Attack Design for Continuous and Discrete Systems

DJ Passey

BYU Information and Decision Algorithms Laboratories
Professor: Sean Warnick

March 20th, 2018

Constructing Discrete Time $\Delta(z)$

Because the z-transform acts similarly to the Laplace transform, when we create an attack on a discrete time system, many of the principles from the continuous time attack carry over. Most importantly, the small gain theorem still applies.

Proof Assume $G(z)$ is the transfer function for some discrete time system. If $G(z)$ is in feedback with some $\Delta(z)$, by the small gain theorem, $\Delta(z)$ will destabilize the system if for some $e^{j\phi_0}$, $||\Delta(e^{j\phi_0})G(e^{j\phi_0})|| \geq 1$. Then for some $e^{j\phi_0}$, a minimal destabilizing attack has norm $||\Delta(e^{j\phi_0})|| = \frac{1}{||G(e^{j\phi_0})||}$. Then the construction of $\Delta(j\omega_0)$ from the continuous time case will work for discrete time $\Delta(e^{j\phi_0})$ as well. If $G(e^{j\phi_0}) = U\Sigma V^*$ We have,

$$\Delta(e^{j\phi_0}) = V \begin{bmatrix} \frac{1}{\sigma_1} & & \\ & 0 & \\ & & \ddots \end{bmatrix} U^* = \frac{1}{\sigma_1} v_1 u_1^* = \frac{1}{\sigma_1} \begin{bmatrix} r_1 e^{i\theta_1} \\ \vdots \\ r_n e^{i\theta_n} \end{bmatrix} \begin{bmatrix} \rho_1 e^{i\phi_1} \cdots \rho_n e^{i\phi_n} \end{bmatrix}$$

Then, we can create $\Delta(z)$ in a similar way to $\Delta(s)$ by setting,

$$\Delta(z) = \frac{1}{\sigma_1} \begin{bmatrix} r_1 f_1(z) \\ \vdots \\ r_n f_n(z) \end{bmatrix} \begin{bmatrix} \rho_1 g_1(z) \cdots \rho_n g_n(z) \end{bmatrix}$$

Then $\Delta(z)$ is viable, if the entry functions $f_i(z)$ and $g_i(z)$ are viable.

Discrete Time Entry Functions

Each $f_i(s)$ and $g_i(s)$ must have the following properties:

1. $f_i(e^{j\phi_0}) = e^{j\theta_i}$ and $g_i(e^{j\phi_0}) = e^{j\phi_i}$
2. The poles of f_i and g_i are within the unit circle
3. Each f_i and g_i is unitary
4. Each f_i and g_i is a rational polynomial

Once again, the constant function, $f_i(z) = e^{j\theta_i}$ satisfies each of the requirements. It has no poles, is always unitary and is a degree zero polynomial. A second option is the function:

$$f_i(z) = z^{-1} e^{j(\theta_i + \phi_0)}$$

We satisfy the first requirement by construction, the function has no poles, is a polynomial of degree one and is unitary because for any $e^{j\phi}$, $||f_i(e^{j\phi})|| = 1$. Thus, the function is a viable entry function.

To complete our analog of the continuous time attack design, we turn lastly to the discrete time all-pass filter:

$$f_i(z) = \frac{z^{-1} - \alpha^*}{1 - \alpha z^{-1}}$$

In order to solve for an appropriate α parameter we solve the following equation for alpha:

$$f_i(e^{j\phi_0}) = \frac{e^{-j\phi_0} - \alpha_i^*}{1 - \alpha_i e^{-j\phi_0}} = e^{j\theta_i}$$

For simplicity, in the following calculations we will drop the subscripts from f, α, θ, and ϕ.

$$\begin{aligned} f(e^{j\phi}) &= \frac{e^{-j\phi} - \alpha^*}{1 - \alpha e^{-j\phi}} = e^{j\theta} \\ \frac{(1 - \alpha e^{-j\phi})^*}{1 - \alpha e^{-j\phi}} &= e^{j(\theta+\phi)} \end{aligned}$$

Let $w = 1 - \alpha e^{-j\phi} = re^{j\varphi}$. Then

$$\begin{aligned} \frac{w*}{w} &= e^{j(\theta+\phi)} \\ e^{-2j\varphi} &= e^{j(\theta+\phi)} \\ e^{j\varphi} &= e^{-j\frac{\theta+\phi}{2}} \end{aligned}$$

This implies that

$$\begin{aligned} w &= re^{-j\frac{\theta+\phi}{2}} \\ 1 - \alpha e^{-j\phi} &= re^{-j\frac{\theta+\phi}{2}} \\ \alpha &= e^{j\phi} - re^{j\frac{\phi-\theta}{2}} \end{aligned}$$

where r is a free variable. For our purposes here, it suffices to let $r = 1$. In order for the function to be viable, it is necessary that $||\alpha|| < 1$ because α is a pole. In the case that $||\alpha|| > 1$ simply use the function, $e^{2j\theta}\frac{1}{f(z)}$, noting that with the solution for α above,

$$\frac{e^{2j\theta}}{f(e^{j\phi})} = e^{2j\theta}\frac{1 - \alpha e^{-j\phi}}{e^{-j\phi} - \alpha^*} = e^{2j\theta}e^{-j\theta} = e^{j\theta}.$$

The pole of the function $e^{2j\theta}\frac{1}{f(z)}$ is $1/\alpha$. By choosing between $f(z)$ and $e^{2j\theta}\frac{1}{f(z)}$ we can produce a rational polynomial with a stable pole. Lastly we demonstrate that $f(z)$ is unitary. Let ϕ be given. Then

$$||f(e^{j\phi})|| = ||\frac{e^{-j\phi} - \alpha^*}{1 - \alpha e^{-j\phi}}|| = ||e^{-j\phi}\frac{(1 - \alpha e^{-j\phi})^*}{1 - \alpha e^{-j\phi}}|| = 1.$$

Thus, the all pass filter satisfies the requirements of an entry function and can be used to create a viable $\Delta(z)$.

■

Conclusion

Using the tools above, it is possible to produce minimal attacks on any system. Further work includes determining how to execute the attack in the time domain and determining how the different types of attacks affect systems differently.