情報通信と符号化

韓　承鎬

電気通信大学

第二回目

現代通信システムの構成

アナログシステム $\Longrightarrow$ デジタルシステム
アナロ信号 $\Longrightarrow$ デジタル信号

標本化

時間的に連続な信号 $x(t)$ から時間的に離散的な信号を生成

Theorem

標本化定理：情報信号 $x(t)$ の帯域を B とすると，時間間隔 $T_s \leq \frac{1}{2B}$ で抽出した標本から情報信号を完全に復元できる．

量子化

- 実数の値から有限集合の値に変換する操作
- 歪みなく元の値を復元できる量子化の方法はない
- 線形量子化の場合，量子化ビットが 1 ビット増えると信号対雑音比は 6dB 改善

デジタル通信方式で送信できるもの

1. $x(t) \in \mathbb{R}$
2. $x(t) \in [0\ 1]$
3. $x(t) \in \mathbb{Z}^{+}$
4. $x(t) \in \{\pi/2, \pi\}$
5. $x(t) \in \{0, 1\}$

情報源符号化/復号化

- 有限集合に M 個の要素があると仮定
- 各要素を $0, 1, 2, \cdots, M-1$ と番号付け順序を送信
- 情報は順序を二進数展開したビット列

情報源符号化

情報を冗長な表現を省いたもっとも短いビット列で表す

- 種類：無歪み符号化と歪み符号化
- 完全圧縮：0 と 1 は独立で同確率

暗号化/暗号復号化

- 秘密鍵暗号
  - 送信側と受信側が鍵を密かに共有する暗号化方式
  - $k = 2$ のシフト暗号：HELLO$\Longrightarrow$JGNNQ
    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 公開鍵暗号
  - メッセージを受け取る側が公開鍵（錠）と秘密鍵（鍵）を作り，公開鍵を公開
  - 秘密鍵は公開鍵からは計算できない

通信路符号化/復号化

目的

雑音や干渉への耐性を強める

繰り返し符号の例

1. 0 が現れたら (000) を, 1 が現れたら (111) を出力
   1 ビットまでの誤りを訂正
2. 0 が現れたら (00000) を, 1 が現れたら (11111) を出力
   2 ビットまでの誤りを訂正

- 符号化レート k/n
  情報ビット k ビットを n ビットの符号語に変換
- 符号化レートが低いほど雑音に強くなるが情報ビットの伝送速度は遅くなる

変調/復調

目的

ビット列を通信路の上で伝搬しやすい電気信号の波形に変換

- 二値変調：$0 \to s_0(t),\ \ 1 \to s_1(t)$
- 多値変調：$s_i(t), i = 0, 1, \cdots, .M-1,\ M = 2^b$, で b ビットの符号語列を送信

種類

$$s(t) = A\cos(ft + \theta)$$

1. 振幅変調，周波数変調，位相変調
2. 直行振幅変調

多重化/逆多重化

目的

複数のユーザが同一の通信路を通じて通信を行うとき，情報を希望の相手に届けるため

1. 第一世代：アナログ FDMA 方式
2. 第二世代：デジタル TDMA 方式
3. 第三世代：CDMA 方式
4. 第四世代：OFDM 方式
5. 第五世代：?

通信路

電話線，同軸ケーブル，電磁波，光ファイバーなどの物理的な媒体

共通の特性

雑音：固定の値を持たず，ランダム性を持つ

特徴を簡潔に記述する数学モデル

1. 加法性雑音通信路
2. 線形フィルタ通信路
3. 線形時変フィルタ通信路

通信路

- 受信機の電子装置と増幅器などから入る
- 統計的に熱雑音はガウス過程

線形フィルタ通信路

信号の送信時にフィルタを用いる

$$\begin{aligned} r(t) &= s(t) * c(t) + n(t) \\ &= \int_{-\infty}^{\infty} c(\tau) s(t-\tau) d\tau + n(t) \end{aligned}$$

$c(t)$ は線形フィルタのインパルス応答で $*$ は畳み込み

線形時変フィルタ通信路

$$r(t) = s(t) * c(\tau; t) + n(t) = \int_{-\infty}^{\infty} c(\tau; t) s(t-\tau) d\tau + n(t)$$

$c(\tau; t)$：時間 t における時刻 $t-\tau$ のインパルスに起因する応答

電離層や移動通信の場合

$$c(\tau;t) = \sum_{k=1}^{L} a_k(t)\delta(\tau - \tau_k)$$

から

$$r(t) = \sum_{k=1}^{L} a_k(t)s(t - \tau_k) + n(t)$$

$\{a_k(t)\}$ と $\{\tau_k\}$：L 個のパスの中の k 番目のパスの振幅と遅延