From Cramer Rule to Lagrange Interpolation

Zhengjun Cao, Lihua Liu

Abstract. Multivariate interpolation arises in a wide range, including computer graphics, multi-secret sharing and secure multiparty computation. But its general representation is rarely discussed. In this note, a general representation for univariate interpolation and multivariate interpolation is formulated, which is helpful for multi-secret sharing illustrations and security arguments. The finding offers a new glimpse into the relation between Cramer rule and Lagrange interpolation formula.
Keywords: Cramer rule, Lagrange interpolation, multivariate interpolation, multi-secret sharing.

1 Introduction

Consider a system of linear equations with n variables $x_1, x_2, \cdots, x_n$, written in the matrix form $AX = B$, where coefficient matrix A is an $n \times n$ square matrix, X is an $n \times 1$ column matrix with variables, and B is an $n \times 1$ column matrix with the constants. The Cramer rule [7] is a method for solving systems of equations, owing to the Swiss mathematician Gabriel Cramer (1704-1752). It specifies that if the determinant $|A| \neq 0$ then

$$x_1 = \frac{|A_1|}{|A|}, \ x_2 = \frac{|A_2|}{|A|}, \ \cdots, \ x_n = \frac{|A_n|}{|A|} \tag{1}$$

where A_i is the matrix by replacing the i-th column of A with B.

Let $a_1, a_2, \cdots a_{n-1} \in \mathcal{R}$, and $f(x) = a_0 + a_1 x + \cdots a_{n-1} x^{n-1}$ be a univariate polynomial of degree $n-1$. Given n points $(x_i, f(x_i))_{i=1}^n$, the polynomial can be recovered by Lagrange interpolation formula (Joseph L. Lagrange, 1736-1813)

$$f(x) = \sum_{i=1}^{n} f(x_i) \prod_{j=1, j\neq i}^{n} \frac{x - x_j}{x_i - x_j} \tag{2}$$

It seems that Cramer rule has no clear relevance to Lagrange interpolation formula. But the works [5, 6] reveals that there is a simple expression for multivariate Lagrange interpolation based on Cramer rule. We revisit the interesting representation, and show it is consistent with the famous Lagrange interpolation formula.

Z. Cao, Department of Mathematics, Shanghai University, Shanghai, 200444, China.
L. Liu, Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

2 Cramer rule implies Lagrange interpolation

2.1 The univariate case

Given n distinct nodes $(x_i, f(x_i))_{i=1}^n$ with respect to the $n-1$ degree polynomial $f(x)$, rewrite them as

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_n) \end{pmatrix}$$

Denote the leftmost matrix by S. It is a Vandermonde matrix and its determinant $|S| = \prod_{1\le i\le j\le n}(x_j - x_i) \neq 0$. By Cramer rule, we have

$$a_0 = \frac{|S_1|}{|S|},\ a_1 = \frac{|S_2|}{|S|},\ \cdots,\ a_{n-1} = \frac{|S_n|}{|S|}$$

where S_i, $i = 1, 2, \cdots, n$, is the matrix by replacing the i-th column of S with the column vector $(f(x_1), f(x_2), \cdots, f(x_n))^\top$. Hence, the polynomial is represented as

$$\begin{aligned} f(x) =& \frac{1}{|S|}(|S_1| + |S_2|x + \cdots + |S_2|x^{n-1}) \\ =& \frac{1}{|S|}\left(\begin{vmatrix} f(x_1) & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ f(x_2) & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ f(x_n) & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} + \begin{vmatrix} 1 & f(x_1) & x_1^2 & \cdots & x_1^{n-1} \\ 1 & f(x_2) & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & f(x_n) & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} x + \cdots \right. \\ & \left. + \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & f(x_1) \\ 1 & x_2 & x_2^2 & \cdots & f(x_2) \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & f(x_n) \end{vmatrix} x^{n-1} \right) \end{aligned}$$

Collecting the factor $f(x_1)$, we have

$$\begin{aligned} & \frac{f(x_1)}{|S|}\left(\begin{vmatrix} x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & \ddots & \\ x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} + (-1)^{1+2}\begin{vmatrix} 1 & x_2^2 & \cdots & x_2^{n-1} \\ & & \ddots & \\ 1 & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} x + \cdots \right. \\ & \left. + (-1)^{1+n}\begin{vmatrix} 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} \end{vmatrix} x^{n-1} \right) = \frac{f(x_1)}{|S|}\begin{vmatrix} 1 & x & x^2 & \cdots & x^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}. \end{aligned}$$

Likewise, the polynomial can be rearranged as

$$
\begin{aligned}
f(x) =& f(x_1) \times \frac{\begin{vmatrix} 1 & x & x^2 & \cdots & x^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}}{\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}} + f(x_2) \times \frac{\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x & x^2 & \cdots & x^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}}{\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}} \\
& + \cdots + f(x_n) \times \frac{\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x & x^2 & \cdots & x^{n-1} \end{vmatrix}}{\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \ddots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}} = \sum_{i=1}^{n} f(x_i) \times \frac{|\hat{S}_i|}{|S|} \qquad (3)
\end{aligned}
$$

where $\hat{S}_i$ is the matrix by replacing the i-th row of S with $(1, x, x^2, \cdots, x^{n-1})$. Expanding the determinants, it leads to the popular Lagrange interpolation formula Eq.(2).

2.2 The multivariate case

The representation Eq.(3) can be directly extended to the multivariate case. Let $k = \binom{n+m}{n}$,

$$f(x_1, \cdots, x_m) = c_0 + c_1 x_1 + c_2 x_2 + \cdots + c_{k-1} x_m^n, \quad c_0, c_1, \cdots, c_{k-1} \in \mathcal{R}$$

be an m-variable function of degree n, under the lexicographic ordering, $1; x_1, x_2, \cdots, x_m; x_1^2, x_1x_2, x_1x_3, \cdots, x_1x_m; x_2^2, x_2x_3, \cdots, x_2x_m; \cdots, x_m^n$. Given k nodes $\{x_{1i}, x_{2i}, \cdots, x_{mi}; f_i\}_{i=1}^k$, such that $f_i = f(x_{1i}, x_{2i}, \cdots, x_{mi})$, the multivariate polynomial can be recovered as

$$f(x_1, x_2, \cdots, x_m) = \sum_{i=1}^{k} f_i \times \frac{|\hat{S}_i|}{|S|} \qquad (4)$$

where S is a $k \times k$ matrix,

$$S = \begin{pmatrix} 1 & x_{11} & x_{21} & \cdots & x_{m1} & x_{11}^2 & x_{11}x_{21} & \cdots & x_{11}x_{m1} & \cdots & x_{m1}^n \\ 1 & x_{12} & x_{22} & \cdots & x_{m2} & x_{12}^2 & x_{12}x_{22} & \cdots & x_{12}x_{m2} & \cdots & x_{m2}^n \\ & & & \ddots & & & & \ddots & & \ddots & \\ 1 & x_{1k} & x_{2k} & \cdots & x_{mk} & x_{1k}^2 & x_{1k}x_{2k} & \cdots & x_{1k}x_{mk} & \cdots & x_{mk}^n \end{pmatrix}, \ |S| \neq 0,$$

and S_i is the matrix by replacing the i-th row of S with the row vector

$$(1, x_1, x_2, \cdots, x_m, x_1^2, x_1x_2, \cdots, x_1x_m, \cdots, x_m^n)$$

Example 1. Suppose that $f(x, y) = c_0+c_1x+c_2y+c_3x^2+c_4xy+c_5y^2$ is a bivariate polynomial of degree 2. Given six nodes $(0, 1, 10), (1, 0, 7), (1, 1, 21), (1, 2, 47), (2, 1, 40), (2, 2, 71)$, we have

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ y \\ x^2 \\ xy \\ y^2 \end{pmatrix} = \begin{pmatrix} 10 \\ 7 \\ 21 \\ 47 \\ 40 \\ 71 \end{pmatrix}, \quad |S| = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{vmatrix} = 4,$$

$$|S_1| = \begin{vmatrix} 1 & x & y & x^2 & xy & y^2 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{vmatrix} = 2x^2 - 6x + 4, |S_2| = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & x & y & x^2 & xy & y^2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{vmatrix} = 2y^2 - 6y + 4,$$

$$|S_3| = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & x & y & x^2 & xy & y^2 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{vmatrix} = -4x^2 + 4yx + 4x - 4y^2 + 4y,$$

$$|S_4| = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & y & x^2 & xy & y^2 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{vmatrix} = 2y^2 - 4xy + 2y + 4x - 4,$$

$$|S_5| = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & x & y & x^2 & xy & y^2 \\ 1 & 2 & 2 & 4 & 4 & 4 \end{vmatrix} = 2x^2 - 4yx + 2x + 4y - 4,$$

$$|S_6| = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 4 \\ 1 & 2 & 1 & 4 & 2 & 1 \\ 1 & x & y & x^2 & xy & y^2 \end{vmatrix} = 4yx - 4x - 4y + 4.$$

Therefore, the interpolated polynomial is

$$\begin{aligned} f(x,y) =& 10 \times \frac{2x^2-6x+4}{4} + 7 \times \frac{2y^2-6y+4}{4} \\ &+ 21 \times \frac{-4x^2+4xy+4x-4y^2+4y}{4} + 47 \times \frac{2y^2-4xy+2y+4x-4}{4} \\ &+ 40 \times \frac{2x^2-4xy+2x+4y-4}{4} + 71 \times \frac{4xy-4x-4y+4}{4} \\ =& 1+2x+3y+4x^2+5xy+6y^2 \end{aligned}$$

It is worth noting that multivariate interpolation can be used for multi-secret sharing [2, 4] and secure multiparty computation [1, 3]. The general representation Eq.(4) is helpful for their illustrations and security arguments.

3 Conclusion

The uniform representation for multivariate interpolation could be of less computational importance, because it needs to compute many determinants. The usual method naturally needs to compute one inverse matrix so as to determine all coefficients. But the representation may be useful for theoretical analysis without explicitly solving for those coefficients.

References

[1] A. Appan, A. Chandramouli, and A. Choudhury. Network agnostic perfectly secure multiparty computation against general adversaries. *IEEE Trans. Inf. Theory*, 71(1):644–682, 2025.

[2] G. Couteau, L. Devadas, A. Hegde, A. Jain, and S. Schreiber. Multi-key homomorphic secret sharing. In *Advances in Cryptology - EUROCRYPT 2025, Proceedings, Part V*, volume 15605 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2025.

[3] M. Dutta, C. Ganesh, S. Patranabis, and N. Singh. Compute, but verify: Efficient multiparty computation over authenticated inputs. In *Advances in Cryptology - ASIACRYPT 2024 - Proceedings, Part VI*, volume 15489 of *Lecture Notes in Computer Science*, pages 133–166. Springer, 2024.

[4] M. Mkadmi, T. Abualrub, and I. Siap. A verifiable multi-secret sharing scheme based on LCD quadratic residue codes. *Int. J. Comput. Math.*, 102(9):1350–1364, 2025.

[5] P. J. Olver. On multivariate interpolation. *Studies in Applied Mathematics*, 116(2):201–240, 2006.

[6] K. Saniee. A simple expression for multivariate Lagrange interpolation. *SIAM Undergraduate Research Online*, 2007.

[7] D. Serre. *Matrices Theory and Applications, 2 Edition*. Springer, US, New York, 2010.