Sviluppo di Algoritmi Quantistici: Dal Modello Circuitale a Qiskit.

Gabriele Rossini,
Mat. 712391
11/02/2026

Dipartimento dell’ingegneria dell’informazione
Corso di Laurea in Ingegneria Informatica

Sviluppo di Algoritmi Quantistici: Dal Modello Circuitale a Qiskit.

Relatore
Chiar.mo Prof. Luca Giuzzi

Laureando
Gabriele Rossini
Matricola n. 712391

UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Dal Qubit: Formalismo e Modello Circuitale

- Lo Stato (Memoria):
  - Classico: Valore discreto $b \in \{0,1\}$.
  - Quantistico: Vettore unitario in uno spazio di Hilbert complesso.
  - Definizione: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ con vincolo $|\alpha|^2+|\beta|^2=1$ (Normalizzazione).
  - Nota: α, β sono ampiezze di probabilità, non probabilità dirette.

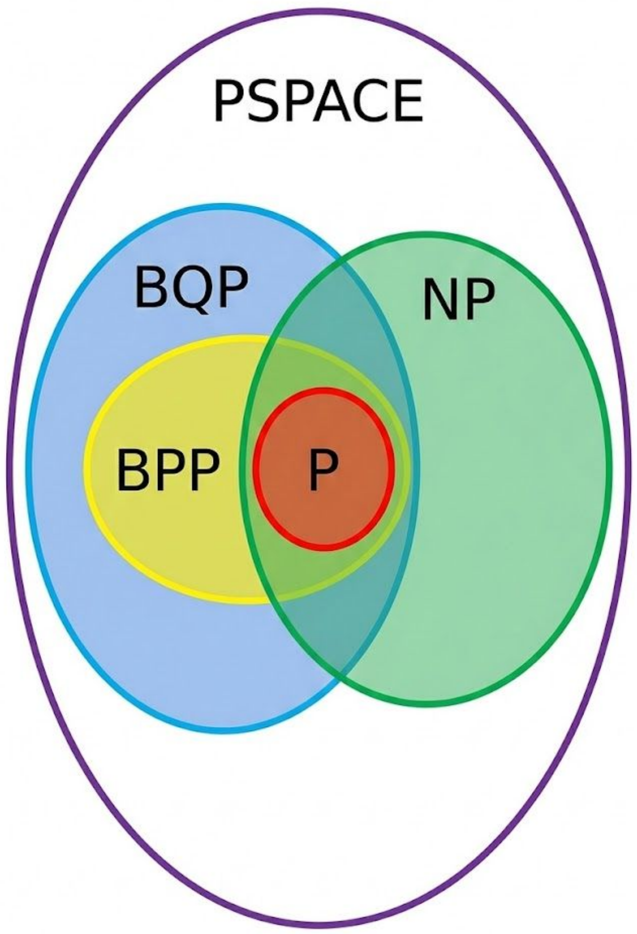
- L'Elaborazione (Logic Gates):
  - Classico: Algebra Booleana, spesso irreversibile.
  - Quantistico: Operatori Unitari lineari.
  - Vincolo: L'Informazione non viene mai persa durante l'evoluzione.

- L'Output (Interfaccia Classica):
  - Misurazione: L'osservazione proietta lo stato $|\psi\rangle$ in una base (es. $\{|0\rangle,|1\rangle\}$) distruggendo la sovrapposizione.
  - Probabilita: $P(0)=|\alpha|^2$, $P(1)=|\beta|^2$ (Regola di Born).

UNIVERSITÀ DEGLI STUDI DI BRESCIA

Oltre il Calcolo Classico: Le Classi di Complessità

- Estensione del Modello Probabilistico:
  - BPP (Bounded-error Probabilistic Polynomial): La classe dei problemi risolvibili efficientemente da un computer classico con accesso a casualità (randomness).
  - BQP (Bounded-error Quantum Polynomial): La classe dei problemi risolvibili da un computer quantistico in tempo polinomiale con probabilità di errore limitata (<1/3).
- La Catena di Inclusione:
  - La relazione gerarchica fondamentale è: $P \subseteq BPP \subseteq BQP \subseteq PSPACE$
  - Nota: Un computer quantistico può simulare qualsiasi computer classico (P e BPP), ma non sappiamo ancora se BQP contenga problemi in NP−Complete.
- Il Limite Superiore:
  - Il Quantum Computing non viola la tesi di Church-Turing sulla computabilità, ma estende la Tesi di Church-Turing Estesa sulla trattabilità efficiente.



UNIVERSITÀ DEGLI STUDI DI BRESCIA

Il Problema della Separazione: *BQP vs BPP*

Inclusione (Certezza):

- È dimostrato che BPP ⊆ BQP.
- Un computer quantistico può simulare qualsiasi circuito classico probabilistico (es. tramite gate reversibili come Toffoli).
- Conseguenza: Il Quantum Computing generalizza il modello classico, non lo sostituisce per task semplici.

Separazione Stretta (Congettura):

- Non esiste ancora una dimostrazione formale che BPP ≠ BQP.

Evidenza Empirica (Il "Muro" Esponenziale):

- La simulazione classica di un sistema quantistico richiede risorse esponenziali.
- Per simulare n qubit, servono 2^n coefficienti complessi.
- Esempio: Con n=50, la memoria richiesta supera i Petabyte.

UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Dalla Teoria alla Pratica: Deutsch-Jozsa e Grover

Algoritmo di Deutsch-Jozsa (Il Proof-of-Concept)

- Problema: Determinare se una funzione $f:\{0,1\}^n \to \{0,1\}$ è costante o bilanciata (Promise Problem).
- Complessità (Query Complexity):
  - Classico (Worst-case): Richiede $2^{(n-1)}+1$ valutazioni per la certezza deterministica.
  - Quantistico: Richiede 1 sola query all'oracolo, indipendentemente da n.
- Significato: Dimostra una separazione esponenziale deterministica rispetto al calcolo classico, sfruttando il parallelismo quantistico e l'interferenza.

Algoritmo di Grover (L'Applicazione Reale)

- Problema: Ricerca in un database non strutturato di dimensione $N=2^n$.
- Speedup:
  - Classico: $O(N)$ *(ricerca lineare)*.
  - Quantistico: $O(N^{1/2})$ *(speedup quadratico)*.
- Ottimalità: È dimostrato (Bennett, Bernstein, Brassard, Vazirani) che $\Omega(N^{1/2})$ è il limite inferiore teorico: non è possibile fare meglio di così per la ricerca black-box.

UNIVERSITÀ DEGLI STUDI DI BRESCIA

Validazione Sperimentale: Grover su IBM Heron r2

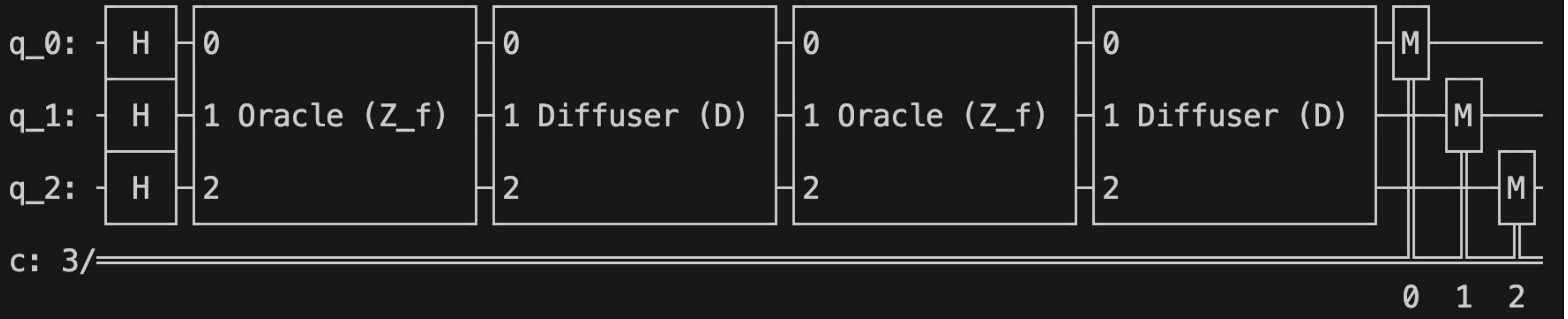
- Setup dell'Esperimento:
  - Algoritmo: Grover per N=8 (n=3 qubit).
  - Target: Stato ∣101⟩ (Indice 5).
  - Backend: ibm_fez (Processore IBM Heron r2).
  - Iterazioni: k≈ (π/4)N^1/2 ≈ 2.
- Il Costo dell'Astrazione (Transpilation):
  - Il gate astratto Toffoli (CCX) non esiste nativamente sull'hardware.
  - Il compilatore (Transpiler) lo decompone in gate nativi (SX, RZ, CZ).
  - Profondità Circuito: Da 10 (logico) a 139 (fisico) → +1290%.
- Implicazione: L'aumento della profondità espone il calcolo alla decoerenza (T≈113μs).
- Probabilità Successo (∣101⟩):
  - Simulatore Ideale: 94.06% (Limite teorico dell'algoritmo).
  - Hardware Reale: 74.99%.
- Rumore: Il ~25% di errore è distribuito sugli stati non-target a causa di errori nei gate e di lettura (readout error).

Analisi: Schema del Circuito Logico

```
=== Grover's Algorithm Simulation ===
Configuration Loaded:
  - Qubits: 3
  - Target: |101>
  - Shots:  1024


> Optimal iterations calculated: 2

=== Abstract Circuit Diagram ===
```



Esecuzione: Simulazione Locale

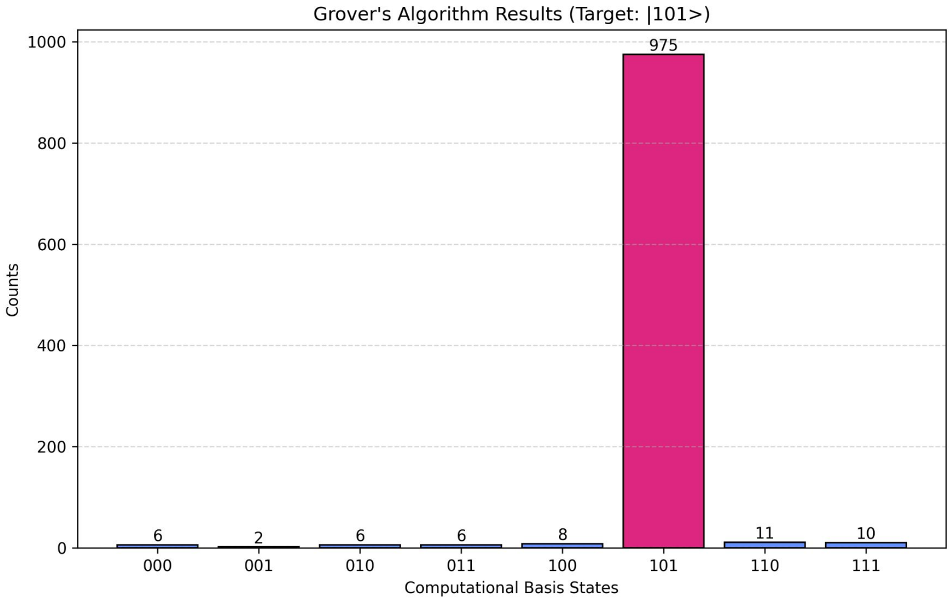
```
> Transpiling circuit for aer_simulator...
  - Depth: 10
  - Gate Count: OrderedDict({'u2': 12, 'ccx': 4, 'measure': 3, 'h': 1, 'u1': 1})

> Executing job with 1024 shots...

=== Experimental Results ===
{'101': 979, '111': 12, '011': 9, '000': 7, '100': 5, '001': 5, '110': 4, '010': 3}
> Histogram saved successfully: output.png

> Target state |101> found in 95.61% of shots.

[OUTCOME] SUCCESS: Probability peak matches target.
```



Esecuzione: Reale IBM Fez

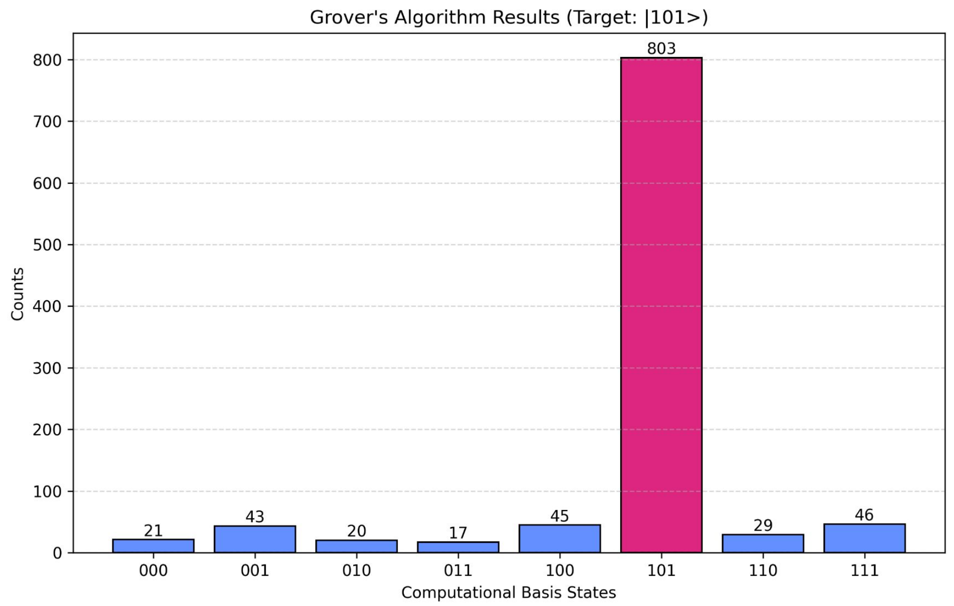
```
> Transpiling circuit for ibm_fez...
  - Depth: 138
  - Gate Count: OrderedDict({'sx': 77, 'rz': 61, 'cz': 39, 'measure': 3, 'x': 1})

> Executing job with 1024 shots...

=== Experimental Results ===
{'101': 803, '111': 46, '100': 45, '001': 43, '110': 29, '000': 21, '010': 20, '011': 17}
> Histogram saved successfully: output.png

> Target state |101> found in 78.42% of shots.

[OUTCOME] SUCCESS: Probability peak matches target.
```



UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Conclusioni

- Il Paradosso della Complessità:
  - Sebbene la separazione BQP ≠ BPP non sia formalmente dimostrata, gli speedup algoritmici (Grover, Shor) e il costo esponenziale della simulazione classica validano il paradigma quantistico come possibile via per superare i limiti di Moore.
- La Realtà NISQ e il Costo dell'Astrazione:
  - I risultati sperimentali dimostrano che l'astrazione software non è "gratuita".
  - Il processo di transpilation (adattamento alla topologia fisica) può aumentare la profondità del circuito di oltre un ordine di grandezza (+1290%), introducendo errori fatali.
- Nuovo Paradigma di Sviluppo:
  - L'ingegnere del software non può limitarsi alla logica astratta; è necessaria una sensibilità "hardware-aware".
  - Il futuro immediato è ibrido: CPU classica per il controllo di flusso, QPU (Quantum Processing Unit) come coprocessore per task specifici (es. oracoli).

Grazie per l'attenzione, sono a disposizione per eventuali domande.