

Re: Integer-Valued Polynomials

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-03/msg00024.html>

- *From:* "Chip Eastham" <hardmath@xxxxxxxxxx>
 - *Date:* 28 Feb 2006 19:04:58 -0800
-

Maury Barbato wrote:

Maury wrote:

Two remarks:

(I) Newton method works also for several variables and for general fields?

There is a risk of confusion in terminology here. I mentioned (1) interpolation and (2) Newton divided differences (as a specific approach to finding an interpolating polynomial). Newton's method often refers to root finding, and while a multivariate form of this (usually called Newton-Raphson) exists, it has little to do with the question of interpolation.

Interpolating polynomials in many variables, versus in one variable, does introduce a complication of choosing interpolating points not "correlated" by a polynomial of smaller degree. See this easily read survey-style article for more information:

[Polynomial interpolation in several variables –
by Tomas Sauer]
<http://www.uni-giessen.de/tomas.sauer/Publ/MAIA.pdf>

(II) Even if it works, it can't be very useful. How

could

you apply it, to use later the "Identity

Polynomials

Principle"?

Re: Integer-Valued Polynomials

But your argument intended maybe to be only intuitive.

My "argument" is an outline, but if you have specific questions perhaps I can fill in more details.

regards, chip

Maury writes:

The point is: let $P(x_1, \dots, x_n)$ be a complex polynomial with integer values when (x_1, \dots, x_n) is in Z^n . How do you construct a rational polynomial $Q(x_1, \dots, x_n)$ which agrees with P on Z^n ?

It seems to me a weak point in your argument.

Considering the polynomials in $C[x_1, \dots, x_n]$ as a vector space over C , the complex numbers, there is a linear functional for each point in Z^n given by the "evaluation" map. These may be employed in a variety of ways to obtain a system of linear equations to solve for the coefficients of an interpolating polynomial for any finite set of points in Z^n .

For example, to uniquely identify a polynomial such that no x_i appears to a power greater than d , we might choose interpolation over the Cartesian product $\{0, 1, \dots, d\}^n$.

It is simple to check that we have $(d+1)^n$ coefficients to determine and $(d+1)^n$ evaluation conditions to satisfy, which leads to a linear system $Au = b$.

One should note that the matrix A contains entries which are ring elements of Z (or more generally of D), since these are the values of monic monomials at the "integer valued" interpolation points, and the entries of right-hand side b are also integer values in the problem you have posed.

The usual elementary row operations will therefore lead us to a rational solution of such a problem, ie. a polynomial with coefficients in Q (or more generally in the field of quotients of D).

Is the solution unique? While you did not directly raise this issue, it is the key to knowing that the rational polynomial we find agrees with P not only on $\{0,1,\dots,d\}^n$ but on all of Z^n (and for that matter on C^n).

The point is that if d is a bound on the degree of any indeterminate x_i appearing in $P(x_1,\dots,x_n)$, then the uniqueness of a solution guaranteed by the invertibility of A applies to the computation as done in $C[x_1,\dots,x_n]$.

Therefore we will say a few words about why the matrix A is invertible, and I'll wait to see if you have further questions.

Using the monic monomials $\text{PROD } x_i^{(k_i)}$ as a basis for this subspace of $C[x_1,\dots,x_n]$ results in the matrix A being a tensor product of the familiar Vandermonde matrices in one dimension, whose nonsingularity depends only on the distinctness of the "knots" (interpolation points) in 1D. A tensor product of nonsingular matrices is again nonsingular.

Let's illustrate with the case of polynomials in X and Y with no powers higher than the first in either unknown:

$$f(X,Y) = pXY + qX + rY + s$$

Then A =

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

$$\text{and } A [s \ r \ q \ p]' = [P(0,0) \ P(1,0) \ P(0,1) \ P(1,1)].$$

A is the tensor product of two 2x2 matrices, both:

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

corresponding to the evaluation of first degree polynomials in one variable at points $\{0,1\}$.

Interpolation at the four indicated points is

Re: Integer-Valued Polynomials

therefore sufficient to uniquely determine a polynomial of the form of $f(X,Y)$.

regards, chip

.