A Linear Algebraic Approach in Teaching Interpolation

Tamir Tassa
Department of Mathematics and Computer Science
The Open University
Ra'anana, Israel
Email: tamirta@openu.ac.il

A Linear Algebraic Approach in Teaching Interpolation

Abstract

A novel approach for teaching interpolation in the introductory course in numerical analysis is presented. The interpolation problem is viewed as a problem in linear algebra, whence the various forms of the interpolating polynomial are seen as different choices of a basis to the subspace of polynomials of the corresponding degree. This approach enables the instructor to relate this topic to the topic of numerical solution of linear algebraic systems and, consequently, to introduce the important notion of stability. Finally, it is proposed to spice up the discussion of interpolation by describing its usage in cryptography for secret sharing.

Subject Classification: Numerical Analysis, Linear Algebra

1 Introduction

One of the fundamental topics in numerical analysis is function approximation. Given a metric linear space V and a subspace $U \subset V$ of "simple" functions, the approximation problem takes the following form: given $f \in V$, find $P \in U$ that best approximates f, in the sense that it minimizes $d(f, P)$, where $d(\cdot, \cdot)$ is the underlying metric. Students of introductory courses in numerical analysis usually encounter three versions of this general approximation problem:

Uniform approximation:

V is the space of bounded functions on some finite closed interval $I \subset \mathbb{R}$; U is the subspace of polynomials of degree less than or equal to k, for some $k \in \mathbb{N}$; and

(1) $$d(f, g) = \max_{x \in I} | f(x) - g(x) |$$

Least squares approximation:

V is the space of square-integrable functions on some finite closed interval $I \subset \mathbb{R}$; U is the subspace of polynomials of degree less than or equal to k, for some $k \in \mathbb{N}$; and

(2) $$d(f, g) = \int_{x \in I} | f(x) - g(x) |^2 \, dx$$

Interpolation:

V is the space of continuous functions on some finite closed interval $I \subset \mathbb{R}$; U is the subspace of polynomials of degree less than or equal to k, for some $k \in \mathbb{N}$; and

(3) $$d(f, g) = \sum_{j=0}^{k} | f(x_j) - g(x_j) |$$

where $x_j \in I$ for all $0 \le j \le k$. (Here d is only a semi-metric since $d(f, g) = 0$ does not imply that $f = g$ in the interval I.)

This paper concentrates on the interpolation problem and describes a novel approach in teaching this topic. The structure of the paper is as follows. The common approach in which interpolation is taught is described in Section 2. Then, in Section 3, an equivalent linear algebraic approach is proposed for teaching this topic. Finally, an

interesting application of interpolation to cryptography is described in Section 4. Such an example could be very attractive, as it differs from the computational examples that are usually given in introductory numerical analysis courses.

2 The common approach

The interpolation problem is defined as follows in all textbooks, e.g. [1,3,4,5,7,8,9]: Given $k+1$ distinct points in $\mathbb{R}$, $\{x_j\}_{0\le j\le k}$, and a function f, find a polynomial of degree less than or equal to k that agrees with f on these points.

The first question that arises is whether that problem is well-posed. Namely, does a solution (an interpolating polynomial) exist and is it unique. Existence is usually demonstrated by the Lagrange polynomials. The Lagrange polynomials for $\{x_j\}_{0\le j\le k}$ are defined as follows:

$$L_j(x) = \prod_{0\le i\le k,\, i\ne j} \frac{x - x_i}{x_j - x_i}, \quad 0 \le j \le k. \tag{4}$$

Since

$$L_j(x_i) = \delta_{i,j}, \quad 0 \le i, j \le k, \tag{5}$$

where $\delta_{i,j}$ is the Kronecker delta (namely, $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise), the polynomial

$$P(x) = \sum_{j=0}^{k} f(x_j) L_j(x) \tag{6}$$

is a polynomial of degree at most k that satisfies $P(x_j) = f(x_j)$ for all $0 \le j \le k$. As for uniqueness, assume that $Q(x)$ is another interpolating polynomial of degree at most k. Then $D = P - Q$ is a polynomial of degree at most k that vanishes in the $k+1$ distinct points $\{x_j\}_{0\le j\le k}$. This is possible only if $D \equiv 0$, namely, if P and Q are the same polynomial.

The Lagrange polynomials, (4), provide a neat closed form formula for the interpolating polynomial, (6). However, this form of the interpolating polynomial suffers from two major disadvantages. First, the evaluation of the expression in (6) is inefficient as it involves a large number of multiplications and divisions. Moreover, having the value of the interpolating polynomial to f on the set of points

$\{x_j\}_{0\le j\le k}$, denoted P_k, at some intermediate point ξ, it is impossible to use $P_k(\xi)$ in order to compute the value of a higher degree interpolating polynomial to f at ξ, $P_{k+1}(\xi)$, once we are given the value of f in an additional point x_{k+1}. A new computation that begins from scratch is inevitable.

In view of these disadvantages, the Lagrange form of the interpolating polynomial is considered to be mainly of a theoretical value. The alternative Newton form is more practical. The Newton form of the polynomial is

$$P(x) = \sum_{j=0}^{k} a_j \prod_{i=0}^{j-1} (x - x_i) \ .$$

The coefficients in this representation are the so-called divided differences of f,

$$a_j = f[x_0,\ldots,x_j] \ , \quad 0 \le j \le k \ ,$$

where the divided differences of a function f are defined recursively as follows:

$$(7)_1 \qquad f[x_0,\ldots,x_j] = \frac{f[x_1,\ldots,x_j] - f[x_0,\ldots,x_{j-1}]}{x_j - x_0} \ ,$$

$$(7)_2 \qquad f[x_i] = f(x_i) \ .$$

This form of the interpolating polynomial is much more practical than that of the Lagrange form. It may be efficiently evaluated using Horner's method, and when given the value of f at a new sampling point, x_{k+1}, all we have to do is to compute the $(k+1)$-th order divided difference $f[x_0,\ldots,x_{k+1}]$, using (7) and the k-th order divided differences, and then add to $P_k(x)$ the value of the last term only, namely,

$$P_k(x) \mapsto P_{k+1}(x) = P_k(x) + f[x_0,\ldots,x_{k+1}] \cdot \prod_{i=0}^{k} (x - x_i) \ .$$

3 A linear algebraic approach

The interpolation problem is nothing but a problem of solving a system of linear equations. It is proposed to present the interpolation problem as such, and then present the various forms of the interpolating polynomial as different choices of a basis to the subspace of polynomials. We begin by reformulating the interpolation problem in a way that ignores the approximating origin of the problem (i.e., we do not care that the given data are samples of some function f) and focuses on the main issue in hand:

finding a vector in a given finite-dimensional space that satisfies a number of linear equalities.

The interpolation problem: Given $k+1$ points in $\mathbb{R}^2$, $\{(x_j, y_j)\}_{0\le j\le k}$, find the polynomial $P \in \mathbb{R}_k[x]$, where $\mathbb{R}_k[x]$ is the linear space of real univariate polynomials of degree at most k, such that $P(x_j) = y_j$ for all $0 \le j \le k$.

The standard basis for $\mathbb{R}_k[x]$ is $\{x^j\}_{0\le j\le k}$. Seeking the solution for the interpolation problem in its representation with respect to this basis, $P(x) = \sum_{j=0}^{k} a_j x^j$, we need to solve a full system of linear equations,

(8) $V\mathbf{a} = \mathbf{y}$,

where V is the Vandermonde matrix over $\{x_j\}_{0\le j\le k}$, namely, $V_{i,j} = x_i^j$, $0 \le i, j \le k$, $\mathbf{a} = (a_0, \ldots, a_k)^T$ is the vector of unknown coefficients, and $\mathbf{y} = (y_0, \ldots, y_k)^T$ is the vector of required polynomial values. As done in several textbooks [1,3,7,8], the linear system (8) may be shown to have a unique solution, since

(9) $$\det V = \prod_{0\le i<j\le k} (x_j - x_i) \neq 0 .$$

This provides a unified and a beautiful proof of the existence as well as uniqueness of the interpolating polynomial. We believe that this proof must be presented alongside the two separate proofs of existence and uniqueness that were described in Section 2 because of the importance of the Vandermonde matrix, the beauty of the proof of (9), and, most importantly, because existence of a solution of a square linear system is equivalent to uniqueness, and, therefore, it is wrong to discuss these two questions as though they are not related.

There is another advantage for beginning the discussion of the interpolation problem by presenting the linear system (8). One of the most important notions in mathematical analysis is the notion of well-posedness. Loosely speaking, a mathematical problem is well-posed if it has a solution, the solution is unique, and its dependence on the problem parameters is stable. Stability, the last ingredient, is of paramount importance especially in numerical analysis since it is important to

consider the effect of small rounding, measurement and truncation errors on the solution of the problem. For some reason, the question of stability is usually not addressed in the context of the interpolation problem. Assuming that the students have already learnt the subject of numerical solutions to linear systems, equality (8) implies that

$$\|\mathbf{a}\| \le \left\|V^{-1}\right\| \cdot \|\mathbf{y}\| \ ,$$

for any vector norm $\|\cdot\|$ and the corresponding induced matrix norm (denoted also by $\|\cdot\|$). Hence, the maximal error in the value of the coefficients of the polynomial is bounded by the l_∞-norm of V^{-1} times the maximal error in the data. This establishes the stability of the interpolation problem, whence, together with existence and uniqueness, it is a well posed problem. In our opinion, a first course in numerical analysis must introduce the terms of stability and well-posedness, even informally, and then the interpolation problem provides an excellent framework in which those terms may be exemplified.

The next step is to discuss the linear system (8) from a numerical point of view. This is a full system that needs to be solved, and, in addition, the Vandermonde matrices are often ill-conditioned [6]. While the analysis of the condition number of Vandermonde matrices is beyond the scope of an introductory course, it is important to state this and exemplify it, as a good example for the theory of numerical solution of linear systems. Having said that, the standard basis proves to be of theoretical importance only, whence we proceed to seek an alternative basis of $\mathbb{R}_k[x]$.

As our next choice of a basis of $\mathbb{R}_k[x]$, we consider the basis of Lagrange polynomials, (4). The instructor may ask the students to show their linear independence and conclude that they form a basis of $\mathbb{R}_k[x]$. Then, looking for our interpolating polynomial in its representation with respect to this basis, we find out, thanks to (5), that the matrix of coefficients is the identity matrix. Hence, this basis seems like the best that one may hope for, as it replaces a full ill-conditioned system with the trivial system. However, due to the problems that were discussed before, this is still not the basis of choice.

Finally, we arrive at the most suitable choice of a basis of $\mathbb{R}_k[x]$, i.e., the Newton basis:

$$N_j(x) = \prod_{i=0}^{j-1}(x - x_i), \qquad 0 \le j \le k \ .$$

Once again, it is a good exercise to prove that this set of polynomials is linearly independent, and, consequently, a basis of $\mathbb{R}_k[x]$. Trying to find the representation of the interpolating polynomial with respect to this basis, we get a triangular system of equations, since $N_j(x_i) = 0$ for all $0 \le i \le j-1$. A triangular system is definitely better than a full system, as in (8), since its cost of solution is $O(k^2)$ rather than $O(k^3)$. On the other hand, it is inferior to the trivial system, where the solution is given for free. However, the advantages that were discussed before make the Newton basis the basis of choice.

To summarize, a linear algebraic approach to the problem of interpolation enables to introduce the three forms of the interpolating polynomial as representations with respect to three different bases of the subspace of polynomials of degree at most k; it conveys the important message that having identified a problem as a problem in linear algebra is not enough - a good choice of a basis is of paramount importance. This approach highlights the advantages and disadvantages of those three forms; it enables to relate this discussion to the topic of numerical solution of linear systems that is usually also taught in introductory courses of numerical analysis; and it provides an appropriate stage for the introduction of the important notion of stability.

4 Secret sharing

It is not a secret that the introductory course in numerical analysis is not considered an attractive course. Students, as well as some instructors whose areas of interest do not include numerical analysis and scientific computing, tend to consider it a dull course that deals with "errors" and "number crunching", and the main reason for studying it is the simple fact that in many programs in both mathematics and computer science it is a mandatory course. However, we believe that by highlighting the theoretical foundations of numerical analysis (namely, focusing more on the *analysis* and less on the *numerical* aspects), may make this course more attractive. This is one of the main

incentives behind the linear algebraic approach that we proposed herein and, from our classroom experience, this approach indeed caught the attention and interest of the students.

Another way of spicing up the course is by providing more refreshing examples than the ones that are usually given. The typical examples of interpolation revolve around the computation of some function in intermediate points based on some samples of that function. We found that giving the following usage of interpolation fascinated the students and contributed a lot to their enthusiasm in class.

The topic of **secret sharing** was introduced, independently, by Blakley and Shamir in their seminal works [2,10]. It deals with the safe sharing of a secret among a group of people. For example, assume that *Interpolania* is a country that has nuclear missiles. In order to launch those missiles, a secret password must be introduced. This password should be given to the president, the prime minister, the minister of defense, and the chief of staff only. However, providing the password to each of these persons gives each one of them the power to launch the missiles. This is a very risky situation. Instead, as a security measure, we would like to give each one of them a piece of information that, on its own, reveals nothing on the actual secret, but any two of these pieces enable the reconstruction of the secret. This way, at least two of the above mentioned persons must collaborate in order to launch the missiles.

More generally, let S be a secret and let U be a group of n participants. We would like to give each of these participants a piece of information, called *a share*, so that any $k \le n$ shares enable the reconstruction of S, while any lesser number of shares reveal no information about S.

The solution that was proposed by Shamir is extremely elegant. The secret S in his method is presented as an element in a large finite field F. Every participant $u \in U$ is identified with some distinct field element, $x_u \in F$, where $x_u \neq 0$. Next, the dealer (the party that generates the secret S and deals to each participant her or his share) generates $k-1$ random field elements $a_i \in F$, and creates the polynomial $P(x) = S + \sum_{i=1}^{k-1} a_i x^i$. Then, each participant $u \in U$ receives the share $P(x_u)$.

Obviously, every k participants from U may recover P by means of interpolation and then deduce the value of $S = P(0)$. On the other hand, any lesser number of participants may learn no information on S, even if they pool together all of their shares, since any $k' < k$ point values of P at points $x_u \neq 0$ still allow $P(0)$ to equal any value in the field F (this is a consequence of the *existence* of a solution to the interpolation problem).

To illustrate this method, assume a bank that has a safe that must be opened every working day by punching an 8-digit password on its panel. That password is to be shared among the employees of the bank so that any three of them may open the safe, while any lesser number of employees cannot. To that end, we think of the password as an element in a finite field that contains all possible 8-digit passwords. The finite field F_p of the prime order $p = 100,000,007$ is an adequate choice in this case. Assume that the secret password is $S = 12345678$. Next, the bank generates a random quadratic polynomial with S being its free coefficient. Such a polynomial takes the form $P(x) = S + a_1 x + a_2 x^2$ where a_1 and a_2 are two random and independent numbers from F_p. Then, each employee is identified with some field element x and receives the secret share $P(x)$. For example, if Alice is identified with the field element $x = 2$, her secret share will be $S_{\text{Alice}} = \left(S + 2a_1 + 4a_2\right) \bmod p$. Finally, every three employees can find the value of S by recovering $P(x)$ by means of interpolation and then substituting $S = P(x = 0)$. On the other hand, any two employees posses an under-determined system of two linear equations in the three unknown coefficients of the polynomial, where the subspace of possible solutions of that system includes a solution (S, a_1, a_2) for each possible value $S \in F_p$. Hence, the shares of any two employees do not reveal any information on the value of the secret S.

It should be made clear that all of the formulas of both Lagrange and Newton interpolation work also above finite fields, when all of the arithmetic operations are interpreted in the sense of modulo p. While addition, subtraction and multiplication modulo p are straightforward, the operation of division requires to compute an inverse modulo p. More specifically, the fraction $\frac{a}{b}$ is meaningful if and only if b is

invertible modulo p, namely, when $\gcd(b, p) = 1$, and then the fraction equals $ab^{-1} \bmod p$.

Secret sharing is a very good example of a possible usage of interpolation since it is different from the typical examples from engineering or physics and since it is a discrete example: numerical analysis, by definition, deals with the approximate solution of problems of *continuous* nature. Hence, the underlying field is usually $\mathbb{R}$ (or $\mathbb{C}$ in some cases). Here, the underlying field is a finite one. Nevertheless, the theory of interpolation is indifferent to the underlying field.

In this context, the following exercises may be very illustrative:

1. To show that the secret S may be the coefficient of the highest power x^{k-1} (as opposed to the original suggestion to use the coefficient of x^0 as the secret). To that end, the students need to show that every k participants may deduce the value of S while any lesser number of participants cannot reveal anything about its value.
2. To show that apart from the two extreme coefficients, none of the intermediate coefficients can serve for that matter.

References

[1] K.E. Atkinson, *An Introduction to Numerical Analysis*, John Wiley & Sons, New York, 1978 (ISBN: 0471624896).

[2] G.R. Blakley, Safeguarding cryptographic keys, In *Proceedings of the National Computer Conference 1979*, AFIPS 48 (1979), 313-317 (ISSN: 00956880).

[3] B. Bradie, A *Friendly Introduction to Numerical Analysis*, Pearson Education, New Jersey, 2006 (ISBN: 0130130540).

[4] R.L. Burden and J.D. Faires, *Numerical Analysis*, 8th edition, Thomson Brooks/Cole, 2005 (ISBN: 0534392008).

[5] S.D. Conte and C. de Boor, *Elementary Numerical Analysis, An Algorithmic Approach*, 3rd edition, McGraw-Hill, 1981 (ISBN: 0070124477).

[6] W. Gautschi, Questions of numerical condition related to polynomials. In *Studies in Numerical Analysis* (G.H. Golub, ed.), MAA Studies in Mathematics, 24 (1984), 140-177 (ISBN: 0883851261).

[7] E. Isaacson and H.B. Keller, *Analysis of Numerical Methods*, John Wiley & Sons, New York, 1996 (ISBN: 0486680290).

[8] D. Kincaid and W. Cheney, *Numerical Analysis: Mathematics of Scientific Computing*, 3rd edition, Brooks/Cole, 2002 (ISBN: 0534389058).

[9] A.Quarteroni, R. Sacco and F. Saleri, *Numerical Mathematics*, Springer, 2000 (ISBN: 0387989595).

[10] A. Shamir, How to share a secret, *Communications of the ACM*, 22 (1979), 612-613 (ISSN: 00010782).