Notes on computing minimal approximant bases

Arne Storjohann

David R. Cheriton School of Computer Science
University of Waterloo, Ontario, Canada N2L 3G1

August 21, 2006

1 Introduction

Let k be a field. The *vector Hermite Padé approximation problem* takes as input

- $N \in \mathbb{Z}_{>0}$, the desired order of the approximant;
- $\mathbf{F} = (f_1, \ldots, f_m)^T \in k[x]^{m\times s}$, a vector of truncated formal power series, say each $f_i \in k[x]^{1\times s}$ of degree bounded by $N-1$;
- $\mathbf{n} = (n_1, \ldots, n_m) \in \mathbb{Z}^m_{[-1,N-1]}$, a tuple of degree constraints with norm defined by $\|\mathbf{n}\| := (n_1+1) + \cdots + (n_m+1)$.

The goal is to compute linearly independant row vectors $\mathbf{P} = (P_1, \ldots, P_m) \in k[x]^{1\times m}$ such that

$$\mathbf{P}(x) \cdot \mathbf{F}(x) = \overbrace{P_1(x)}^{\deg \leq n_1} f_1(x) + \cdots + \overbrace{P_m(x)}^{\deg \leq n_m} f_m(x) = O(x^N). \tag{1}$$

When $s = 1$ and $N = \|\mathbf{n}\| - 1$ this is the classical *Hermite Padé approximation problem.* Here we allow N to be arbitrary. We describe algorithms for computing an order N *genset* of type $\mathbf{n}$: a matrix $V \in k[x]^{*\times m}$ such that every row of V is a solution to (1) and every solution $\mathbf{P}$ of (1) can be expressed as a $k[x]$-linear combination of the rows of V. Ideally, V will be a *minbasis* of solutions: V has full row rank, and if $\bar{n} \geq \max_i n_i$ then $V \mathrm{diag}(\bar{n}-n_1, \ldots, \bar{n}-n_m)$ is row reduced (e.g., in weak Popov form). To compare with [1], an order N minbasis of type $\mathbf{n}$ will be comprised of those rows of a σ-basis (with $\sigma = sN$) which satisfy the degree constraints (i.e., have positive defect), and vice versa. For example, the Popov form of the

Dagstuhl Seminar Proceedings 06271
Challenges in Symbolic Computation Software
http://drops.dagstuhl.de/opus/volltexte/2006/776

order 8 minbasis of type $(1,1,1,1,1)$ for

$$\mathbf{F} = \begin{bmatrix} 90\,x^7 + 22\,x^6 + 42\,x^5 + 3\,x^4 + 87\,x^3 + 41\,x^2 + 35 \\ 24\,x^6 + 93\,x^5 + 14\,x^4 + 87\,x^3 + 62\,x^2 + 15\,x + 80 \\ 53\,x^7 + 71\,x^6 + 80\,x^5 + 22\,x^4 + 87\,x^3 + 90\,x^2 + 57\,x + 42 \\ 47\,x^7 + 23\,x^6 + 75\,x^5 + 5\,x^4 + 6\,x^3 + 74\,x^2 + 72\,x + 37 \\ 74\,x^7 + 87\,x^6 + 44\,x^5 + 29\,x^4 + x^3 + 74\,x^2 + 10\,x + 36 \end{bmatrix} \in \mathbb{Z}/(97)[x]^{5\times 1}$$

is

$$\begin{bmatrix} x+47 & 57 & 58\,x+44 & 9\,x+23 & 93\,x+76 \\ 15 & x+18 & 52\,x+23 & 15\,x+58 & 93\,x+88 \end{bmatrix} \in \mathbb{Z}/(97)[x]^{5\times 5}.$$

The Popov form of the complete σ-basis (with $\sigma = 8$) of $\mathbf{F}$ is

$$\left[\begin{array}{ccccc} x+47 & 57 & 58\,x+44 & 9\,x+23 & 93\,x+76 \\ 15 & x+18 & 52\,x+23 & 15\,x+58 & 93\,x+88 \\ \hline 17 & 86 & x^2+77\,x+16 & 76\,x+29 & 90\,x+78 \\ 44 & 36 & 3\,x+42 & x^2+50\,x+26 & 85\,x+44 \\ 2 & 22 & 54\,x+94 & 73\,x+24 & x^2+2\,x+25 \end{array}\right] \in \mathbb{Z}/(97)[x]^{5\times 5}.$$

Recall that σ-bases, or minimal approximant bases, are always square and nonsingular $m \times m$ matrices. A σ-basis gives a minbasis of type $(n_1 - j, \ldots, n_m - j)$ for all integer shifts j: as in the example above some rows in a σ-basis may not be solutions to (1). A minbasis of type $(n_1, \ldots, n_m)$ gives a minbasis of type $(n_1 - j, \ldots, n_m - j)$ only for all nonnegative integer shifts j: every row is a solution to (1). Restricting the definition of minbasis and genset to actual solutions of (1) allows us avoid computation of the full σ-basis.

Consider algorithm SPHS from [1] and algorithms `M-Basis/PM-Basis` from [2]. Let us assume[1] that $s \le m$. Each of the calls SPHPS($\mathbf{F}(x^s)[1, x, \ldots, x^{s-1}]^T, \sigma, 2^{\lceil \log_2 \sigma \rceil}, \mathbf{n}$) and `M-Basis/PM-Basis`($\mathbf{F}, N, \mathbf{n}$) will compute a σ-basis of type $\mathbf{n}$. Algorithm SPHPS has cost $O((m^2 + ms)(sN)^{1+\epsilon})$ field operations, while `M-Basis` and `PM-Basis` have cost $O(m^2 s^{\omega-2} N^2)$ and $O(m^\omega N^{1+\epsilon})$, respectively.

On the one hand, algorithms `M-Basis` and `PM-Basis` are particularly efficient when $s \approx m$ and N is not too large. On the other hand, if $s = 1$ and N is large, say $N = m(d+1) - 1$ where $d = \|\mathbf{n}\|/m - 1$, which precisely covers the case of classical Hermite Padé approximation, the resulting worst case runtime estimates for `M-Basis` and `PM-Basis` of $O(m^4 d^2)$ and $O(m^\omega (md)^{1+\epsilon})$, respectively, seem too high. Indeed, algorithm SHPS from [1] uses only $O(m^2 (md)^{1+\epsilon})$ field operations for this case. Here we observe that algorithms `M-Basis` and `PM-Basis` can be used to compute an order N genset of type $\mathbf{n}$ for this case in time $O(m^\omega d^2)$ and $O(m^\omega d^{1+\epsilon})$, respectively.

[1] This restriction on s is not required but simplifies the cost estimates. Moreover, all the classical application of the vector Hermite Padé approximation problem seem to satisfy $s \le m$: see [1, Table 1].

We can outline our approach by giving an example of Hermite Padé approximation as in the last paragraph. Suppose we are starting with the following problem: $\mathbf{F} \in k[x]^{m\times 1}$ and $N = \|\mathbf{n}\| - 1$ where

$$\mathbf{n} = (\overbrace{d,\ldots,d}^{m/2}, \overbrace{2d,\ldots,2d}^{m/4}, \overbrace{4d,\ldots,4d}^{m/8}, \ldots,\ldots, \overbrace{md/2}^{1}).$$

Note that $\|\mathbf{n}\| = \Theta(md\log m)$ for this example. First we transform to a new problem $\bar{\mathbf{F}} \in k[x]^{O(m)\times 1}$ of the same order but of type $\bar{\mathbf{n}}$, each element of $\bar{\mathbf{n}}$ bounded by $O(\|\mathbf{n}\|/m)$, which for this example is $O(d\log m)$. Then we transform to a new problem $\hat{\mathbf{F}} \in k[x]^{O(m)\times O(m)}$ of type type $\hat{\mathbf{n}}$ with $\max_i \hat{n}_i = \max_i \bar{n}_i$. An order $\Theta(\|\mathbf{n}\|/m)$ genset for $\hat{\mathbf{F}}$ of type $\hat{\mathbf{n}}$ can be computed with `PM-Basis` in time $O(n^\omega(d\log m)^{1+\epsilon})$ and gives a genset for the original $\mathbf{F}$.

In general, it is possible to compute an order N genset in time $O(m^\omega(\|\mathbf{n}\|/m)^{1+\epsilon})$ for all problems with $sN = O(\|\mathbf{n}\|)$. This seems to cover most cases arising in practice since a generic problem instance will have no solutions for $sN \geq \|\mathbf{n}\|$, and exactly one solution for $sN = \|\mathbf{n}\| - 1$.

2 Reduction to lower order

For convenience, suppose that $s = 1$, that is, that $\mathbf{F} \in k[x]^{m\times 1}$. Recall that the multi-index of degree constraints $\mathbf{n} = (n_1, \ldots, n_m)$ satisfies $n_i < N$, N the desired order of the approximants. We will show how to construct an equivalent problem of order d, any d satisfying $\max_i n_i \leq d < N$.

First note that, for any $k \geq 0$, an order N minbasis of type $\mathbf{n}$ for $\mathbf{F}$ is an order $N + k$ minbasis of type $\mathbf{n}$ for $x^k\mathbf{F}$, and vice versa. This shows that, up to the transformation $(N, \mathbf{F}) \leftarrow (N + k, x^k\mathbf{F})$ with $k = \mathrm{modp}(d - N, d + 1) \in [0, d]$, we may assume without loss of generality that $N > 2d$ and that $d + 1$ divides $N - d$.

Define $\bar{s} := (N - d)/(d + 1)$, $\bar{m} := m + \bar{s} - 1$,

$$\bar{\mathbf{n}} := (n_1, \ldots, n_m, \overbrace{d-1, \ldots, d-1}^{\bar{s}-1})$$

and construct the matrix

$$\bar{\mathbf{F}} := \left[\begin{array}{c|c|c|c|c} \mathbf{F} & \mathrm{Left}(\mathbf{F}, d+1) & \mathrm{Left}(\mathbf{F}, 2(d+1)) & \cdots & \mathrm{Left}(\mathbf{F}, N-2d-1) \\ \hline & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{array}\right] \bmod x^{2d+1} \in k[x]^{\bar{m}\times\bar{s}}.$$

Suppose $W \in k[x]^{*\times\bar{m}}$ is an order $2d + 1$ minbasis of type $\bar{\mathbf{n}}$ for $\bar{\mathbf{F}}$. Write $W = \left[\begin{array}{c|c} W_1 & W_2 \end{array}\right]$ where $W_1 \in k[x]^{*\times m}$. We claim that W_1 is an order N minbasis of type $\mathbf{n}$ for $\mathbf{F}$. To see that W_1 is a genset it suffices to verify that every row of W_1 is a solution to (1), and in the reverse direction, every solution $\mathbf{P}$ of (1) can be extended to give a solution to the new problem. To see that W_1 is a minbasis it suffices to verify that W_1 is row reduced.

Worked example

We are working over $k = \mathbb{Z}/(97)$. The Popov form of the the order 7 minbasis of type $\mathbf{n} = (1, 1, 0, 1, 1)$ of

$$\mathbf{F} = \begin{bmatrix} 90\,x^6 + 22\,x^5 + 42\,x^4 + 3\,x^3 + 87\,x^2 + 41\,x \\ 35\,x^6 + 24\,x^4 + 93\,x^3 + 14\,x^2 + 87\,x + 62 \\ 15\,x^6 + 80\,x^5 + 53\,x^4 + 71\,x^3 + 80\,x^2 + 22\,x + 87 \\ 90\,x^6 + 57\,x^5 + 42\,x^4 + 47\,x^3 + 23\,x^2 + 75\,x + 5 \\ 6\,x^6 + 74\,x^5 + 72\,x^4 + 37\,x^3 + 74\,x^2 + 87\,x + 44 \end{bmatrix} \in k[x]^{5\times 1}$$

is

$$\begin{bmatrix} x + 40 & 20 & 78 & 9\,x + 84 & 11\,x + 77 \\ 30 & x + 17 & 93 & 32\,x + 9 & 78\,x + 16 \end{bmatrix} \in k[x]^{2\times 5}.$$

For $d = 1$ the above recipe gives

$$\bar{\mathbf{F}} = \begin{bmatrix} 87\,x^2 + 41\,x & 42\,x^2 + 3\,x + 87 & 90\,x^2 + 22\,x + 42 \\ 14\,x^2 + 87\,x + 62 & 24\,x^2 + 93\,x + 14 & 35\,x^2 + 24 \\ 80\,x^2 + 22\,x + 87 & 53\,x^2 + 71\,x + 80 & 15\,x^2 + 80\,x + 53 \\ 23\,x^2 + 75\,x + 5 & 42\,x^2 + 47\,x + 23 & 90\,x^2 + 57\,x + 42 \\ 74\,x^2 + 87\,x + 44 & 72\,x^2 + 37\,x + 74 & 6\,x^2 + 74\,x + 72 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in k[x]^{7\times 3}.$$

The Popov form of the order 3 minbasis of type $(1, 1, 0, 1, 1, 0, 0)$ of $\bar{\mathbf{F}}$ is equal to

$$\left[\begin{array}{ccccc|cc} x + 40 & 20 & 78 & 9\,x + 84 & 11\,x + 77 & 24 & 57 \\ 30 & x + 17 & 93 & 32\,x + 9 & 78\,x + 16 & 58 & 21 \end{array}\right] \in k[x]^{2\times 7}.$$

3 Reduction to smaller degree constraints

Consider the multi-index $(n_1, \ldots, n_m)$. For $b \geq 0$, let ϕ_b be the function which maps a single degree bound n_i to a sequence of degree bounds, all element of the sequence equal to b except for possibly the last, and such that $\|(n_i)\| = n_i + 1 = \|(\phi_b(n_i))\|$. Let $\mathrm{len}(\phi_b(n_i))$ denote the length of the sequence. For example, we have $\phi_3(10) = 3, 3, 2$ with $\mathrm{len}(\phi_3(10)) = 3$, while $\phi_2(11) = 2, 2, 2, 2$ and $\mathrm{len}(\phi_2(11)) = 4$. Computing a genset of solutions to (1) can be reduced to computing an order N genset of type $\bar{\mathbf{n}} = (\phi_b(n_1), \ldots, \phi_b(n_m))$. Corresponding to $\bar{\mathbf{n}}$ define the expansion/compression matrix

$$B := \left[\begin{array}{c|c|c} 1 & & \\ x^{b+1} & & \\ \vdots & & \\ x^{(b+1)\mathrm{len}(\phi_b(n_1))-1} & & \\ \hline & 1 & \\ & x^{b+1} & \\ & \vdots & \\ & x^{(b+1)(\mathrm{len}(\phi_b(n_2))-1)} & \\ \hline & & \ddots \end{array}\right] \in k[x]^{\bar{m}\times m}$$

where $\bar{m} = \sum_i^m \mathrm{len}(\phi_b(n_i)) = \sum_i^m \lceil (n_i+1)/(b+1)\rceil$. Now "expand" to construct

$$\bar{\mathbf{F}} := B \overset{\mathbf{F}}{\left[\begin{array}{c} f_1 \\ \hline f_2 \\ \hline \vdots \end{array}\right]} = \left[\begin{array}{c} f_1 \\ f_1 x^{b+1} \\ \vdots \\ f_1 x^{(b+1)(\mathrm{len}(\phi_b(n_1)-1)} \\ \hline f_2 \\ f_2 x^{b+1} \\ \vdots \\ f_2 x^{(b+1)(\mathrm{len}(\phi_b(n_2)-1)} \\ \hline \vdots \end{array}\right] \in k[x]^{\bar{m}\times s}$$

Let $W \in k[x]^{*\times\bar{m}}$ be an order N genset of type $\bar{\mathbf{n}}$ for $\bar{\mathbf{F}}$. Then the "compression" $WB \in k[x]^{*\times m}$ is an order N genset of type $\mathbf{n}$ for $\mathbf{F}$. In general, WB will not be a minbasis even if W is. However, because W is a minbasis of type $\bar{\mathbf{n}}$, and each element of $\bar{\mathbf{n}}$ is bounded by b, we know that WB has the following very nice property: every approximant $\mathbf{P}$ of type $\mathbf{n}$ for $\mathbf{F}$ can be expressed as a $P = vWB$ for a vector v over $k[x]$ that has degrees bounded by b.

Note: The construction above is obviously just a partial linearization of the problem. On the one hand, the choice $b = 0$ fully linearizes, transforming to an $\|\mathbf{n}\| \times N$ linear system over k, thus reducing the problem to computing a left nullspace. On the other hand, the key point here is that any choice $b = \Omega(\lceil \|\mathbf{n}\|/m\rceil)$ will balance the degree constraints but not increase significantly the dimension of the problem (i.e., $\bar{m} = O(m)$).

Worked example

We are working over $k = \mathbb{Z}/(97)$. The Popov form the order 5 minbasis of type $(0,1,4)$ of

$$\mathbf{F} = \begin{bmatrix} 90\,x^3 + 22\,x^2 + 42\,x + 3 \\ 87\,x^3 + 41\,x^2 + 35 \\ 24\,x^2 + 93\,x + 14 \end{bmatrix} \in k[x]^{3\times 1}$$

is

$$\begin{bmatrix} 0 & 1 & 56\,x^3+16\,x^2+27\,x+46 \\ 1 & 0 & 28\,x^3+18\,x^2+88\,x+76 \\ 0 & 0 & x^4 \end{bmatrix} k[x]^{3\times 3}.$$

If we apply the above recipe with $b=1$ we reduce to a problem

$$\bar{\mathbf{F}} = \begin{bmatrix} 90\,x^3+22\,x^2+42\,x+3 \\ 87\,x^3+41\,x^2+35 \\ 24\,x^2+93\,x+14 \\ 93\,x^3+14\,x^2 \\ 0 \end{bmatrix} \in k[x]^{5\times 1}.$$

If we compute a genset W for $\bar{\mathbf{F}}$ of type $(0,1,1,1,0)$ we can compress to recover a genset G for $\mathbf{F}$:

$$\overset{W}{\begin{bmatrix} 1 & 65 & 59 & 79\,x+88 & 0 \\ 0 & x+45 & 33 & 14\,x+68 & 0 \\ 0 & 18 & x+52 & 38\,x+94 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}} \overset{B}{\left[\begin{array}{c|c|c} 1 & & \\ \hline & 1 & \\ \hline & & 1 \\ & & x^2 \\ & & x^4 \end{array}\right]} = \overset{G}{\begin{bmatrix} 1 & 65 & 79\,x^3+88\,x^2+59 \\ 0 & x+45 & 14\,x^3+68\,x^2+33 \\ 0 & 18 & 38\,x^3+94\,x^2+x+52 \\ 0 & 0 & x^4 \end{bmatrix}} \in k[x]^{4\times 3}.$$

Note that although W is a minbasis for $\bar{\mathbf{F}}$, G is not a minbasis for $\mathbf{F}$, only a genset.

References

[1] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix–type Padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3):804–823, 1994.

[2] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations, 2003. Research Report 2003-2. Laboratoire LIP, ENS Lyon, France.