http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (8): 1758-1760, 2010
ISSN 1812-5638

Constructing Error Correcting Codes for Wireless Sensor Networks

[1]Xiao-Lin Yang, [2]Yu-Mei Chen and [3]Bin Zhou
[1]College of Information Management, Chengdu University of Technology, Chengdu 610059, China
[2]College of Mathematics and Information, China West Normal University, Nanchong, 637009, China
[3]College of Science, Xi'an University of Science and Technology, Xi'an 710054, China

Abstract: Many application scenarios have been revealed with Wireless Sensor Networks (WSNs). An Error Correcting Code (ECC) will be advantageous to communications in these applications. With the different expecting on efficiency, security, usability, etc., different codes have been constructed for various purposes. The methods based on algebra theory can work well for constructing simple and usability codes. The theory of algebraic geometry can help construct more complex codes with different properties. With the applications of these codes, it is convenient to arrive the purpose in digital communications.

Key words: Wireless sensor networks, error correcting code, algebraic geometry, cyclotomic coset, minimal polynomials

INTRODUCTION

The history of Error Correcting Coding (ECC) started with the work Error Detecting and Error Correcting Codes (Hamming, 1950), at or about the same time as the seminal work A mathematical theory of communication (Shannon, 1948). Error correcting codes play an important role in many digital technologies, from modems to cell phones to compact disk players. Recently, with the rapid growth, Wireless Sensor Networks (WSNs) have been brought to many applicable scenarios (Akyildiz *et al*., 2007; Akyildiz *et al*., 2002; Zhou *et al*., 2010; Wei *et al*., 2009, 2010). It is important to construct corresponding error correcting codes. In some scenarios, such as environmental monitoring, the efficiency is more expected while the security is more expected in some other scenarios such as identity verify. More proper error correcting codes will be advantageous to the applications. There are many approaches about error correcting codes in the past years (Momihara and Buratti, 2009; Liu and Yang, 2007).

In practice, almost everyone of the ECCs is linear. Considering the differences in the structure and the processing of information sequences, the codes can be divided into block codes and convolutional codes. Algebra is the important basis in theory. With the algebraic principle, most good properties of the codes can be represented in formulas.

Attributing to the approaches of Hocquenghem, Bose and Ray-Chaudhuri, BCH codes are presented as important cyclic codes. They are simple and easy to be constructed for certain error correcting capability. Also they are easy to be decoded and it is a common code in linear block codes. Reed-Solomon codes are also important and widely applied cyclic codes.

Algebraic geometry codes (Goppa, 1981) came as a result of many years of thinking over the possible generalizations of Reed-Solomon codes, BCH codes and classical Goppa codes. Surprised relation between coding theory and algebraic geometry theory is found and some curves helpful to construct some linear codes over a finite field.

Turbo codes are proposed in the article Near Shannon limit error-correcting coding and decoding: Turbo codes (Berrrou *et al*., 1993) and the shannon bound can be approximated. It has been found that the principle of turbo codes is similar as the Low density pairty check codes, namely, LDPC codes (Gallager, 1962). Turbo codes can be applied in many communications especially the mobile communications or personal communications.

Many nonlinear codes have been discovered such as Nordstrom-Robinson codes, Kerdock codes, Preparata codes, Delsarte-Goethals codes, Goethals codes and so on. Each of these codes holds stronger error correcting capability and has more words than any known linear code. Hammons found that above four codes can be denoted as the ideals of polynomial ring over Z_4. More approaches have been processed on codes over common rings.

FUNDAMENTAL MATHEMATICAL FORMULATIONS

Now we consider the BCH error correcting codes. Supposed that (n, q) = 1, $\beta \epsilon F_{q^m}$ and β is n-th order, integer

Corresponding Author: Bin Zhou, College of Science, Xi'an University of Science and Technology, Xi'an 710054, China

$l>0$, $2\le\delta\le n-1$, then a BCH code with the design distance δ can be denoted as following:

$$C=\{c(x)=\sum_{i=0}^{n-1}c_i x^i\in F_q[x]\,|\,c(\beta^l)=c(\beta^{l+1})=\cdots=c(\beta^{l+\delta-2})\} \quad (1)$$

If the minimal polynomials of β^l, β^{l+1}, ..., $\beta^{l+\delta-2}$ are denoted as $m_0(x)$, $m_1(x)$, ..., $m_{\delta-2}(x)$, then it is easy to be found that the generator polynomial of above code C is the Lowest Common Multiple(LCM) of $m_0(x)$, $m_1(x)$, .., $m_{\delta-2}(x)$. In fact, we can say more about the code C such as the minimal distance $d\ge\delta$. Introducing Euler function and Möbius function, the dual code of C, periodic distributions and the calculating formulas about non-cyclic equivalent classes can be deduced.

Then we look at the Goppa codes. Assumed that $g(z)\in F_{q^m}[z]$, $\alpha_i\in F_{q^m}$ (I = 1, 2, ..., n), $L=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$, $\alpha_i\neq\alpha_j$ $(i\neq j)$, $g(\alpha_i)\neq 0$ (i = 1, 2, ..., n). A classical Goppa code can be defined as following:

$$C=\{(c_1,c_2,\cdots,c_n)\in(F_q)^n\,|\,\sum_{i=1}^{n}\frac{c_i}{z-\alpha_i}\equiv 0 \mod g(z)\} \quad (2)$$

Obviously, the Goppa codes are linear codes. After construct all the reasonable function f(z) with several properties over the Goppa function g(z), a new linear code can be obtained. Moreover these, with the introducing of Reed-Solomon codes, the other algebraic geometry codes can be constructed.

CONSTRUCTING A BCH CODE WITH THE DESIGN DISTANCE 11

Cyclotomic coset plays an important role in the constructing of BCH codes. Assumed that nonnegative integer $s<p^m-1$, $m_s=\min\{r\in Z^+\,|\,p^{r+1}s\equiv s \bmod p^m-1\}$, then the Cyclotmic coset including s modulo p^m-1 can be denoted as:

$$C_s=\{s,ps,p^2s,\cdots,p^{m_s}s\} \quad (3)$$

The least element of C_s means the representative element. The set $\{0, 1, ..., p^m-1\}$ can be divided into several disjoint cyclotomic cosets.

The Euler function and Möbius function can be defined as:

$$\phi(n)=\sum_{d|n}1 \quad (4)$$

and

Table 1: Cyclotomic cosets, minimal polynomials and conjunagte roots

Cyclotomic coset	Conjugate roots	Minimal polynomial
$C_0=\{0\}$	1	$m^{(0)}(x)=x+1$
$C_1=\{1, 2, 4, 8, 16\}$	$\beta, \beta^2, \beta^4, \beta^8, \beta^{16}$	$m^{(1)}(x)=x^5+x^2+1$
$C_3=\{3, 6, 12, 24, 17\}$	$\beta^3, \beta^6, \beta^{12}, \beta^{24}, \beta^{17}$	$m^{(3)}(x)=x^5+x^4+x^3+x^2+1$
$C_5=\{5, 10, 20, 9, 18\}$	$\beta^5, \beta^{10}, \beta^{20}, \beta^9, \beta^{18}$	$m^{(5)}(x)=x^5+x^4+x^2+x+1$
$C_7=\{7, 14, 28, 25, 19\}$	$\beta^7, \beta^{14}, \beta^{28}, \beta^{25}, \beta^{19}$	$m^{(7)}(x)=x^5+x^3+x^2+x+1$

$$u(n)=\begin{cases}1, & n=1,\\ (-1)^k, & n=p_1p_2\cdots p_k\\ 0, & \text{otherwise}\end{cases} \quad (5)$$

where, p_i (i = 1, 2, ..., k) are all primes and $p_i\neq p_j$ $(i\neq j)$.

Based on the Möbius inversion formula, periodic distributions and the calculating formulas about non-cyclic equivalent classes can be proved. The cyclotomic cosets, minimal polynomials and the conjugate roots of binary BCH code (31, 11, $d\ge 11$) are shown in follow Table 1. The primitive polynomial is $p(x)=x^5+x^2+1$.

Table 1 Cyclotomic cosets, minimal polynomials and conjunagte roots.

So, the generator polynomial $g(x)=\text{LCM}\{m^{(1)}, m^{(3)}, m^{(5)}, m^{(7)}\}$ that is:

$$g(x)=x^{20}+x^{18}+x^{17}+x^{13}+x^{10}+x^9+x^7+x^6+x^4+x^2+1 \quad (6)$$

Coding and decoding can be achieved based on the generator polynomial, Berlekamp-Massey algorithm and Chien search algorithm.

Example: The sent code word is 10011111011110100011 10001111011 while the received code word is 10111110011011100001110011111011. It means the received polynomial is:

$$v(x)=x^{30}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{21}+x^{20}+x^{18}+x^{17}+x^{16}+x^{12}+x^{11}+x^{10}+x^7+x^6+x^5+x^4+x^3+x+1 \quad (7)$$

The misplacement polynomial can be obtained after the implementation of Berlekamp-Massey algorithm as following:

$$\delta(x)=1+\beta^{21}x+\beta^{25}x^2+\beta^{15}x^3+\beta^4x^4+\beta x^5 \quad (8)$$

The error polynomial can be obtained after the implementation of Chien search algorithm:

$$\varepsilon(x)=x^{28}+x^{23}+x^{19}+x^{17}+x^7 \quad (9)$$

Then the message polynomial can be computed as:

$$c(x) = v(x) + \varepsilon(x)$$
$$= x^{30} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{19} + x^{18} \quad (10)$$
$$= +x^{16} + x^{12} + x^{11} + x^{10} + x^{6} + x^{5} + x^{4} + x^{3} + x + 1$$

It is the same as the sent code word. Error correcting succeed.

CONCLUSIONS

In this study, we explore the error correcting codes in Wireless Sensor Networks. Algebra theory can work well for constructing simple and usability codes such as BCH codes. The theory of algebraic geometry can help construct more complex codes with different properties. For different purpose of digital communications, it is need to construct different codes. Möbius function Euler function can be used to obtain the periodic distributions and the calculating formulas about non-cyclic equivalent classes. Based on cyclotomic cosets, minimal polynomials and conjugate roots, the coding and decoding process can be completed efficiently as shown in the example. More useful codes can be constructed with the help of algebraic geometry theory such as binary BCH codes (31, 11, $d \leq 11$) shown above. All these codes are advantageous and convenient to be applied in digital communication systems such as Wireless Sensor Networks.

ACKNOWLEDGMENTS

This study is supported by National Natural Science Foundation of China (No. 10926055). The authors would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Akyildiz, I.F., T. Melodia and K.R. Chowdhury, 2007. A survey on wireless multimedia sensor networks. Comput. Networks, 51: 921-960.

Berrrou, C., A. Glavieux and O. Thitimajshima, 1993. Near shannon limit error-correcting coding and decoding: Turbo codes. Proceedings of the IEEE International Conference on Communication, May 23-26, Geneva, Switzerland, pp: 1064-1070.

Gallager, R.G., 1962. Low density parity check codes. IRE Trans. Inform. Theory, 8: 21-28.

Goppa, V.D., 1981. Codes on algebraic curves. Soviet Math. Dokl., 24: 170-172.

Hamming, R.W., 1950. Error detecting and error correcting codes. Bell. Syst. Technical J., 29: 147-160.

Liu, R. and X.L. Yang, 2007. Some conclusions of finite sub-simple groups. J. Southwest Univ. Nationalities, 33: 1294-1296.

Momihara, K.and M. Buratti, 2009. Bounds and constructions of optimal (n, 4, 2, 1) optical orthogonal codes. IEEE Trans. Inform. Theory, 55: 514-523.

Shannon, C.E., 1948. A mathematical theory of communicatio. Bell. Syst. Technical J., 27: 379-423.

Wei, W., X. Wang, B. Zhou, A. Gao and H. Xin, 2009. Diverse-rate based dual energy aware efficiency task scheduling scheme in WSNs. Proceedings of the 1st International Symposium Computer Network Multimedia Technology, December 2009, Wuhan, China, pp: 580-583.

Wei, W., B. Zhou, A. Gao and Y.D. Mei, 2010. A new approximation to information fields in sensornets. Inform. Technol. J., 9: 1415-1420.

Zhou, B., X.L. Yang and W. Wei, 2010. Constructing smoothing information potential fields with partial differential equations. Inform. Technol. J., 9: 1426-1430.