TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 09/19 pp474-477
Volume 14, Number 4, August 2009

A Low Power Error Detection in the Syndrome Calculator Block for Reed-Solomon Codes: RS(204,188)*

Richard Huynh, GE Ning (葛 宁)**, YANG Huazhong (杨华中)

Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

Abstract: Reed-Solomon (RS) codes have been widely adopted in many modern communication systems. This paper describes a new method for error detection in the syndrome calculator block of RS decoders. The main feature of this method is to prove that it is possible to compute only a few syndrome coefficients — less than half — to detect whether the codeword is correct. The theoretical estimate of the probability that the new algorithm failed is shown to depend on the number of syndrome coefficients computed. The algorithm is tested using the RS(204,188) code with the first four coefficients. With a bit error rate of 1×10^{-4}, this method reduces the power consumption by 6% compared to the basic RS(204,188) decoder. The error detection algorithm for the syndrome calculator block does not require modification of the basic hardware implementation of the syndrome coefficients computation. The algorithm significantly reduces the computation complexity of the syndrome calculator block, thus lowering the power needed.

Key words: Reed-Solomon codes; syndrome calculator block; error detection; bit error rate

Introduction

Communication technologies are widely used these days. Due to the growing percentage of people using these technologies, methods are needed to increase the transmission rate without reducing the quality. One of these methods is the Reed-Solomon (RS) codes which are used to correct errors in many systems such as storage devices (CD, DVD, etc.) and digital video broadcasting (DVB).

An RS codeword is a packet of symbols which are commonly bytes (8-bit symbols), denoted as RS(n, k) where n is the number of symbols in the encoded message and k is the number of symbols in the original message. Each RS codeword can correct a maximum of $t=(n-k)/2$ errors in a received packet.

This work seeks to reduce the number of computations needed for error detection. We prove that it is possible to compute less than half of the syndrome coefficients with quasi-similar error detection reliability. The main parameter of this method is the number of computed syndrome coefficients. The algorithm only computes a few syndrome coefficients. If they are all zero, the codeword is considered to be correct. If the codeword is not correct, the entire syndrome polynomial is obtained so the errors can be corrected through the other blocks[1]. This paper focuses on proving that this method is reliable by estimating the probability that it fails. The algorithm is also tested and compared to the basic RS decoder.

1 Background and Related Work

The syndrome calculator block provides two results. The first result is whether the received codeword is correct. The second result provides the syndrome

Received: 2008-04-22; revised: 2008-10-31

* Supported by the National High-Tech Research and Development (863) Program of China (No. 2007AA01Z2B3)

** To whom correspondence should be addressed.
E-mail: gening@tsinghua.edu.cn; Tel: 86-10-62771118

polynomial which will be used to correct the codeword if the codeword is erroneous. The most common algorithm[2] to perform the syndrome calculation needs $2t$ basic cells as defined in Fig. 1 with each cell, c_i, giving one syndrome coefficient, S_i, with $1 \leqslant i \leqslant 2t$.

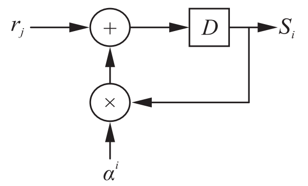

Fig. 1 Basic syndrome calculator cell

In Fig. 1, r_j, $1 \leqslant j \leqslant n$, is the j-th coefficient of the received codeword polynomial, $r(x)$, so n computations are needed to compute the syndrome polynomial. All the syndrome coefficients will be equal to 0 if the received codeword is correct with at least one coefficient different from 0 if the codeword is not correct.

Much work has been done to reduce time-consuming computational steps. Costa et al.[3] developed a new fast Fourier transform (FFT) method based on the cyclotomic FFT to compute the syndrome using a method that corresponds to the partial discrete Fourier transform (DFT) of $D(x)$. This algorithm is better than the Horner rule[4] and the Zakharova method[5]. In 2007, Lin et al.[6] developed a method based on the Trifono-Fedorenko[7] procedure, showing that the problem of computing the syndromes for time-domain RS decoders can be solved by the use of affine polynomials with a sequence of vectors. Their method has very good results for finite fields.

All these algorithms depend on modifications of the conventional syndrome computational method. Lee et al.[8] provided a method for reducing the number of computations in syndrome polynomials by decoding error correction codes without modifying the standard method. The relationship between the syndromes and the coefficients of the error locator polynomial[1] infers that if the first t syndromes are zeros, the next t syndromes must also be zeros. Thus, only half of the syndromes must be calculated to know if the codeword is correct.

2 Theory of the Error Checking Algorithm

Some following notations are defined to simplify the explanation:

- h is the number of zeros in the syndrome vector.
- N_{synd}, $1 \leqslant N_{\text{synd}} \leqslant t-1$, corresponds to the number of first coefficients in the syndrome vector. For instance, if $N_{\text{synd}}=4$, the calculation uses S_1, S_2, S_3, and S_4.
- P_{zeros} is the probability to have h or N_{synd} verified.

The objective is to show that less than half of the syndromes are needed to check whether the codeword is correct. The only parameter in the algorithm shown in Fig. 2 is N_{synd}.

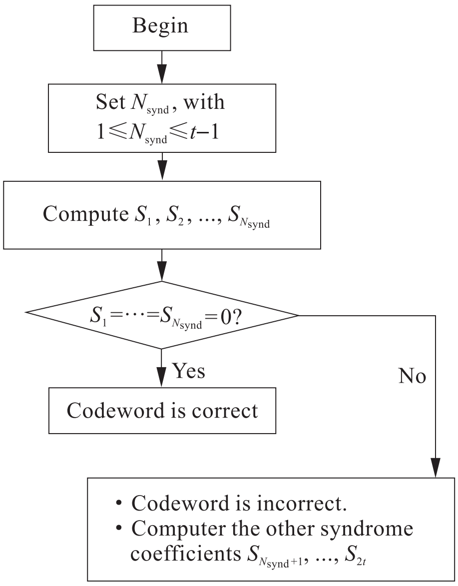

Fig. 2 Error checking algorithm

From the algorithm in Fig. 2,

- For a correct codeword, the algorithm never fails.
- For an erroneous codeword, the algorithm could fail if the few first components, N_{synd}, of the syndrome vector are zero.

The Hamming distance implies that i syndrome coefficients with $i < t$ are able to detect only $i-1$ errors. Therefore, this algorithm could fail in some cases. The following estimates the failure rate:

The RS(n, k) syndrome calculator computes the syndrome vector with R as the received codeword, C the sent codeword, and E the errors in the received codeword.

$$S_{i+1} = R(\alpha^i) = C(\alpha^i) + E(\alpha^i) = E(\alpha^i),\ \ 0 \leqslant i \leqslant 2t-1 \tag{1}$$

$C(\alpha^i)=0$ according to the definition of the RS codeword, and

$$R(x) = R_0 + R_1 x + R_2 x^2 + \cdots + R_{N-1} x^{N-1} \tag{2}$$

R_{N-1} is the first received symbol.

If the codeword R is correct, the syndrome vector is zero, but if the codeword is erroneous and given by

R',

$$S'_{i+1}=R'(\alpha^i)=C(\alpha^i)+E(\alpha^i)=E(\alpha^i),\ 0\leqslant i\leqslant 2t-1 \tag{3}$$

$$E(\alpha^i)=R'_0+R'_1\alpha^i+R'_2(\alpha^i)^2+\cdots+R'_{N-1}(\alpha^i)^{N-1} \tag{4}$$

Suppose that ($E_0, E_1, \ldots, E_{t-1}$) are the error amplitude and ($x_{j_0}, x_{j_1}, \ldots, x_{j_{t-1}}$) are the error position. If there are more than t errors, the RS decoder will fail.

$$E(\alpha^i)=E_0(\alpha^i)^{j_0}+E_1(\alpha^i)^{j_1}+\cdots+E_{t-1}(\alpha^i)^{j_{t-1}} \tag{5}$$

- If there is only 1 error, $E(\alpha^i)=E_0(\alpha^i)^{j_0}\neq 0$, one can deduce that the syndrome vector cannot be zero.
- If there are 2 errors, $E(\alpha^i)=E_0(\alpha^i)^{j_0}+E_1(\alpha^i)^{j_1}=0\rightarrow E_0(\alpha^i)^{j_0}=E_1(\alpha^i)^{j_1}$.
- With 3 errors, $E_0(\alpha^i)^{j_0}+E_1(\alpha^i)^{j_1}+E_2(\alpha^i)^{j_1}=0\rightarrow E_0(\alpha^i)^{j_0}=E_1(\alpha^i)^{j_1}+E_2(\alpha^i)^{j_1}$ with $A=E_1(\alpha^i)^{j_1}+E_2(\alpha^i)^{j_1}\rightarrow E_0(\alpha^i)^{j_0}=A$ which is the same problem as with 2 errors.

Thus, for more than 2 errors, the failure rate does not depend on the number of errors because a syndrome coefficient is obtained by an addition and not a multiplication.

The probability $P(h)$ to have h zeros in the syndrome is as follows:

For a codeword with 1 error,

$$P(0)=1 \tag{6}$$

For a codeword with 2, 3, …, t–1 errors,

$$\begin{cases} P(h)\approx\left(\dfrac{2t}{2^m}\right)^h, & 1\leqslant h\leqslant t; \\ P(0)\approx 1-\sum\limits_{i=1}^{t}P(i), & h=0 \end{cases} \tag{7}$$

The function $\dfrac{1}{2^m}$ is used to indicate that the amplitude and the position of the error both vary from 1 to 2^m, where m is the number of bits per symbol. The function $2t$ is used because there are $2t$ coefficients in a syndrome polynomial so there are $2t$ possibilities to have a zero.

Next, focus on the position of the zero and more exactly, about how many syndromes have N_{synd} coefficients equal to 0. Basic probability methods can be used to approximate the probability to have N_{synd} zeros at the N_{synd} coefficients so that $S_1=S_2=\cdots=S_{N_{\text{synd}}}=0$ with $1\leqslant N_{\text{synd}}\leqslant t-1$:

$$P_j=\frac{P(j)}{\prod\limits_{i=0}^{i=j-1}(2t-i)} \tag{8}$$

where P_j is the probability to have the first "j" coefficients equal to 0.

This result is verified by simulations in Section 3.

3 Simulations and Results

3.1 Simulation

The simulations sent 1×10^8 erroneous RS(204,188) codewords with random numbers of errors, from 2 to 8 errors per codeword, through the syndrome calculator block to calculate the number of zeros and the positions of these zeros for each syndrome polynomial.

The results in Figs. 3 and 4 show that the theoretical probabilities agree well with the simulation for Eq. (7) for h up to 5 and for Eq. (8) for N_{synd} up to 2. Thus, if one received only erroneous codewords and checked the first two coefficients, this method would fail only once every 10^{-5} times.

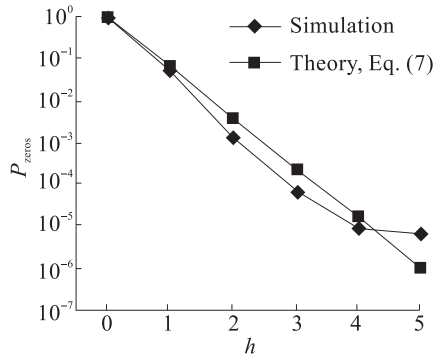

Fig. 3 Predicted and actual probabilities of a syndrome having *h* zeros

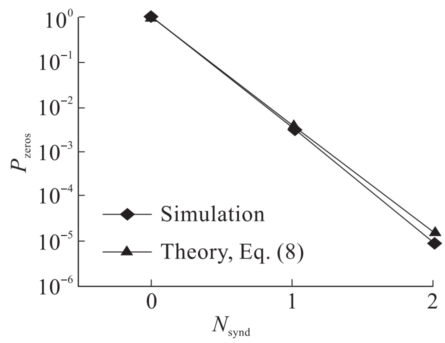

Fig. 4 Predicted and actual probabilities of the number of syndromes having N_{synd} zeros

3.2 Comparison of algorithms

The modified syndrome computational algorithm was implemented on the RS(204,188) decoder to check the robustness and complexity of this method by sending a packet of 100 000 RS(204,188) codewords with various bit error rate (BER) (10^{-3}, 10^{-4}, and 10^{-5}) through the RS(204,188) decoder with the quarter syndrome computation with $N_{\text{synd}} = 4$.

The decoding error is the same as the quarter syndrome computation and the standard RS(204,188) decoder. Then, as shown in Fig. 5, for a BER of 10^{-4}, this method reduces the power consumption by 6% compared to the basic algorithm. Then, this method becomes even more efficient as the BER improves.

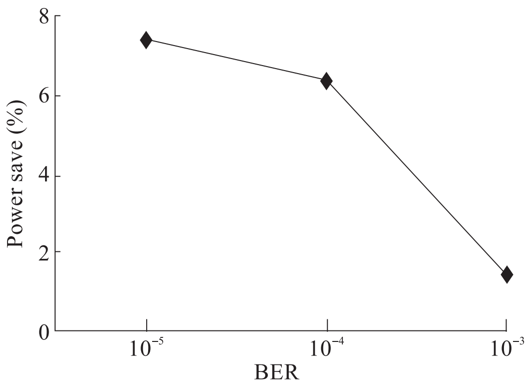

Fig. 5 Power saved compared to the basic RS(204, 188) decoder

4 Conclusions

An error detection method was developed to analyze RS codewords with less than half of the syndrome computed. Simulations show that erroneous codewords can be reliably detected by computing only three or four syndrome coefficients. With more syndrome coefficients, up to t−1, the detection will be even more reliable. The theoretical reliability is presented for 1 to 7 syndrome coefficients for RS(204,188). The quarter syndrome computation with a BER of 10^{-4} can save 6% of power compared to the basic algorithm with the same decoding error for the basic RS(204,188) decoder.

References

[1] Chang H C, Shung C B, Lee C Y. A Reed-Solomon product-pode (RS-PC) decoder chip for DVD applications. *IEEE Journal of Solid-State Circuits*, 2001, **36**(2): 229-238.

[2] Berlekamp E R. Algebraic Coding Theory. New York: McGraw-Hill, 1968.

[3] Costa E, Fedorenko S V, Trifonov P V. On computing the syndrome polynomial in Reed-Solomon decoder. *Eur. Trans. Telecommun.*, 2004, **15**(4): 337-342.

[4] Wicker S B, Bhargava V K. Reed-Solomon Codes and Their Application. New York, USA: IEEE Press, 1994.

[5] Zakharova T G. Fourier transform evaluation in fields of characteristic 2. *Problems Inf. Transmiss.*, 1992, **28**(2): 154-167.

[6] Lin T C, Truong T K, Chen P D. A fast algorithm for the syndrome calculation in algebraic decoding of Reed-Solomon codes. *IEEE Transactions on Communications*, 2007, **55**(12): 2240-2244.

[7] Trifonov P V, Fedorenko S V. A method for fast computation of the Fourier transform over a finite field. *Problems Inf. Transmiss.*, 2003, **39**(3): 231-238.

[8] Lee C Y, Chang H S, Lin C C. Method for calculating syndrome polynomial in decoding error correction codes. United States Patent, 2005.