An Application of Symbolic Computational Algebra in Signal Processing

John B. Little

Department of Mathematics and Computer Science

College of the Holy Cross

Worcester, MA 01610

SCA2002

University of Western Ontario

July 2002

mathcs.holycross.edu/ little/SCA2002.ps

Outline of Talk

1. Signals and filters

2. Filter design problems

3. Selesnick-Burrus equations

4. Solution methods

5. The number of solutions

Signals and Filters

- A *digital* signal is just a function of a *discrete* (time) variable.

- Signal processing operations can be described mathematically by means of "filters"

$$\Gamma : \{\text{signals}\} \to \{\text{signals}\}.$$

- We only consider filters satisfying

  1. (Linearity)

  $$\Gamma(cx + y) = c\Gamma(x) + \Gamma(y).$$

  2. (Shift-invariance) If k is fixed and $y[n] = x[n+k]$ for all n,

  $$\Gamma(y)[n] = \Gamma(x)[n+k]$$

Impulse Response of a Filter

Let δ be the signal

$$\cdots, 0, 0, 1, 0, 0, \cdots$$

(1 at $n = 0$) – a *unit impulse*.

$\Gamma(\delta)$ is called the *impulse response* of Γ, and determines the output on any other input signal.

If $x[n] = \sum_{k=-\infty}^{\infty} x[k]\delta[n-k]$ and $y = \Gamma(x)$, then by linearity and shift-invariance,

$$y[n] = \sum_{k=-\infty}^{\infty} x[k]h[n-k].$$

The Transfer Function

Package $x[n], y[n], h[n]$ by their "z-transforms" X, Y, Z, e.g.

$$X(z) = \sum_{n=-\infty}^{\infty} x[n] z^{-n}$$

$H(z)$ is called the *transfer function* of the filter.

Coefficient of z^{-n} in $H(z)X(z)$ is the convolution:

$$\sum_{k=-\infty}^{\infty} h[k]x[n-k],$$

same as $y[n]$ (!) $\Rightarrow Y(z) = H(z)X(z)$.

Note:

$$H(e^{i\omega}) = \sum_{n=-\infty}^{\infty} h[n] e^{-in\omega}$$

is the (discrete-time) Fourier transform of h, so $H(z)$ also determines the *frequency response* characteristics of the filter on input signals.

Filter Design

Goal is to design filters to perform specified operations on signals, by designing $H(z)$, e.g.

- "Low-pass" filters: remove high-frequency components of signals – typically *smooth out* or *blur* signals (can be used to remove high-frequency "noise")

- "High-pass" filters: remove low-frequency components – typically focus on fine details, rapid changes (can be used to detect features)

Typical problem: design a *low-pass* or *high pass* filter to meet certain specifications.

Selesnick-Burrus Design Paradigm

reference: Selesnick and Burrus, *IEEE Trans. Circuits and Systems II*, v. 45(1), January 1998.

For an FIR low-pass filter

$$H(z) = \sum_{n=0}^{N-1} h[n] z^{-n},$$

let $F(\omega) = |H(e^{i\omega})|^2$, $G(\omega)=$ "group delay". If $K+L+M+1 \leq N$, $L \leq M$, can determine $h[n]$ to make:

- $F^{(2i)}(0) = 0$, $i = 1, \ldots, M$,
- $G^{(2j)}(0) = 0$, $j = 1, \ldots, L$, and
- $(1+z)^K | H(z)$

Form of The Equations in $m[i]$

In terms of the filter *moments*,

$$m_k = \sum_{n=0}^{N-1} n^k h[n],$$

these are polynomial equations:

- Flatness equations (quadratic in the $m[i]$):
  $0 =$
  $$\binom{2i}{i} m_i^2 + 2 \sum_{\ell=0}^{i-1} \binom{2i}{\ell} (-1)^{i+\ell} m_\ell m_{2i-\ell}$$
  $i = 1, \ldots, M$.
  $$\sum_{\ell=0}^{j} (1 - \frac{2\ell}{2j+1}) \binom{2j+1}{\ell} (-1)^\ell m_\ell m_{2j+1-\ell}$$
  $j = 1, \ldots, L$.

- Zeros at $z = -1$: remainder of $H(z)$ on division by $(1+z)^K$ is zero – K linear equations on m_i

A First Observation

Looks like $2M + 1$ variables m_i, $i = 0, \ldots, 2M$, and $K + L + M$ equations.

But the moments m_k, $k \geq N$ are not independent variables. Can express them in terms of $m_0, \ldots, m_{N-1}$ by linear algebra.

This accomplishes a first reduction to N equations in N variables. Expect only finitely many solutions (mainly interested in real ones).

The Case $L = 1, M = 5, K = 1$

The equations:

$$
\begin{aligned}
&2m_1^2 - 2m_2,\\
&6m_2^2 + 2m_4 - 8m_1m_3,\\
&20m_3^2 - 2m_6 + 12m_1m_5 - 30m_2m_4,\\
&70m_4^2 + 2m_8 - 16m_1m_7 + 56m_2m_6\\
&\quad -112m_3m_5,\\
&252m_5^2 - 2m_{10} + 20m_1m_9 - 90m_2m_8\\
&\quad +240m_3m_7 - 420m_4m_6,\\
&-m_3 + m_1m_2
\end{aligned}
$$

(plus 5 additional linear equations)

“Brute-force” solution

- The *lex* Gröbner basis with $m_{10} > m_9 > \cdots > m_1$ is in generic “Shape Lemma” form, with univariate polynomial of degree 16 in m_1.

- Using numerical root-finding, we find 6 approximate real roots: $m_1 \doteq$ .04470426799, 1.233505559, 2.558981682, 4.441018318, 5.766494441, 6.955295732.

- The 6 real roots occur in pairs: $r, 7 - r$ (time reversal)

- Up to time reversal, this gives 3 distinct filters satisfying the Selesnick-Burrus conditions in this case.

“Easy” and “Hard” Cases

- The *easier* cases are
$$\left\lfloor \frac{M-1}{2} \right\rfloor \le L \le M$$
Can eliminate to a univariate polynomial in m_1 using purely linear algebra techniques.

- (”Region II”) The *harder* cases are
$$0 \le L \le \left\lfloor \frac{M-1}{2} \right\rfloor - 1$$

“Brute-force” methods only work in very small cases in Region II!

When $L = 0$, there are 2^M solutions of the S-B equations(!) (the quadrics are already “almost” a Gröbner basis with respect to a *grevlex* order with $m_{N-1} > m_{N-2} > \cdots > m_1$.)

Problems

- Develop an efficient method to solve the S-B equations in the Region II cases

- Understand Region II in more detail:

  1. for given K, L, M, how many solutions?

  2. how many are real?

  3. how many yield monotone decreasing square magnitude response $|H(e^{i\omega})|^2$?

  4. etc.

Some Results in Region II

The number of solutions over $\mathbf{C}$ ($K = 1$):

M/L	0	1	2	3	4	5
5	32	16				
6	64	26				
7	128	48	24			
8	256	78	38			
9	512	152	66	32		
10	1024	278	112	50		
11	2048	512*	192*	86	40	
12	4096	944*	358*	142	62	
13	8192		572*	240*	106	48
14	16384		1020*	402*	174*	74

(* = computed by Bob Lewis of Fordham, using his *Fermat* system for Dixon resultants)

A moment's study of this incomplete table suggests some interesting patterns(!) Can we prove them??

Further Reductions

In fact, can express everything in terms of the moments in $\vec{m} = (m_0, \ldots, m_{L+M})^t$. After normalizing $m[0] = 1$, we get a system of $L + M$ equations in $L + M$ variables, as follows:

- Write $H(z) = (1 + z^{-1})^K P(z)$, $\vec{p} =$ vector of coefficients in P. Then $\vec{h} = T\vec{p}$.

- $\vec{m} = Q\vec{h} = QT\vec{p}$, where Q is a Vandermonde type matrix (from def'n of moments).

- $\Rightarrow \vec{h} = T(QT)^{-1}\vec{m}$

- Hence, can express m_k for $k > L + M$:

  $$m_k = (0, 1^k, 2^k, \ldots, (L + M)^k)T(QT)^{-1}\vec{m}$$

The Variety of the Quadrics

Of course, nothing special about varieties defined by quadrics, but the S-B equations have a *very particular* form:

- The variety $V_{L,M}$ defined by the S-B quadrics in $\mathbf{A}^{2M}$ is smooth of dimension $M - L$

- The S-B quadrics are homogeneous if

  $$\text{weight}(m_i) = i$$

  hence $V_{L,M}$ contains a rational normal curve passing through each point

- In fact, $V_{L,M}$ is the image of an $(M - L)$-fold *rational normal scroll* under a certain "upper-triangular" automorphism of $\mathbf{A}^{2M}$.

- The linear SB equations define a linear section of this "warped scroll".

How We Can Use This

If we write $m_1 = t$ (the common parameter on the curves whose related points are joined to form the scroll), then the equations

$$F^{(2i)}(0) = 0, i = 1, \ldots, L+1$$

and

$$G^{(2j)}(0) = 0, j = 1, \ldots, L$$

imply

$$m_j = t^j, \quad j = 1, \ldots, 2L+2$$

So

$$\vec{m} = (1, t, \ldots, t^{2L+2}, m_{2L+3}, \ldots, m_{L+M})$$

and we can reduce the number of variables even farther.

The "Reduced Equations"

- After making all these reductions, we are left with a system of $M - L - 1$ equations in $M - L - 1$ variables.

- Their form is determined by "how far down into" Region **II** we are from the boundary. That is, for L sufficiently large, all the cases with $M = 2L + q$, for fixed $q \geq 3$ will have a similar shape.

- (There are also "special cases" along early portions of lower diagonals, which are different from the stable form)

- The parameter K enters only in the form of the T matrix. Changing K changes the coefficients of the S-B equations but not their Newton polytopes.

For Instance: $M = 2L + 3$

Along the first diagonal in Region II, of the $M - L - 1 = L + 2$ equations,

- $L + 1$ are linear in $m_{2L+3}, \dots, m_{3L+3}$ (coefficients are polynomials in t)

- Only the last, $(L+2)$nd, equation (the one from the flatness condition $F^{(2M)}(0) = 0$) contains the non-linear term m_{2L+3}^2, plus linear terms in $m_{2L+3}, \dots, m_{3L+3}$.

- To eliminate to a univariate polynomial in t, we can solve the linear equations for $m_{2L+3}, \dots, m_{3L+3}$, then substitute into the last equation. Several non-obvious cancellations occur, yielding following.

- Notation: $[\ell]$ stands for a polynomial of degree ℓ in t.

A Theorem

Several non-obvious cancellations occur, yielding: $m_{2L+3} = [4L+4]/[2L+1]$. As a result,

Theorem 1 *In the cases* $M = 2L+3$, $L \geq 0$, *(the "corners" in Region II boundary), the S-B equations have* $8(L+1)$ *solutions.*

Of these, $2(L+2)$ are real ($L+2$ different filters, up to time reversal). Two of these have monotonic square magnitude response.

This is still actually a "relatively easy" case, as it turns out(!)

For Instance: $M = 2L + 4$

This case (the second diagonal) is somewhat more representative of general phenomena.

Of the $M - L - 1 = L + 3$ equations,

- $L + 1$ are linear in $m_{2L+3}, \ldots, m_{3L+4}$ (coefficients are polynomials in t)

- The $(L+2)$nd equation (the one from the flatness condition $F^{(2M-2)}(0) = 0$) contains the non-linear term m_{2L+3}^2, plus linear terms in $m_{2L+3}, \ldots, m_{3L+4}$.

- The $(L+3)$rd equation contains nonlinear terms m_{2L+4}^2, $m_{2L+3}m_{2L+5}$, and linear terms as above

$M = 2L + 4$, cont.

- To eliminate to a univariate polynomial in t, we can solve the linear equations for $m_{2L+4}, \ldots, m_{3L+4}$, in terms of m_{2L+3}, t, then substitute into the last 2 equations.

- Again, several non-obvious cancellations occur

- Result is two quadratics in m_{2L+3} with coefficients that are polynomials in t.

- Finally, we eliminate m_{2L+3} with by the resultant. Carefully examining the resultant matrix:

Theorem 2 *In the cases $M = 2L + 4$, $L \geq 1$, (the first diagonal below the Region II boundary), the S-B equations have $12L + 14$ solutions.*

$M = 2L + 5$

This is the first time the "stable" form does not begin with $L = 1$. For $L \geq 2$,

- There are $L + 1$ linear equations

- Those allow us to eliminate m_{2k}, $k = L + 2, \ldots, 2L$ and all the odd-order moments except m_{2L+3}, m_{2L+5}

- The remaining 3 equations have quadratic terms in m_{2L+3}, m_{2L+5}

- After linear combinations, can derive an equivalent system with leading terms m_{2L+3}^2, $m_{2L+3}m_{2L+5}$, m_{2L+5}^2.

$M = 2L + 5$, cont.

For simplicity, take $L = 3$.

Solving for m_{13} from the last linear equation gives

$$m_{13} = [4]m_9 + [2]m_{11} + [13]/[3],$$

(where $[\ell]$ means a polynomial of degree ℓ in t).

There are "non-obvious" cancellations in coefficients of m_{13} that remove denominators.

$M = 2L + 5$, cont.

After substituting for m_{13}, and linear combinations to eliminate like terms, additional "non-obvious" cancellations give:

$$
\begin{aligned}
0 &= [0]m_9^2 + [9]m_9 + [7]m_{11} + [18] \\
0 &= [0]m_9 m_{11} + [11]m_9 + [9]m_{11} + [20] \\
0 &= ([3]m_{11}^2 + [16]m_9 + [14]m_{11} + [22])/[3]
\end{aligned}
$$

The multivariable resultant

$$R_{2,2,2} = [3]^2[86]$$

The [3] is the denominator in $m[13]$; the factor of degree 86 is the univariate polynomial we want.

For $L \geq 2$, the general formula on this diagonal is $20L + 26$.

Generalizing This

The following generalizations of the above will work on all the diagonals $M = 2L+q$ in Region II and yield similar results:

- Of the $M - L - 1 = L + q - 1$ equations, $L+1$ will be linear in $m_{2L+4}, \ldots, m_{L+M}$
- The remaining $q-2$ have some quadratic terms in $m_{2L+3}, \ldots, m_{L+M}$
- The general idea is always to solve the linear equations,
- Substitute into the quadratics, then
- Eliminate to a univariate polynomial in t using (multivariable) resultants.

A Word on Methods

The several "non-obvious cancellations" above are actually *quite intricate* – too intricate to discuss in detail here (:( ).

The form of the solutions of the $L+1$ linear equations comes from the *Smith normal form* of the coefficient matrix (a matrix whose entries are polynomials in t).

To determine this, we study the actual coefficients in the polynomials in detail – comes back to $T(QT)^{-1}$ matrix above.

Key tool: the entries of Vandermonde-type matrices like $T(QT)^{-1}$ can be conveniently expressed in terms of *finite-difference operators*.

Vandermondiana

For instance, consider the usual square Vandermonde matrix

$$V = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & n \\ 0 & 1^2 & 2^2 & \cdots & n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1^n & 2^n & \cdots & n^n \end{pmatrix}$$

The last column of the inverse matrix V^{-1} is the vector of coefficients of the finite difference operator Δ^n, ith entry is

$$\frac{(-1)^{i+n}}{n!}\binom{n}{i}$$

The previous column is a linear combination of Δ^n and Δ^{n-1}, and so on.

Vandermondiana, cont.

The entries of coefficient matrices we need can all be expressed in terms of

$$D^j (i-t)^\ell$$

for various j, ℓ, where

$$D^j = (\Delta^j|_{i=0} + \Delta^j|_{i=1})/2$$

Get some very tricky determinant identities for matrices formed of these.