Differential PSK (DPSK) and Its Performance

$$s(t) = A(t)\cos(2\pi f_c t + \theta(t) + \theta)$$

A(t) = amplitude information

θ (t) = phase information

f_c = the carrier frequency

θ = the phase shift introduced by the channel

- In coherent communications, θ is known to receivers
- In non-coherent communications, θ is unknown to receivers and assumed to be a random variable distributed uniformly over (-π, π)

Coherent Detection of Differentially Encoded M-PSK Signals

- In coherent communications, phase estimation is required.
- The receiver usually derives its frequency and phase demodulation references from a carrier synchronization loop.
- The synchronization loop may introduce a phase ambiguity $\phi = \hat{\theta} - \theta$ where $\hat{\theta}$ is the estimate acquired by the receiver through the synchronization loop.
- For M-PSK signals, the phase ambiguity Φ may take any value in

$$\{0, \frac{2\pi}{M}, \cdots \frac{2\pi(M-1)}{M}\}$$

Thus any value of Φ other than 0 will cause a correctly detected phase to be erroneously mistaken for one of the other possible phases, even in the absence of noise.

- Solution: differential encoding while maintaining coherent detection

Differentially Encoded M-PSK Signals

- Instead of encoding information into absolute phases, the information is now encoded using phase differences between successive signal transmission.

Example: 0 mapped to phase 0, 1 mapped to phase π

Binary sequence $\{a_n\}$	0	1 1 0 0 1 1
Absolute phase sequence $\{\Delta\theta_n\}$	0	π π 0 0 π π
Differentially encoded Phase sequence	0	π 0 0 0 π 0

The actually transmitted Phase sequence

Initial value

- The information sequence $\{a_n\}$ is now carried by phase difference in $\{\theta_n\}$.

Differentially Encoded M-PSK Signals

Binary sequence $\{a_n\}$	0	1 1 0 0 1 1
Absolute phase sequence $\{\Delta\theta_n\}$	0	π π 0 0 π π
Differentially encoded Phase sequence	0	π 0 0 0 π 0

The actually transmitted Phase sequence

Initial value

- Assume the phase ambiguity Φ introduced by the synchronization loop is constant during successive signal intervals. In the absence of noise, the receiver would convert the received phase sequence into 0+Φ, π+Φ, 0+Φ, 0+Φ, 0+Φ, π+Φ, 0+Φ.
- The received sequence would be then differentially decoded into π, π, 0, 0, π, π.
- Then we get the original binary sequence (110011) back.

Differentially Encoded M-PSK Signals

Example: M=4. Assume that the following Gray mapping is used

Binary sequence	00	10	11	01
absolute phase	0	π/2	π	3π/2

Binary sequence $\{a_n\}$	10	11	00	10	01	11
Absolute phase sequence $\{\Delta\theta_n\}$	π/2	π	0	π/2	3π/2	π
Differentially encoded phase sequence $\{\theta_n\}$	π/2	3π/2	3π/2	0	3π/2	π/2
Estimated phase sequence $\hat{\theta}_n$ (in the absence of noise)	π/2+Φ	3π/2+Φ	3π/2+Φ	0+Φ	3π/2+Φ	π/2+Φ
Differentially decoded sequence		π	0	π/2	3π/2	π
Decoded binary sequence $\hat{a}_n$		11	00	10	01	11

Φ ϵ { 0, π/2, π, 3π/2} is the phase ambiguity

The Structure of Differential Encoder and Decoder

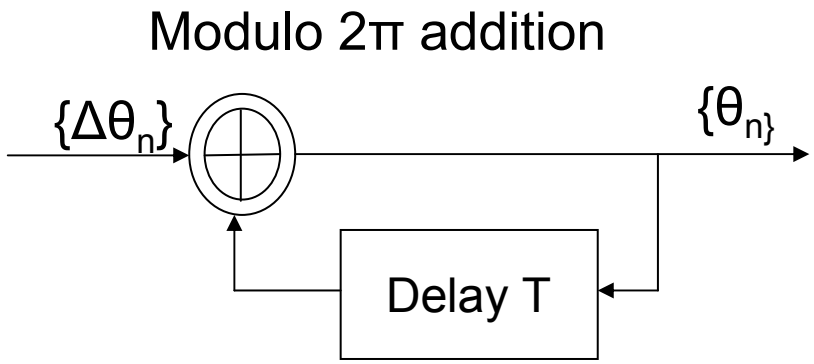


Figure a. A differential encoder

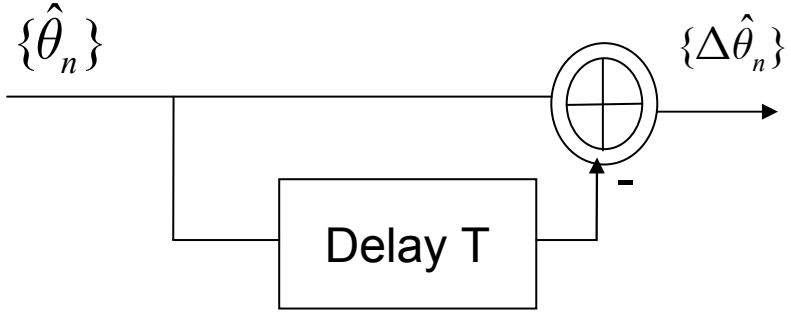


Figure b. A differential decoder

$\{\Delta\theta_n\}$ = the absolute phase sequence

$\{\theta_n\}$ = the transmitted phase sequence

A digital comm. system that employ differential encoding of the inform. Symbols and coherent detection of successive differentially encoded M-PSK signals is called a differentially encoded coherent M-PSK system.

Optimal Coherent Receiver for Differentially Encoded M-PSK

$$r(t) = \sqrt{\frac{2E_s}{T}}\cos(2\pi f_c t + \theta_n + \theta)$$

$nT \le t \le (n+1)T, \quad n = 0, \pm 1, \pm 2, \cdots$

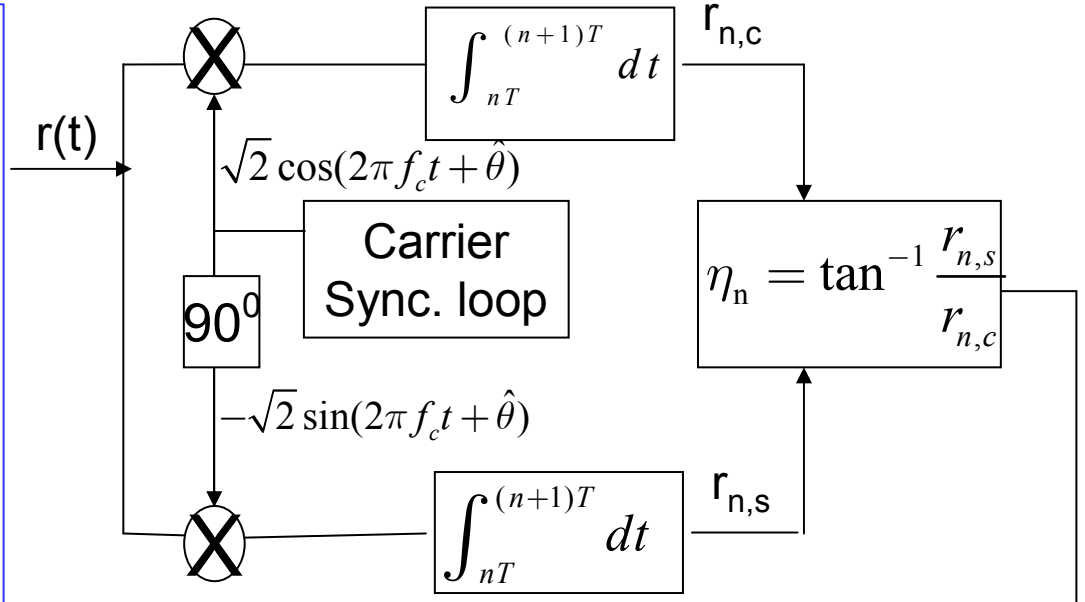
θ = phase shift introduced by the channel

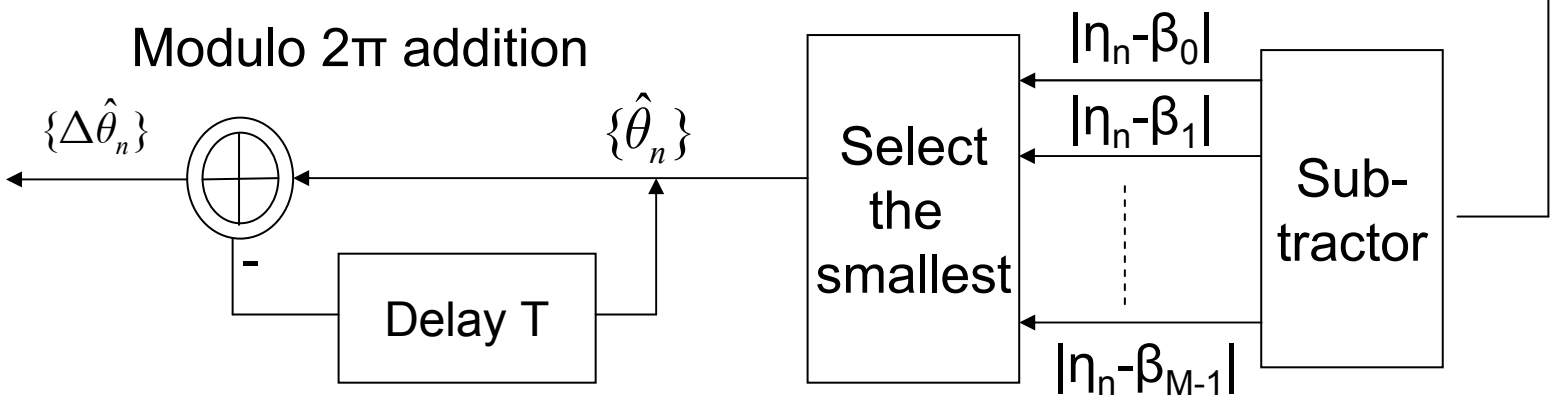
$\hat{\theta}$ = estimate of θ provided by carrier synch. loop

$\phi = \theta - \hat{\theta} =$ the phase ambiguity

$\Delta\theta_n = \theta_n - \theta_{n-1}$,

$\{\Delta\theta_n\}$ represents the inform. sequence





Performance

Let P_i denote $\Pr\{\hat{m} = m_i \mid m = m_0\}$ in the optimal coherent receiver fro M-PSK.

$$P_0 = 1 - \frac{1}{\pi}\int_0^{\pi - \frac{\pi}{M}} \exp\{-\frac{E_s \sin^2\frac{\pi}{M}}{N_0 \sin^2\alpha}\} d\alpha$$

$$E_s = \text{energy/symbol.}$$

One can show that the prob. of correct decision in the optimal coherent receiver for differentially encoded M-PSK is

$$P_c = \sum_{i=0}^{M-1} P_i^2$$

$$\Rightarrow P_e = 1 - P_c = 1 - \sum_{i=0}^{M-1} P_i^2$$

Since $P_i < P_0$ for $i \neq 0$, it follows that

$$P_c < \sum_{i=0}^{M-1} P_o P_i = P_0 = P_C\,|_{\text{coherent M-PSK}}$$

The symbol error

$P_e > P_e|_{\text{coherent M-PSK}}$

$$P_e = 1 - P_0^2 - \sum_{i=1}^{M-1} P_i^2$$

$$= 2P_{e|M-PSK} - (P_{e|M-PSK})^2 - \sum_{i=1}^{M-1} P_i^2$$

Differential PSK (DPSK)

- The phase shift is treated as a random variable distributed uniformly over (-π, π), and no phase estimation is provided at the receiver.
- We are now concerned with non-coherent communications
- The phase shift θ is the same during two consecutive signal transmission intervals [*(n-1)T*, *nT*) and [*nT, (n+1)T*).
- The information phase sequence $\{\Delta\theta_n\}$ is still differentially encoded as before.
- The transmitted signal *s(t)* in the interval [*(n-1)T, (n+1)T*] is

$$s(t)=\begin{cases}\sqrt{\dfrac{2E_s}{T}}\cos(2\pi f_c t+\theta_{n-1}+\theta), & (\text{n-1})\text{T}\le t<\text{nT}\\ \sqrt{\dfrac{2E_s}{T}}\cos(2\pi f_c t+\theta_n+\theta), & \text{nT}\le t<(\text{n+1})\text{T}\end{cases}$$

- $\Delta\theta_n=\theta_n-\theta_{n-1}$. θ_n and θ_{n-1} are independent. Both of them take values uniformly over

$$\left\{0,\frac{2\pi}{M},\cdots\frac{2\pi(M-1)}{M}\right\}$$

- $\{\Delta\theta_n\}$ and $\{\theta_n\}$ are i.i.d. sequences

Differential PSK (DPSK)

- The received waveform is then *r(t)=s(t)+n(t)*
- To derive the optimal receiver, the observation interval should be taken as *(n-1)T* $\leqslant$ *t* <*(n+1)T* since θ is the same in this interval.
- We have four orthonormal basis functions:

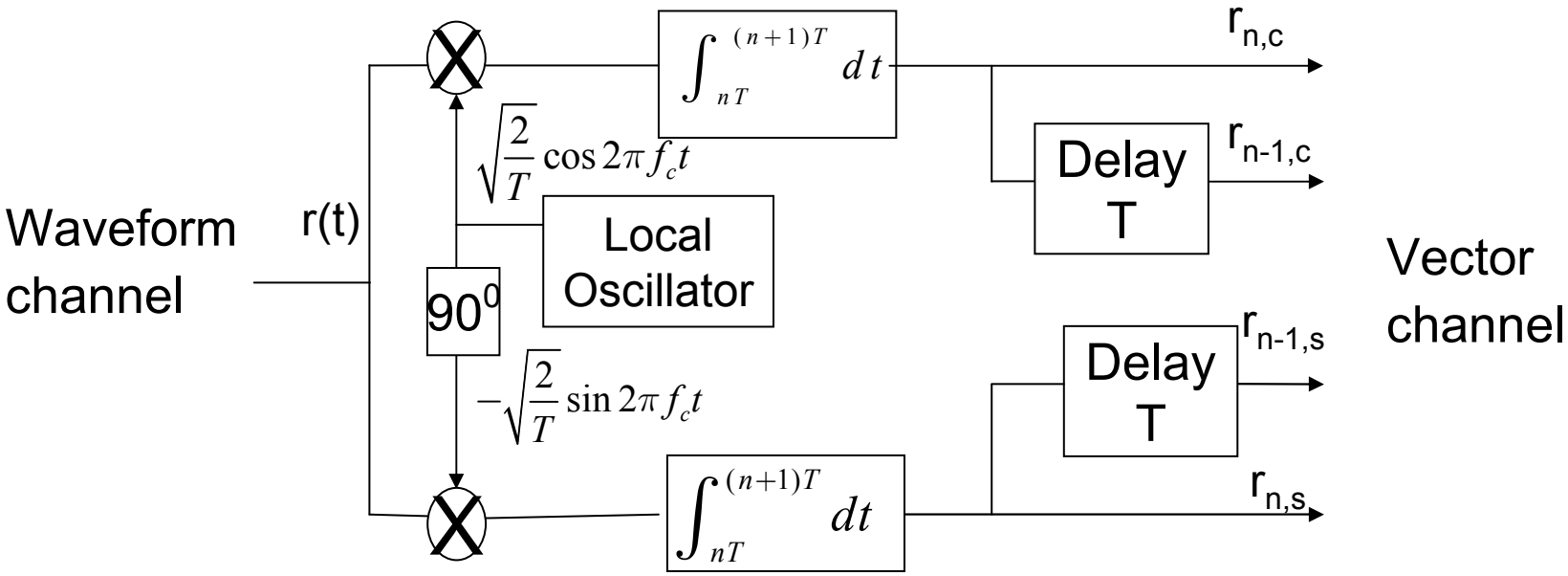
$$\phi_1(t)=\begin{cases}\sqrt{\frac{2}{T}}\cos 2\pi f_c t & (n-1)T \le t \le nT \\ 0 & nT < t \le (n+1)T\end{cases}$$

$$\phi_2(t)=\begin{cases}-\sqrt{\frac{2}{T}}\sin 2\pi f_c t & (n-1)T \le t \le nT \\ 0 & nT < t \le (n+1)T\end{cases}$$

$$\phi_3(t)=\begin{cases}0 & (n-1)T \le t \le nT \\ \sqrt{\frac{2}{T}}\cos 2\pi f_c t & nT < t \le (n+1)T\end{cases}$$

$$\phi_4(t)=\begin{cases}0 & (n-1)T \le t \le nT \\ -\sqrt{\frac{2}{T}}\sin 2\pi f_c t & nT < t \le (n+1)T\end{cases}$$

Differential PSK (DPSK)



$$r_{n,c} = \sqrt{E_s}\cos(\theta_n + \theta) + \eta_{n,c},\ r_{n,s} = \sqrt{E_s}\sin(\theta_n + \theta) + \eta_{n,s}$$

$\eta_{n,c}, \eta_{n,s}, \eta_{n-1,c}, \eta_{n-1,s}$ are i.i.d

Each of them $\sim$ N(0, $N_0/2$)

We estimate $\Delta\theta_n$ from the new observation ($r_{n,c}$, $r_{n,s}$, $r_{n-1,c}$, $r_{n-1,s}$)

Differential PSK (DPSK)

Let $\beta_i = \frac{2\pi i}{M}, 0 \le i \le M-1.$

Given $\Delta\theta_n = \beta_i, \theta_{n-1}, \text{and } \theta$

$$P(r_{n,c}, r_{n,s}, r_{n-1}, c, r_{n-1,s} \mid \Delta\theta_n = \beta_i, \theta_{n-1,}\theta)$$

$$= \frac{1}{(\pi N_0)^2} \exp\left\{ -\frac{\sum_{j=n-1}^{n} [(r_{j,c} - \sqrt{E_s}\cos(\theta_j + \theta)]^2 + [(r_{j,s} - \sqrt{E_s}\sin(\theta_j + \theta)]^2}{N_0} \right\}$$

$$= c \exp\left\{ -\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\theta_n} + r_{n-1} \mid \cos(\theta - \alpha) \right\}$$

1) c does not depend on θ, θ_{n-1} and $\Delta\theta_n$
2) $r_n = r_{n,c} + jr_{n,s}$ and $r_{n-1}=r_{n-1,c} + jr_{n-1,s}$
3) α is given by $r_n e^{-j\theta n} + r_{n-1} e^{-j\theta n-1} = | r_n e^{-j\theta n} + r_{n-1} | e^{j\alpha}$

Differential PSK (DPSK)

θ is distributed uniformly over (-π, π) and θ_{n-1} tales values uniformly over $\{0, \frac{2\pi}{M}, \cdots, \frac{2\pi(M-1)}{M}\}$

$$P(r_{n,c}, r_{n,s}, r_{n-1,c}, r_{n-1,s} \mid \Delta\theta_n = \beta_i, \theta_{n-1,})$$

$$= \frac{1}{2\pi}\int_{-\pi}^{\pi} c \exp\{\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\theta_n} + r_{n-1} \mid \cos(\theta - \alpha)\} d\theta$$

$$= cI_0(\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\theta_n} + r_{n-1} \mid) = cI_0(\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\beta_i} + r_{n-1} \mid)$$

where $I_0(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{x\cos y} dy$ is modified Bessel function

The above formula is independent of θ_{n-1}

$$\Rightarrow P(r_{n,c}, r_{n,s}, r_{n-1,c}, r_{n-1,s} \mid \Delta\theta_n = \beta_i) = cI_0(\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\beta_i} + r_{n-1} \mid)$$

Differential PSK (DPSK)

Applying the MAP rule, we now

choose $\Delta\hat{\theta}_n$ as β_k iff

$$P(r_{n,c}, r_{n,s}, r_{n-1,c}, r_{n-1,s} \mid \Delta\theta_n = \beta_k) = \max_i P(r_{n,c}, r_{n,s}, r_{n-1,c}, r_{n-1,s} \mid \Delta\theta_n = \beta_i)$$

$$\Leftrightarrow I_0\left(\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\beta_k} + r_{n-1} \mid\right) = \max_i I_0\left(\frac{2\sqrt{E_s}}{N_0} \mid r_n e^{-j\Delta\beta_i} + r_{n-1} \mid\right)$$

$(x > 0, I_0(x)$ is an increasing function)

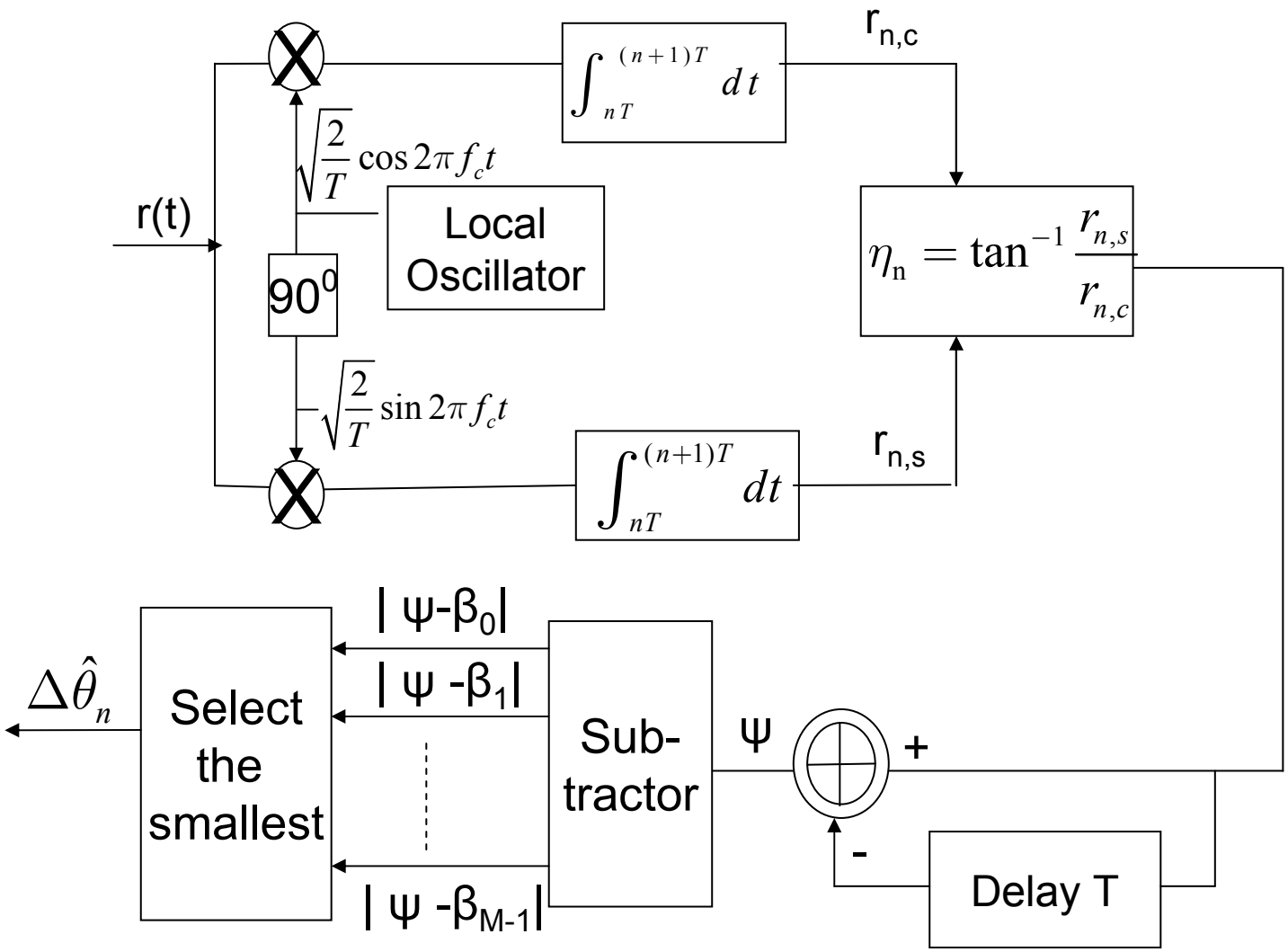
$$\Leftrightarrow \mid r_n e^{-j\Delta\beta_k} + r_{n-1} \mid = \max_i \mid r_n e^{-j\Delta\beta_i} + r_{n-1} \mid$$

$$\Leftrightarrow \mid r_n \mid \mid r_{n-1} \mid \cos(\eta_n - \eta_{n-1} - \beta_k) = \max_i [\mid r_n \mid \mid r_{n-1} \mid \cos(\eta_n - \eta_{n-1} - \beta_i)]$$

$$\Leftrightarrow \mid \eta_n - \eta_{n-1} - \beta_k \mid = \min_i \mid \eta_n - \eta_{n-1} - \beta_i \mid$$

where $r_n = \mid r_n \mid e^{j\eta_n}$ and $r_{n-1} = \mid r_{n-1} \mid e^{j\eta_{n-1}}$

Optimal Receiver for M-DPSK



Difference from the receiver for differentially encoded M-PSK?

Performance of M-DPSK

$$r_{n,c} = \sqrt{E_s}\cos(\theta_n + \theta) + \eta_{n,c} = \sqrt{E_s}\cos(\theta_{n-1} + \Delta\theta_n + \theta) + \eta_{n,c}$$

$$r_{n,s} = \sqrt{E_s}\sin(\theta_{n-1} + \Delta\theta_n + \theta) + \eta_{n,s}$$

$$r_{n-1,c} = \sqrt{E_s}\cos(\theta_{n-1} + \theta) + \eta_{n-1,c}$$

$$r_{n-1,s} = \sqrt{E_s}\sin(\theta_{n-1} + \theta) + \eta_{n-1,s}$$

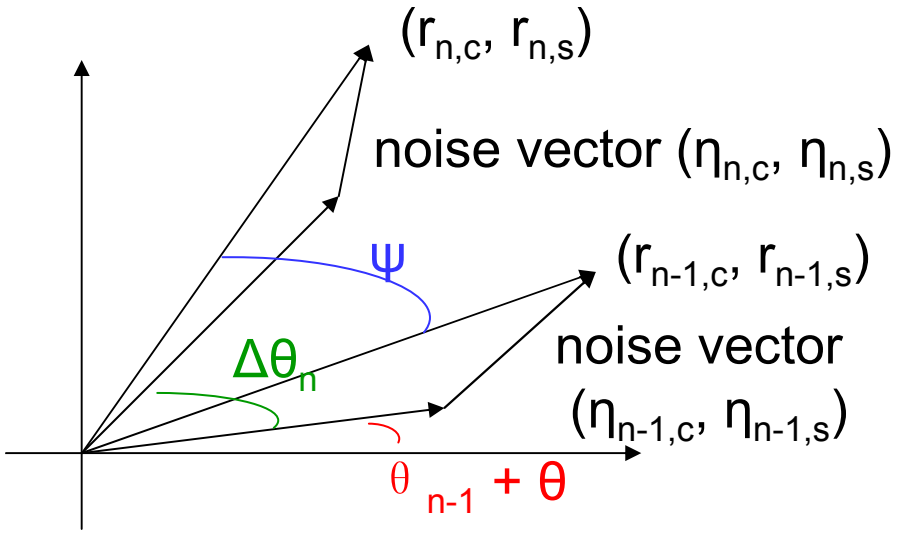
$$\eta_{n,c}, \eta_{n,s}, \eta_{n-1,c}, \eta_{n-1,s} \sim \mathrm{N}(0, \frac{\mathrm{N}_0}{2} I_{4x4})$$

One way to calculate the performance of M-DPSK is to find first the pdf of phase difference

$$\psi = \eta_n - \eta_{n-1}$$

$$\eta_n = \tan^{-1}\frac{r_{n,s}}{r_{n,c}}, \text{and } \eta_{n-1} = \tan^{-1}\frac{r_{n-1,s}}{r_{n-1,c}}$$

Performance of M-DPSK



It follows that the pdf of ψ is independent of the angle $\theta_{n-1}+\theta$. It can be shown that the conditional pdf of ψ given $\Delta\theta_n$ satisfies the following equation

$$P(\psi_1 \le \psi \le \psi_2 \mid \Delta\theta_n) = \int_{\psi_1}^{\psi_2} f_\psi(\psi \mid \Delta\theta_n) d\psi$$

$$= \begin{cases} F_{\Delta\theta_n}(\psi_2) - F_{\Delta\theta_n}(\psi_1) + 1 & \psi_1 < \Delta\theta_n < \psi_2 \\ F_{\Delta\theta_n}(\psi_2) - F_{\Delta\theta_n}(\psi_1) & \psi_1 > \Delta\theta_n \text{ or } \Delta\theta_n > \psi_2 \end{cases}$$

$$F_{\Delta\theta_n}(\psi) = \frac{\sin(\Delta\theta_n - \psi)}{4\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\exp\{-\frac{E_s}{N_0}[1 - \cos(\Delta\theta_n - -\psi)\cos t]\}}{1 - \cos(\Delta\theta_n - \psi)\cos t} dt$$

Performance of M-DPSK

We then get

$$P(\Delta\hat{\theta}_n = \beta_i \mid \Delta\theta_n = \beta_i)$$

$$= P(\beta_i - \frac{\pi}{M} \le \psi \le \beta_i + \frac{\pi}{M} \mid \Delta\theta_n = \beta_i)$$

$$= F_{\beta_i}(\beta_i + \frac{\pi}{M}) - F_{\beta_i}(\beta_i - \frac{\pi}{M}) + 1$$

$$= 1 - \frac{\sin\frac{\pi}{M}}{4\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\exp\{-\frac{E_s}{N_0}(1-\cos\frac{\pi}{4}\cos t]\}}{1-\cos\frac{\pi}{M}\cos t}dt$$

$$\Rightarrow P_c = 1 - \frac{\sin\frac{\pi}{M}}{4\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\exp\{-\frac{E_s}{N_0}(1-\cos\frac{\pi}{4}\cos t]\}}{1-\cos\frac{\pi}{M}\cos t}dt$$

$$\Rightarrow P_e = \frac{\sin\frac{\pi}{M}}{4\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\exp\{-\frac{E_s}{N_0}(1-\cos\frac{\pi}{4}\cos t]\}}{1-\cos\frac{\pi}{M}\cos t}dt$$

Special case

- M=2

$$P_b = P_e = 1/2 e^{-E_b/N_0}$$

- For large M, M-DPSK requires 3dB more Eb/N0 than coherent M-PSK

Comparison of Digital Modulation Methods

- To make a fair comparison among different digital modulation methods, one must investigate the tradeoff among the bandwidth efficiency, bit error probability, and bit SNR.
- The bandwidth efficiency of a modulation method is defined as the bit rate (R_b) to bandwidth (W) ratio R_b/W
- The bandwidth is calculated from the power spectral density function of the transmitted waveform, which in turn depends on the signal set used.

Comparison of Digital Modulation Methods

Assume that the optimal signal set is used.

Theorem 3.7.1: The maximum number N of dimension of the signal source spanned by a set of signals of duration of T and “bandwidth” W grows linearly with time T and bandwidth W, respectively:

$$N=KWT$$

where K is a constant around 2.

The value of K depends on specific definitions of bandwidth. We normally choose K=2.

Examples

PAM signals: N=1 => W=1/(2T) (single sideband)

The bandwidth efficiency of M-ary PAM is

$$\frac{R_b}{W} = \frac{\log M / T}{1/2T} = 2\log M \text{ bits/second/Hz}$$

M-PSK: N=2 => W=1/T

$$\frac{R_b}{W} = \frac{\log M / T}{1/T} = \log M \text{ bits/second/Hz}$$

M^2-QAM: N=2 => W=1/T

$$\frac{R_b}{W} = \frac{\log M^2 / T}{1/2T} = 2\log M \text{ bits/second/Hz}$$

M-FSK: N=M => W=M/(2T)

$$\frac{R_b}{W} = \frac{\log M / T}{M/2T} = \frac{2\log M}{\mathrm{M}} \text{ bits/second/Hz}$$

As M approaches infinity, R_b/W goes to 0

Comparison of Digital Modulation Methods

- In the case of PAM, QAM, and PSK, increasing M results in a higher bit rate-to-bandwidth ratio R/W.
- However, the cost of achieving the higher data rate is an increase in the SNR per bit.
- Therefore, these modulation methods are appropriate for channels that are bandlimited, where we desire R/W>1 and where there is sufficient high SNR to support increases in M.
- Example: Telephone channels

Comparison of Digital Modulation Methods

- M-ary orthogonal signals yields $R/W \leqslant 1$. As M increases, R/W decreases.
- However, the SNR/bit required to achieve a given error probability (10^{-5}) decreases as M increases.
- Consequently, M-ary orthogonal signals are appropriate for power-limited channels that have sufficiently large bandwidth to accommodate a large number of signals.
- As M goes to infinity, Pe approaches zero provided that SNR/bit $\geqslant$ -1.6 dB

Digital Communication Block Diagram
数字通信系统框图

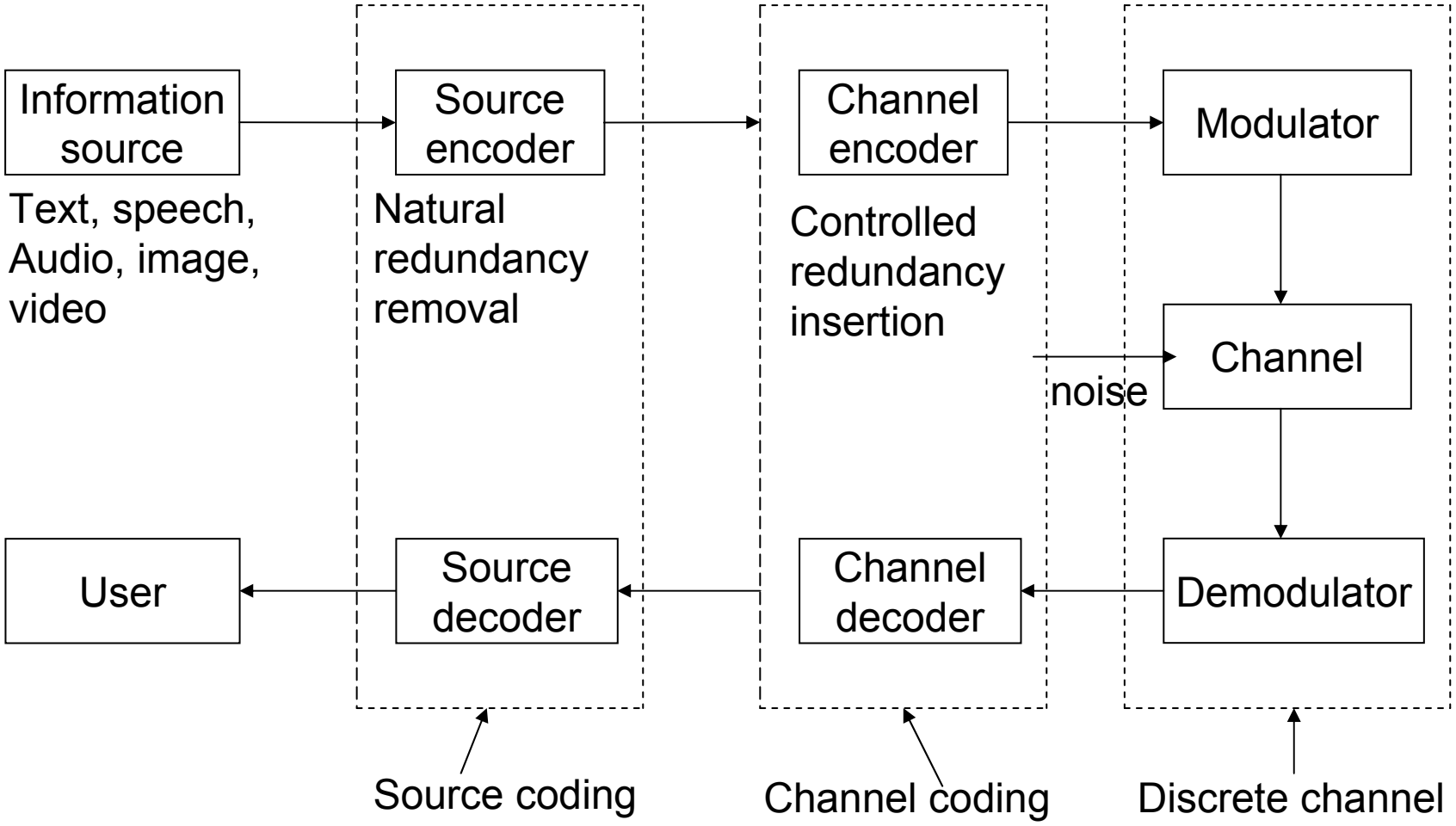
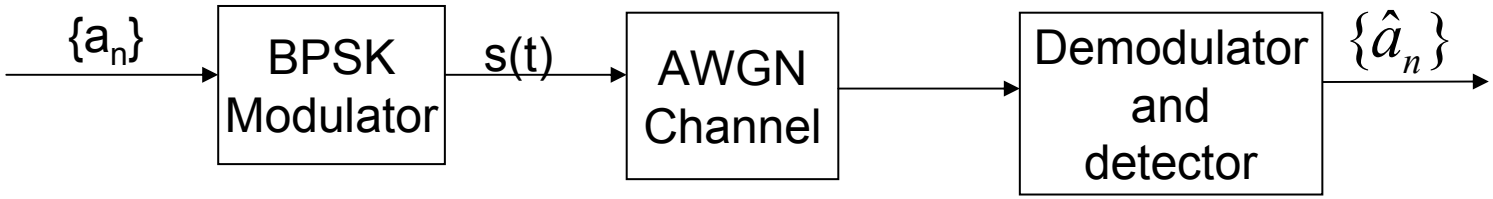


Fig 1.1 数字通信系统框图

Channel Capacity and Coded Modulation

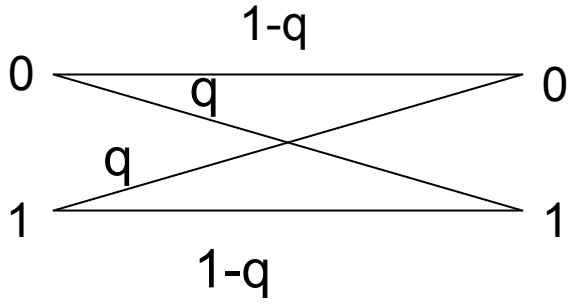
Channel Models and Channel Capacity

Binary Symmetric Channels



Assume that a_n=0 or 1, i.i.d, and symbol 0 and 1 are equally likely. Then

$$P_b = P(\hat{a}_n \neq a_n) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$



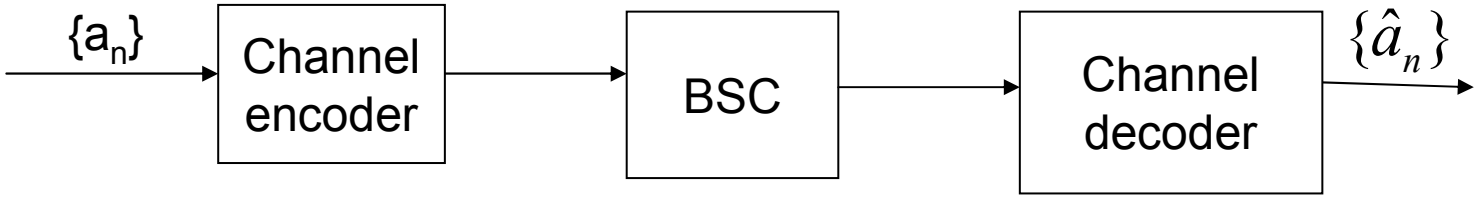
Equivalent diagram

Binary Symmetric Channels

$$P(\hat{a}_1\hat{a}_2\cdots\hat{a}_n \neq a_1a_2\cdots a_n) = 1-[1-p_b]^n$$

For any fixed bit SNR E_b/N_0, the block error prob. goes to 1 as n approaches infinity.

In order to transmit information reliably over the BSC, one has to employ channel encoders and decoders.



An important question: with the use of channel encoders and decoders, how many number of bits of information can be reliably transmitted over the BSC?

The answer is the channel capacity of the BSC.

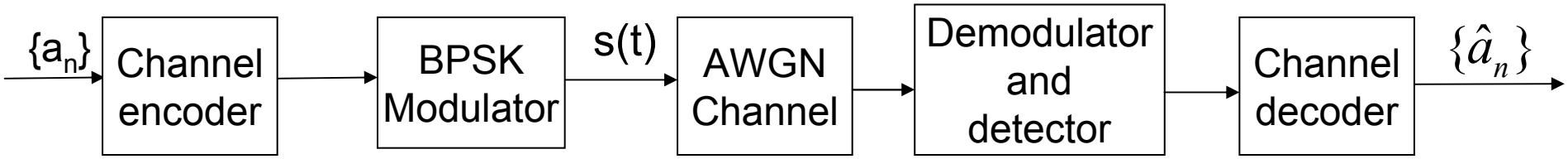
Channel Capacity of the BSC

$$C = \max_{X} I(X;Y)$$

X is the input random variable to the BSC, Y is the corresponding output. The maximization is taken over all possible input random variable X.

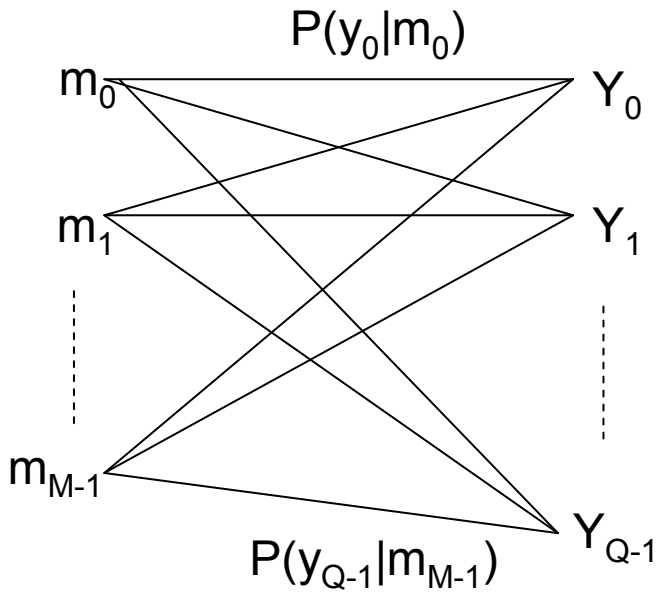
For BSC, C = 1 – H(q) with the maximum achieved by the equally likely input X.

Channel Capacity of the BSC



- The concatenation of the channel encoder and BPSK modulator is a binary coded modulation scheme and gives binary coded signals.
- The BPSK detector is not optimal any more since coded signals are correlated and the BPSK makes a hard decision (0 or 1) bit by bit.
- To improve the performance, we may consider a detector that outputs Q>2 outputs. That is, a detector quantizes the demodulator output into Q>2 outputs (or no quantization). In this case, we say that the detector has made a soft decision.
- With a detector making a soft decision, we get an equivalent discrete channel with two inputs and Q>2 possible outputs.

Discrete Memoryless Channels



A general discrete channel

- With any M-ary modulator and a soft (or hard) decision detector, we get an equivalent discrete channel with M inputs and Q $\geqslant$ M possible outputs.
- The maximum number of bits of information that can be reliably transmitted over the channel is given by channel capacity

$$C = \max_{X} I(X;Y)$$

Discrete Input, Continuous-Output Channels

- The demodulator converts the received waveform into scalar vectors, no estimation is made at this point. The corresponding composite channel is then equivalent to the scalar channel

$$Y = X + n$$

- X takes values in the amplitude set of the PAM modulator
- n is a Gaussian random variable with n ~ N(0, $N_0/2$)
- Channel capacity

$$C = \max_X I(X;Y)$$

- The modulator is given, but coded PAM signal and their receiver including the detector and channel decoder are left open.

Band-limited, power-limited AWGN channels

Assume the channel is band limited and power limited

$$r(t) = x(t) + n(t)$$

$x(t)$ is the input waveform band-limited to W and power-limited to P

$n(t)$ = the AWGN with $S_n(f) = N_0/2$.

To compute the channel capacity, we first convert the waveform channel into discrete time Gaussian channel.

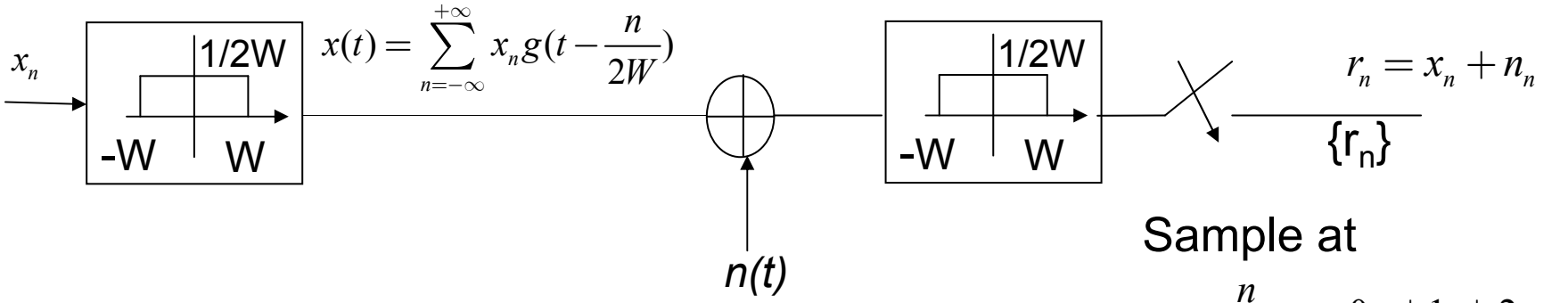
$$x(t) = \sum_{n=-\infty}^{+\infty} x_n g(t - \frac{n}{2W})$$

$$x_n = x(\frac{n}{2W}),\ g(t) = \sin c2Wt = \frac{\sin 2\pi wt}{2\pi wt}$$

This is equivalent to projecting $x(t)$ into the space spanned by the orthonormal basis $\{\sqrt{2W}\, g(t - \frac{n}{2W})\}_{-\infty}^{+\infty}$:

$$x_n = 2w \int_{-\infty}^{+\infty} x(t) g(t - \frac{n}{2W}) dt$$

Band-limited, power-limited AWGN channels



$\{n_i\}_{-\infty}^{+\infty}$ is i.i.d and each n_i is Gaussian, $n_i \sim N(0, N_0W)$

Since *x(t)* is power-limited to P, each sample x_n is then energy limited to P. The channel capacity C_N per use of the discrete-time Gaussian channel is

$C_N = max\ \{I(X_n; r_n: X_n \text{ is an input with } E[x_n^2] \le P\} = \frac{1}{2}\log(1 + \frac{P}{N_0W})$

During T seconds, we have 2WT samples, and the discrete-time channel is used 2WT times. Thus, the channel capacity C in bits per second is

$$C = 2W \times C_N = W \log(1 + \frac{P}{N_0W}) \text{ bits/second}$$

Bandwidth Efficiency versus Bit SNR

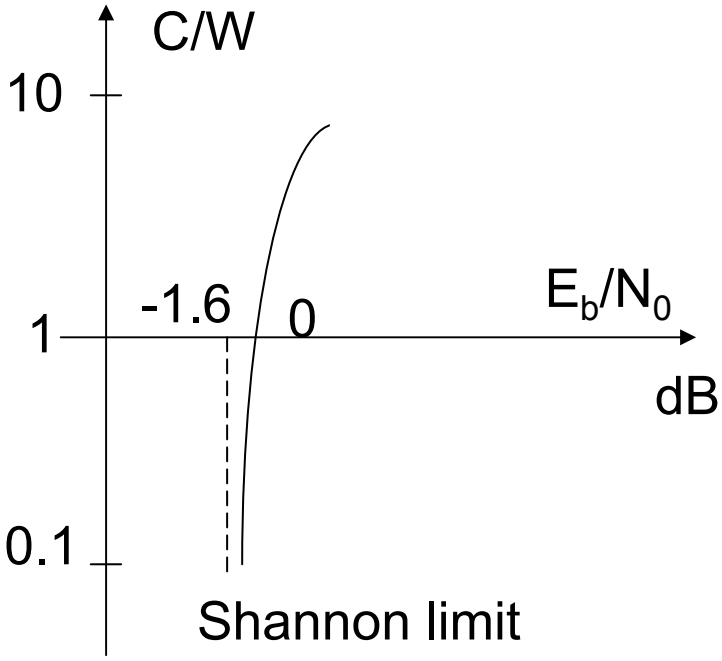
$$\frac{C}{W} = \log(1 + \frac{P}{N_0 W}) = \log(1 + \frac{E_b C}{N_0 W})$$

$$P = \text{Energy/second} = E_b C$$

$$\Rightarrow \frac{E_b}{N_0} = \frac{2^{C/W} - 1}{C/W}$$

E_b/N_0 bit SNR

C/W bandwidth efficiency



Ideal diagram of bandwidth efficiency versus bit SNR

Bandwidth Efficiency versus Bit SNR

1) Let $W \to \infty$, we have

$$C_\infty = \frac{P}{N_0} \log e \text{ bits/second}$$

$$\frac{\mathrm{E_b}}{\mathrm{N_0}} = \lim_{C/W->0} \frac{2^{C/W} - 1}{C/W} = \ln 2 \approx -1.6dB$$

2) In order to achieve essentially error free transmission, E_b/N_0 must be $\geqslant$-1.6 dB (Shannon limit)

3) An transmission rate $R_b < C$ is achievable, any rate $R_b > C$ is not achievable (Shannon noisy channel coding theorem)

4) The proof of noise channel coding theorem involves the well-known random coding argument

Achieving Channel Capacity with Orthogonal Signals

$$P_e = \begin{cases} 2 \bullet 2^{-T\left(\frac{C_\infty}{2} - R_b\right)} & \text{if } 0 \le \mathrm{R_b} \le \mathrm{C}_\infty/4 \\ 2 \bullet 2^{-T\left(\sqrt{C_\infty} - \sqrt{R_b}\right)^2} & \text{if } \mathrm{C}_\infty/4 \le \mathrm{R_b} \le \mathrm{C}_\infty \end{cases}$$

- The error probability can be made arbitrarily small as T goes to infinity (M goes to infinity for a fixed bit rate R_b = log M/T).
- For a power-limited AWGN channel with unbounded bandwidth orthogonal signaling (or M-FSK) is asymptotically optimal in the sense that the corresponding (symbol) error probability goes to o exponentially as M goes to infinity if the bit rate R_b = log M/T is less than the channel capacity.

Coded Modulation-A Probabilistic Approach

- Although orthogonal signaling is asymptotically optimal, there is a considerable gap between the performance of practical uncoded communication systems and the optimal performance theoretically achievable given by the noisy channel coding theorem.
- To reduce the gap, one must resort to coded modulation.
  - Algebraic approach (specific coding design techniques)
  - Probabilistic approach (analysis of the performance of a general class of coded signals)

Random Coding Based on M-ary Binary Coded Signals

- Objective
  - Design a binary code ***C*** consisting of M binary codewords $C_i=(C_{i1},C_{i2},\cdots, C_{in})$, $0 \leqslant i \leqslant M-1$
  - The corresponding coded signals $\{s_i(t)\}$ gives good error prob. performance

$$s_i(t) = (2C_{ij} - 1)\sqrt{\frac{2\varepsilon_c}{T_b}} \cos 2\pi f_c t,\ 1 \le j \le n,\ t \in [(j\text{-}1)Tc, jTc]$$

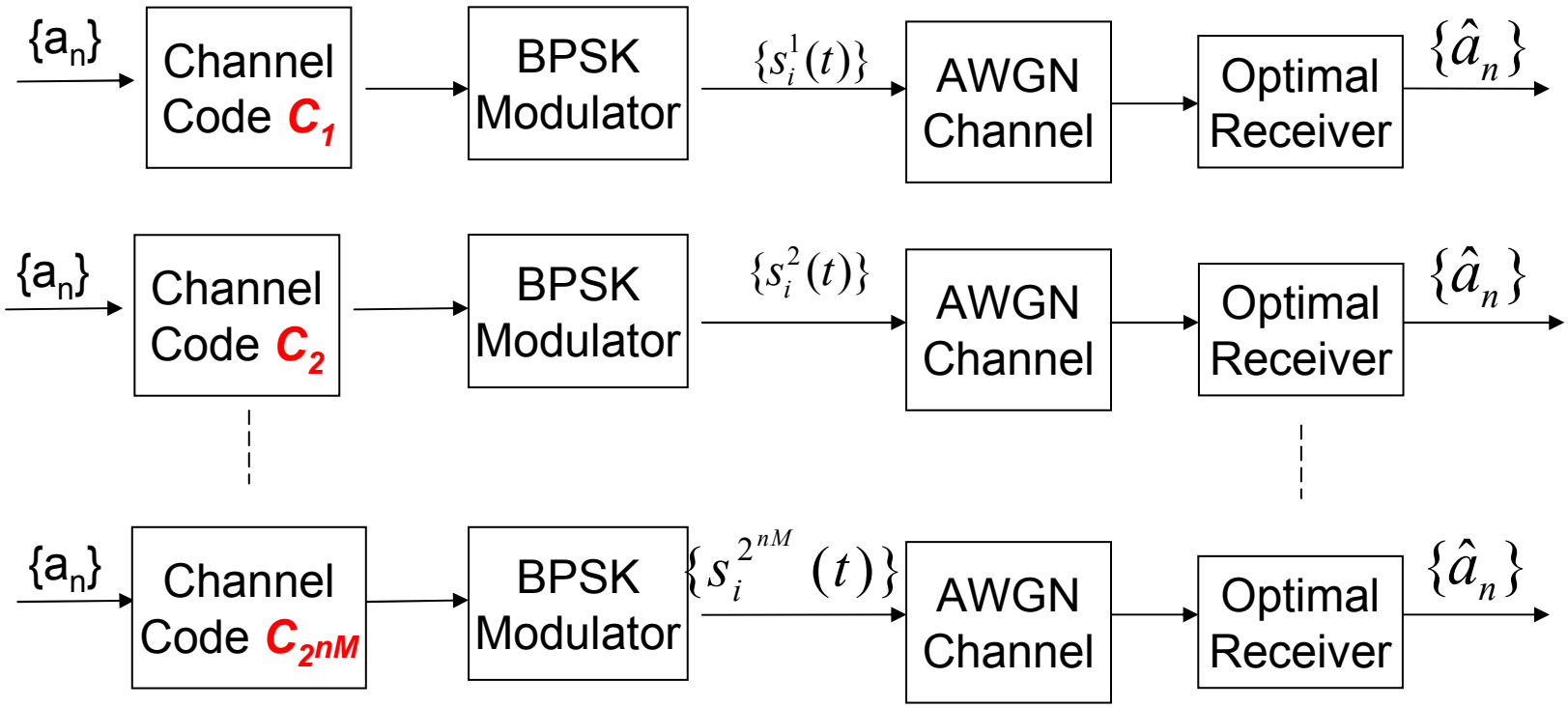
$$\underline{s}_i = [(2C_{i1} - 1), \cdots, (2C_{in} - 1)]\sqrt{\varepsilon_c}$$

- The encoding bit rate is R_b bits/second
- Blocks of k bits are encoded at a time into one of the M waveforms $\{s_i(t)\}_{i=0}^{M-1}$, $M = 2^k = 2^{RbT}$
- Assume $R_b<1/T_c$, $T=nT_c$. This implies that k < n, and

$$\frac{M}{2^n} = \frac{2^k}{2^n} = 2^{-(n-k)} = 2^{-T(D-R_b)},\ D = 1/T_c$$

Random Coding Based on M-ary Binary Coded Signals

- We consider the ensemble of $(2^n)^M$ distinct ways in which we can select M codewords from the total 2^n possible binary sequences.
- Associated with each of the $(2^n)^M$ binary codes, there is a coded communication system.



Random Coding Based on M-ary Binary Coded Signals

- Instead of evaluating the error prob. $P_e\{\{s_i^j(t)\}\}$ of each coded system individually, we compute the average error prob. of the 2^{nM} coded communication systems:

$$\bar{P}_e = \frac{1}{2^{nM}} \sum_{j=1}^{2^{nM}} P_e\{\{s_i^j(t)\}\}$$

- This is equivalent to choosing a binary code $\bar{\mathbf{C}}$ from the set of all possible code $\mathbf{C}_j$, $1 \leqslant j \leqslant 2^{nM}$, and evaluate the average error prob. $E[P_e(\bar{\mathbf{C}})]$, where

$$P(\bar{\mathbf{C}} = \mathbf{C}_j) = \frac{1}{2^{Mn}},\ 1 \leq j \leq 2^{Mn}$$

$$\bar{P}_e = E[P_e(\bar{\mathbf{C}})] = \sum_{j=1}^{2^{nM}} P_e\{\{s_i^j(t)\}\} P(\mathbf{C}_j)$$

Applying the union bound, we get

$$P_e\{\{S_i^j(t)\}\} \leq \frac{1}{M} \sum_{i=0}^{M-1} \sum_{l=0, l\neq i}^{M-1} Q\left(\frac{\| s_i^j(t) - s_l^j(t) \|}{\sqrt{2N_0}}\right) = \frac{1}{M} \sum_{\substack{i,l \\ i\neq l}} Q\left(\frac{2\sqrt{\varepsilon_c d(C_i^j, C_l^j)}}{\sqrt{2N_0}}\right)$$

where C_i^j denotes the *ith* codeword of the *jth* codebook $\mathbf{C}_j$.

Random Coding Based on M-ary Binary Coded Signals

$$\text{Since } Q(x) \le e^{-\frac{x^2}{2}} \text{ for any } x > 0,\ P_e\{\{s_i^j(t)\}\} \le \frac{1}{M}\sum_{\substack{i,l \\ i\neq l}} \exp\{-\frac{\varepsilon_c d(C_i^j, C_l^j)}{N_0}\}$$

$$\bar{P}_e \le \frac{1}{2^{nM}}\sum_{j=1}^{2^{nM}} \frac{1}{M}\sum_{\substack{i,l \\ i\neq l}} \exp\{-\frac{\varepsilon_c d(C_i^j, C_l^j)}{N_0}\}$$

$$= \frac{1}{M}\sum_{\substack{i,l \\ i\neq l}} [\frac{1}{2^{nM}} \exp\{-\frac{\varepsilon_c d(C_i^j, C_l^j)}{N_0}\}]$$

$$= \frac{1}{M}\sum_{\substack{i,l \\ i\neq l}} E[\exp\{-\frac{\varepsilon_c d(C_i, C_l)}{N_0}\}]$$

where C_i and C_l are the *ith* and *lth* codeword of the random codebook $\bar{C}$ respectively.

Random Coding Based on M-ary Binary Coded Signals

C_i and C_l are independent, each taking values uniformly over the set (0,1)

$$P(d(C_i, C_l) = d) = 2^{-n}\binom{n}{d}$$

$$\Rightarrow E[\exp\{-\frac{\varepsilon_c d(C_i, C_l)}{N_0}\}] = \sum_{d=0}^{n} 2^{-n}\binom{n}{d} e^{-\frac{d\varepsilon_c}{N_0}}$$

$$= 2^{-n}\left(1 + e^{-\frac{\varepsilon_c}{N_0}}\right)^n = 2^{-n}[1 - \log(1 + e^{-\frac{\varepsilon_c}{N_0}})]$$

$$\Rightarrow$$

$$\overline{P}_e \le (M-1)2^{-n}[1 - \log(1 + e^{-\frac{\varepsilon_C}{N_0}})] < 2^{\mathrm{R_b}T - TDR_0} = 2^{-T(DR_0 - \mathrm{R_b})}$$

$$\text{where } R_0 = 1 - \log(1 + e^{-\frac{\varepsilon_C}{N_0}}), D = \frac{1}{T_c}, n = TD$$

Random Coding Based on M-ary Binary Coded Signals

Since $\overline{P}_e$ is the average error prob. of the 2^{nM} coded comm. Systems, There exists at least one binary code C_j such that the corresponding error prob.

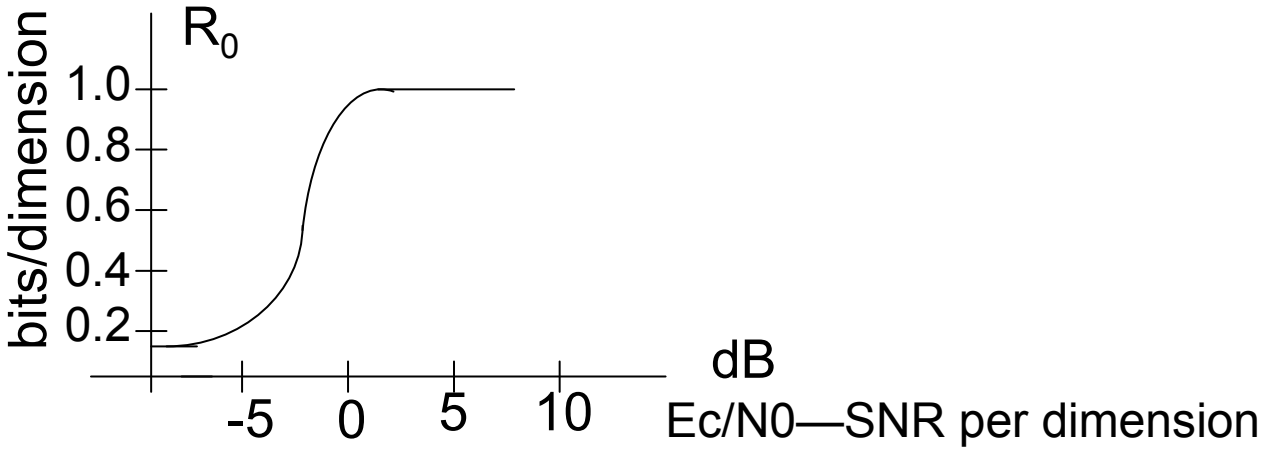
$$P_e(C_j) < 2^{-T(DR_0 - R_b)} < 2^{-n(R_0 - R_c)}$$

where $R_c = k/n = R_b/D$ is referred to as the code rate.

When $R_b < DR_0$ (or $R_c < R_0$), one can always design a binary coded system so that the block error prob. goes to 0 exponentially fast as the block length *n* approached infinity.

Random Coding Based on M-ary Binary Coded Signals

- If one selects a code at random, then this code is good with a very high probability.
- The probability that the error probability of the randomly chosen code $P_e \geq \alpha \overline{P}_e$ is less than 1/α.
- As the dimension n is large enough, good codes are abundant. But the implementation complexity is high.
- The rate R_0 is called the cutoff rate.



Review of Finite Fields

Group Structures

Definition 1 A group is a set G together with a binary operation * on G such that the following three properties hold:

1) * is associative, that is,
for any $a,b,c \in G$, $(a*b)*c=a*(b*c)$

2) There is an identity or (unity) element e in G such that for all $a \in G$,
$$a*e = e*a = a$$

3) For each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that
$$a*a^{-1} = e$$

Sometimes, we denote the group as a triple (G, *, e). If the group also satisfies
4) for all a, b
$$a * b = b * a$$
Then the group is called abelian or commutative.

Example 1 Let

- Z, the set consisting of all integers
- Q, the set of all rational numbers

+ and · are ordinary addition and multiplication.

Then $(Z, +, 0)$, $(Q, +, 0)$, $(Q^*, \cdot, 1)$
are all groups where Q^* is the all nonzero rational numbers.

Furthermore, they are abelian

How about $(Z^*, \cdot, 1)$?

Let n be a positive integer (n>1) and Z_n represent the set of remainder of all integers on division n, i.e.,

$$Z_n = \{0, 1, 2, \cdots, n-1\}$$

We define $a+b$ and ab the ordinary sum and product of a and b reduced by modulo n respectively.

Let $Z_n^* = \{ a \in Z_n | \, a \neq 0\}$

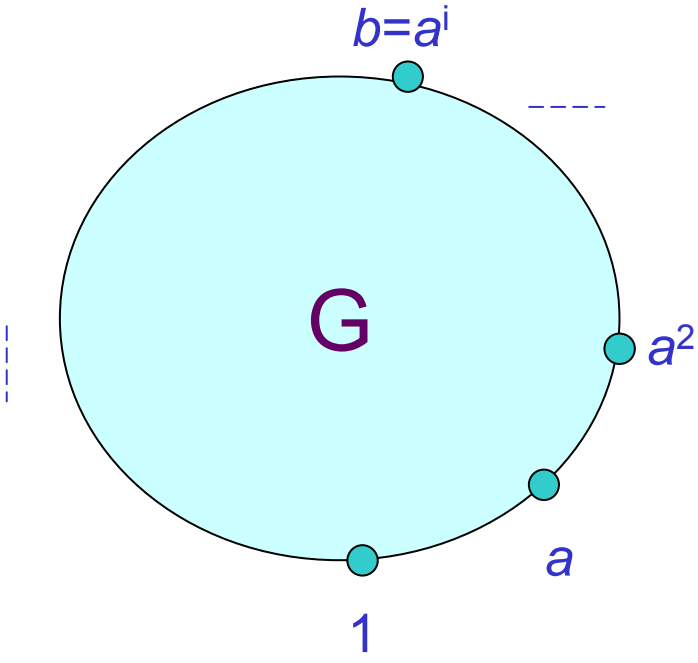
Proposition 1

(a) $(Z_n, +, 0)$ forms a group

(b) $(Z_p^*, ., 1)$ forms a group for any prime p

Definition 2 A multiplicative group is said to be cyclic if there is an element $a \in G$ such that for any $b \in G$ there is some integer i with $b = a^i$. Such and element is called the generator of the cyclic group, and we write

$$G = \langle a \rangle$$



Examples

$(Z_3^*, \cdot, 1)$ is a cyclic group with generator 2.

$Z_3 = \{1, 2\} = \langle 2 \rangle$, $2^0 = 1$, $2^2 = 1 \bmod 3$

$(Z_7^*, \cdot, 1)$ is a cyclic group with generator 3.

$3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1 \bmod 7$

$(Z_5^*, \cdot, 1)$ is a cyclic group with generator 2.

$2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1 \bmod 7$

Every element in Z_5^* can be written in a power of 2

Finite Groups

Definition 3 A group G is called finite if it contains a finite number of elements. The number of elements in G is called

the order of G, denoted as |G|

Rings

Definition 4 A ring $(R,+,\cdot)$ is a set R, together with two binary operations, denoted by + and · such that

1) R is an abelian group with respective to +

2) · is associative, that is

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

3) The distributive law holds:

$a \cdot (b + c) = a \cdot b + a \cdot c$

$(b + c) \cdot a = b \cdot a + c \cdot a$

$(Z, +, \cdot)$ and $(Q, +, \cdot)$ are rings

$(Z_n, +, \cdot)$ forms a ring, called residue class ring modulo n

$(Z_4, +, \cdot)$ is a ring.

Fields

Let $(F,+,\cdot)$ be a ring, and let

$F^* = \{ a \in F \mid a \neq 0 \}$

The set of nonzero elements in F.

Definition 5 A field is a ring $(F,+,\cdot)$ such that F^* together with the multiplication $\cdot$ forms an abelian group.

- $(Q,+,\cdot)$,
- $(R,+,\cdot)$, and
- $(C,+,\cdot)$ are fields

where R is the set of all real numbers, and C is the set of all complex numbers

Finite Fields

Definition 6 A finite field F is a field that contains a finite number q of elements. This number is called the order of the field. F is also called a Galois field, denoted by GF(q).

Proposition 2 Let P be a prime, then $(Z_p, +, \cdot)$ is finite field with order p. This field is denoted as GF(p).
The addition and multiplication are carried out modulo p.

Examples: GF(2) and GF(3) on page 266

Polynomials

Let R be an arbitrary ring. A polynomial over R is an expression of the form

$$f(x) = a_0 + a_1 x + \cdots a_n x^n$$

where n is an nonnegative integer, the coefficients a_i are elements of *R*. *x* is a symbol not belonging to *R*, called an indeterminant over *R*.

f(x) is said to to be irreducible if f(x) cannot be factored into a product of lower degree polynomials over R

x^2+x+1 is irreducible in GF(2)

Construction of $GF(2^n)$ and $GF(q^n)$

Step 1 Selcet n, a positive integer and p a prime.

Step 2 Choose that *f(x)* is an irreducible polynomial over GF(p) of degree n.

Step 3 We agree that α is an element that satisfies $f(\alpha) = 0$.

Let $GF(p^n) = \{a_0 + a_1 \alpha + \cdots a_n \alpha^n | a_i \in GF(p)\}$

Construction of $GF(2^n)$ and $GF(p^n)$

For two elements $g(\alpha)$ and $h(\alpha)$ in $GF(P^n)$,

$$g(\alpha)=a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1}$$

$$h(\alpha)=b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}$$

Define two operations:

a) Addition

$$g(\alpha)+ h(\alpha)= a_0+b_0+(a_1+b_1)\alpha +\cdots+(a_{n-1}+b_{n-1}) \alpha^{n-1}$$

b) Multiplication

$$g(\alpha)\, h(\alpha)= r(\alpha)$$

where r(x) is the remainder of g(x)h(x) divided by f(x)

Theorem: The set $GF(p^n)$ together with the two operations above forms a finite field, and the order of the field is p^n

Example: Let p=2 and $f(x) = 1+x+x^3$. Then f(x) is irreducible over GF(2). Let α be a root of f(x). That is, $f(\alpha)=0$. The finite field $GF(2^3)$ is defined by

$$GF(2^3)=\{a_0 + a_1 \alpha + \cdots a_2 \alpha^2 | \ a_i \in GF(2) \}$$

As a 3-tupe	As a polynomial	As a power of α
000=	0	=0
001=	1	=1
010=	α	=α
100=	α^2	$=\alpha^2$
011=	1+ α	$=\alpha^3$
110=	$\alpha + \alpha^2$	$=\alpha^4$
111=	$1+ \alpha + \alpha^2$	$=\alpha^5$
101=	$1+ \alpha^2$	$=\alpha^6$
$\alpha^7 = 1$		

Primitive Elements and Primitive Polynomials

Fact: For any finite field F, its mutliplcative field F*, the set of nonzero elements in F is cyclic.

Definition: A generator of the cyclic group $GF(p^n)^*$ is called a primitive element of $GF(p^n)$. A polynomial has a primitive element as zero is called a primitive polynomial

Example: x^3+x+1 is primitive polynormial over GF(2)

$x^7-1 = (x+1)(x^3+x+1)(x^3+x^2+1)$