

Power-Management-Based Chien Search for Low Power BCH Decoder

Shu-Yi Wong

Chunhong Chen

Q. M. Jonathan Wu

Department of Electrical and Computer Engineering
University of Windsor, Ontario, Canada N9B 3P4

{wong11j, cchen, jwu}@uwindsor.ca

ABSTRACT

Chien search is a computation-intensive VLSI design in BCH (Bose-Chaudhuri-Hocquenghem) decoders for a variety of applications such as digital video and data storage. Existing low power approaches to this subject are effective only for single-bit error case, and their power efficiency decreases dramatically for multiple-bit-correcting code. This paper presents a novel approach of using register-transfer-level (RTL) power management in the search process, leading to significant power savings for BCH codes with higher correction capability. A (255, 187, 9) BCH code is implemented in 0.18 μ m CMOS technology as an example.

Categories and Subject Descriptors

B.4.1 [Input/Output and Data Communications]: Data Communications Devices – processors, receivers

General Terms

Design

Keywords

BCH decoder, Chien search, low power, power management

1. INTRODUCTION

A BCH (Bose-Chaudhuri-Hocquenghem) [1] code is a form of forward error correcting block code described by (n, k, t) , where n is the block size in bits, k is the message size, and t is the error correcting capability. On the subject of low-power BCH decoder, a lot of research has been done for the first and second decoding steps, namely the syndrome computation [2] and the key equation solver [2-4]. However, it is Chien search [6], the most common VLSI implementation [2-5, 8] for the final decoding step, that has been shown as the most significant contributor to the decoder's overall power consumption [5]. In [5], a low power Chien search method claims up to 50% power savings for $t = 1$, but its performance is severely degraded as the value of t increases. The

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ISLPED'09, August 19–21, 2009, San Francisco, California, USA.
Copyright 2009 ACM 978-1-60558-684-7/09/08...\$10.00.

power savings for $t = 2$ and $t = 8$, in particular, are only 39.6% and 19.7%, respectively. This is a serious drawback as the recent increase in portable digital video ($t = 5, 7, 11$) [7] and data storage ($t = 4$) [8] applications requires simultaneous low-power design and high error-correction capability for Chien search. Targeting this problem, this paper presents a new method of using register-transfer (RT)-level power management for low power Chien search.

2. SAVING POWER FOR CHIEN SEARCH

2.1 Conventional Chien Search

Figure 1 (solid lines) illustrates the conventional Chien search [2, 4, 8]. All power savings discussed in this paper are with respect to the power consumption of this circuit for an error polynomial over $GF(2^m)$:

$$\begin{cases} \Lambda_t(R_i) = 1 + \sum_{i=1}^t R_i \\ \text{where } R_i = \sigma_i X^i \text{ and } X = \alpha^z \end{cases} \quad (1)$$

With the assumption of polynomial bases, α is the primitive element of $GF(2^m)$ in the form of m -tuple. The multiplier symbols in Figure 1 are Finite-Field Multipliers (FFMs). The R_i registers (middle square boxes in the figure) are used for storing the products except for the very beginning of a search cycle when the registers are loaded, through multiplexors, with σ_i , the initial coefficient values of the error polynomial. A complete search for each received message $r(X)$ involves n clock-cycles. It is therefore an exhaustive linear search of all possible error positions, and an error is found when $\Lambda_t(R_i) = 0$.

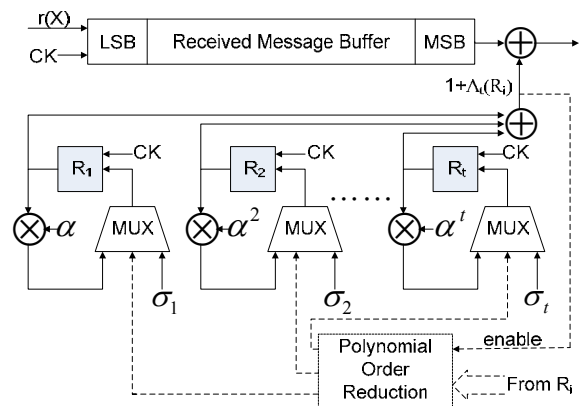


Figure 1. Block diagram of Chien search

2.2 Existing Low-Power Methods

In the conventional Chien search, FFMs are always powered on. The method of [5] achieves power savings by terminating the whole Chien search after all errors are corrected. Its analysis assumed equal probabilities of receiving 1 to t random error-bits per message, leading to the estimated power savings of:

$$S_c = \frac{1}{t} \sum_{r=1}^t (1 - r\sqrt{0.5}) \quad (2)$$

for a (n, k, t) BCH decoder. Negligible power consumption of the supporting circuitry was assumed without experimental proof.

Another low power solution is parallel Chien search architecture proposed in [3]. Since dynamic power dissipation P is proportional to the frequency f and the square of voltage V , as shown below:

$$P \propto V^2 f \quad (3)$$

To achieve power savings, V can be reduced with f being K times slower but at a cost of increasing silicon area by roughly $K \times 100\%$. Savings of 40% have been reported when $K = 2$.

2.3 The Proposed Method

The existing methods including [5] are by no means a perfect power optimizer for Chien search circuit. Additional power savings could arise from power disabling some circuits in Figure 1 prior to the eventual power-down of the entire Chien search at the final error-bit. This idea is illustrated in the dotted-line blocks of Figure 1, where the 2-to-1 multiplexors have also been replaced by 3-to-1 multiplexors. When no error bit is encountered, the block is disabled and the circuit's operation is the same as that of the conventional search. Upon the detection of an error, $\Lambda_i(R_i)$ becomes zero, which signals not only the correction of the most significant bit for the received message buffer but also enables a polynomial order reduction (POR) circuit (refer to Section 2.4). When this happens, the clock to the received message buffer is halted for one clock cycle. Meanwhile, the product registers are loaded with new values determined by the polynomial order reduction process. After each order reduction cycle, the clock signal to the received message buffer resumes, and the Chien search operates the same as before. In addition, the highest order register carrying a non-zero value will also be updated to zero. This register is then disabled by clock gating. As the updating process continues, all registers will eventually become zero, and the required power for the associated circuits is hence saved.

To see how the polynomial order reduction process can disable one register for every detected error, (1) is rewritten as

$$\Lambda_t(X) = (1 + \beta_1 X)(1 + \beta_2 X) \dots (1 + \beta_t X) \quad (4)$$

Thus, the Chien search is essentially a process of finding all roots of (4), namely $1/\beta_1, 1/\beta_2, \dots, 1/\beta_t$. If, for instance, $1/\beta_t$ has been found, then the last term of (4) will no longer be significant for the determination of other roots and (4) can be factored out, leading to the reduced order from t to $t-1$. The obtained polynomial requires only $t-1$ instead of t FFMs. As the Chien search progresses from the most to the least significant error positions, the aforementioned process can continue until the order of the error polynomial becomes zero. To further clarify how

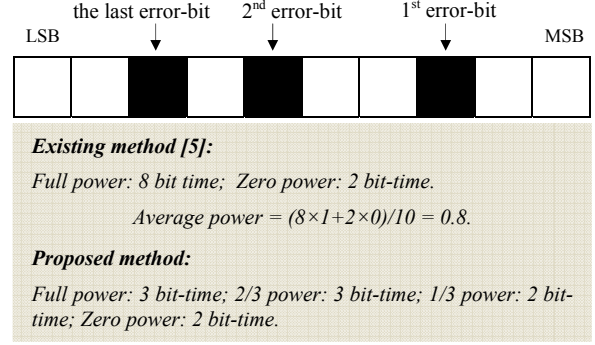


Figure 2. An example for 10-bit BCH code with 3 FFMs

additional power can be saved when compared to [5], a 10-bit BCH code using three FFMs is given in Figure 2 as a motivational example. For the method of [5], all three FFMs would consume power for eight out of ten clock cycles. The power consumption, therefore, equals 0.8 (assuming the power consumption for the conventional Chien search is normalized to unity and that the power consumption is identical for every clock cycle). The proposed method, however, stays in the full-power condition for only three clock cycles with reduced power consumption for clock cycles # 4 through #8, promising better power performance with average power of 0.56.

At RT-level, in order to predict power savings with respect to the conventional Chien search, it is assumed that (a) the power dissipation of Chien search comes solely from active FFMs, and (b) all FFMs consume the same amount of power when becoming active. Hence, the power modeling that follows focuses only on FFMs (the effect of POR will be discussed in Section 2.5).

On the other hand, for a (n, k, t) BCH decoder, more power will be consumed by the Chien search correcting t errors than the same circuit correcting only one error as the former requires $t-1$ more FFMs than the latter. Therefore, error distribution affects power consumption. For a fair comparison with the power data of [5], the same equal-probability assumption of (2) is used. As such, the average power savings can be determined by combinatorial analysis, resulting in (without proof):

$$\bar{S}_p = 1 - \frac{n+1}{2nt} \cdot \sum_{q=1}^t \frac{q}{t} \quad (5)$$

or

$$\bar{S}_p \approx \frac{1}{4} \left[3 - \frac{1}{n} - \frac{1}{t} \left(1 + \frac{1}{n} \right) \right] \approx 0.75 \quad (6)$$

for $n, t \gg 1$

Figure 3 illustrates the clear advantage of our proposed method over the method of [5] for $(255, k, t)$ BCH codes.

2.4 A Polynomial Order Reduction Algorithm

Polynomial Order Reduction (POR) is a factorization process signaled by $\Lambda_i(R_i) = 0$ upon detection of an error position. The new error polynomial of order u is represented by:

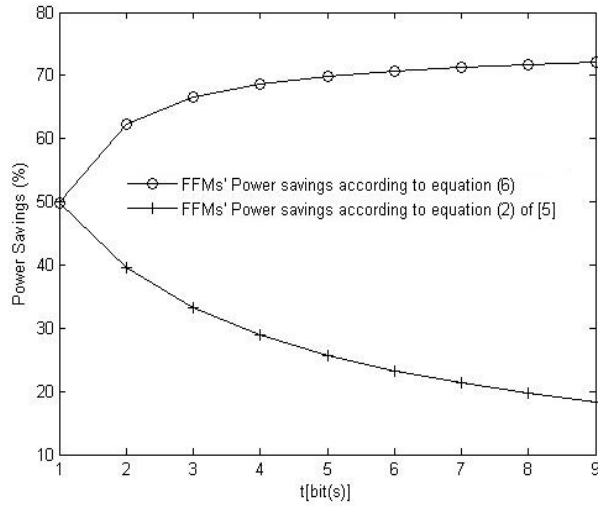


Figure 3. Power comparison of [5] vs. the proposed method

$$\begin{cases} \Lambda_u(R_w) = 1 + \sum_{w=1}^u R_w \\ R_w = \sigma_w(\varepsilon)X^w \end{cases} \quad (7)$$

where the coefficients of X are functions of ε , and ε ($\varepsilon = 1, 2, \dots, t$) corresponds to the number of polynomial order reductions already performed. When an error polynomial's order is reduced from u to $u' = u - 1$, the update values R_w ' for R_w can be shown as:

$$R_w^i = \sum_{\lambda=w+1}^u R_\lambda \quad (8)$$

which means that the update value for the w -th order register is simply the sum of all higher-order register values.

2.5 Miscellaneous Effects

The POR process requires extra clock cycles in comparison with the conventional Chien search. To compensate for the interfacing differences, the input clock frequency can be increased by q/n to keep the same output rate of corrected bit-stream, where q is the number of error-bits in the received message and n is the message length. Since q ranges from 1 to t and is far smaller than n for practical BCH decoders, accurate modeling is not necessary and the average power increase can reasonably be estimated by averaging factors of q/n , resulting in only a negligible power increase of 2% for a (255,187,9) BCH code.

To get some idea of how the proposed power savings vary with the input error distribution, it is found by some analysis that power savings for the FFMs are approximately 50% if the probability of q being equal to t is high, and approach $1 - 0.5/t$ (or 94% for $t = 9$) when the probability of q being 1 is very high.

3. CIRCUIT DESIGN

3.1 Adders and Multiplexors

POR does not use any power-hungry components such as FFM because it consists of simple adders. Figure 4 illustrates one out of

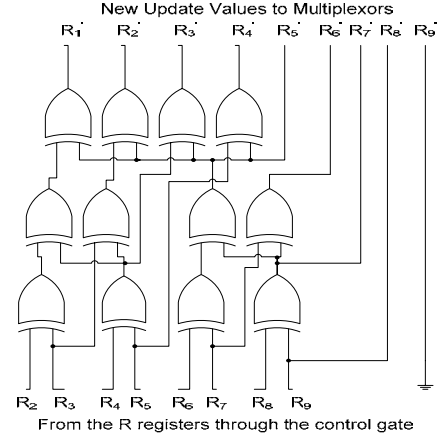


Figure 4. Individual bit of the POR circuitry

8-bits of the adder circuit, which is fed by R_w registers. The inputs of the POR are gated by the enable signal (refer to Figure 1), which is only active for q out of n clock cycle for a given received message. Since q ranges from 1 to t and $n \gg t$, the extra power consumption will be minimal. While the 3-to-1 multiplexors demand more power, reduction in switching at multipliers could bring down switching activities at other parts (such as adders and multiplexors) and hence result in overall power savings.

3.2 Layout Design

To verify the effectiveness of our method, a (255, 187, 9) BCH code was used. Both onventional and proposed Chien search circuits were designed with 0.18 μ m CMOS technology. Synopsys Design Vision and Cadence Encounter were used for synthesis and layout design, respectively. Verilog-XL was used for all gate-level and post-layout simulation with the results to be presented in the next section. As expected, the silicon area increases due to the POR circuitry. Overall core size rises by 24% to 0.041mm² compared to 0.033mm² for the conventional circuit. This also demonstrates the obvious area efficiency of our method over that of the parallel Chien search architecture [3] where the size increases by 106% for a parallel factor of two.

4. SIMULATION RESULTS

MATLAB was used for generating a large number of random input test vectors, which were sent to Device-Under-Tests via Verilog testbench with switching activities being collected for all internal circuit nodes. The power analysis uses Cadence Encounter tool with extracted RC information from the layout for high accuracy.

The power consumption due to different components for both conventional and proposed methods is shown in Tables 1 and 2, respectively. The μ W/MHz values for our proposed circuit are effective values adjusted to include the effect of extra clock cycles mentioned in Section 2.5. The FFMs and registers, which account for 56% of the total power on average, are the most power hungry within the conventional Chien search. Meanwhile, with the equal-probability assumption, their power savings for the proposed method are 60%, compared to a mere 18% estimated by (2) for the method of [5].

Simulated power savings for (255, k, t) BCH codes are plotted in Figure 5 where the top curve represents the power savings of FFMs and registers for BCH codes with different values of t . Its trend generally matches that of (6) in Figure 3. However, at $t = 9$ in particular, the power savings of 60% are still 12% short of the predicted value from (5) and (6) for two reasons: The first is the effect of extra clock cycles, as described in Section 2.5, and the

Table 1. Component power for the conventional circuit

Error-bits (q)	FFMs & Registers ($\mu\text{W}/\text{MHz}$)	MUXs ($\mu\text{W}/\text{MHz}$)	Adders ($\mu\text{W}/\text{MHz}$)	Clock Tree ($\mu\text{W}/\text{MHz}$)
1	3.98	0.14	0.62	2.49
2	4.42	0.38	0.59	2.49
3	4.90	0.62	0.86	2.49
4	5.39	0.87	0.84	2.49
5	5.95	1.14	1.29	2.49
6	6.53	1.48	1.26	2.49
7	7.30	1.85	1.44	2.49
8	7.96	2.20	1.41	2.49
9	8.65	2.59	1.61	2.49

Table 2. Component power for the proposed circuit

Error-bits (q)	FFMs & Registers ($\mu\text{W}/\text{MHz}$)	MUXs & Zero-Detector ($\mu\text{W}/\text{MHz}$)	Adders ($\mu\text{W}/\text{MHz}$)	Clock Tree ($\mu\text{W}/\text{MHz}$)
1	0.51	0.14	0.43	2.42
2	0.95	0.30	0.55	2.53
3	1.39	0.47	0.67	2.64
4	1.85	0.66	0.75	2.76
5	2.39	0.89	0.91	2.88
6	2.94	1.13	1.03	3.00
7	3.48	1.36	1.18	3.11
8	4.04	1.60	1.34	3.22
9	4.67	1.89	1.51	3.34

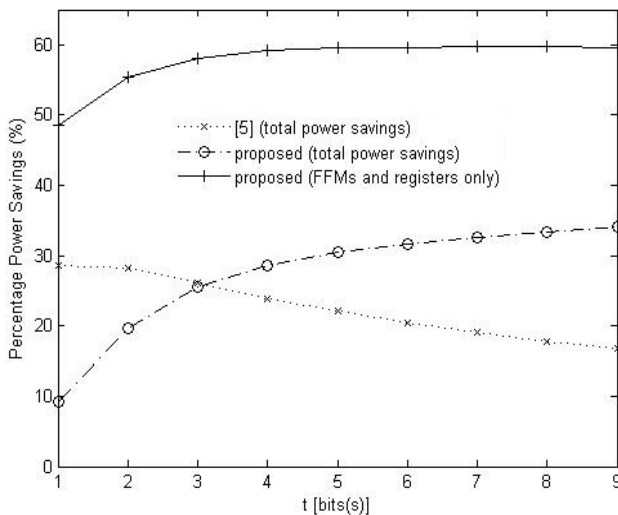


Figure 5. Simulated power savings for (255, k, t) BCH codes

second is the overestimate of the registers' power consumption for the conventional Chien search when they are initially loaded with zero.

Although the method of [5] claims reduction of all power including the clock-tree power by 50% when $t = 1$, the actual power savings would be less because the clock-tree must be kept active for the controlling state machine. Clock gating also causes additional clock-tree power overhead. With these considerations, Figure 5 also shows the overall power savings for different methods over the conventional circuit. It can be seen from the figure that power savings of the proposed circuit exceed that of [5] when t equals four or higher.

5. CONCLUSIONS

We have proposed a new power optimization method for Chien search. The novelty of our approach lies in a power efficient factorization algorithm, which allows fine-grain RT-level power management. Circuits for (255, 187, 9) binary BCH code have been synthesized with 0.18 μm CMOS technology. Simulation shows overall average power savings of 34% at $t = 9$, which double the amount achievable for the method of [5]. Thus, the proposed method is suitable for portable digital video and data storage applications where highly correction-capable BCH codes are used.

6. ACKNOWLEDGMENTS

This work was funded by the AUTO21 Network of Centres of Excellence, Canada.

7. REFERENCES

- [1] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Chapter 6, Prentice Hall, 1983.
- [2] H. Chang, C. Lin and C. Lee, "A low power Reed Solomon decoder for STM-16 optical communications," *Proc. of IEEE Asia-Pacific Conf. on ASIC*, Aug. 2002, pp. 351-354.
- [3] A. Raghupathy and K. J. R. Liu, "Algorithm-based low-power/high-speed Reed-Solomon decoder design," *IEEE Trans. Circuits and Systems-II: Analog and Digital Signal Processing*, vol. 47, no. 11, Nov. 2000, pp. 1254-1270.
- [4] L. Song, M. Yu and M. S. Shaffer, "10- and 40-Gb/s forward error correction devices for optical communications," *IEEE J. of Solid-State Circuits*, vol. 37, no. 11, Nov. 2002, pp. 1565-1573.
- [5] Y. Wu, "Low power decoding of BCH codes," *Proc. of ISCAS 2004*, vol. 2, May 2004, pp. II-369-372.
- [6] R. T. Chien, "Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes," *IEEE Trans. Information Theory*, IT-10, October 1964, pp. 357-363.
- [7] W. P. L. Soon and W. C. Wong, "Robust H.263 portable video coding," *Proc. of Information, Communications and Signal Processing*, September 1997, vol. 1, pp. 306-310.
- [8] W. Liu, J. Rho and W. Sung, "Low-power high-throughput BCH error correction VLSI design for multi-level cell NAND flash memories," *Signal Processing Systems*, Oct. 2006, pp. 303-308.