18th Mediterranean Conference on Control & Automation
Congress Palace Hotel, Marrakech, Morocco
June 23-25, 2010

Computing Approximate GCD of Univariate Polynomials

S. R. Khare, H. K. Pillai*, M. N. Belur

Abstract— **In this paper we discuss the problem of computing the approximate GCD of two univariate polynomials. We construct a linearly structured resultant matrix from given polynomials. We show the equivalence of the full rank property of this resultant matrix and the coprimeness of the polynomials. Further we show that the nearest structured low rank approximation (SLRA) of the resultant matrix gives the approximate GCD of the polynomials. We formulate the problem of computing the nearest SLRA as an optimization problem on a smooth manifold, namely the unit sphere S^{N-1} in $\mathbb{R}^N$.**

Index Terms— **Approximate GCD of polynomials, Nullspace of a Polynomial Matrix, SVD, Structured Low Rank Approximation (SLRA)**

I. INTRODUCTION

Checking for coprimeness of univariate polynomials is not a numerically stable problem as the degree of the GCD polynomial changes drastically with small perturbations in the coefficients of the polynomials (see [1]). This is illustrated in the following example.

Example 1.1: Let $a(s) = s^2+5s+6$ and $b(s) = s+3$. Then clearly $b(s)$ is a factor of $a(s)$, that is $b(s)|a(s)$. However if $b(s)$ is perturbed to $b_\varepsilon(s) = s+3+\varepsilon$ for $\varepsilon \neq 0,-1$, then $b_\varepsilon(s) \nmid a(s)$. Thus a small perturbation in the coefficient of $b(s)$ forces the degree of the GCD polynomial to drop to 0 from 1.

From the above example it is clear that just answering whether the polynomials are coprime is not enough. In order to overcome this problem, the concept of approximate GCD is proposed in [2], [3].

In [2] "the nearest GCD problem" is defined as follows: for given polynomials $a(s)$ and $b(s)$ of degrees m and n respectively and some norm on the space of polynomials, compute polynomials $\tilde{a}$ and $\tilde{b}$ such that $\|a(s)-\tilde{a}(s)\|+\|b(s)-\tilde{b}(s)\|$ is minimized and $\tilde{a}(s)$ and $\tilde{b}(s)$ have nontrivial GCD (that is the degree of the GCD polynomial is at least one).

ε-GCD of polynomials is defined as follows in [3]:

Definition 1.2: Let $a(s)$ and $b(s)$ be given polynomials with degrees n and m respectively. Let some polynomial norm be given and some $\varepsilon > 0$. Then the ε GCD of polynomials is defined as $d^*(s) = \gcd(\tilde{a}(s), \tilde{b}(s))$ where $\tilde{a}(s)$ and $\tilde{b}(s)$ are the ε perturbations of $a(s)$ and $b(s)$ respectively and degrees of $\tilde{a}$ and $\tilde{b}$ are less or equal to n and m respectively.

Using these formulations several approaches to compute the approximate GCD of polynomials are discussed in the literature. These approaches include the matrix pencil approach (see [4]), the subspace method (see [5]), the *QR* decomposition based methods (see [6], [7]), the structured matrix based methods ([8], [9], [10], [11], [12], [13]). The structured matrix methods involve constructing some resultant matrix from the polynomials, for example Sylvester matrix or Bezout matrix and obtaining the nearest Structured Low Rank Approximation (SLRA) of the resultant matrix which yields the approximate GCD of the polynomials. Due to a lot of applications, the problem of computing the nearest SLRA is studied extensively in the literature. Several numerical algorithms to compute the nearest SLRA exist: algorithm called lift and project algorithm (see [14]), algorithm using the linearity of the structure to compute the nearest SLRA (see [15], [16]), the structured total least squares approach (see [12], [13]).

In this paper we construct a sequence of linearly structured resultant matrices from given polynomials $a(s)$ and $b(s)$. We show that the full rank property of some resultant matrix in the sequence is equivalent to the coprimeness of these polynomials. The nearest SLRA of this resultant matrix gives the approximate GCD of given polynomials. The approximate GCDs of different degrees can be obtained by computing the nearest SLRA of appropriate matrix in the sequence. The paper is organized as follows: the remainder of the section is devoted to some preliminaries and problem formulation. In section II we prove the main results of the paper. In section III we introduce the SLRA problem and numerical algorithms to solve the SLRA problem at hand. In section IV we discuss numerical examples to illustrate the algorithms in section III. Finally we conclude in section V.

Let $a(s) = \sum_{i=0}^{n} a_i s^i$ and $b(s) = \sum_{i=0}^{m} b_i s^i$ be given polynomials of degrees n and m respectively. Note that corresponding to each polynomial $a(s)$ of degree n, there is an $(n+1)$ dimensional vector $\mathbf{a} = [a_0 \;\; a_1 \;\; \cdots \;\; a_n]^T \in \mathbb{R}^{n+1}$. Denote by $\mathscr{P}_n$ the space of all polynomials of degree upto n with coefficients from the real field. The norm function $\|\cdot\| : \mathscr{P}_n \to \mathbb{R}_+$ is defined as $\|a(s)\| := \|\mathbf{a}\|_2$. Now we define the problem formally.

Problem Statement 1.3: Let $a(s)$ and $b(s)$ be given polynomials of degrees n and m respectively. Fix $k \in \mathbb{N}$ such that $k \leq \min\{n,m\}$. Find $\tilde{a}(s), \tilde{b}(s) \in \mathscr{P}_{\max\{n,m\}}$ such that degree of $\gcd(\tilde{a}(s), \tilde{b}(s))$ is k and

$$\|(a(s)-\tilde{a}(s)) + (b(s)-\tilde{b}(s))\|$$

*Corresponding Author

S. R. Khare is a Research Scholar in the Department of Electrical Engineering, Indian Institute of Technology Bombay, Powai, Mumbai, India 400076 swanand@ee.iitb.ac.in

H. K. Pillai is with the Department of Electrical Engineering, Indian Institute of Technology Bombay, Powai, Mumbai, India 400076 hp@ee.iitb.ac.in

M. N. Belur is with the Department of Electrical Engineering, Indian Institute of Technology Bombay, Powai, Mumbai, India 400076 belur@ee.iitb.ac.in

is minimized. Compute k common roots of $\tilde{a}(s)$ and $\tilde{b}(s)$, the roots of the approximate GCD of $a(s)$ and $b(s)$.

We now discuss some preliminaries of polynomial matrices which are required to prove the main results of this paper. Let $R(s) \in \mathbb{R}^{1\times 2}[s]$, the space of all polynomial matrices of size 1×2. The degree of the polynomial matrix $R(s)$ is the maximum of the degrees of each polynomial component. The polynomial matrix $R(s) \in \mathbb{R}^{1\times 2}[s]$ with degree n can be written in the matrix polynomial form where the coefficients of the polynomial are real matrices of appropriate size.

$$R(s) = R_0 + R_1 s + \cdots + R_n s^n \tag{1}$$

where $R_j \in \mathbb{R}^{1\times 2}$ for $j = 0,1,\ldots,n$. A polynomial matrix $R(s) \in \mathbb{R}^{1\times 2}[s]$ has rank 1 if at least one of the entries in $R(s)$ is a nonzero polynomial. The nullspace of $R(s)$, denoted by $\mathscr{N}$, is defined as

$$\mathscr{N} = \{y(s) \in \mathbb{R}^{2\times 1}[s] \mid R(s)y(s) = 0\}.$$

The degree of the nullspace $\mathscr{N}$ is defined as the $\min_{y(s)\in\mathscr{N}} \deg\ y(s)$, where $\deg\ y(s)$ denotes the degree of the polynomial vector $y(s)$. For $R(s) \in \mathbb{R}^{1\times 2}[s]$, we find a polynomial vector $y(s) \in \mathscr{N}$ such that $\deg\ y(s)$ is same as the degree of $\mathscr{N}$. Then every vector in $\mathscr{N}$ is a polynomial multiple of $y(s)$. That is

$$\mathscr{N} = \{y(s)\alpha(s) \mid \alpha(s) \in \mathbb{R}[s]\}. \tag{2}$$

II. Main Results

In this section we prove the main results of the paper which are further used in the next section to compute the approximate GCD of polynomials. We start with the following theorem.

Theorem 2.1: Let $a(s)$ and $b(s)$ be given polynomials of degrees n and m respectively. Let $R(s) = [a(s)\ \ b(s)] \in \mathbb{R}^{1\times 2}[s]$. Let $\mathscr{N}$ denote the nullspace of $R(s)$. Then $a(s)$ and $b(s)$ are coprime if and only if degree of $\mathscr{N}$ is $\max\{m,n\}$.

Proof: Let $g(s) = \gcd(a(s),b(s))$ and $\ell(s)$=lcm$(a(s),b(s))$. Define

$$p(s) = \frac{\ell(s)}{a(s)}, \quad q(s) = -\frac{\ell(s)}{b(s)}. \tag{3}$$

Then the polynomials $p(s)$ and $q(s)$ satisfy the following equation:

$$a(s)p(s) + b(s)q(s) \quad = \quad 0. \tag{4}$$

That is $y(s) = [p(s)\ \ q(s)]^T \in \mathscr{N}$. When $\deg\ g(s) = 0$, that is polynomials are coprime, $\deg\ p(s) = m$ and $\deg\ q(s) = n$. Note that no polynomials with lesser degrees satisfy (4) in this case. This implies that the degree of $\mathscr{N}$ is $\max\{m,n\}$. Conversely assume that the degree of $\mathscr{N}$ is $\max\{m,n\}$. Since $y(s) \in \mathscr{N}$, this implies that $\ell(s) = a(s)b(s)$ and $\deg\ g(s) = 0$. ∎

We now construct a sequence of structured matrices from the given polynomial matrix $R(s) \in \mathbb{R}^{1\times 2}[s]$ and discuss the relation of the nullspace $\mathscr{N}$ with the nullspaces of these structured matrices. Let $a(s) = \sum_{i=0}^{n} a_i s^i$ and $b(s) = \sum_{i=0}^{m} b_i s^i$ be given polynomials. Without loss of generality, assume that $n \geq m$. Construct a polynomial matrix $R(s) = [a(s)\ \ b(s)] \in \mathbb{R}^{1\times 2}[s]$ with degree n. Let $X_0 = \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ R_n \end{bmatrix} \in \mathbb{R}^{(n+1)\times 2}$. We now construct the sequence of structured matrices $X_1, X_2, \ldots$ as follows:

$$X_1 = \left[\begin{array}{c|c} X_0 & 0 \\ \hline 0 & X_0 \end{array}\right], \quad X_2 = \left[\begin{array}{c|cc} X_0 & 0 & 0 \\ \hline 0 & & X_1 \\ 0 & & \end{array}\right], \ldots \tag{5}$$

where 0 in the above equation is a zero matrix of size 1×2. For any $i \in \mathbb{N}$, $X_i \in \mathbb{R}^{(i+n+1)\times 2(i+1)}$. Let $\mathscr{K}_i$ be the nullspace of matrix X_i and let $d_i = \dim(\mathscr{K}_i)$. The nullspace $\mathscr{N}$ of the polynomial matrix is related to the nullspaces $\mathscr{K}_i$ of structured matrices in the following way: for any $i \in \mathbb{N}\cup\{0\}$, let $y \in \mathscr{K}_i$. Then partition $y \in \mathbb{R}^{2(i+1)}$ as $y = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_i \end{bmatrix}$ where $y_j \in \mathbb{R}^2$ for $j = 0,1,\ldots,i$. Let $y(s) = \sum_{j=0}^{i} y_j s^j \in \mathbb{R}^{2\times 1}[s]$. It is easy to verify that $y(s) \in \mathscr{N}$. Note that at ith stage of this sequence, if $\mathscr{K}_i \neq \{0\}$, then we get an element of $\mathscr{N}$ of degree i. We prove some important properties of the sequence $\{d_i\}_{i=0,1,\ldots}$ in the following theorem.

Theorem 2.2: Let $R(s) \in \mathbb{R}^{1\times 2}[s]$ be a polynomial matrix of degree n. Let $\{X_i\}_{i=0,1,\ldots}$ be the sequence of structured matrices constructed from $R(s)$ as in the equation (5). Let $\mathscr{K}_i = \ker(X_i)$ and $d_i = \dim(\mathscr{K}_i)$. Then the following statements hold:

(a) The sequence $\{d_i\}_{i=0,1,2,\ldots}$ is a nondecreasing sequence of nonnegative integers.

(b) There exists $n_0 \in \mathbb{N}$ such that $d_{k+1} = d_k + 1$ for all $k \geq n_0$.

Proof: (a) Let $n_0 \in \mathbb{N}$ be the smallest positive integer such that $d_{n_0} > 0$. Let $y \in \mathbb{R}^{(n_0+1)}$ be such that $y \in \mathscr{K}_{n_0}$. Then from the structure of matrices X_i it is clear that for $0 \in \mathbb{R}^2$ $\begin{bmatrix} y \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ y \end{bmatrix} \in \mathscr{K}_{n_0+1}$. Thus $d_{n_0+1} \geq 2d_{n_0}$. In particular $d_{n_0+1} > d_{n_0}$. Let $d_{n_0+1} = 2d_{n_0} + \alpha_1$. Then using similar argument we can show that $d_{n_0+2} = 3d_{n_0} + 2\alpha_1 + \alpha_2 = d_{n_0+1} + d_{n_0} + \alpha_1 + \alpha_2 > d_{n_0+1}$. Generalizing this argument we can show that

$$\begin{aligned} d_{n_0+j+1} &= jd_0 + \sum_{k=1}^{j-1}(j-k)\alpha_k \\ &= d_{n_0+j} + \left(d_0 + \sum_{k=1}^{j}\alpha_k\right) \\ &\geq d_{n_0+j} \end{aligned}$$

for $j = 0,1,2,\ldots$. The first $n_0 - 1$ terms of the sequence are 0. This proves that $\{d_i\}_{i=0,1,2,\ldots}$ is a nondecreasing sequence of nonnegative integers.

(b) From equation (2) it is clear that once we find a polynomial vector $y(s) \in \mathscr{N}$ such that $\deg\ y(s)$ is same as the degree of $\mathscr{N}$, all polynomial vectors in $\mathscr{N}$ can be obtained from linear span of polynomial vectors $y(s), sy(s), s^2y(s), \ldots$.

Further every vector in $\mathscr{K}_i$ corresponds to a degree i polynomial vector in $\mathscr{N}$. Let $n_0 \in \mathbb{N}$ be the smallest number such that $d_{n_0} \neq 0$. This proves that $\alpha_j = 0$ for all $j > n_0$ in part (a). Then it follows that $d_{k+1} = d_k + 1$ for $k \geq n_0$. ■

Corollary 2.3: Let $R(s) \in \mathbb{R}^{1\times 2}[s]$ be a given polynomial matrix with degree n. Construct the sequence $\{d_i\}_{i=0,1,\ldots}$ from $R(s)$ as discussed above. Then the degree of $\mathscr{N}$ denoted by n_0 is the positive integer such that $d_{n_0} = 1$.

Proof: The proof follows from the nullspace characterization as stated in equation (2) and the nondecreasing nature of the sequence $\{d_i\}_{i=0,1,\ldots}$. ■

We now prove the main result of this paper which relates the coprimeness of the polynomials $a(s)$ and $b(s)$ to the full rank property of some structured matrix.

Theorem 2.4: Let $a(s)$ and $b(s)$ be two given polynomials with degrees n and m respectively. Without loss of generality assume that $n \geq m$. Let $R(s) = [a(s) \;\; b(s)] \in \mathbb{R}^{1\times 2}[s]$ with degree n. Construct the sequence of structured matrices $\{X_i\}_{i=0,1,\ldots}$ as in equation (5). Let $g(s) = \gcd(a(s), b(s))$ with $\deg\; g(s) = \mathrm{g}$. Then the following statements hold:

(a) The polynomials $a(s)$ and $b(s)$ are coprime, that is, $\mathrm{g} = 0$ if and only if $d_i = 0$ for $i = 0, 1, \ldots, n-1$.

(b) The degree of the gcd polynomial $g(s)$ is given by $\mathrm{g} = n - n_0$ where n_0 is the positive integer for which $d_{n_0} = 1$.

Proof: (a) Follows from Theorem 2.1 and Corollary 2.3.

(b) Let n_0 be the positive integer such that $d_{n_0} = 1$. Then from Corollary 2.3 the degree of $\mathscr{N}$ is n_0. Also from the arguments in the proof of Theorem 2.1, it follows that the degrees of polynomials $q(s) = -\frac{\ell(s)}{b(s)}$, $p(s) = \frac{\ell(s)}{a(s)}$ are $n - n_0$ and $m - n_0$ respectively. This implies that $\deg\; g(s) = n - n_0$ using the relation $a(s)b(s) = g(s)\ell(s)$. ■

From above theorem, it is clear that the polynomials are not coprime if the matrix X_{n-1} loses rank. Thus if we perturb the matrix X_{n-1} to $\tilde{X}_{n-1}$ such that the matrix $\tilde{X}_{n-1}$ is rank deficient and it has same structure as that of X_{n-1}, then the polynomials $\tilde{a}(s)$ and $\tilde{b}(s)$ obtained from $\tilde{X}_{n-1}$ are not coprime. If this perturbation is given in some optimal way to be explained in the next section, we compute the nearest polynomials $\tilde{a}(s)$ and $\tilde{b}(s)$, such that they have a nontrivial GCD.

III. SLRA: Formulations and Algorithms

In this section we first state the problem of computing the nearest SLRA of a given linearly structured matrix. Then we formulate the approximate GCD problem as an SLRA problem and give an algorithm to compute the approximate GCD. Finally we discuss some numerical algorithms to compute the nearest SLRA of a given matrix.

A. SLRA formulation

Let $\Omega \subset \mathbb{R}^{p\times q}$ denote the subspace of matrices with given structure. Let $B = \{B_1, B_2, \ldots, B_N\}$ be a basis of Ω. Now we define SLRA problem as it is defined in [14].

Problem Statement 3.1: Given $\Omega \subset \mathbb{R}^{p\times q}$, the subspace of matrices with the given structure, and $X \in \Omega$ such that $\mathrm{rank}(X) = k$ for $k \leq \min\{p, q\}$, find a matrix Y such that

$$\min_{Y\in\Omega, \mathrm{rank}(Y)=k-1} \|X - Y\|_F.$$

In this paper, we consider the Frobenius norm as the matrix norm. However in the problem definition above, one can use any matrix norm. We now give another optimization formulation of the SLRA problem as discussed in [15].

Problem Statement 3.2: Let $X \in \Omega$ be given as $X = \sum_{i=1}^{N} x_i B_i$. WLOG we assume $p \geq q$. Let $\mathrm{rank}(X) = q$. Then to find $Z \in \Omega$ such that $Z = \sum_{i=1}^{N} z_i B_i$ such that

$$\min_{z_i, v} \sum_{i=1}^{N} c(B_i)(x_i - z_i)^2$$
$$\text{subject to}$$
$$\left(\sum_{i=1}^{N} z_i B_i\right) v = 0 \;,\; v^T v = 1$$

where $c : B \longrightarrow \mathbb{R}_+$ is a function which relates the cost function in terms of vectors $x = [x_1, x_2, \ldots, x_N]^T$ and $z = [z_1, z_2, \ldots, z_N]^T$ to the Frobenius norm of the difference of the matrices X and Z.

We now give an algorithm to compute the approximate GCD of given polynomials using the SLRA formulations discussed above. Let $a(s)$ and $b(s)$ be given polynomials with $\deg\; a(s) = n$ and $\deg\; b(s) = m$. WLOG assume that $n \geq m$. Then $R(s) = [a(s) \;\; b(s)] \in \mathbb{R}^{1\times 2}[s]$ is a degree n polynomial matrix. Construct the sequence of structured matrices $\{X_i\}_{i=0,1,\ldots}$ as in equation (5). Fix g, the degree of approximate GCD of $a(s)$ and $b(s)$. From Theorem 2.4 we know that if $d_{n-\mathrm{g}} = 1$, then $\deg\; g(s) = \mathrm{g}$. Consider $X_{n-\mathrm{g}} \in \mathbb{R}^{(2n-\mathrm{g}+1)\times 2(n-\mathrm{g}+1)}$. Let $\Omega \subset \mathbb{R}^{(2n-\mathrm{g}+1)\times 2(n-\mathrm{g}+1)}$ be the subspace of all the matrices with same structure as that of $X_{n-\mathrm{g}}$. Then we compute the nearest SLRA $\tilde{X}_{n-\mathrm{g}} \in \Omega$ of $X_{n-\mathrm{g}}$. We construct polynomials $\tilde{a}(s)$ and $\tilde{b}(s)$ from $\tilde{X}_{n-\mathrm{g}}$. The g common roots of these polynomials are the roots of the approximate GCD.

Algorithm 3.3: Algorithm to Compute Approximate GCD

Input: Polynomials $a(s)$ and $b(s)$ with degrees n and m respectively. The degree g of approximate GCD.
Output: The g roots of approximate GCD.

step 1: Construct matrix $R(s) = [a(s) \;\; b(s)] \in \mathbb{R}^{1\times 2}$.
step 2: Construct the structured matrix $X_{n-\mathrm{g}}$.
step 3: Obtain the nearest SLRA $\tilde{X}_{n-\mathrm{g}}$ of $X_{n-\mathrm{g}}$.
step 4: Construct polynomials $\tilde{a}(s)$ and $\tilde{b}(s)$ from $\tilde{X}_{n-\mathrm{g}}$.
step 5: Obtain the common roots of $\tilde{a}(s)$ and $\tilde{b}(s)$.

In the following subsection we discuss an algorithm to compute the nearest SLRA of the given linearly structured matrix.

B. Numerical Algorithm to Compute the Nearest SLRA

We discuss Lift and Project algorithm (see [14]) to compute an SLRA of a given matrix. This algorithm does not yield the nearest SLRA, however we use the output of this algorithm as an initial guess for the method that we propose.

Before writing the algorithm formally, we describe the idea behind the algorithm briefly. Let $X \in \mathbb{R}^{p\times q}$ be a structured matrix of rank r. Then the nearest rank $r-1$ approximation of X is computed using the SVD of X. However this destroys the structure of the matrix. So this low rank approximation is projected back onto the space of structured matrices. This procedure is iterated until one gets the structured low rank approximation. This procedure can shown to be a descent method and hence the convergence of this procedure is guaranteed. Now we write the algorithm formally. Let $\mathbf{P}$ be the projection operator defined on the subspace of matrices with given structure, that is $\mathbf{P} : \mathbb{R}^{p\times q} \to \Omega$.

Algorithm 3.4: Lift and Project Algorithm for SLRA

Input: $X \in \Omega$, a rank r matrix
Output: $\tilde{X} \in \Omega$, a rank $r-1$ matrix

Initialize $\tilde{X} = X$
while rank $(\tilde{X}) == r$
  Compute the SVD of X as $X = \sum_{i=1}^{r} \sigma_i u_i v_i^T$
  Compute the low rank approximation as
  $\hat{X} = \sum_{i=1}^{r-1} \sigma_i u_i v_i^T$
  $\tilde{X} = \mathbf{P}\hat{X}$
end while

We now propose a method to compute the nearest SLRA as follows: we use the formulation as stated in the Problem Statement 3.2. However we do not solve the optimization problem as in [15] and [16]. We break the optimization problem into two nested optimization problems as follows:

$$\min_{v\in\mathbb{R}^q} \left\{ \begin{array}{c} \min_{z_i} \sum_{i=1}^{N} c(B_i)(x_i - z_i)^2 \\ \text{subject to} \\ \left(\sum_{i=1}^{N} z_i B_i\right) v = 0 \end{array} \right\}$$
$$\text{subject to}$$
$$v^T v = 1.$$

The optimization problem inside the braces is called the inner optimization problem. This inner optimization is shown to have a closed form solution. This solution can be completely expressed in terms of the optimization variable v of the outer optimization. In order to solve the inner optimization problem we use Lagrange multiplier approach. Thus the inner optimization problem, I, becomes:

$$I : \min_{z_i,\lambda} \sum_{i=1}^{N} c(B_i)(x_i - z_i)^2 + \lambda^T \left(\sum_{i=1}^{N} z_i B_i\right) v$$

where λ is a vector of Lagrange multipliers. Now differentiating with respect to z_i and λ we get,

$$\text{wrt } z_i: \; z_i = x_i - \frac{1}{2c(B_i)} \lambda^T B_i v \text{ for } i = 1,2,\ldots,N \quad (6)$$
$$\text{wrt } \lambda: \; \left(\sum_{i=1}^{N} z_i B_i\right) v = 0. \quad (7)$$

From equations (6) and (7), we get,

$$\left(\sum_{i=1}^{N} (x_i - \frac{1}{2c(B_i)} \lambda^T B_i v) B_i\right) v = 0$$
$$\Rightarrow \quad \left(\sum_{i=1}^{N} x_i B_i\right) v = \sum_{i=1}^{N} \frac{1}{2c(B_i)} \lambda^T B_i v B_i v$$
$$\Rightarrow \quad X v = D_v \lambda \quad (8)$$

where D_v is defined as

$$D_v = \sum_{i=1}^{N} \frac{1}{2c(B_i)} B_i v (B_i v)^T. \quad (9)$$

Note that D_v is a symmetric nonnegative definite matrix. In order to compute λ we solve linear system (8) to get

$$\lambda = D_v^{-1} X v. \quad (10)$$

Substituting λ from (10) in equation (6), we get,

$$z_i = x_i - \frac{1}{2c(B_i)} v^T X^T D_v^{-1} B_i v \text{ for } i = 1,2,\ldots,N. \quad (11)$$

Thus the optimal value for the inner optimization problem I is given by,

$$\sum_{i=1}^{N} c(B_i)(x_i - z_i)^2 = \sum_{i=1}^{N} (v^T X^T D_v^{-1} B_i v)^2. \quad (12)$$

The outer optimization can be stated completely in the optimization variable v as follows:

$$\min_{v\in\mathbb{R}^q} \sum_{i=1}^{N} \left(v^T X^T D_v^{-1} B_i v\right)^2 \quad (13)$$
$$\text{subject to}$$
$$v^T v = 1.$$

Notice that the constraint set of this optimization problem is S^{q-1}, a unit sphere in $\mathbb{R}^q$, a smooth manifold. Alternatively we can view this constrained optimization problem as a non constrained optimization problem on the manifold S^{q-1}. We use the gradient search algorithm (see [17]) to solve this problem. Before proceeding further, we state the unconstrained optimization problem.

$$\min_{v\in S^{q-1}} f(v) \quad (14)$$

where

$$f(v) = \sum_{i=1}^{N} \left(v^T X^T D_v^{-1} B_i v\right)^2. \quad (15)$$

IV. Numerical Examples

In this section we discuss some numerical examples. We also compare the performance of our algorithm using the numerical examples with some algorithms already existing in the literature.

Example 4.1: (See [2]) Given the polynomials $a(s) = s^2 - 6s + 5$ and $b(s) = s^2 - 6.3s + 5.72$, we compute the nearest noncoprime polynomials. Using our algorithm, we get the polynomials $\tilde{a}(s) = 0.9850s^2 - 6.0030s + 4.9994$ and $\tilde{b}(s) = 1.0149s^2 - 6.2971 + 5.7206$. Here we give only 4 significant digits of the polynomial coefficients. $\|[a(s) \;\; b(s)] -$

$[\hat{a}(s) \;\; \hat{b}(s)]\| = 0.0216$. The common root between $\hat{a}(s)$ and $\hat{b}(s)$ is 5.0989. This example is also addressed in the paper [10] where the results are obtained using the SLRA of the Sylvester matrix. Our results match with the results obtained in [10].

Example 4.2: Consider the polynomials $a(s) = s^2 + 2s - 1$ and $b(s) = s^4 + 4s^3 + 3s + 1$. We compute the approximate GCDs of degrees 1 and 2 for these polynomials. For the case when $\mathrm{g} = 1$, we construct X_3 and compute the nearest SLRA $\tilde{X}_3$. Here $\|(a(s) - \tilde{a}(s)) + (b(s) - \tilde{b}(s))\| = 0.0259$ and the common root is -4.1611. For the case when $\mathrm{g} = 2$, we construct X_2 and compute the nearest SLRA $\tilde{X}_2$. In this case $\|(a(s) - \tilde{a}(s)) + (b(s) - \tilde{b}(s))\| = 1.3697$ and the common roots are -0.1312 and -4.1807.

V. Concluding Remarks

In this paper we address the problem of computing the approximate GCD of univariate polynomials. We construct a linearly structured resultant matrix from given polynomials. The full rank property of this resultant matrix is equivalent to the coprimeness of the polynomials. The nearest SLRA of this structured matrix gives the approximate GCD of the polynomials. The problem of computing the nearest SLRA is formulated as an optimization problem on a smooth matrix manifold, namely unit sphere S^{N-1} in $\mathbb{R}^N$. This approach of computing an approximate GCD is based on the nullspace properties of the polynomial matrix obtained from given polynomials. Hence this approach may be useful to generalize the results of this paper for the case when several polynomials are considered.

References

[1] Z. Zeng, "The approximate GCD of inexact polynomials part I: A univariate algorithm," *Preprint*, 2004.

[2] N. Karmarkar and Y. Lakshman, "On approximate GCDs of univariate polynomials," *Journal of Symbolic Computations*, vol. 26, pp. 653–666, 1998.

[3] V. Y. Pan, "Computation of approximate polynomial GCDs and an extension," *Information and Computation*, vol. 167, pp. 71–85, 2001.

[4] N. Karcanias, M. Mitrouli, and D. Triantafyllou, "Matrix pencil methodologies for computing the greatest common divisor of polynomials: Hybrid algorithm and their performance," *International Journal of Control*, vol. 79, pp. 1447–1461, 2006.

[5] W. Qiu, Y. Hua, and K. Abed-Meraim, "A subspace method for the computation of the GCD polynomial," *Automatica*, vol. 33, pp. 741–743, 1997.

[6] C. J. Zarowski, X. Ma, and F. M. Fairman, "*QR* factorization method for computing the greatest common divisor of polynomials with inexact coefficients," *IEEE Transactions on Signal Processing*, vol. 48, pp. 3042–3051, 2000.

[7] R. M. Corless, S. M. Watt, and L. Zhi, "*QR* factoring to compute the GCD of univariate approximate polynomials," *IEEE Transactions on Signal Processing*, vol. 52, pp. 3394–3402, 2004.

[8] R. Bitmead, S. Kung, B. Anderson, and T. Kailath, "Greatest common divisors via generalized sylvester and bezout matrices," *IEEE Trans. Automat. Control*, vol. AC-23, pp. 1043–1047, 1978.

[9] D. A. Bini and L. Gemignani, "Bernstein-Bezoutian matrices," *Theoretical Computer Science*, vol. 315, pp. 319–336, 2004.

[10] E. Kaltofen, Z. Yang, and L. Zhi, "Structured low rank approximation of Sylvester matrix," in *Dongming Wang and Lihong Zhi, editors, International Workshop on Symbolic-Numeric Computation SNC*, 2005.

[11] D. Sun and L. Zhi, "Structured low rank approximation of a Bezout matrix," *Mathematics in Computer Science*, vol. 1, pp. 427–437, 2007.

[12] J. Winkler and J. Allan, "Structured low rank approximations of the Sylvester resultant matrix for approximate GCDs of Bernstein basis polynomials," *Electronic Transctions on Numerical Analysis*, vol. 31, pp. 141–155, 2008.

[13] J. Winkler and J. Allan, "Structured total least norm and approximate GCDs of inexact polynomials," *Journal of Computational and Applied Mathematics*, vol. 215, pp. 1–13, 2008.

[14] M. T. Chu, R. E. Funderlic, and R. J. Plemmons, "Structured low rank approximation," *Linear Algebra and Its Applications*, vol. 366, pp. 157–172, 2003.

[15] B. D. Moor, "Structured total least squares and l_2 approximation problems," *Linear Algebra and its Applications*, vol. 188,189, pp. 163–205, 1993.

[16] B. D. Moor, "Total least squares for affinely structured matrices and the noisy realization problem," *IEEE Transactions on Signal Processing*, vol. 42, pp. 3104–3114, 1994.

[17] P. A. Absil, R. Mahony, and R. Sepulchre, *Optimization Algorithms on Matrix Manifolds*. Princetion University Press, 2008.