**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **Informative text on BCH Code Construction for Information Reconciliation** | |
| Date Submitted | Jan. 2016 | |
| Source | [[Byung-Jae Kwak, Seong-Soon Joo]1, [Sangseok Yun, Sanghun Im, Jeongseok Ha]2, [Youn-Kwan Kim]3] [] [address] | Voice: [ ] Fax: [ ] E-mail: [bjkwak@etri.re.kr]1,  [ssyun@kaist.ac.kr]2,  [ykkim123@catholic.ac.kr]3 |
| Re: |  | |
| Abstract | Informative text on BCH Code Construction for Information Reconciliation | |
| Purpose | Approval | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

# Annex E

(informative)

**E.1 Design procedure of a primitive *(n,k,t)* BCH code**

* Determine field size *m* where *n = 2m -* 1
* Determine error correction capability *t*
* Find a primitive *n*-th root α of unity in a field GF(2*m*)
* Select 2*t* consecutive powers of α, starting with for some non-negative integer

For uniqueness, , (i.e. narrow sense)

* Let be the least common multiple of the minimal polynomials for the selected powers of with respect to . (Each of the minimal polynomials should appear only once in the product)  
    
  where is the minimal polynomial for .

**E.2 Example of generation of parity bits of BCH Code**

Assume *n=*15 and *t=*2. Then, to generate a narrow sense primitive BCH code with *n=*15 and *t=*2,

1. Find , the root of , i.e. .
2. Select consecutive powers of starting with
3. Calculate . The minimal polynomials for are shown in Table 1. (See E.3 for how to construct minimal polynomials.)

Table —Minimal polynomials for

|  |  |
| --- | --- |
| Power of root, | Minimal polynomial, |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. From Table 1, , since . By substituting and , we have

To obtain the parity bits of BCH coding

1. Multiply the message polynomial by .
2. Divide the result by the generator polynomial .
3. Let be the remainder, then is the parity for .

In case of (15,7,2) BCH code, assuming the message bits are [1 0 1 1 0 1 1],

and since

we have

From , the parity bits are [0 1 1 0 1 1 0 1].

**E.3 Generation of minimal polynomials**

Assume GF(23) = GF(8).

**E.3.1 Cyclotomic coset**

Cyclotomic cosets on are sets for all . Assuming , .

* If , then .
* If , then since in .
* If , then since in .

**E.3.2 Minimal polynomial**

Minimal polynomial for each cyclotomic coset on is defined as

where is the cyclotomic coset on which includes . For example, , the minimal polynomial for each cyclotomic coset is as follows.

* Minimal polynomial for :
* Minimal polynomial for :
* Minimal polynomial for :

Table —Elements of GF(23) with primitive polynomial .

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Since ,  (negative sign is ignored on binary calculation).  From , ,,since 2 equals to 0 on binary calculation | |