Equalization, Diversity, and Channel Coding

- Introduction
- Equalization Techniques
- Algorithms for Adaptive Equalization
- Diversity Techniques
- RAKE Receiver
- Channel Coding

Introduction[1]

- Three techniques are used independently or in tandem to improve receiver signal quality
- *Equalization* compensates for ISI created by multipath with time dispersive channels ($W>B_C$)
  - ➢Linear equalization, nonlinear equalization
- *Diversity* also compensates for fading channel impairments, and is usually implemented by using two or more receiving antennas
  - ➢Spatial diversity, antenna polarization diversity, frequency diversity, time diversity

Introduction[1]

- The former counters the effects of time dispersion (ISI), while the latter reduces the depth and duration of the fades experienced by a receiver in a flat fading (narrowband) channel
- *Channel Coding* improves mobile communication link performance by adding redundant data bits in the transmitted message
- Channel coding is used by the Rx to detect or correct some (or all) of the errors introduced by the channel (Post detection technique)

➢Block code and convolutional code

Equalization Techniques

- The term *equalization* can be used to describe any signal processing operation that minimizes ISI [2]
- Two operation modes for an adaptive equalizer: training and tracking
- Three factors affect the time spanning over which an equalizer converges: equalizer algorithm, equalizer structure and time rate of change of the multipath radio channel
- TDMA wireless systems are particularly well suited for equalizers

Equalization Techniques

- Equalizer is usually implemented at baseband or at IF in a receiver (see Fig. 1)

$$y(t) = x(t) * f^*(t) + n_b(t)$$

$f^*(t)$: complex conjugate of $f(t)$

$n_b(t)$: baseband noise at the input of the equalizer

$h_{eq}(t)$: impulse response of the equalizer

Equalization Techniques

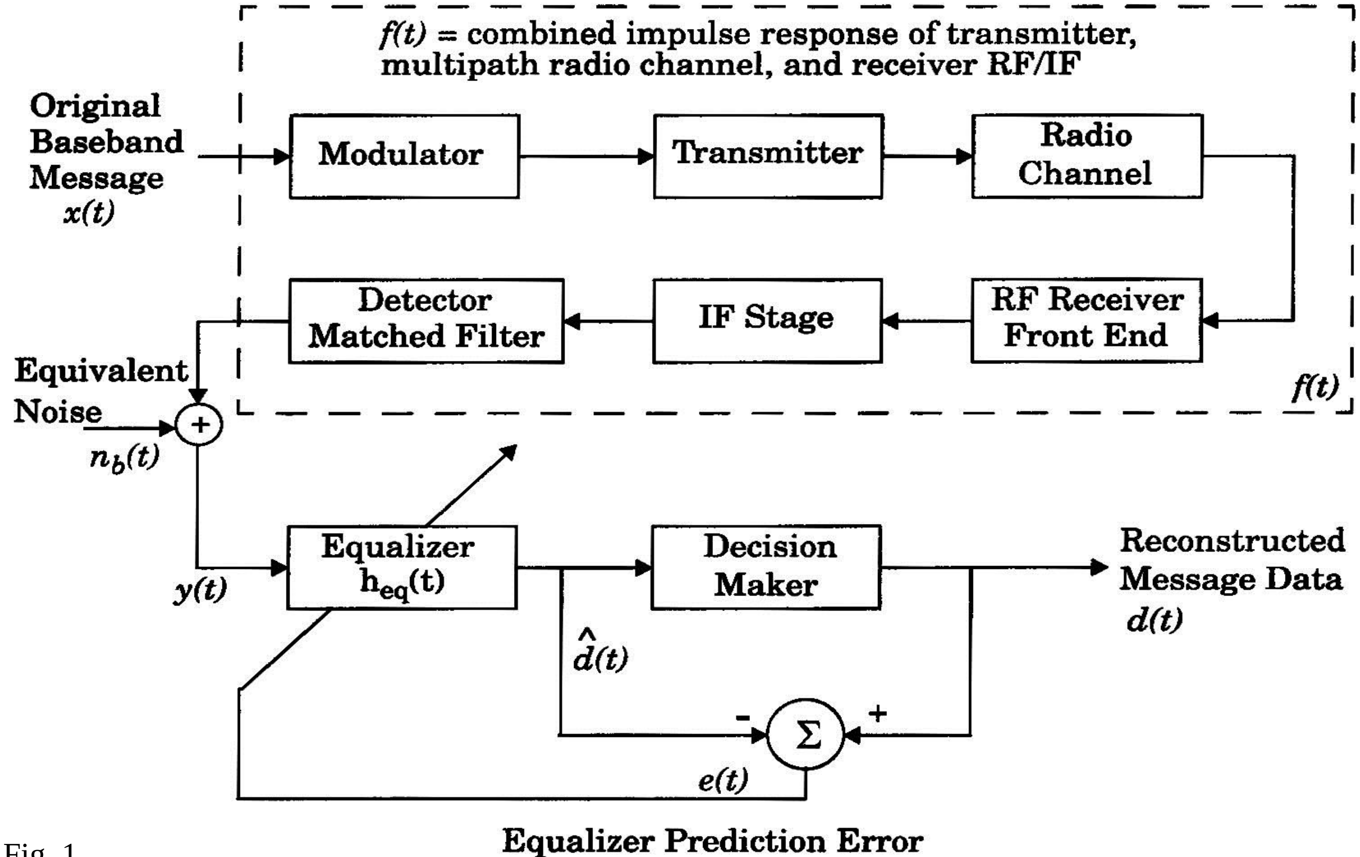


Fig. 1

Block diagram of a simplified communications system using an adaptive equalizer at the receiver.

Equalization Technologies

$$\hat{d}(t) = y(t) * h_{eq}(t)$$

$$= x(t) * \underbrace{f^*(t) * h_{eq}(t)}_{\Downarrow} + m_b(t) * h_{eq}(t)$$

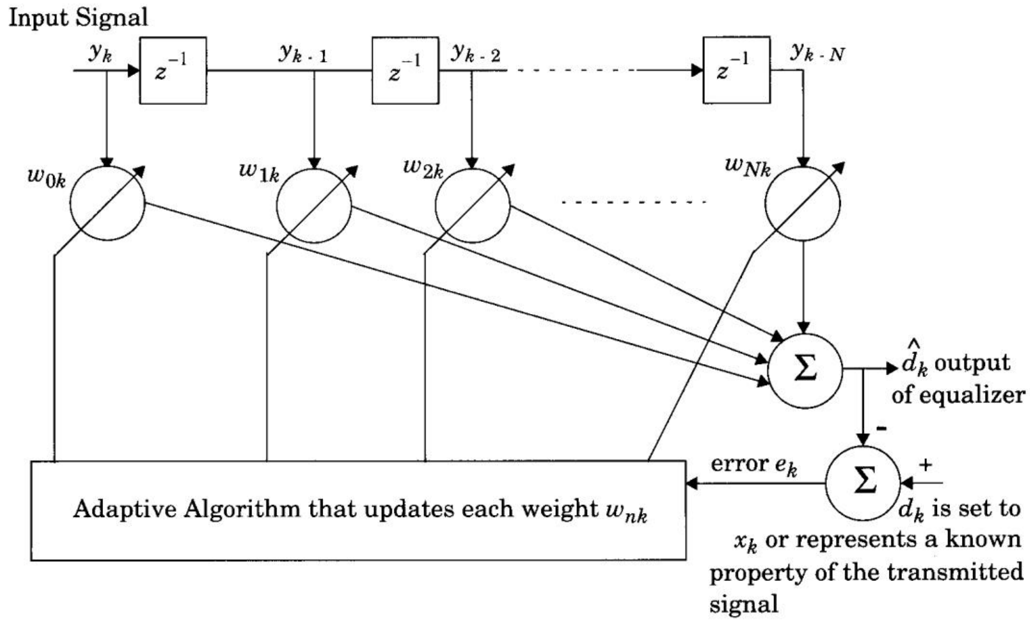
$$= \delta(t)$$

$$\therefore \quad F^*(-f) * H_{eq}(f) = 1$$

- If the channel is frequency selective, the equalizer enhances the frequency components with small amplitudes and attenuates the strong frequencies in the received frequency response
- For a time-varying channel, an adaptive equalizer is needed to track the channel variations

Basic Structure of Adaptive Equalizer

- Transversal filter with N delay elements, N+1 taps, and N+1 tunable complex weights



A basic linear equalizer during training.

- These weights are updated continuously by an adaptive algorithm
- The adaptive algorithm is controlled by the error signal e_k

Equalization Techniques

- Classical equalization theory : using training sequence to minimize the cost function

$$E[e(k)\, e^*(k)]$$

- Recent techniques for adaptive algorithm : blind algorithms
  - Constant Modulus Algorithm (CMA, used for constant envelope modulation) [3]
  - Spectral Coherence Restoral Algorithm (SCORE, exploits spectral redundancy or cyclostationarity in the Tx signal) [4]

Solutions for Optimum Weights of Figure 2 (一)

- Error signal $\quad e_k = x_k - \boldsymbol{y}_k^T \boldsymbol{\omega}_k = x_k - \boldsymbol{\omega}_k^T \boldsymbol{y}_k$

  where $\quad \boldsymbol{y}_k = [y_k \quad y_{k-1} \quad y_{k-2} \quad \ldots. \quad y_{k-N}]^T$

  $$\boldsymbol{\omega}_k = [\omega_k \quad \omega_{k-1} \quad \omega_{k-2} \quad \ldots. \quad \omega_{k-N}]^T$$

- Mean square error $\quad |e_k|^2 = x_k^2 + \boldsymbol{\omega}_k^T \boldsymbol{y}_k \boldsymbol{y}_k^T \boldsymbol{\omega}_k - 2 x_k \boldsymbol{y}_k^T \boldsymbol{\omega}_k$
- Expected MSE $\quad \xi = \mathrm{E}\left[|e_k|^2\right] = \mathrm{E}\left[x_k^2\right] + \boldsymbol{\omega}^T \mathbf{R} \boldsymbol{\omega} - 2\mathbf{p}^T \boldsymbol{\omega}$

  where

$$\mathbf{R} = \mathrm{E}\left[\boldsymbol{y}_k \boldsymbol{y}_k^*\right] = \mathrm{E}\begin{bmatrix} y_k^2 & y_k y_{k-1} & y_k y_{k-2} & \ldots. \; y_k y_{k-N} \\ y_{k-1} y_k & y_{k-1}^2 & y_{k-1} y_{k-2} & \ldots. \, y_{k-1} y_{k-N} \\ \ldots. & \ldots. & \ldots. & \ldots. \quad \ldots. \\ y_{k-N} y_k & y_{k-N} y_{k-1} & y_{k-N} y_{k-2} & \ldots. \quad y_{k-N}^2 \end{bmatrix}$$

$$\mathbf{p} = \mathrm{E}\left[x_k y_k\right] = \mathrm{E}\left[x_k y_k \quad x_k y_{k-1} \quad x_k y_{k-2} \quad \ldots. \quad x_k y_{k-N}\right]^T$$

Solutions for Optimum Weights of Figure 2 (二)

- Optimum weight vector

$$\hat{\omega} = \mathbf{R}^{-1}\mathbf{p}$$

- Minimum mean square error (MMSE)

$$\begin{aligned}\xi_{\min} &= \mathrm{E}\left[\chi_{\kappa}^{2}\right] - \mathbf{p}^{\mathbf{T}}\mathbf{R}^{-1}\mathbf{p} \\ &= \mathrm{E}\left[\chi_{\kappa}^{2}\right] - \mathbf{p}^{\mathrm{T}}\hat{\omega}\end{aligned}$$

- Minimizing the MSE tends to reduce the bit error rate

Equalization Techniques

- Two general categories - linear and nonlinear equalization (see Fig. 3)
- In Fig. 1, if d(t) is not the feedback path to adapt the equalizer, the equalization is *linear*
- In Fig. 1, if d(t) is fed back to change the subsequent outputs of the equalizer, the equalization is *nonlinear*

Equalization Techniques

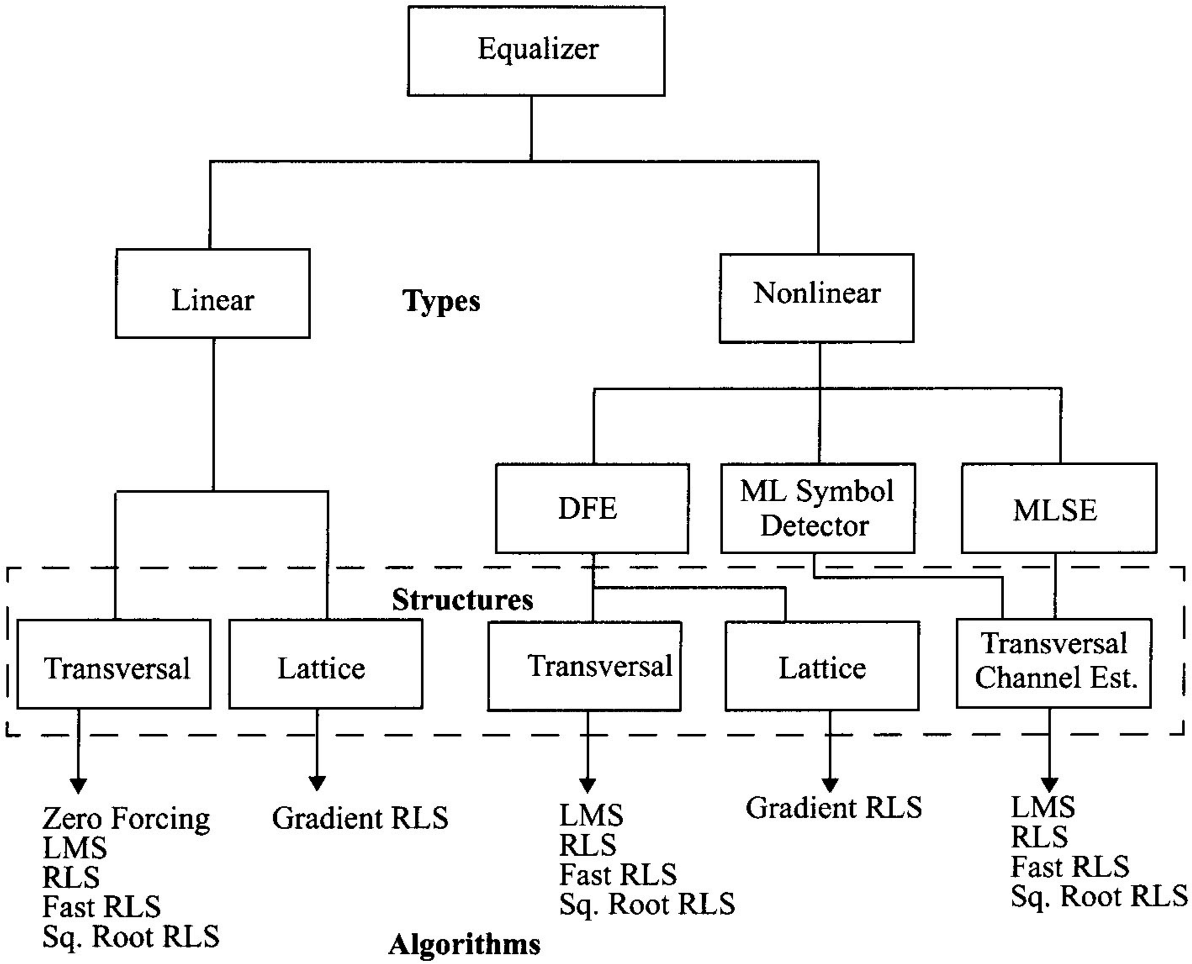


Fig.3 Classification of equalizers

Equalizer Techniques

- Linear transversal equalizer (LTE, made up of tapped delay lines as shown in Fig.4)

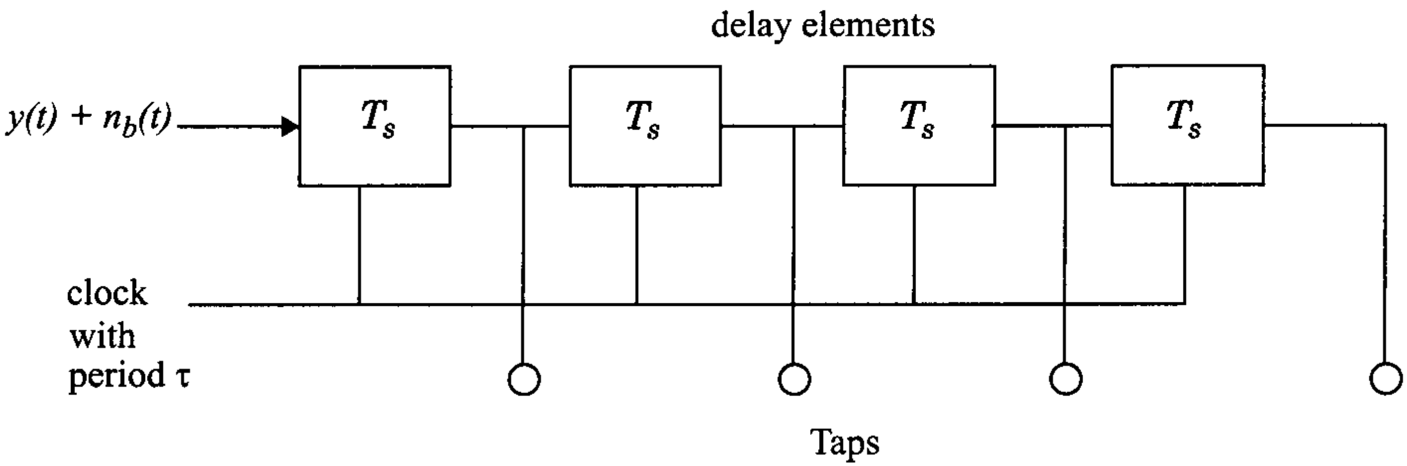


Fig.4 Basic linear transversal equalizer structure

- Finite impulse response (FIR) filter (see Fig.5)
- Infinite impulse response (IIR) filter (see Fig.5)

Equalizer Techniques

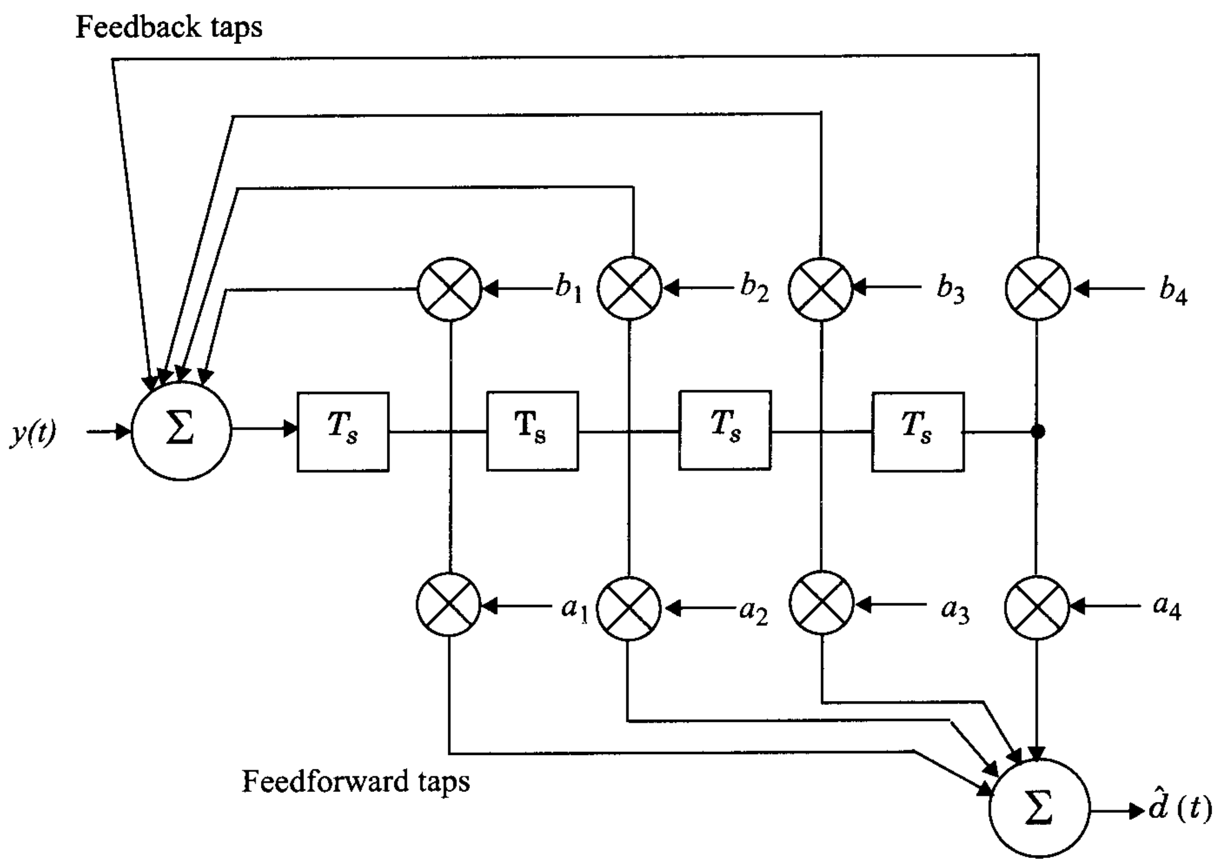
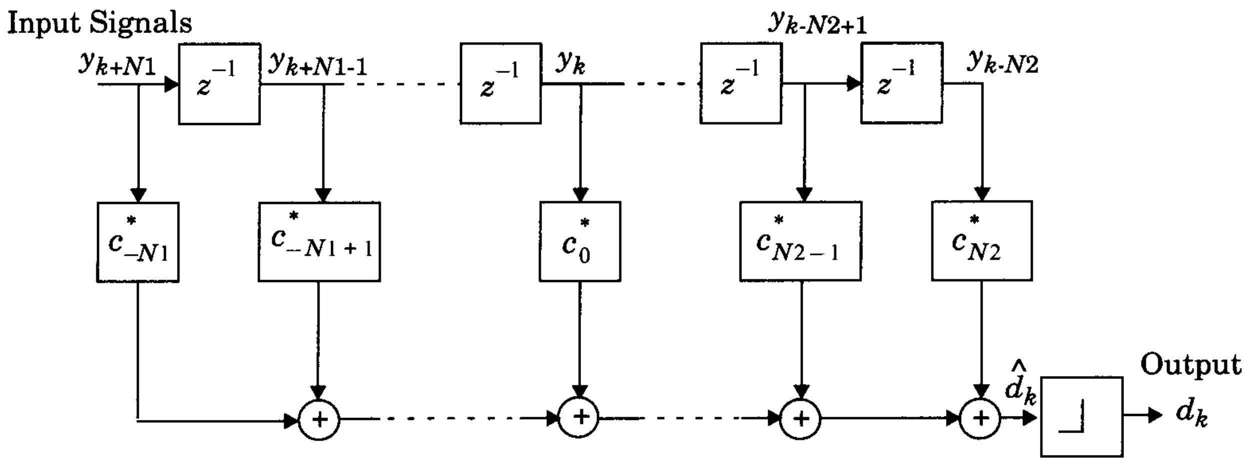


Fig.5 Tapped delay line filter with both feedforward and feedback taps

Structure of a Linear Transversal Equalizer [5]



- $$\hat{d}_k = \sum_{n=-N_1}^{N_2} C_n^* y_{k-n}$$
- $$\mathrm{E}\left[\left|e(n)\right|^2\right] = \frac{T}{2\pi}\int_{-\frac{\pi}{T}}^{\frac{\pi}{T}} \frac{N_o}{\left|\mathrm{F}(e^{j\omega t})\right|^2 + N_o} d\omega$$

$\mathrm{F}(e^{j\omega t})$:frequency response of the channel

N_o :noise spectral density

Structure of a Lattice Equalizer [6-7]

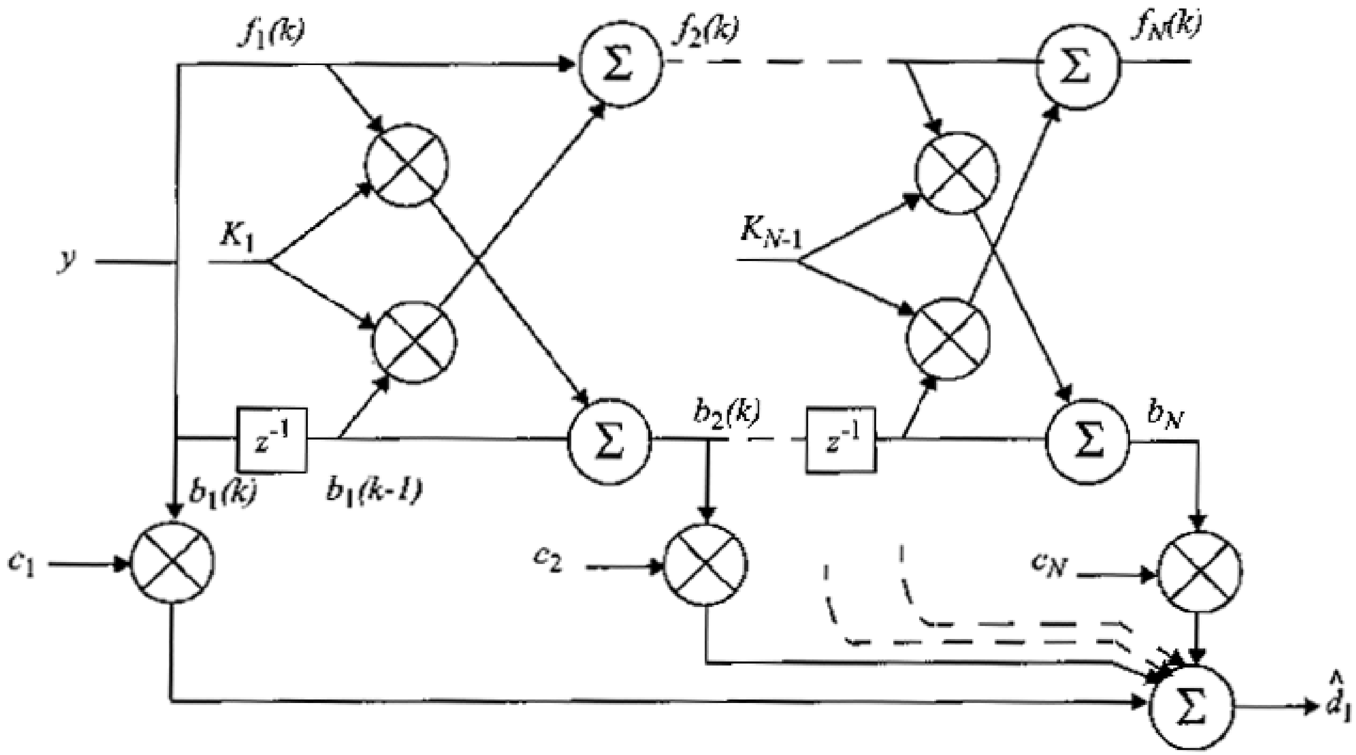


Fig.7 The structure of a Lattice Equalizer

Characteristics of Lattice Filter

- Advantages
  - ➢Numerical stability
  - ➢Faster convergence
  - ➢Unique structure allows the dynamic assignment of the most effective length
- Disadvantages
  - ➢The structure is more complicated

Nonlinear Equalization

- Used in applications where the channel distrotion is too severe
- Three effective methods [6]
  - Decision Feedback Equalization (DFE)
  - Maximum Likelihood Symbol Detection
  - Maximum Likelihood Sequence Estimator (MLSE)

Nonlinear Equalization--DFE

- Basic idea : once an information symbol has been detected and decided upon, the ISI that it induces on future symbols can be estimated and substracted out before detection of subsequent symbols
- Can be realized in either the direct transversal form (see Fig.8) or as a lattice filter

- $$\hat{d}_k = \sum_{n=-N_1}^{N_2} C_n^* y_{k-n} + \sum_{i=1}^{N_3} F_i d_{k-i}$$

- $$\mathrm{E}\left[|e(n)|^2\right]_{min} = exp\{\frac{T}{2\pi}\int_{-\frac{\pi}{T}}^{\frac{\pi}{T}} ln[\frac{N_o}{|\mathrm{F}(e^{j\omega T})|^2 + N_o}]d\omega\}$$

Nonlinear Equalizer-DFE

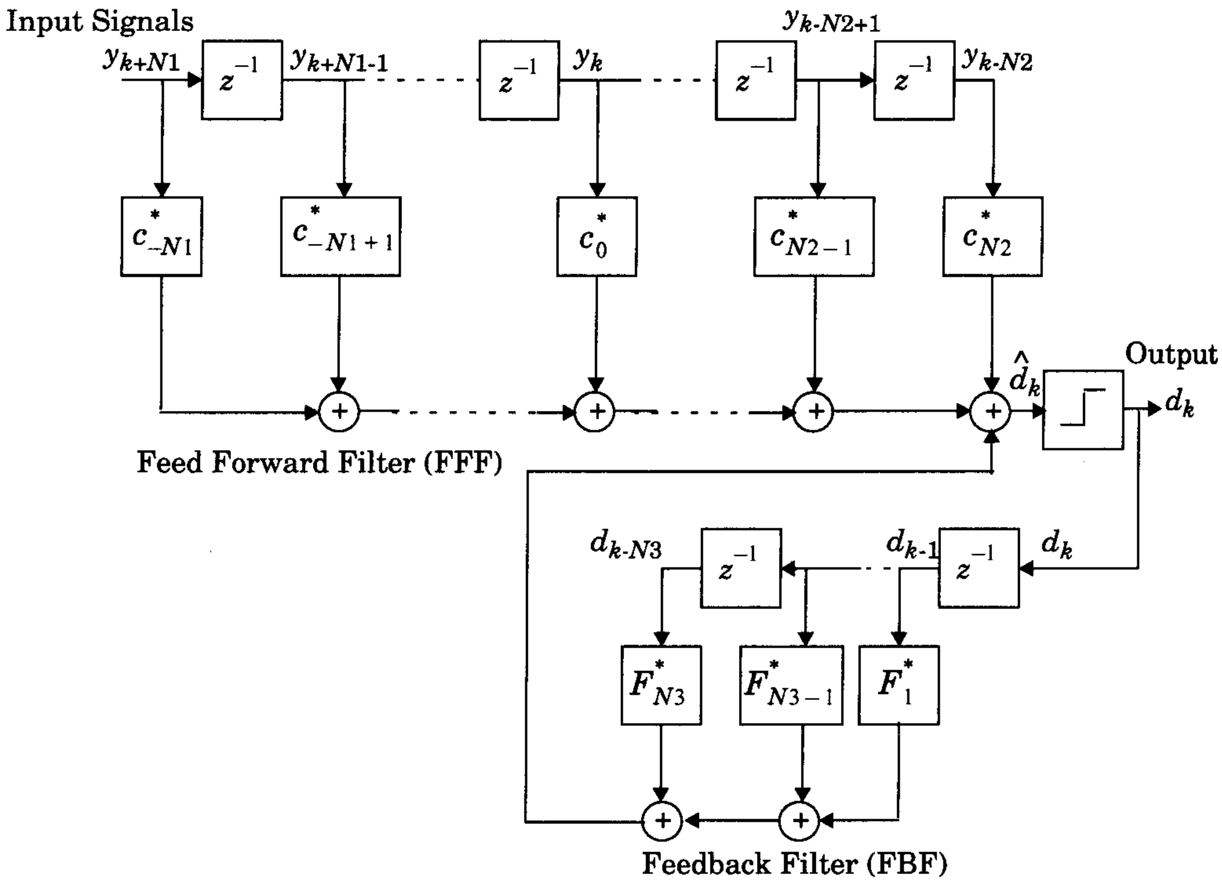


Fig.8 Decision feedback equalizer (DFE)

Nonlinear Equalization--DFE

- *Predictive* DFE (proposed by Belfiore and Park, [8])
- Consists of an FFF and an FBF, the latter is called a *noise predictor* (see Fig.9)
- Predictive DFE performs as well as conventional DFE as the limit in the number of taps in FFF and the FBF approach infinity
- The FBF in predictive DFE can also be realized as a lattice structure [9]. The RLS algorithm can be used to yield fast convergence

Nonlinear Equalizer-DFE

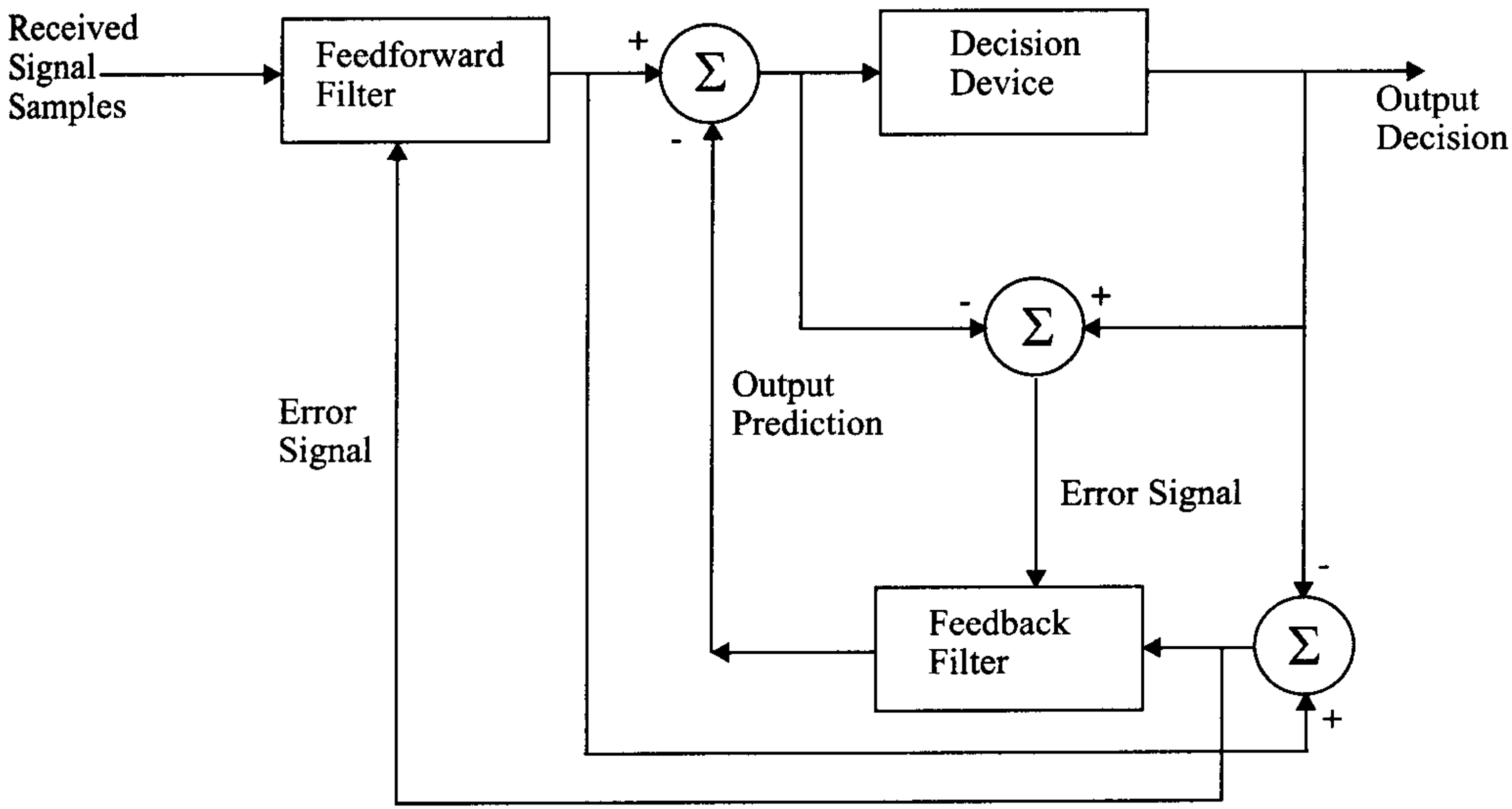


Fig.9 Predictive decision feedback equalizer

Nonlinear Equalization--MLSE

- MLSE tests all possible data sequences (rather than decoding each received symbol by itself), and chooses the data sequence with the maximum probability as the output
- Usually has a large computational requirement
- First proposed by Forney [10] using a basic MLSE estimator structure and implementing it with the Viterbi algorithm
- The block diagram of MLSE receiver (see Fig.10)

Nonlinear Equalizer-MLSE

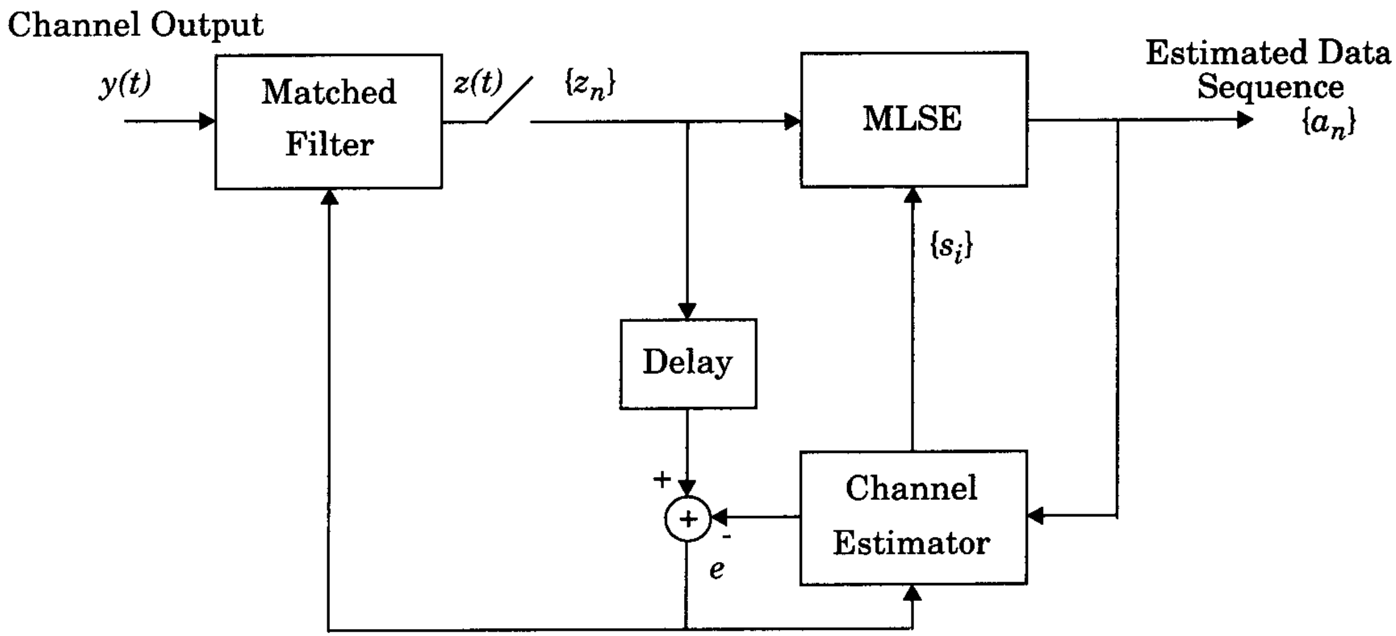


Fig.10 The structure of a maximum likelihood sequence equalizer(MLSE) with an adaptive matched filter

- MLSE requires knowledge of the channel characteristics in order to compute the matrics for making decisions
- MLSE also requires knowledge of the statistical distribution of the noise corrupting the signal

Algorithm for Adaptive Equalization

- Excellent references [6, 11--12]
- Performance measures for an algorithm
  - Rate of convergence
  - Misadjustment
  - Computational complexity
  - Numerical properties
- Factors dominate the choice of an equalization structure and its algorithm
  - The cost of computing platform
  - The power budget
  - The radio propagation characteristics

Algorithm for Adaptive Equalization

- The speed of the mobile unit determines the channel fading rate and the Dopper spread, which is related to the coherent time of the channel directly
- The choice of algorithm, and its corresponding rate of convergence, depends on the channel data rate and coherent time
- The number of taps used in the equalizer design depends on the maximum expected time delay spread of the channel
- The circuit complexity and processing time increases with the number of taps and delay elements

Algorithm for Adaptive Equalization

- Three classic equalizer algorithms : zero forcing (ZF), least mean squares (LMS), and recursive least squares (RLS) algorithms
- Summary of algorithms (see Table 1)

Summary of algorithms

Algorithm	Number of Multiply Operations	Advantages	Disadvantages
LMS Gradient DFE	$2N + 1$	Low computational complexity, simple program	Slow convergence, poor tracking
Kalman RLS	$2.5N^2 + 4.5N$	Fast convergence, good tracking ability	High computational complexity
FTF	$7N + 14$	Fast convergence, good tracking, low computational complexity	Complex programming, unstable (but can use rescue method)
Gradient Lattice	$13N - 8$	Stable, low computational complexity, flexible structure	Performance not as good as other RLS, complex programming
Gradient Lattice DFE	$13N_1 + 33N_2 - 36$	Low computational complexity	Complex programming
Fast Kalman DFE	$20N + 5$	Can be used for DFE, fast convergence and good tracking	Complex programming, computation not low, unstable
Square Root RLS DFE	$1.5N^2 + 6.5N$	Better numerical properties	High computational complexity

Table 1 Comparison of various algorithms for adaptive equalization

Diversity Techniques

- Requires no training overhead
- Can provides significant link improvement with little added cost
- Diversity decisions are made by the Rx, and are unknown to the Tx
- Diversity concept
  - If one radio path undergoes a deep fade, another independent path may have a strong signal
  - By having more than one path to select from, both the instantaneous and average SNRs at the receiver may be improved, often by as much as 20 dB to 30 dB

Diversity Techniques

- *Microscopic diversity* and *Macroscopic diversity*
  - ➢The former is used for small-scale fading while the latter for large-scale fading
  - ➢Antenna diversity (or space diversity)
- Performance for M branch selection diversity (see Fig.11)

$$Pr\left[SNR > r\right] = 1 - Pr\left[\gamma_1, \quad \ldots \quad, \gamma_M \le r\right]$$
$$= 1 - (1 - e^{-r/\Gamma})^M$$

$$P_M(r) = \frac{d}{dr} Pr\left[SNR \le r\right] = \frac{M}{\Gamma}(1 - e^{-r/\Gamma})^{M-1} e^{-r/\Gamma}$$

$$\frac{\bar{r}}{\Gamma} = \sum_{k=1}^{M} \frac{1}{k}$$

Diversity techniques

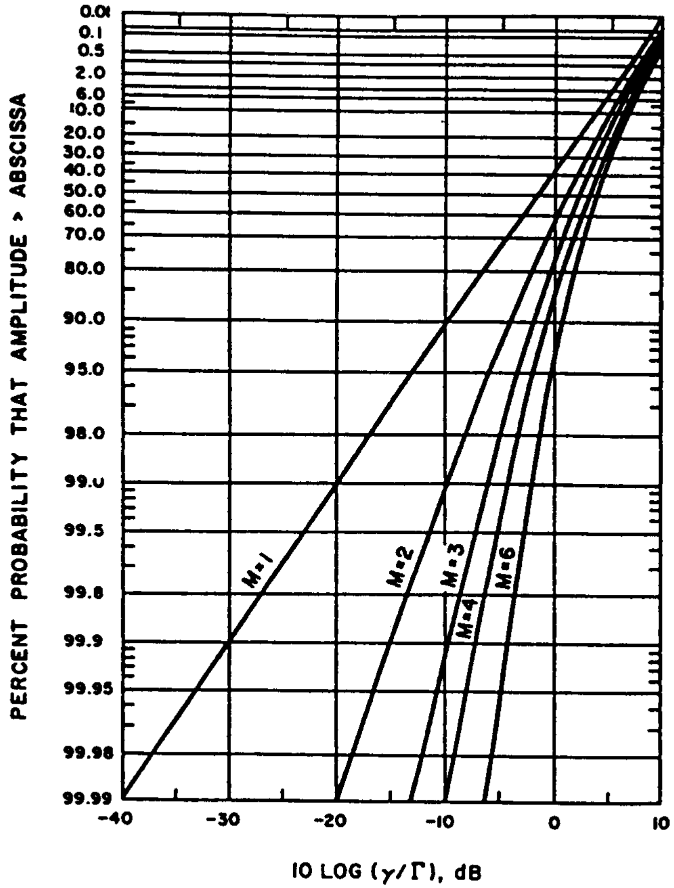


Fig. 11 Graph of probability distributions of *SNR*=γ threshold for M branch selection diversity. The term Γ represents the mean SNR on each branch

Diversity Techniques

- Performance for Maximal Ratio Combining Diversity [13] (see Fig. 12)

$$\gamma_M = \sum_{i=1}^{M} G_i \gamma_i \qquad N_T = N \sum_{i=1}^{M} G_i^{\ 2}$$

$$r_M = \frac{\gamma_M^2}{2N_T}$$

$$Pr\{r_M \le r\} = \int_0^r p(r_M)\,dr_M = 1 - e^{-r/\Gamma} \sum_{k=1}^{M} \frac{(r/\Gamma)^{k-1}}{(k-1)!}$$

$$P(r_M) = \frac{r_M^{\ M-1} e^{-r_M/\Gamma}}{\Gamma^M (M-1)!}$$

Diversity Techniques

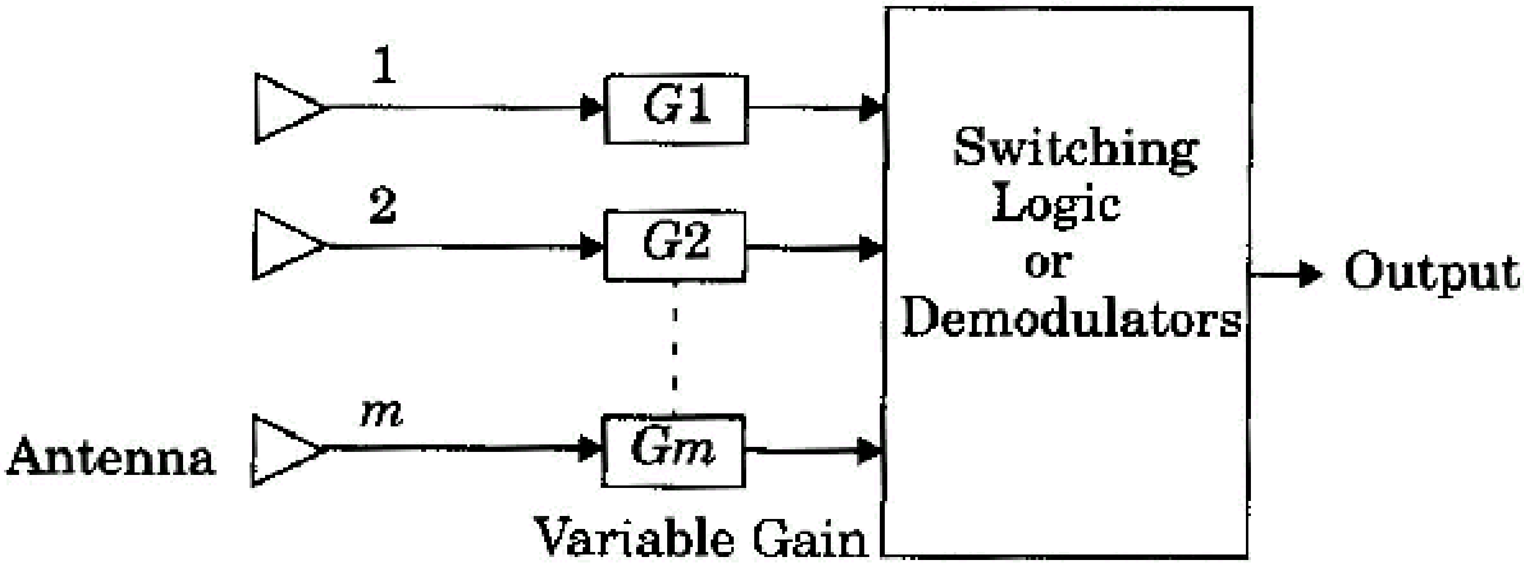


Fig. 12 Generalized block diagram for space diversity

Diversity Techniques

- Space diversity [14]
  - Selection diversity
  - Feedback diversity
  - Maximal ration combining
  - Equal gain diversity

- Selection diversity (see Fig. 13)
  - ➢ The receiver branch having the highest instantaneous SNR is connected to the demodulator
  - ➢ The antenna signals themselves could be sampled and the best one sent to a single demodulation

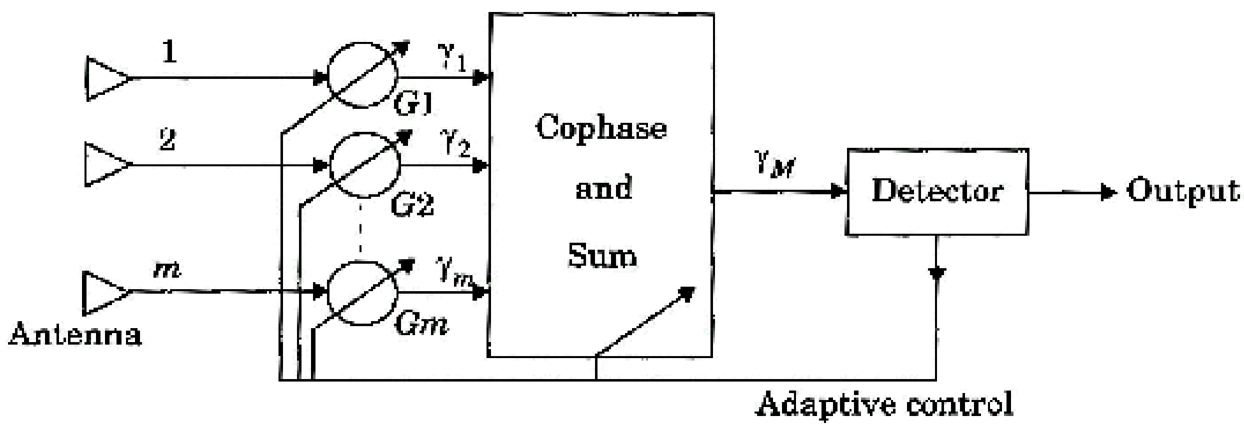


Fig. 13 Maximal ratio combiner

Diversity Techniques

- Feedback or scanning diversity (see Fig. 14)
  - ➢ The signal, the best of M signals, is received until it falls below threshold and the scanning process is again initiated

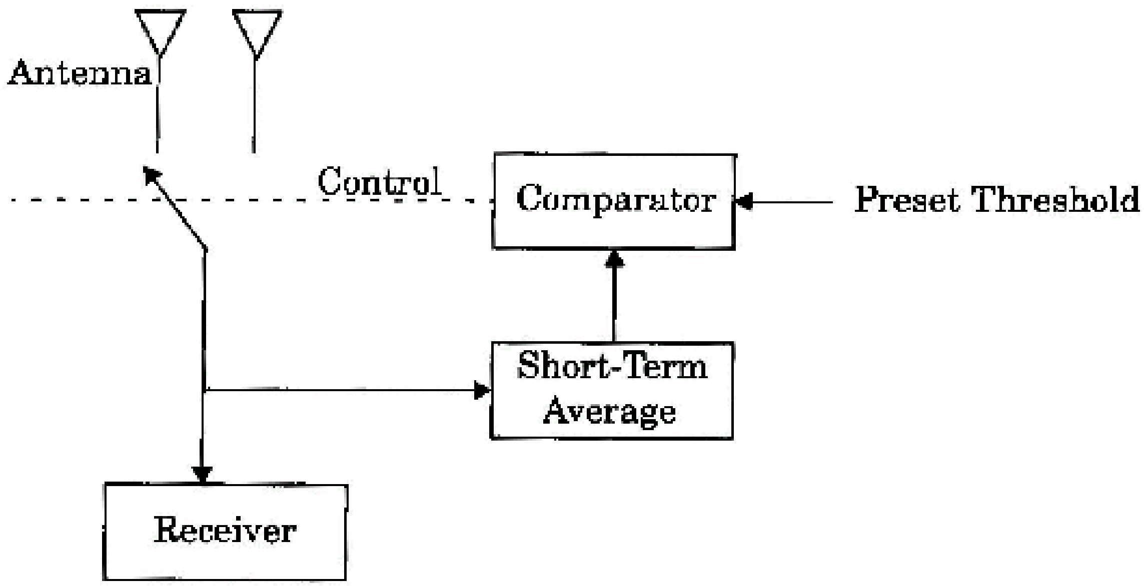


Fig. 14 Basic form for scanning diversity

Diversity Techniques

- Maximal ratio combining [15] (see Fig. 12)
  - The signals from all of the M branches are weighted according to their signal voltage to noise power ratios and then summed
- Equal gain diversity
  - The branch weights are all set to unity but the signals from each are co-phased to provide equal gain combining diversity

Diversity Techniques

- Polarization diversity
  - ➢ Theoretical model for polarization diversity [16] (see Fig.15)

the signal arrive at the base station

$$x = r_1 \cos(\omega t + \phi_1)$$
$$y = r_2 \cos(\omega t + \phi_2)$$

the correlation coefficient can be written as

$$\rho = \left(\frac{\tan^2(\alpha)\cos^2(\beta) - \Gamma}{\tan^2(\alpha)\cos^2(\beta) + \Gamma} \right)^2$$

$$\Gamma = \frac{\langle R_2^2 \rangle}{\langle R_1^2 \rangle}$$

$$R_1 = \sqrt{r_1^2 a_2 + r_2^2 b_2 + 2 r_1 r_2 ab \cos(\phi_1 + \phi_2)}$$

$$R_1 = \sqrt{r_1^2 a_2 + r_2^2 b_2 - 2 r_1 r_2 ab \cos(\phi_1 + \phi_2)}$$

Diversity Techniques

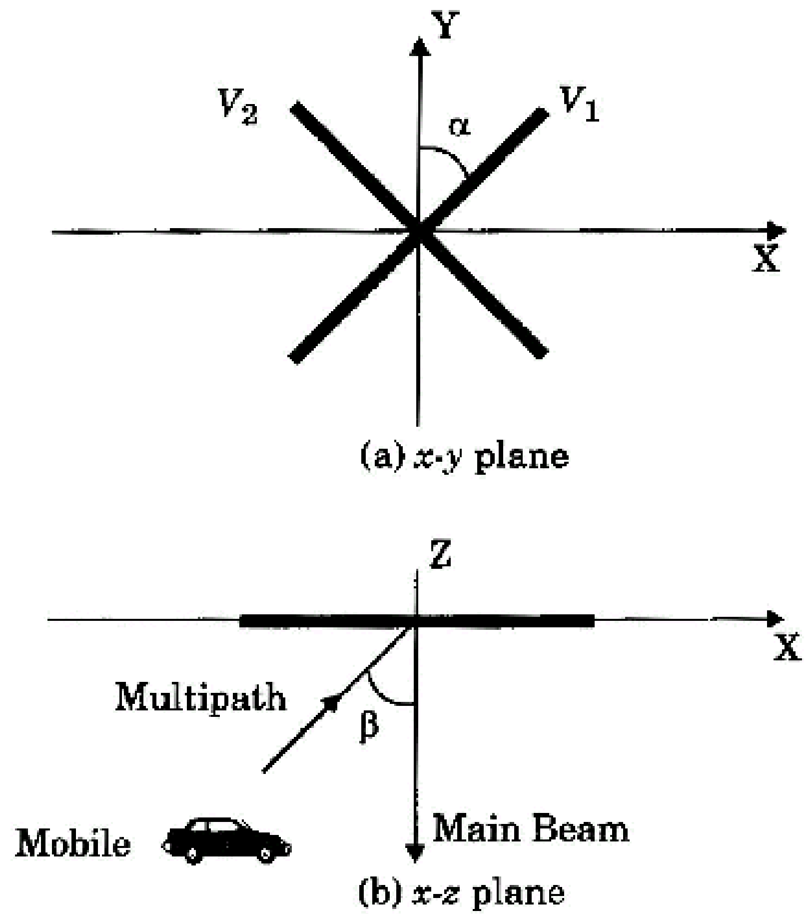


Fig. 15 Theoretical Model for base station polarization diversity based on [Koz85]

Diversity Techniques

- Frequency diversity
  - Frequency diversity transmits information on more than one carrier frequency
  - Frequencies separated by more than the coherence bandwidth of the channel will not experience the same fads
- Time diversity
  - Time diversity repeatedly transmits information at time spacings that exceed the coherence time of the channel

RAKE Receiver

- RAKE Receiver [17]

$$Z' = \sum_{m=1}^{M} \alpha_m Z_m \qquad \alpha_m = \frac{Z_m^2}{\sum_{m=1}^{M} Z_m^2}$$

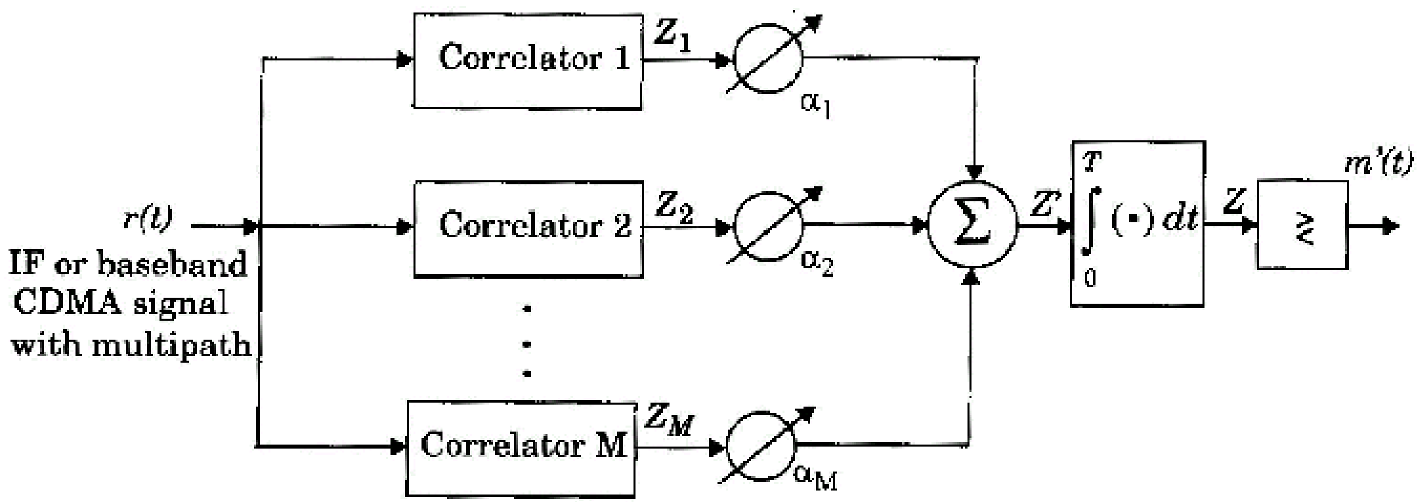


Fig. 16 An M-branch (M-finger) RAKE receiver implementation. Each correlator detects a time shifted version of the original CDMA transmission, and each finger of the RAKE correlates to a portion of the signal which is delayed by at least one chip in time from the other finger.

Interleaving

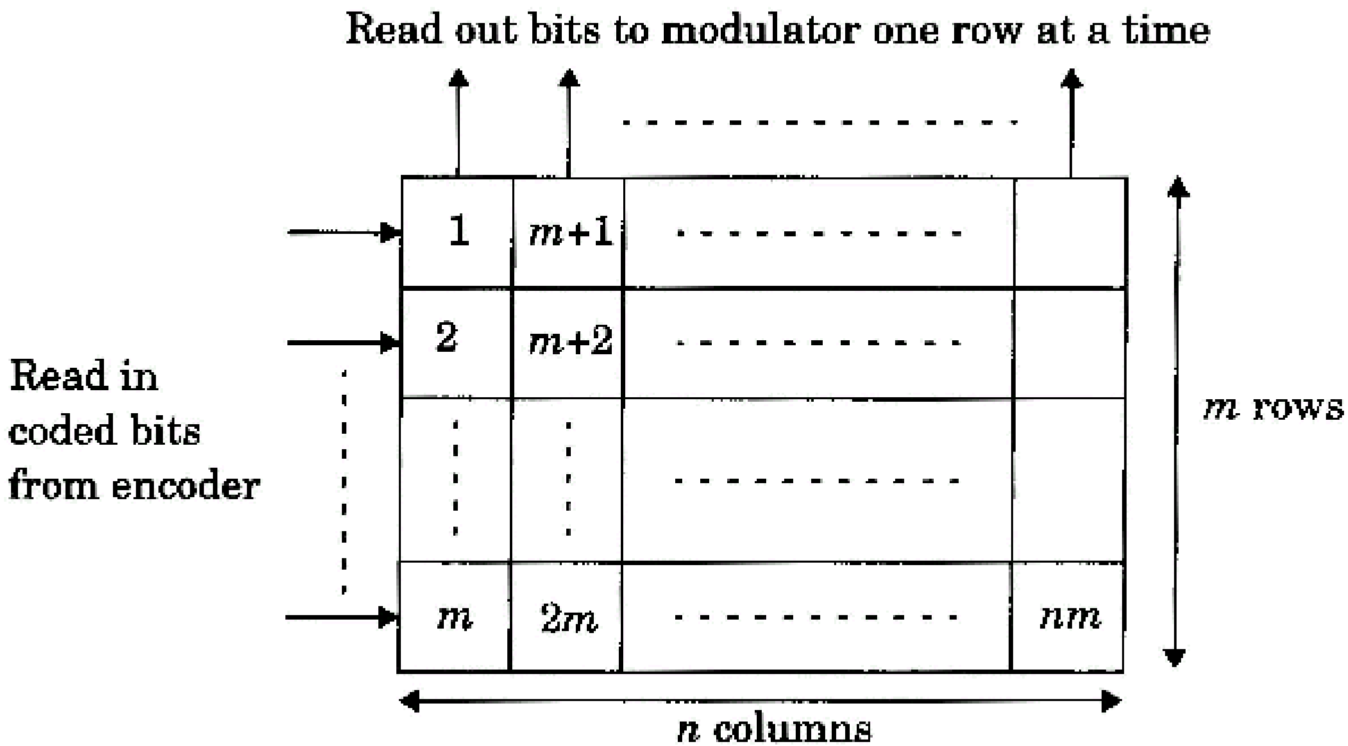


Fig. 17 Block interleaver where source bits are read into columns and out as n-bit rows

Hamming Code

- H(n,k): k information bit length, n overall code length
- n=2^m-1, k=2^m-m-1:
- H(7,4), rate (4/7); H(15,11), rate (11/15); H(31,26), rate (26/31)
- H(7,4): Distance d=3, correction ability 1, detection ability 2.
- Remember that it is good to have larger distance and rate.
- Larger n means larger delay, but usually better code

Hamming Code Example

$$\mathbf{G} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

- **H(7,4)**
- **Generator matrix G: first** $\mathbf{p} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ **4 ident...**
  matrix
- **Message information vect...**

$$\mathbf{Gp} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \mathbf{x}$$

$$\mathbf{r} = \mathbf{x} + \mathbf{e}_i$$

- **Tran...**
- **Rece...**

$$\mathbf{H} := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

and error vector e

Parity check matrix H

Error Correction

If there is no error, syndrome vector z=zeros

$$\mathbf{Hr} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \mathbf{z}$$

$$\mathbf{Hr} = \mathbf{H}(\mathbf{x} + \mathbf{e}_i) = \mathbf{Hx} + \mathbf{He}_i = 0 + \mathbf{He}_i = \mathbf{He}_i$$

If there is one error at locatio

$$\mathbf{r} = \mathbf{x} + \mathbf{e}_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\mathbf{Hr} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \mathbf{z}$$

s

Important Hamming Codes

- **Hamming (7,4,3) -code. It has 16 codewords of length 7. It can be used to send $2^7 = 128$ messages and can be used to correct 1 error.**
- **Golay (23,12,7) -code. It has 4 096 codewords. It can be used to transmit 8 3888 608 messages and can correct 3 errors.**
- **Quadratic residue (47,24,11) -code. It has 16 777 216 codewords and can be used to transmit 140 737 488 355 238 messages and correct 5 errors.**

Reed–Muller code

Reed-Muller codes form a family of codes defined recursively with interesting properties and easy decoding.

If D_1 is a binary $[n,k_1,d_1]$ -code and D_2 is a binary $[n,k_2,d_2]$ -code, a binary code C of length $2n$ is defined as follows $C = \{ \mid u \mid u + v \mid, \text{ where } u \in D_1, v \in D_2\}$.

Lemma C is $[2n,k_1 + k_2, \min\{2d_1,d_2\}]$ -code and if G_i is a generator matrix for D_i, $i = 1, 2$, then $\begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$ is a generator matrix for C.

Reed-Muller codes $R(r,m)$, with $0 \le r \le m$ are binary codes of length $n = 2^m$. $R(m,m)$ is the whole set of words of length n, $R(0,m)$ is the repetition code.

If $0 < r < m$, then $R(r + 1,m + 1)$ is obtained from codes $R(r + 1,m)$ and $R(r,m)$ by the above construction.

Cyclic code

Cyclic codes are of interest and importance because

- They posses rich algebraic structure that can be utilized in a variety of ways.
- They have extremely concise specifications.
- They can be efficiently implemented using simple *shift register*
- Many practically important codes are cyclic

In practice, cyclic codes are often used for error detection (Cyclic redundancy check,

BASIC DEFINITION of Cyclic Code

Definition A code C is cyclic if

(i) C is a linear code;

(ii) any cyclic shift of a codeword is also a codeword, i.e. whenever $a_0, \ldots a_{n-1} \in C$, then also $a_{n-1}\, a_0 \ldots a_{n-2} \in C$.

Example

(i) Code C = {000, 101, 011, 110} is cyclic.

(ii)

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

is equivalent to a cyclic co

FREQUENCY of CYCLIC CODES

Comparing with linear codes, the cyclic codes are quite scarce. For, example there are 11 811 linear (7,3) linear binary codes, but only two of them are cyclic.

Trivial cyclic codes. For any field F and any integer $n >= 3$ there are always the following cyclic codes of length n over F:

- No-information code - code consisting of just one all-zero codeword.
- Repetition code - code consisting of code-words $(a, a, \ldots, a)$ for $a \in F$.
- Single-parity-check code - code consisting of all code-words with parity 0.
- No-parity code - code consisting of all code-words of length n

For some cases, for example for $n = 19$ and $F = GF(2)$, the above four trivial cyclic codes are the only cyclic codes.

EXAMPLE of a CYCLIC CODE

The code with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

has code-words

$$c_1 = 1011100 \qquad c_2 = 0101110 \qquad c_3 = 0010111$$

$$c_1 + c_2 = 1110010 \qquad c_1 + c_3 = 1001011 \qquad c_2 + c_3 = 0111001$$

$$c_1 + c_2 + c_3 = 1100101$$

and it is cyclic because the right shifts have the following impacts

$$c_1 \to c_2, \qquad c_2 \to c_3, \qquad c_3 \to c_1 + c_3$$

$$c_1 + c_2 \to c_2 + c_3, \qquad c_1 + c_3 \to c_1 + c_2 + c_3, \qquad c_2 + c_3 \to c_1$$

$$c_1 + c_2 + c_3 \to c_1 + c_2$$

POLYNOMIALS over GF(q)

A codeword of a cyclic code is usually denoted

$$a_0 a_1 \ldots a_{n-1}$$

and to each such a codeword the polynomial

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$$

is associated.

$F_q[x]$ denotes the set of all polynomials over $GF(q)$.

deg (f(x)) = the largest m such that x^m has a non-zero coefficient in $f(x)$.

Multiplication of polynomials If f(x), g(x) $\in F_q[x]$, then

$$deg\ (f(x)\,g(x)) = deg\ (f(x)) + deg\ (g(x)).$$

Division of polynomials For every pair of polynomials a(x), b(x) $\neq 0$ in $F_q[x]$ there exists a unique pair of polynomials q(x), r(x) in $F_q[x]$ such that

$$a(x) = q(x)b(x) + r(x),\ deg\ (r(x)) < deg\ (b(x)).$$

Example Divide $x^3 + x + 1$ by $x^2 + x + 1$ in $F_2[x]$.

Definition Let f(x) be a fixed polynomial in $F_q[x]$. Two polynomials g(x), h(x) are said to be congruent modulo f(x), notation

$$g(x) \equiv h(x)\ (\mathrm{mod}\ f(x)),$$

if g(x) - h(x) is divisible by f(x).

NCCU
Wireless Comm. Lab.

EXAMPLE

The task is to determine all ternary codes of length 4 and generators for them.

Factorization of $x^4 - 1$ over $GF(3)$ has the form

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1) = (x - 1)(x + 1)(x^2 + 1)$$

Therefore there are $2^3 = 8$ divisors of $x^4 - 1$ and each generates a cyclic code.

Generator polynomial	Generator matrix
1	I_4
x	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x + 1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
$x^2 + 1$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x + 1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x^2 + 1) = x^3 - x^2 + x - 1$	$[\,-1\ 1\ -1\ 1\,]$
$(x + 1)(x^2 + 1)$	$[\,1\ 1\ 1\ 1\,]$
$x^4 - 1 = 0$	$[\,0\ 0\ 0\ 0\,]$

Cyclic Code Encoder

Encoding using a cyclic code can be done by a multiplication of two polynomials - a message polynomial and the generating polynomial for the cyclic code.

Let C be an (n,k)-code over an field F with the generator polynomial

$g(x) = g_0 + g_1 x + \ldots + g_{r-1} x^{r-1}$ of degree $r = n - k$.

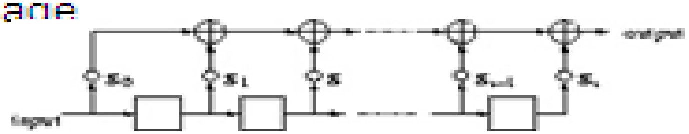
If a message vector m is represented by a polynomial $m(x)$ of degree k and m is encoded by

$$m \Rightarrow c = mG_1,$$

then the following relation between $m(x)$ and $c(x)$ holds

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

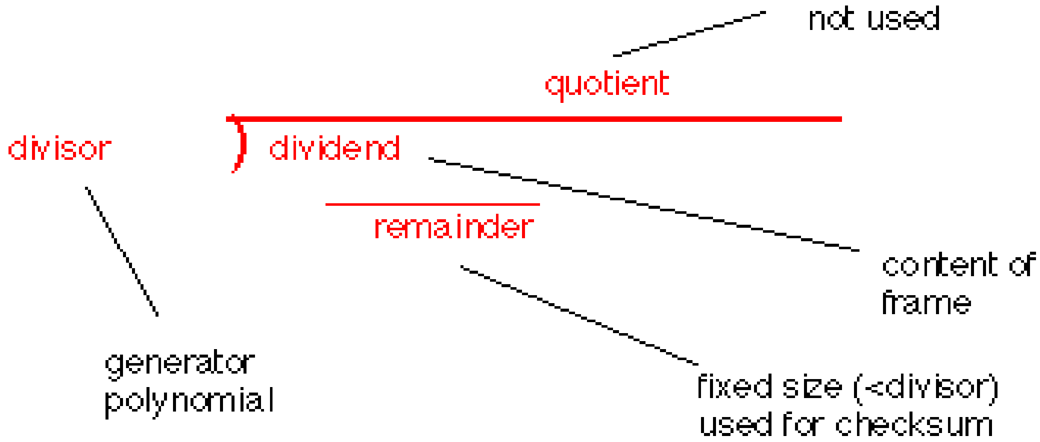
Such an encoding can be realized by the shift register shown in Figure below, where input is the k-bit message to be encoded followed by $n - k$ 0' and the output will be the encoded message



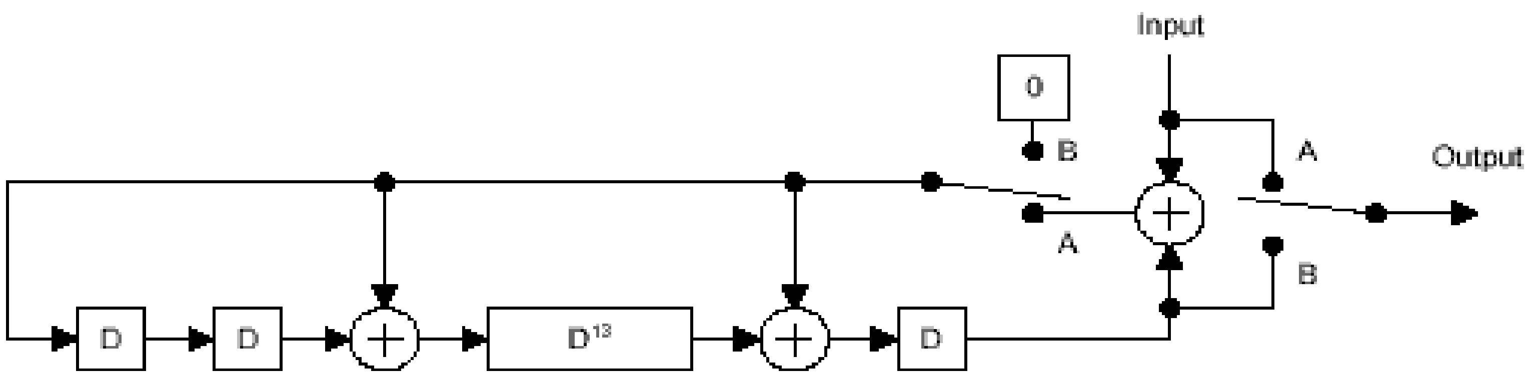
Shift-register encodings of cyclic codes. Small circles represent multiplication by the corresponding constant, $\oplus$ nodes represent modular addition, squares are delay elements

Cyclic Code Decoder

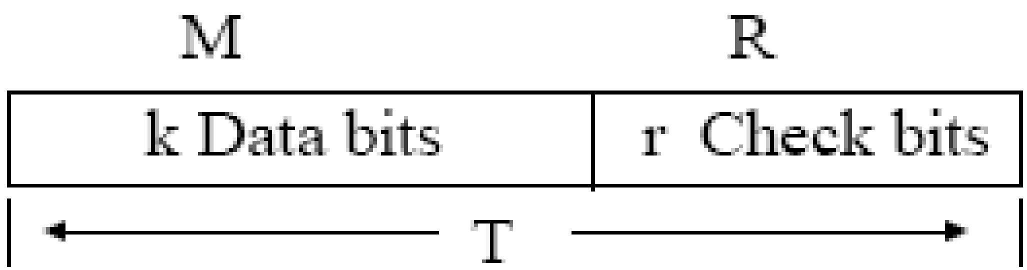
Divider



Si



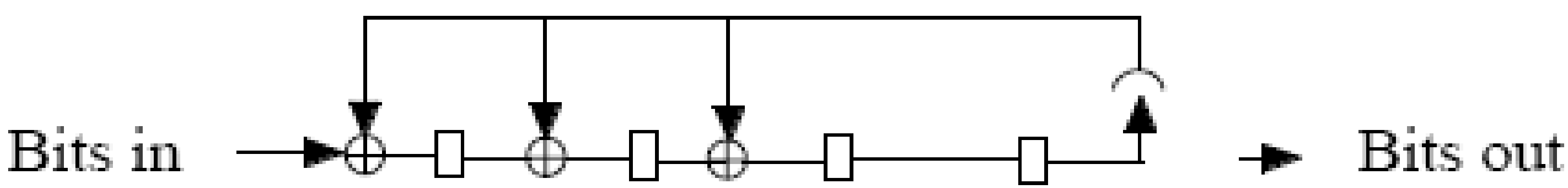
Cyclic Redundancy Checks (CRC)



M = info bits
R = check bits
T = codeword

$$T = M\,2^{r} + R$$

A CRC is implemented using a feedback shift register



Example of CRC

$r = 3$, $G = 1001$

$M = 110101 \Rightarrow M2^r = 110101000$

```
             110011
       ______________
1001  |  110101000
         1001
         ----
         01000
          1001
          ----
          0001100
             1001
             ----
             01010
              1001
              ----
               011 = R (3 bits)
```

Modulo 2 Division

Checking for errors

- Let T' be the received sequence
- Divide T' by G
  - If remainder = 0 assume no errors
  - If remainder is non zero errors must have occurred

Example:
Send T = 110101011
Receive T' = 110101011
(no errors)

No way of knowing how many errors occurred or which bits are In error

```
1001 | 110101011
       1001
       ----
       01000
        1001
        ----
        0001101
           1001
           ----
           01001
            1001
            ----
             000 => No errors
```

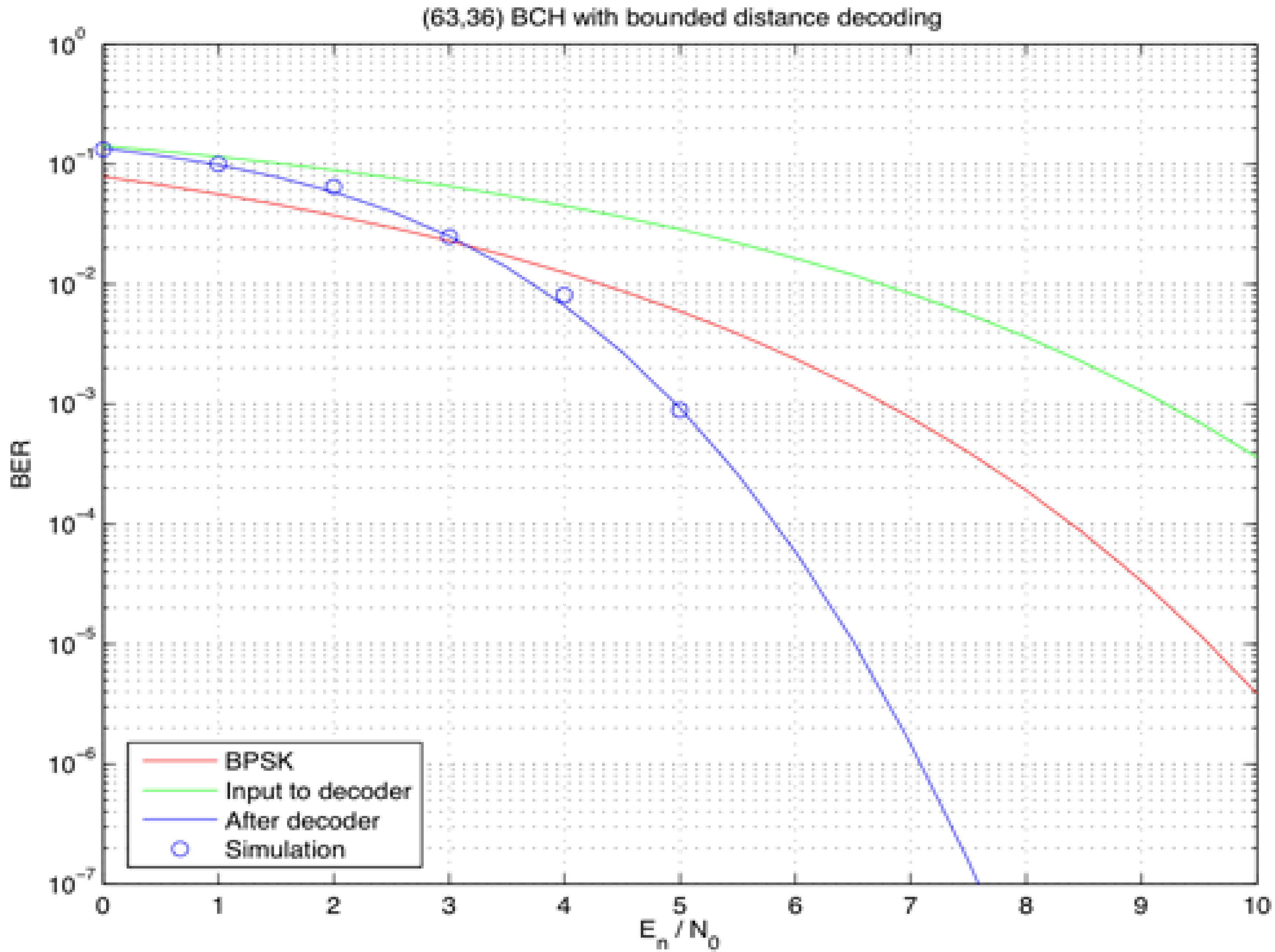
Capability of CRC

- **An error E(X) is undetectable if it is divisible by G(x). The following can be detected.**
  - All single-bit errors if G(x) has more than one nonzero term
  - All double-bit errors if G(x) has a factor with three terms
  - Any odd number of errors, if P(x) contain a factor x+1
  - Any burst with length less or equal to n-k
  - A fraction of error burst of length n-k+1; the fraction

BCH Code

- **Bose, Ray-Chaudhuri, Hocquenghem**
  - Multiple error correcting ability
  - Ease of encoding and decoding
- **Most powerful cyclic code**
  - For any positive integer m and t<2^(m-1), there exists a t-error correcting (n,k) code with n=2^m-1 and n-k<=mt.
- **Industry standards**
  - (511, 493) BCH code in ITU-T. Rec. H.261 "video codec for audiovisual service at kbit/s" a video

BCH Performance



Reed-Solomon Codes

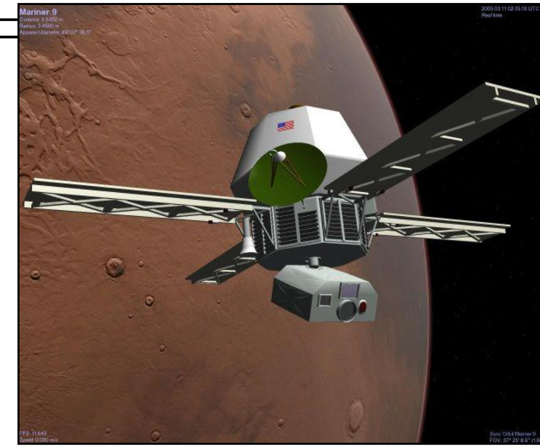
An important subclass of non-binary BCH

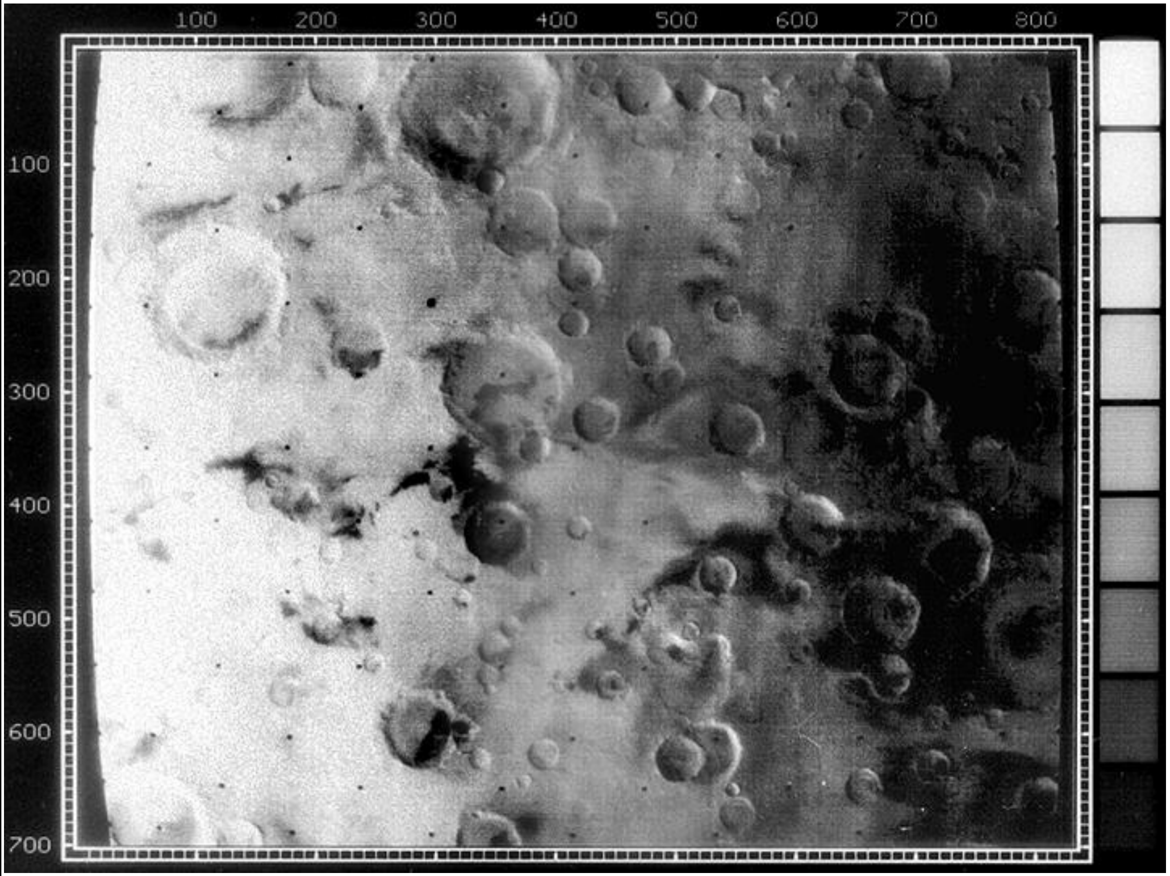
Wide range of applications

- Storage devices (tape, CD, DVD…)
- Wireless or mobile communication
- Satellite communication
- Digital television/Digital Video Broadcast(DVB)
- High-speed modems (ADSL, xDSL…)

1971: Mariner 9

- Mariner 9 used a [32,6,16] *Reed-Muller* code to transmit its grey images of Mars.





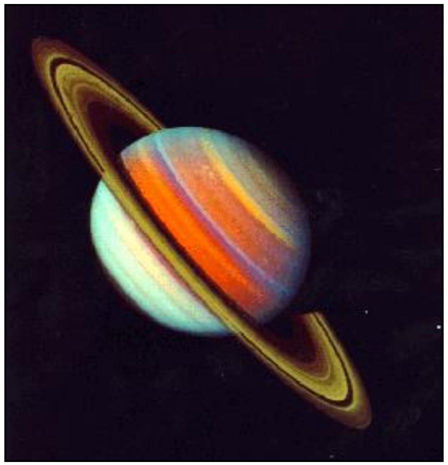
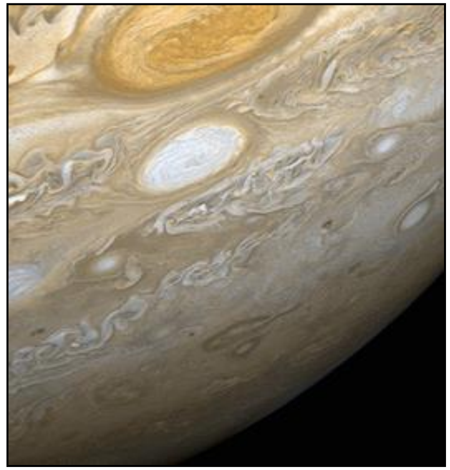
camera rate:

100,000 bits/second

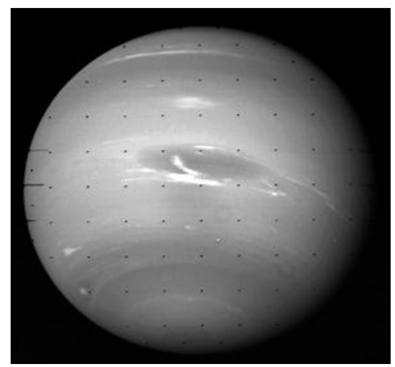
transmission speed:
16,000 bits/second

1979+: Voyagers I & II

- Voyagers I & II used a [24,12,8] *Golay* code to send its color images of Jupiter and Saturn.

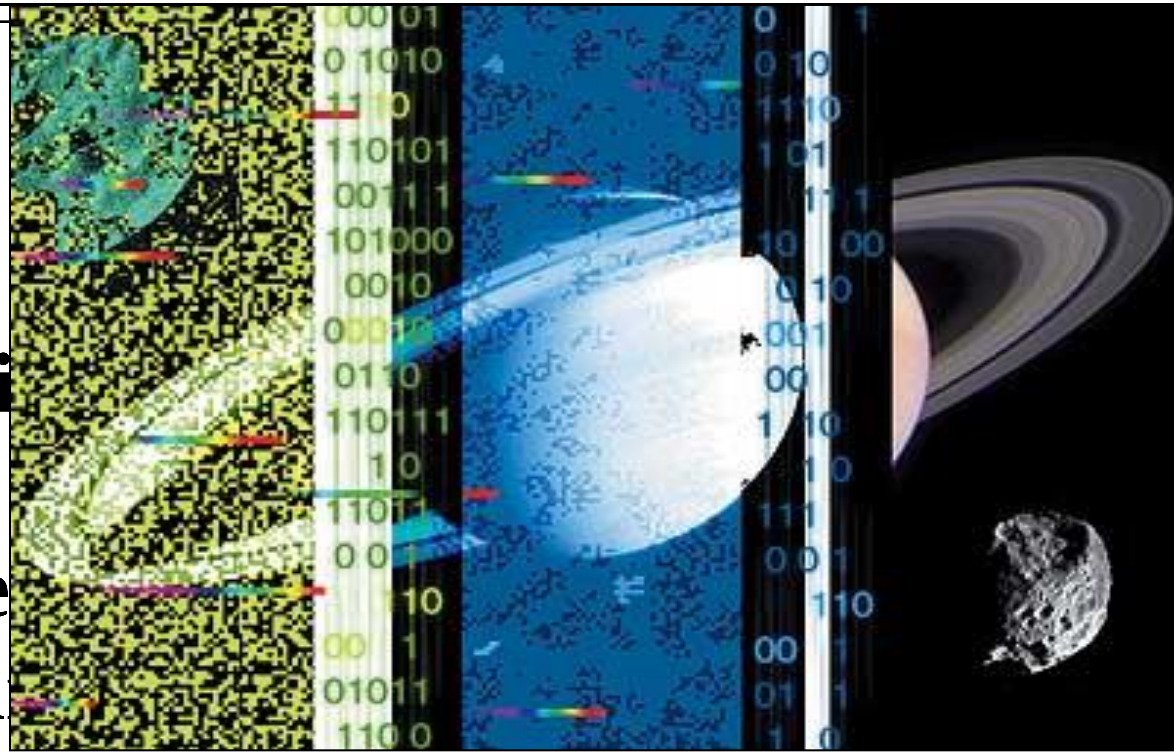




- Voyager 2 traveled further to Uranus and Neptune. Because of the higher error rate it switched to the more robust *Reed-Solomon* code.



Modern Codes

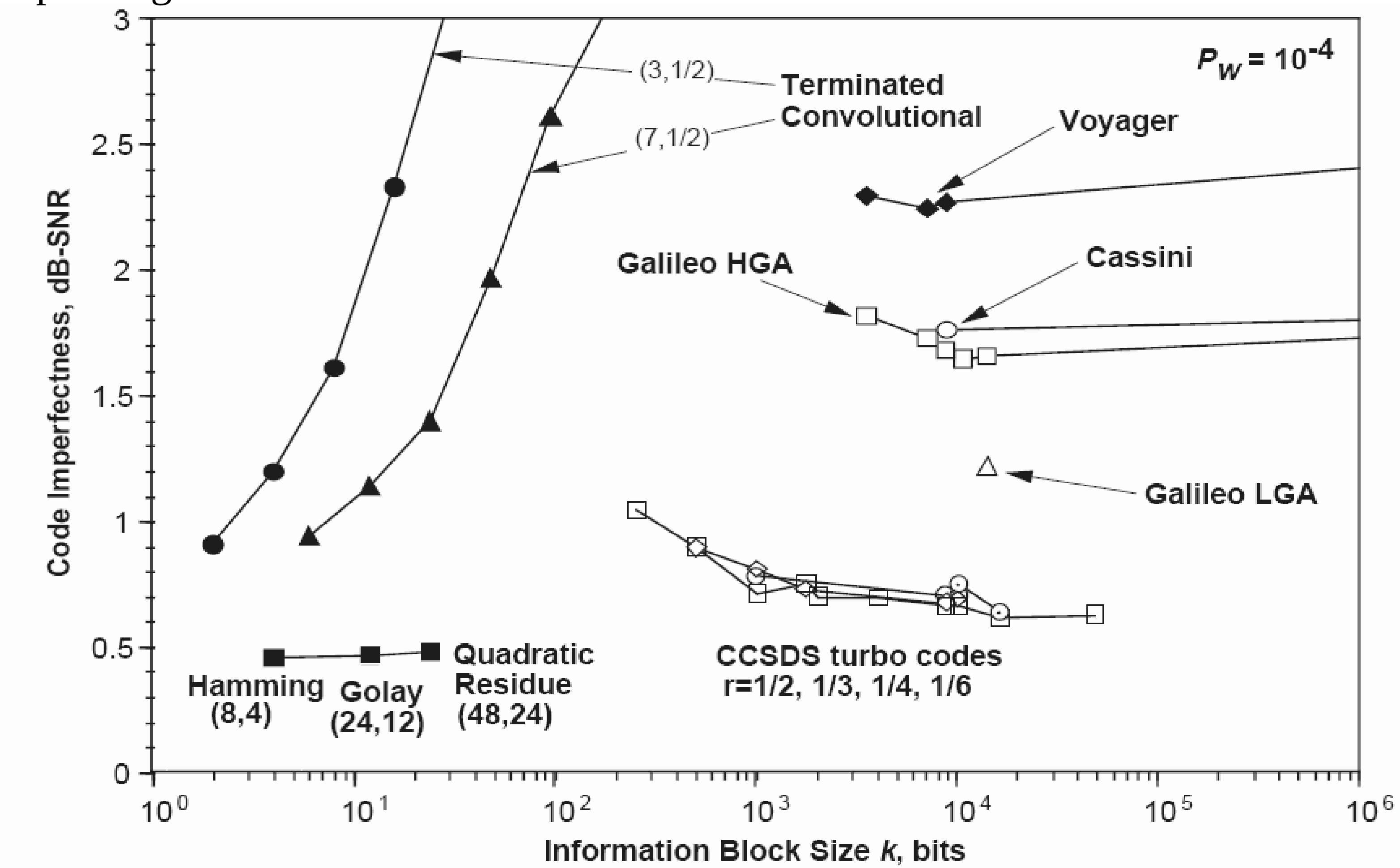
More recently
Turbo codes
were invented,
which are used i
3G cell phones,
(future) satellite
and in the Cassi
Huygens space
probe [1997–].



Other modern codes: Fountain, Raptor, LT, online

Error Correcting Codes

imperfectness of a given code as the difference between the code's required Eb/No to attain a given word error probability (Pw), and the minimum possible Eb/No required to attain the same Pw, as implied by the sphere-packing bound for codes with the same block size *k* and code rate *r*.



References

[1] T. S. Rappaport, *Wireless Communications -- Principles and Practice*, Prentice Hall Inc., New Jersey, 1996.

[2] S.U.H. Qureshi, "Adaptive equalization, " *Proceeding of IEEE*, vol. 37 no.9, pp.1340 -- 1387, Sept. 1985.

[3] J. R. Treichler, and B.G. Agoe, "A new approach to multipath correction of constant modulus signals, " *IEEE Trans. Acoustics, Speech, and Signal Processing*, vol. ASSP--31, pp. 459--471, 1983

[4] W. A. Gardner, "Exploitation of spectral redundancy in cyclostationary signals, " *IEEE Signal Processing Magazine*, pp. 14-- 36, April 1991.

[5] I.Korn, *Digital Communications*, Van Nostrand Reinhold, 1985.

[6] J. Proakis, "Adaptive equalization for TDMA digital mobile radio, " *IEEE Trans. Commun.*, vol. 40, no.2, pp.333--341, May 1991.

[7] J. A. C. Bingham, *The Theory and Practice of Modem Design*, John Wiley & sons, New York.

[8] C. A, Belfiori, and J.H. Park, "Decision feedback equalization, " *Proceedings of IEEE*, vol. 67, pp. 1143--1156, Aug. 1979.

[9] K. Zhou, J.G. Proakis, F. Ling, "Decision feedback equalization of time dispersive channels with coded modulation, " *IEEE Trans. Commun.*, vol. 38, pp. 18--24, Jan. 1990.

References

[10] G. D. Forney, "The Viterbi algorithm, " *Proceedings of the IEEE*, vol.61, no.3, pp. 268--278, March 1978.

[11] B. Widrow, and S.D. Stearns, *Adaptive Signal Processing*, Prentice Hall, 1985.

[12] S. Haykin, *Adaptive Filter Theory*, Prentice Hall, Englewood Cliffs, NJ, 1986.

[13] T. Eng, N. Kong, and L. B. Milstein, "Comparison of Diversity Combining Techniques for Rayleigh-Fading Channels," *IEEE Trans. Commun*., vol. 44, pp. 1117-1129, Sep. 1996.

[14] W. C. Jakes, "A Comparision of Space Diversity Techniques for Reduction of Fast Fading in UHF Mobile Radio Systems," *IEEE Trans. Veh. Technol.*, vol. VT-20, No. 4, pp. 81-93,
Nov. 1971.

[15] L. Kahn, "Radio Square," *Proceedings of IRE*, vol. 42, pp. 1074, Nov. 1954.

[16] S. Kozono, *et al*, "Base Station Polarization Diversity Reception for Mobile Radio," *IEEE Trans. Veh. Technol.*, vol VT-33, No. 4, pp. 301-306, Nov. 1985.

[17] R. Price, P. E. Green, "A Communication Technique for Multipath Channel," *Proceeding of the IRE*, pp. 555-570, March 1958