I codici di correzione d'errore

La realizzazione pratica della computazione e della crittografia quantistiche dipende criticamente dalla capacità di mantenere inalterato nel tempo o nello spazio lo stato di un insieme di "bit quantistici" che codificano l'informazione che intendiamo trasmettere o elaborare. Tuttavia, lo stato attuale della tecnologia pone delle serie limitazioni sui tempi e sulle condizioni in cui l'isolamento del sistema di bit dall'ambiente circostante può essere realizzato. Il miglioramento dei gate e delle tecniche di controllo dei sistemi rimane ovviamente una esigenza prioritaria; un ulteriore progresso può tuttavia derivare, e forse non può che derivare, da un approccio di tipo algoritmico.

Il senso di questa affermazione risulta evidente nel contesto classico della scienza delle telecomunicazioni. La trasmissione a distanza di informazione si scontra infatti, anche in tal caso, con la degradazione del segnale dovuta alla rumorosità del canale. Nei lunghi secoli che costituiscono la storia delle telecomunicazioni questo problema è stato affrontato cercando via via di realizzare trasmettitori più potenti (ad esempio accendendo fuochi più grandi), ovvero sfruttando canali meno rumorosi (segnali visivi piuttosto che acustici, fili elettrici invece di semafori). In altri termini, lo sforzo centrale è stato per secoli rivolto ad aumentare il rapporto segnale/rumore (SNR), seguendo in fondo la stessa logica innata che ci porta ad alzare la voce in un ambiente rumoroso.

Solo verso la metà di questo secolo, con lo sviluppo della teoria dell'informazione e i risultati ottenuti da Shannon, ci si è resi conto che questo non è l'unico approccio possibile, risultando anzi spesso il meno attuabile o conveniente. Il miglioramento dell'SNR trova infatti un limite da un lato per la naturale rumorosità termica dei canali fisici, dall'altro per l'impossibilità pratica, talora particolarmente stringente, di aumentare la potenza del segnale. Forse il

miglior esempio in questo senso è fornito dalle esplorazioni spaziali per mezzo di sonde, che si trovano a dover trasmettere dati su distanze enormi assorbendo la minima potenza possibile. In tale caso, seguendo l'idea di Shannon, risulta economico affidare l'integrità dell'informazione non ad un elevato (e praticamente irraggiungibile) rapporto segnale/rumore, bensì alla ridondanza dell'informazione, che viene distribuita su una sequenza di bit più lunga di quella normalmente necessaria a codificarla.

Nello stabilire i criteri di codifica ha importanza fondamentale il *secondo teorema di Shannon*, che stabilisce la possibilità asintotica di una comunicazione libera da errori qualora il rapporto tra il numero di bit di informazione trasmessi e la lunghezza della parola che li codifica non superi un certo limite, funzione della probabilità di errore sul canale.

Un esempio "classico"

Il modello di canale di trasmissione rumoroso al quale generalmente ci si riferisce nello studio dei codici classici di correzione d'errore è quello *del canale binario simmetrico* o BSC (Figura 15). Esso rappresenta una linea dati che connette un trasmettitore T ad un ricevitore R permettendo al primo di trasmettere un bit alla volta. Si ipotizza che un bit "1" trasmesso da T abbia una probabilità p di essere affetto da errore e comparire perciò all'altro estremo del canale come uno "0". Si suppone inoltre che un bit "0" abbia la stessa probabilità p di essere trasmesso come un "1", da cui l'aggettivo *simmetrico*.

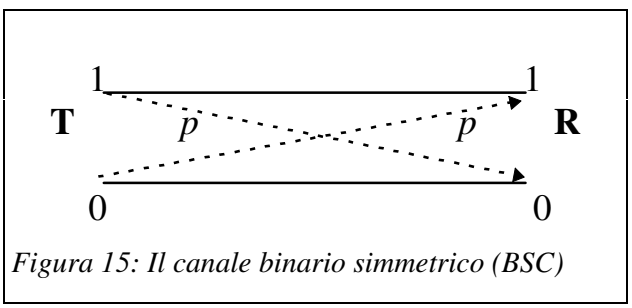


Figura 15: Il canale binario simmetrico (BSC)

Dato un messaggio costituito da un singolo bit di informazione, la probabilità di trasmetterlo con successo lungo il canale è chiaramente $(1-p)$. Un messaggio di n bit sarà però

esente da errore soltanto con probabilità $(1-p)^n$, che tende esponenzialmente a zero con l'aumentare di n. Da questo punto di vista la situazione appare particolarmente infelice, in quanto nessun canale reale risulta essere abbastanza silenzioso per trasmettere un messaggio di lunghezza arbitraria. Si può ora avere l'erronea impressione che generare della ridondanza non faccia che peggiorare le cose, in quanto comporta un allungamento del messaggio con conseguente aumento della probabilità di errore. Il seguente esempio illustra però come il pur reale incremento del numero medio totale di errori non infici la possibilità del ricevente di utilizzare la ridondanza per ricostruire il messaggio originale con una probabilità di successo superiore a quella altrimenti ottenibile.

Consideriamo la codifica elementare consistente in una tripla ripetizione del bit da trasmettere: conveniamo perciò che T trasmetta "000" per indicare un bit nello stato zero e "111" per indicare un bit nello stato uno. In corrispondenza R userà, per decodificare il segnale, la regola della *votazione a maggioranza*, assegnando alla terna di bit ricevuta il valore di verità sul quale almeno due dei tre bit concordano (che ovviamente esiste). Analizziamo nella seguente tabella i possibili esiti della trasmissione:

Numero di errori	***Esempio***	***Probabilità***	***Ricezione***
0	"000"→"000"	$(1-p)^3$	corretta
1	"000"→"010"	$3p(1-p)^2$	corretta
2	"000"→"101"	$3p^2(1-p)$	errata
3	"000"→"111"	p^3	errata

La probabilità totale di errore nella trasmissione risulta ora pari a $3p^2(1-p) + p^3 = 3p^2-2p^3$, che per $p < ½$ è minore di p; conversamente, la probabilità di ricezione corretta è aumentata da $1-p$ a $1-O(p^2)$.

Questo esempio è noto come *codice a tripla ripetizione*, e costituisce il più semplice codice in grado di correggere un errore. Se indichiamo con $\mathbf{Z}_2$ il campo formato dall'insieme $\{0,1\}$ le *parole* del codice, ovvero le sequenze trasmesse,

sono un sottoinsieme dello spazio vettoriale $(\mathbf{Z}_2)^3$ sul campo $\mathbf{Z}_2$. Tale spazio è manifestamente costituito da un totale di otto triple della forma (x,y,z) con x, y e z uguali a zero o a uno. I vettori sono rappresentabili come formanti i vertici di un cubo di lato unitario (Figura 16). Sono evidenziate in figura le due parole del codice "000" ed "111". Supponiamo ora che T trasmetta uno zero: in caso si verifichi un singolo errore di trasmissione, la sequenza che R effettivamente riceve corrisponde ad uno dei vertici collegati all'origine mediante le frecce continue. Viceversa, se T trasmette "111", R può ricevere la sequenza corretta o una delle tre da essa raggiungibili seguendo le frecce tratteggiate. Siccome non esistono vertici raggiungibili con un solo spostamento sia da "000" sia da "111", questo codice permette di correggere un errore. Notiamo inoltre che non esistono configurazioni che non siano raggiungibili a partire dalle parole nell'ipotesi di zero od un errore: il codice risulta perciò essere ottimale, in quanto sfrutta appieno lo spazio vettoriale nel quale è immerso.

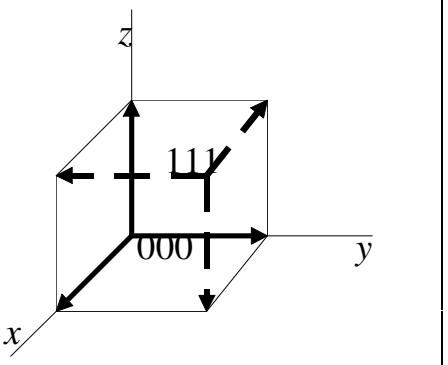


Figura 16

Gli spazi vettoriali su $\mathbf{Z}_2$ presentano una metrica naturale, *detta distanza di Hamming*. Se **v**, **w** sono vettori in uno $\mathbf{Z}_2$-spazio **V**, la distanza di Hamming d tra **v** e **w** è definita da $\mathrm{d}(\mathbf{v},\mathbf{w}) = \sum_{j=1}^{\dim(\mathbf{V})} \mathbf{v}_j \,\mathrm{XOR}\, \mathbf{w}_j$. Tale distanza conta il numero di lati dell'ipercubo che ha per vertici i vettori di **V** che occorre percorrere per raggiungere **v** a partire da **w**. L'attraversamento di ogni lato di tale ipercubo corrisponde ad alterare il valore di un bit.

Ritornando al codice di tripla ripetizione visto sopra, è evidente che le parole del codice, "000" ed "111", sono il centro di due sfere di raggio unitario, ciascuna costituita da una parola e dai tre vertici da essa raggiungibili seguendo le

frecce. Esse sono evidentemente le massime sfere non intersecantisi che è possibile costruire, in quanto riempiono tutto lo spazio. Questo indica che mediante un codice in $(\mathbf{Z}_2)^3$ non possiamo correggere più di un errore. Lo spazio $(\mathbf{Z}_2)^3$ non può inoltre contenere più di due sfere di raggio unitario; ciò implica che un codice con parole di tre bit, per correggere almeno un errore, deve contenere due sole parole, ovvero può avere un contenuto informativo massimo di 1 bit, con un *rate* (rapporto tra contenuto di informazione e lunghezza delle parole) di 1/3.

I codici di correzione d'errore sono normalmente caratterizzati dalla tripla [*n*,*k*,*d*] dove *n* indica la dimensione dello spazio (ovvero la lunghezza delle parole), *k* il numero di bit di informazione codificati negli *n* bit e *d* la distanza di Hamming minima tra due parole. Perché un codice possa correggere *t* errori è necessario che *d* sia almeno il doppio di *t*, o più precisamente $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, dove le parentesi di Gauss indicano il massimo intero non superiore al numero che racchiudono. Fissati *n* e *t*, ragionamenti geometrici sul numero di sfere di raggio *t* che lo spazio è in grado di contenere racchiudono i valori utili di *k* tra un limite inferiore, detto di Gilbert-Varshamov, e un limite superiore, di Hamming:

$$\frac{2^n}{\sum_{i=0}^{2t}\binom{n}{i}} \le 2^k \le \frac{2^n}{\sum_{i=0}^{t}\binom{n}{i}}.$$

Il rapporto fra *k* ed *n*, ovvero il *rate* di trasmissione, è inoltre limitato dal secondo teorema di Shannon, che afferma che la probabilità che si verifichi un errore non recuperabile tende a zero con l'aumentare di *n* purché il rapporto *k*/*n* (che si intende fissato) sia minore o uguale di 1−H(*p*) [Khinchin]. Quest'ultima espressione, nota come *capacità del canale BSC*, è funzione della probabilità di errore *p* mediante H, la funzione *entropia*, che gioca un ruolo centrale nella teoria dell'informazione ed assume nel nostro caso la forma $\mathrm{H}(x) = -x \log_2 x - (1-x)\log_2(1-x)$.

Un semplice codice quantistico

Presentiamo ora un analogo quantistico del codice di tripla ripetizione, dimostrando che esso è in grado di proteggere lo stato di un bit quantistico da uno specifico tipo di interazione con il canale di trasmissione.

Sia dato un bit nello stato $\alpha|0\rangle+\beta|1\rangle$, che può anche non essere noto a chi trasmette. Supponiamo che il canale abbia una probabilità *p* di interagire con il bit durante la trasmissione, e questa interazione porti il bit ed il canale a correlarsi secondo il seguente schema:

$$|0\rangle|R\rangle \rightarrow |0\rangle|R_0\rangle$$

$$|1\rangle|R\rangle \rightarrow |1\rangle|R_1\rangle$$

dove $|R\rangle$ è lo stato iniziale del canale, e in generale $\langle R_0|R_1\rangle \neq 0$. Questa interazione è nota in ottica quantistica col nome di *decoerenza*, il cui senso si comprende confrontando la matrice densità del bit prima e dopo l'interazione. Inizialmente il bit è scorrelato dal canale, e la sua matrice densità è

$$\rho = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix};$$

dopo l'interazione il bit si è correlato col canale, e la sua matrice densità ridotta è ora

$$\overline{\rho} = \begin{pmatrix} |\alpha|^2 & 2\alpha\beta^*\langle R_1|R_0\rangle \\ 2\alpha^*\beta\langle R_0|R_1\rangle & |\beta|^2 \end{pmatrix}.$$

Come si vede, gli unici termini ad essere mutati sono quelli al di fuori della diagonale. Essi sono usualmente indicati col nome di *coerenze*, in quanto mantengono la traccia della relazione di fase con cui $|0\rangle$ ed $|1\rangle$ compaiono nella sovrapposizione. I termini sulla diagonale sono invece denominati *popolazioni*, in quanto indicano la probabilità di trovare il bit nel livello $|0\rangle$ o nel livello $|1\rangle$.

Ciò che in altri termini accade quando si verifica una *decoerenza* è che il canale tenta di "misurare" lo stato del bit. L'informazione che esso riesce ad ottenere su tale stato è tanto maggiore quanto minore è il prodotto $\langle R_0 | R_1 \rangle$. Quando i due vettori sono ortogonali, infatti, il canale "sa esattamente" se il bit si trova nello stato $|0\rangle$ o nello stato $|1\rangle$; questo distrugge la relazione di fase dello stato iniziale, per cui i due termini fuori dalla diagonale in $\bar{\rho}$ si azzerano. Viceversa se $|R_0\rangle$ è quasi parallelo ad $|R_1\rangle$ il canale non è in grado di identificare con sicurezza lo stato del bit, e $\bar{\rho} \approx \rho$.

Questo tipo di interazione risulta particolarmente significativo ad esempio nel caso di bit quantistici realizzati secondo il modello di Cirac e Zoller con ioni intrappolati (vedi pag. 74 e seguenti), essendo causato delle collisioni elastiche degli ioni con gli atomi di gas residuo presenti nella cavità.

Ritorniamo ora al problema della trasmissione. Riassumendo, il generico stato di un bit quantistico ha nelle ipotesi fatte probabilità *p* di subire, durante la trasmissione, il seguente processo [Ekert4]:

$$(\alpha|0\rangle + \beta|1\rangle)|R\rangle \rightarrow \alpha|0\rangle|R_0\rangle + \beta|1\rangle|R_1\rangle.$$

Per costruire un codice di correzione di errore è anzitutto conveniente eseguire sul bit una trasformazione unitaria in modo da trasformarne lo stato in $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$, con $|\bar{0}\rangle = |0\rangle + |1\rangle$ e $|\bar{1}\rangle = |0\rangle - |1\rangle$ (omettiamo qui e nel segito i fattori di normalizzazione).

L'effetto dell'interazione col canale sui vettori della nuova base è:

$$|\bar{0}\rangle|R\rangle \rightarrow |\bar{0}\rangle|R^+\rangle + |\bar{1}\rangle|R^-\rangle$$

$$|\bar{1}\rangle|R\rangle \rightarrow |\bar{0}\rangle|R^-\rangle + |\bar{1}\rangle|R^+\rangle$$

dove $|R^+\rangle = |R_0\rangle + |R_1\rangle$ e $|R^-\rangle = |R_0\rangle - |R_1\rangle$.

Successivamente, analogamente a quanto prescritto dal codice classico di tripla ripetizione, utilizziamo altri due bit per creare il seguente stato:

$$|\psi\rangle = \alpha|\overline{0}\,\overline{0}\,\overline{0}\rangle + \beta|\overline{1}\,\overline{1}\,\overline{1}\rangle.$$

Questa operazione non richiede, come illustrato nel seguito, la conoscenza esplicita dello stato che deve essere codificato. Supponiamo ora ad esempio che il primo bit interagisca con il canale. L'evoluzione dello stato complessivo $|\psi\rangle|R\rangle$ dell'insieme dei tre bit e del canale è allora

$$\left(\alpha|\overline{0}\,\overline{0}\,\overline{0}\rangle + \beta|\overline{1}\,\overline{1}\,\overline{1}\rangle\right)|R\rangle \quad \rightarrow \quad \left(\alpha|\overline{0}\,\overline{0}\,\overline{0}\rangle + \beta|\overline{1}\,\overline{1}\,\overline{1}\rangle\right)|R^{+}\rangle + \left(\alpha|\overline{1}\,\overline{0}\,\overline{0}\rangle + \beta|\overline{0}\,\overline{1}\,\overline{1}\rangle\right)|R^{-}\rangle.$$

Denotiamo lo stato finale, che rappresenta il messaggio degradato dal canale, con $|\tilde{\psi}\rangle$. Per ricostruire $|\psi\rangle$ è sufficiente, indipendentemente da quale bit ha effettivamente interagito con il canale, eseguire successivamente due proiezioni di $|\tilde{\psi}\rangle$ sui sottospazi $\mathbf{L}_1$ ed $\mathbf{L}_2$ definiti da

$$\mathbf{L}_1 = \text{Span}\left\{|\overline{0}\,\overline{0}\,\overline{0}\rangle, |\overline{1}\,\overline{1}\,\overline{1}\rangle, |\overline{1}\,\overline{0}\,\overline{0}\rangle, |\overline{0}\,\overline{1}\,\overline{1}\rangle\right\}$$

$$\mathbf{L}_2 = \text{Span}\left\{|\overline{0}\,\overline{0}\,\overline{0}\rangle, |\overline{1}\,\overline{1}\,\overline{1}\rangle, |\overline{0}\,\overline{1}\,\overline{0}\rangle, |\overline{1}\,\overline{0}\,\overline{1}\rangle\right\}$$

Nel caso da noi considerato, nel quale il primo bit ha interagito con il canale, la proiezione su $\mathbf{L}_1$ ha sempre successo e lascia $|\tilde{\psi}\rangle$ inalterato. La proiezione su $\mathbf{L}_2$ può invece avere due esiti. Se $|\tilde{\psi}\rangle$ si proietta parallelamente ad $\mathbf{L}_2$ i tre bit risultano, dopo la misura, nello stato originale $|\psi\rangle = \alpha|\overline{0}\,\overline{0}\,\overline{0}\rangle + \beta|\overline{1}\,\overline{1}\,\overline{1}\rangle$. Se al contrario la proiezione fa collassare $|\tilde{\psi}\rangle$ sull'ortogonale di $\mathbf{L}_2$ allora lo stato finale dei tre bit viene ad essere $|\psi'\rangle = \alpha|\overline{1}\,\overline{0}\,\overline{0}\rangle + \beta|\overline{0}\,\overline{1}\,\overline{1}\rangle$, che permette di recuperare $|\psi\rangle$ mediante la semplice applicazione di un NOT al primo bit.

Le due proiezioni su $\mathbf{L}_1$ ed $\mathbf{L}_2$ forniscono l'informazione necessaria per correggere un errore dovuto a decoerenza su uno qualsiasi dei bit. Illustriamo nella seguente tabella le diverse possibilità, indicando il risultato delle proiezioni

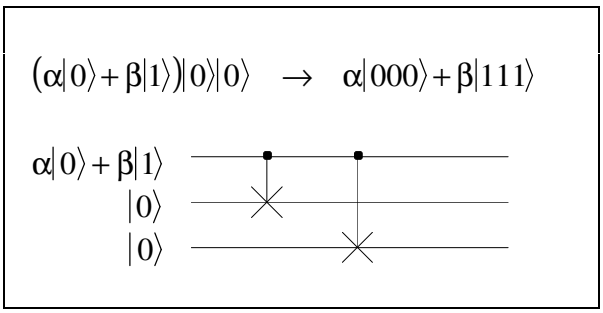
con 1 quando lo stato collassa sul sottospazio $\mathbf{L}_i$ e con 0 quando è proiettato sul suo ortogonale.

Numero del bit che ha interagito	*Proiezione su* $\mathbf{L}_1$	*Proiezione su* $\mathbf{L}_2$	*Correzione da applicare*
nessun errore	1	1	nessuna
bit 1, 2 o 3	1	1	nessuna
bit 1	1	0	NOT sul bit 1
bit 2	0	1	NOT sul bit 2
bit 3	0	0	NOT sul bit 3

Notiamo che, ai fini di effettuare l'eventuale correzione, non è necessario sapere né se un errore si è effettivamente verificato né quale bit esso ha interessato, in quanto l'azione da intraprendere è univocamente determinata dal risultato delle proiezioni su $\mathbf{L}_1$ ed $\mathbf{L}_2$.

Illustriamo ora una semplice implementazione del codice per mezzo di gate quantistici. Nel seguito, sottintenderemo la barra sugli stati dei singoli bit, scrivendo ad esempio $|101\rangle$ in luogo di $|\bar{1}\,\bar{0}\,\bar{1}\rangle$.

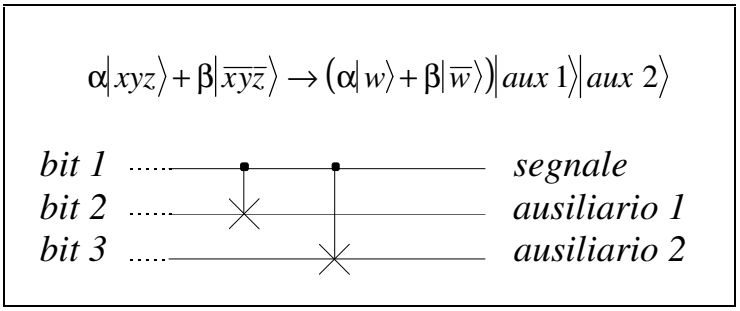
Figura 17: Rete di codifica.



La preparazione di $|\psi\rangle$ viene effettuata dalla rete a lato illustrata (Figura 17). Essa è costituita da due porte CONTROL-NOT che vengono utilizzate per copiare lo stato da trasmettere, che supponiamo sia lo stato del primo bit, sui bit ausiliari. Questo esaurisce il procedimento di codifica; i tre bit sono a questo punto pronti per essere trasmessi al destinatario.

La decodifica viene effettuata da una rete identica alla precedente (Figura 18). Essa riceve in ingresso il messaggio degradato $|\tilde{\psi}\rangle$ e restituisce in uscita tre bit *non correlati fra loro*, nello stato complessivo $(\alpha|w\rangle+\beta|\bar{w}\rangle)|aux\,1\rangle|aux\,2\rangle$, dove la barra indica il NOT logico. Come è evidente il primo bit contiene, a meno di un

Figura 18: Rete di decodifica ($\bar{x}$ = NOT x).



NOT, la ricostruzione dello stato originale $\alpha|0\rangle + \beta|1\rangle$. I due bit rimanenti o bit ausiliari, indicati con $|aux\ \mathrm{n}\rangle$, specificano se il primo bit debba effettivamente essere negato o meno per ricostruire lo stato originale. Essendo scorrelati dal primo, inoltre, questi bit possono essere misurati in maniera irreversibile, per quanto ciò non sia strettamente necessario ai fini dell'eventuale correzione, che può essere eseguita da un gate di Toffoli operante sul primo bit e controllato dalle due linee ausiliarie.

Riportiamo nella seguente tabella i possibili ingressi della rete di decodifica e l'azione dei due gate CONTROL-NOT:

Stato degradato in ingresso	*Dopo il primo* C-NOT	*Dopo il secondo* C-NOT	*Correzione da effettuare sul primo bit*
$\alpha\|000\rangle + \beta\|111\rangle$	$\alpha\|000\rangle + \beta\|101\rangle$	$(\alpha\|0\rangle + \beta\|1\rangle)\|0\rangle\|0\rangle$	nessuna
$\alpha\|100\rangle + \beta\|011\rangle$	$\alpha\|110\rangle + \beta\|011\rangle$	$(\alpha\|1\rangle + \beta\|0\rangle)\|1\rangle\|1\rangle$	NOT
$\alpha\|010\rangle + \beta\|101\rangle$	$\alpha\|010\rangle + \beta\|111\rangle$	$(\alpha\|0\rangle + \beta\|1\rangle)\|1\rangle\|0\rangle$	nessuna
$\alpha\|001\rangle + \beta\|110\rangle$	$\alpha\|001\rangle + \beta\|100\rangle$	$(\alpha\|0\rangle + \beta\|1\rangle)\|0\rangle\|1\rangle$	nessuna

La tabella evidenzia come i due bit ausiliari siano in realtà ridondanti, potendo il tipo di correzione richiesto (un NOT o nessuna correzione) essere codificato in un solo bit. I due bit "ricordano" in realtà molto di più del necessario, ovverosia il numero di errori (zero o uno) e la posizione esatta dell'errore. Ciò è dovuto al fatto che ad ogni possibile errore corrisponde uno stato ortogonale nello spazio di tre bit. Una codifica più concisa passa perciò attraverso l'abbandono del vincolo di ortogonalità, che è attualmente uno degli obiettivi di ricerca perseguiti da A. Ekert e dai suoi colleghi all'Università di Oxford.

“Trasmissione” nel tempo

I codici di correzione di errore sono stati qui descritti in relazione alla trasmissione di stati quantici tra due località distinte nello spazio, come è ad esempio il caso della crittografia quantistica. Tuttavia, un’altra interessante area di applicazione è costituita dalla conservazione nel tempo di uno stato quantico. I codici di correzione di errore permettono infatti, mediante successivi processi di codifica e di decodifica, di proteggere un sistema dall’interazione con l’ambiente per un tempo teoricamente arbitrario. Una delle applicazioni che al momento vengono prese in considerazione è ad esempio il prolungamento del tempo di decoerenza degli ioni intrappolati utilizzati per stabilire gli standard di frequenza, che porterebbe ad una diminuzione della larghezza naturale delle bande dovuta al principio di indeterminazione e quindi ad un miglioramento nella precisione degli standard [Itano].

Il teletrasporto quantistico

La dicitura "*teletrasporto quantistico*" è stata introdotta nel 1993 da C. H. Bennett ed altri per indicare un protocollo di comunicazione che metta in grado due interlocutori distanti fra loro in possesso di sistemi quantistici identici di trasferire dall'uno all'altro sistema un generico stato, in modo tale che il sistema del destinatario si trovi, alla fine, nello stesso stato in cui si trovava all'inizio il sistema del mittente ([Bennett], [Bennett7], [Davidovich]). Una simile trasmissione dello stato è stata a lungo ritenuta impossibile, in quanto in generale non esiste alcuna osservazione in grado di estrarre "tutta" l'informazione sullo stato di un sistema. Supponiamo ad esempio che Alice abbia una particella di spin ½ od un fotone in uno stato incognito $|\phi\rangle$ e voglia trasmettere a Bob l'informazione sufficiente per prepararne uno identico. Lo sviluppo di $|\phi\rangle$ su una base ortogonale servirebbe chiaramente allo scopo, ma disgraziatamente non esiste modo per ricavarlo. Soltanto se Alice *sa già* che $|\phi\rangle$ è uno degli stati di una certa base ortogonale può compiere una misura che consenta a Bob di ricostruirlo esattamente. Se invece $|\phi\rangle$ può essere uno fra due o più stati non ortogonali, nessun processo di misura fornirà una informazione sufficiente a ricreare lo stato.

Un metodo banale per trasferire l'informazione completa su $|\phi\rangle$ consiste chiaramente nel prendere la particella stessa ed inviarla a Bob. Alice può anche fare evolvere la sua particella congiuntamente con un sistema ausiliario, inizialmente in uno stato noto $|a_0\rangle$, in modo tale che dopo l'interazione la particella originale sia lasciata nello stato convenzionale $|\phi_0\rangle$ e il sistema ausiliario sia nello stato incognito $|a\rangle$ che codifica l'informazione completa su $|\phi\rangle$. Se ora Alice invia a Bob il sistema ausiliario, cosa che può essere tecnicamente più fattibile che non trasportare la particella originale, questi sarà in grado di invertire il procedimento per ricostruire una copia di $|\phi\rangle$. Questi metodi hanno in

comune il fatto che tutta l'informazione su $|\phi\rangle$ viene veicolata da un'unica trasmissione su un canale quantistico. Il teletrasporto quantistico permette invece di scorporare l'informazione su uno stato in una parte puramente classica ed una intrinsecamente quantistica, che vengono trasmesse utilizzando rispettivamente un canale classico e la correlazione non-locale di una coppia di particelle. Questo "teletrasporto" non viola alcune delle leggi fisiche; in particolare non può avvenire istantaneamente, in quanto comporta l'invio di un segnale classico. Esso distrugge inoltre lo stato originale di Alice e non permette quindi di ricavare "tutta" l'informazione su $|\phi\rangle$ osservandone un numero arbitrario di copie, cosa che contrasterebbe con il principio di indeterminazione.

Illustriamo ora come teletrasportare lo stato $|\phi\rangle$ di una particella di spin ½. La parte non classica viene trasmessa per prima. Per fare ciò, Alice prepara due particelle di spin ½ nello stato EPR di singoletto

$$\left|\Psi_{23}^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_2\right\rangle\left|\downarrow_3\right\rangle - \left|\downarrow_2\right\rangle\left|\uparrow_3\right\rangle\right).$$

Gli indici 2 e 3 identificano le particelle così preparate, mentre la particella originale di Alice, il cui stato deve essere teletrasportato, sarà indicata con l'indice 1.

Alice trattiene la particella numero due e consegna la numero tre a Bob. Anche se tali particelle presentano una correlazione non classica esse non contengono, al momento, alcuna informazione su $|\phi\rangle$; Bob può anzi prelevare la sua particella prima ancora che lo stato $|\phi\rangle$ venga creato. Quando Alice ottiene la particella incognita e decide di teletrasportarla il sistema complessivo si trova nello stato fattorizzabile $\left|\phi_1\right\rangle\left|\psi_{23}^{(-)}\right\rangle$, che non presenta correlazioni classiche né quantistiche fra la particella 1 e la coppia EPR. Fino a quel momento, perciò, nessuna misura separata o congiunta sulle particelle 2 e 3 può fornire alcuna informazione su $|\phi\rangle$.

Per correlare la prima particella con la coppia EPR Alice proietta il sistema costituito dalle particelle numero 1 e 2 sulla base ortonormale degli stati di Bell, formata da $\left|\psi_{12}^{(-)}\right\rangle$ e dagli stati

$$\left|\Psi_{12}^{(+)}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|\uparrow_1\right\rangle\left|\downarrow_2\right\rangle+\left|\downarrow_1\right\rangle\left|\uparrow_2\right\rangle\right) \qquad \text{e} \qquad \left|\Phi_{12}^{(\pm)}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|\uparrow_1\right\rangle\left|\uparrow_2\right\rangle\pm\left|\downarrow_1\right\rangle\left|\downarrow_2\right\rangle\right).$$

E' conveniente scrivere lo stato incognito $|\phi\rangle$ come

$$\left|\phi_1\right\rangle=\alpha\left|\uparrow_1\right\rangle+\beta\left|\downarrow_1\right\rangle,$$

dove $|\alpha|^2+|\beta|^2=1$. Lo stato completo delle tre particelle prima che Alice le misuri è così

$$\left|\Pi_{123}\right\rangle=\frac{\alpha}{\sqrt{2}}\left(\left|\uparrow_1\right\rangle\left|\uparrow_2\right\rangle\left|\downarrow_3\right\rangle-\left|\uparrow_1\right\rangle\left|\downarrow_2\right\rangle\left|\uparrow_3\right\rangle\right)+\frac{\beta}{\sqrt{2}}\left(\left|\downarrow_1\right\rangle\left|\uparrow_2\right\rangle\left|\downarrow_3\right\rangle-\left|\downarrow_1\right\rangle\left|\downarrow_2\right\rangle\left|\uparrow_3\right\rangle\right).$$

In questa equazione ogni prodotto tensoriale della forma $\left|\ _1\right\rangle\left|\ _2\right\rangle$ può essere espresso in termini degli stati $\left|\Psi_{12}^{(\pm)}\right\rangle$ e $\left|\Phi_{12}^{(\pm)}\right\rangle$, ottenendo in tal modo

$$\begin{aligned}\left|\Pi_{123}\right\rangle=\frac{1}{2}\Big[&\left|\Psi_{12}^{(-)}\right\rangle\left(-\alpha\left|\uparrow_3\right\rangle-\beta\left|\downarrow_3\right\rangle\right)+\left|\Psi_{12}^{(+)}\right\rangle\left(-\alpha\left|\uparrow_3\right\rangle+\beta\left|\downarrow_3\right\rangle\right)+\\&+\left|\Phi_{12}^{(-)}\right\rangle\left(\alpha\left|\downarrow_3\right\rangle+\beta\left|\uparrow_3\right\rangle\right)+\left|\Phi_{12}^{(+)}\right\rangle\left(\alpha\left|\downarrow_3\right\rangle-\beta\left|\uparrow_3\right\rangle\right)\Big].\end{aligned}$$

Ne segue che, a prescindere da $\left|\phi_1\right\rangle$, i possibili risultati dell'osservazione sono equiprobabili, avendo ciascuno probabilità 1/4. La particella 3 di Bob viene proiettata sullo stato che moltiplica, nell'equazione precedente, lo stato di Bell ottenuto da Alice con la misura, ovvero su uno dei quattro stati

$$-\left|\phi_3\right\rangle\equiv-\begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \qquad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\left|\phi_3\right\rangle, \qquad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\left|\phi_3\right\rangle \qquad \text{o} \qquad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\left|\phi_3\right\rangle.$$

Ognuno di questi possibili esiti permette a Bob di ricavare facilmente lo stato $|\phi\rangle$ che Alice intendeva teletrasportare. Nel caso che Alice abbia proiettato le sue particelle sul singoletto la particella di Bob si trova, a meno di un fattore di fase, nello stato $|\phi\rangle$. Negli altri tre casi Bob deve applicare uno dei tre operatori unitari

che compaiono nell'espressione sopra riportata e che corrispondono, a meno di un fattore di fase, alle matrici di Pauli.

Per completare il teletrasporto, Alice informa Bob mediante un canale classico del risultato della sua misura; ricevuto il messaggio Bob effettuare la rotazione appropriata, mettendo così la propria particella nello stato $|\phi\rangle$. Ad Alice rimangono solo le particelle 1 e 2 ormai in uno degli stati $|\Psi_{12}^{(\pm)}\rangle$ o $|\Phi_{12}^{(\pm)}\rangle$, senza più alcuna traccia di $|\phi\rangle$; la particella 2 di Alice, in particolare, non è più correlata con la particella 3 di Bob.

Diversamente dalla correlazione non locale della coppia EPR formata dalla particella 2 di Alice e dalla particella 3 di Bob, il risultato della misura di Alice costituisce un'informazione puramente classica che può essere trasmessa, copiata o memorizzata su qualunque supporto. Tale informazione non deve inoltre essere distrutta o cancellata per completare l'operazione di teletrasporto. I due bit classici necessari per distinguere fra i quattro esiti equiprobabili della misura rappresentano quindi una sorta di sottoprodotto del trasferimento; il loro contenuto è completamente casuale e non è in alcun modo correlato con lo stato $|\phi\rangle$.

Il ruolo dei due bit di informazione classica è cruciale nel teletrasporto. Supponiamo infatti che Bob sia impaziente e voglia utilizzare la sua particella senza attendere l'arrivo del messaggio classico. Quella che egli ha in mano è però una sovrapposizione incoerente con probabilità 1/4 dei quattro possibili stati finali, descritta dalla matrice densità

$$\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

corrispondente ad uno stato totalmente non polarizzato e quindi del tutto inutile per ottenere informazioni su $|\phi\rangle$.

Ci si può ora domandare se vi sia arbitrarietà nella scomposizione dell'informazione su $|\phi\rangle$ in una parte classica ed una quantistica. E' possibile dimostrare che la trasmissione dello stato di una particella di spin ½ richiede esattamente due bit di informazione classica. Se il teletrasporto fosse realizzabile con un canale classico di capacità minore si avrebbe infatti la possibilità di trasferire messaggi a velocità superiore a quella della luce indovinandone il contenuto prima che essi arrivino a destinazione ([Bennett6], [Bennett7]).

Per quanto riguarda la parte quantistica, si dimostra che gli unici stati correlati delle particelle 2 e 3 che lasciano quest'ultima in uno stato legato a $|\phi\rangle$ da una trasformazione unitaria tra quattro fissate sono della forma

$$\frac{1}{\sqrt{2}}\left(|u_2\rangle|p_3\rangle+|v_2\rangle|q_3\rangle\right),$$

dove $\{|u\rangle,|v\rangle\}$ e $\{|p\rangle,|q\rangle\}$ sono due coppie di stati ortogonali. Si tratta, come per il singoletto, di stati completamente correlati, che danno luogo a risultati del tutto casuali per misure effettuate su una delle due particelle separatamente. Tali stati possono essere ottenuti a partire da un singoletto effettuando una trasformazione unitaria su una sola delle due particelle.

Alla luce delle precedenti considerazioni, il teletrasporto comporta una ripartizione dell'informazione tra classica e quantistica sostanzialmente univoca, che sembra caratterizzare intrinsecamente il contenuto informativo di uno stato quantistico.

Il principale ostacolo alla realizzazione pratica del teletrasporto risiede attualmente nell'impossibilità di conservare le particelle EPR per più di qualche istante. Qualora Alice e Bob fossero in grado di mantenere abbastanza a lungo una serie di coppie EPR non eccessivamente degradate dal rumore, applicando localmente delle trasformazioni unitarie alle proprie particelle potrebbero in qualunque momento "distillare" dalle loro scorte un numero inferiore di stati di singoletto arbitrariamente puri [Bennett8]. A quel punto, Alice potrebbe

teletrasportare stati quantistici a Bob senza alcun problema di attenuazione o di rumorosità del canale quali si avrebbero, ad esempio, per un fotone inviato lungo una fibra ottica. L'unico requisito resterebbe la possibilità di trasmettere dei robusti segnali classici. Di più, il teletrasporto rimarrebbe possibile anche nel caso in cui Alice e Bob ignorassero ciascuno la posizione dell'altro; sarebbe infatti sufficiente che Alice facesse giungere il messaggio classico in tutti i luoghi dove Bob potrebbe trovarsi, cosa che sarebbe chiaramente impossibile a farsi se si dovesse inviare direttamente la particella originale.

Conclusione

Al termine di questa trattazione della crittografia e della computazione quantistica sembra opportuno tentare alcune riflessioni di carattere generale, per quanto soggettive e quindi parziali, sul futuro di questi settori di ricerca.

La crittografia quantistica si trova al presente in una situazione privilegiata per quanto riguarda le possibilità realizzative. Alcune implementazioni sperimentali sono state direttamente realizzate dalle grandi società di telecomunicazioni; la ricerca di protocolli crittografici sicuri è supportata da interessi economici, politici e strategici tanto forti da fare sperare in un rapido sviluppo delle tecnologie richieste per una realizzazione su vasta scala. D'altra parte, la teoria della crittografia quantistica è fondata su conoscenze da tempo acquisite nell'ambito della meccanica quantistica e della teoria dell'informazione, e costituisce pertanto un quadro abbastanza completo. I tempi sembrano dunque maturi perché lo studio delle applicazioni assuma una importanza predominante nel settore.

Lo stato della computazione quantistica appare al contrario più problematico. La realizzazione pratica del calcolatore quantistico è molto al di là dello stato dell'arte, ed anche a livello teorico rimangono aperte questioni di

fondo sulla realizzabilità di un controllo abbastanza fine di sistemi quantistici reali affetti da rumore. A parte queste considerazioni, però, rimane il fatto che la teoria quantistica della computazione è un campo ancora largamente inesplorato. L'algoritmo di Shor, pur costituendo di per sé, anche grazie alle sue implicazioni nei confronti della crittografia a chiave pubblica, una valida spinta verso la realizzazione del calcolatore quantistico, rappresenta tuttavia al presente un risultato isolato: le potenzialità del parallelismo quantistico rimangono in gran parte incognite.

Alla luce delle precedenti considerazioni emerge una duplice direttiva di sviluppo per il calcolo quantistico. La prima, forse al momento più seguita, è quella guidata dallo studio delle implementazioni, che potrà in futuro facilitare anche lo sviluppo di nuovi algoritmi ancorandoli ad un modello di calcolo più specifico, perché vicino ai dispositivi fisici reali. La seconda, non meno importante, è rappresentata dallo studio degli algoritmi realizzabili mediante generiche trasformazioni unitarie. Se la fattorizzazione degli interi è un'importante conquista, il vero obiettivo che all'orizzonte si profila è la classe dei problemi **NPC**. Contro tale ostacolo l'intelligenza artificiale ha inutilmente esaurito i suoi sforzi, rinunciando via via a tutte le mete più ambiziose. Se il futuro calcolo quantistico si rivelasse almeno teoricamente capace di affrontare tali problemi, la questione della sua implementazione pratica diverrebbe prioritaria.

Già al presente, tuttavia, si stanno raccogliendo i frutti dell'incontro tra la teoria dell'informazione e la meccanica quantistica. Idee come il teletrasporto quantistico gettano nuova luce sul paradosso EPR e sulla natura stessa delle limitazioni che la meccanica quantistica impone alla nostra conoscenza dello stato dei sistemi. Possiamo quindi concludere che, come auspicato nel 1981 da R. P. Feynman [Feynman2], il "*computer-type of thinking*" si è rivelato ancora una volta prodigo di nuove idee.

Ringraziamenti

Si ringraziano il Relatore Prof. Dott. Enrico Beltrametti ed il Dott. Giovanni Costantini per la costante disponibilità dimostrata ed il prezioso aiuto fornito nello studio di questi argomenti.