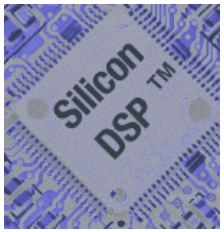
Introduction to Reed Solomon Coding



Silicon DSP Corporation

History

- Invented in 1958 by Reed and Solomon MIT Lincoln Labs.
- Modified and Published in SIAM 1960.
- Breakthrough in decoding in 1967 by E. Berlekamp
- Berlekamp-Massey Algorithm $O(n^2)$
- Earliest use by military one-byte error-correction code in deep-space telecom about 1970.
- Voyager II used 255-byte and 223-byte RS Code 1977 corrected 16 byte-errors.

Abelian Group, Ring, Field

Can’t do justice. See Blahut and Books on Modern Algebra.

“Loosely speaking, an abelian group is a set in which one can add and subtract, and a ring is a set in which one can add, subtract, and multiply. A more powerful algebraic structure, known as a field, is a set in which one can add, subtract, multiply, and divide." p27, Blahut

Examples of well known fields:

- The set of real numbers.
- The set of complex numbers.
- The set of rational numbers.

These have an infinite number of elements.

Richard E. Blahut, “Theory and Practice of Error Control Codes,”Addison-Wesley Publishing Company, 1983

A field with q elements, if it exists, is called a *finite field* , or a *Galois Field,* and is denoted by the label $GF(q)$.

GF(3)= {0,1,2}

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

If we can find a prime polynomial of degree *n* over *GF(q)* then a Galois field with q^n elements can be constructed.

Example build *GF(4)* or *GF(2^2)* from *GF(2)* using the prime polynomial $p(x)=x^2+x+1$.

Representations of *GF(4)*

Polynomial Notation	Binary Notation	Integer Notation	Exponential Notation
0	00	0	0
1	01	1	x^0
x	10	2	x^1
x+1	11	3	x^2

$p(x)=x^2+x+1$

Definition: A primitive field element of $GF(q)$ is a an element α such that every field element except zero can be expresed as a power of α.

Example $2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$

$$\alpha^1, \alpha^2, \alpha^3, \alpha^4$$

$\alpha = 2$ is a primitive element in $GF(5)$.

Table 4.1 Prime polynomials over *GF*(2).

Degree	Primitive Polynomials
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x^3 + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^6 + x^4 + x + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^{10} + x^6 + x + 1$
15	$x^{15} + x + 1$
16	$x^{16} + x^{12} + x^3 + x + 1$
17	$x^{17} + x^3 + 1$
18	$x^{18} + x^7 + 1$
19	$x^{19} + x^5 + x^2 + x + 1$
20	$x^{20} + x^3 + 1$
21	$x^{21} + x^2 + 1$
22	$x^{22} + x + 1$
23	$x^{23} + x^5 + 1$
24	$x^{24} + x^7 + x^2 + x + 1$
25	$x^{25} + x^3 + 1$
26	$x^{26} + x^6 + x^2 + x + 1$
27	$x^{27} + x^5 + x^2 + x + 1$
28	$x^{28} + x^3 + 1$

Note: All entries are primitive polynomials.

Blahut, 1983

Polynomial Encoding and Decoding

Example:

Let $g(x)=x^3+x+1$ and $n=7$. Then $k=7-3=4$. Let $m(x)=x^2+1$ be the message polynomial corresponding to the word $m=0101$. The message $m(x)$ is encoded as

$c(x)=m(x)g(x)$,

so

$c(x)=(x^2+1)(x^3+x+1)=x^5+x^2+x+1$

With $c= 0100111$ as the corresponding codeword.

From: Coding Theory: The Essentials, Hoffman, et. Al., Marcel Dekker, New York, 1991, *Changed MSB*

$$GF(8) = GF(2^3)$$

$$p(x) = x^3 + x + 1$$

word	$x^i \bmod p(x)$
001	1
010	x
100	x^2
011	$x^3 \equiv x+1$
110	$x^4 \equiv x^2+x$
111	$x^5 \equiv x^2+x+1$
101	$x^6 \equiv x^2+1$

Multiplication:

$$(011)(100) \longleftrightarrow (x+1)x^2$$

$$(x^2)(x+1) \equiv x^2 \bullet x^3$$
$$\equiv x^5$$
$$\equiv x^2 + x + 1 (\text{mod } p(x))$$

$$(011)(100) = 111$$

$$GF(8) = GF(2^3)$$

α	z
α^2	z^2
α^3	$z+1$
α^4	z^2+z
α^5	z^2+z+1
α^6	z^2+1

$$\alpha^7 = \alpha^0 = 1$$

$$p(z) = z^3 + z + 1$$

Generator Polynomial for Reed Solomon Codes

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1}) \cdots (x - \alpha^{j_0+2t-1})$$

For $GF(8) = GF(2^3)$

Elements are octal numbers.

n=7,t=2

then

k=n-2t=7-4=3

Example Let $j_0 = 4$ and $t = 2$

$$g(x) = (x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^0)$$

$$\begin{aligned} g(x) = x^4 &- (\alpha^0 + \alpha^6 + \alpha^5 + \alpha^4)x^3 + \\ &[\alpha^6 + \alpha^9 + (\alpha^5 + \alpha^4)(\alpha^0 + \alpha^6)]x^2 - \\ &[\alpha^6(\alpha^5 + \alpha^4) + \alpha^9(\alpha^0 + \alpha^6)]x + \alpha^{15} \end{aligned}$$

For x^0 coefficient:

$$\alpha^{15} = \alpha^7 \alpha^7 \alpha = z$$

For x coefficient:

$$(\alpha^5 + \alpha^4)\alpha^6 + (\alpha^0 + \alpha^6)\alpha^9$$

$$\alpha^6(\alpha^5 + \alpha^4 + \alpha^3 + \alpha^9)$$

$$\alpha^6(z^2 + z + 1 + z^2 + z + z + 1 + z^2)$$

$$\alpha^6(z + z^2) = \alpha^6\alpha^4 = \alpha^{10} = \alpha^3 = z + 1$$

For x^2 coefficient:

$$\alpha^6 + \alpha^9 + (\alpha^5 + \alpha^4)(\alpha^0 + \alpha^6) = \alpha^6 + \alpha^9 + \alpha^5 + \alpha^{11} + \alpha^4 + \alpha^{10}$$

$$= \alpha^4(\alpha^2 + \alpha^5 + +\alpha + \alpha^7 + 1 + \alpha^6)$$

$$= \alpha^4(z^2 + z^2 + z + 1 + z + 1 + 1 + z^2 + 1)$$

$$= \alpha^4(z^2) = \alpha^4\alpha^2 = \alpha^6 = z^2 + 1$$

For x^3 coefficient:

$$\alpha^0 + \alpha^6 + \alpha^5 + \alpha^4 = 1 + z^2 + 1 + z^2 + z + 1 + z^2 + z = 1 + z^2$$

$$g(x) = x^4 + (z^2+1)x^3 + (z^2+1)x^2 + (z+1)x + z$$

$$g(x) = x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha$$

The field elements of $GF(8)$ are expressed as polynomials in z.

Information polynomial is a sequence of three octal (8-ary) symbols (equivalent to nine bits).

Let,

$$i(x) = (z^2 + z)x^2 + x + (z + 1)$$

This corresponds to $(110, 001, 011)$ or $(6_8, 1_8, 3_8)$

$$i(x) = \alpha^4 x^2 + x + \alpha^3$$

Then the nonsystematic codeword $c(x)$

is generated using the generator polynomial $g(x)$

$$c(x) = i(x)g(x)$$

$$= (\alpha^4 x^2 + x + \alpha^3)(x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha)$$

$$= \alpha^4 x^6 + \alpha x^5 + \alpha^6 x^4 + 0x^3 + 0x^2 + \alpha^5 x + \alpha^4$$

Which is the sequence $(110, 010, 101, 000, 000, 111, 110)$ or

$$6, 2, 5, 0, 0, 7, 6$$

Message was $6, 1, 3$

n=7,k=3 , t=2

$$GF(8) = GF(2^3)$$

α	z
α^2	z^2
α^3	$z+1$
α^4	z^2+z
α^5	z^2+z+1
α^6	z^2+1

$$\alpha^7 = \alpha^0 = 1$$

$$p(z) = z^3 + z + 1$$

Correcting Errors

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1}) \cdots (x - \alpha^{j_0+2t-1})$$

Let the zeroes of $g(x)$ be denoted as $\gamma_1, \cdots, \gamma_r$. Then,

$$g(\gamma_j) = 0 \quad j = 1, \cdots, r$$

Let $c(x)$ be a codeword polynomial.

Let $e(x)$ be an error polynomial.

The received polynomial is

$$v(x) = c(x) + e(x)$$

Evaluate the received polynomial with the roots of $g(x)$.

$$v(\gamma_j) = c(\gamma_j) + e(\gamma_j)$$

$$v(\gamma_j) = e(\gamma_j) \qquad j = 1, \cdots, r$$

Hence,

$$v(\gamma_j) = \sum_{i=0}^{n-1} e_i \gamma_j^i \qquad j = 1, \cdots, r$$

If this set of equations can be solved for e_i, then the error pattern can be determined.

$$e(x) = e_{j_1} x^{j_1} + e_{j_2} x^{j_2} + \cdots + e_{j_v} x^{j_v}$$

Error locations are $j_1, j_2, \cdot, j_v$ and values $e_{j_1}, e_{j_2}, \cdot, e_{j_v}$ both unknown.

$$Y_l = e_{j_l} \quad \text{for } l = 1, 2, \cdots, v$$

$$X_l = \gamma_j^l \quad \text{for } l = 1, 2, \cdots, v$$

$$S_j = Y_1 X_1^j + Y_2 X_2^j + \cdots + Y_v X_v^j \quad \text{for } j = 1, 2, \cdots, r$$

where

$$S_j = v(\gamma_j) \quad \text{for } j = 1, 2, \cdots, r$$

Simultaneous Nonlinear Equations

Number of errors v

Solution is unique if $0 \leq v \leq t$

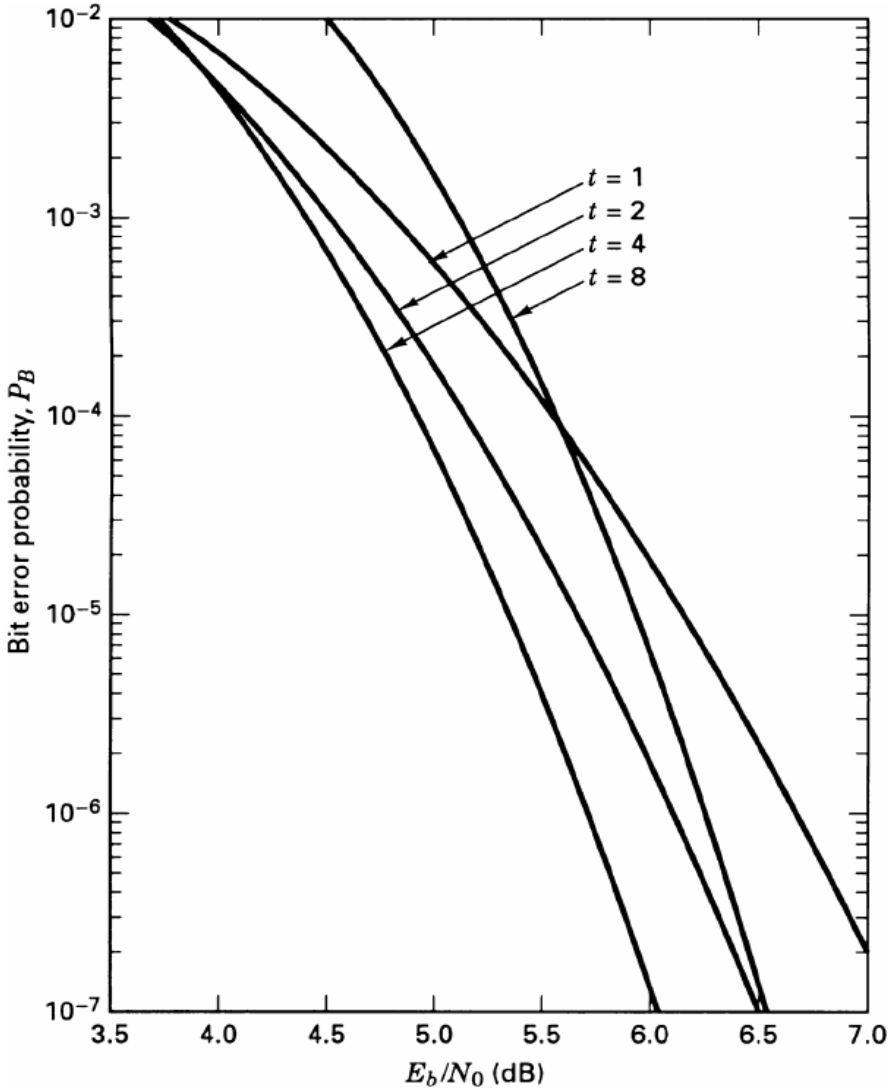
$Y_l = e_{j_l}$ for $l = 1, 2, \cdots, v$ v Unknown Error Values.

$X_l = \gamma_j^l$ for $l = 1, 2, \cdots, v$ v Unknown Error Locations.

Note that $r = 2t$.

$2t$ Equations.

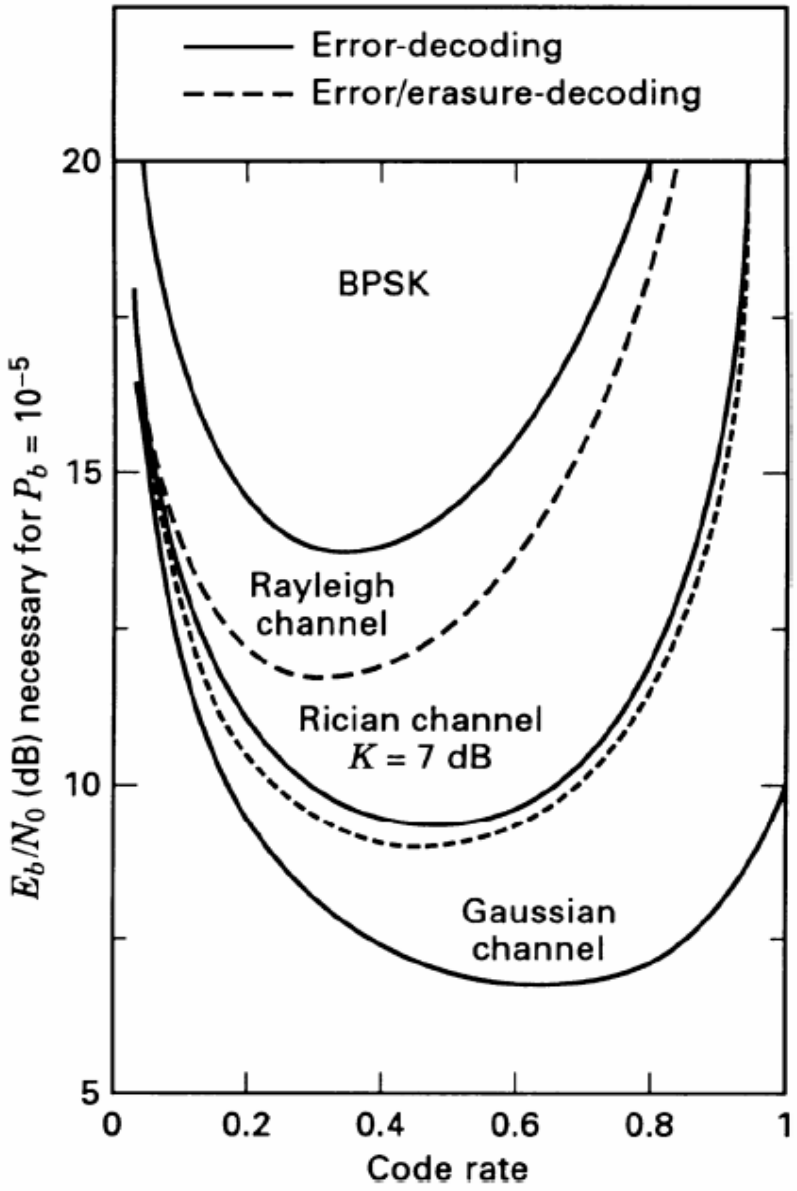
$$S_j = Y_1 X_1^j + Y_2 X_2^j + \cdots + Y_v X_v^j \quad \text{for } j = 1, 2, \cdots, r$$



32-ary MFSK modulation over an AWGN channel

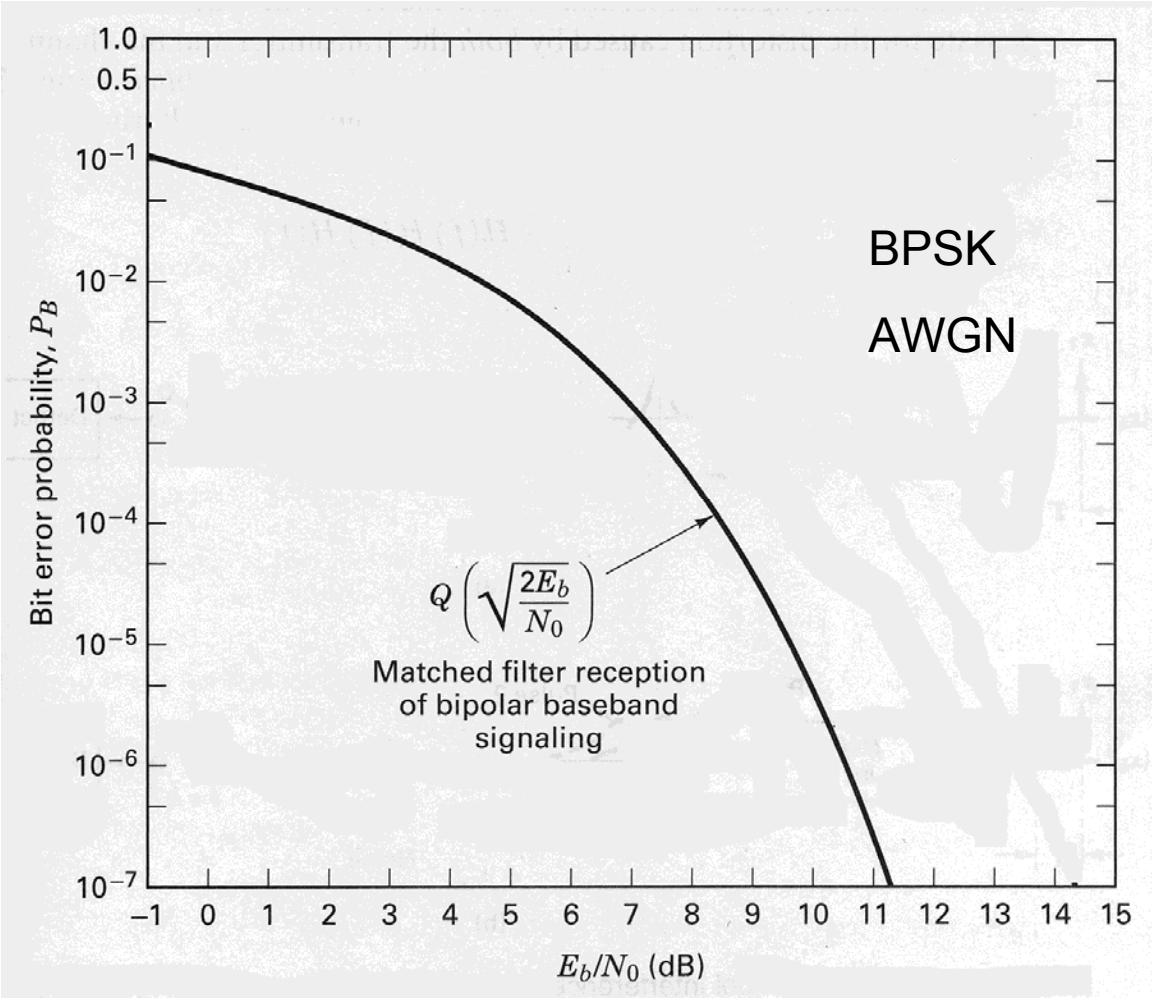
Odenwalder, J. P., *Error Control Coding Handbook*, Linkabit Corporation, San Diego, CA, July 15, 1976.

Reed-Solomon Codes,Bernard Sklar, www.phptr.com Also see Sklar, *Digital Communications: Fundamentals and Applications, Second Edition* (Prentice-Hall, 2001).



BPSK plus Reed-Solomon (31, *k*) decoder performance as a function of code rate.

Reed-Solomon Codes, Bernard Sklar, www.phptr.com Also see Sklar, *Digital Communications: Fundamentals and Applications, Second Edition* (Prentice-Hall, 2001).



Source:

Bernard Sklar, Digital Communications, Prentice Hall, 2001

For Architecture and Implementations for RS Coders and Decoders including VLSI issues see:

Irvine S. Reed, Xuemin Chen, **Error-Control Coding for Data Networks**, Kluwer Academic Publishers, 1999, Second Printing 2001.

Also worked examples.