

Implementation of Euclidean Algorithm Based on Embedded System

黃偉凱、胡大湘

E-mail: 9607573@mail.dyu.edu.tw

ABSTRACT

Based on consideration for data security and confidential communication, information is constantly encoded on transmission. The noise interference and data loss are hardly avoided on transmission. Therefore, dealing with data error and loss is the main goal of error control coding. The simplified Euclidean algorithm of Reed-Solomon codes, which would correct data errors and erasures, is realized with an embedded system in this thesis. In the process of verification, the simplified Euclidean algorithm is firstly down loaded into the embedded system. Then, a friendly interface is made with a computer program of BCB, which provides functions such as display of images and input of image data, random noise interference, and data erasure. After image data have been suffered from interference and erasure artificially, they are passed to the embedded system via RS 232 transmission line. When error and erasure corrections have completed in this embedded system, these image data are sent back and displayed on this BCB interface, which shows differences between these two images. From this verification, this implementation of simplified Euclidean algorithm is successfully achieved

Keywords : RS code ; Euclidean algorithm ; Error control coding ; Embedded system

Table of Contents

封面內頁 簽名頁 授權書	iii	中文摘要	iii
. . . iv 英文摘要	v	誌謝	vi
.	vii	圖目錄	x
.	xii	第一章 緒論 1.1 前言	1
.	2	1.3 全文架構	3
.	3	第二章 Reed-Solomon碼原理	
2.1 有限場	4	2.1.1 群與場	4
.	4	2.1.2 有限場的基	
本運算	7	2.2 里德所羅門碼(Reed-Solomon)定義介紹	7
.	7	2.3 里德所羅門碼(Reed-Solomon)編	
碼演算法則	9	2.3.1 生成多項式	9
.	9	2.3.2 Parity Check Message	10
2.4 里德所羅門碼(Reed-Solomon)解碼演算法則	12	2.4.1 特徵值(Syndrome)	12
.	14	2.4.2.1 Peterson-Gorenstein-Zierler演算法	15
.	19	2.4.2.2 Berlekamp-Massey演算法	19
.	19	2.4.2.3 Euclidean演算法	23
.	29	第三章 簡化程序之歐基里德演算法 3.1 前言	29
.	29	3.2 文獻探討	29
.	30	3.3 解碼過程比較與分析	30
.	30	3.3.1 解碼過程比較	30
.	32	3.3.2 簡化程序演算過程分析	32
.	32	3.4 解碼演算範例	37
.	37	第四章 硬體實現與系統實驗設計 4.1	
Reed-Solomon碼嵌入式控制實現	43	4.2 Reed-Solomon編解碼硬體電路實現與模擬	46
.	43	4.2.1	
Reed-Solomon編碼電路硬體架構	47	4.2.2 Reed-Solomon解碼電路硬體架構	49
.	47	4.2.2.1 Syndrome電	
路硬體架構	50	4.2.2.2 ECU(Euclidean)電路硬體架構	52
.	50	4.2.2.3 Chien Search電路硬體架構	52
.	56	4.2.2.4 Reed-Solomon解碼電路集合模擬	58
.	56	4.3 實驗流程設計與驗證	61
.	61	4.3.1 Borland C++	62
.	61	4.3.2 驗證結果	64
.	61	第五章	
結論及未來展望	69	參考文獻	71

REFERENCES

- [1] Y. SUGIYAMA, M. KASAHARA, S. HIRASAWA, and T. NAMEKAWA, "A method for solving key equation for decoding Goppa codes", *Inf and Contr*, 1975, 27, pp.87-99
- [2] G.D. FORNEY, "On decoding BCH codes", *IEEE Trans On Information Theory*, 1965, IT-11, pp.549-557
- [3] R.E. BLAHUT, "Theory and practice of error control codes", Addison-Wesley Publishing Co, 1984, pp.258
- [4] I.S. REED, T.K. TRUONG, and R.L. MILLER, "Decoding of B.C.H. and RS codes with errors and erasures using continued fractions", *Electron. Lett*, 1979, 15, (17), pp.542-544
- [5] E.P. BERLEKAMP, "Algebraic coding theory", McGraw-Hill, 1968
- [6] E.P. BERLEKAMP, "Bit-serial Reed-Solomon encoders", *IEEE Transactions Information Theory*, 1982, IT-28, (6), pp.869-874
- [7] I.S. HSU, I.S. REED, T.K. TRUONG, and W.L. EASTMAN, "Simplified procedure for correcting both errors and erasures of Reed-Solomon code using Euclidean algorithm", *Int Jnl*,

- pp.318-324 [8] S. Lin and D.J. Costello, Jr, " Error Control Coding ", 2nd edition Prentice Hall, 2004 [9] 謝坤宏, " Design and Implementation of Small-Area Reed-Solomon Decoder ", 交通大學 電信工程學系碩士班碩士論文, 2003 [10] 謝瑋霖, " Reed-Solomon Decoder Hardware Implementation for Digital Video Broadcasting Standard for Terrestrial Transmission(DVB-T) Channel Coding ", 中央大學 通訊工程研究所碩士論文, 2005 [11] G.L. Feng and K.K. Tzeng, " A generalized Euclidean algorithm for multisequence shift-register synthesis ", IEEE Transactions on Information Theory, Vol. 35, Issue 3, pp.584-594, May 1989.
- [12] M. Srinivasan and D.V. Sarwate, " Malfunction in the Peterson-Gorenstein-Zierler decoder ", IEEE Transactions on Information Theory, Vol. 40, Issue 5, pp.1649-1653, Sept. 1994.
- [13] D.J. Jr. Costello, J. Hagenauer, H. Imai and S.B. Wicker, " Applications of error-control coding ", IEEE Transactions on Information Theory, Vol. 44, No. 6, pp.2531-2560, Oct. 1998.
- [14] 張志瑋, " Reed-Solomon Decodc for Digital Communication Systems ", 中正大學 電機工程研究所碩士論文, 2003 [15] I. S. Reed, M. T. Shih, and T. K. Truong, " VLSI Design of Inverse-free Berlekamp-Massey Algorithm ", IEE Proceedings-E, vol. 138, no. 5, pp. 295-298, Sept. 1991.
- [16] W. Wilhelm, " A New Scalable VLSI Architecture for Reed-Solomon Decoder ", IEEE Journal of Solid-State Circuits, vol. 34, pp. 388-396, Mar. 1999.
- [17] R. P. Brent and H. T. Kung, " Systolic VLSI Arrays for Polynomial GCD Computation ", IEEE Transactions on Computers, vol. c-33, no. 8, pp. 731-736, August 1984.
- [18] 劉紹漢、林灶生、劉新民, VHDL晶片設計, 全華科技圖書, 台北, 第7-33頁, 2004。