (A.11) relates to the *average* number of codewords with information weight i and parity weight j in the ensemble of binary and

systematic $\left(2^m - 1, 2^m - m - 1\right)$ block codes. The $\left(2^m - 1, 2^m - m - 1\right)$ Hamming code is a particular code of this ensemble of codes, that behaves approximately like the average of the whole ensemble. The approximation (A.11) is very tight for $m \geq 5$, as is clearly indicated in the following two examples:

1. For $m = 5$, the (31,26) Hamming code, and for $i = 3$ and $j = 4$, the accurate analysis yields $A_{i,j} = 400$, while the approximated value in (A.11) is 406.25.

2. For $m = 6$, the (63,57) Hamming code, and for $i = 6$, $j = 4$, the accurate analysis yields $A_{i,j} = 8.504 \cdot 10^6$, while the approximated value in (A.11) is $8.505 \cdot 10^6$.

References

[1] P. Adde, R. Pyndiah and O. Raoul, "Performance and complexity of block turbo decoder circuits", *Proceedings of the Third IEEE International Conference on Electronics, Circuits and Systems (ICECS '96)*, pp. 172–175, New-York, USA, 1996.

[2] P. Adde, R. Pyndiah, O. Raoul and J. R. Inisan, "Turbo block decoder design", *Proceedings of the International Symposium on Turbo Codes and Related Topics*, pp. 166–169, Brest, France, 3–5 September 1997.

[3] O. Aitsab and R. Pyndiah, "Performance of Reed-Solomon block turbo code", *Proceedings of the IEEE GLOBECOM 1996*, pp. 121–125, London, England, 18–21 November 1996.

[4] L. R. Bahl. J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate", *IEEE Trans. on Information Theory*, vol. 25, pp. 342–345, 1979.

[5] S. A. Barbulescu, "Iterative decoding of turbo codes and other concatenated codes", Ph.D. dissertation, Faculty of Engineering, University of South Australia, February 1996.

[6] S. Benedetto and G. Montorsi, "Unveiling turbo codes: some results on parallel concatenated coding schemes", *IEEE Trans. on Information Theory*, vol. 42, no. 2, pp. 409–428, March 1996.

[7] S. Benedetto, D. Divsalar, G. Montorsi and F. Pollara, "Serial concatenation of interleaved codes: performance, analysis, design and iterative decoding", *IEEE Trans. on Information Theory*, vol. 44, no. 3, pp. 909–926, May 1998.

[8] C. Berrou, S. Evano and G. Battail, "Turbo-Block-Codes", Seminar on Turbo Coding, Lund University, Sweden, 28–29 August 1996.

[9] G. Buch and F. Burkert, "Unequal error protection with product-like turbo codes", *Proceedings 1998 IEEE International Symposium on Information Theory (ISIT '98)*, p. 60, MIT Cambridge, MA, USA, 16–21 August 1998.

[10] J. F. Cheng and R. J. McEliece, "Unit-memory Hamming turbo codes", *Proceedings 1995 IEEE International Symposium on Information Theory*, Whistler, British Columbia, Canada, September 17–22, 1995.

[11] D. Divsalar, H. Jin and R. J. McEliece, "Coding theorems for turbo-like codes", *1998 Allerton Conference*, September 23–25, 1998.

[12] R. G. Gallager, "Low density parity check codes", MIT Press, Cambridge, Massachusetts, 1963.

[13] A. Goalic and R. Pyndiah, "Real-time turbo-decoding of product codes on a digital signal processor", *Proceedings of IEEE GLOBECOM 1997*, pp. 624–628, Phoenix, Arizona USA, 3–8 November 1997.

[14] P. Guinand, J. Lodge and L. Papke, "An alternative approach to the design of interleavers for block-turbo codes", *Information Theory and Applications II, 4th Canadian Workshop*, Canada, May 1995. Selected Papers: Springer-Verlag, pp. 95–103, Berlin, Germany, 1996.

[15] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes", *IEEE Trans. On Information Theory*, vol. 42, no. 2, pp. 429–445, March 1996.

[16] J. Huber, M. Schetelig and U. Wachsmann, "Turbo codes over simple block codes and turbo-product codes", *Mediterranean Workshop on Coding and Information Integrity*, Palma De Mallorca, Spain, 28 February, 1996.

[17] G. L. Katsman and M. A. Tsafsman, "Spectra of algebraic geometric codes", *Problems of Information Transmission*, vol. 23, no. 1–4, pp. 262–275, 1987.

[18] M. Lentmaier and K. Sh. Zigangirov, "Iterative decoding of generalized low-density parity-check codes", *Proceedings 1998 IEEE International Symposium on Information Theory (ISIT '98)*, p. 149, MIT Cambridge, MA, USA, 16–21 August 1998.

[19] J. Lodge, R. Young, P. Hoeher and J. Hagenauer, "Separable MAP 'filters' for the decoding of product and concatenated codes", *Proceedings of the IEEE International Conference on Communications ICC'93*, pp. 1740–1745, Geneva, Switzerland, May 23–26, 1993.

[20] R. Lucas, "On iterative soft-decision decoding of linear binary block codes", Ph.D. dissertation, Univ. Ulm, Germany, 1997.

[21] R. Lucas, M. Bossert and M. Breitbach, "On iterative soft-decision decoding of linear binary block codes and product codes", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 2, pp. 276–296, February 1998.

[22] M. Moher and T.A. Gulliver, "Cross-entropy and iterative decoding", *IEEE Trans. on Information Theory*, vol. 44, no. 7, pp. 3014–3097, November 1998.

[23] H.T. Moorthy, S. Lin and T. Kassami, "Soft decision decoding of binary linear block codes based on iterative search algorithm", *IEEE Trans. On Information Theory*, vol. 43, no. 3, pp. 1030–1039, May 1997.

[24] H. Nickl, J. Hagenauer and F. Burkert, "Approaching Shannon's capacity limit by 0.27 dB using simple Hamming codes", *IEEE Communications Letters*, vol. 1, no. 5, pp. 130–132, September 1997. See also: H. Nickl, J. Hagenauer and F. Burkert, "The race to Shannon's limit: Discipline high-rate codes", *Proceedings of the International Symposium on Turbo Codes and Related Topics*, pp. 239–242, Brest, France, 3–5 September 1997.

[25] Li Ping, S. Chan and K. L. Yeung, "Iterative decoding of multidimensional concatenated single parity check codes", *Proceedings 1998 IEEE International Conference on Communications*, Atlanta, USA, June 1998.

[26] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra", *IEEE Trans. on Information Theory*, vol. 40, no. 4, July 1994. See also: H. Herzberg and G. Poltyrev, "The error probability of M-ary PSK block coded modulation schemes", *IEEE Trans. on Communications*, vol. 44, no. 4, pp. 427–433, April 1996.

[27] R. Pyndiah, A. Glavieux, A. Picart and S. Jacq, "Near optimum decoding of product codes", *Proceedings of IEEE GLOBECOM 1994 Conference*, pp. 339–343, San Francisco, USA, 28 November–2nd December, 1994.

[28] R. Pyndiah, A. Picart and A. Glavieux, "Performance of block turbo coded 16–QAM and 64–QAM modulations", *Proceedings of IEEE GLOBECOM 1995 Conference*, pp. 1039–1043, Singapore, 13–17 November 1995.

[29] R. Pyndiah, P. Combelles and P. Adde, "A very low complexity block turbo decoder for product codes", *Proceedings of IEEE GLOBECOM 1996*, pp. 101–105, London, England, 18–22 November 1996.

[30] R. Pyndiah, "Iterative decoding of product codes: block turbo codes", *Proceedings of the International Symposium on Turbo Codes and Related Topics*, pp. 71–79, Brest, France, 3–5 September 1997.

[31] R. Pyndiah, "Near Optimum decoding of product codes: block turbo codes", *IEEE Trans. on Communications*, vol. 46, no. 8, pp. 1003–1010, August 1998.

[32] I. Sason and S. Shamai (Shitz), "Improved upper bounds on the decoding error probability of parallel and serial concatenated turbo codes via their ensemble distance spectrum", Technical Report No. CC–237, Technion—Israel Institute of Technology, February 1998. To appear in *IEEE Trans. on Information Theory*. See also: *Proceedings 1998 IEEE International Symposium on Information Theory (ISIT '98)*, p. 30, MIT, Cambridge, MA, USA, 16–21 August 1998.

[33] I. Sason and S. Shamai (Shitz), "Gallager's 1963 bound: Extensions and Observations", Technical Report No. CC–258, Technion, October 1998.

[34] S. Schaffler and J. Hagenauer, "Soft decision MAP decoding of binary linear block via global optimization", *Proceedings 1997 IEEE International Symposium on Information Theory (ISIT '97)*, p. 231, Ulm, Germany.

[35] E. Soljanin and R. Urbanke, "On the performance of recursive decoding schemes", *Proceedings 1997 IEEE International Symposium on Information Theory (ISIT '97)*, p. 9, Ulm, Germany. See also: Bell Laboratories, Lucent Technologies, Technical Report 1997.

[36] Y.V. Svirid, "Weight distributions and bounds for turbo-codes", *European Trans. on Telecommunications (ETT)*, vol. 6, no. 5, pp. 543–555, September-October 1995.

[37] L. Tulhuizen and S. Baggen, "On the weight enumerator of product codes", *Discrete Mathematics*, Vol. 106/107, pp. 483–488, 1992.

[38] L. Tulhuizen, S. Baggen and E. H. Nowacka, "Union bounds on the performance of product codes", *Proceedings 1998 IEEE International Symposium on Information Theory (ISIT'98)*, p. 267, MIT, Cambridge, MA, USA, 16–21 August, 1998.

Figure Captions

Figure 1: A comparison between the performance of the iterative decoding algorithm [21] and bounds on the block error probability of soft decision ML decoding for the (42,21) DC block code.

Figure 2: A comparison between the performance of the iterative decoding algorithm [21] and bounds on the block error probability of soft decision ML decoding for the (63,24) BCH block code.

Figure 3: A comparison between the performance of the iterative decoding algorithm [21] and bounds on the block error probability of soft decision ML decoding for the (63,39) BCH block code.

Figure 4: A comparison between the performance of the iterative decoding algorithm [21] and bounds on the block error probability of soft decision ML decoding for the (64,22) RM block code.

Figure 5: A comparison between the performance of the iterative decoding algorithm [21] and bounds on the block error probability of soft decision ML decoding for the (64,42) RM block code.

Figure 6: A comparison between the performance of the iterative decoding algorithm [21] for the (1023,781) EG block code and upper bounds on the bit error probability of two ensembles of random binary (1023,781) block codes with soft decision ML decoding.

Figure 7: A comparison between the performance of the iterative decoding algorithm [21] for the product (3969,1369) code, constructed by a direct product of two (63,37) EG codes, and an upper bound on the bit error probability of soft-decision ML decoding for the ensemble of random, systematic and binary (3969,1369) block codes.

Figure 8: The distance spectrum of some ensembles of uniformly interleaved, and serially concatenated, (qN, N) RA codes versus the normalized Hamming weights of the codewords (normalized with respect to the block length qN): $N = 1024$, $q = 2, 3, 4$.

Figure 9: A comparison between upper bounds on the block and bit error probabilities of two ensembles of uniformly interleaved and serially concatenated RA codes. The upper bounds considered are the tangential sphere bound and the union bound in Q-form.

Figure 10: A comparison between the block error probability of an iterative decoding algorithm for the (4096,1024) RA code ($N = 1024$, $q = 4$) for a *specific* structured interleaver (of length $qN = 4096$) [11], and upper bounds of ML decoding (considering a *uniform* interleaver).

Figure 11: A comparison between the block error probability of an iterative decoding algorithm for the (3072,1024) RA code ($N = 1024$, $q = 3$) for a *specific* structured interleaver (of length $qN = 3072$) [11], and upper bounds of ML decoding (considering a *uniform* interleaver).

Figure 12: The logarithm on base 10 of the IOWEF of the (31,26) Hamming code versus the information weight and the parity weight of its codewords.

Figure 13: The logarithm on base 10 of the IOWEF of the (255,247) Hamming code versus the information weight and the parity weight of its codewords.

Figure 14: The logarithm on base 10 of the IOWEF of the ensemble of parallel concatenated (209,121) turbo-Hamming codes, constructed by a uniform interleaver of length $N = 121$ and two identical (15,11) Hamming codes.

Figure 15: A comparison between analytical upper bounds on the bit error probability of soft decision ML decoding for the ensemble of parallel concatenated (209,121) turbo-Hamming

codes (constructed by a uniform interleaver of length $N = 121$ and two identical (15,11) Hamming codes), and iterative decoding simulation results with some different types of interleavers (based on [16]).

Figure 16: The logarithm on base 10 of the IOWEF of the ensemble of parallel concatenated (936,676) turbo-Hamming codes, constructed by a uniform interleaver of length $N = 676$ and two identical (31,26) Hamming codes.

Figure 17: A comparison between analytical upper bounds on the bit error probability of soft decision ML decoding for the ensemble of parallel concatenated (936,676) turbo-Hamming codes (constructed by a uniform interleaver of length $N = 676$ and two identical (31,26) Hamming codes), and iterative decoding simulation results for some different types of interleavers (based on [16]).

Table Captions

Table 1: The performance of iterative decoding algorithm [21] as compared to soft decision ML decoding for structured, binary systematic block codes of moderate length. The upper and lower bounds for ML decoding are based on the tangential sphere bound [26] and a simulated lower bound (see section B.6) respectively.

Table 2: A comparison between the bit error probability of iteratively decoded structured, binary and systematic long block codes as compared to upper bounds on the bit error probability of ML decoded random, binary and systematic block codes with the same block length and code rate. The upper bounds of ML decoding are based on a particular version of Gallager's 1963 bound (see section B.2).

Table 3: Comparison of some parameters of block and diagonal interleavers of turbo-Hamming codes.

The considered block code	$\frac{E_b}{N_0}$ required for a **block** error probability of 10^{-3}		Estimated loss in suboptimality
	iterative decoding algorithm [21]	ML decoding	
(42, 21) DC	3.93 dB	3.66 - 3.83 dB	0.10 - 0.27 dB
(63, 24) BCH	3.55 dB	2.98 - 3.28 dB	0.27 - 0.57 dB
(63, 39) BCH	4.16 dB	3.48 - 3.79 dB	0.37 - 0.69 dB
(64, 22) RM	3.59 dB	3.35 - 3.45 dB	0.14 - 0.24 dB
(64, 42) RM	4.19 dB	4.05 - 4.16 dB	0.03 - 0.14 dB

Table 1.

The considered block code	$\frac{E_b}{N_0}$ required for a **bit** error probability of 10^{-4}		Estimated loss in suboptimality
	iterative decoding algorithm [21]	Upper bound for ML decoding (soft decision)	
(1023, 781) EG	3.81 dB	2.93 dB	at least 0.88 dB
(3969, 1369) (product code)	1.48 dB	0.38 dB	at least 1.10 dB

Table 2.

The value of m	The quantity of different number(s) of check equations per symbol for the following type of interleaver of length N:			Average	standard deviation of the
	Block	Diagonal	Block/diagonal	Block	Diagonal
3	3	2	4.500	0.612	0.500
4	5	3	5.091	0.927	0.514
5	7	3	5.769	1.198	0.576
6	9	3	6.526	1.440	0.565
7	11	3	7.350	1.655	0.511
8	13	3	8.227	1.846	0.438

Table 3.

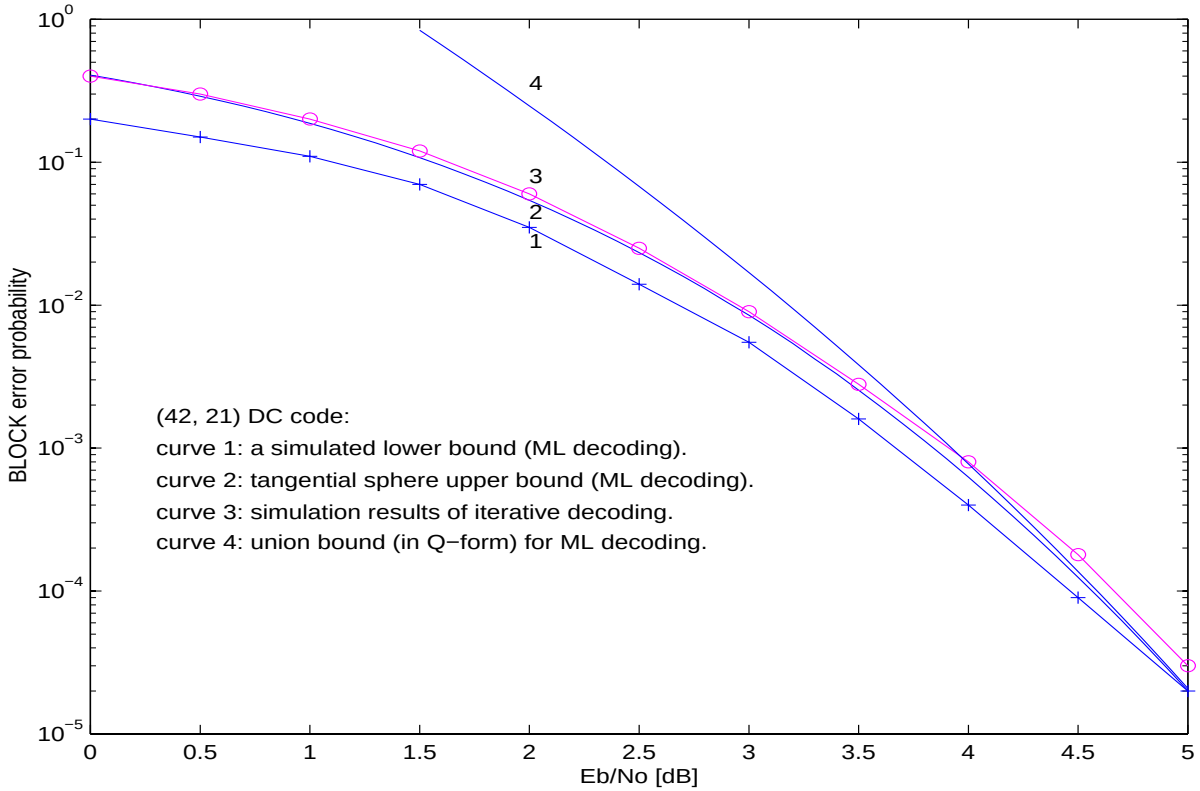

Figure 1.

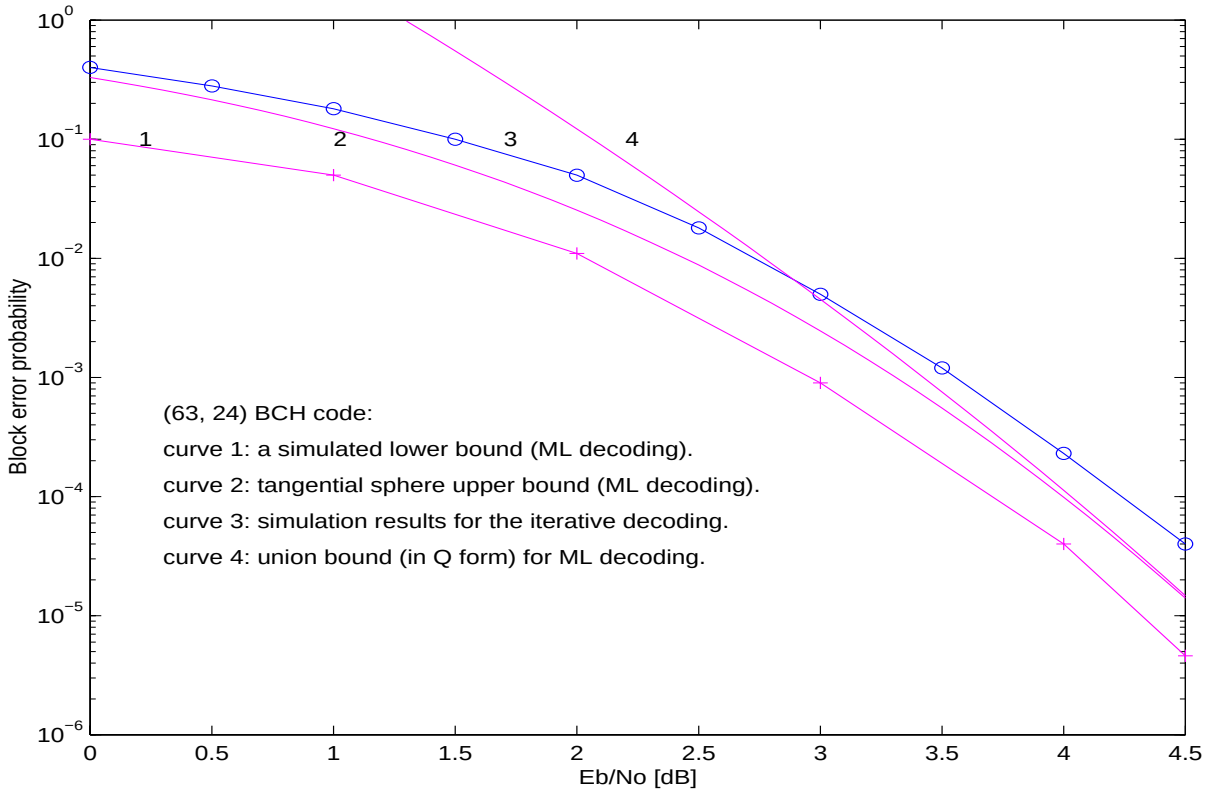

Figure 2.

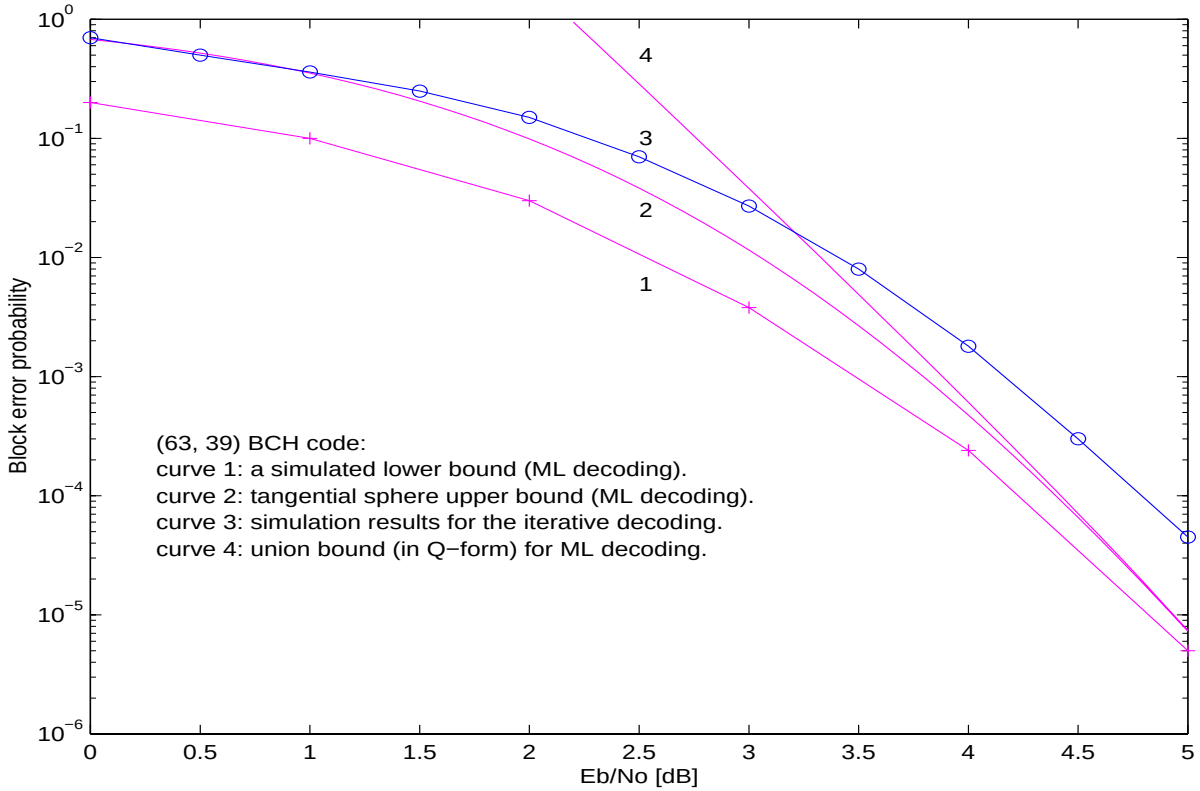

Figure 3.

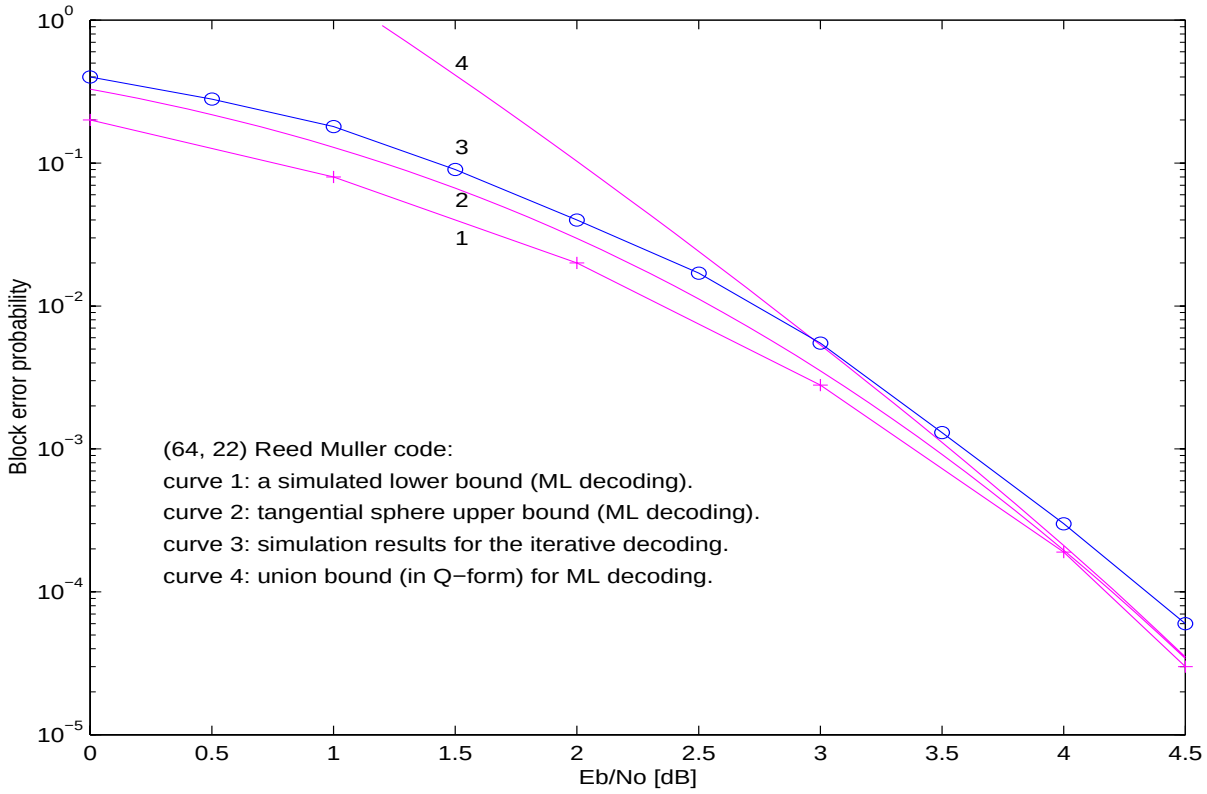

Figure 4.

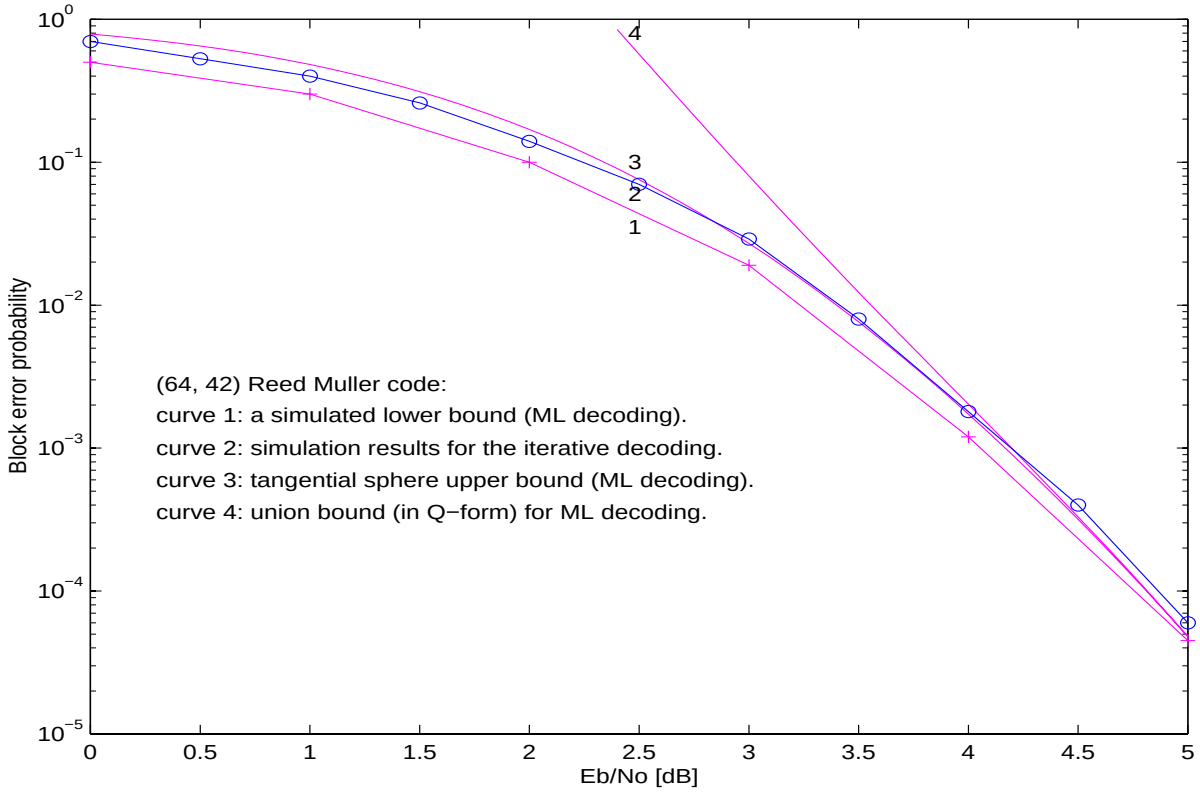

Figure 5.

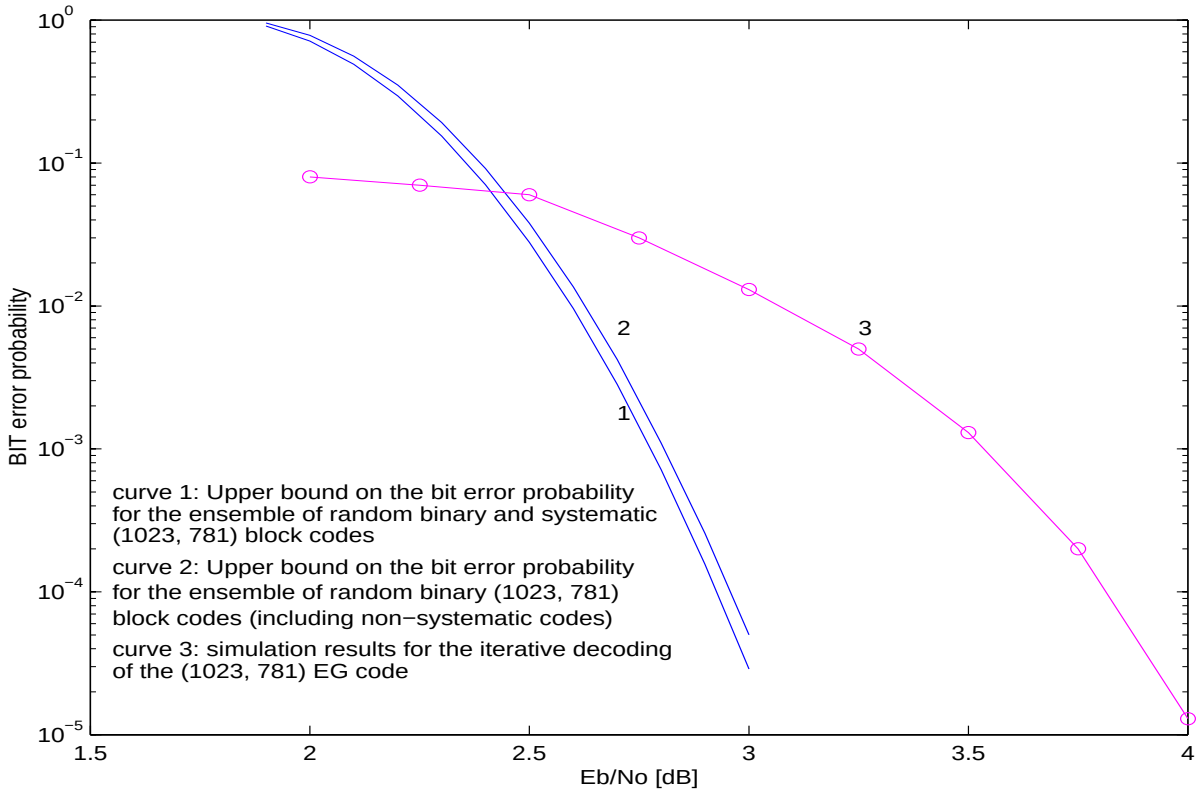

Figure 6.

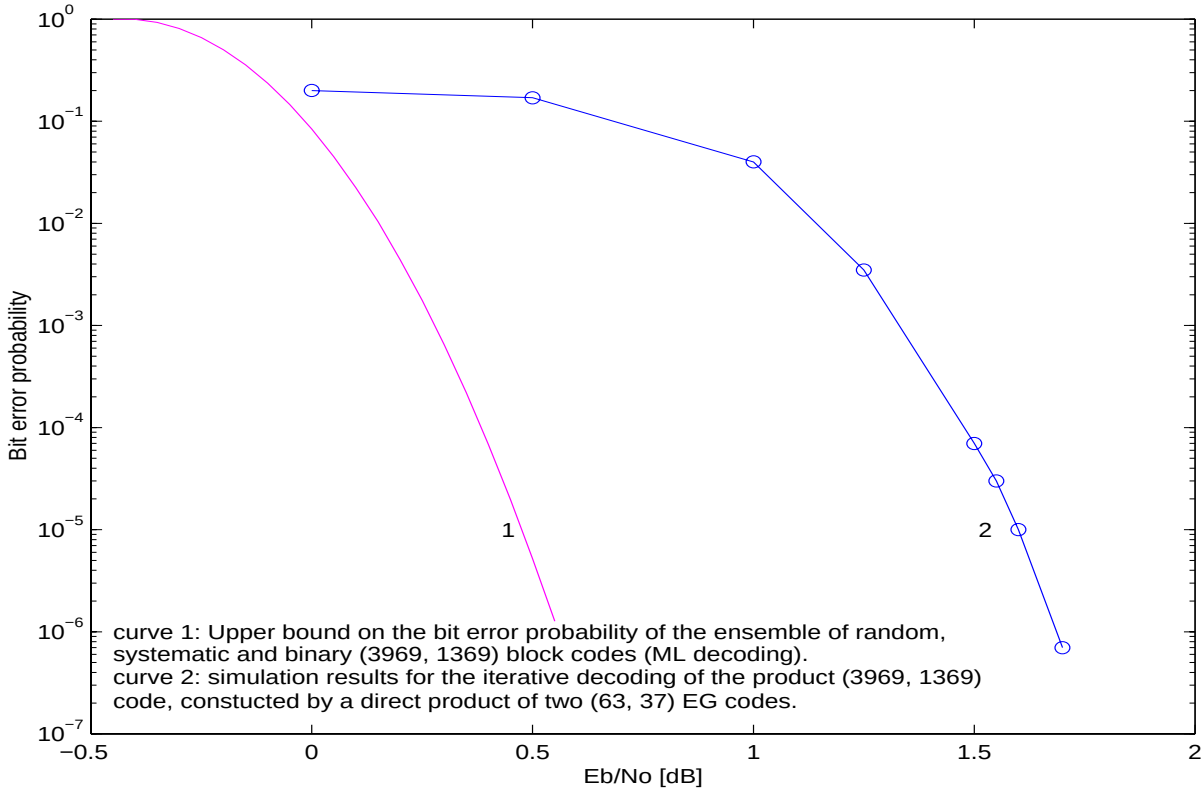
Bit error probability
Eb/No [dB]
1
2
curve 1: Upper bound on the bit error probability of the ensemble of random, systematic and binary (3969, 1369) block codes (ML decoding).
curve 2: simulation results for the iterative decoding of the product (3969, 1369) code, constucted by a direct product of two (63, 37) EG codes.

Figure 7.

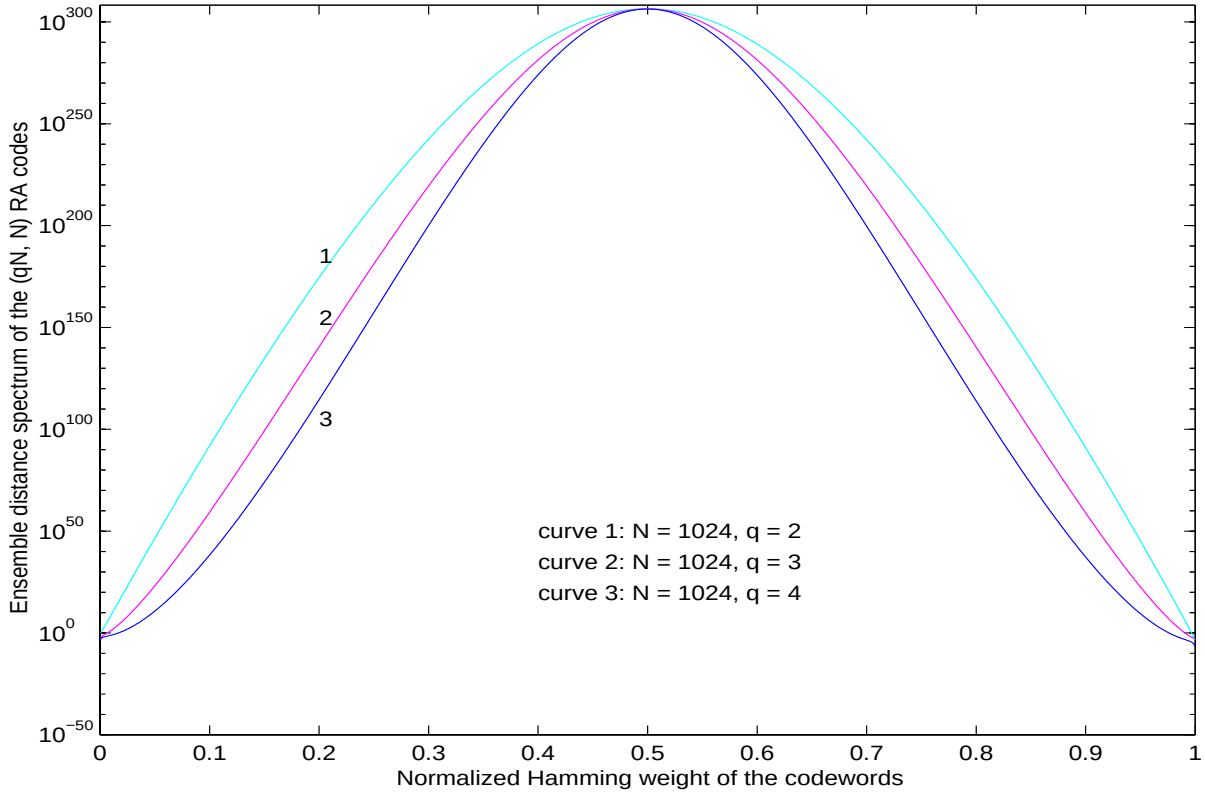

Figure 8.

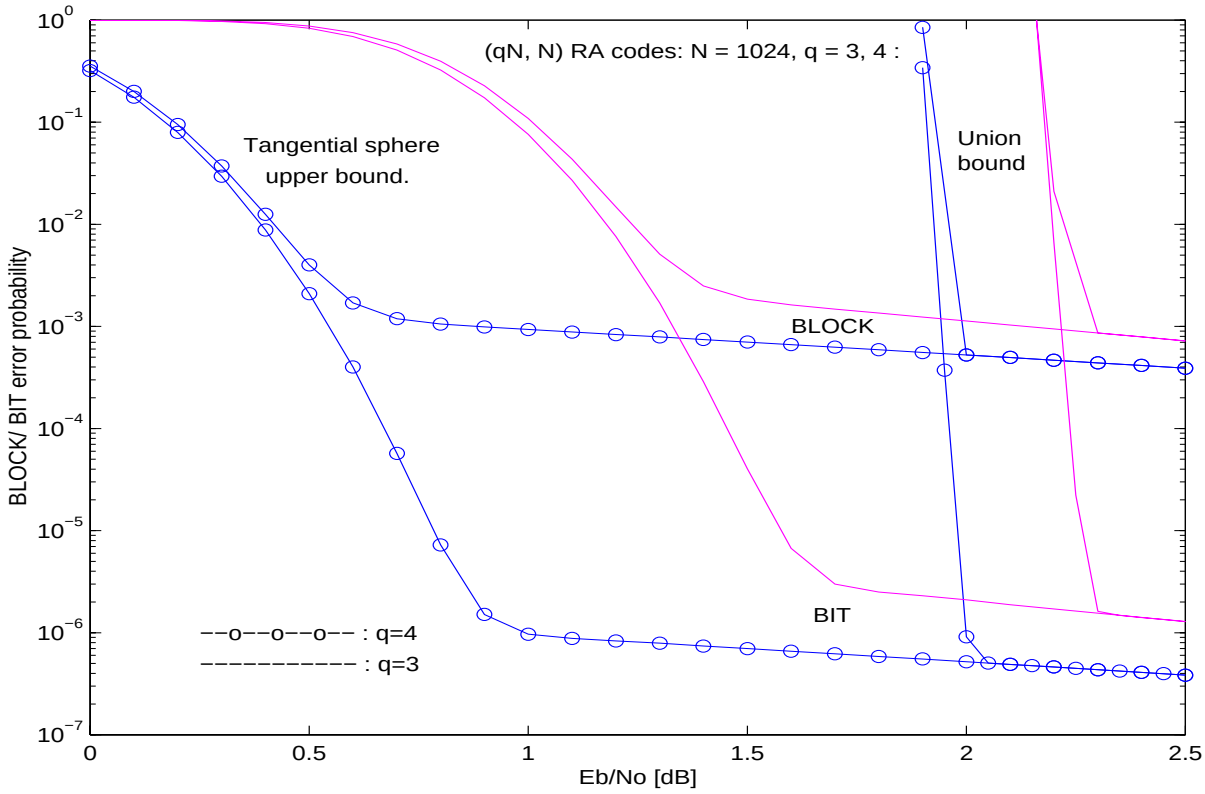

Figure 9.

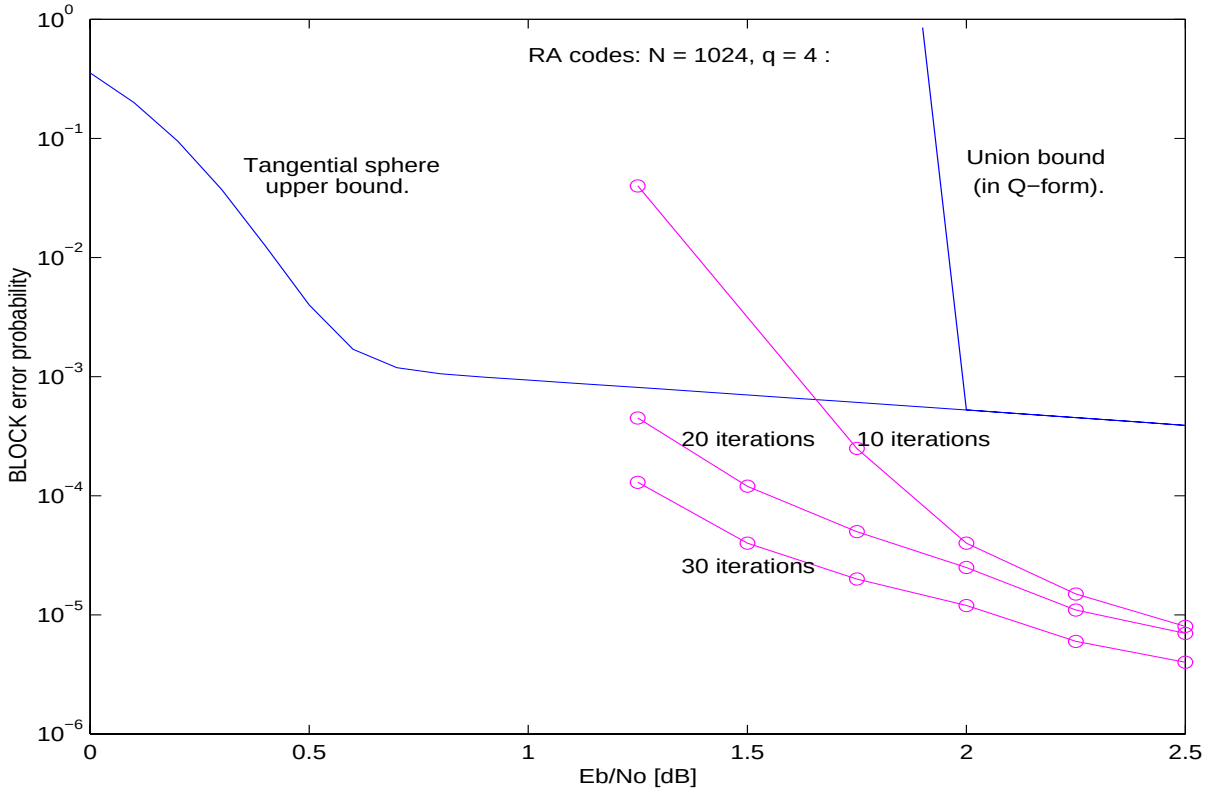

Figure 10.

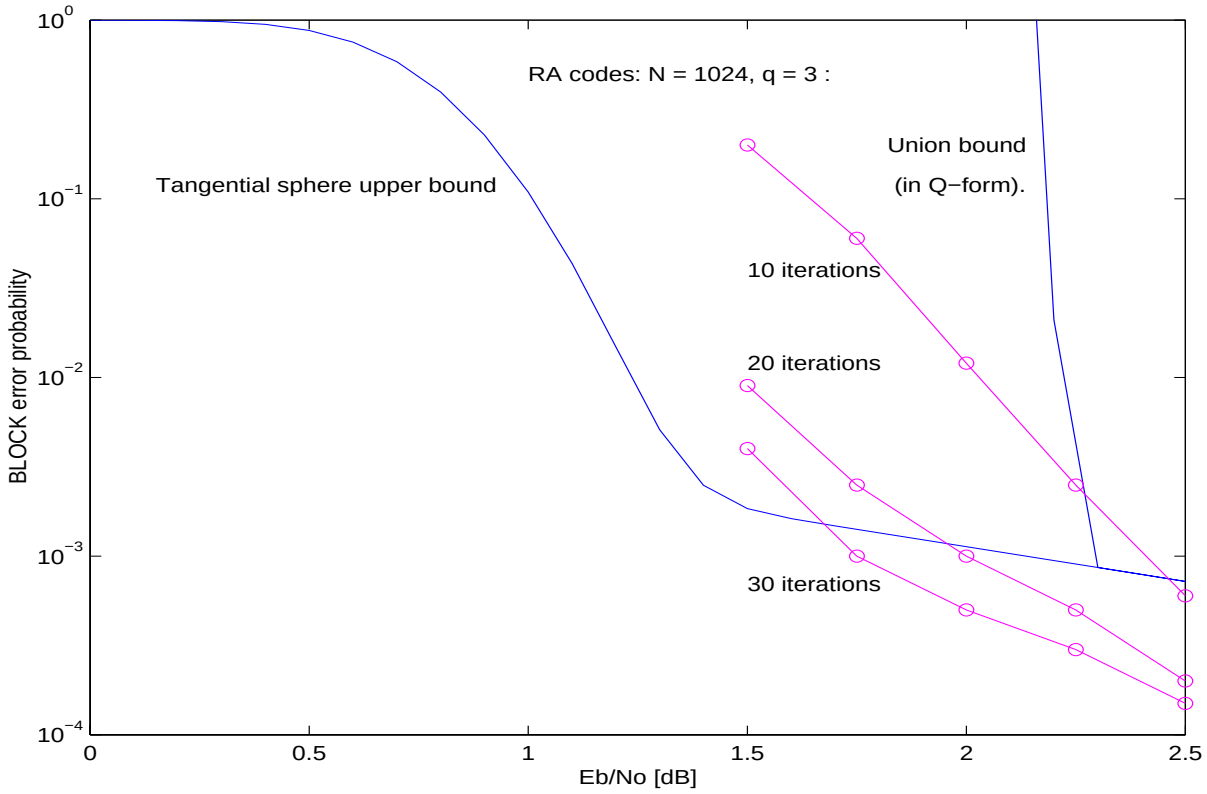

Figure 11.

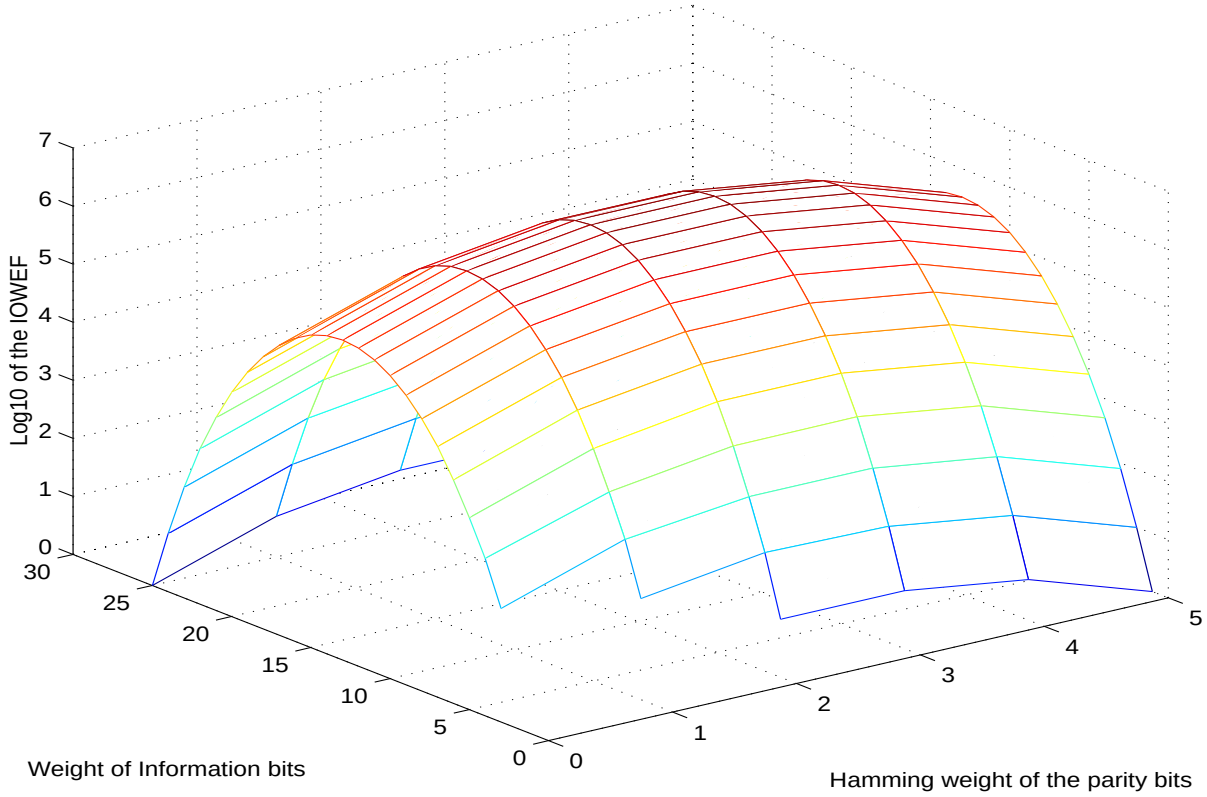

Figure 12.

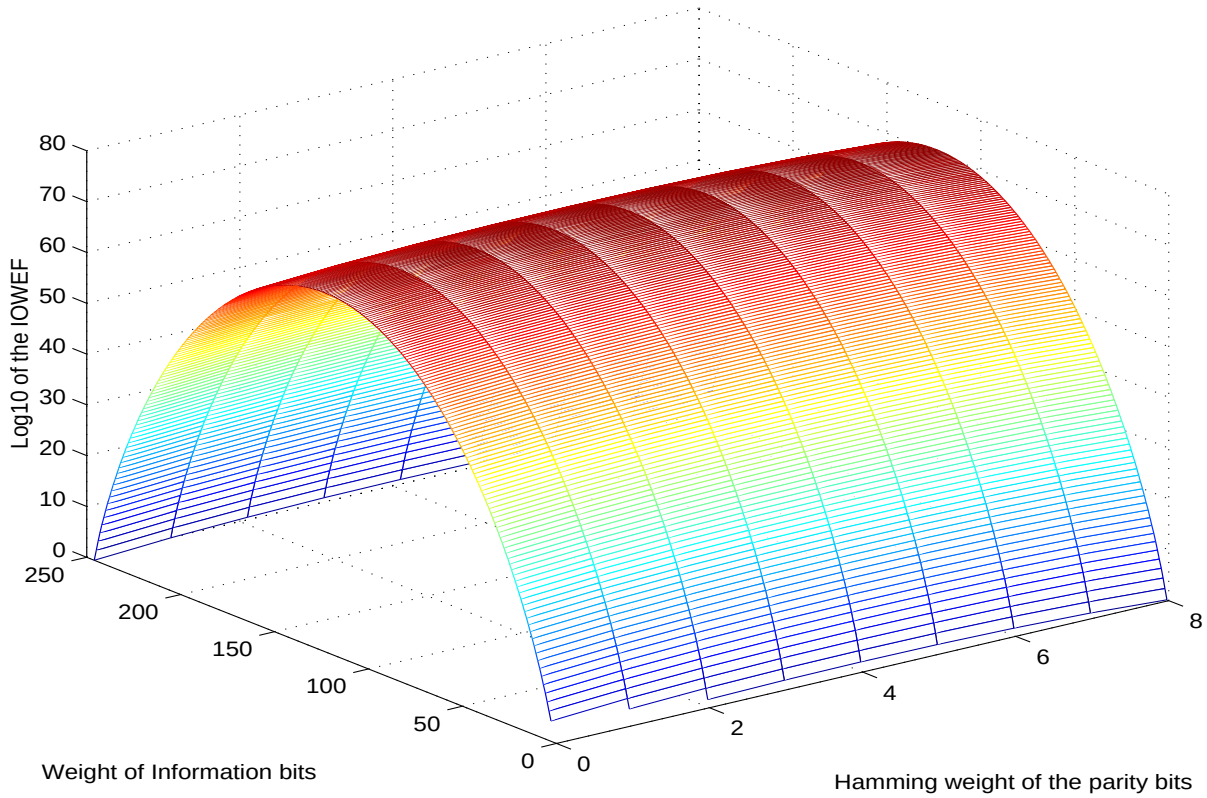

Figure 13.

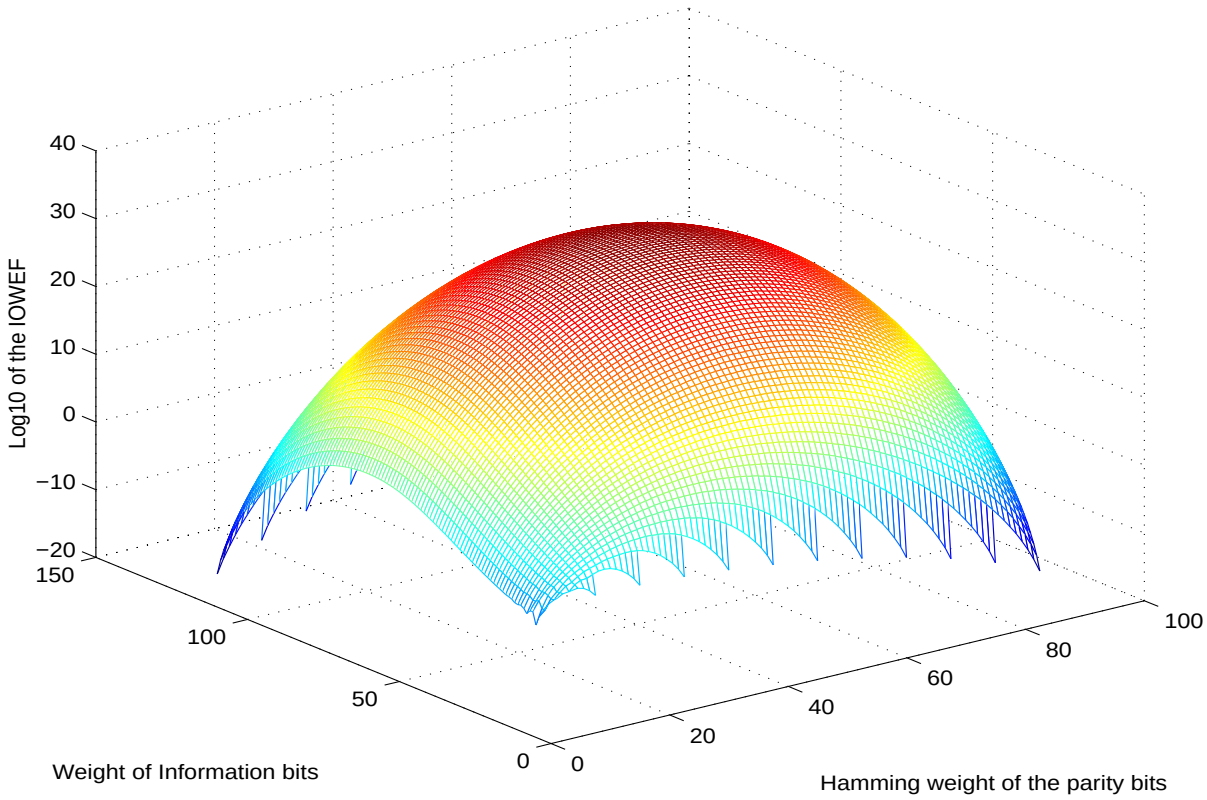

Figure 14.

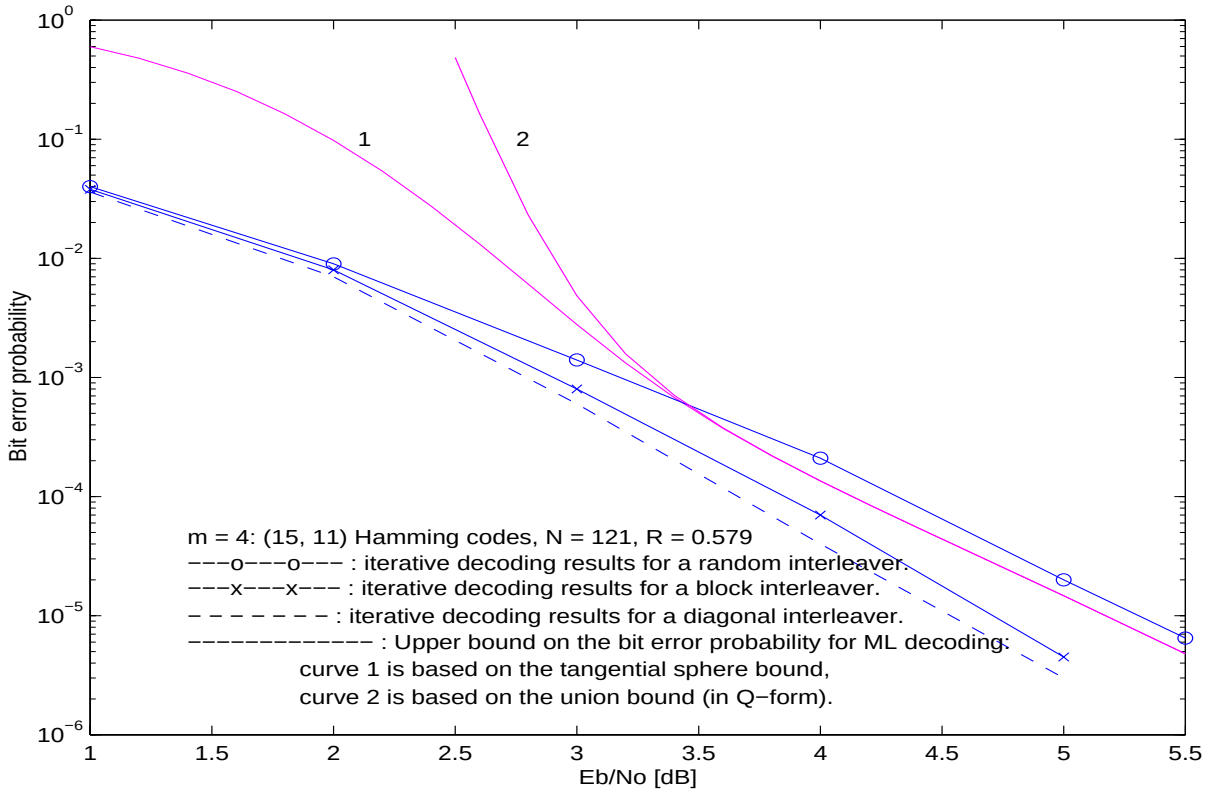

Figure 15.

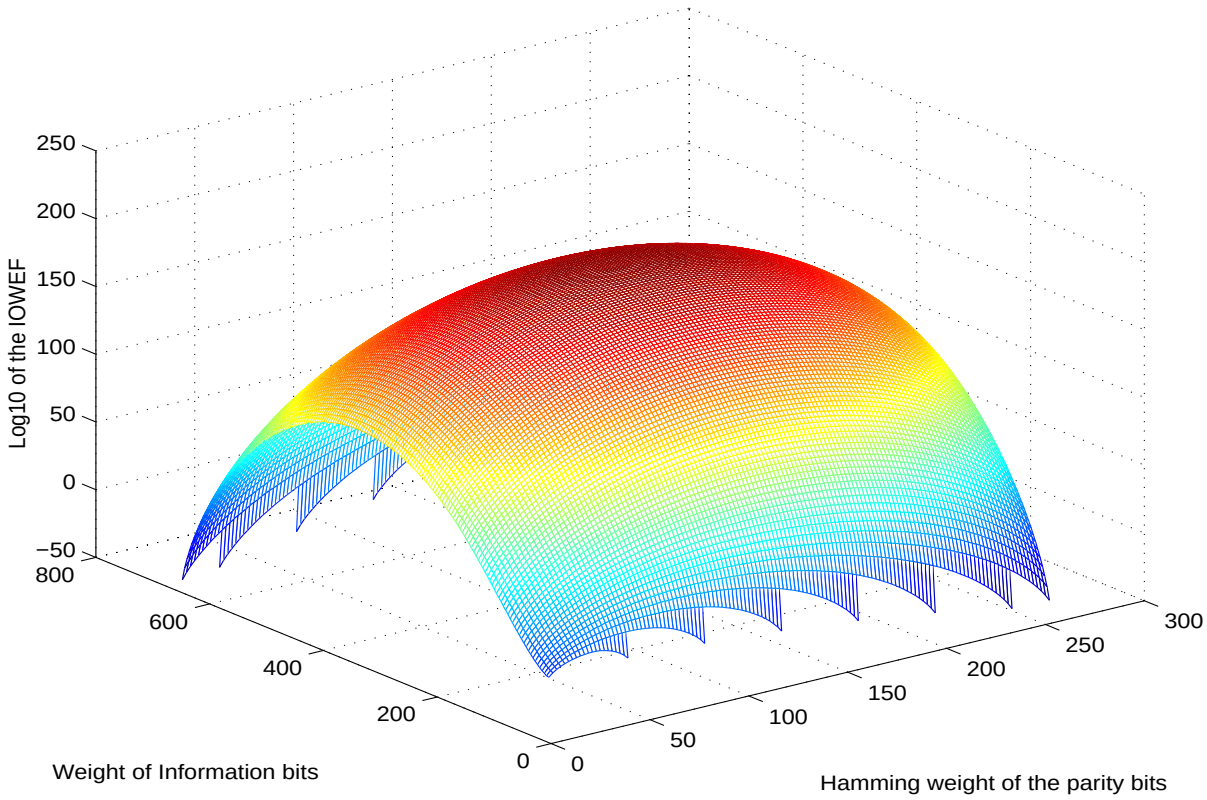

Figure 16.

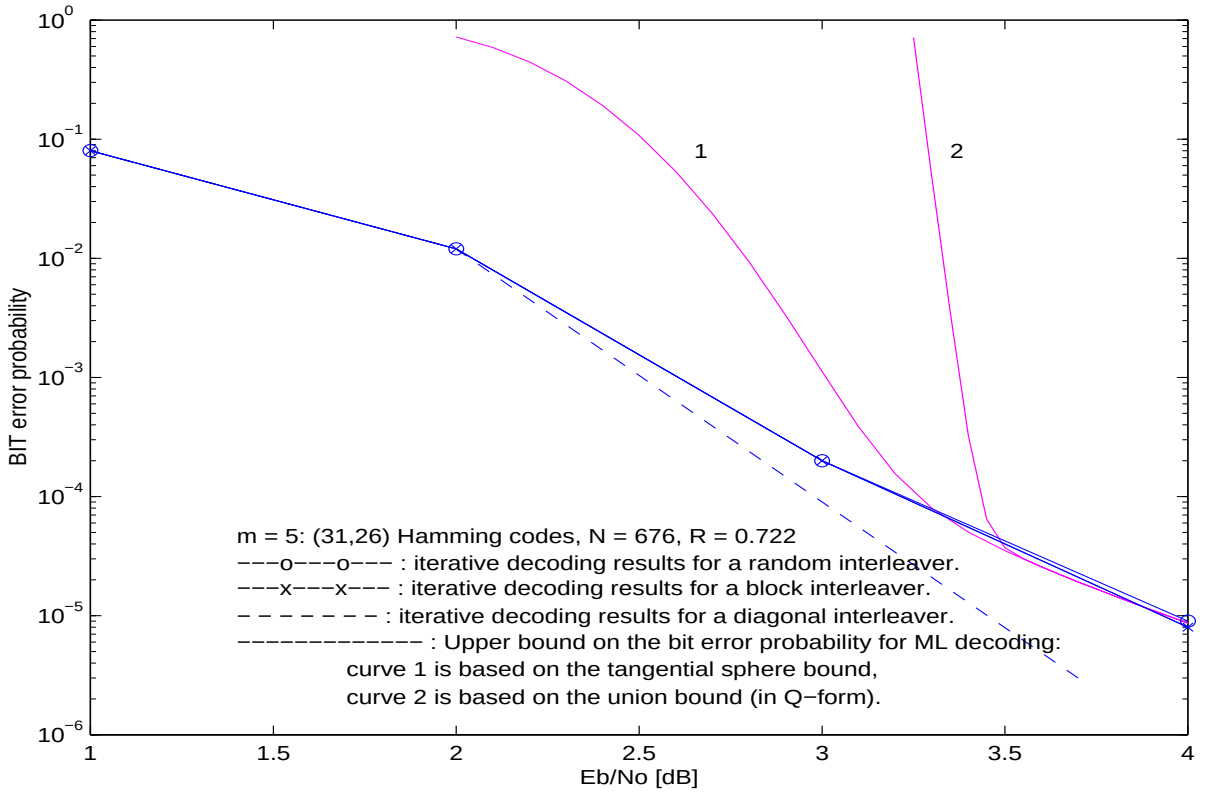

Figure 17.