www.ietdl.org

Published in IET Communications
Received on 18th April 2011
Revised on 19th July 2011
doi: 10.1049/iet-com.2011.0318

ISSN 1751-8628

Soft decoding of the (23, 12, 7) Golay-code up to five errors

Y. Li[1] *L. Wang*[1] *T.-K. Truong*[2,3]

[1]*Department of Communication Engineering, Xiamen University, Fujian 361005, China*
[2]*Department of Information Engineering, I-Shou University, Kaohsiung County 840, Taiwan*
[3]*Department of Computer Science and Engineering, National Sun Yat-sen University, Taiwan*
E-mail: wanglin@xmu.edu.cn

Abstract: A new decoder is proposed to decode the (23, 12, 7) binary Golay-code up to five errors. It is based on the algorithm that can correct up to four errors for the (24, 12, 8) extended Golay-code proposed by Lin *et al.*, thereby achieving the soft decoding in the real sense for the Golay-code. For a weight-2 or weight-3 error pattern decoded by the hard decoder for correcting up to three errors, one can find the corresponding 21 weight-4 or weight-5 error patterns and choose the one with the maximum emblematic probability value, which is defined as the product of individual bit-error probabilities corresponding to the non-zero locations of the error pattern as the ultimate choice. Finally, simulation results of this decoder over additive white Gaussian noise (AWGN) channels show that the proposed method provides 0.9 dB coding gain than that of Lin *et al.*'s algorithm at bit-error rate of 10^{-5}.

1 Introduction

The (23, 12, 7) Golay-code was first discovered by Golay [1] in 1949. It is a very useful perfect linear error-correcting code. Several efficient decoding algorithms of the Golay-code are as follows. The standard array decoding [2], the algebraic decoding algorithm developed by Elia [3], the shift-search algorithm proposed by Reed *et al.* [4] and the error trapping method developed by Kasami [5]. Particularly, for other applications of the Golay-code, a parity bit is added to each word to yield the (24, 12, 8) extended Golay-code. This code is also attractive for use on a deep space network uplink, where the spacecraft uses software decoding with an onboard computer. It has been used on a number of communication links in the past decades, including the Voyager imaging system link of NASA [4, 6].

In 1995, Lu *et al.* [7] developed two fast-decoding algorithms of the (23, 12, 7) Golay-code for correcting up to four errors. The advantages of these algorithms are that one method requires a small amount of computation for correcting errors of the received word and the other method is suitable for hardware implementation. Recently, the reliability-search algorithm [8] was developed to facilitate further decoding of the (23, 12, 7) Golay-code. In that algorithm, using real channel data, the method developed by Reed [9] can be used to estimate the individual bit-error probabilities in a received word. More recently, Lin *et al.* [10] proposed a new soft-decoding (SD) algorithm, which achieves a better percentage of successful decoding for four errors over AWGN channels than Lu *et al.*'s algorithm. In this paper, the algorithm in [10] is extended and modified to correct up to five errors for the (23, 12, 7) Golay-code. First, a 23-bit error pattern is always obtained by decoding the 23-bit received word via a conventional hard-decoding (HD) algorithm of the perfect (23, 12, 7) Golay-code up to three errors. All the candidate error patterns corresponding to the decoded error pattern are then found. Based on the idea given in [9], one can estimate the 23 individual bit-error probabilities in the received code-word. For each possible error pattern, the emblematic probability value is defined as the product of the individual bit-error probabilities corresponding to the locations of error bits. Finally, according to the greatest emblematic probability value, the most likely error pattern is chosen. As shown in this paper, the modified algorithm improves the performance further compared with the algorithm in [10].

The remaining sections of this paper are organised as follows: The background of the algebraic decoding of the binary (23, 12, 7) Golay-code is given in Section 2. Section 3 develops a soft-decision decoding algorithm for decoding the (23, 12, 7) Golay-code up to five errors. Section 4 gives the simulation results. Finally, Section 5 concludes this paper.

2 Preliminaries

For the binary (23, 12, 7) Golay-code of length 23 over $GF(2^{11})$, its quadratic residue (QR) set is the collection of all non-zero quadratic residues modulo n given by

$$\begin{aligned} Q_{23} &= \{i | i \equiv j^2 \bmod 23 \text{ for } 1 \le j \le 22\} \\ &= \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \end{aligned} \quad (1)$$

Let β be a primitive element in $GF(2^{11})$ such that β is a generator of the multiplicative group of 2^{11}-1 non-zero elements in $GF(2^{11})$. A binary (23, 12, 7) QR code is a

cyclic code with the generator polynomial $g(x)$ of the form

$$g(x) = \prod_{i \in Q_{23}} (x - \alpha^i) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \tag{2}$$

where $\alpha = \beta^{89}$ is a primitive 23rd root unity in the finite field $GF(2^m)$, with $m = 11$, the smallest positive integer such that $23|2^{11} - 1$.

The (23, 12, 7) Golay-code C is a perfect or close-packed code, in the sense that the code-words and their three-error correction spheres exhaust the vector space of 23-bit binary vectors. It is shown in [11] that the (23, 12, 7) Golay-code is, besides being a cyclic Bose–Chaudhuri–Hocquenghem (BCH) code, a QR code [12]. Since the minimum distance of the code is $d = 7$, the error-correcting capacity of this code is $t = 3$. In other words, the (23, 12, 7) Golay-code allows for the correction of up to three errors.

The code-word of the code C over $GF(2)$ are expressed as the coefficients of a polynomial. In such a representation, a code-word is represented by

$$c(x) = \sum_{i=0}^{22} c_i x^i \tag{3}$$

where $c_i \in \mathrm{GF}(2)$. The code-word of the code C, $c(x)$, must also be a multiple of the generator polynomial $g(x)$. Written as a vector, the code-word is $c = (c_0, c_1, \ldots, c_{22})$.

To illustrate the algebraic decoding algorithm, define

$$e(x) = e_{22}x^{22} + e_{21}x^{21} + \cdots + e_1 x + e_0 \tag{4}$$

to be the error polynomial. The received word has the form

$$r(x) = c(x) + e(x) \tag{5}$$

Written as a vector, the received word and the error pattern are $r = (r_0, r_1, \ldots, r_{22})$ and $e = (e_0, e_1, \ldots, e_{22})$, respectively. Suppose that v errors occur in the received word $r(x)$ and assume that $v \leq t = 3$.

The set of known syndromes obtained by evaluating $r(x)$ at the roots of $g(x)$ is given by

$$S_i = r(a^i) = c(a^i) + e(a^i) = e(a^i), \quad i \in Q_{23} \tag{6}$$

Assume that v errors occur in the received word. The plain error-locator polynomial is defined to be a polynomial of degree v; that is

$$L(z) = \prod_{i=1}^{v} (z - Z_i) = z^v + \sum_{j=1}^{v} \sigma_j z^{v-j} \tag{7}$$

where $v \leq 3$, Z_j for $1 \leq j \leq v$ are the locations of the v errors, that is, $Z_j = \alpha^{r_j}$ and r_j locates the position of the error to be corrected.

Given the known syndromes S_1, S_3 and S_9, Elia's algorithm for decoding the (23, 12, 7) Golay-code [3] is summarised as follows

$$L(z) = \begin{cases} 0, & \text{no error if } S_1 = 0 \\ z + S_1, & \text{one error if } S_1^3 = S_3 \text{ and } S_1^9 = S_9 \\ z^2 + S_1 z + \left(S_1^2 + \dfrac{S_3}{S_1}\right), & \text{two errors if } S_1 D^{1/3} = S_3 \\ z^3 + S_1 z^2 + (S_1^2 + D^{1/3})z + (S_3 + S_1 D^{1/3}); & \\ \text{otherwise, three errors} & \end{cases} \tag{8}$$

Here, $D = S_1^6 + S_3^2 + (S_1^9 + S_9)/(S_1^3 + S_3) \in GF(2^{11})$ and the cube root $D^{1/3}$ in $GF(2^{11})$ is equal to D^{1365} which may be implemented directly. However, the exponent of D, namely 1365, is so large that the multiplicative complexity of the direct method is very high. Towards this end, Fermat's theorem given in [13] can be used to compute the cube root $D^{1/3}$ needed in Elia's decoding algorithm.

The binary (24, 12, 8) extended Golay-code C' can be formed by adding a parity-check bit to the binary (23, 12, 7) Golay-code. It is easy to prove that the following extension of the decoding algorithm [4] for the binary Golay-code can be used to correct up to three errors and detect four errors. It is convenient also to let the symbol $\boldsymbol{P}$ denote the conventional HD algorithm, such as the algebraic decoding algorithm for the (23, 12, 7) Golay-code C. Recall that $\boldsymbol{r}$ is the received word without its overall parity bit p. In the $\boldsymbol{P}$ algorithm, the syndromes of $\boldsymbol{r}$ are first calculated and the number of errors is determined by the error conditions. The roots of $L(z)$ are the error locations found by the Chien search algorithm and the error pattern is thus obtained. Thus, $\boldsymbol{P}$ can be used to compute the error pattern $\boldsymbol{E_P}$ from the known $\boldsymbol{r}$. Hence, the decoding scheme of the code augmented by a parity bit, called extended $\boldsymbol{P}$, is given as follows:

1. If the weight of $\boldsymbol{E_P}$ is less than 3, then $\boldsymbol{r}$ can be decoded as $\boldsymbol{r} + \boldsymbol{E_P}$ and the parity p' of $\boldsymbol{r} + \boldsymbol{E_P}$ is computed.
2. If the weight of $\boldsymbol{E_P}$ is equal to 3, then the parity p' of $\boldsymbol{r} + \boldsymbol{E_P}$ is computed and compared with the received parity p. If $p' \neq p$, then the decoder detects four errors.

Consider a received word $\boldsymbol{r}$ of code C that is corrupted by a weight-4 error pattern $\boldsymbol{e}$. Since the (23, 12, 7) Golay-code is a well-known triple error-correcting perfect code, the received word $\boldsymbol{r}$ is decoded as a code-word $\hat{\boldsymbol{c}}$ by the HD algorithm and its corresponding error pattern $\hat{\boldsymbol{e}}$ is thus obtained; that is, $\boldsymbol{c} + \boldsymbol{e} = \boldsymbol{r} = \hat{\boldsymbol{c}} + \hat{\boldsymbol{e}}$, where the weight of $\hat{\boldsymbol{e}}$ is less than or equal to 3, that is, $w(\hat{\boldsymbol{e}}) \leq 3$. Owing to the linear property of the code, $w(\boldsymbol{e}) = 4$ and $d = 7$, one yields the results given by

$$(\boldsymbol{e} + \hat{\boldsymbol{e}}) \in C, \quad w(\hat{\boldsymbol{e}}) = 3 \quad \text{and} \quad w(\boldsymbol{e} + \hat{\boldsymbol{e}}) = 7 \tag{9}$$

For four errors detected in the (24, 12, 8) extended Golay-code C', either three error bits and one error bit occur in code C and the overall parity bit, respectively, or all four-error bits occur in code C. In these two cases, the weight-3 error pattern $\boldsymbol{E_P}$ from $\boldsymbol{P}$ is thus obtained.

3 SD of the (23, 12, 7) Golay-code up to five errors

In the section, three useful theorems that are needed to decode the Golay-code for correcting up to five errors are introduced.

First, a brief review about t-design is described as follows. Let X be a set of v elements called points. For $k < v$, let $\boldsymbol{B}$ be a collection of distinct k-subsets of X called blocks. A pair $(X, \boldsymbol{B})$ is called an s-$(v, k, \boldsymbol{\lambda})$ design if every s-subset of X is contained in exactly $\boldsymbol{\lambda}$ blocks, which belong to $\boldsymbol{B}$.

Theorem 1 [14]: A linear $(n, k, d = 2t + 1)$ code over $GF(q)$ is perfect if and only if the support design of the minimum weight code-words is a $(t + 1) - (n, 2t + 1, (q - 1)^t)$ design.

Theorem 2 [15, Theorem 88, p. 144]: An s-$(v, k, \boldsymbol{\lambda})$ design $(X, \boldsymbol{B})$ is also an i-(v, k, λ_i) design for $1 \leq i \leq s$. Furthermore

$$\lambda_i = \lambda \frac{\binom{v-i}{s-i}}{\binom{k-i}{s-i}} = \lambda \frac{(v-i)\cdots(v-s+1)}{(k-i)\cdots(k-s+1)} \tag{10}$$

Theorem 3: The weight numerator of (23, 12, 7) Golay-code $A(z)$ can be written as

$$A(z) = 1 + 253z^7 + 506z^8 + 1288z^{11} + 1288z^{12} + 506z^{15} + 253z^{16} + z^{23}$$

Given indexes $j_1, j_2, \ldots, j_k$, where $k \leq 3$, the number λ of weight-7 code-words or weight-8 code-words which have the same k locations of non-zero components can be computed by

$$\lambda = 253 \cdot \binom{7}{k} \Big/ \binom{23}{k} \quad \text{or} \quad \lambda = 506 \cdot \binom{8}{k} \Big/ \binom{23}{k} \tag{11}$$

Proof: Without loss of generality, only weight-7 code-words are considered. For any combination of k indexes $j_1, j_2, \ldots, j_k$, where $k \leq 3$, the corresponding number λ of weight-7 code-words which have the same k locations of non-zero components is constant. There are $\binom{23}{k}$ combinations, which corresponds to $\lambda\binom{23}{k}$ weight-7 code-words. Obviously, every code-word repeats $\binom{7}{k}$ times, and so we have

$$\lambda\binom{23}{k} = 253 \cdot \binom{7}{k} \quad \text{or} \quad \lambda = 253 \cdot \binom{7}{k} \Big/ \binom{23}{k}$$

Similarly

$$\lambda = 506 \cdot \binom{8}{k} \Big/ \binom{23}{k}$$

for the case of weight-8 code-words.

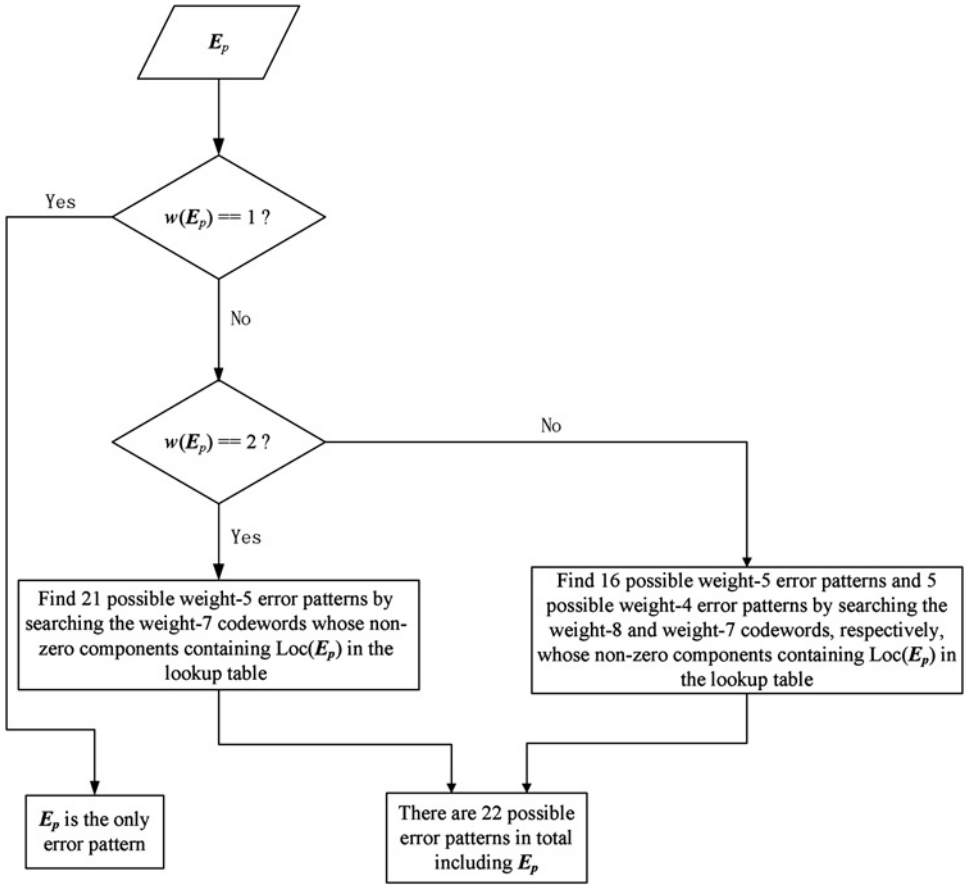

Fig. 1 *Flow-chart for determining the possible error patterns by the case-by-case method*

doi: 10.1049/iet-com.2011.0318

In this paper, a new SD algorithm of the (23, 12, 7) Golay-code for correcting up to five errors is proposed. This algorithm uses the error pattern $\boldsymbol{E_P}$ obtained from $\boldsymbol{P}$ algorithm introduced in Section 2 to determine all the 23-bit possible error patterns. Among them, one of which may occur really in a noise channel. After the determination of all 23-bit possible errors, the individual bit-error probabilities, namely $p_0, p_1, \ldots, p_{22}$, are first determined by an extension of the ideas given in [10] in a received word of length 23. The individual bit-error probability p_k for $0 \le k \le 22$ is given by

$$p_k = \frac{1}{1 + \exp(2A|x_k|/\sigma^2)}, \quad -\infty < x_k < \infty \tag{12}$$

where σ^2, A and x_k are the channel noise power, the received bit amplitude estimated from the sequence x_k and particular realisations of a discrete-time conditional Gaussian random sequence, respectively.

In the following, we make use of the above three theorems in developing the new decoding method, which is used to determine all possible error patterns.

First, a lookup table that only consist of weight-7 and weight-8 code-words of the (23, 12, 7) Golay-code are generated. Assume an error pattern $\boldsymbol{E_P}$ is obtained by the hard decoder and the number v after the word 'Case' indicates that the weight of $\boldsymbol{E_P}$. Then all the 23-bit possible error patterns are determined with a following case-by-case method.

Case 1: Let $w(\boldsymbol{E_P}) = 1$. $\boldsymbol{E_P}$ is the only candidate error pattern.
Case 2: Let $w(\boldsymbol{E_P}) = 2$. From Section 2, we know that $(\boldsymbol{e} + \boldsymbol{E_P}) \in C$ and $w(\boldsymbol{e} + \boldsymbol{E_P}) \ge 7$. Now $w(\boldsymbol{E_P}) = 2$, and so the weight-5 error patterns are the candidate error patterns. According to Theorems 1–3, one yields

$$\lambda = 253 \cdot \binom{7}{k} / \binom{23}{k} = 253 \cdot \binom{7}{2} / \binom{23}{2} = 21$$

weight-7 code-words; that is, $\boldsymbol{C}_1 = \boldsymbol{e}_1 + \boldsymbol{E_P}$, $\boldsymbol{C}_2 = \boldsymbol{e}_2 + \boldsymbol{E_P}, \ldots, \boldsymbol{C}_{21} = \boldsymbol{e}_{21} + \boldsymbol{E_P}$, where $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_{21}$ are possible weight-5 error patterns. All the possible weight-5 error patterns can be obtained by searching the weight-7 code-words whose non-zero components containing $\mathrm{Loc}(\boldsymbol{E_P})$ in the lookup table, where $\mathrm{Loc}(w) = \{i | w_i \ne 0\} \subseteq \{0, 1, \ldots, n-1\}$ is a set of the locations of non-zero components in a vector $w = (w_0, w_1, \ldots, w_{n-1})$. The number of possible error patterns is equal to 22 including $\boldsymbol{E_P}$

Case 3: Let $w(\boldsymbol{E_P}) = 3$. Similar to that in Case 2, there are $253 \cdot \binom{7}{3} / \binom{23}{3} = 5$ weight-4 candidate error patterns and $506 \cdot \binom{8}{3} / \binom{23}{3} = 16$ weight-5 candidate error patterns, which can be found by searching the lookup table. Thus, the total candidate error patterns including $\boldsymbol{E_P}$ is also 22.

A detailed flow-chart of the above method to determine all the possible error patterns is shown in Fig. 1. For further comprehension, an explicit example is given in the following:

Assume that a weight-3 error $\boldsymbol{E_P} = (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ is obtained by the HD algorithm, then $\mathrm{Loc}(\boldsymbol{E_P}) = \{2, 3, 11\}$. As mentioned above, there are five possible weight-4 and 16 possible weight-5 error patterns. By searching in the lookup table, one yields these code-words whose non-zero components contain the set {2, 3, 11}; that is, $\mathrm{Loc}(\boldsymbol{C}_1) = \{2, 3, 7, 8, 9, 11, 13\}$, $\mathrm{Loc}(\boldsymbol{C}_2) = \{0, 2, 3, 4, 5, 11, 14\}$, $\mathrm{Loc}(\boldsymbol{C}_3) = \{1, 2, 3, 6, 11, 16, 17\}$, $\mathrm{Loc}(\boldsymbol{C}_4) = \{2, 3, 10, 11, 12, 15, 20\}$, $\mathrm{Loc}(\boldsymbol{C}_5) = \{2, 3, 11, 18, 19, 21, 22\}$, $\mathrm{Loc}(\boldsymbol{C}_6) = \{2, 3, 9, 11, 12, 14, 16, 18\}$, $\mathrm{Loc}(\boldsymbol{C}_7) = \{0, 1, 2, 3, 7, 10, 11, 18\}$, $\mathrm{Loc}(\boldsymbol{C}_8) = \{2, 3, 4, 6, 11, 13, 15, 18\}$, $\mathrm{Loc}(\boldsymbol{C}_9) = \{2, 3, 7, 11, 14, 15, 17, 19\}$, $\mathrm{Loc}(\boldsymbol{C}_{10}) = \{1, 2, 3, 4, 8, 11, 12, 19\}$, $\mathrm{Loc}(\boldsymbol{C}_{11}) = \{2, 3, 5, 10, 11, 13, 16, 19\}$, $\mathrm{Loc}(\boldsymbol{C}_{12}) = \{2, 3, 5, 8, 11, 17, 18, 20\}$, $\mathrm{Loc}(\boldsymbol{C}_{13}) = \{0, 2, 3, 6, 9, 11, 19, 20\}$, $\mathrm{Loc}(\boldsymbol{C}_{14}) = \{0, 2, 3, 8, 11, 15, 16, 21\}$, $\mathrm{Loc}(\boldsymbol{C}_{15}) = \{2, 3, 5, 6, 7, 11, 12, 21\}$, $\mathrm{Loc}(\boldsymbol{C}_{16}) = \{2, 3, 4, 9, 10, 11, 17, 21\}$, $\mathrm{Loc}(\boldsymbol{C}_{17}) = \{1, 2, 3, 11, 13, 14, 20, 21\}$, $\mathrm{Loc}(\boldsymbol{C}_{18}) = \{2, 3, 4, 7, 11, 16, 20, 22\}$, $\mathrm{Loc}(\boldsymbol{C}_{19}) = \{0, 2, 3, 11, 12, 13, 17, 22\}$, $\mathrm{Loc}(\boldsymbol{C}_{20}) = \{2, 3, 6, 8, 10, 11, 14, 22\}$ and $\mathrm{Loc}(\boldsymbol{C}_{21}) = \{2, 3, 6, 8, 10, 11, 14, 22\}$.

Consequently, all the 22 possible error vectors $\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_{22}$ are obtained. Among them, the emblematic probability values of the 22 possible patterns can be defined by

$$\hat{p}_i = \prod_{j \in \mathrm{Loc}(\tilde{e}_i)} p_j, \quad i = 1, 2, \ldots, 22 \tag{13}$$

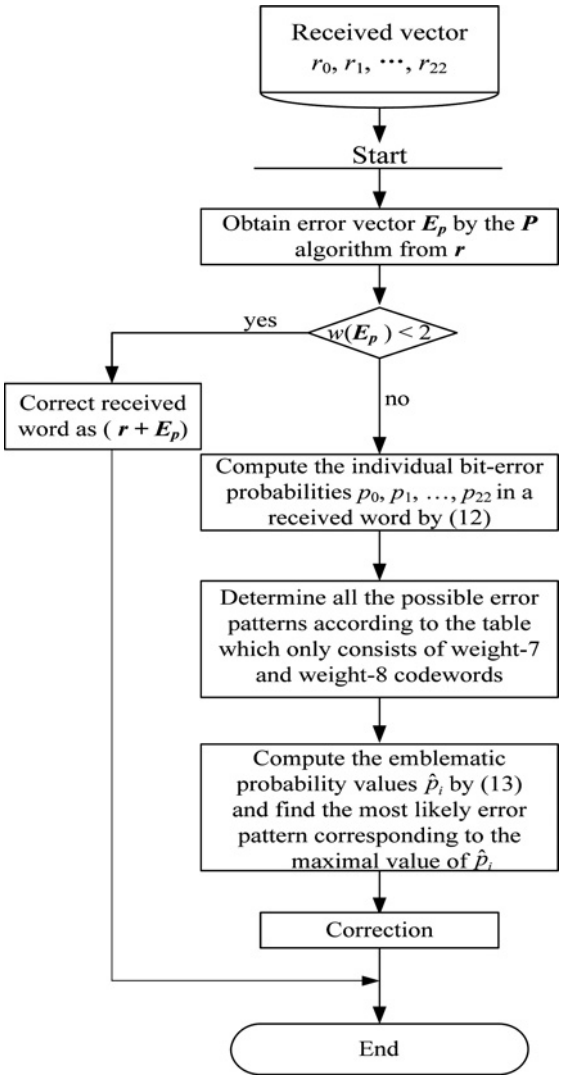

Fig. 2 *Flow-chart of soft-decision decoder of the (23, 12, 7) Golay-code up to five errors*

Finally, the most likely error pattern corresponding to the maximal value of $\hat{p}_i$ in (14) is chosen.

The flow-chart of the proposed decoding algorithm is shown in Fig. 2.

4 Simulation results

Simulations of the proposed decoding algorithm were conducted using C++ programming language on a 2.93 GHz Intel Core i3 Processor. Moreover, bit error rate (BER) and block error rate (BLER) performance in AWGN are illustrated in Figs. 3 and 4, respectively. It is obvious to see that at BER of 10^{-5}, the algorithm in [10] to correct up to four errors is approximate 0.9 dB away from the new decoder and at BLER of 4×10^{-5}, the gap between the both is also about 0.9 dB. Besides, obtaining the performance curves for the new algorithm and Lin *et al.*'s algorithm [10] requires 1682 and 414 s in terms of CPU time, respectively. However, considering the 0.9 dB coding gain, the increased complexity of the proposed algorithm is acceptable. In addition, the percentage of quadruple and quintuple error patterns decoded successfully is given in Table 1.

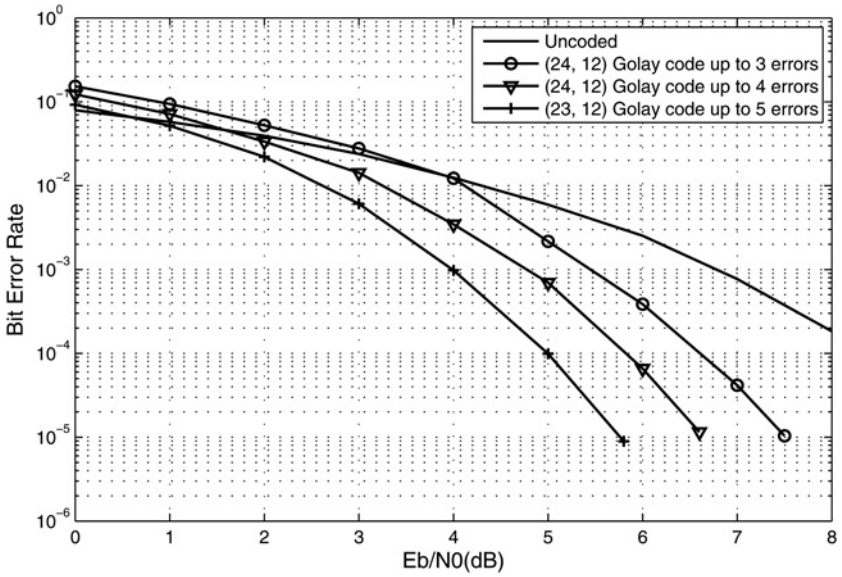

Fig. 3 *BER performance of Golay-codes in AWGN channels*

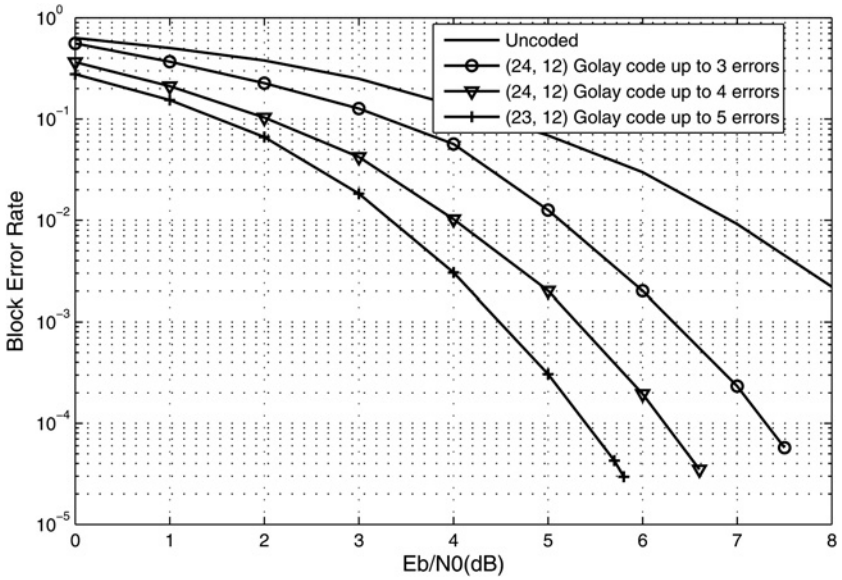

Fig. 4 *BLER performance of Golay-codes in AWGN channels*

Table 1 Percentage of quadruple and quintuple error patterns decoded successfully

Eb/N0 (dB), %	0	1	2	3	4	5	6
quadruple error patterns	76.54	81.91	86.14	94.39	96.00	98.63	99.28
quintuple error patterns	31.45	41.72	54.70	70.23	83.57	91.08	97.59

doi: 10.1049/iet-com.2011.0318

5 Conclusions

In this paper, Lin *et al.*'s algorithm is modified to correct up to five errors for the (23, 12, 7) Golay-code. The proposed soft-decision decoder for the (23, 12, 7) Golay-code can be utilised to correct a very large percentage of quadruple and quintuple error patterns. Computer simulations show that without the overall check bit, as much as 0.9 dB can be achieved by the new decoder instead of the one given in [10] that can correct up to the error-correcting capacity 4.

6 Acknowledgments

The authors thank the editor and the reviewers for their constructive comments and suggestions on improving the quality and the presentation of this paper. This work was partially supported by the NSF of China under Grant no. 60972053 and by the NSF of Fujian Province under Grant no. 2008J0035.

7 References

1 Golay, M.J.E.: 'Notes on digital coding', *Proc. IRE*, 1949, **37**, (1), p. 67
2 McEliece, R.: 'Theory of information and coding' (Addison Wesley, 1977)
3 Elia, M.: 'Algebraic decoding of the (23, 12, 7) Golay code', *IEEE Trans. Inf. Theory*, 1987, **33**, (1), pp. 150–151
4 Reed, I.S., Yin, X., Truong, T.K., Holmes, J.K.: 'Decoding the (24, 12, 8) Golay code', *IEE Proc. Commun.*, 1990, **137**, (3), pp. 202–206
5 Kasami, T.: 'A decoding procedure for multiple error correcting cyclic codes', *IEEE Trans. Inf. Theory*, 1964, **IT-10**, (2), pp. 134–138
6 Wicker, S.B.: 'Error control systems for digital communication and storage' (Prentice-Hall, Englewood Cliffs, NJ, 1995)
7 Lu, E.H., Wuu, H.P., Cheng, Y.C., Lu, P.C.: 'Fast algorithm for decoding the (23, 12) binary Golay code with four-error-correcting capability', *Int. J. Syst. Sci.*, 1995, **26**, (4), pp. 93–945
8 Dubney, G., Reed, I.S.: 'Decoding the (23, 12, 7) Golay code using bit-error probability estimates'. Proc. IEEE Conf. Globecom'05, St. Louis, Missouri, December 2005, vol. 3, pp. 1325–1330
9 Reed, I.S.: 'Statistical error control of a realizable binary symmetric channel'. Group Report 47.35, Massachusetts Institute of Technology, Lincoln Laboratory, Massachusetts, 1959
10 Lin, T.-C., Truong, T.-K., Su, W.-K., Shih, P.-Y., Dubney, G.: 'Decoding of the (24, 12, 8) extended Golay-code up to four errors', *IET Commun.*, 2009, **3**, (2), pp. 232–238
11 Berlekamp, E.: 'Algebraic coding theory' (McGraw-Hill, New York, 1968)
12 Prange, E.: 'Some cyclic error-correcting codes with simple decoding algorithms'. Air Force Cambridge Research Center-TN-58–156 Report, 1958
13 Wang, C., Truong, T.K., Omura, J.K., Reed, I.S., Shao, H.M.: 'VLSI architectures for computing multiplications and inverses in GF(2 m)', *IEEE Trans. Comput.*, 1985, **C-34**, (8), pp. 709–717
14 Assmus, Jr. E.F., Mattson, Jr. H.F.: 'Coding and combinatorics', *SIAM Rev.*, 1974, **16**, (3), pp. 349–388
15 Pless, V.: 'Introduction to the theory of error-correcting codes' (Wiley-Interscience, New York, 1998)