

APPROFONDIMENTO n.01

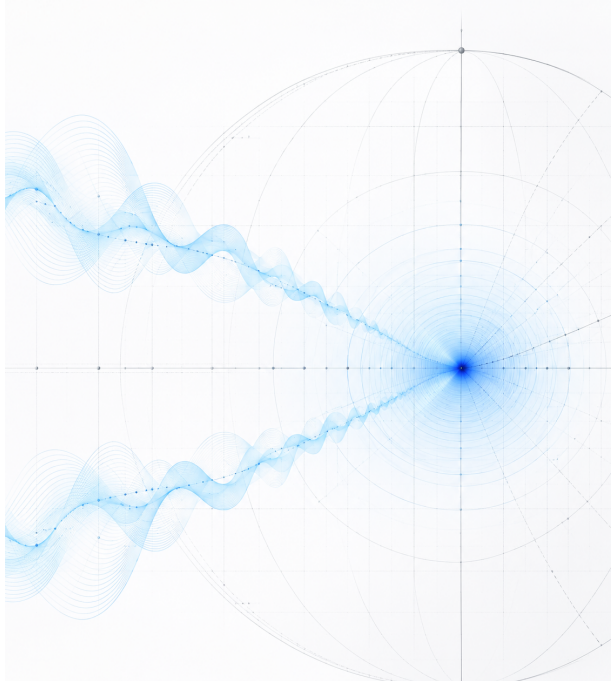
Metodi della Fisica Quantistica per l'Ingegneria

Funzioni classiche e reversibilità

Come inserire una funzione
irreversibile in un circuito
quantistico?

Prof. Vincenzo Berardi · Politecnico di Bari Ultimo

aggiornamento: 24 Settembre 2026



Definizione del problema

Consideriamo una generica FUNZIONE

$$f : \{0, 1\}^n \longrightarrow \{0, 1\}^m$$

Una funzione classica può perdere informazione e quindi non essere reversibile. Un circuito quantistico unitario, invece, deve essere invertibile. L'obiettivo è costruire una trasformazione reversibile che contenga il calcolo di f senza cancellare l'ingresso.

Una funzione classica trasforma n bit in m bit

FUNZIONE

$$f : \{0, 1\}^n \longrightarrow \{0, 1\}^m$$

Un ingresso x di n bit viene trasformato in un'uscita $f(x)$ di m bit.

SCHEMA CLASSICO

$$x \longmapsto f(x)$$

Se usiamo soltanto l'uscita, l'informazione contenuta in x può andare perduta.

In generale, conoscere $f(x)$ non basta per ricostruire univocamente x .

AND perde informazione

ESEMPIO

$$f(a, b) = a \wedge b$$

a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

PERDITA DI INFORMAZIONE

Tre ingressi diversi producono la stessa uscita:

$$(0, 0), (0, 1), (1, 0) \mapsto 0.$$

Conoscendo soltanto lo zero in uscita non possiamo sapere quale coppia fosse entrata.

AND non è reversibile perché la mappa ingresso–uscita non è uno-a-uno.

L'idea è conservare x e aggiungere un registro ausiliario

INGRESSO ESTESO

$$(x, y), \quad y \in \{0, 1\}^m$$

Il registro y ha la stessa lunghezza dell'uscita $f(x)$. Il registro x non

viene cancellato.

TRASFORMAZIONE

$$U_f : (x, y) \mapsto (x, y \oplus f(x))$$

Lo XOR è eseguito bit a bit sul secondo registro.

La funzione f non viene sostituita: viene incorporata in una trasformazione più grande.

Perché U_f è reversibile

PRIMA APPLICAZIONE

$$(x, y) \xrightarrow{U_f} (x, y \oplus f(x))$$

SECONDA APPLICAZIONE

$$(x, y \oplus f(x)) \xrightarrow{U_f} (x, y \oplus f(x) \oplus f(x))$$

$$f(x) \oplus f(x) = 0 \quad \implies \quad y \oplus 0 = y$$

$U_f^2 = I$ e quindi $U_f^{-1} = U_f$: la trasformazione è reversibile.

Due ingredienti rendono reversibile U_f

1 · CONSERVARE x

Conoscendo x possiamo ricalcolare $f(x)$ durante l'operazione inversa.

2 · USARE XOR

Lo stesso $f(x)$ applicato una seconda volta annulla la modifica di y .

$$y \oplus f(x) \oplus f(x) = y$$

Non è lo XOR da solo a rendere reversibile il calcolo: è essenziale anche conservare x .

$f(x) = x$: l'esempio della CNOT

FUNZIONE

$$f(x) = x$$

$$(x, y) \mapsto (x, y \oplus x)$$

x è il controllo; y viene invertito soltanto quando $x = 1$.

TABELLA COMPLETA

x	y	x'	y'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Le quattro configurazioni di uscita sono tutte diverse.

Con $y = 0$ otteniamo $(x, f(x))$

$$(x, 0) \xrightarrow{U_f} (x, 0 \oplus f(x)) = (x, f(x))$$

CALCOLO CLASSICO

$$x \longmapsto f(x)$$

L'ingresso può essere sovrascritto e quindi l'operazione può essere irreversibile.

EMBEDDING REVERSIBILE

$$(x, 0) \longmapsto (x, f(x))$$

Il risultato compare nel registro ausiliario, mentre l'ingresso rimane disponibile.

Non rendiamo reversibile f

Costruiamo una trasformazione reversibile che contiene f .

FUNZIONE ORIGINALE

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^m$$

Può essere multi-a-uno e quindi irreversibile.

ORACLE REVERSIBILE

$$U_f : (x, y) \mapsto (x, y \oplus f(x))$$

Collega una uscita ad una sola combinazione in ingresso: funzione biiettiva