

4.7. proof of uniqueness. Today I explained why the algorithm always gives the correct answer. Namely, the minimal polynomial is uniquely determined and the algorithm will always give it to you (assuming the number of errors is $\leq m = r/2$).

4.7.1. *a, b are relatively prime.* The algorithm starts with $f(X) = X^{2m}$ and

$$g(X) = d_0 + d_1X + \cdots + d_{2m-1}X^{2m-1}$$

where the coefficients satisfy some homogeneous linear recurrence of degree $\leq m$. The algorithm produces polynomials $h(X), a(X), b(X)$ so that $\deg h < m, \deg b \leq m$ and

$$h(X) = a(X)X^{2m} + b(X)g(X).$$

Lemma 4.9. *a(X), b(X) are relatively prime.*

Proof. The reason is that the 2×2 matrix formed by the last two entries in the a and b columns has determinant ± 1 . This is by induction. We start with the 2×2 matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which has determinant 1. Then, to get the third line, we subtract $Q_1(X)$ times the second row from the first row. This is an elementary row operation which does not change the determinant of the matrix. However, the new row goes to the bottom so the second matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & -Q_1(X) \end{pmatrix}$$

has determinant -1 . Then we subtract $Q_2(X)$ times the third line from the second line. These are rows 2 and 1 in this second matrix. So, again, the determinant remains 1 in absolute value and changes sign. At the end we have a matrix of determinant ± 1 whose last row is (a, b) . So, the greatest common divisor of a, b is 1. \square

4.7.2. $b(0) \neq 0$. The next point I made was that $b(0) \neq 0$. This is the same as saying that X does not divide $b(X)$. This is important for two reasons. First, we use the equation:

$$p(X) = \frac{X^{\deg b} b(1/X)}{b(0)}$$

to obtain the polynomial of the recurrence. The second reason is that, this will imply that $h(X), b(X)$ are relatively prime. By the following lemma, this will imply that a, b, h are unique up to a scalar multiple.

Lemma 4.10. *Suppose that $a_0(X), b_0(X), h_0(X) \in F[X]$ and $a_1, b_1, h_1 \in F[X]$ are two triples of polynomials so that $\deg h_i < m$, $\deg b_i \leq m$ and*

$$h_i(X) = a_i(X)X^{2m} + b_i(X)g(X).$$

Suppose also that $(b_0, h_0) = 1$. Then

$$a_1 = a_0q, \quad b_1 = b_0q, \quad h_1 = h_0q$$

for some $q \in F[X]$.

Proof. The point is that $h_i \equiv b_i g$ modulo X^{2m} . This implies that

$$h_0 b_1 \equiv b_0 b_1 g \equiv h_1 b_0.$$

But $h_i b_j$ has degree less than $2m$. So, we must have

$$h_0(X)b_1(X) = h_1(X)b_0(X).$$

Since b_0, h_0 are relatively prime, $b_0|b_1$ and $h_0|h_1$ with the same quotient q . This also implies that $a_1 = qa_0$. \square

Lemma 4.11. *If the coefficients of $g(X)$ satisfy a homogeneous linear recurrence of degree $\leq m$ then, the polynomial $b(X)$ obtained by the division algorithm has nonzero constant term.*

Proof. I will go over the same example that I did in class, then point out how the argument can be generalized. To make the general argument rigorous, we need to work a little harder.

Suppose that the minimal polynomial is $p(X) = X - 1$. Then the recurrence relation is $d_n = d_{n-1}$ which means that all of the coefficients of $g(X)$ are equal. The reversal of $p(X)$ is the same: $b(X) = X - 1$. Suppose that the algorithm gives a different polynomial: $b(X) = X(X - 1) = X^2 - X$. Since $(a, b) = 1$, we know that $a(0) \neq 0$. But then, the equation

$$h(X) = a(X)X^{2m} + b(X)g(X)$$

tells us that the coefficients of X^{2m-1}, X^{2m-2} in $g(X)$ are not equal, giving a contradiction:

$$\begin{aligned} a(X)X^{2m} + b(X)g(X) &= (X^2 - X)(d_{2m-1}X^{2m-1} + d_{2m-2}X^{2m-2} + \dots) \\ &= (\text{terms of deg } \geq 2m+1) + (a(0) + d_{2m-2} - d_{2m-1})X^{2m} + (\text{lower terms}) \end{aligned}$$

Since $\deg h(X) < m$ we get

$$d_{2m-2} - d_{2m-1} = -a(0) \neq 0$$

which is a contradiction.

In general what happens is that, if $b(0) = 0$, we must have $a(0) \neq 0$ and $h(0) = 0$. If we divide by X we then get:

$$\frac{h(X)}{X} = a(X)X^{2m-1} + \frac{b(X)}{X}g(X)$$

which implies (by induction on m) that the coefficients of $g(X)$ up to degree $2m-2$ satisfy a uniquely determined recurrence of order $\leq m-1$ and furthermore $a(0) \neq 0$ implies that the coefficient of X^{2m-1} does not satisfy this recurrence. Since the recurrence is unique, the coefficients of $g(X)$ do not satisfy any recurrence of degree $< m$. The argument below implies that $g(X)$ will not satisfy a recurrence of degree exactly equal to m . So we get a contradiction.

Claim: Under the conditions above, $g(X)$ does not satisfy any recurrence of degree exactly equal to m , i.e., with minimal polynomial $p(X)$ of degree m .

Suppose it did. Then, letting $b_0(X)$ be the reverse polynomial

$$b_0(X) = \frac{X^m p(1/X)}{p(0)}.$$

(From the definition of the minimal recurrence polynomial we get $p(0) \neq 0$. Also the equation for b_0 implies $b_0(0) \neq 0$.) Then $b_0(X)g(X)$ has no terms of degree $m, m+1, \dots, 2m-1$. So, there is a polynomial $a_0(X)$ so that

$$h_0(X) = a_0(X)X^{2m} + b_0(X)g(X)$$

has degree $< m$. But then b_0, h_0 must be relatively prime (otherwise, we could divide the entire equation by the common factor to obtain a recurrence relation on g of order less than m .) Therefore, by the previous lemma (4.10), b_0 must divide b . But this is a contradiction since b is X times a polynomial of degree $< m$. \square

Putting these two lemmas together we get the following.

Theorem 4.12. *Assuming that the coefficients of $g(X)$ satisfy a homogeneous linear recurrence of order $\leq m$, the division algorithm gives the minimal polynomial $p_0(X)$ of this recurrence and any other recurrence of degree $\leq m$ has polynomial a multiple of $p_0(X)$.*

4.7.3. *proof of uniqueness.* Let me go back to the beginning. The polynomial $g(X) = \sum_{s=0}^{2m-1} d_s X^s$ has coefficients

$$d_s = \sum_{i \in A} c_i \alpha_i^s, \quad c_i = \frac{\epsilon_i}{L_i(\alpha_i)}.$$

The scalars c_i are nonzero for all $i \in A$ by definition of the error set A . Therefore, the numbers d_s satisfy a recurrence with polynomial

$$p(X) = \prod_{i \in A} (X - \alpha_i).$$

The algorithm gives the minimal polynomial $p_0(X)$. So, we still need to show that $p(X)$ is minimal. In class I just said it is because the number ϵ_i are nonzero. But here is a more detailed proof.

Suppose that $p(X)$ is not the minimal polynomial. Then Theorem 4.12 (in fact Lemma 4.10) implies that $p_0(X)$ divides $p(X)$. Thus

$$p_0(X) = \prod_{i \in A'} (X - \alpha_i)$$

for some proper subset $A' \subset A$. But this implies that

$$d_s = \sum_{i \in A'} a_i \alpha_i^s.$$

Subtracting these (letting $a_i = 0$ for $i \in A - A'$) we get

$$\sum_{i \in A} (c_i - a_i) \alpha_i^s = 0$$

for $0 \leq s < 2m$. But this is impossible. This sum represents a linear combination of $|A| \leq m$ columns of the $2m \times 2m$ Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{2m} \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{2m}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2m-1} & \alpha_2^{2m-1} & \alpha_3^{2m-1} & \cdots & \alpha_{2m}^{2m-1} \end{pmatrix}$$

Since $c_i - a_i \neq 0$ for $i \in A - A'$ we have a nontrivial linear relation among the columns of this matrix which is impossible since the Vandermonde determinant is nonzero.