

有理函數BCH和Reed-Solomon碼之研究

阮仲義、胡大湘

E-mail: 381834@mail.dyu.edu.tw

摘要

由於數位技術的發展，要求數據傳輸和連接效率的人越來越多，用量也隨之提高。通信系統研究和開發服務的進一步要求，不僅在於速度，也重視質量。錯誤更正碼，為提高產品質量信息系統的相關研究領域之一。在這研究中，non-Bose-Chaudhuri-Hocquenghem (BCH)和Reed-Solomon (RS) 基於“有理函數”運作，產生一個新最小距離極大化的碼。這種結合提高BCH上限，在某些時候Hartmann-Tzeng (HT)亦有相同情況。本研究主要目的為基於新的最小距離界線上，提高錯誤校正能力。我們提出修正Berlekamp演算法 (BA) 和歐幾里得演算法 (EA)，並包括執行必要的解碼步驟。

關鍵詞：非BCH碼、RS碼、有理函數、BCH界限、HT界限、Berlekamp演算法、歐幾里得演算法

目錄

中文摘要.....	iii
ABSTRACT.....	iv
TABLE OF CONTENTS.....	v
LIST OF FIGURES.....	vii
LIST OF TABLES.....	viii
Chapter I. Introduction and Motivation.....	1
1.1 Communication System.....	1
1.2 Role of Coding in Communication System.....	3
1.2.1 Channel coding (Error control coding).....	3
1.2.2 Block codes.....	4
1.3 Motivation of Study.....	7
Chapter II. Literatures Review.....	9
2.1 q-ary linear block codes.....	9
2.2 Non-binary BCH Codes.....	10
2.3 Reed-Solomon Codes.....	12
2.3.1 Encoding of Reed-Solomon codes.....	13
2.3.1.1 Non-systematic form.....	13
2.3.1.2 Systematic form.....	14
2.3.2 Decoding of Reed-Solomon Codes.....	17
2.3.2.1 The Berlekamp Algorithm	17
2.3.2.2 The Euclidean Algorithm(EA)	21
2.4 Some concept of bounds on the minimum distance [5].....	22
2.4.1 BCH bound:.....	23
2.4.2 Hartmann-Tzeng (HT) bound:.....	23
2.5 Correction of errors and erasures.....	23
2.6 The “ Ration Functions ” [3],[4] method makes a new bound on the minimum distance.....	27
Chapter III. “ Rational functions ” method applied to Reed-Solomon Codes.....	30
3.1 Reed-Solomon codes with “ Rational functions ” method.....	30
3.2 Decoding of the new method [1], [2], [8].....	34
3.3 Find error evaluation for error and erasure symbols:.....	36
3.4 Correction of errors and erasures with “ Rational functions ” method.....	38
3.5 Decoding with Extended Euclidean Algorithm (EEA).....	39
3.6 Decoding with Berlekamp Algorithm (BA).....	43
Chapter IV. Implement Real Program for Algorithm and Results.....	46
4.1 Introductions.....	46
4.2 Flowchart and implementation.....	46
4.3 Results and comparison.....	48
Chapter V. Conclusion and Future Work.....	55
References.....	56

[1] Shu Lin and Daniel J. Costello Jr, Error Control Coding, Pearson Education, New Jersey, 2004. [2] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968. [3] A. Zeh, A. Wachter, and S. Bezzateev, “ Efficient decoding of some classes of binary cyclic code beyond the Hartmann-Tzeng bound, ” in Information Theory Proceedings (ISIT), 2011 IEEE International Symposium, Aug 2011, pp. 1017-1021. [4] A. Zeh, A. Wachter, and S. Bezzateev, “ Decoding Cyclic Codes up to a New Bound on the Minimum Distance, ” in Information Theory Proceedings (ISIT), 2012 IEEE International Symposium, Mar 2012, pp. 3951-3960. [5] Jacobus H. Van Lint, Richard M. Wilson, “ On the minimum Distance of Cyclic Codes, ” in IEEE transactions on information theory, Vol. IT-32, No.1, Jan 1986, pp.23-40. [6] Gui-Liang Feng and Kenneth K. Tzeng, “ A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes, ” in IEEE transactions on information theory, Vol. 37, No.5, Sep 1991, pp.1274-1287. [7] Nadia Ben Atti, Gema M. Diaz-Toca, and Henri Lombardi, “ The Berlekamp-Massey Algorithm revisited, ” Journal of Applied Algebra in Engineering, Communication and Computing, Vol. 17, Apr 2006, pp. 75-82. [8] Jean Louis Dornstetter, “ On the Equivalence Between Berlekamp’s and Euclid’s Algorithms, ” in IEEE transactions on information theory, Vol. 33, No.3, 1987, pp. 428-431. [9] Ulrich K. Sorger, “ A New Reed-Solomon Code Decoding Algorithm Based on Newton’s Interpolation, ” in IEEE transactions on information theory, Vol. 39, No.2, Mar 1993, pp. 358-365. [10] C. R. P. Hartmann and K. K. Tzeng, “ Decoding Beyond the BCH Bound Using Multiple Sets of Syndrome Sequences, ” in IEEE transactions on information theory, Vol. 20, No.2, Mar 1974, pp. 292-295. [11] G. D. Forney, “ On Decoding BCH Codes, ” in IEEE transactions on information theory, Vol. 11, No.4, Oct 1965, pp. 549-557. [12] J. L. Massey, “ Step-by-Step Decoding of the Bose-Chaudhuri-Hocquenghem codes, ” in IEEE transactions on information theory, Vol. 11, No.4, Oct 1965, pp. 580-585. [13] C. Roos, “ A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, ” Journal of Combinatorial Theory, Series A, Vol. 33, No.2, Sep 1982, pp. 229-232. [14] I. S. Reed and G. Solomon, “ Polynomial Codes over Certain Fields, ” J. Soc. Ind. Appl. Math., No.8, June 1960, pp. 300-304. [15] J. L. Massey, “ Shift-register synthesis and BCH decoding, ” in IEEE transactions on information

theory, Vol. IT-15, No.1, Jan 1969, pp. 122-127. [16]C. R. P. Hartmann and K.K. Tzeng, " Generalization of the BCH bound, " Inform. Contr., Vol. 20, No.5, June 1972, pp. 489-498.

參考文獻

- [1] Shu Lin and Daniel J. Costello Jr, Error Control Coding, Pearson Education, New Jersey, 2004.
- [2] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.
- [3] A. Zeh, A. Wachter, and S. Bezzateev, " Efficient decoding of some classes of binary cyclic code beyond the Hartmann-Tzeng bound, " in Information Theory Proceedings (ISIT), 2011 IEEE International Symposium, Aug 2011, pp. 1017-1021.
- [4] A. Zeh, A. Wachter, and S. Bezzateev, " Decoding Cyclic Codes up to a New Bound on the Minimum Distance, " in Information Theory Proceedings (ISIT), 2012 IEEE International Symposium, Mar 2012, pp. 3951-3960.
- [5] Jacobus H. Van Lint, Richard M. Wilson, " On the minimum Distance of Cyclic Codes, " in IEEE transactions on information theory, Vol. IT-32, No.1, Jan 1986, pp.23-40.
- [6] Gui-Liang Feng and Kenneth K. Tzeng, " A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes, " in IEEE transactions on information theory, Vol. 37, No.5, Sep 1991, pp.1274-1287.
- [7] Nadia Ben Atti, Gema M. Diaz-Toca, and Henri Lombardi, " The Berlekamp-Massey Algorithm revisited, " Journal Applicable Algebra in Engineering, Communication and Computing, Vol. 17, Arp 2006, pp. 75-82.
- [8] Jean Louis Dornstetter, " On the Equivalence Between Berlekamp ' s and Euclid ' s Algorithms, " in IEEE transactions on information theory, Vol. 33, No.3, 1987, pp. 428-431.
- [9] Ulrich K. Sorger, " A New Reed-Solomon Code Decoding Algorithm Based on Newton ' s Interpolation, " in IEEE transactions on information theory, Vol. 39, No.2, Mar 1993, pp. 358-365.
- [10] C. R. P. Hartmann and K.K. Tzeng, " Decoding Beyond the BCH Bound Using Multiple Sets of Syndrome Sequences, " , in IEEE transactions on information theory, Vol. 20, No.2, Mar 1974, pp. 292-295.
- [11] G. D. Forney, " On Decoding BCH Codes, " in IEEE transactions on information theory, Vol. 11, No.4, Oct 1965, pp. 549-557.
- [12] J. L. Massey, " Step-by-Step Decoding of the Bose-Chaudhuri-Hocquenghem codes, " in IEEE transactions on information theory, Vol. 11, No.4, Oct 1965, pp. 580-585.
- [13] C. Roos, " A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, " Journal of Combinatorial Theory, Series A, Vol. 33, No.2, Sep 1982, pp. 229-232.
- [14] I.S. Reed and G. Solomon, " Polynomial Codes over Certain Fields, " J. Soc. Ind. Appl. Math. , No.8, June 1960, pp. 300-304.
- [15] J. L. Massey, " Shift-register synthesis and BCH decoding, " in IEEE transactions on information theory, Vol. IT-15, No.1, Jan 1969, pp. 122-127.
- [16] C. R. P. Hartmann and K.K. Tzeng, " Generalization of the BCH bound, " Inform. Contr., Vol. 20, No.5, June 1972, pp. 489-498.