Lecture 16

Thursday, April 10, 2014

3:37 PM

Secrecy:

One-time-pad:

Key: 0 1 1 0 1 1 1 0 0 1

Message: 1 1 1 1 1 0 0 0 0 0

xor

Transmit: 1 0 0 1 0 1 1 0 0 1

$$p(\text{transmit} \mid \text{message}) = p(\text{transmit})$$

$$p(\text{message} \mid \text{transmit}) = p(\text{message})$$

Perfect Secrecy:

Linear Time Invariant Systems:

Assume $\mathcal{H}$ is LTI:

Impulse Response:

Memoryless: Amplifier (mult. by const):

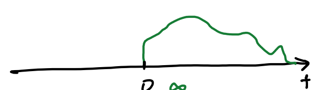
$h(t) = c\,\delta(t)$

$h[n] = c\,\delta[n]$

$x(t) * (c\,\delta(t)) = c\; x(t) * \delta(t) = c\,x(t)$

Causal: $h(t) = 0 \quad \forall t < 0$

$h[n] = 0 \quad \forall n < 0$



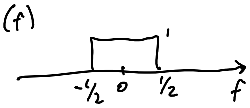
$$x * h = \int_{-\infty}^{\infty} x(\tau)\, h(t-\tau)\, d\tau$$

BIBO Stable

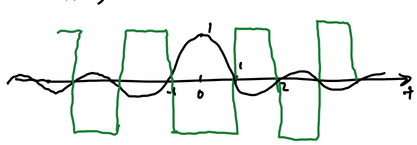
Invertible

Example of unstable system:

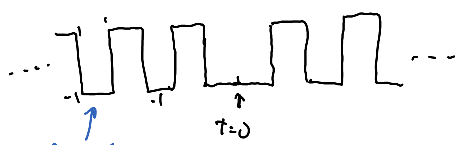
$F(f)$



$h(t)$



Let the input be



freq. $\frac{1}{2}$

mult. $-|\text{sinc}(t)|$

$$-\left|\frac{\sin(\pi t)}{\pi t}\right|$$

Integral is infinite.

Stable = $\int^{\infty} |h(\tau)|\, d\tau$

Integral is infinite.

$$\text{Stable} = \int_{-\infty}^{\infty} |h(\tau)|\, d\tau$$

Absolutely integrible

Assume $\int_{-\infty}^{\infty} |h(\tau)| d\tau < \infty$:
and $|x(t)| \le B \quad \forall t$

Let $y(t) = (x * h)(t)$.

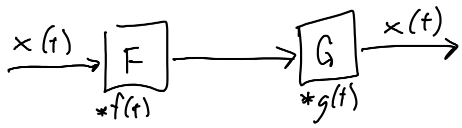
$$|y(t)| = \left| \int_{-\infty}^{\infty} h(\tau)\, x(t-\tau)\, d\tau \right| \le \int_{-\infty}^{\infty} |h(\tau)\, x(t-\tau)|\, d\tau$$

$$= \int_{-\infty}^{\infty} |h(\tau)|\, |x(t-\tau)|\, d\tau$$

$$\le \int_{-\infty}^{\infty} |h(\tau)|\, B\, d\tau = B \int_{-\infty}^{\infty} |h(\tau)|\, d\tau$$

Invertible:

If F and G are inverse systems.



For LTI systems: $X(f) \cdot F(f) \cdot G(f) = X(f)$

$$\Rightarrow \quad G(f) = \frac{1}{F(f)} \quad \forall f$$

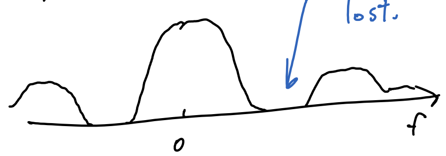
If Fourier transform is 0 for some f, then no inverse.

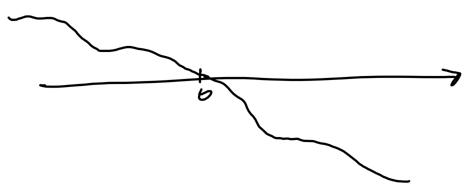
Consider Magnitude and phase:

$|F(f)|$ $\quad$ $\measuredangle F(f)$

Not invertible

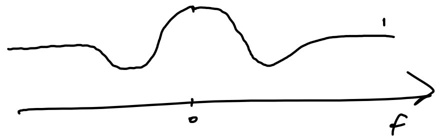
information is lost.

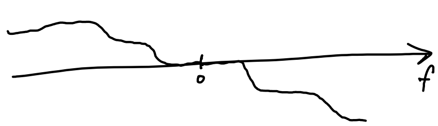




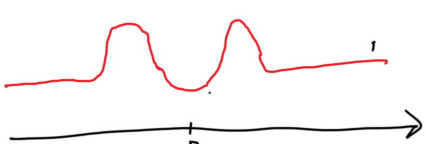
$|F(f)|$ $\quad$ $\measuredangle F(f)$

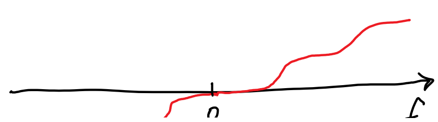
Invertible

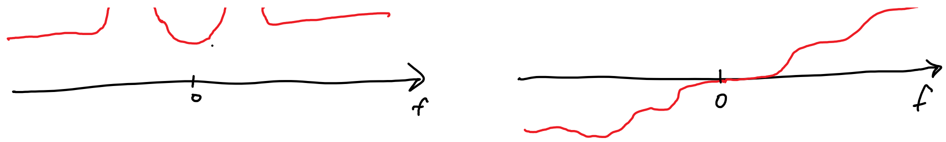




$|G(f)|$ $\quad$ $\measuredangle G(f)$







$$F(f) \cdot G(f) = 1$$

$$|F(f) \cdot G(f)| = |F(f)|\,|G(f)|$$

$$\measuredangle(F(f) \cdot G(f)) = \measuredangle F(f) + \measuredangle G(f)$$

Filtering: Designing LTI to behave a certain way in freq. domain.

- $h(t)$

$H(f) = \mathcal{F}(h(t))$ – Frequency response
– Transfer function

$$x(t) \longrightarrow \boxed{*h(t)} \xrightarrow{y(t)}$$

$$|Y(f)| = |X(f)|\,|H(f)|$$

$$\measuredangle Y(f) = \measuredangle X(f) + \measuredangle H(f)$$

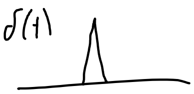
Example of system inverse:

$$x(t) \longrightarrow \boxed{\text{Differentiator}} \xrightarrow{x'(t)}$$

Linear: $(a x_1(t) + b x_2(t))' = a x_1'(t) + b x_2'(t)$

Time-invariant: $(x(t-T))' = x'(t-T) \cdot \cancel{\frac{d}{dt}(t-T)}$

LTI $\quad h(t) = \delta'(t)$

$\delta(t)$  $\delta'(t)$ 

$$\int_{-\infty}^{\infty} \delta'(t-T) f(t)\, d\tau = -f'(T)$$

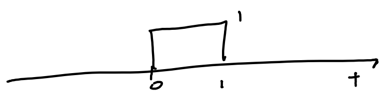
$$x(t) \longrightarrow \boxed{\begin{matrix}\text{Integrator}\\ 1\end{matrix}} \longrightarrow \int_{-\infty}^{t} x(\tau)\, d\tau$$

LTI $\quad h(t) = u(t)$

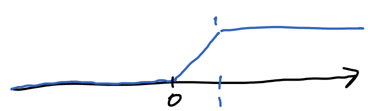
$$x(t) \longrightarrow \boxed{\begin{matrix}\text{Integrator}\\ 2\end{matrix}} \longrightarrow \int_{0}^{t} x(\tau)\, d\tau$$

Not LTI : Not time-invariant.

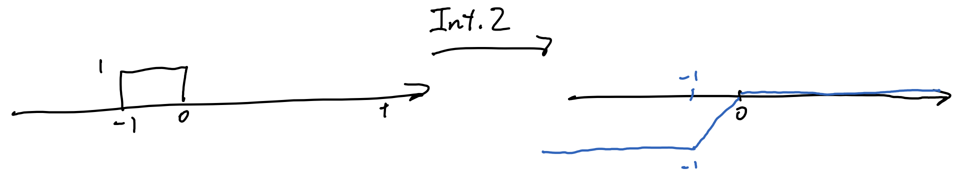
$x(t) = \mathrm{rect}(t - \frac{1}{2})$



$\xrightarrow{\text{Int. 2}}$



$x(t) = \mathrm{rect}\left(t+\frac{1}{2}\right)$



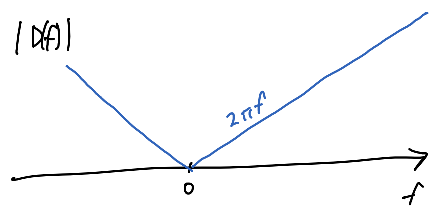
Frequency Response of differentiator:

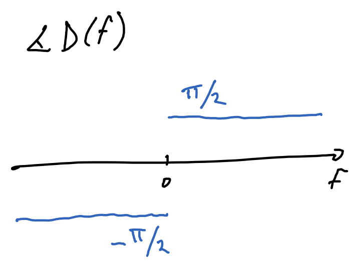
$$\mathcal{F}(\delta'(t)) = \int_{-\infty}^{\infty} \delta'(t) e^{-i2\pi f t}\, dt = -\left(e^{-i2\pi f t}\right)'\Big|_{t=0} = -(-i2\pi f) e^{-i2\pi f(0)} = \boxed{i2\pi f}$$

$$D(f) = i2\pi f$$

$$|D(f)| = \sqrt{D(f)D^*(f)} = \sqrt{(-i2\pi f)(i2\pi f)} = \sqrt{(2\pi f)^2} = \boxed{|2\pi f|}$$

$$\measuredangle D(f) = \begin{cases} -\pi/2, & f \geq 0 \\ \pi/2, & f < 0 \end{cases}$$





Let $I(f)$ be the transfer function for the integrator:

$$I(f) = \frac{1}{D(f)} = \frac{1}{i2\pi f} + \frac{1}{2}\delta(f)$$