ITU Telecommunication Standardization Sector
Study Group 15
Experts Group for Video Coding and Systems
in ATM and Other Network Environments

Document AVC-765
May 1995

Source : JAPAN
Title : Binary Primitive Polynomial and Generator Polynomial of Reed-Solomon Code
Purpose : Information

----

1. Introduction

In the Kamifukuoka meeting, the use of FEC for bit errors was clarified that its use is mandatory in the case of H.310 terminal types A2 and B2, and the choice of polynomials was raised as one of the working items [1]. The binary primitive polynomial and the generator polynomial of Reed-Solomon (RS) code are as important factors as its code length to decide the hardware logic. The purpose of this document is to give information to choice those polynomials.

2. Binary primitive polynomial

There are eight kinds of binary primitive polynomials on the Galois Extension Field $GF(2^8)$. Each binary primitive polynomial has also a reciprocal polynomial. Therefore, counting those reciprocal polynomials, the number of binary primitive polynomials becomes 16 as follows :

$$P(X) = X^8+X^4+X^3+X^2+1 \ , \tag{1}$$
$$P(X) = X^8+X^6+X^5+X^4+1 \ , \tag{2}$$
$$P(X) = X^8+X^5+X^3+X^2+1 \ , \tag{3}$$
$$P(X) = X^8+X^6+X^5+X^3+1 \ , \tag{4}$$
$$P(X) = X^8+X^7+X^6+X^5+X^2+X+1 \ , \tag{5}$$
$$P(X) = X^8+X^7+X^6+X^3+X^2+X+1 \ , \tag{6}$$
$$P(X) = X^8+X^5+X^3+X+1 \ , \tag{7}$$
$$P(X) = X^8+X^7+X^5+X^3+1 \ , \tag{8}$$
$$P(X) = X^8+X^6+X^5+X^2+1 \ , \tag{9}$$
$$P(X) = X^8+X^6+X^3+X^2+1 \ , \tag{10}$$
$$P(X) = X^8+X^7+X^3+X^2+1 \ , \tag{11}$$
$$P(X) = X^8+X^6+X^5+X+1 \ , \tag{12}$$
$$P(X) = X^8+X^6+X^4+X^3+X^2+X+1 \ , \tag{13}$$
$$P(X) = X^8+X^7+X^6+X^5+X^4+X^2+1 \ , \tag{14}$$
$$P(X) = X^8+X^7+X^2+X+1 \ , \tag{15}$$
$$P(X) = X^8+X^7+X^6+X+1 \ . \tag{16}$$

For above equations, the reciprocal equation of odd-numbered equation is the next even-numbered equation, respectively. The hardware complexity is almost independent of those binary primitive polynomials. Though the equation (4) is reported to be the optimal one reducing the hardware complexity, the difference of each number of gates between those binary primitive polynomials is less than several 10 gates.

3. Generator polynomial

In general, a generator polynomial $G(X)$ is given as follow :

$$G(X) = \prod_{j=\gamma}^{\gamma+R} (X-\alpha^{\lambda j}) , \qquad (17)$$

R : number of check symbols – 1,

α : a root of the binary primitive polynomial,

λ : 1 or any value of relatively prime with 255.

The error correction performance of RS code is decided by R and its code length (i.e., FEC frame length). Usually, γ is set to 0 and λ is set to 1. The hardware complexity of RS encoding/decoding process depends on the generator polynomial. If R or code length becomes large, the hardware complexity will increase.

4. Applications

The equations (1), (3) and (15) are well-known as the binary primitive polynomials actually in use for some applications. Table 1 shows the binary primitive polynomials and the generator polynomials of RS codes for some applications.

4.1 Binary primitive polynomial : $P(X) = X^8+X^4+X^3+X^2+1$ ...... (1)

This binary primitive polynomial is widely used in the audiovisual applications such as compact disc, DAT, digital VTR and so on. ITU-T Recommendation J.81 (former CCIR Rec. 723) and DVB project in Europe also adopt this polynomial. The generator polynomial is usually given as follow :

$$G(X) = \prod_{j=0}^{R} (X-\alpha^{j}) . \qquad (18)$$

4.2 Binary primitive polynomial : $P(X) = X^8+X^5+X^3+X^2+1$ ...... (3)

This binary primitive polynomial is used in the optical disc. The generator polynomial is given by :

$$G(X) = \prod_{j=120}^{135} (X-\alpha^{88j}) . \qquad (19)$$

4.3 Binary primitive polynomial : $P(X) = X^8+X^7+X^2+X+1$ ...... (15)

This binary primitive polynomial was recommended by the CCSDS (Consultative Committee for Space Data Systems) for the telemetry channel. The generator polynomial is given by :

$$G(X) = \prod_{j=112}^{143} (X-\alpha^{11j}) . \qquad (20)$$

The error correction methods recommended in the ITU-T draft recommendation I.363.X, i.e., the long interleave method and the short interleave method, adopt this binary primitive polynomial, respectively. The generator polynomial of the long interleave method is :

$$G(X) = \prod_{j=120}^{123} (X-\alpha^j) . \qquad (21)$$

The generator polynomial of the short interleave method is :

$$G(X) = \prod_{j=120}^{125} (X-\alpha^j) . \qquad (22)$$

4.4 Others

The binary primitive equation recommended by the ESA (European Space Agency) for the telemetry channel is given by equation (13) and its generator polynomial is given by equation (20).

5. Conclusion

The binary primitive polynomial and the generator polynomials of RS codes are summarized from the aspects of applications and standardization. The hardware complexity of RS encoding/decoding process is independent of the binary primitive polynomial. It mostly depends on the generator polynomial. To choice a binary primitive polynomial for H.310 terminal, the 'application' in Table 1 will be an important factor to be considered. The equation (1) and(15) will be adequate alternatives.

Reference

[1] §6.7.1/AVC-743R "REPORT OF THE EIGHTEENTH EXPERTS GROUP MEETING IN KAMIFUKUOKA (24-27 January 1995) (Rapporteur)", January 1995.

Table 1 Examples of binary primitive polynomials and generator polynomials of RS codes

Binary primitive polynomial	Application	RS code	Generator polynomial
$P(X) = X^8+X^4+X^3+X^2+1$	Compact Disc	C1 code RS (32, 28)	$G(X) = \prod_{j=0}^{3} (X-\alpha^j)$
		C2 code RS (28, 24)	$G(X) = \prod_{j=0}^{3} (X-\alpha^j)$
	D-1 DVTR	Inner code RS (64, 60)	$G(X) = \prod_{j=0}^{3} (X-\alpha^j)$
		Outer code RS (32, 30)	$G(X) = \prod_{j=0}^{1} (X-\alpha^j)$
	D-2 DVTR	Inner Code RS (95, 87) , RS (93, 85)	$G(X) = \prod_{j=0}^{7} (X-\alpha^j)$
		Outer Code RS (68, 64)	$G(X) = \prod_{j=0}^{3} (X-\alpha^j)$
	ITU-T Rec. J.81 (CCIR Rec. 723)	RS (255, 239)	$G(X) = \prod_{j=0}^{15} (X-\alpha^j)$
	DVB-S (outer code), DVB-C	RS (204, 188)	$G(X) = \prod_{j=0}^{15} (X-\alpha^j)$
	ATV (outer code)	RS (207, 187)	$G(X) = \prod_{j=0}^{19} (X-\alpha^j)$
$P(X) = X^8+X^5+X^3+X^2+1$	Optical disc	RS (120, 104)	$G(X) = \prod_{j=120}^{135} (X-\alpha^{88j})$
$P(X) = X^8+X^7+X^2+X+1$	ITU-T Rec. I.363.X	Long interleave RS (128, 124)	$G(X) = \prod_{j=120}^{123} (X-\alpha^j)$
		Short interleave RS (94, 88)	$G(X) = \prod_{j=120}^{125} (X-\alpha^j)$
	Telemetry channel (CCSDS)	RS (255, 223)	$G(X) = \prod_{j=112}^{143} (X-\alpha^{11j})$
$P(X) = X^8+X^6+X^4+X^3+X^2+X+1$	Telemetry channel (ESA)	RS (255, 223)	$G(X) = \prod_{j=112}^{143} (X-\alpha^{11j})$

END