

PREPARING OF CALCULATIONS IN GF(Q) OF ORDER TWO EXTENSIONS FOR BCH-CODE

V Poltorak

*Dept of Automatics & Control in Technical Systems, Faculty of Informatics and Computing Technique, National Technical University of Ukraine "Kyiv Polytechnic Institute", Ph D, 37, Prospect Peremogy, 03056, Kyiv-56, Ukraine,
Email: poltorak@acts.kiev.ua*

ABSTRACT

It is known a renewal of interest to cyclic Error Correcting Codes for some engineering branches at resent years. It is true for those branches where we can not accept Error Detection only and wait for an Error Correcting by means of data retransmitting. We should to correct errors in real-time data flow. In some of such engineering branches BCH-codes are used. For example, that is true at a real-time video-conferencing over packet-switched networks.

The paper objectives are to find a set of parameters for BCH-code and look for conditions of its implementation, which allow getting a code redundancy minimization. An analysis of boundaries for minimal code distance and generating polynomial roots structure examination were used. It was find that code locators field as order two extensions for code elements field can impart the property desirable.

Keywords: cyclic code, error correcting, BCH-code, code redundancy, minimal code distance, generating polynomial, roots structure, Galois field

1 INTRODUCTION

There are some data transmission tasks where we should to correct errors in real-time data flow. In some of such cases cyclic BCH-codes are used [1].

From the other hand, a general definition of the BCH-code not guarantee a code redundancy $D = r/n$ minimization, where n is code length and $r = 2mt$ is a number of code redundant elements, t is a number of errors corrected per code block, m is an order of GF(q) extension up to GF(q^m), $q = p^l$ is a code base (an integer power l of prime number p), GF(q) is Galois Field of q cardinal number [2]. We should to look for a certain code parameter sets for the code redundancy D minimization. It is well known now, that increasing of q lead to the code redundancy reducing even if a short code length n . That is why we are interested in non binary BCH-codes (with base $q > 2$). GF(q) is known as field of code elements and GF(q^m) – as field of locators.

It was found, in special case when $m = 2$, a set of roots of code generating polynomial $g(x)$ can be choose in a such way, that we get a value of $r = 2t$, even if an $m = 2$ (a general BCH-code theory promise such possibility, but not show the way to get the result). And we get a value of $D = 2t/n$ - the least value from existing for BCH-code. That fact open attractive perspective in BCH-code using, thanks to D minimization.

Decoding procedure needs of calculations over GF(q^m). It is much more complex, then calculations over GF(q). In special case, presented above, at $m = 2$, a possibility to reduce a calculations complexity over GF(q^2) was obtained, thanks to a special form of GF(q^2) elements presentation and taking to consideration of their connection with GF(q) elements.

2 PLACE OF BCH-CODE IN DATA TRANSMISSION SYSTEM

The BCH-code role and place in Data Transmission System (DTS) are defined by set of goals to be achieved. Main tasks of BCH-code used in DTS are to detect and correct errors during data transmission over the channel. No obvious tasks are bandwidth and energy cost per unit reducing, what leads to bit rate (or transmission distance) increasing from the other hand.

Well-known generic one-directional DTS structure is presented on Figure 1, where BCH-code is implemented in the Channel codec layer (between B and C separating surfaces).

One can single out two models of BCH-code. First is typical wide used binary code with base $q = 2$. Second is no binary code with base $q > 2$.

In the second case all data procedures and devices left side from B separating surface on Figure 1 may stay binary ones. While at the right side from B, at least the Channel codec layer should be no binary one.

Modem may stay both binary and no binary one. This has an effect on effectiveness of Shared Transmission Media utilization.

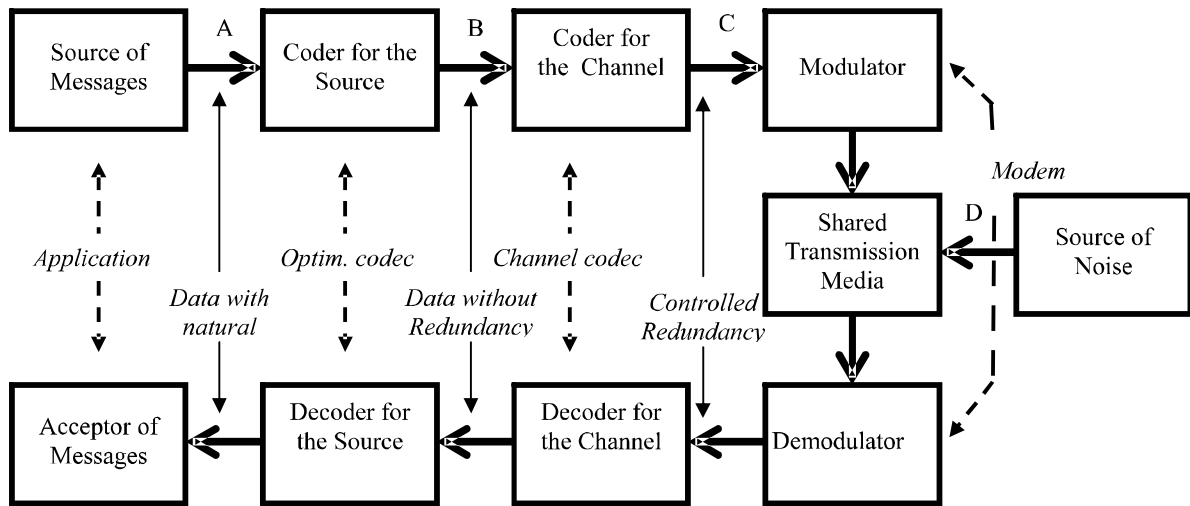


Figure 1. Generic structure of one-directional Data Transmission System

3 REDUNDANT CODE EFFECTIVENESS

The total redundant code effectiveness is illustrated on Figure 2 and Figure 3 by means of R-factor in relation to $(d/2n)$ - factor. Where $R=k/n$ is relative code speed, $k = n-r$. $(d/2n)$ - factor is relative portion of correctable errors on the code block length n . Value d is minimal Hamming code distance.

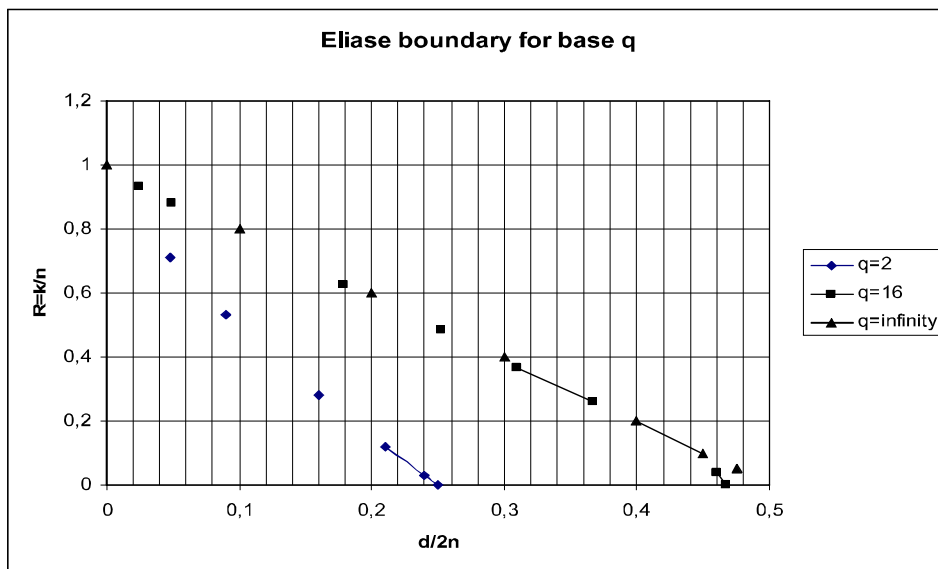


Figure 2. Elias upper code distance boundary for base q

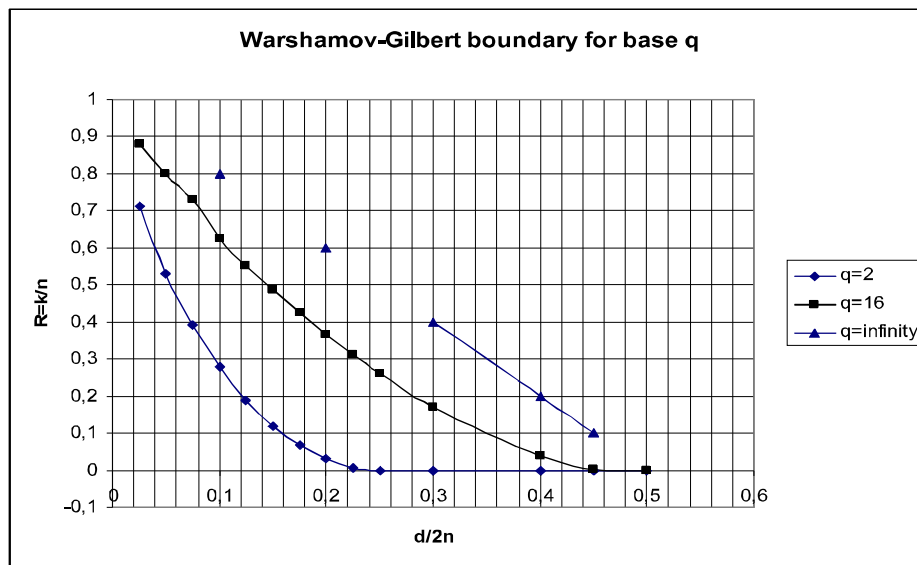


Figure 3. Warshamov-Gilbert bottom code distance boundary for base q

Both Figure 2 and Figure 3 show redundant code effectiveness R increase depend on base q rising. That is why no binary BCH-code with base $q > 2$ is of great importance for generation of effective real-time Data Transmission Systems, for example, packet-switched videoconferencing.

4 SPECIFICITY OF ROOT STRUCTURE OF BCH-CODE

It follows from the general BCH-code definition, that one must choose a minimum number $r = 2t$ of redundant code elements per code block. And one must choose the same number r of minimal polynomials $m_i(x)$ to create a generating BCH-code polynomial $g(x)$, to guarantee error correcting of weight t . From the other hand, each from all of r roots of $g(x)$ has $(m-1)$ conjugate algebraic numbers belong to $GF(q^m)$. Their total number is m per $m_i(x)$. So, total value of r may be find as $2t \leq r \leq 2mt$.

4.1 Spectrum of BCH-code roots

General requirements to the r BCH-code roots are those, that they should be chosen in series one by one, and must be of minimal polynomials $m_i(x)$ roots (m per $m_i(x)$). In closed set of $GF(q^m)$, this situation may be illustrated by next Figure 4.

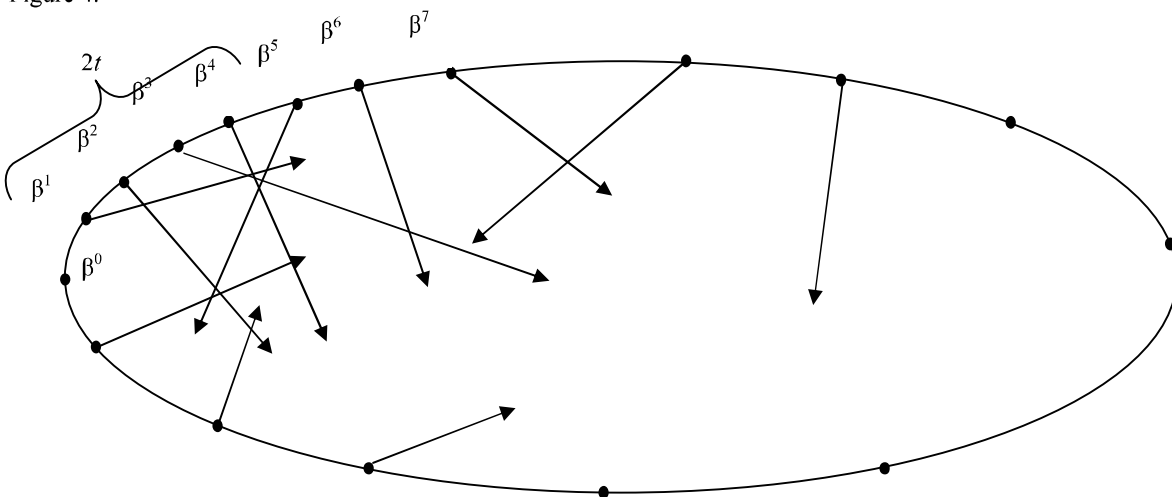


Figure 4. Closed set of $GF(q^m)$ elements (the source of $m_i(x)$ and $g(x)$ roots).

The bracket on Figure 4 associates a set of serial (one by one) $g(x)$ roots, each has $(m-1)$ another conjugate elements belong to $GF(q^m)$, arranged in some sort of their own order.

4.2 Ordered Spectrum of BCH-code roots

Detailed analysis of the BCH-code roots spectrum leads us to finding a set of parameters $GF(q)$ and $GF(q^m)$, which gives to us an ordered spectrum of BCH-code roots for $g(x)$. A next Figure 5 illustrates that situation.

The bracket on Figure 5 associates a set of $2t$ serial (one by one) $g(x)$ roots, each has $(m-1)$ another conjugate elements belong to $GF(q^m)$, but situated at the same set of roots. That $GF(q^m)$ elements are arranged in such sort of order, when all of them are “co- m ”-conjugated and compose just $r = 2t$ roots of $g(x)$. Those parameters are: $GF(q)$ and $GF(q^m)$, where $m = 2$; $n = q + 1$. And root spectrum is: $\beta^{((n-1)/2-t)}$ up to $\beta^{((n-1)/2+t)}$.

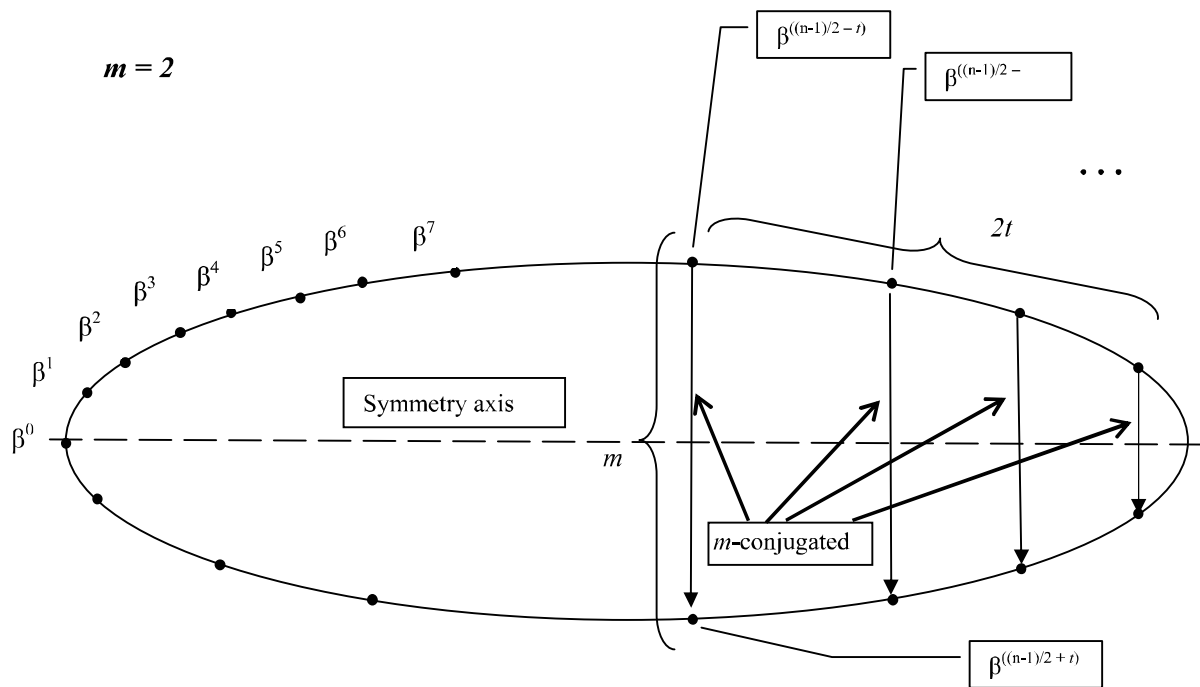


Figure 5. An ordered spectrum of BCH-code roots for $g(x)$.

5 CONCLUSION

There is an important problem in data transmission systems with real-time data flowing, such as different radio systems or a real-time video-conferencing over packet-switched networks.

There we can't wait for retransmitting result; we should to correct errors in real-time mode. But using of error correcting code causes some value of redundancy. This work examines a set of parameters for BCH-code and look for conditions of its implementation, which allow getting a code redundancy minimization up to value of $D = 2t/n$. It was find that code locators field as order two extensions for code elements field can impart the property desirable.

6 REFERENCES

Lin S. & Costello D. (2004) Error Control Coding: Fundamentals and Applications, NJ, USA: Prentice-Hall, Englewood Cliffs.

(2008). Finite field. From Wikipedia, the free encyclopedia. Retrieved June 10, 2008 from the World Wide Web:

http://en.wikipedia.org/wiki/Finite_field