

CLASE

3

MÉTODOS NUMÉRICOS

Solución de Ecuaciones No
Lineales II

Educación de calidad

INTRO DUC CIÓN

DE LA CLASE

GRADO / POSGRADO / TECNOLOGÍAS

Estudia a tu tiempo
son interrupciones

EDUCACIÓN EN LÍNEA DE CALIDAD



En esta clase se profundiza en el análisis teórico de la convergencia de los métodos numéricos aplicados a la determinación de raíces de ecuaciones no lineales, estableciendo un marco que permita evaluar el comportamiento de los procesos iterativos, partiendo de la definición de convergencia como la propiedad mediante la cual una sucesión generada por un algoritmo se aproxima progresivamente a la solución exacta, analizando cómo este proceso depende no solo del método utilizado sino también de factores como la naturaleza de la función, las condiciones iniciales y la estructura del problema, lo que permite distinguir entre métodos que garantizan convergencia bajo ciertas condiciones y aquellos que pueden fallar si no se aplican adecuadamente, incorporando además criterios matemáticos basados en continuidad, derivadas y propiedades contractivas que permiten determinar la validez de un método, junto con el estudio del orden de convergencia como medida de la rapidez con la que se alcanza la solución, diferenciando entre convergencia lineal, superlineal y cuadrática.

A partir de ello, se realiza una comparación entre distintos métodos de búsqueda de raíces como bisección, punto fijo, Newton–Raphson y secante, analizando sus ventajas, limitaciones y eficiencia computacional tanto desde una perspectiva teórica como práctica, considerando aspectos como la estabilidad numérica, la sensibilidad a las condiciones iniciales, la necesidad de calcular derivadas y el costo computacional asociado a cada método, lo que permite comprender que no existe un método universalmente mejor sino que su elección depende del problema, de las condiciones en las que se trabaja y del nivel de precisión requerido, permitiendo al estudiante evaluar el desempeño de los métodos iterativos, estimar su velocidad de convergencia y seleccionar de manera fundamentada la técnica más adecuada en cada caso.

Solución de Ecuaciones No Lineales II

En la clase anterior exploramos métodos cerrados (de acotamiento) para encontrar raíces de ecuaciones no lineales $f(x) = 0$. Ahora pasamos a los métodos abiertos (open methods), que no requieren intervalos que acoten la raíz y suelen converger más rápido cuando se inicia cerca de la solución, aunque pueden divergir si la aproximación inicial es mala o la función tiene propiedades desfavorables.

En esta clase nos centramos en tres métodos abiertos clásicos: el de punto fijo, Newton-Raphson y secante. Presentamos primero la formulación matemática formal, teoremas de convergencia y orden, y luego las aplicaciones en ciberseguridad, como en criptoanálisis polinómico (e.g., ataques Coppersmith para RSA) o recuperación de claves parciales.

Métodos abiertos

Los métodos abiertos son una clase de técnicas numéricas que se utilizan para encontrar las raíces de una ecuación. A diferencia de los métodos cerrados, que requieren un intervalo en el que se sabe que existe una raíz, los métodos abiertos parten de una aproximación inicial x_0 (o dos, en el caso del método de la secante) y generan sucesivas aproximaciones x_k para acercarse a la solución. La idea es aplicar una fórmula iterativa, como $x_{k+1} = g(x_k)$, donde $g(x)$ es una función que se deriva de la ecuación original y se utiliza para obtener el siguiente valor de la iteración a partir del anterior.

Una característica clave de los métodos abiertos es que no necesitan que la raíz esté dentro de un intervalo específico, lo que los hace más flexibles que los métodos cerrados. Sin embargo, su principal desventaja es que no siempre garantizan que las iteraciones converjan a la solución. La convergencia depende de la función elegida y de la elección de la aproximación inicial. Además, estos métodos no ofrecen una "acotación" de la solución, es decir, no aseguran que los valores de las iteraciones se mantendrán dentro de un rango cercano a la solución verdadera, lo que puede llevar a resultados erróneos si no se seleccionan correctamente.

La velocidad de convergencia de los métodos abiertos es una propiedad importante y está relacionada con el orden de convergencia. El orden de convergencia se refiere a la rapidez con que las iteraciones se acercan a la solución exacta. Los métodos que tienen un mayor orden de convergencia son más eficientes porque requieren menos iteraciones para alcanzar una



precisión dada. Algunos métodos populares, como el método de Newton-Raphson o el método de la secante, se incluyen en esta categoría, siendo el primero de ellos particularmente conocido por su alta velocidad de convergencia, que es cuadrática, siempre y cuando se elija una buena aproximación inicial.

Método del punto fijo

El método del punto fijo transforma $f(x) = 0$ en $x = g(x)$, donde $g(x)$ es una función continua tal que si α es raíz de f entonces $\alpha = g(\alpha)$ (punto fijo de g).

La iteración es: $x_{k+1} = g(x_k)$, $k = 0, 1, 2,$

Teorema de convergencia

Suponga que g es continua en un intervalo cerrado I que contiene α , y que g es contractiva en I , es decir, existe $L < 1$ tal que $|g'(x)| \leq L$ para todo x en I (o Lipschitz con constante $L < 1$).

Entonces:

- Existe un único punto fijo α en I .
- Para cualquier x_0 en I , la secuencia $\{x_k\}$ converge a α .
- La convergencia es lineal: $|x_{k+1} - \alpha| \leq L |x_k - \alpha|$.

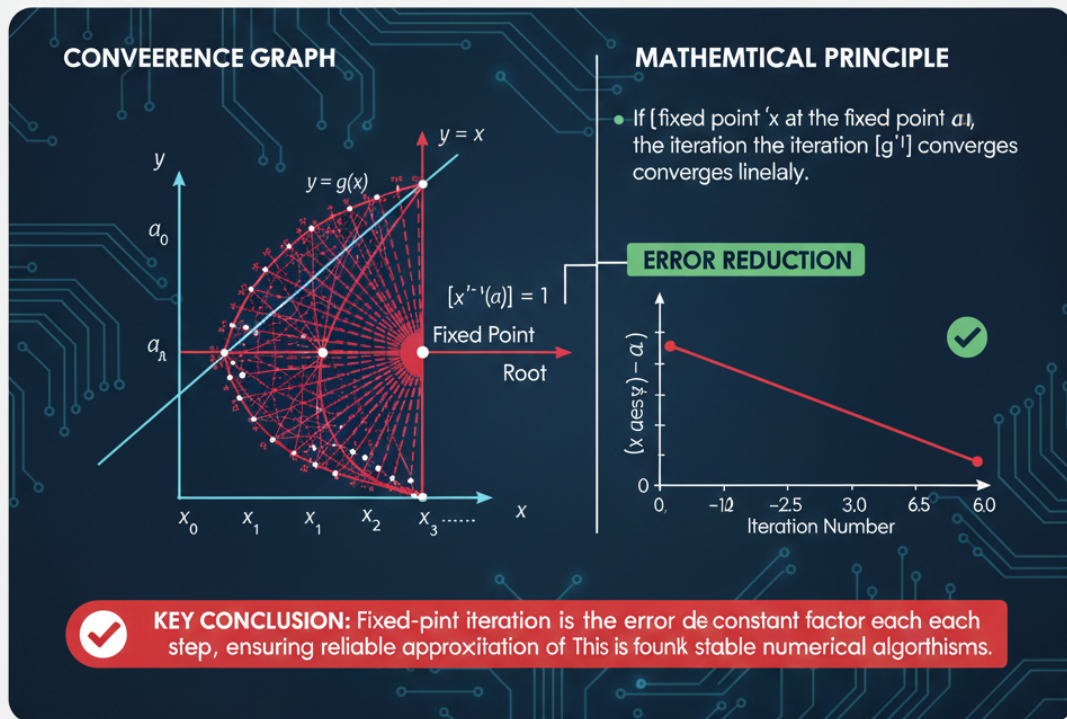
Si $g \in C^1$ cerca de α y $|g'(\alpha)| < 1$, entonces existe un vecindario donde la iteración converge linealmente con tasa $|g'(\alpha)|$. Si $|g'(\alpha)| > 1$ diverge; si $=1$, convergencia más lenta o no garantizada.

Orden de convergencia Lineal (orden 1) si $g'(\alpha) \neq 0$; superlineal o más alto si $g'(\alpha) = 0$ y derivadas superiores controladas.



LINEAR CONVERGENCE: Fixed-Point Iteration

Visualizing guaranteed Convergence when $|g'(a)| < 1$



THE THEORY OF ITERATIVE METHODS

Figura 1: Diagrama de convergencia lineal en iteración de punto fijo con $|g'(\alpha)| < 1$.

Creación propia.

Método de Newton-Raphson

Definimos el Método de Newton-Raphson: derivado de la aproximación lineal (tangente) de f cerca de x_k :

$$f(x_k + h) \approx f(x_k) + f'(x_k)h = 0 \Rightarrow h \approx -f(x_k)/f'(x_k) \Rightarrow x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}$$

Teorema de convergencia

Suponga $f \in C^2$ en un vecindario de α (raíz simple, $f(\alpha)=0$, $f'(\alpha) \neq 0$). Entonces existe $\delta > 0$ tal que si $|x_0 - \alpha| < \delta$, la secuencia converge a α .

Orden de convergencia Cuadrático (orden 2): si $f'(\alpha) \neq 0$ y $f \in C^2$, entonces:

$$\lim_{k \rightarrow \infty} \frac{|x_{k+1} - \alpha|}{|x_k - \alpha|^2} = \left| \frac{f''(\alpha)}{2f'(\alpha)} \right|$$

Derivación vía expansión de Taylor:

$$x_{k+1} - \alpha = x_k - \alpha - \frac{f(x_k)}{f'(x_k)} = (x_k - \alpha) - \frac{f'(\alpha)(x_k - \alpha) + \frac{1}{2}f''(\alpha)(x_k - \alpha)^2 + O((x_k - \alpha)^3)}{f'(\alpha)} \approx (x_k - \alpha) - \frac{f'(\alpha)}{2f'(\alpha)}(x_k - \alpha)^2 + O((x_k - \alpha)^3) \Rightarrow \text{error}_{k+1} \approx C(\text{error}_k)^2, \text{ con } C = -f''(\alpha)/(2f'(\alpha))$$

Fundamental en ataques Coppersmith: encontrar raíces pequeñas de polinomios modulares (e.g., RSA con MSB/LSB conocidos o mensajes pequeños). Newton refina aproximaciones iniciales de raíces modulares. También en optimización de ataques side-channel (ajuste de parámetros) o entrenamiento de ML para detección (gradiente descendente es Newton-like).

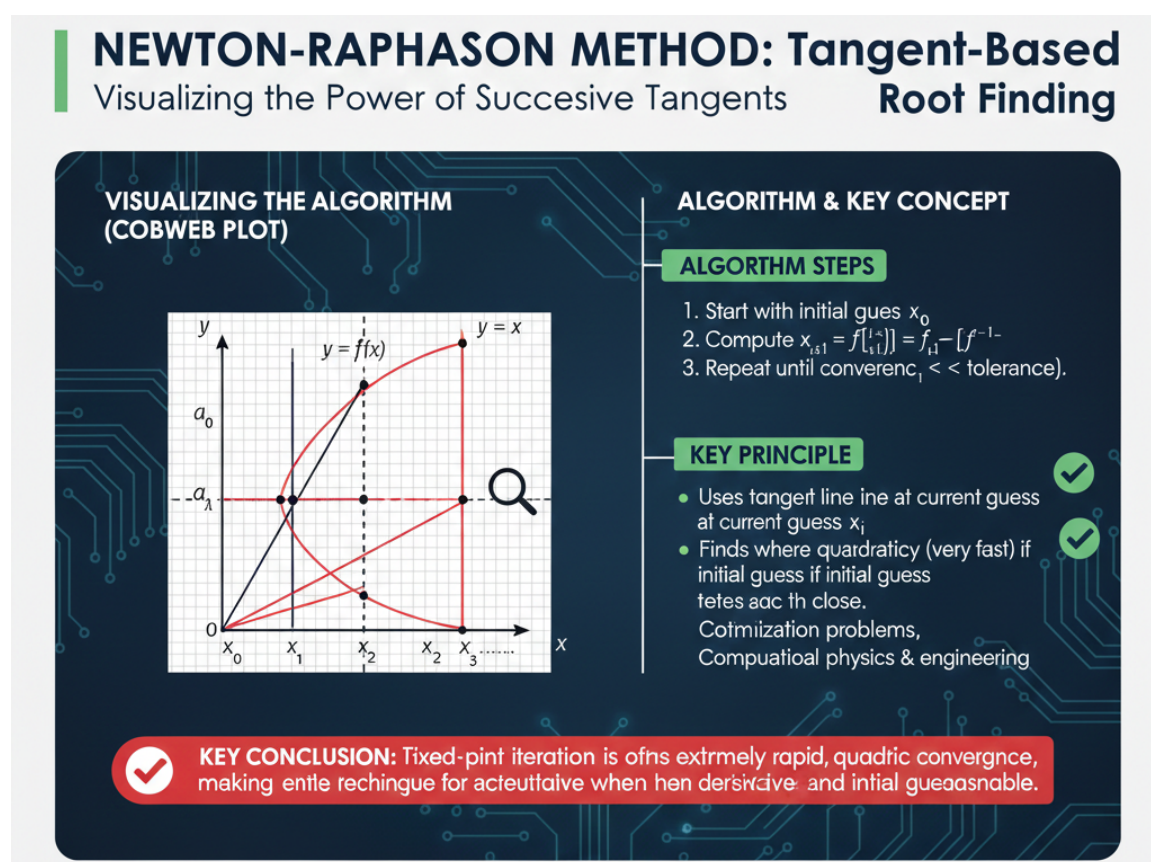


Figura 2: Pasos gráficos del método de Newton-Raphson: tangentes sucesivas aproximando la raíz.

Creación propia.

Enlace 1: https://en.wikipedia.org/wiki/Newton%27s_method Ver en Wikipedia: Newton's method Este artículo detalla la derivación matemática, prueba de convergencia cuadrática y condiciones.

Método de la secante

Aproximación de la derivada por diferencia finita:

$$f'(x_k) \approx \frac{f(x_k) - f(x_{k-1})}{x_k - x_{k-1}} \Rightarrow x_{k+1} = x_k - f(x_k) \frac{x_k - x_{k-1}}{f(x_k) - f(x_{k-1})}$$

Requiere dos iniciales x_0, x_1 .

Teorema de convergencia

Suponga $f \in C^2$ cerca de α (raíz simple, $f'(\alpha) \neq 0$). Si x_0, x_1 suficientemente cercanos a α , converge a α .

Orden de convergencia Superlineal con orden $\phi = (1 + \sqrt{5})/2 \approx 1.618$ (razón áurea):

$$\lim_{k \rightarrow \infty} \frac{|x_{k+1} - \alpha|}{|x_k - \alpha|^\phi} = \left| \frac{f''(\alpha)}{2f'(\alpha)} \right|^{1/\phi}$$

Derivación vía error: $\text{error}_{k+1} \approx \text{Cerror}_k \text{error}_{k-1}$, llevando a la ecuación característica $r^2 - r - 1 = 0$, raíces ϕ y $1-\phi$ (tomamos la positiva).

SECANT METHOD: Approximating with a Secant Line

Visualizing Rapid Error Tangent with a Secant Line

VISUALIZING THE ALGORITHM

Iteration 2 and Iteration 3 are shown below the main graph, illustrating the iterative process of finding the root.

ALGORITHM & KEY CONCEPT

ALGORITHM STEPS

1. Start with initial guess x_0
2. Compute $x_{i+1} = f^{-1}(f(x_i)) = f^{-1} \circ f(x_i)$
3. Repeat until convergence, $< \epsilon$ (tolerance).

KEY PRINCIPLE

- Uses a secant line to approximate to current Bisection. Avoids the slow convergence of Bisection (no need a $f'(x)$).
- Faster than Bisection, slower than Newton's method. Few iterations achieve a good approximation. It's very fast.

KEY CONCLUSION

The secant method is of an extremely rapid convergence, using only the function values and not the derivative to find roots.

Figura 3: Ilustración del método de la secante: cuerda (secante) entre dos puntos aproximando la tangente.

Creación propia.

El método de la secante es un método iterativo utilizado para encontrar las raíces de una función no lineal, y es una alternativa al método de Newton-Raphson. En este método, en lugar de utilizar la derivada de la función para aproximar la tangente en cada iteración, se utiliza una cuerda (o secante) que conecta dos puntos cercanos en el gráfico de la función para aproximar la tangente en el punto de interés.

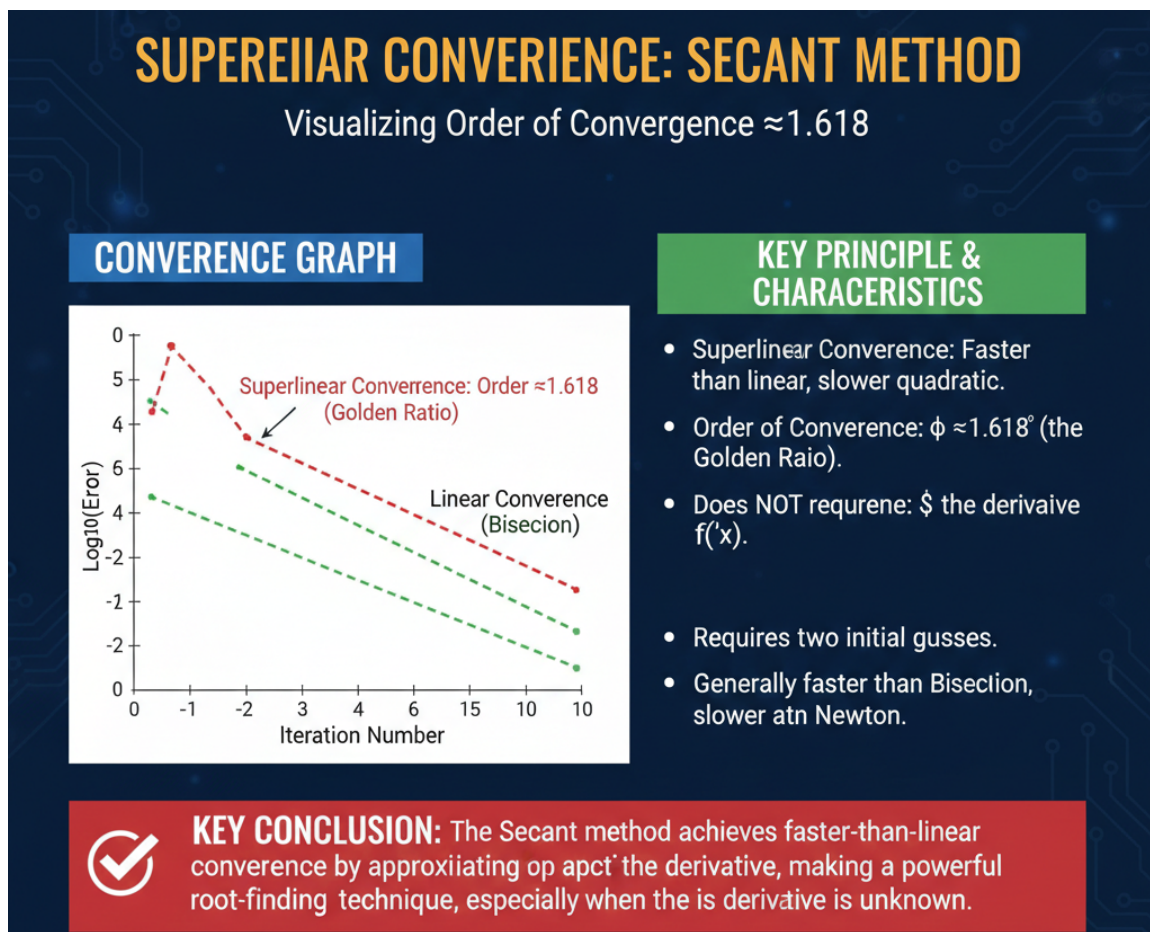


Figura 4: Convergencia superlineal del método de secante mostrando orden ≈ 1.618 .

Creación propia.

Consideremos que estamos resolviendo la ecuación $f(x) = 0$ utilizando el método de la secante, con una función $f(x)$ y dos valores iniciales x_0 y x_1 . Supongamos que la raíz real es α , y en las iteraciones sucesivas calculamos los valores aproximados $x_0, x_1, x_2, \dots$

- En la primera iteración, el error es $|x_1 - \alpha|$.
- En la segunda iteración, el error es $|x_2 - \alpha|$.
- En la tercera iteración, el error es $|x_3 - \alpha|$.

La tasa de reducción del error en cada iteración debería ser proporcional a un factor cercano a $1/\varphi$, lo que significa que el error se reduce aproximadamente por un factor de 1.618 en cada paso.

Si calculamos el ratio de los errores en dos iteraciones consecutivas $|x_n - \alpha|$ y $|x_{n+1} - \alpha|$, el valor de este ratio debe converger a φ . Es decir:

$$\frac{\log |x_{n+1} - \alpha|}{\log |x_n - \alpha|} \approx \frac{1}{\varphi} \approx 0.618$$

Este valor indica que la reducción del error en cada iteración sigue una tasa de convergencia superlineal, con un orden de convergencia de aproximadamente 1.618.

Análisis de Convergencia de Métodos para Raíces

En las clases anteriores hemos estudiado métodos cerrados (bisección, falsa posición) y abiertos (punto fijo, Newton-Raphson, secante) para resolver $f(x) = 0$. Ahora analizamos su comportamiento cuantitativo: si convergen, con qué velocidad y cómo compararlos. Este análisis es esencial para seleccionar el método adecuado en aplicaciones de ciberseguridad, donde la eficiencia computacional y la robustez frente a errores numéricos pueden marcar la diferencia entre un ataque exitoso y uno fallido.

Presentamos primero los conceptos matemáticos formales, teoremas y definiciones, y después las implicaciones en ciberseguridad.

Concepto de convergencia

Una secuencia x_n converge a α (raíz de $f(x) = 0$) si $\lim_{n \rightarrow \infty} |x_n - \alpha| = 0$.

En métodos iterativos $x_{n+1} = g(x_n)$ (punto fijo) o variantes, la convergencia depende de la aproximación inicial x_0 , propiedades de g y la naturaleza de la raíz (simple o múltiple).

Convergencia local: existe $\delta > 0$ tal que si $|x_0 - \alpha| < \delta$, entonces $\{x_n\} \rightarrow \alpha$.

Convergencia global: converge para cualquier x_0 en un dominio amplio (raro en métodos abiertos).

En ciberseguridad: convergencia local es común (e.g., Newton en Coppersmith requiere buena inicial cerca de la raíz pequeña); convergencia global es deseable en búsquedas exhaustivas o ataques side-channel.

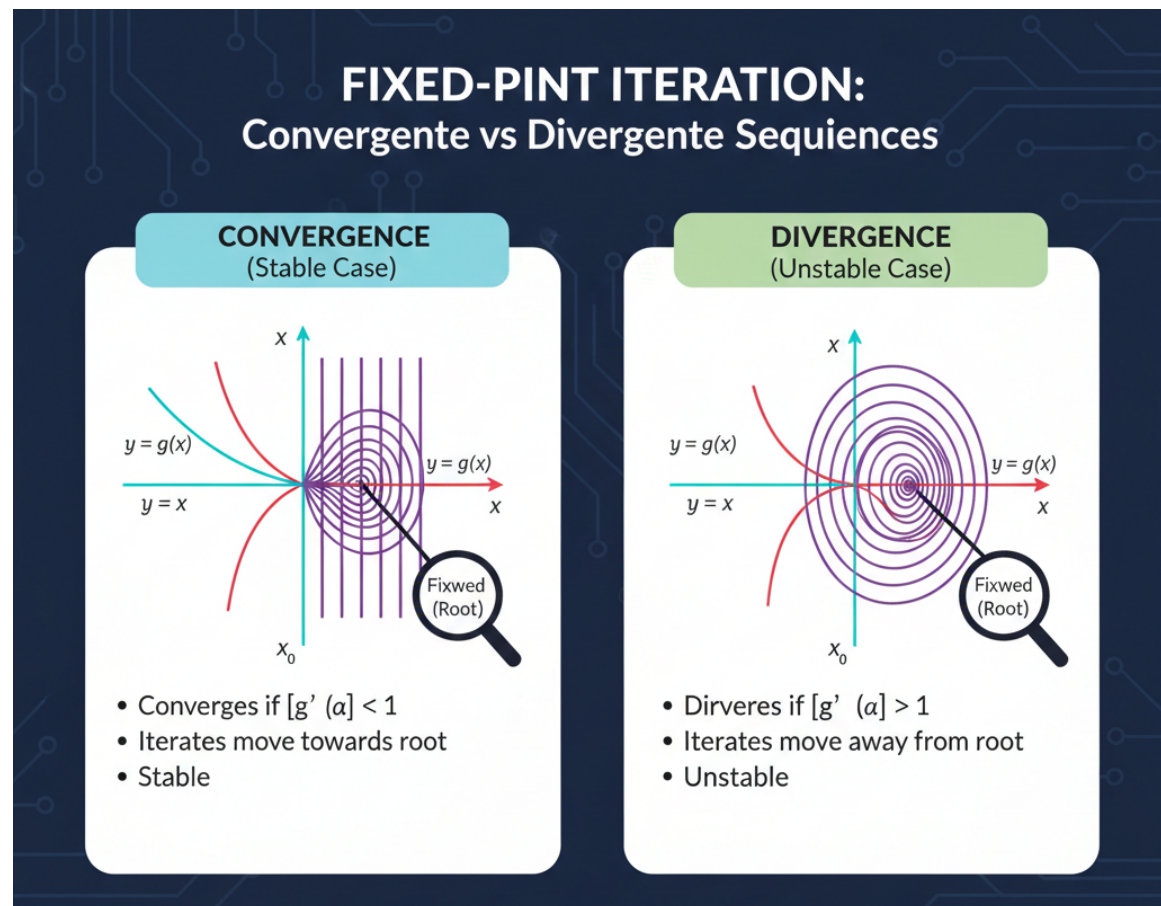


Figura 5: Secuencia convergente vs divergente en iteración de punto fijo.

Creación propia.

a) Características de la convergencia:

- La función $g(x)$ debe cumplir con ciertas condiciones para garantizar la convergencia, como que $|g'(x)| < 1$ en la vecindad de la raíz α . Esto significa que la pendiente de la función en ese punto es menor que 1, lo que asegura que el valor iterado se acerque más a la raíz en cada paso.

- A medida que se realizan más iteraciones, los puntos x_n se aproximan progresivamente al valor de la raíz α .

b) Características de la divergencia:

- La divergencia generalmente ocurre cuando la función $g(x)$ no satisface los criterios de convergencia, como cuando $|g'(x)| \geq 1$ cerca de la raíz. Si la pendiente de la función es mayor o igual a 1, los valores iterados pueden alejarse de la raíz en lugar de acercarse a ella.

Enlace 2: https://en.wikipedia.org/wiki/Root-finding_algorithm Ver en Wikipedia: Root-finding algorithm Este artículo resume orden de convergencia y comparación entre bisección, Newton y secante.

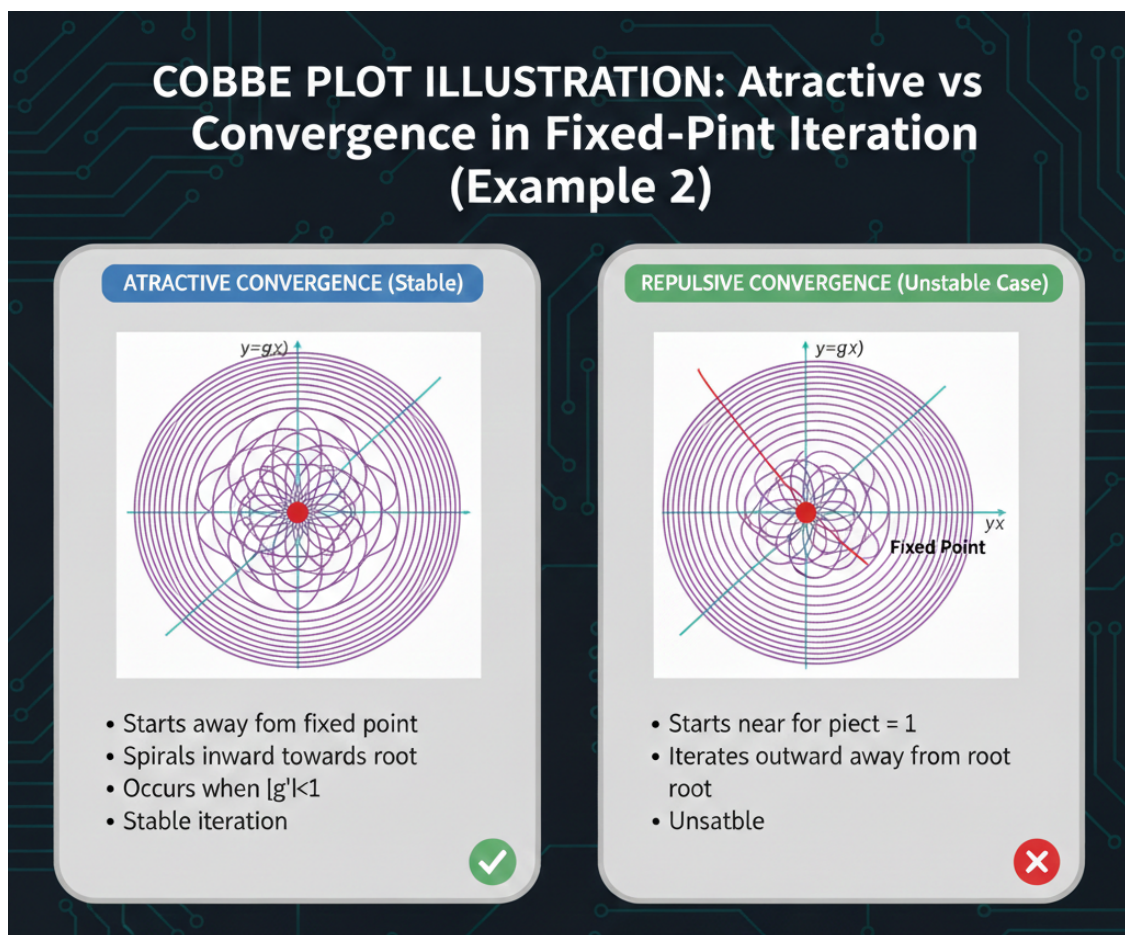


Figura 6: Cobweb plot ilustrando convergencia atractiva y repulsiva en punto fijo. Creación propia.

Criterios de convergencia

Criterio práctico de parada (en implementación):

- $|x_{n+1} - x_n| < \varepsilon$ (cambio absoluto pequeño).
- $|f(x_{n+1})| < \varepsilon$ (residuo pequeño).
- $|x_{n+1} - x_n|/|x_{n+1}| < \varepsilon$ (error relativo).
- Número máximo de iteraciones alcanzado (para evitar bucles infinitos).

Teorema de convergencia para punto fijo

Sea $g \in C^1$ en intervalo I que contiene $\alpha = g(\alpha)$. Si $|g'(\alpha)| < 1$, entonces existe vecindario donde la iteración converge linealmente con tasa $|g'(\alpha)|$. Si $|g'(\alpha)| > 1$, diverge; si $=1$, convergencia sublineal o no garantizada.

Para Newton-Raphson: si $f \in C^2$, $f(\alpha)=0$, $f'(\alpha) \neq 0$ (raíz simple), converge localmente cuadráticamente.

Para secante: si $f \in C^2$, $f'(\alpha) \neq 0$, converge localmente con orden $(1 + \sqrt{5})/2 \approx 1.618$.

Para bisección: converge siempre si f continua y $f(a)f(b) < 0$; tasa lineal con constante $1/2$ (error $\leq (b-a)/2^n$).

Para falsa posición: converge si f continua y cambio de signo, pero tasa variable (lineal en peor caso, superlineal si función convexa).

En ciberseguridad: criterios estrictos evitan falsos positivos en detección (e.g., residuo $< 10^{-12}$ en correlación CPA); convergencia garantizada (bisección) es clave en búsquedas seguras de claves parciales.

CONVERGENCE & STOPPING CRITERIA

Error vs Iterations for Different Stopping Conditions

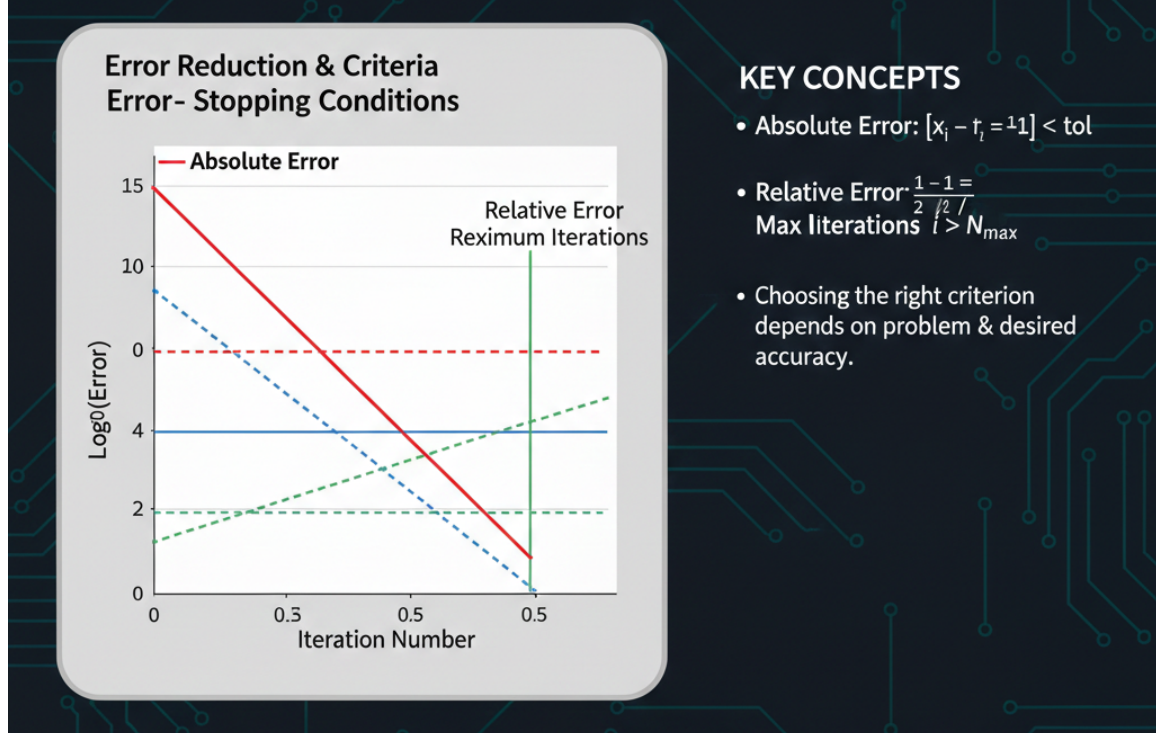


Figura 7: Gráfico de error vs iteraciones para diferentes criterios de parada.

Orden de convergencia

Definición formal: Una secuencia x_n converge a α con orden $p \geq 1$ si existe constante $\lambda > 0$ tal

$$\text{que } \lim_{n \rightarrow \infty} \frac{|x_{n+1} - \alpha|}{|x_n - \alpha|^p} = \lambda.$$

- $p = 1$: convergencia lineal (tasa constante < 1).
- $p = 2$: cuadrática (error se cuadra cada iteración).
- $p \approx 1.618$: superlineal (secante, razón áurea).

Teorema para Newton-Raphson (raíz simple): Si $f \in C^2$ cerca de α , $f'(\alpha) \neq 0$, entonces orden

$$p = 2 \text{ y } \lim_{n \rightarrow \infty} \frac{|x_{n+1} - \alpha|}{|x_n - \alpha|^2} = \left| \frac{f''(\alpha)}{2f'(\alpha)} \right|.$$

Para secante: Orden $p = (1 + \sqrt{5})/2 \approx 1.618$ (raíz positiva de $r^2 - r - 1 = 0$), constante asintótica involucra f''/f' .

Para punto fijo: $p = 1$ si $|g'(\alpha)| < 1 \neq 0$; $p > 1$ si $g'(\alpha) = 0$ y derivadas superiores nulas hasta cierto orden.

Para bisección: $p = 1$, tasa $1/2$ (error se reduce a la mitad cada iteración).

Para falsa posición: $p = 1$ en peor caso (estancamiento en un lado), pero puede ser superlineal en casos favorables.

En ciberseguridad: métodos de orden alto (Newton $p=2$) son preferidos en criptoanálisis (Coppersmith, lattices) por su rapidez; bisección ($p=1$ garantizado) en búsquedas seguras donde no se tolera divergencia.

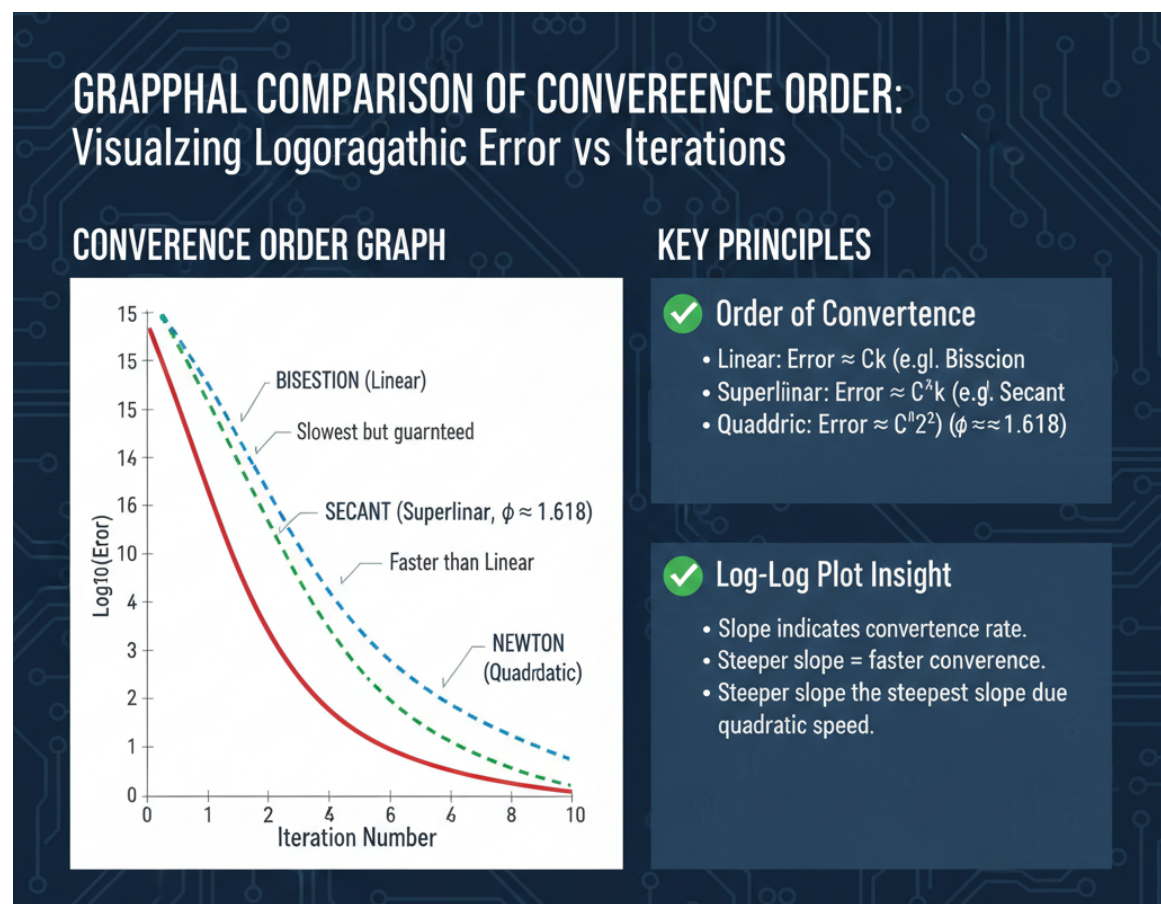


Figura 8: Comparación gráfica de orden de convergencia: error logarítmico vs iteraciones (bisección lineal, Newton cuadrática, secante superlineal).

Creación propia.

El orden de convergencia de un método numérico describe cómo el error en la solución disminuye con cada iteración. Formalmente, si x_n es la aproximación de la raíz en la n -ésima iteración y α es la raíz exacta, el error e_n es:

$$e_n = |x_n - \alpha|$$

El orden de convergencia p se define mediante la siguiente relación:

$$\lim_{n \rightarrow \infty} \frac{\log |e_{n+1}|}{\log |e_n|^p} = C$$

Donde:

- $e_n = |x_n - \alpha|$ es el error en la n -ésima iteración,
- p es el orden de convergencia,
- C es una constante.

En términos sencillos:

- Convergencia lineal significa que el error disminuye de manera proporcional a un factor constante en cada iteración.
- Convergencia cuadrática significa que el error disminuye exponencialmente, con el error reduciéndose de manera cuadrática en cada iteración.
- Convergencia superlineal es más rápida que la lineal, pero más lenta que la cuadrática.

Comportamiento de los Métodos Comparados:

Método de Bisección (Convergencia Lineal):

El método de bisección es un método muy confiable que siempre converge hacia la raíz de una función, pero su convergencia es lineal, lo que significa que el error disminuye de manera proporcional en cada iteración.

- **Comportamiento en el gráfico:**
 - El error absoluto en la bisección disminuye de forma constante en cada iteración.
 - El gráfico mostrará una pendiente suave y lenta, con una reducción gradual del error en cada paso.

- La curva de la bisección será una línea recta inclinada, que refleja la reducción constante del intervalo en cada paso, lo que reduce el error en una cantidad proporcional con cada iteración.

Método de Newton-Raphson (Convergencia Cuadrática):

El método de Newton-Raphson tiene una convergencia cuadrática, lo que significa que el error disminuye de forma exponencial en cada iteración. Esto se traduce en que, si la aproximación inicial está cerca de la raíz, la solución se encuentra muy rápidamente.

- **Comportamiento en el gráfico:**

- La curva de error absoluto será muy pronunciada en las primeras iteraciones, ya que el error disminuye muy rápidamente en cada paso.
- Al principio, la reducción del error es muy grande, pero conforme el valor de la raíz se aproxima más y más, la disminución del error se vuelve más lenta.
- El gráfico tendrá una pendiente empinada al inicio, que luego se va aplanando conforme las iteraciones avanzan y el error se reduce a niveles más pequeños.
- La convergencia cuadrática es lo que hace que el método de Newton-Raphson sea extremadamente eficiente cuando la aproximación inicial está cerca de la raíz.

Método de Secante (Convergencia Superlineal):

El método de secante tiene una convergencia superlineal, lo que significa que su tasa de convergencia es más rápida que la convergencia lineal de la bisección, pero no tan rápida como la convergencia cuadrática de Newton-Raphson.

- **Comportamiento en el gráfico:**

- La curva de error absoluto para el método de secante será más empinada que la de la bisección, pero no tan empinada como la de Newton-Raphson.
- El error se reduce más rápidamente que en la bisección, pero no alcanza la misma rapidez de convergencia que el método de Newton-Raphson.

- La curva mostrará una reducción acelerada del error en las primeras iteraciones, pero la tasa de disminución del error se estabiliza de manera más gradual en comparación con Newton-Raphson.

Comparación entre métodos

Método	Tipo	Garantía de convergencia	Orden p	Tasa asintótica	Ventajas	Desventajas	Aplicación típica en ciberseguridad
Bisección	Cerrado	Siempre (si cambio signo)	1 (lineal)	1/2	Robusto, global en intervalo	Lento, no aprovecha pendiente	Búsqueda exhaustiva en claves parciales
Falsa posición	Cerrado	Sí (cambio signo)	1 (variable)	Variable, puede estancarse	Más rápido que bisección en convexas	Estancamiento en funciones planas	Refinamiento en modelos de leakage
Punto fijo	Abierto	Local si	$g'(\alpha)$	< 1	1 (lineal)		$g'(\alpha)$
Newton-Raphson	Abierto	Local (cerca de raíz simple)	2 (cuadrática)		$f''(\alpha)/(2f'(\alpha))$		Muy rápido, cuadrático
Secante	Abierto	Local	≈ 1.618 (superlineal)	Constante con f''/f'	No requiere derivada, rápido	Dos iniciales, puede divergir	Ataques sin derivadas explícitas

En general: métodos cerrados → robustez; abiertos → velocidad (cuando convergen). Elección: usar cerrado para inicializar, abierto para refinar.

En ciberseguridad: Newton/secante en ataques eficientes (criptoanálisis polinómico, lattices); bisección en validaciones seguras donde divergencia no es aceptable.

Referencias

RE FE REN CIAS

- **Burden, R. L., Faires, J. D., & Burden, A. M. (2015).** Numerical analysis (10ª ed.). Cengage Learning.
- **Higham, N. J. (2002).** Accuracy and stability of numerical algorithms (2ª ed.). SIAM.
- **Paar, C., & Pelzl, J. (2010).** Understanding cryptography: A textbook for students and practitioners. Springer.
- **Boneh, D., & Shoup, V. (2020).** A graduate course in applied cryptography. <https://toc.cryptobook.us>
- **Atkinson, K. E. (1989).** An introduction to numerical analysis. Wiley.



síguenos en:



www.pucevirtual.puce.edu.ec