

Research and implementation of SEC-DED Hamming code algorithm

Yuanyuan Cui, Mian Lou, Jianqing Xiao, Xunying Zhang, Senmao Shi, Pengwei Lu

dept. Graduate

Xi'an Microelectronics Technology Institute

Xi'an, China

Abstract—For the space application, error detection and correction (EDAC) technique is often adopted to protect memory cells against Single Event Upset (SEU) errors. To improve the EDAC ability and in view of the parity memory having 8 bits width, a single error correction and double error detection (SEC-DED) (40,32) Hamming code is proposed. This scheme is on the base of (39,32) Hsiao code, adding a check bit to minimize the probability of 3 bits faults corrected in error. To optimize the EDAC circuit area, an algorithm solving mutual expressions is proposed. Experimental results indicate that, compared with the (39,32) Hsiao code method, the critical path delay of the encoder and that of the decoder are not increased, the EDAC circuit area only adds 297.044982 μm^2 , and if the 2GB external memory is protected by the two schemes respectively, the SEU failure rate using the (40,32) Hamming code method can be lower by one order of magnitude. By using the proposed algorithm solving mutual expressions, the circuit area of the encoder and decoder of the (40,32) Hamming code scheme all reduce 72.988199 μm^2 , and the encoder area decreases by 5.9%.

Keywords—error detection and correction code; Single Event Upset; encoder; decoder; failure rate

I. INTRODUCTION

For the space application, single event upset (SEU) is one of the most inducements of the on-chip memory elements generating faults. If such faults aren't corrected in time, the data used by the system will be erroneous. Adding the EDAC circuit is the effective method avoiding SEU fault. The SEC-DED (single error correction and double error detection) Hamming code has the broad application [1-3], but the probability of proton-induced multiple-bit upset (MBU) has increased in highly-scaled technologies, because device dimensions are small relative to particle event track size. To mitigate MBU, cell interleaving technique is used [4], the Hamming code can be adopted [5], because all fault bits for a MBU are from the different words. In our design, the Hamming code scheme is used to protected the external memory, due to the parity memory having 8 bits width, a (40, 32) Hamming code is used, it is on the base of (39,32) Hsiao code, adding a parity bit to minimize the probability of 3 bits faults corrected in error. To minimize the area overhead of the EDAC circuit, an algorithm of solving mutual expression is proposed, the area of the encoder and decoder all reduce 72.988199 μm^2 , the encoder area decreases by 5.9 %.

This work was supported by a grant from the National High Technology Research and Development of China (863 program) (No. 2011AA120201).

II. (40,32) HAMMING CODE ALGORITHM

Hamming code is well known for its single error correction and double error detection capability. It is based on the principle of adding ‘r’ redundancy bits to ‘n’ data bits such that $2^{r-1} \geq n+r$. Therefore, for 32-bit data message, at least 7-bit checksum is needed. However, due to using the 8-bit width check-bits memory, the 8th check bit can be increased, and (40,32) Hamming code scheme can be adopted.

A. Hamming Code Algorithm Summary

In fact, Hamming encoding is the process of calculating the corresponding check bits according to data message. For the (39,32) Hamming code, 7-bit checksum needs to be obtained basing on the correlative 32-bit data message. The check bits vector P can be attained by solving $P=GT$, the addition operation in the formula is the ‘XOR’ Boolean calculation; G is the generation matrix, its dimension is 7*32; T is the column vector of the 32-bit data message. The corresponding row vector of the generation matrix G determines which data message components verified by the check bit P_i ($i=1, \dots, 7$).

Let the received data message is R, which is a 32-bit column vector, let the received check bits is P_R , which is a 7-bit column vector. Therefore, the received whole code word C can be expressed as $C=[R^T, P_R^T]^T$. The parity-check matrix H corresponding to the generation matrix is $H=[G, I]$, I is the 7*7 unit matrix. As a result, the decoding process is as follows:

Step 1: Calculate the syndrome $S=HC$;

Step 2: If S is the zero vector, then the received code word is correct; otherwise, turn to step 3;

Step 3: If S is the same with one column of the matrix H, then there is a correctable fault; otherwise, turn to step 4. If S is the same with j column of the matrix G, $j=0, 1, \dots, 31$, the j^{th} bit of the data R should be corrected; if S is the same with hth column of the matrix I, $h=0, 1, \dots, 6$, the h^{th} bit of the checksum P_{Rj} should be corrected.

Step 4: The code word C has a multiple bits error, this fault can not be corrected.

B. Choice of Parity-check Matrix

According to Hamming decoding algorithm, if a component of the code word has a fault, the syndrome S will equal to the

corresponding column vector of the parity-check matrix; if some components are upset, the syndrome S will equal to the result of those corresponding column vectors from the matrix H doing the bitwise XOR logic operation. Therefore, for the sake of meeting the SEC-DED ability for 32-bit data, the parity-check matrix must satisfy two conditions: (1) all column vectors from the matrix H are different; and (2) the 'XOR' result of the arbitrary two column vectors unequal to other one from the matrix H. The parity-check matrixes satisfying the two conditions are not exclusive. To meet the SEC-DED for 32-bit data and to minimize the area and time overhead, Hsiao abstracts three conditions [6]: (1) the columns of the generation matrix G are all odd weight; (2) the number of 1 in the matrix G is minimum; (3) the difference of the number of 1 in the rows of the matrix G is minimum. Some best matrixes are obtained basing on the above three conditions. We choose such a parity-check $H_{7*32} = [G_{7*32}, I]$, G_{7*32} is as follows:

C. Addition of the Eighth Check Bit

Due to the parity memory having 8 bits width, we can add a parity bit. Except for 1 bit and 2 bits faults, the probability of 3 bits faults should be the highest, adding the 8th parity bit hopes that the number of 3 bits faults corrected in error is least. For all 3 bits faults of the (39, 32) Hsiao code, there are 5452 miscoding cases (3 bits fault is regarded as 1 bit fault). To reduce the miscoding cases, 5452 equations are formed:

$$x_i^m \oplus x_j^m \oplus x_k^m \oplus x_l^m = 1; \quad 0 \leq i, j, k, l \leq 38, \quad m=1,2,\dots,5452 \quad (1)$$

x_i^m , x_j^m , x_k^m and x_l^m indicate whether the 8th parity bit verify the corresponding component of 32-bit data. When $32 \leq p \leq 38$, $x_p^m = 0$, because the check-bit does not verifying other ones. For example, if the 0th, 1st and 4th components of 32-bit data are upset at one time, by (39, 32) Hsiao code scheme decoding, the 3rd component of check-bits is erroneous, so the equation $x_0 \oplus x_1 \oplus x_4 \oplus x_{35} = 1$ should be formed, and $x_{35} = 0$. Therefore, the 8th check-bit should verify (one of) the former 3 components, the aim is, for the 0th, 1st, 4th and 35th columns of H matrix, any 3 columns' 'xor' result different from another one. Any 3 bits are upset synchronously, by the (39,32) Hsiao decoding, the remaining bit is erroneous. The 3/4 of the 5452 equations are reduplicate, so we can search a vector $\mathbf{x} = (x_0, x_1, \dots, x_{31})$ from the following equation group:

$$x_i^m \oplus x_j^m \oplus x_k^m \oplus x_l^m = 1; \quad 0 \leq i < j < k < l \leq 38, \quad m=1,2,\dots,1363 \quad (2)$$

$$x_p^m = 0; 32 \leq p \leq 38 \quad (3)$$

$$\sum_{q=0}^{31} x_q \leq 14; \quad (4)$$

$$x_t = 0/1; t=0,1,\dots,38 \quad (5)$$

This vector should try to satisfy the 1363 equations; the inequation (4) shows the number of 1 of the increased 8th row is not greater than that of other rows of the H matrix; the increased 8th check bit doesn't add the EDAC circuit's critical path delay. We obtain a optimal solution $x=(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$, it can meet 726 equations, so generation matrix of the (40,32) Hamming code is $G_{8*32}=[G_{7*32}^T, x^T]^T$, parity-check matrix $H_{8*40}=[G_{8*32}, I_{8*8}]$, I_{8*8} is the 8*8 unit matrix.

D. EDAC Capability Analyses

For the (39,32) Hsiao code, in the all 3-bit faults ($C_{39}^3 = 9139$), 5452 faults are regarded as 1-bit faults, 3687 faults can be detected, if the 3-bits faults are consider, the SEU failure rate is

$$P_{39} = 1 - [(1-p)^{39} + C_{39}^1 p(1-p)^{38} + C_{39}^2 p^2(1-p)^{37} + 3687 p^3(1-p)^{36}] \quad (6)$$

The p is the SEU failure rate of the one bit data. The order of magnitude of SEU failure rate in LEO is 10^{-7} error/(bit·day), it can be increased in some abnormal regions, here $p=10^{-6}$ error/(bit·day) is selected, so $P_{39}=6.55e-15$ error/(bit·day).

For the (40, 32) Hamming code, in the all 3-bit faults ($C_{40}^3 = 9880$), 7332 can be detected, so the SEU failure rate is:

$$P_{40} = 1 - [(1-p)^{40} + C_{40}^1 p(1-p)^{39} + C_{40}^2 p^2(1-p)^{38} + 7332 p^3(1-p)^{37}] \quad (7)$$

$P_{40}=3.77e-15$ error/(bit·day). P_{39} is greater than P_{40} , so the SEC-DED (40, 32) Hamming code is adopted in this paper.

III. DESIGN OPTIMIZATION

A large number of XOR logic operation are included in the encoder and decoder. To minimize EDAC circuit area overhead, the mutual expressions can be found, namely, if a check bit p_m contains expression $T(w) \oplus T(z)$ ($T(w)$ and $T(z)$ are data message components), and another check bit $p_n (m \neq n)$ also has the same expression, then a xor gate can be shared.

$$X = \begin{bmatrix} 0 & x_{12} & x_{13} & \cdots & x_{1k-1} & x_{1k} \\ 0 & 0 & x_{23} & \cdots & x_{2k-1} & x_{2k} \\ 0 & 0 & 0 & \cdots & x_{3k-1} & x_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & x_{k-1k} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

can be assumed, k is the number of data message components, $x_{ij}=1$ shows $(T(i) \text{ xor } T(j))$ needs to be used for obtaining the check bits, $x_{ij}=0$ shows this expression is needless. x_{ij} and x_{ji} express the same meaning, to avoid repeat, the matrix X 's lower triangular elements are zero. $(T(i) \text{ xor } T(i))=0$, namely, two same component does not appear, so the matrix X 's diagonal elements are zeros too. For each check bit, a similar matrix Xpi can be calculated, according to the following algorithm, all mutual expressions can be found. A greed algorithm solving mutual expression is proposed in [7], but this algorithm is discommodious for acquiring all mutual expressions of the whole scheme, so a more convenient algorithm is proposed.

Algorithm 1:

Initialization: checking all checksum components, if the number of data message components checked by some a checksum component is not power of 2, the least auxiliary message components will be complemented, and the number of the total data message components will just be 2's power. The purpose is that the data message components verified by each check bit can be matched in couples, and the process of solving mutual expressions can be simplified. And let data message component $S_1=\{\text{all data message components, and auxiliary message components}\}$; let deletion check bits indexes set $D=\emptyset$ (empty set); let the set $N=\{\text{the number of data message components verified by each check bit}\}$; let $t=1$.

Step 1: The check bits are expressed by the elements of the set S_1 . If a certain checksum component only checks one of the message components, namely, the corresponding element of the set N equals to 1, then the index of the checksum component will be added to set D ; if all elements of the set N all equal to 1, then turn to step 8, otherwise, turn to step 2.

Step 2: Calculate all matrixes X_{Pi} of increasing auxiliary message components ($i \in I=\{1, \dots, r\} - D$), r is the number of checksum components.

Step 3: Calculate $X_P = \sum_i X_{Pi}$, search for the maximal component $x_{m,i} = \max\{X_{Pi,j}\}$;

Step 4: If the component $x_{m,i}$ of the matrix X_{Pi} equals to zero, then the m^{th} and i^{th} rows, the m^{th} and i^{th} columns are all set to zero vectors;

Step 5: $(m, i, np_1, \dots, np_r)$ is added to the new components set S_{t+1} . If the component $x_{m,i}$ of the matrix X_{Pi} equals to 1, then $np_i=1$, otherwise, $np_i=0$, $i=1, 2, \dots, r$;

Step 6: Examine all matrixes X_{Pi} , if they are not all zero matrixes, then turn to step 3, otherwise, turn to step 7;

Step 7: The new components set S_{t+1} is obtained, $t=t+1$; the elements greater than 1 in the set N all divided by 2, the elements equaling to 1 keep the former values, turn to step 1;

Step 8: Stop, according to the relationship of the sets S_1, S_2, \dots, S_t , a directed group can be constructed, and removing all nodes correlative with auxiliary message components, all mutual expressions are obtained.

A small example is constructed as follows; this example has no practical value only in order to illuminating the above algorithm. Data message has 6 components d_1, d_2, \dots, d_6 , checksum has $r=2$ components p_1 and p_2 , and $p_1=d_1 \oplus d_3 \oplus d_4 \oplus d_6$, $p_2=d_1 \oplus d_2 \oplus d_3 \oplus d_4 \oplus d_5 \oplus d_6$. According to the above algorithm, first of all, we should do initialization step. p_1 includes 4 data message components, 4 is just 2's power; but p_2 contains 6 components; in order to be 2's power, 2 auxiliary message components d_7 and d_8 are increased, $p_2=d_1 \oplus d_2 \oplus d_3 \oplus d_4 \oplus d_5 \oplus d_6 \oplus d_7 \oplus d_8$.

Therefore, the message components set $S_1=\{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8\}$, $N=\{4, 8\}$, $D=\emptyset$. After the first iteration, the components set $S_2=\{(S_1(1), S_1(3), 1, 1), (S_1(4), S_1(6), 1, 1), (S_1(2), S_1(5), 0, 1), (S_1(7), S_1(8), 0, 1)\}$, $N=\{2, 4\}$, $D=\emptyset$, it is not difficult to see the set S_2 is not exclusive, as a result, the final mutual expressions set is not exclusive, but the number of using 2-input XOR logic gates is uniform. After the second iteration, the set $S_3=\{(S_2(1), S_2(2), 1, 1), (S_2(3), S_2(4), 0, 1)\}$, $N=\{1, 2\}$, $D=\{1\}$, so all mutual expressions of the first checksum component p_1 have been obtained. After the last iteration, $S_4=\{(S_3(1), S_3(2), 0, 1)\}$, $N=\{1, 1\}$, $D=\{1, 2\}$. According to the relationship of S_1, S_2, S_3 and S_4 , the corresponding directed group is constructed. Figure 1 shows that the checksum components p_1 and p_2 share $(d_1 \oplus d_3)$, $(d_4 \oplus d_6)$ and $((d_1 \oplus d_3) \oplus (d_4 \oplus d_6))$, the area overhead of three 2-input XOR gates is saved.

In order to simplify the problem, some auxiliary message components are increased, but they are not existent in actual problem, so these auxiliary variables should be removed, finally, figure 2 shows the whole mutual expressions.

Therefore, the proposed (40,32) Hamming encode circuit can be optimized using the above algorithm, the optimal solution shows that 29 2-input 'XOR' logic gates are saved. It is well known that the decode circuit includes the encode circuit in fact, so the decoder can also be reduced the area overhead of 29 2-input 'XOR' logic circuits.

IV. EXPERIMENTAL RESULTS ANALYSES

In order to verify the validity of the proposed (40,32) Hamming code, this scheme is compared with the (39,32) Hsiao code scheme. Table 1 shows the EDAC scheme area overhead comparison using SMIC 130nm standard CMOS process to synthesize. In view of the parity memory having 8 bits width, the size of check bits memory using the two schemes respectively, are all 25% of that of data memory. Due to the synthesis tool, DC (Design Compiler), including optimization policy, the area overhead of encode circuit of the (39,32) Hsiao code scheme is 1305.300573 um^2 , but under the same constraints conditions, that of the proposed (40,32) Hamming code scheme is only 1228.917570 um^2 , the overhead of encoder decreased 76.383003 um^2 . It is shown that the optimization policy for the (40,32) Hamming code scheme has a better solution. The decoder area overhead of the proposed scheme only adds 373.427985 um^2 .

TABLE I. EADC SCHEME AREA OVERHEAD COMPARISON

EDAC Scheme	Area Overhead		
	check bits memory percent	Encode circuit area /um ²	Decode circuit area /um ²
(39,32) Hsiao	25%	1305.300573	5881.490971
(40,32)Hamming	25%	1228.917570	6254.918956

TABLE III. EADC SCHEME SEU FAILURE RATE COMPARISON

EDAC Scheme	SEU Failure Rate
(39,32) Hsiao	1.41e-5
(40,32)Hamming	8.10e-6

In order to verify the validity of the proposed algorithm solving mutual expressions, the encoder and decoder of the proposed (40,32) Hamming code scheme are synthesized under the using and no using algorithm 1 condition respectively. Table 4 shows the area overhead. Although the synthesis tool including optimization policy, a global optimal solution can be obtained basing on the proposed algorithm in this paper. As a result, the circuit area of the encoder and decoder all reduce 72.988199 um², the encoder area increases by 5.9%.

TABLE IV. AREA OVERHEAD OF ENCODER AND DECODER COMPARISON

Using Algorithm 1	Area Overhead	
	Encoding Circuit area /um ²	Decoding Circuit area /um ²
YES	1228.917570	6254.918956
NO	1155.929371	6181.930757

V. CONCLUSIONS

Due to using the 8-bit width check-bits memory in our design, this paper presented a SEC-DED (40,32) Hamming code algorithm, it is on the base of (39,32) Hsiao code, adding a parity bit to minimize the probability of 3 bits faults corrected in error. A large number of ‘XOR’ logic operations are included in the encoder and decoder, if some checksum components all check two same data message components, namely, they have a mutual expression, then these checksum components can be share a ‘XOR’ gate. To optimize the EDAC circuit, an algorithm solving mutual expressions is proposed. Compared with the (39,32) Hsiao code method, the critical path delay of the encoder and that of the decoder are not increased, the EDAC circuit area only adds 297.044982 um², but if the 2GB exterior memory is protected by the two schemes respectively, the SEU failure rate using the proposed method can be lower by one order of magnitude. By using the algorithm solving mutual expressions, the EDAC circuit area of the (40,32) Hamming code scheme reduces 145.976398 um².

ACKNOWLEDGMENT

We would like to thank all members of the SOC design team Xi'an Microelectronics Technology Institute for support and encouragement during this work.

REFERENCES

- [1] Mohr, Karl C., Giby Samson, and Lawrence T. Clark. "A Radiation Hardened by Design Register File With Lightweight Error Detection and Correction." IEEE Trans. On Nucl. Sci., Vol.54, pp. 1335-1342, August 2007.
- [2] M. Tang, G. Zhang, and H. Zhang, "Auto error correction hardware implementation of AES algorithm," Acta Ele. Sin., vol.33, pp. 2013-2016, November 2005.

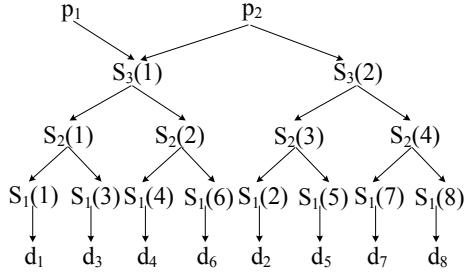


Fig. 1. The directed group with auxiliary message components

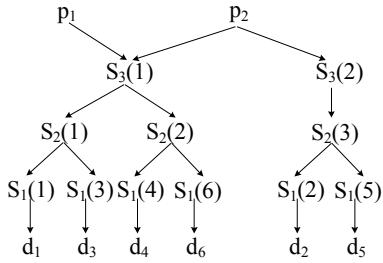


Fig. 2. The directed group without auxiliary message components

Table 2 shows the EDAC scheme performance comparison. For the proposed (40,32) Hamming code algorithm, although the 8th check bit is added, the precondition is the critical path delay is not greater than that of the (39,32) Hsiao code algorithm. Therefore, the encoding delay and the decoding delay are not increased.

TABLE II. EADC SCHEME PERFORMANCE COMPARISON

EDAC Scheme	Critical Path Delay	
	Encoding Delay /ns	Decoding Delay /ns
(39,32) Hsiao	1.01	2.37
(40,32)Hamming	0.98	2.37

To prove the proposed (40,32) Hamming code scheme having a higher reliability, the 2GB external memory is protected by the two schemes respectively. If the (39,32) Hsiao code scheme is used, the SEU failure rate of the external memory is:

$$P_{\text{mem_39}} = 1 - (1 - P_{39})^{2^{147483648}} \quad (8)$$

If the proposed (40,32) Hamming code scheme is used, the SEU failure rate of the external memory is:

$$P_{\text{mem_40}} = 1 - (1 - P_{40})^{2^{147483648}} \quad (9)$$

According to Eq. (8) and Eq. (9), the SEU failure rate of the external memory can be attained shown in table 3. Compared with the first scheme, the SEU failure rate of the external memory using the proposed scheme is lower by one order of magnitude, the reliability of the memory operation is improved.

- [3] R. Xu, Z. Gu and J. Luo, "Design of radiation hardened error detection and correction circuit," *Microelectronics*, vol. 40, pp. 547-550, August 2010.
- [4] A. D. Tipton, J.A. Pelli, R.A. Reed, R.D. Schrimpf, R.A. Weller, M.H. Mendenhall et al, "Multiple-bit upset in 130nm CMOS technology," *IEEE Trans. On Nucl. Sci.*, vol. 53, pp. 3259-3264, December 2006.
- [5] J.Gaisler, "A portable and fault-tolerant microprocessor based on the SPARC v8 architecture," In *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, pp. 409-415.
- [6] M.Y. Hsiao, "A class of optimal minimum odd-weight-column SEC-DED codes," *IBM J. Res. Develop.*, vol. 14, pp. 395-401, July,1970.
- [7] Y. Cui, X. Zhang, "Research and implementation of interleaving grouping Hamming code algorithm," unpublished.