Pinocchio e l'informazione quantistica

Stefano Mancini e Lorenzo Maccone

Questo articolo va un po' al di là dei criteri di generale leggibilità che ci siamo imposti per questa rivista. Tuttavia, la prima parte (classica) è veramente accessibile a tutti, visto che richiede solo la capacità di dividere ripetutamente per due. Certo, la parte quantistica è di più complessa accessibilità, anche per i suoi aspetti formali; ma, scusandoci con i lettori, ci permettiamo di sottolineare che è, forse, il modo più semplice di evidenziare la differenza tra il modo di ragionare classico e quello quantistico. Chiunque abbia interrogativi al riguardo può scrivere agli autori o alla rivista per porre le sue domande. (C.B.)

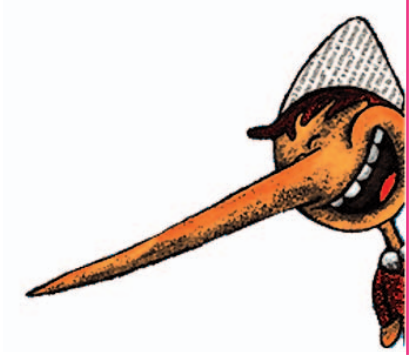
Trovare una strategia efficiente per ottenere la verità da un mentitore è compito molto arduo. Con riferimento al mondo fiabesco, Pinocchio è il personaggio più legato alle bugie in virtù del suo naso. Supponiamo che Geppetto voglia scoprire qualcosa da Pinocchio prescindendo però dal suo naso e potendo utilizzare solo domande la cui risposta sia «sì» o «no». Pinocchio mentirà in alcune delle sue risposte, ma supponiamo che non voglia dire più di un numero l di bugie. Quante domande saranno necessarie a Geppetto per ottenere la verità? Questa è una rilettura del famoso *problema di Ulam* di cui, ad oggi, non si conosce una soluzione ottimale.

La meccanica quantistica è ricca di effetti talmente controintuitivi da risultare spesso quasi paradossali. Talvolta è possibile sfruttarli proficuamente nel manipolare informazione. Questo è uno degli scopi del fecondo campo della *Informazione Quantistica* che negli ultimi anni ha visto un enorme sviluppo [1]. In questo articolo ne daremo un'applicazione, illustrando come risolvere in maniera efficiente proprio il problema di Ulam.

Il nostro scopo qui è di renderci comprensibili a tutti, quindi partiremo con una descrizione la più elementare possibile. I dettagli tecnici verranno affrontati solo in un secondo momento. Rimandiamo il lettore più esperto all'articolo citato in bibliografia [2].

Supponiamo che Pinocchio stia pensando a un numero compreso tra 1 e 1.000.000. Geppetto può adottare diverse strategie, ovvero fare domande di tipo diverso, per scoprire tale numero. Se Pinocchio è sincero, una buona strategia è quella di porre domande che discriminino tra due insiemi aventi circa la stessa dimensione. Per esempio, la prima domanda di Geppetto può essere «il numero è maggiore di 500.000?». Se la risposta è «no», la seconda domanda sarà «il numero è compreso tra 250.000 e 500.000?», e così via. Una simile strategia permetterà a Geppetto di indovinare un qualunque numero compreso tra 1 e 1.000.000, con 20 domande, dato che 1.000.000 è inferiore a 2^{20}. È questa la *strategia adattiva a bisezione*, in quanto equivale a domandare «il numero appartiene all'intervallo A?», dove A è un intervallo di numeri che viene dimezzato a ogni nuova domanda. D'altro canto, una strategia *naïve* è quella di chiedere: «il numero è 1?», «il numero è 2?», e così via. Chiaramente quest'ultima strategia permetterà a Geppetto di indovinare il numero, ma in maniera del tutto inefficiente. Invece la strategia adattiva a bisezione risulta ottimale,

I



richiede cioè il numero minimo di domande. La situazione si complica se Pinocchio decide di mentire in alcune delle sue risposte. Supponiamo che (per non incorrere nelle ire della Fata turchina) voglia limitarsi a dire non più di l bugie. Ci si aspetta in tal caso la necessità di aumentare il numero di domande. Una semplice strategia prevede che Geppetto ripeta ciascuna domanda un numero di volte pari a $2l+1$. La risposta sarà «sì» se egli ottiene più «sì» che «no» e viceversa sarà «no» se ottiene più «no» che «sì»: dato che Pinocchio dirà solo l bugie, le altre $l+1$ risposte alla domanda ripetuta saranno la verità. Pertanto, il numero totale di domande risulterà $20(2l+1)$.

D'altro canto, una strategia ottimale (cioè che richieda il minimo numero di domande possibile) è nota solo in alcuni casi speciali [3], per i quali il numero di domande risulta comunque sempre maggiore di 20. Il problema del gioco delle 20 domande con interlocutore menzognero è stato posto e analizzato da Alfred Rényi (1921-1970) e Stanislaw Ulam (1909-1984) ma è generalmente noto come *problema di Ulam* [4]. Una soluzione generale di tale problema avrebbe ripercussioni in ambiti che vanno dalla logica alla teoria della correzione degli errori nelle telecomunicazioni. Infatti, un canale di comunicazione digitale si comporta come un interlocutore che risponde con bit di informazione alle nostre domande. Gli errori nella trasmissione e ricezione sono analoghi a bugie, in quanto ribaltano il valore del bit di informazione.

Sorprendentemente, in ambito quantistico è possibile risolvere il problema di Ulam in modo più efficiente. La domanda di Geppetto sarà una sovrapposizione quantistica (vedi testo a lato pag. 80) di domande del tipo «il tuo numero appartiene all'intervallo A?» con A che varia in un insieme di possibili intervalli che definiremo dopo. (Per semplicità ci limiteremo a considerare il caso in cui Pinocchio pensa a un numero, ma la procedura si può anche estendere al caso in cui pensi a un oggetto arbitrario). Iniziamo ad analizzare il caso in cui Pinocchio è sempre sincero (cioè il caso con $l=0$). È possibile scoprire la verità mediante un algoritmo quantistico [2]. Per poter utilizzare tale metodo, Geppetto dovrà studiare un set di intervalli A che sia efficiente. Il modo in cui li sceglie è il seguente. Ogni intervallo può essere identificato da un numero v, tale per cui un numero c cade nell'intervallo A_v se e solo se v e c scritti in notazione binaria hanno un numero dispari di uno nelle stesse posizioni. Se, invece, il numero di uno nelle stesse posizioni è pari, allora c non appartiene all'intervallo A_v. Matematicamente tale procedura si può descrivere dicendo che Geppetto fornisce a Pinocchio un vettore $\vec{v}$ di zeri ed uno: ovvero una stringa contenente il numero v in notazione binaria. Pinocchio possiede un analogo vettore che descrive il numero c a cui aveva pensato (che supponiamo compreso tra 1 e 2 elevato al numero di domande che Geppetto può fare). La risposta di Pinocchio sarà data dalla funzione $f(\vec{v})=\vec{v}\cdot\vec{c}$, cioè il prodotto scalare tra due stringhe binarie, ovvero la somma modulo-2 dei risultati del prodotto bit per bit delle due stringhe (vedi riquadro pag. 80).

In ambito quantistico, invece della stringa di bit, Geppetto e Pinocchio si scambieranno una stringa di qubit (vedi testo a lato pag. 80). Geppetto sottoporrà a Pinocchio il vettore di n qubit $|\vec{v}\rangle_G$ che contiene il valore dei bit di v. Inoltre, Geppetto manderà a Pinocchio un ulteriore qubit $|y\rangle_P$ dove Pinocchio registrerà il qubit della sua risposta, cioè il valore di $f(\vec{v})$ (i pedici G e P denotano rispettivamente il registro su cui Geppetto scrive la domanda e il registro su cui Pinocchio scrive la risposta). Quindi, dopo aver ricevuto $|\vec{v}\rangle_G|y\rangle_P$, Pinocchio restituirà a Geppetto la sua risposta nella forma $|\vec{v}\rangle_G|y\oplus f(\vec{v})\rangle_P$, dove $\oplus$ è la somma modulo 2 (vedi box pag. 80). Se, $y=0$, il qubit nel registro P conterrà la risposta alla domanda «Il numero appartiene all'intervallo A_v?», cioè il valore della funzione $f(\vec{v})$. L'uso di un algoritmo quantistico (vedi box pag. 81) permette a Geppetto di scoprire il valore del numero c pensato da Pinocchio con un'unica domanda. Ciò come conseguenza di una possibilità offerta solo dalla meccanica quantistica: la sovrapposizione di stati. Essa fa sì che si possa valutare in un solo colpo una funzione su tanti inputs, anziché su uno alla volta come accade «classicamente». È questo il concetto di parallelismo quantistico.

Nel caso in cui Pinocchio decida di dire qualche bugia, egli può mentire in due modi. O mentirà nella sua risposta (cioè risponderà «sì» quando c non appartiene all'intervallo A_v e risponderà «no» quando vi appartiene), oppure mentirà nel calcolare la funzione $f(\vec{v})$, cambiando un certo numero di bits nella stringa (ogni bit cambiato rappresenta una bugia di Pinocchio). In entrambi i casi

Cos'è un qubit?

Il *qubit* (contrazione di quantum bit) è l'analogo quantistico del bit. Invece di poter assumere i due valori (0 e 1) associati a due stati di un sistema classico, assume tutti gli infiniti possibili valori associati agli stati di un sistema quantistico con due gradi di libertà (per esempio lo spin di un elettrone). I valori 0 e 1 di un qubit sono indicati solitamente con i simboli $|0\rangle$ e $|1\rangle$ rispettivamente. Il valore più generale di un qubit si esprime come una somma di queste due quantità $\alpha|0\rangle+\beta e^{i\varphi}|1\rangle$, dove α e β sono due numeri reali tali che $\alpha^2 + \beta^2 = 1$, φ è un numero reale (compreso tra 0 e 2π) detto fattore di fase e i è l'unità immaginaria. Si può dire che un qubit nello stato $\alpha|0\rangle+\beta e^{i\varphi}|1\rangle$ possieda contemporaneamente i due valori 0 e 1. Questo è il concetto di *sovrapposizione quantistica*: se un sistema può esistere in uno di due stati diversi, allora può esistere contemporaneamente in entrambi. Tuttavia, quando tale valore viene misurato, l'atto stesso della misura farà in modo che esso risulterà 0 con una probabilità di α^2, e 1 con una probabilità di β^2 (è il meccanismo del cosiddetto *collasso della funzione d'onda*). Le ampiezze α e β si possono quindi interpretare come le radici quadrate della probabilità di misurare il valore corrispondente. La fase φ, invece, è in un certo senso legata all'aspetto ondulatorio del qubit (in meccanica quantistica ogni oggetto ha una doppia natura: *corpuscolare e ondulatoria*) e non ha una interpretazione classica diretta. Ciononostante gli effetti di tale fase diventano importanti nel momento in cui si fanno delle misure di interferometria quantistica. Praticamente, in tutti gli algoritmi quantistici che presentano un vantaggio sui corrispondenti algoritmi classici si impiega questo grado di libertà in maniera «creativa».

Geppetto è in grado di scoprire la verità. Se Pinocchio decide di mentire nella sua risposta, vuol dire che, invece di calcolare la funzione $f(\vec{v})$, calcolerà la funzione $f(\vec{v}) \oplus 1$, che vale 0 se $f(\vec{v})$ vale 1 e viceversa. In questo caso (vedere box pag. 81) la sommatoria all'interno della parentesi quadra nell'Eq. (4) acquista un segno meno. Questo però non cambia il risultato finale: ancora una volta l'unico termine non nullo della somma è per $\vec{c} \oplus \vec{w} = \vec{0}$ e quindi l'unico possibile risultato della misura sul registro G sarà $\vec{w} = \vec{c}$. Geppetto è ancora in grado di ottenere la verità con una singola domanda.

Supponiamo che, invece, Pinocchio decida di mentire l volte, girando l dei bit nel suo numero c, cioè del vettore $\vec{c}$. La soluzione più banale per Geppetto è ripetere la domanda un numero di volte pari a $2l + 1$. In tal caso Geppetto otterrà diverse possibili stringhe per $\vec{w}$ (ovvero $\vec{c}$), di cui almeno $l + 1$ uguali. La stringa giusta sarà quindi quella di maggioranza.

Come già abbiamo osservato, la strategia di ripetere le domande più volte permette di ottenere la verità anche in ambito classico. Mentre in ambito classico questa strategia necessita comunque di $n(2l + 1)$ domande ($n = 20$ nel «gioco delle 20 domande»), in ambito quantistico esse sono ridotte di un fattore n. In realtà l'algoritmo quantistico è molto piu efficiente mostrando vantaggi rispetto a qualsiasi strategia classica conosciuta, tuttavia per ragioni di semplicità ci siamo limitati alla presente esposizione.

Concludendo, mentre nel mondo delle fiabe è semplice scoprire le menzogne dalla lunghezza del naso di Pinocchio, nel mondo reale non è altrettanto semplice, ma la meccanica quantistica può aiutarci. Le applicazioni per l'algoritmo che abbiamo presentato possono quindi essere numerose. Tuttavia, più che per gestire i bugiardi, avrà applicazioni più promettenti nella correzione degli errori in telecomunicazioni, computazioni o ambiti simili.

Incoraggiamo il lettore che volesse approfondire con domande o curiosità a contattare gli autori. ●

BIBLIOGRAFIA

[1] **BENNETT C.H., DI VINCENZO D.P.**, «Quantum Information and Computation», *Nature*, London, vol. 404, pp. 247-255, 2000.

[2] **MANCINI S., MACCONE L.**, «Using Quantum Mechanics to Cope with Liars», *Interna-tional Journal of Quantum Information*, Vol. 3, pp. 729-733, 2005; ottenibile anche presso http://arxiv.org/abs/quant-ph/ 0508156.

[3] **PELC A.**, «Searching games with errors - fifty years of coping with liars», *Theoretical Computer Science*, Vol. 270, pp.71-109, 2002.

[4] **ULAM S.**, *Adventures of a Mathematician*, Scribner, New York, 1976, p. 281.

Calcolo della funzione $f(\vec{v}) = \vec{v} \cdot \vec{c}$

Introduciamo la somma-modulo-2 '⊕' definita come $0 \oplus 1 = 1 \oplus 0 = 1$; e $0 \oplus 0 = 1 \oplus 1 = 0$.

Consideriamo l'esempio:

		notazione binaria				$f(\vec{v}) = \vec{v} \cdot \vec{c}$.
numero $c = 14$	$\leftrightarrow \vec{c} =$	1	1	1	0	
intervallo $v = 5$	$\leftrightarrow \vec{v} =$	0	1	0	1	
prodotto bit per bit:		0	1	0	0	

somma modulo-2 dei risultati: $0 \oplus 1 \oplus 0 \oplus 0 = 1$. Quindi, $f(\vec{v}) = \vec{v} \cdot \vec{c} = 1$.

Consideriamo un altro esempio:

		notazione binaria			
numero $c = 14$	$\leftrightarrow \vec{c} =$	1	1	1	0
intervallo $v = 11$	$\leftrightarrow \vec{v} =$	1	0	1	1
prodotto bit per bit:		1	0	1	0

somma modulo-2 dei risultati: $1 \oplus 0 \oplus 1 \oplus 0 = 0$. Quindi, $f(\vec{v}) \equiv \vec{v} \cdot \vec{c} = 0$.

Si noti che $f(\vec{v}) = 0$ se i due vettori $\vec{v}$ e $\vec{c}$ hanno un numero pari di uno in corrispondenza e $f(\vec{v}) = 1$ se ne hanno un numero dispari.

L'algoritmo applicato da Geppetto

La procedura è descritta dai seguenti passi:
1. Geppetto prepara all'inizio i registri di qubit *G* e *P* come $|\vec{0}\rangle_G |1\rangle_R$. Poi applica una trasformazione di Hadamard a entrambi i registri. Una trasformazione di Hadamard H applicata a $|0\rangle$ e $|1\rangle$ crea una sovrapposizione equipesata dei due vettori:

$$|0\rangle \xrightarrow{H} (|0\rangle + |1\rangle)/\sqrt{2},$$

$$|1\rangle \xrightarrow{H} (|0\rangle + |1\rangle)/\sqrt{2}.$$

In generale, applicando una trasformazione di Hadamard su di un vettore $|\vec{u}\rangle$ di *n* qubit si otterrà una sovrapposizione equipesata dei vettori corrispondenti alle possibili stringhe di *n* bit

$$|\vec{u}\rangle \xrightarrow{H} \frac{1}{\sqrt{2^n}} \sum_{\vec{v}} (-1)^{\vec{v}\cdot\vec{u}} |\vec{v}\rangle \qquad (1)$$

dove $\sum_{\vec{v}}$ indica la somma su tutte le possibili stringhe $\vec{v}$ di *n* bit (che sono appunto 2^n). Geppetto otterrà, quindi, lo stato

$$|\vec{0}\rangle_G |1\rangle_P \xrightarrow{H} \frac{1}{\sqrt{2^n}} \sum_{\vec{v}} |\vec{v}\rangle_G \frac{|0\rangle_P - |1\rangle_P}{\sqrt{2}}. \qquad (2)$$

In sostanza, nel registro *G* Geppetto ha creato una sovrapposizione quantistica di domande riguardanti tutti i possibili intervalli A_v.
2. Pinocchio risponde a Geppetto calcolando la funzione $f(\vec{v})$. Siccome, però, Geppetto gli ha mandato tutti i possibili $\vec{v}$ in uno stato di sovrapposizione quantistica, Pinocchio risponderà (grazie al parallelismo quantistico) a *tutte* le possibilità allo stesso tempo! Il registro *P* contiene inizialmente lo stato $(|0\rangle - |1\rangle)/\sqrt{2}$, quindi le domande con risposta negativa verranno lasciate invariate, mentre quelle con risposta positiva acquisteranno un segno meno: infatti, $|0 \oplus 1\rangle - |1 \oplus 1\rangle = -(|0\rangle - |1\rangle)$. Dopo che Pinocchio ha calcolato il valore di $f(\vec{v})$, lo stato di Eq. (2) diventa

$$\frac{1}{\sqrt{2^n}} \sum_{\vec{v}} (-1)^{\vec{v}\cdot\vec{c}} |\vec{v}\rangle_G \frac{|0\rangle_P - |1\rangle_P}{\sqrt{2}}. \qquad (3)$$

3. Geppetto vuole ora desumere dallo stato di Eq. (3) il valore di $\vec{c}$. A tal fine, prima agisce nuovamente con una trasformazione di Hadamard su entrambi i registri ed ottiene lo stato

$$\frac{1}{2^n} \sum_{\vec{w}} \left[\sum_{\vec{v}} (-1)^{\vec{v}\cdot\vec{c} \oplus \vec{v}\cdot\vec{w}} \right] |\vec{w}\rangle_G |1\rangle_P, \qquad (4)$$

e poi compie una misura sul registro *G*. I potenziali risultati della misura sarebbero tutte le stringhe $\vec{w}$, ognuna ottenibile con una probabilità proporzionale all'ampiezza rappresentata dalla somma entro le parentesi quadre. Si noti però che essa risulta diversa da zero se e solo se $\vec{w} = \vec{c}$ (altrimenti essa è la somma di termini eguali ma di segno alterno, e come tale nulla). Pertanto, l'unico possibile risultato della misura è $\vec{w} = \vec{c}$: Geppetto ha scoperto $\vec{c}$ facendo una sola domanda a Pinocchio!

Stefano Mancini
è ricercatore presso il Dipartimento di Fisica, Università di Camerino & INFN Sezione di Perugia
email: stefano.mancini@unicam.it

Lorenzo Maccone
è ricercatore presso il QUIT - Quantum Information Theory Group,
Dipartimento di Fisica «A. Volta» Università di Pavia - email: maccone@qubit.it.