Lecture 34  Linear Equations and Polynomial GCDs

It is still open whether one can find the greatest common divisor (gcd) of two integers in $NC$. In this lecture we will show how to compute the gcd of two polynomials in $NC$. We essentially reduce the problem to linear algebra. First we show how to solve systems of linear equations in $NC$; then we reduce the polynomial gcd problem to such a linear system.

### 34.1 Systems of Linear Equations

We are given a system of $m$ linear equations in $n$ unknowns

\[
\begin{align*}
    a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
    a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
    \vdots \\
    a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m
\end{align*}
\]  

(47)

and wish to find a solution vector $x_1, \ldots, x_n$ if one exists. This is equivalent to solving the matrix-vector equation

\[
Ax = b
\]  

(48)

where $A$ is an $m \times n$ matrix whose $ij^{th}$ element is $a_{ij}$, $x$ is a column vector of $n$ unknowns, and $b$ is an $m$-vector whose $i^{th}$ element is $b_i$.

We have already seen how to solve the following problems in $NC$: 

181
• compute the rank of a matrix;
• find a maximal linearly independent set of columns of a matrix;
• invert a nonsingular square matrix.

The last allows us to solve the system (47) if $A$ is square and nonsingular. What about cases where the system is not square, or where it is square but $A$ is singular?

If we just wish to determine whether the system (48) has a solution at all, we can append $b$ to $A$ as a new column and ask whether this matrix has the same rank as $A$. If so, then $b$ can be expressed as a linear combination of the columns of $A$; the coefficients of this linear combination provide a solution $x$ to (48). If not, then $b$ lies outside the subspace spanned by the columns of $A$ and no such solution exists.

The following NC algorithm will produce a solution to (48) if one exists. First we can assume without loss of generality that $A$ is of full column rank; that is, the columns are linearly independent. If not, we can find a maximal linearly independent set $A'$ of columns of $A$; if $b$ can be expressed as a linear combination of columns of $A$, then it can be expressed as a linear combination of the columns of $A'$, and any solution to $A'x = b$ gives a solution to (48) by extending the solution vector with zeros.

Assume now that $A$ is of full column rank. Using the same technique, we can find a maximal linearly independent set of rows. Since the row rank and column rank of a matrix are equal, the resulting matrix $A''$ is square and nonsingular, so the system $A''x = b''$ has a unique solution, where $b''$ is obtained from $b$ by dropping the same rows as were dropped from $A$ to get $A''$. Either $x$ is also a solution to (48), or no solution exists.

### 34.2 Resultants and Polynomial GCDs

Suppose we are given two polynomials

$$f(x) = a_mx^m + a_{m-1}x^{m-1} + \cdots + a_0$$
$$g(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0$$

and wish to find their gcd. The usual sequential method is the Euclidean algorithm, which generates a sequence of polynomials

$$f_0, f_1, \ldots, f_n,$$

where $f_0 = f$, $f_1 = g$, and $f_{i+1}$ is the remainder obtained when dividing $f_{i-1}$ by $f_i$. In other words, $f_{i+1}$ is the unique polynomial of degree less than the degree of $f_i$ for which there exists a quotient $q_i$ such that

$$f_{i-1} = q_i f_i + f_{i+1}. \quad (49)$$
This sequence is called the *Euclidean remainder sequence*. It must end, since the degrees of the \( f_i \) decrease strictly. The last nonzero polynomial \( f_n \) in the list is the gcd of \( f \) and \( g \). This is proved by showing that a polynomial divides \( f_{i-1} \) and \( f_i \) iff it divides \( f_i \) and \( f_{i+1} \), which is immediate from (49). It follows that all adjacent pairs \( f_i, f_{i+1} \) in the sequence have the same gcd. Since \( f_{n+1} = 0, f_n \) divides \( f_{n-1} \), therefore gcd \( (f_n, f_{n-1}) = f_n \) and gcd \( (f, g) = f_n \) as well.

One can obtain an NC algorithm using the classical *Sylvester resultant* \[17, 15\]. This technique is based on the following relationship:

**Lemma 34.1**

(i) There exist polynomials \( s \) and \( t \) with \( \deg s < \deg g \) and \( \deg t < \deg f \) such that \( \gcd (f, g) = sf + tg \).

(ii) For any polynomials \( s \) and \( t \), \( \gcd (f, g) \) divides \( sf + tg \).

**Proof.**

(i) The proof is by backwards induction on \( n \). For the basis, take \( s = 0 \) and \( t = 1 \). Then \( \deg s = -1 < \deg f_n \) (\( \deg 0 = -1 \) by convention), \( \deg t = 0 < \deg f_{n-1} \), and \( sf_{n-1} + tf_n = f_n \). For the induction step, assume there exist \( s \) and \( t \) with \( \deg s < \deg f_{i+1} \), \( \deg t < \deg f_i \), and \( sf_i + tf_{i+1} = f_n \). Using (49), we have

\[
\begin{align*}
f_n &= sf_i + tf_{i+1} \\
 &= sf_i + t(f_{i-1} - q_if_i) \\
 &= tf_{i-1} + (s - q_i)f_i .
\end{align*}
\]

Moreover, since \( \deg q_i = \deg f_{i-1} - \deg f_i \), we have that \( \deg t < \deg f_i \) and \( \deg (s - q_i) < \deg f_{i-1} \).

(ii) Certainly \( \gcd (f, g) \) divides \( f \) and \( g \). It therefore divides any \( sf + tg \).

\(\square\)

Using Lemma 34.1, we can express the polynomial gcd problem as a problem in linear algebra. Arrange the coefficients of \( f \) and \( g \) in staggered columns to form a square matrix \( S \) as in the following figure, with \( n = \deg g \) columns of coefficients of \( f \) and \( m = \deg f \) columns of coefficients of \( g \). The figure
illustrates the case \( m = 5 \) and \( n = 4 \).

\[
S = \begin{bmatrix}
a_5 & 0 & 0 & 0 & b_4 & 0 & 0 & 0 \\
a_4 & a_5 & 0 & 0 & b_3 & b_4 & 0 & 0 \\
a_3 & a_4 & a_5 & 0 & b_2 & b_3 & b_4 & 0 \\
a_2 & a_3 & a_4 & a_5 & b_1 & b_2 & b_3 & b_4 \\
a_1 & a_2 & a_3 & a_4 & b_0 & b_1 & b_2 & b_3 \\
a_0 & a_1 & a_2 & a_3 & 0 & b_0 & b_1 & b_2 \\
0 & a_0 & a_1 & a_2 & 0 & 0 & b_0 & b_1 \\
0 & 0 & a_0 & a_1 & 0 & 0 & 0 & b_0 \\
0 & 0 & 0 & a_0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

The matrix \( S \) is called the *Sylvester matrix* of \( f \) and \( g \). If we multiply \( S \) on the right by a column vector

\[
x = (s_{n-1}, s_{n-2}, \ldots, s_0, t_{m-1}, t_{m-2}, \ldots, t_0)^T
\]

containing the coefficients of polynomials \( s \) and \( t \) of degree at most \( n - 1 \) and \( m - 1 \), respectively, then the product \( Sx \) gives the coefficients of the polynomial \( sf + tg \), which is of degree at most \( m + n - 1 \).

**Theorem 34.2** The matrix \( S \) is nonsingular if and only if the gcd of \( f \) and \( g \) is 1.

**Proof.**

\((\rightarrow)\) Suppose \( \gcd(f, g) \neq 1 \). Then \( \deg \gcd(f, g) > 0 \). By Lemma 34.1(ii), there exist no \( s \) and \( t \) with \( sf + tg = 1 \), therefore the system \( Sx = (0, \ldots, 0, 1)^T \) has no solution.

\((\leftarrow)\) Suppose \( S \) is singular. Then there exists some nonzero vector \( x \) such that \( Sx = 0 \). This says there exists some pair of polynomials \( s, t \) such that \( sf + tg = 0 \), \( \deg s < \deg g \), and \( \deg t < \deg f \). Then \( sf = -tg \) and \( \deg sf = \deg tg < \deg fg \). Since \( f \) and \( g \) both divide \( sf = -tg \), so does their least common multiple (lcm), thus \( \deg \text{lcm}(f, g) < \deg fg \). Since \( \gcd(f, g) \cdot \text{lcm}(f, g) = fg \),

\[
\deg \gcd(f, g) = \deg fg - \deg \text{lcm}(f, g) > 0,
\]

therefore \( \gcd(f, g) \neq 1 \).

\(\square\)

By Theorem 34.2, we can determine whether the polynomials \( f \) and \( g \) have a nontrivial gcd by computing the determinant of \( S \). This quantity is called the *resultant* of \( f \) and \( g \).

Let us now show how to compute the gcd. Suppose

\[
\gcd(f, g) = x^d + c_{d-1}x^{d-1} + c_{d-2}x^{d-2} + \cdots + c_1x + c_0,
\]
assuming without loss of generality that the leading coefficient is 1. Let \( c \) be the column vector

\[
  c = (0, 0, \ldots, 0, 1, c_{d-1}, c_{d-2}, \ldots, c_1, c_0)^T.
\]

By Lemma 34.1(i), \( Sx = c \) for some \( x \). For any \( e \), let \( S^{(e)} \) be the matrix obtained by dropping the last \( e \) rows of \( S \), and let \( c^{(e)} \) be the vector obtained by dropping the last \( e \) elements of \( c \). Let \( u^{(e)} \) be the vector of the form \((0, 0, \ldots, 0, 1)^T\) of length \( m + n - e \). Note that \( c^{(d)} = u^{(d)} \), where \( d \) is the degree of \( \text{gcd} (f, g) \). Since \( Sx = c \), we have

\[
  S^{(d)} x = u^{(d)} = c^{(d)} \quad (51)
\]

Moreover, for no \( e < d \) does

\[
  S^{(e)} x = u^{(e)} \quad (52)
\]

have a solution; if it did, then \( Sx \) would give a polynomial \( sf + tg \) of degree strictly less than the degree of \( \text{gcd} (f, g) \), contradicting Lemma 34.1(ii). We can thus find the degree \( d \) of \( \text{gcd} (f, g) \) by trying all \( e \) in parallel and taking \( d \) to be the least \( e \) such that (52) has a solution. Once we have found \( d \) and a solution \( x \) for (51), we are done: the solution vector \( x \) is also a solution to \( Sx = c \), thereby giving coefficients of polynomials \( s \) and \( t \) such that

\[
  \text{gcd} (f, g) = sf + tg = Sx.
\]

It is interesting to note that the traditional Euclidean algorithm for polynomial \( \text{gcd} \) amounts to triangulation of the Sylvester matrix (50) by Gaussian elimination.