DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA,
ELETTRONICA E SISTEMISTICA

Corso di Laurea Triennale in Ingegneria Informatica

Tesi di Laurea

Crittografia quantistica e cyber security

Relatore:

Prof.
Floriano De Rango

Candidato:

Giovanni Lorenzo
Murfuni
Mat. 230599

ANNO ACCADEMICO 23/24

Dedica e Ringraziamenti...

Indice

Indice **2**

1 Introduzione **3**

1.1 Come funziona l'esame? 3

1.2 Concetti Iniziali 3

1.2.1 Problemi della matematica del continuo 3

1.2.2 Radici 5

Schema Iterativo (5 punti essenziali): 5

2 Analisi degli errori numerici **6**

Capitolo 1

Introduzione

1.1 Come funziona l'esame?

Il professore prende le presenze e assegnerà dei progettini, solo con presenze e progrttini, si arriva al 18. L'esame consiste in un esercizio, una domanda teorica e poi un orale.

1.2 Concetti Iniziali

Definizione 1. *La matematica del continuo si basa sul concetto di numero reale ed è ampiamente usata nelle scienze applicate.*

Definizione 2. *Il calcolo numerico è una branca della matematica che si occupa dello sviluppo di algoritmi per la risoluzione dei problemi alla matematica del continuo.*

Di base, il calcolo numerico si occupa i problemi di risoluzione prettamente numerici e dei problemi di approssimazione.

1.2.1 Problemi della matematica del continuo

I problemi classici nella matematica del continuo sono come: **La risoluzione di funzioni** come $f(x) = 0$, dove $x \in [a, b] \subset \mathbb{R}$.

Nozione 1. *Un'equazione si dice risolubile elementarmente se esiste una formula risolutiva, o un procedimento, che permette di esprimere la soluzione partendo dai dati per mezzo di funzioni elementari*[1]

Tra le funzioni elementari, somma e sottrazione sono le più problematiche, perché comportano moltissimi errori di approssimazione.
Il primo problema consiste nello studiare l'esistenza della soluzione, secondariamente, tale soluzione deve essere unica. Importantissimo è anche studiare il tipo di errore, dal punto di vista numerico, in modo da riuscire a capire quando un'approssimazione è applicabile o meno.

carrellata di definizioni su integrale e altre funzioni, quando è continua? quando esiste? come la approssimiamo? come la risolviamo?

Definizione 3. *Gli algoritmi di calcolo numerico forniscono, in generale, solo un'approssimazione della soluzione del problema della matematica del continuo che si vuole risolvere.*

Tale approssimazione può essere buona quanto si vuole. IL prezzo che si paga per un'approssimazione migliore è il tempo di esexuzione dell'algoritmo. Tuttavia il "check" sull'approssimazione non è sempre fattibile poiché nella realtà non conosciamo la soluzione esatta di quello che stiamo appprossimando.

Ogni volta che sviluppiamo un algoritmo di calcolo, bisogna verificare la convergenza, secondariamente dobbiamo troncare n in base allo studio di convergenza, nell'esempio di problema $\sqrt{a}$ il metodo di Newtono ha bisogno di $n = 3$.

subsubsection-Esempio di problema

[1] Le funzioni matematiche elementari sono:

- somma, differenza, prodotto e divisione.
- estrazioni di radici: $\sqrt[n]{n}$
- le funzioni trigonometriche
- esponenziali e logaritmici

In questa branca della matematica si procede sostituendo le tecniche di risoluzione del continuo con tecniche numeriche. Come ad esempio la soluzione di Riemann per l'integrale[2] I computer commettono errori, poiché anch'essi eseguono approssimazioni, come l'errore round-off (di arrotondamento: arrotondamento o troncamento nel senso che quando si usa un computer si possono commettere questi errori che non sono sinonimo di quelli che seguono, anche se si usano gli stessi termini).

Approfondire sugli errori

1.2.2 Radici

Dati in ingresso: $a \in \mathbb{R}, a > 0$

Schema Iterativo (5 punti essenziali):

1. Schema ricorsivo:

$$x_{n+1} = \frac{1}{2}(x_n + \frac{a}{x_n}). \qquad n = 0, 1, 2, ...$$

2. Soluzione iniziale (punto di partenza): $x_0 > 0$

3. Convergenza $\lim_{a\to\infty}(x_n = \sqrt{a})$

4. Velocità di convergenza, quanto più x_0 è prossimo alla radice tanto migliore è la convergenza dell'algoritmo

5. Criterio di arresto: *Quando mi fermo per avere una buona approssimazione?* $x_n - x_{n-1} < \epsilon$.

[2] COnsiste nell'andare a scomporre la figura sottostante all'integrale in piccole sezioni da andare a sommare e ad approssimare.

Capitolo 2

Analisi degli errori numerici