
ELEMENTOS DE CÁLCULO NUMÉRICO

Primer Cuatrimestre 2026

Práctica N° 3: Interpolación

Problema de Interpolación: Dados $n + 1$ puntos distintos x_0, \dots, x_n (llamados nodos) y $n + 1$ valores y_0, \dots, y_n , buscamos un polinomio $p(x)$ de grado menor o igual a n tal que $p(x_i) = y_i$ para todo $i = 0, \dots, n$.

Ejercicio 1 (Interpolación como problema lineal) *El problema de interpolación se puede ver como una transformación lineal entre espacios vectoriales.*

- (a) Sea \mathcal{P}_n el espacio de polinomios de grado a lo sumo n . Verifique que \mathcal{P}_n es un espacio vectorial y que $\{1, x, x^2, \dots, x^n\}$ es una base.
- (b) Defina el operador de evaluación $\Phi : \mathcal{P}_n \rightarrow \mathbb{R}^{n+1}$ dado por:

$$\Phi(p) = (p(x_0), p(x_1), \dots, p(x_n)).$$

Demuestre que Φ es una transformación lineal.

- (c) Interprete el problema de interpolación como la búsqueda de la transformación inversa Φ^{-1} : ¿qué representan la entrada y la salida de Φ^{-1} ?
- (d) Demuestre que si los nodos x_0, \dots, x_n son distintos, el problema de interpolación tiene solución única.

Sugerencia: Pruebe que Φ es inyectiva. Use que un polinomio no nulo de grado $\leq n$ tiene a lo sumo n raíces.

Ejercicio 2 (Matriz de Vandermonde) *Dados nodos x_0, x_1, \dots, x_n distintos y valores y_0, y_1, \dots, y_n , queremos encontrar el polinomio $p(x) = \sum_{k=0}^n a_k x^k$ que satisface $p(x_i) = y_i$.*

- (a) Escriba el sistema lineal correspondiente en forma matricial $Va = y$. La matriz V se conoce como matriz de Vandermonde.
- (b) Analice el condicionamiento en norma 2 utilizando la caracterización variacional del valor singular mínimo: $\sigma_{\min}(V) = \min_{a \neq 0} \frac{\|Va\|_2}{\|a\|_2}$.
- i. Observe que $\|Va\|_2^2 = \sum_{i=0}^n (p(x_i))^2$, donde $p(x)$ es el polinomio con coeficientes a . Si los nodos x_i cubren densamente el intervalo $[-1, 1]$, interprete esta suma como una aproximación de Riemann escalada para justificar la relación aproximada (donde $C_n = O(n)$):

$$\|Va\|_2^2 \approx C_n \int_{-1}^1 (p(x))^2 dx.$$

- ii. Considere el polinomio de prueba $p(x) = (1 - x^2)^n$. Identifique sus coeficientes no nulos y demuestre usando la identidad $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$ que la norma de los coeficientes satisface $\|a\|_2^2 \geq 4^n/(2n+1)$.
- iii. Justifique que la integral $\int_{-1}^1 (1 - x^2)^{2n} dx$ es pequeña (tiende a 0 con n) mientras que $\|a\|_2^2$ crece exponencialmente.
- iv. Concluya que $\sigma_{\min}(V)$ decae exponencialmente con n , lo que implica que $\kappa_2(V)$ crece exponencialmente.

Ejercicio 3 (Polinomios base de Lagrange) (a) Para los nodos $x_0 = -1, x_1 = 0, x_2 = 1$, calcule explícitamente los tres polinomios base de Lagrange:

$$\ell_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^2 \frac{x - x_j}{x_k - x_j}, \quad k = 0, 1, 2.$$

- (b) Verifique que $\ell_k(x_j) = \delta_{kj}$ (propiedad de Kronecker).
- (c) Verifique que $\ell_0(x) + \ell_1(x) + \ell_2(x) = 1$ para todo x (propiedad de partición de la unidad).
- (d) Use la fórmula de Lagrange para encontrar el polinomio que interpola los puntos $(-1, 2), (0, -1), (1, 4)$.
- (e) Evalúe $p(0.5)$ y compare con evaluación directa en los polinomios base.

Ejercicio 4 (Forma baricéntrica de Lagrange) La forma baricéntrica es una reformulación de la interpolación de Lagrange.

- (a) Defina los pesos baricéntricos:

$$w_k = \frac{1}{\prod_{\substack{j=0 \\ j \neq k}}^n (x_k - x_j)}, \quad k = 0, \dots, n.$$

- (b) Demuestre que el polinomio interpolante se puede escribir como:

$$p(x) = \frac{\sum_{k=0}^n \frac{w_k}{x - x_k} y_k}{\sum_{k=0}^n \frac{w_k}{x - x_k}}.$$

- (c) Compare el costo computacional de evaluar:

- La fórmula de Lagrange estándar: $O(n^2)$ por evaluación.
- La forma baricéntrica: $O(n^2)$ preproceso + $O(n)$ por evaluación.

Ejercicio 5 (Error de interpolación) Sea $f \in C^{n+1}([a, b])$ y p_n el polinomio que interpola f en $n+1$ nodos $x_0, \dots, x_n \in [a, b]$.

- (a) Para $f(x) = e^x$ en $[0, 1]$ con nodos $x_0 = 0, x_1 = 0.5, x_2 = 1$:

- Encuentre el polinomio interpolante $p_2(x)$.

- Estime el error máximo en $[0, 1]$ usando la fórmula del error.
- Compare con el error real $|f(0.25) - p_2(0.25)|$.

(b) ¿En qué puntos x el error es exactamente cero?

Ejercicio 6 (Interpolación a trozos) Dados nodos $x_0 < \dots < x_n$ y valores y_i , la interpolación lineal a trozos $s(x)$ conecta los puntos (x_i, y_i) con segmentos de recta.

(a) Escriba la expresión de $s(x)$ en $[x_i, x_{i+1}]$ y verifique su continuidad en los nodos. Verifique que no es diferenciable en general.

(b) Demuestre la cota de error $\|f - s\|_\infty \leq \frac{h^2}{8} \|f''\|_\infty$, donde $h = \max_i \Delta x_i$.

Ejercicio 7 (Splines cúbicos) Un **spline cúbico** $s(x)$ es una función C^2 que coincide con un polinomio cúbico en cada subintervalo $[x_i, x_{i+1}]$ e interpola los datos.

(a) Cuente los grados de libertad ($4n$ coeficientes) y restricciones ($2n$ de interpolación/continuidad en extremos de intervalos, $2(n-1)$ de suavidad C^1, C^2). Concluya que faltan 2 condiciones de frontera (ej. “natural” $s'' = 0$, o “sujeto” $s' = f'$ en extremos).

(b) Demuestre la propiedad variacional: El spline cúbico natural minimiza la energía de curvatura $\int_a^b [u''(x)]^2 dx$ entre todas las funciones C^2 que interpolan los datos.

Ejercicio 8 (Cuadratura interpolatoria) Un método muy común y general de integración numérica es interpolar el integrando, e integrar el polinomio resultante de manera analítica.

(a) **Regla del trapecio:** Interpole $f(x)$ en $[a, b]$ con una línea recta pasando por $(a, f(a))$ y $(b, f(b))$. Demuestre que obtiene la aproximación:

$$\int_a^b f(x) dx \approx \frac{b-a}{2} (f(a) + f(b)).$$

(b) **Regla de Simpson:** Interpole $f(x)$ en $[a, b]$ con una parábola pasando por $x_0 = a$, $x_1 = (a+b)/2$, $x_2 = b$. Demuestre que obtiene la aproximación:

$$\int_a^b f(x) dx \approx \frac{b-a}{6} \left(f(a) + 4f\left(\frac{a+b}{2}\right) + f(b) \right).$$

(c) Use el teorema del error de interpolación para estimar el error de cada fórmula.

Ejercicio 9 (Límite de precisión de las reglas de cuadratura) Sea $Q_n(f) = \sum_{i=0}^n w_i f(x_i)$ una regla de cuadratura interpolatoria basada en $n+1$ nodos distintos x_0, \dots, x_n .

(a) Si es posible elegir tanto los nodos como los pesos, ¿Cuántos grados de libertad existen?

(b) Demuestre que es imposible construir una regla de cuadratura con $n+1$ nodos que sea exacta para todos los polinomios de grado $2n+2$. **Sugerencia:** Considere el polinomio $P(x) = \prod_{i=0}^n (x - x_i)^2$.

Ejercicio 10 (Diferenciación numérica) Muchas fórmulas de diferenciación numérica se pueden obtener derivando polinomios que interpolan los datos.

(a) Interpole $f(x)$ en $x_0, x_0 + h$ con el polinomio $p_1(x)$ de Lagrange.

(b) Derive $p_1(x)$ para obtener la aproximación de diferencias finitas:

$$f'(x_0) \approx \frac{f(x_0 + h) - f(x_0)}{h}.$$

(c) Interpole $f(x)$ en $x_0 - h, x_0, x_0 + h$ con el polinomio $p_2(x)$.

(d) Derive $p_2(x)$ y evalúe en x_0 para obtener la fórmula centrada:

$$f'(x_0) \approx \frac{f(x_0 + h) - f(x_0 - h)}{2h}.$$

(e) Use el teorema del error de interpolación para estimar el error de truncamiento de cada fórmula.

Transformada Discreta de Fourier

Dado $x \in \mathbb{C}^N$, definimos su DFT como $\hat{x} \in \mathbb{C}^N$ con

$$\hat{x}_k = \sum_{j=0}^{N-1} x_j \omega_N^{jk}, \quad k = 0, \dots, N-1, \quad \text{donde } \omega_N = e^{2\pi i/N}.$$

Ejercicio 11 (Aliasing) Sea $x_j = \omega_N^{mj}$ el modo de Fourier de frecuencia m muestreado en la grilla $j = 0, \dots, N-1$.

(a) Demuestre que $\omega_N^{(m+N)j} = \omega_N^{mj}$ para todo j . Concluya que los modos de frecuencia m y $m + N$ producen exactamente la misma señal discreta.

(b) Más generalmente, demuestre que los modos de frecuencia m y $m + kN$ son indistinguibles para todo $k \in \mathbb{Z}$.

(c) Concluya que con N muestras solo se pueden representar N frecuencias distintas. ¿Cuáles son las frecuencias “esencialmente distintas”?

Ejercicio 12 (Reindexación de frecuencias) La DFT indexa las frecuencias como $k = 0, 1, \dots, N-1$. Pero usando aliasing, las frecuencias altas se pueden reinterpretar como frecuencias negativas.

(a) Para N par, demuestre que el modo $k = N - \ell$ (con $1 \leq \ell \leq N/2 - 1$) es idéntico al modo de frecuencia $-\ell$. Concluya que la DFT con índices $k = 0, \dots, N-1$ es equivalente a usar frecuencias $k = -N/2, \dots, N/2 - 1$.

(b) Si $x \in \mathbb{R}^N$ (señal real), demuestre que $\hat{x}_{N-k} = \overline{\hat{x}_k}$. Concluya que los coeficientes de Fourier para frecuencias negativas son los conjugados de los positivos, y que por lo tanto la DFT de una señal real queda determinada por los coeficientes $\hat{x}_0, \hat{x}_1, \dots, \hat{x}_{N/2}$.

Ejercicio 13 (Difracción por rendijas múltiples) Una red de difracción tiene N rendijas equiespaciadas con separación d . La amplitud compleja en el ángulo θ es proporcional a la suma $A(\theta) = \sum_{n=0}^{N-1} a_n e^{inqd}$, donde $q = \frac{2\pi \sin \theta}{\lambda}$ y $a_n \in \{0, 1\}$ indica si la rendija n -ésima está abierta.

- (a) Identifique $A(\theta)$ como la evaluación del polinomio $P_a(z) = \sum_{n=0}^{N-1} a_n z^n$ en $z = e^{iqd}$. Concluya que calcular la intensidad $I(\theta) = |A(\theta)|^2$ en los N ángulos $q_k = \frac{2\pi k}{Nd}$ equivale a calcular la DFT de a .
- (b) Explique por qué usar la FFT para obtener el patrón de difracción completo es más eficiente que evaluar $A(\theta)$ en cada ángulo por separado.

Ejercicio 14 (La DFT como producto matricial) (a) Escriba la DFT $\hat{x}_k = \sum_{j=0}^{N-1} x_j \omega_N^{jk}$ como un producto matricial $\hat{x} = F x$, donde $F \in \mathbb{C}^{N \times N}$ es la matriz de Fourier con entradas $F_{kj} = \omega_N^{jk}$.

- (b) Observe que F es la matriz de Vandermonde evaluada en los nodos $z_0 = 1, z_1 = \omega_N, z_2 = \omega_N^2, \dots, z_{N-1} = \omega_N^{N-1}$:

$$F = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)^2} \end{pmatrix}.$$

- (c) Interprete: calcular la DFT es evaluar el polinomio $P_x(z) = \sum_{j=0}^{N-1} x_j z^j$ en las N raíces de la unidad. Calcular la DFT inversa es interpolar a partir de esas evaluaciones. ¿Por qué la inversión es posible?

Ejercicio 15 (Unitariedad de la matriz de Fourier) Sea F la matriz de Fourier del ejercicio anterior.

- (a) Demuestre la identidad de ortogonalidad: $\sum_{j=0}^{N-1} \omega_N^{jk} \overline{\omega_N^{j\ell}} = N \delta_{k\ell}$.

Sugerencia: La suma es una serie geométrica.

- (b) Deduzca que $F\overline{F} = NI$, y por lo tanto $F^{-1} = \frac{1}{N}\overline{F}$.

- (c) Escriba explícitamente la fórmula de la DFT inversa:

$$x_j = \frac{1}{N} \sum_{k=0}^{N-1} \hat{x}_k \omega_N^{-jk}.$$

Compare con la fórmula de la DFT directa. ¿En qué se diferencian?

- (d) Concluya que $\frac{1}{\sqrt{N}}F$ es una matriz unitaria.

Ejercicio 16 (Teorema de Parseval discreto) Usando que $\frac{1}{\sqrt{N}}F$ es unitaria, demuestre la identidad de Parseval:

$$\sum_{k=0}^{N-1} |\hat{x}_k|^2 = N \sum_{j=0}^{N-1} |x_j|^2.$$

Interprete: la energía en el dominio del tiempo es proporcional a la energía en frecuencia.

Ejercicio 17 (Convolución Discreta) Una de las propiedades más importantes de la DFT es su relación con la convolución.

(a) Dadas dos secuencias $u, v \in \mathbb{C}^N$, definimos su **convolución circular** $w = u * v$ como:

$$w_k = \sum_{j=0}^{N-1} u_j v_{(k-j) \pmod{N}}, \quad k = 0, \dots, N-1.$$

(b) Demuestre el Teorema de la Convolución: La DFT de la convolución es el producto punto a punto de las DFTs (salvo por un factor de escala dependiente de la normalización):

$$\widehat{(u * v)}_k = \sqrt{N} \hat{u}_k \hat{v}_k.$$

(c) Explique cómo esto permite calcular la convolución de dos vectores muy largos de manera eficiente ($O(N \log N)$) usando la Transformada Rápida de Fourier (FFT), en contraste con el costo $O(N^2)$ de la definición directa.

Ejercicio 18 (Superposición e invariancia traslacional) Considere N fuentes equiespaciadas en un intervalo $[0, L)$ con condiciones de contorno periódicas, ubicadas en $x_j = jh$ con $h = L/N$ ($j = 0, \dots, N-1$). La fuente en x_j tiene amplitud $\rho_j \in \mathbb{C}$. Cada fuente unitaria genera un potencial dado por una función g que depende solo de la distancia: el potencial en x debido a una fuente unitaria en x' es $g(x - x')$.

(a) (**Invariancia traslacional**) Defina $f_m = g(mh)$ para $m = 0, \dots, N-1$. Demuestre que el potencial en x_n debido a una fuente unitaria en x_j es $f_{(n-j) \pmod{N}}$, es decir, depende solo de $n - j$.

(b) (**Linealidad**) Usando que el potencial total es la suma de las contribuciones individuales ponderadas por las amplitudes, demuestre que el potencial total en x_n es $\phi_n = \sum_{j=0}^{N-1} \rho_j f_{(n-j) \pmod{N}}$. Concluya que $\phi = \rho * f$ (convolución circular).

(c) Use el Teorema de la Convolución para concluir que ϕ se puede calcular en $O(N \log N)$ operaciones en vez de $O(N^2)$.

Ejercicio 19 (Multiplicación rápida de polinomios) Sean $P(x) = \sum_{j=0}^{n-1} a_j x^j$ y $Q(x) = \sum_{k=0}^{n-1} b_k x^k$ dos polinomios de grado menor que n . Queremos calcular su producto $R(x) = P(x)Q(x)$.

(a) Muestre que el coeficiente c_k del término x^k en $R(x)$ está dado por la convolución de los coeficientes de P y Q :

$$c_k = \sum_{j=0}^k a_j b_{k-j}.$$

- (b) Observe que el grado de $R(x)$ puede ser hasta $2n-2$. Para usar el Teorema de la Convulsión Cíclica (que opera en vectores de longitud fija N), necesitamos "rellenar con ceros" (zero-padding). Defina vectores extendidos $A, B \in \mathbb{C}^N$ con $N \geq 2n-1$ completando con ceros.
- (c) Describa el algoritmo completo para multiplicar polinomios usando FFT:
- Extender coeficientes a tamaño N .
 - Calcular $\text{FFT}(A)$ y $\text{FFT}(B)$.
 - Multiplicar punto a punto.
 - Calcular IFFT del resultado.
- (d) Compare la complejidad asintótica de este método con la multiplicación clásica "todos con todos" ($O(n^2)$). ¿A partir de qué grado n aproximado cree que vale la pena usar FFT?

Interpolación en cuerpos finitos (*)

Ejercicio 20 (Interpolación en cuerpos finitos: definiciones básicas) La interpolación polinomial también funciona sobre cuerpos finitos \mathbb{Z}_p donde p es primo.

- (a) Verifique que el espacio de polinomios $\mathcal{P}_n(\mathbb{Z}_p) = \{a_0 + a_1x + \dots + a_nx^n : a_i \in \mathbb{Z}_p\}$ es un espacio vectorial sobre \mathbb{Z}_p . ¿Cuál es su dimensión?
- (b) Demuestre que un polinomio no nulo $q \in \mathcal{P}_n(\mathbb{Z}_p)$ tiene a lo sumo n raíces en \mathbb{Z}_p .
Sugerencia: Use inducción en n . Si $q(\beta) = 0$, divida $q(x)$ por el polinomio mónico $(x - \beta)$ usando el algoritmo de división para obtener $q(x) = (x - \beta)\tilde{q}(x)$ con $\tilde{q} \in \mathcal{P}_{n-1}(\mathbb{Z}_p)$.
- (c) Dados $n+1$ puntos distintos $(x_0, y_0), \dots, (x_n, y_n)$ con $x_i, y_i \in \mathbb{Z}_p$, demuestre que existe un único polinomio $p \in \mathcal{P}_n(\mathbb{Z}_p)$ tal que $p(x_i) = y_i$ para todo i .

Ejercicio 21 (Interpolación en \mathbb{Z}_7) Considere los puntos $(1, 3), (2, 5), (4, 2)$ en \mathbb{Z}_7 .

- (a) Halle los coeficientes del polinomio interpolante $p(x) = a_0 + a_1x + a_2x^2$ resolviendo el sistema de Vandermonde $Va = y$ en \mathbb{Z}_7 .
- (b) Evalúe $p(3)$ usando la fórmula de Lagrange (sin calcular los coeficientes).

Ejercicio 22 (Esquema de Shamir) Un esquema de compartición de secretos (k, n) permite dividir un secreto entre n personas de modo que cualquier k de ellas puedan reconstruirlo, pero $k-1$ no pueden obtener información alguna.

El secreto es un número $s \in \mathbb{Z}_p$ (con p primo grande). Se elige un polinomio $f(x) = s + a_1x + \dots + a_{k-1}x^{k-1} \pmod{p}$ de grado $k-1$ con $f(0) = s$. Los coeficientes a_i se eligen al azar en \mathbb{Z}_p siguiendo una distribución uniforme. Luego, se distribuyen las n "porciones" (shares): $(1, f(1)), (2, f(2)), \dots, (n, f(n))$.

- (a) Explique por qué cualquier k porciones permiten reconstruir $f(x)$ mediante interpolación de Lagrange en \mathbb{Z}_p , y por tanto recuperar $s = f(0)$.

- (b) Explique por qué con solo $k-1$ porciones, el secreto s puede ser cualquier valor en \mathbb{Z}_p con igual probabilidad. **Sugerencia:** Muestre que existe un único polinomio de grado $\leq k-1$ compatible con la información parcial y un candidato a secreto $\tilde{s} \in \mathbb{Z}_p$ dado. Concluya el resultado a partir del hecho de que los coeficientes se eligieron uniformemente al azar.

Ejercicio 23 (Códigos de Reed-Solomon) Un código de Reed-Solomon $RS(n, k)$ sobre \mathbb{Z}_p codifica un mensaje $(m_0, \dots, m_{k-1}) \in \mathbb{Z}_p^k$ como las evaluaciones del polinomio $m(x) = m_0 + m_1x + \dots + m_{k-1}x^{k-1}$ en n puntos prefijados $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_p$, produciendo la palabra código $c = (m(\alpha_1), \dots, m(\alpha_n))$.

Suponga que se recibe un vector $r \in \mathbb{Z}_p^n$ que difiere de la verdadera palabra código $c \in \mathbb{Z}_p^n$ en a lo sumo t posiciones (desconocidas). Se definen dos polinomios desconocidos:

- El polinomio localizador de errores $E(x) = e_0 + e_1x + \dots + e_{t-1}x^{t-1} + x^t$ (mónico de grado t), cuyas raíces son exactamente los puntos de evaluación α_j donde ocurrieron errores.
- El polinomio $N(x) = m(x) \cdot E(x) = n_0 + n_1x + \dots + n_{k-1+t}x^{k-1+t}$, de grado $\leq k-1+t$.

- (a) Demuestre que para todo $i = 1, \dots, n$ vale la “ecuación clave” de la corrección de errores:

$$r_i \cdot E(\alpha_i) = N(\alpha_i).$$

Sugerencia: Distinga dos casos. Si no hay error en la posición i , entonces $r_i = m(\alpha_i)$. Si hay error en la posición i , entonces α_i es raíz de E .

- (b) Demuestre que si $n \geq k + 2t$, el mensaje $m(x)$ queda unívocamente determinado por el vector recibido r y la ecuación clave. Concluya que se pueden corregir hasta $t \leq \lfloor (n-k)/2 \rfloor$ errores.

Sugerencia: Suponga que (E, N) y (E', N') son dos soluciones de la ecuación clave y considere $P(x) = N(x)E'(x) - N'(x)E(x)$. Demuestre que $P(\alpha_i) = 0$ para todo i , acote $\deg(P)$, y use el Ejercicio 15(b) para concluir que $P \equiv 0$. ¿Qué implica esto sobre el cociente N/E ?

- (c) Observe que la ecuación clave es lineal en los coeficientes (desconocidos) de E y N . Escriba explícitamente el sistema $A\mathbf{x} = \mathbf{b}$ en \mathbb{Z}_p de tamaño $n \times (k + 2t)$ que permite encontrar los coeficientes de E y N a partir de r y los puntos de evaluación α_i .
- (d) Usando el resultado de (b), deduzca que el sistema lineal tiene solución única. ¿Cuál es la complejidad de resolver el sistema? ¿Depende de p ? ¿Tiene sentido hablar del número de condición en aritmética modular?