Low Complexity Soft-Input Soft-Output Hamming Decoder

Benjamin Müller, Martin Holters, Udo Zölzer
Helmut Schmidt University
University of the Federal Armed Forces
Department of Signal Processing and Communications
Holstenhofweg 85, 22043 Hamburg, Germany
mimo@hsu-hh.de

***Abstract*—We investigate a low complexity *Soft-Input Soft-Output* (SISO) Hamming Decoder. The Decoding is based on error patterns which belong to the same syndrome. It is shown that it is sufficient to investigate error patterns with one and two errors to gain up to $1.35\,$dB compared to *hard decision decoding*. The proposed decoding algorithm has a linearly rising complexity, $\mathcal{O}(N_c)$, with the code word length N_c. The further consideration of error patterns with three errors which belong to the determined syndrome gain further $0.2\,$dB and improves the quality of the soft-output due to the increased number of comparisons with valid code words. However, this also increases the complexity of the decoding process to $\mathcal{O}(N_c^2)$. We present simulation results for soft decoding of Hamming codes up to a code word length of 63 bit. Furthermore, we present results for turbo decoding with the $63, 57$-Hamming code as a component code.**

***Index Terms*—Syndrome based soft decoding, Hamming Code, low complexity, soft-output, turbo decoding**

I. Introduction

The decoding algorithms of Hamming-codes were investigated in several papers. The exhaustive maximum likelihood decoding of a $(63, 57)$-Hamming code would require the comparison of 2^{57} valid code words. Chase reduced the complexity by checking a fixed number of the error patterns with a slight performance degradation [1]. A further reduction of considered error patterns was obtained in [2]. Based on this approach we show that the group of error patterns can be reduced to single and double errors to gain up to $1.35\,$dB compared to *hard decision decoding* (HDD). In contrasts to the proposed decoding technique there are Trellis-based decoding algorithms [3] [4] which have a quadratic complexity $\mathcal{O}(N_c^2)$ for Hamming and Reed-Muller codes. A further different approach was considered in [5], which is based on systematic bit-flipping. In [6] MAP decoding is performed based on Hadamard transforms, which leads to a complexity of $\mathcal{O}(N_c \mathrm{ld} N_c)$.

One of the here proposed decoding algorithms can achieve a linear complexity with a performance degradation of $0.2\,$dB compared to maximum likelihood decoding. For a $(63, 57)$-Hamming code, only 32 valid code words have to be compared in terms of their soft information which is equivalent to a linear complexity $\mathcal{O}(N_c)$, with the code word length N_c. In addition, the proposed soft-output decoding makes the algorithm suitable for further applications like turbo decoding.

II. Encoding and Transmission

The encoding of the message bits $\mathbf{a}$ can be performed by a modulo 2 vector matrix multiplication of $\mathbf{a}$ and the generator matrix $\mathbf{G}$

$$\mathbf{c} \equiv \mathbf{a} \cdot \mathbf{G} \tag{1}$$

The expression "$\equiv$" is equivalent with

$$\mathbf{c} = (\mathbf{a} \cdot \mathbf{G}) \bmod 2.$$

The generator matrix of systematic $7, 4$-Hamming code is given by

$$\mathbf{G} = \underbrace{\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right.}_{\mathbf{I}} \Bigg| \underbrace{\left.\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{array}\right]}_{\mathbf{P}}. \tag{2}$$

$\mathbf{c}$ is modulated, so that a logical zero is equivalent to a $+1$ and a logical one is equivalent to a -1, $\mathbf{x} \in \{+1, -1\}$. The modulated signal $\mathbf{x}$ is distorted by the *additive white Gaussian noise* (AWGN) $\mathbf{w}$ and results in the receive signal $\mathbf{y}$,

$$\mathbf{y} = \mathbf{x} + \mathbf{w}. \tag{3}$$

III. Hard Decision Decoding

For *hard decision decoding* (HDD) it is required to derive the bit sequence $\tilde{\mathbf{c}}$ from the distorted signal $\mathbf{y}$. The syndrome $\mathbf{z}$ can be calculated as follows

$$\mathbf{z} \equiv \tilde{\mathbf{c}} \cdot \mathbf{H}^T \equiv (\mathbf{c} + \mathbf{e}) \cdot \mathbf{H}^T, \tag{4}$$

where $\mathbf{H}$ is the parity check matrix and $\mathbf{e}$ is the error pattern belonging to the syndrome. In this manner, every syndrome leads to exactly one single error pattern and the decoding can be performed based on a syndrome table. If the error pattern is $\vec{0}$, the syndrome is also $\vec{0}$ which means that the received code word is a valid code word and no decoding is required. Error patterns with 2 (duets) or 3 errors (triplets) which belong to the same syndrome are not taken into account for the decoding and the distorted code word $\tilde{\mathbf{c}}$ is corrected to

$$\hat{\mathbf{c}} \equiv \tilde{\mathbf{c}} + \mathbf{e}. \tag{5}$$

In fact, every double error is decoded to a valid but wrong code word. This explains the poor performance of HDD for Hamming codes, which are illustrated in Fig. 2, 3, 4 and 5 for the different code word lengths.

IV. Syndrome based soft decision decoding

For the syndrome based soft decision decoding it is required to calculate the *log-likelihood ratios* (LLR or L-values) from the received signal $\mathbf{y}$,

$$L\left(x|y\right) = \ln \frac{P\left(x=+1|y\right)}{P\left(x=-1|y\right)}, \tag{6}$$

which finally leads to

$$L\left(x|y\right) = \ln \frac{\exp\left(-\frac{E_b}{N_0}\left(y-1\right)^2\right)}{\exp\left(-\frac{E_b}{N_0}\left(y+1\right)^2\right)} = \frac{4E_b}{N_0}y, \tag{7}$$

assuming that a logical zero and one have the same probability [7].

Let us assume that the syndrome of a distorted bit sequence of a $7,4$-Hamming code is $\mathbf{z} = (0\ 0\ 1)$. The possible error patterns are collected in matrix $\mathbf{E}$ with its elements $e_{j,i}$

$$\mathbf{E} = \left(\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right), \tag{8}$$

where the second to fourth row bears the duets and the fifth to eighth row bears the triplets. The error patterns for all syndromes are determined in advance and stored in a list. The size of the list rises quadratically for double errors and cubically for triple errors (see Tab. I). Every row of $\mathbf{E}$ is multiplied by the absolute value of log-likelihood ratios of the received signal $L\left(x|y\right)$. Afterwards, the resulting row vector is added up. The vector with the lowest sum of L-values suggests the error pattern with the highest probability of a correct decoding. For the $7,4$-Hamming code $N_{e1} + N_{e2} = 4$ error patterns have to be multiplied by $|L\left(x|y\right)|$ to cover single and double errors. If it is required to take triplets into account, $N_{e3} = 4$ more error patterns have to be multiplied by $|L\left(x|y\right)|$.

In order to estimate the complexity, the number of duets belonging to one syndrome is given by

$$N_{e2} = \frac{1}{N_c}\frac{N_c!}{(N_c-2)!\cdot 2!} = \frac{N_c-1}{2}, \tag{9}$$

with N_c being the length of the code word. The number of triplets can be calculated similarly by

$$N_{e3} = \frac{1}{N_c}\left(\frac{N_c!}{(N_c-3)!\cdot 3!} - \frac{N_{e2}}{3}\right) = \frac{N_c-1}{2}\cdot\frac{N_c-3}{3}. \tag{10}$$

Eq. 9 and 10 show that the complexity rises linearly for the duets and quadratically for the triplets. Table I shows the number of duets N_{e2} and triplets N_{e3} belonging to one syndrome.

TABLE I
Number of duets N_{e2} and triplets N_{e3} belonging to one syndrome, size of error pattern lists for all syndromes

N_c	N_{e2}	List size	N_{e3}	List size
7	3	28×7	4	56×7
15	7	120×15	28	540×15
31	15	496×31	140	4836×31
63	31	2016×63	620	41076×63

V. soft-output Decoding

In general, soft-output decoding provides output values for iterative or turbo decoding. In order to generate soft-outputs, the following algorithm is proposed. The probability values of a code word are given by

$$P\left(\tilde{c}_j = c_j|y_j\right) = \frac{\exp\left(|L\left(x_j|y_j\right)|\right)}{1+\exp\left(|L\left(x_j|y_j\right)|\right)}. \tag{11}$$

In the next step, the probability values are multiplied column-wise for the given error pattern of every row i.

$$\dot{P}_i = \prod_j \begin{cases} P\left(\tilde{c}_j = c_j|y_j\right) & \text{if } e_{i,j}=0 \\ 1-P\left(\tilde{c}_j = c_j|y_j\right) & \text{if } e_{i,j}=1 \end{cases} \tag{12}$$

Now $\dot{P}_i$ is normalized, so that the sum of the normalized probabilities P_i over all rows i is equal to 1, $\sum\limits_i P_i = 1$. The normalized probabilities P_i are given by

$$P_i = \frac{\dot{P}_i}{\sum\limits_{i'}\dot{P}_{i'}}. \tag{13}$$

P_i can be interpreted as the probability of correct decoding for the given error pattern of row i. In a last step, the probability that $x_j = +1$, for a given received code word y, is calculated by the sum of P_i over all rows i, if $e_{i,j} = \tilde{c}_j$, where $\tilde{c}_j$ is defined as the logical received bit sequence. $\hat{}$ indicates the estimation of the new probabilities after the soft decoding.

$$\hat{P}\left(x_j = +1|\mathbf{y}\right) = \sum_{\substack{i \\ e_{i,j}=\tilde{c}_j}} P_i \tag{14}$$

Due to the normalization, so that $\sum\limits_i P_i = 1$, the probability of $\hat{P}\left(x_j = -1|\mathbf{y}\right)$ can be calculated by

$$\hat{P}\left(x_j = -1|\mathbf{y}\right) = 1 - \hat{P}\left(x_j = +1|\mathbf{y}\right). \tag{15}$$

In order to exchange the information for turbo decoding it is required to calculate L-values from the derived probabilities.

VI. Turbo Decoding

With the ability of soft-output decoding, we can utilize the soft-outputs for turbo decoding. In order to do so, the systematic data bits have to be encoded twice. The first encoding can be performed as shown in Eq. 1. The second encoding requires an additional interleaver prior to the encoding. We only investigate an interleaver of the length of the systematic bits of one code word. The interleaved data bits are bit reverse to the uninterleaved data bits. This short interleaver enables similar delays as for the original code length. Finally the uninterleaved and the parity bits of the first encoder and the second encoder are multiplexed to the code word which is transmitted.

Fig. 1 shows the schematic structure of a turbo decoder. The received code word $\mathbf{y}$ is separated into systematic bits and the parity bits of the first encoder and the parity bits of the second encoder. Based on the soft-input the encoders calculate soft-outputs as described in section V. The encoder output, subtracted by their soft-input, result in the extrinsic information of the decoding process. This extrinsic information is directed to the other encoder and is added to the soft information of the received systematic bits.

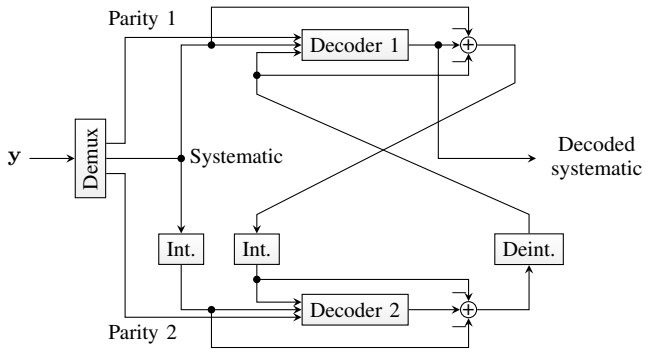

Fig. 1. Schematics of turbo decoding

VII. Simulation Results

For the simulation results Hamming codes of a code word length for 7 till 63 bit were investigated. Fig. 2, 3, 4 and 5 illustrate the performance of the different decoding strategies for a certain code word length. Tab. II summarizes the results for all non-iterative codes. Fig. 2 shows the bit error rate of the $7, 4$-Hamming code for different types of decoding. It is shown that the decoding performance of the duet and triplet decoding is quite similar and very close to the union bound which is an upper bound for the bit error probability after maximum likelihood decoding. For the evaluation we focus on a BER $= 10^{-4}$. The coding gain amounts to $0.31\,\mathrm{dB}$ for the HDD and $1.66\,\mathrm{dB}$ for the duet decoding.

TABLE II
Simulation results for required E_b/N_0 in dB for a bit error rate of 10^{-4} and the resulting coding gain (uncoded $8.37\,\mathrm{dB}$ for BER $= 10^{-4}$)

N_c	K_c	HDD	Gain	Duets	Gain	Triplets	Gain
7	4	8.06	0.31	6.71	1.66	6.67	1.7
15	11	7.42	0.95	6.14	2.23	6.04	2.33
31	26	7.17	1.20	6.02	2.35	5.88	2.49
63	57	7.16	1.21	6.11	2.26	5.92	2.45

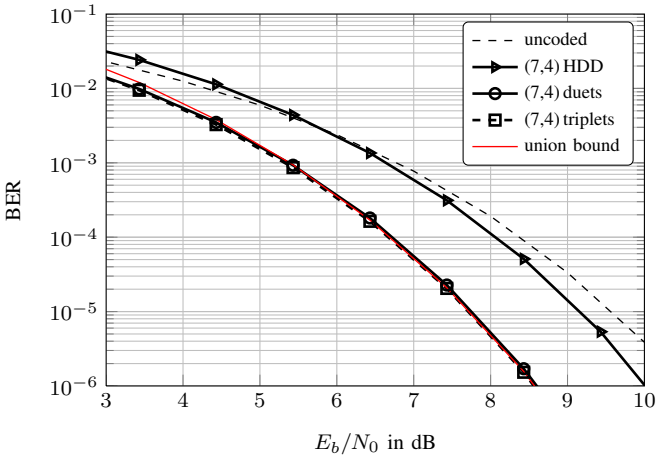

Fig. 2. Bit error rate for different types of decoding for a $7, 4$-Hamming code

The extension of the code word length, up to 15 bit, results in a further performance gain. It is also apparent that the difference between duet decoding and triplet decoding rises. The coding gain amounts to $0.95\,\mathrm{dB}$ for the HDD and $2.23\,\mathrm{dB}$ for the duet decoding. Further $0.1\,\mathrm{dB}$ can be gained by triplet decoding.

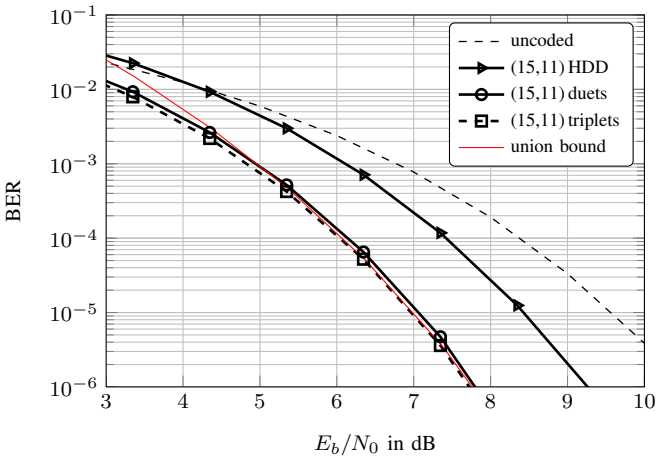

Fig. 3. Bit error rate for different types of decoding for a $15, 11$-Hamming code

The $32, 26$-Hamming code obtained the best results for the non-iterative codes, for duets as well as for triplets. Fig. 4 shows that the coding gain amounts to $2.35\,\mathrm{dB}$ for the duet decoding and $2.49\,\mathrm{dB}$ for the triplet decoding.

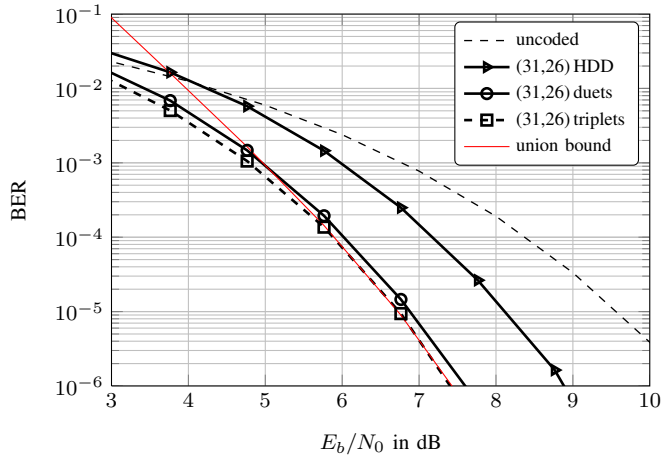

Fig. 4. Bit error rate for different types of decoding for a $31, 26$-Hamming code

Quite a similar picture can be drawn for the $63, 57$-Hamming code which has the highest code rate ($R_c = 0.905$) of the considered Hamming codes (see Fig. 5). The coding gain is lower than for the $32, 26$-Hamming code ($2.26\,\text{dB}$ gain for the duet and $2.45\,\text{dB}$ gain for the triplets), but the bit error curve falls more sharply. It is also shown that the difference between duet and triplet decoding is the highest with $0.19\,\text{dB}$.

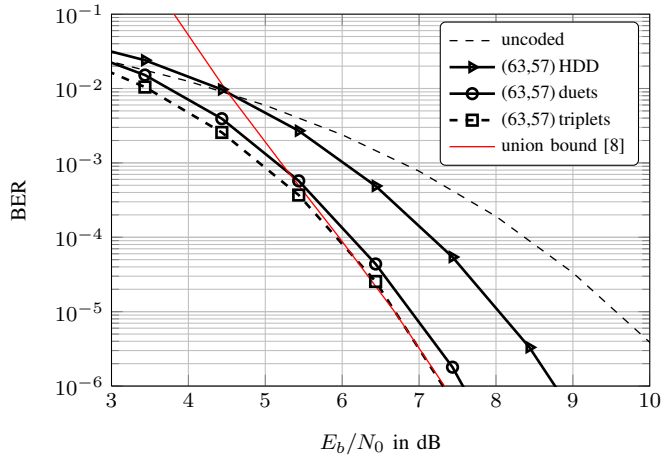

Fig. 5. Bit error rate for different types of decoding for a $63, 57$-Hamming code

Fig. 6 shows the simulation results of the bit error rate of turbo decoding with the $63, 57$-Hamming code as a component code. The soft-outputs for the turbo decoding were calculated as shown in section V for double and triple errors. The turbo decoder considering single error, duets and triplets performs $0.36\,\text{dB}$ better than the non-iterative triplet decoder. Turbo decoding only considering single and double errors leads to no further gain compared to non-iterative duet or triplet decoding. In fact, the coding gain decreases by $0.5\,\text{dB}$ compared to non-iterative duet decoding. This can be explained with the small numbers of comparison with other valid code words which lead to an inaccurate soft-output after the decoding process. In addition, the assumption of a normalization for $\sum_i P_i = 1$ can lead to inaccurate soft-outputs.

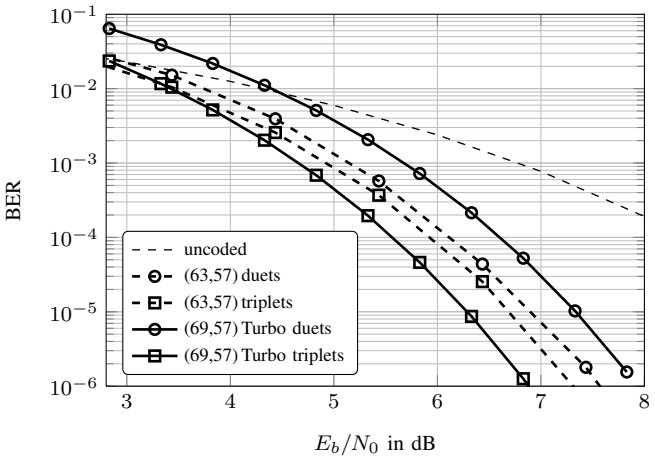

Fig. 6. Comparison of non-iterative decoding and turbo decoding for duet and triplet decoding

VIII. Conclusion

We have proposed a soft-input Hamming decoder which either considers error patterns with up to 2 or up to 3 errors belonging to the determined syndrome. The complexity of duet decoding rises linearly with the code word length and quadratically for triplet decoding. The duet decoding can gain up to $1.35\,\text{dB}$ compared to hard decision decoding (BER$= 10^{-4}$). Considering error patterns up to 3 errors gains further $0.2\,\text{dB}$, where the gain for triplet decoding increases with the code word length. Furthermore, we proposed a soft-output decoder based on the soft-input Hamming decoder. The soft-outputs where utilized for turbo decoding. It was shown that duet decoding is unsuitable for turbo decoding, due to the poor quality of the soft-outputs. The turbo decoding based on triplet decoding $(69, 57$-Hamming code) showed a performance gain of $0.36\,\text{dB}$ compared to the triplet decoding of the $63, 57$-Hamming code. These results were obtained with the smallest possible interleaver of one data word length.

References

[1] D. Chase, "Class of algorithms for decoding block codes with channel measurement information," *Information Theory, IEEE Transactions on*, vol. 18, no. 1, pp. 170 – 182, Jan. 1972.

[2] J. Snyders, "Reduced lists of error patterns for maximum likelihood soft decoding," *Information Theory, IEEE Transactions on*, vol. 37, no. 4, pp. 1194 –1200, July 1991.

[3] J. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *Information Theory, IEEE Transactions on*, vol. 24, no. 1, pp. 76 – 80, Jan. 1978.

[4] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes," *Information Theory, IEEE Transactions on*, vol. 39, no. 1, pp. 242 –245, Jan. 1993.

[5] Simon Hirst and Bahram Honary, "A simple soft-input/soft-output decoder for hamming codes," in *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, London, UK, 2001, pp. 38–43, Springer-Verlag.

[6] A. Ashikhmin and S. Litsyn, "Simple MAP decoding of first-order Reed-Muller and Hamming codes," *Information Theory, IEEE Transactions on*, vol. 50, no. 8, pp. 1812 – 1818, 2004.
[7] L. Hanzo, T. Liew, and B. Yeap, *Turbo coding, turbo equalisation and space-time coding*, Wiley, 2002.
[8] Marco Baldi, Giovanni Cancellieri, and Franco Chiaraluce, "Low complexity soft-decision decoding of BCH and RS codes based on belief propagation," in *Riunione Annuale GTTI 2008 Sessione su Trasmissione Numerica*, 2008.