Polynomial Methods

Division of polynomial by polynomial

Let \( a(s) = a_0 s^n + a_1 s^{n-1} + \ldots + a_n \) and
\( b(s) = b_0 s^m + b_1 s^{m-1} + \ldots + b_m \) be two scalar polynomials with \( b_0 \neq 0 \), \( n > m \).

There exist unique polynomials \( q(s) \) (the QUOTIENT) and \( r(s) \) (the REMAINDER) such that
\[
a(s) = q(s) b(s) + r(s)
\]
and \( \deg r(s) < \deg b(s) \).

The algorithm which accomplishes division is the EUCLIDEAN algorithm.

\[
a(s) = a_0 s^n + a_1 s^{n-1} + \ldots + a_n
\]

\[
= a_0 b_0^{-1} s^{n-m} (b_0 s^m + \ldots + b_m)
\]

\[
+ (a_1 s^{n-1} + a_2 s^{n-2} + \ldots + a_n)
\]

\[
\quad - (b_1 s^{m-1} + b_2 s^{m-2} + \ldots + b_m) b_0^{-1} b_0^{-1} s^{n-m}
\]

\[
= a_0 b_0^{-1} s^{n-m} b(s) + r^{(1)}(s)
\]

where \( r^{(1)}(s) = (a_1 - b_1 a_0 b_0^{-1}) s^{n-1} + (a_2 - b_2 a_0 b_0^{-1}) s^{n-2} + \ldots + a_n - b_n a_0 b_0^{-1}
\]

\[
= (a_{n-m} - b_{m} a_0 b_0^{-1}) s^{n-m} + a_{m+1} s^{n-m-1} + \ldots + a_n
\]
and \( \deg (\gamma'(s)) \leq n-1 \).

Thus the above substitution lowers the degree of \( \gamma'(s) \) by 1. Repeat by dividing \( \gamma'(s) \) by \( b(s) \) to obtain \( \gamma''(s) \) and \( \bar{\gamma}''(s) \), etc, of degree \( \leq (n-2) \), until we end up with \( \gamma(s) \) with degree \( \gamma(s) < m \).

This is when the algorithm terminates.

Unique follows from observation that

\[
\text{if } \quad a(s) = q(s) b(s) + \gamma(s) = \tilde{q}(s) b(s) + \tilde{\gamma}(s)
\]

where \( \deg (\gamma(s)) < \deg (b(s)) \) and \( \deg (\tilde{\gamma}(s)) < \deg (b(s)) \),

then,

\[
(q(s) - \tilde{q}(s)) b(s) = (\tilde{\gamma}(s) - \gamma(s))
\]

But r.h.s has degree < \( \deg (b(s)) \)
while l.h.s has degree \( \geq \deg (b(s)) \),

if \( q \neq \tilde{q} \) and \( \gamma \neq \tilde{\gamma} \). Hence at least \( q = \tilde{q} \) or \( \gamma = \tilde{\gamma} \).

By the same degree consideration, it must mean \( q = \tilde{q} \) and \( \gamma = \tilde{\gamma} \). □
Finding $\text{g.c.d.}$ of $a(s)$ and $b(s)$.

Without loss of generality, assume $\deg(a(s)) = n > \deg(b(s)) = m$

Apply Euclidean division repeatedly as follows:

\[ a(s) = q_1(s) b(s) + r_1(s) \quad \deg(r_1(s)) < \deg(b(s)) \]

\[ b(s) = q_2(s) r_1(s) + r_2(s) \quad \deg(r_2(s)) < \deg(r_1(s)) \]

\[ r_1(s) = q_3(s) r_2(s) + r_3(s) \quad \deg(r_3(s)) < \deg(r_2(s)) \]

\[ \vdots \]

\[ r_{p-3}(s) = q_{p-2}(s) r_{p-2}(s) + r_{p-1}(s) \]

\[ r_{p-2}(s) = q_p(s) r_{p-1}(s) + 0 \]

where at the $p^{th}$ stage remainder $= 0$ since remainder is always lower in degree than the divisor. We say $r_{p-1}$ divides $r_{p-2}$ exactly (denoted by $r_{p-1} \mid r_{p-2}$). By substitution in the previous step, it follows that
\[ r_{p-1} \mid r_{p-3}, \quad r_{p-1} \mid r_{p-4}, \ldots, \quad r_{p-1} \mid r_{i} \quad r_{p-1} \mid b \quad \text{and hence} \quad r_{p-1} \mid a. \]

Thus, \( r_{p-1} \) is a common factor of \( a(5) \) and \( b(5) \). We need to prove that \( r_{p-1} \) is the g.c.d.

Observe

\[ r_1 = 1 \cdot a + (-q_1) b \]
\[ r_2 = 1 \cdot b + (-q_2) r_1 \]
\[ = 1 \cdot b + (-q_2) (1 \cdot a + (-q_1) b) = (-q_2) a + (1 + q_1 q_2) b \]
\[ r_3 = 1 \cdot r_1 - q_3 \cdot r_2 \]
\[ = 1 \cdot (1 \cdot a + (-q_1) b) + (-q_3) (-q_2) a + (1 + q_1 q_2) b = (1 - q_2 q_3) a + (-q_1 - q_3 + q_1 q_2 q_3) b \]

\[ r_{p-1} = x \cdot a + y \cdot b \]
Hence any exact divisor of \(a(s)\) and \(b(s)\) also divides \(r_{p-1}(s)\) exactly. But \(r_{p-1}\) divides \(a\) and \(b\) exactly.

Thus \(r_{p-1} = \text{g.c.d.} (a, b) \Rightarrow \)

We say \(a(s)\) and \(b(s)\) are \textit{coprime} (or \textit{relatively prime}) if \(\text{g.c.d.} (a, b)\) is a constant, (taken to be \(= 1\)). Then denote

\[ (a, b) = 1 \]

**Theorem [BEZOUT]**

Let \(a(s) = a_0 s^n + a_1 s^{n-1} + \ldots + a_n \)
and \(b(s) = b_0 s^m + b_1 s^{m-1} + \ldots + b_m, \)
\(b_0 \neq 0\) and \(a_0 \neq 0\). Then

\[ (a(s), b(s)) = 1 \quad \text{(coprimeness)} \]

\(\iff\) there exist (necessarily unique) polynomials \(x(s)\) and \(y(s)\) such that

\[ x(s) a(s) + y(s) b(s) \equiv 1 \]
and \deg \((x(s)) < m, \deg \((y(s)) < n. \]
Proof of Bezout's Theorem

(⇒) We showed that

\[ \text{g.c.d. } (a(s), b(s)) = \gamma_{p-1}(s) = x(s) a(s) + y(s) b(s) \]

Thus if \( \text{g.c.d.} \equiv 1 \) then

\[ x(s) a(s) + y(s) b(s) \equiv 1 \]

(⇐) Suppose \( \exists \) solution to

\[ x a + y b \equiv 1 \]

We wish to prove \( \text{g.c.d. } (a, b) \equiv 1 \)

Suppose to the contrary that there is a polynomial \( \Theta(s) \) of degree \( > 1 \) such that \( \Theta | a \) and \( \Theta | b \).

Then

\[ x a + y b = x a_1 + y b_1 \Theta = (x a_1 + y b_1) \Theta \]

Let \( \lambda \in \mathbb{C} \) be such that \( \Theta(\lambda) = 0 \)

\[ x(\lambda) a(\lambda) + y(\lambda) b(\lambda) = (x(\lambda) a_1(\lambda) + y(\lambda) b_1(\lambda)) \]

\[ \equiv 0 \]

\[ \Rightarrow \]
But \( x(\lambda) a(\lambda) + y(\lambda) b(\lambda) = 1 \) by hypothesis. Hence we have a Contradiction. Hence \( \text{g.c.d.}(a, b) = 1 \).

Applying Bezout's Theorem to controller design.

Recall that given a rational, strictly proper transfer function

\[ g(s) = \frac{b(s)}{a(s)}, \quad a, b \text{ coprime} \]

where \( a(s) = s^n + a_1 s^{n-1} + \ldots + a_n \)
and \( b(s) = b_0 s^m + b_1 s^{m-1} + \ldots + b_m \)
where \( m \leq n-1 \) and \( b_0 \neq 0 \), we can write,

\[ a(s) \xi(s) = u(s) \]

\[ y(s) = b(s) \xi(s). \]

From coprimeness of \( a \) and \( b \) and Bezout, there exist unique polynomials \( x(s) \) and \( w(s) \), \( \deg(x) < \deg(b) \), \( \deg(w) < \deg(a) \) such that,
\[ z < + Wb = 1. \]

Consider the "controller" structure with \( m(s) \) a polynomial:

Then \( u(s) = V(s) - m(s) \hat{\xi}(s) \)

\[ = V(s) - m(s) \left( \hat{z}(s) u(s) + W(s) y(s) \right) \]

\[ = V(s) - m(s) \left( \hat{z}(s) a(s) \xi(s) + W(s) b(s) \xi(s) \right) \]

\[ = V(s) - m(s) \left( \hat{z}(s) a(s) + W(s) b(s) \right) \xi(s) \]

\[ = V(s) - m(s) \xi(s) \quad \text{(Bezout)} \]

We thus note \( \hat{\xi} = \xi \).
Hence

\[ u(s) = a(s) \hat{y}(s) = v(s) - m(s)\hat{y}(s) \]

\[ \Rightarrow (a(s) + m(s)) \hat{y}(s) = v(s) \]

Thus the closed-loop transfer function is

\[ g_{\text{closed}}(s) = \frac{b(s)}{a(s) + m(s)} = \frac{y(s)}{v(s)}. \]

The approach above has the flaw that, while \( \frac{b(s)}{a(s)} \) is realizable as a finite dimensional linear system, the blocks \( \hat{z}(s), u(s) \) and \( m(s) \) are not realizable in the same sense since they are polynomials.

Notice that the above structure is reminiscent of the observer-controller structure derived via state space theory.

The situation can be remedied by using precisely this intuition:

Consider again state-space theory of
observer controller design

\[ \dot{x} = Ax + Bu \]
\[ y = Cx \]
\[ \hat{x} = (A - HC)\hat{x} + Ky + Bu \]

Fig 1

re-drawn as:

\[ \dot{x} = Ax + Bu \]
\[ y = Cx \]
\[ \dot{\hat{x}} = (A - HC)\hat{x} + Ky + Bu \]
\[ \hat{e} = K(\hat{x} + Bu) \]

Fig 2

and equivalently in frequency domain as:

\[ + \]
\[ G(s) \]
\[ M(\theta) \]
\[ + \]
\[ NG \]

Fig 3